

**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:

KBK:

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 manfaatlarini 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 kengashining 28.10.2025 yildagi 3-sonli yig'ilish bayonnomasi tomonidan nashrga tavsiya etilgan.

ISBN

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, mintaq 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 kampa-niyalari 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'moqda 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 oqim-larini va shaxsiy ma'lumotlarni nazorat qilishga intilmoqda. Masalan, Xitoy "Buyuk xavfsizlik devori" orqali internetni qat-tiq nazorat qilsa, Yevropa Ittifoqi GDPR qonunlari orqali shax-siy ma'lumotlarni himoya qilmoqda. Bu esa global boshqaruv mexanizmlari va milliy siyosatlar o'rtasida ziddiyatlarni kelti-rib 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 tash-abbuslar O'zbekistonning global jarayonda faol ishtirok etishi-ni 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'yimoqda².

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-qimmat, 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 ishlayotganidir. 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 dolzarblik.

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 oqibatlari 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 kiberxavfsizlik: raqamli iqtisodiyotni himoya qilish" (2024) maqolasida kiberjinoatlarga 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 kiberxavfsizlik 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 kiberxavfsizlik: 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 gibril 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, "Raqqamli 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 qoraladi.

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 muvofiqlashtirish 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.

I-BOB KIBERMAKON XAVFSIZLIGINI TA'MINLASHNING NAZARIY VA METODOLOGIK ASOSLARI

Kibermakon xavfsizligini ta'minlashning nazariy va metodologik asoslari nomli bobimizda kibermakon fenomenining falsafiy va huquqiy talqinlari, xavfsizlik paradigmalari hamda zamonaviy kiberxavf turlari tahlil qilinadi. Kibermakon tushunchasi dastlab adabiyot va texnologiya chorrahasida shakllangan bo'lsa-da, bugungi kunda u global ijtimoiy, siyosiy va huquqiy makonga aylangan. Manuel Castellsning "oqimlar makoni" nazariyasi va Luciano Floridining "infosfera" konsepsiyasi asosida kibermakon insoniyat borligining yangi o'lchovi sifatida ko'riladi. Shu bilan birga, Jean Baudrillardning "simulyakr" nazariyasi kibermakonni haqiqat va virtual chegaralarini yo'qotuvchi hodisa sifatida talqin qiladi.

Huquqiy jihatdan kibermakon milliy suverenitet va xalqaro huquqiy tartibotlar o'rtasidagi murakkab munosabatlarni yuzaga chiqaradi. John Perry Barlowning mashhur "Cyberspace Declaration" bayonoti kibermakonni davlatlardan mustaqil hudud sifatida ko'rsatgan bo'lsa, xalqaro huquq (Budapest Konvensiyasi, BMT OEWG, Tallinn qo'llanmasi) uni davlatlar va xalqaro institutlar tomonidan boshqarilishi lozim bo'lgan makon sifatida belgilaydi. Shu bois kibermakon huquqiy jihatdan pluralistik — qonunlar, me'yorlar, bozor mexanizmlari va texnologik arxitektura birgalikda amal qiladigan tizimdir.

Bobning ikkinchi qismida kibermakon xavfsizligi paradigmalari ko'rib chiqiladi. Realistik paradigma xavfsizlikni milliy manfaatlar asosida tushuntirsa, liberal paradigma xalqaro hamkorlikka urg'u beradi. Konstruktivistik yondashuv xavfsizlikni ijtimoiy konstruksiya sifatida talqin qiladi, texnotsentrik paradigma esa texnologiyani asosiy vosita deb biladi. Shuningdek, ilmiy konsepsiyalar – Cybersecurity Dynamics, Infosfera nazariyasi, kiber suverenitet modeli va xalqaro boshqaruv mexanizmlari – kibermakon xavfsizligini nazariy jihatdan asoslashga xizmat qiladi.

Yakuniy qismda zamonaviy kiberxavflar tahlil qilinadi. Kiberterrorizm jamiyatni qo'rquvga soluvchi va infratuzilmalarga hujum qiluvchi hodisa sifatida, kiberjinoyat esa iqtisodiy va shaxsiy xavfsizlikni izdan chiqaruvchi transchegaraviy hodisa sifatida baholanadi. Kiberpropaganda esa jamiyatni bo'lish, siyosiy jarayonlarga ta'sir o'tkazish va xalqaro munosabatlarda beqarorlik keltiruvchi vosita sifatida ko'rsatiladi.

Shunday qilib, bob kibermakonning ko'p qirrali mohiyatini — falsafiy, huquqiy va xavfsizlik paradigmalari doirasida — izchil tahlil qilib, zamonaviy tahdidlar manzarasini yoritadi hamda keyingi boblarda davlatlar tajribasini o'rganish uchun nazariy poydevor yaratadi.

1.1. Kibermakon tushunchasi va uning falsafiy-huquqiy talqini

Zamonaviy davrda kibermakon (cyberspace) tushunchasi nafaqat texnik jihatdan balki falsafiy va huquqiy nuqtai nazardan ham chuqur tahlil etilmoqda. Ushbu bo'limda kibermakon fenomenining mohiyati, virtual makon sifatida uning okshashliklari va farqlari, shuningdek undan kelib chiqadigan huquqiy muammolarni ko'rib chiqamiz.

William Gibsonning "Neuromancer" romanida "cyberspace" atamasi ilk bor adabiy asarda paydo bo'lib, hozirgi kiberreal muhit haqida metaforik tasavvur yaratdi. Bu atama "ekranlar va parollar bilan chegaralangan makon"ni anglatadi, real geografik chegaralar emas, balki virtual ko'rinishdagi makon mavjudligiga urg'u beradi¹. Ushbu nazariy kontseptsiya kiberxavfsizlik va huquq munozaralarida asosiy bosqichlardan biriga aylandi.

Falsafiy-huquqiy talqinlar

- John Perry Barlow 1996-yilda e'lon qilgan "A Declaration of the Independence of Cyberspace" asarida shunday deydi:

¹ William Gibson, Neuromancer, (1984), adabiy asar. "...space bounded by screens and passwords rather than physical markers".

“...Cyberspace does not lie within your borders... You have no moral right to rule us”¹. Bu yerda kibermakonni an’anaviy davlat suvereniteti doirasidan mustaqil, o’z ijtimoiy shartlariga asoslangan huquqiy makon ekanini ifodalaydi.

- A. Czosseck esa kibermakon tushunchasini davlatlar milliy strategiyalarini shakllantirishi uchun zarur bo’lgan nazariy platforma sifatida ko’rib, quyidagicha ta’kidlaydi: “there has to be a theory that defines all the different concepts that exist and cohabit in the cyber domain”². Unga ko’ra, kiberxavfsizlik strategiyalari faqat texnik choralarga emas, balki kibermakon tushunchalarining aniq ta’riflanishiga asoslanishi zarur.

- K. A. Ivanova, M. Myltykbaev va D. D. Shtodina yozishicha, kibermakon — bu “...unique mode of physical and virtual objects, hardware and software services... all computer networks... including the Internet”³. Ular kibermakon kontseptsiyasini kengroq, nafaqat Internet balki barcha kompyuter tarmoqlaridan tashkil topgan makon sifatida tasavvur qilish zarurligini ta’kidlaydi.

- Lessignig fikricha, kibermakonni faqat huquqiy kod emas, balki “architectural code” ham boshqaradi. U o’zining “Code and Other Laws of Cyberspace” asarida shunday yozadi: “there are actually four major regulators (Law, Norms, Market, Architecture)”⁴.

- S. Savaş (2022) esa kibermakonni shunday ta’riflaydi:

¹ John Perry Barlow, A Declaration of the Independence of Cyberspace, (online, 1996), bet: umumiy mazmun. “...Cyberspace does not lie within your borders... You have no moral right to rule us”

² C. Czosseck, Getting the Essence of Cyberspace: A Theoretical Framework to Face Cyber Issues, CCDCOE, (2008), bet: 113-114. “...there has to be a theory that defines all the different concepts that exist and cohabit in the cyber domain”

³ K. A. Ivanova, M. Myltykbaev, D. D. Shtodina, The concept of cyberspace in international law, Law Enforcement Review 6(4):32-44, (Moscow, RN, 2022), bet: 32-44. “...unique mode of physical and virtual objects, hardware and software services... all computer networks... including the Internet”.

⁴ Lawrence Lessig, Code and Other Laws of Cyberspace, (Basic Books, 1999), bet: umumiy mazmun. “...there are actually four major regulators (Law, Norms, Market, Architecture)”

“Cyberspace means the environment that consists of information systems spread all over the world and space and the networks that connect them”¹. U bu atamani kengroq “kibermuhit”, “kiberzona” shaklida ham ishlatadi, bu ham kibermakonning bir necha terminlar orqali tasvirlanishini ko'rsatadi.

- Kibermakon tushunchasining o'zagi — bu geografik chegarasi bo'lmagan, virtual-fizik elementlardan tashkil topgan makondir. Bunday makon real makonga nisbatan suverenitet va huquqiy nazorat masalalarida yangi muammolarni yuzaga keltiradi.

- Falsafiy talqin kontekstida, kibermakon an'anaviy davlat amirligidan mustaqil bo'lishi mumkinligi, yurisdiksiyaning qayta ko'rib chiqilishi lozimligi mulohaza etiladi (Barlow).

- Huquqiy nazariya asosida, kibermakonda faqat qonunlar emas, balki me'yorlar, bozor kuchlari va texnologiya—“code/architecture” ham — harakatlarni tartibga soladi, ya'ni kiberhududni faqat bir yondashuv bilan emas, balki kompleks nazorat orqali o'rganish zarur.

- Tushunchaning keng doirasi (Ivanova va boshq.; Savaş) — kibermakon Internet bilan chegaralanmaydi, balki barcha tarmoqlarni qamrab oladi, bu esa nazariy va amaliy tahlilda muhimdir.

Kibermakonni tushunishda falsafaning ikki muhim yo'nalishi — ontologiya va epistemologiya — markaziy ahamiyat kasb etadi. Ontologiya “borliq nima?” degan savolga javob izlaydi, epistemologiya esa “biz uni qanday bilamiz?” masalasini o'rganadi. Shu jihatdan qaralganda, kibermakonning tabiatini anglash faqat texnologik tahlil bilan emas, balki falsafiy asos bilan ham bog'lanadi.

Ontologik nuqtai nazardan kibermakon — bu o'ziga xos “yangi borliq” bo'lib, real va virtual elementlarning sintezi

¹ S. Savaş, Cyber governance studies in ensuring cybersecurity, PMC, (2022), bet: umumiy mazmun. “Cyberspace means the environment that consists of information systems spread all over the world and space and the networks that connect them”

sifatida ko'riladi. Manuel Castells o'zining *The Rise of the Network Society* asarida shunday ta'kidlaydi: «the space of flows is the material organization of time-sharing social practices that work through flows»¹. Demak, kibermakon nafaqat texnik tizimlar yig'indisi, balki ijtimoiy amaliyotlarning oqimlar orqali qayta tashkil etilgan shaklidir.

Shu ma'noda, kibermakon "ontologik ikkiyuzlama"ga ega: u ham real dunyoga bog'langan (fizik serverlar, texnik infratuzilma orqali), ham virtual dunyoda mavjud (raqamli identitet, ma'lumot oqimlari shaklida). Shuning uchun A. Floridi uni "infosfera" deb ataydi: «the infosphere is the totality of informational entities, their properties, interactions, processes and mutual relations»².

Epistemologik yondashuv kibermakonni qanday bilishimiz mumkinligi bilan bog'liq. Shouhuai Xu bu haqda shunday yozadi: «Cybersecurity dynamics is about modeling, analysis, quantification, and management of cybersecurity from a holistic perspective»³. Bu ta'rif kibermakondagi bilimni tizimli, ilmiy va modellashtirish asosida tushunishga yo'naltirilgan.

Epistemologik nuqtai nazardan muammo shundaki, kibermakon o'zgaruvchan, chegarasiz va dinamik bo'lgani uchun uni to'liq bilish imkonsizdir. Shu sababdan, kibermakonni o'rganishda ko'proq ko'p fanli yondashuvlar (huquq, sotsiologiya, informatika, falsafa) zarur bo'ladi.

Falsafiy bahslarning markazida shunday savol turadi: kibermakon "haqiqat"mi yoki "virtuallikmi"? Jean Baudrillard "Simulacra and Simulation" asarida shunday yozadi: «the

¹ Manuel Castells, *The Rise of the Network Society*, Oxford: Blackwell, 1996, bet: 412. «the space of flows is the material organization of time-sharing social practices that work through flows».

² Luciano Floridi, *The Philosophy of Information*, Oxford University Press, 2011, bet: 53. «the infosphere is the totality of informational entities, their properties, interactions, processes and mutual relations».

³ Shouhuai Xu, *Cybersecurity Dynamics: A Foundation for the Science of Cybersecurity*, arXiv preprint, 2020, bet: umumiy mazmun. «Cybersecurity dynamics is about modeling, analysis, quantification, and management of cybersecurity from a holistic perspective».

simulacrum is never that which conceals the truth—it is the truth which conceals that there is none»¹. Demak, kibermakon “simulyakr” bo‘lib, real haqiqatni emas, balki uning nusxasini aks ettiradi. Bu nuqtai nazar kibermakonni “haqiqiy borliq” sifatida emas, balki “ijtimoiy-ma’naviy konstruksiya” sifatida talqin qiladi.

Shu bilan birga, Mark Poster ta’rificha, «cyberspace is a new kind of space in which human beings communicate with one another, create identities, and construct communities»². Bu yondashuv kibermakonni faqat texnologik emas, balki ijtimoiy borliq sifatida tasdiqlaydi.

Kibermakonni tushunishda ontologiya va epistemologiya bir-birini to‘ldiradi: ontologik jihatdan kibermakon real-virtual makon sifatida mavjud bo‘lsa, epistemologik jihatdan uni bilish jarayoni har doim nisbiy, fragmentar va konstruktsiyalangan bo‘ladi.

Falsafiy jihatdan tahlil qilgan holda kibermakon haqida quyidagi xulosalarni beramiz:

1. Kibermakonning ontologiyasi uning real va virtual komponentlarning sintezidan iborat ekanini ko‘rsatadi (Castells, Floridi).

2. Epistemologik nuqtai nazar esa kibermakonni bilishning doimo chegaralanganligini, ammo ko‘p fanli yondashuv orqali uni tahlil qilish mumkinligini anglatadi (Xu).

3. Falsafiy muammo sifatida kibermakon “simulyakr” (Baudrillard) bo‘lishi mumkin, lekin ijtimoiy jihatdan yangi identitet va hamjamiyatlarni vujudga keltiradigan real makondir (Poster).

Shunday qilib, kibermakonni faqat texnik infratuzilma sifatida emas, balki falsafiy borliq va bilim maydoni sifatida

¹ Jean Baudrillard, *Simulacra and Simulation*, University of Michigan Press, 1994, bet: 1. «the simulacrum is never that which conceals the truth—it is the truth which conceals that there is none».

² Mark Poster, *CyberDemocracy: Internet and the Public Sphere*, in *Reading Digital Culture*, Blackwell, 2001, bet: 259. «cyberspace is a new kind of space in which human beings communicate with one another, create identities, and construct communities».

ham ko'rish zarur.

Kibermakonni tushunishda huquqiy vjihatlar va suverenitet masalalariga ham alohida e'tibor qaratish lozim. Kibermakonning huquqiy talqini zamonaviy davlatlar uchun eng dolzarb masalalardan biridir. Chunki kibermakon geografik hudud bilan cheklanmagan, biroq davlat yurisdiksiyasi asosan hududiy tamoyillarga asoslanadi. Bu masalada Jon Perri Barlowning mashhur bayonoti asosiy nuqtani ko'rsatadi: «... Cyberspace does not lie within your borders... You have no moral right to rule us»¹. Bu yondashuv kibermakonni milliy davlatlardan mustaqil, o'z-o'zini boshqaradigan hudud sifatida ko'rsatadi.

Shu bilan birga, ko'plab zamonaviy huquqshunoslar kibermakonni davlat yurisdiksiyasi bilan chambarchas bog'lash zarurligini ta'kidlashadi. Masalan, K.A. Ivanova, M. Myltykbaev va D.D. Shtodina ta'rificha, kibermakon ««...unique mode of physical and virtual objects, hardware and software services... all computer networks... including the Internet»»². Ularning fikricha, agar kibermakon real va virtual infratuzilmaga ega bo'lsa, demak uni milliy huquqiy tizimlar orqali tartibga solish ham mumkin.

Kibermakonda suverenitet masalasi xalqaro huquqda eng bahsli nuqtalardan biridir. Xalqaro Huquq Assotsiatsiyasi (ILA) tomonidan tayyorlangan hujjatlarda ta'kidlanishicha: «States have sovereignty over cyber infrastructure located within their territory»³. Bu yondashuvga ko'ra, agar server yoki texnik vosita bir davlat hududida joylashgan bo'lsa, u holda mazkur davlat

¹ John Perry Barlow, A Declaration of the Independence of Cyberspace, 1996, online manba. «...Cyberspace does not lie within your borders... You have no moral right to rule us».

² K.A. Ivanova, M. Myltykbaev, D.D. Shtodina, The concept of cyberspace in international law, Law Enforcement Review 6(4):32-44, Moscow, 2022, bet: 33. «...unique mode of physical and virtual objects, hardware and software services... all computer networks... including the Internet».

³ International Law Association, Report on State Responsibility in Cyberspace, 2018, bet: 5. «States have sovereignty over cyber infrastructure located within their territory».

ularning ustidan to'liq suverenitetga ega. Biroq amaliyotda bu tamoyil juda murakkab. Chunki ma'lumotlar oqimi transchegaraviy xususiyatga ega. Masalan, bir foydalanuvchi O'zbekistonda ijtimoiy tarmoqdan foydalansa, lekin server AQShda joylashgan bo'lsa, kimning yurisdiksiyasi ustuvor bo'lishi kerak? Bu savol hanuzgacha xalqaro huquqdagi eng katta muammolardan biri bo'lib qolmoqda.

Lawrence Lessig kibermakon huquqini faqat qonunlar emas, balki "me'yorlar, bozor va arxitektura" ham tartibga solishini ko'rsatadi: «...there are actually four major regulators (Law, Norms, Market, Architecture)»¹. Demak, kibermakonni huquqiy jihatdan boshqarish faqat milliy qonunchilik doirasida emas, balki global iqtisodiy kuchlar, jamiyat madaniyati va texnologiyaning o'zi orqali ham amalga oshadi.

BMTning "Developments in the field of information and telecommunications in the context of international security" nomli rezolyutsiyalarida kibermakon xavfsizligi xalqaro tinchlik va xavfsizlikka tahdid sifatida ko'riladi². NATO va Yevropa Ittifoqi ham o'z strategiyalarida kibermakonni alohida xavfsizlik sohasi sifatida belgilashgan. Shu bois, kibermakon huquqiy talqinida xalqaro hamkorlik asosiy tamoyil hisoblanadi.

Kibermakon faqat davlat suvereniteti emas, balki inson huquqlari bilan ham bevosita bog'liqdir. Masalan, Yevropa Ittifoqining GDPR (General Data Protection Regulation) qonuni shaxsiy ma'lumotlarni himoya qilishni markaziy masala sifatida ko'radi: «...protection of natural persons with regard to the processing of personal data and on the free movement of

¹ Lawrence Lessig, *Code and Other Laws of Cyberspace*, Basic Books, New York, 1999, bet: 86. «...there are actually four major regulators (Law, Norms, Market, Architecture)».

² United Nations, *Developments in the field of information and telecommunications in the context of international security*, UNGA Resolutions, 2015–2021.

such data»¹. Bu ko'rsatadi-ki, kibermakonni huquqiy tartibga solishda davlat manfaatlari bilan bir qatorda inson erkinliklari ham hisobga olinishi shart.

Kibermakon fenomeni bugungi globallashuv va raqamli jamiyat davrida nafaqat texnologik, balki falsafiy va huquqiy muammo sifatida qaralmoqda. U haqidagi turli konsepsiyalarni tahlil qilish shuni ko'rsatadiki, kibermakonning mohiyati ko'p qirrali va murakkabdir.

Birinchidan, falsafiy talqinlarda kibermakon insoniyatning yangi borliq shakli sifatida qaraladi. Manuel Castells ta'riflaganidek, «the space of flows» – ya'ni oqimlar makoni – ijtimoiy amaliyotlarni vaqt va makondan mustaqil ravishda qayta tashkil etuvchi borliqdir. Shu bilan birga, Luciano Floridi uni «infosfera» deb atab, barcha axborot mavjudotlari va ularning o'zaro aloqalaridan iborat yangi ontologik qatlam sifatida ko'rsatadi.

Ikkinchidan, bu falsafiy qarashlar kibermakonni inson tajribasining yangi o'lchovi sifatida tan olishga undaydi. Biroq Jean Baudrillard nazarida, bu makon ko'pincha “simulyakr” bo'lib, real haqiqatni emas, balki uning virtual nusxasini aks ettiradi: «the simulacrum is never that which conceals the truth—it is the truth which conceals that there is none». Demak, kibermakonning ontologiyasi bahsli – u haqiqiy borliq sifatida ham, sun'iy konstruksiya sifatida ham talqin qilinishi mumkin.

Uchinchidan, Epistemologik jihatdan kibermakonni bilish doimo chegaralangan va fragmentar bo'lib qoladi. Shouhuai Xu ta'rificha, «cybersecurity dynamics is about modeling, analysis, quantification, and management of cybersecurity from a holistic perspective». Demak, kibermakonni bilish jarayoni faqat texnik ma'lumotlar emas, balki ko'p fanli modellashtirish orqali amalga oshiriladi. Shu sababdan falsafiy-epistemologik yondashuv kibermakonni bilishning doimiy ravishda

¹ European Parliament, General Data Protection Regulation (GDPR), Regulation (EU) 2016/679, Official Journal of the European Union, 2016, Art. 1. «...protection of natural persons with regard to the processing of personal data and on the free movement of such data».

nisbiyligini tan oladi.

To'rtinchidan, huquqiy nuqtai nazardan kibermakon an'anaviy davlat yurisdiksiyasi tushunchasini shubha ostiga qo'yadi. John Perry Barlowning mashhur deklaratsiyasi «Cyberspace does not lie within your borders» iborasi kibermakonni suverenitetdan mustaqil maydon sifatida ko'rsatadi. Lekin xalqaro huquq tamoyillari (ILA hujjatlari) davlatlarni o'z hududidagi infratuzilma ustidan suverenitetga ega deb tan oladi.

Beshinchidan, Lawrence Lessigning konsepsiyasi kibermakonni faqat qonunlar emas, balki "normlar, bozor va texnologik arxitektura" orqali ham boshqarilishini ta'kidlaydi. Bu esa huquqiy pluralizmni va global boshqaruv zaruratini anglatadi.

Oltinchidan, Yevropa Ittifoqining GDPR qonuni kibermakondagi shaxsiy ma'lumotlarni himoya qilishni markaziy masala sifatida belgilaydi: «protection of natural persons with regard to the processing of personal data». Bu shuni ko'rsatadiki, kibermakonni tartibga solishda davlat suvereniteti va inson huquqlari o'rtasidagi muvozanat asosiy falsafiy-huquqiy vazifa bo'lib qolmoqda.

Yuqoridagi ilmiy mulohazalarni umumlashtirgan holda quyidagi xulosalarni berishimiz mumkin:

1. Kibermakon falsafiy jihatdan insoniyat borligining yangi qatlamini ifodalaydi, biroq uning ontologik maqomi hanz bahsli.

2. Epistemologik jihatdan kibermakonni to'liq bilish imkonsiz, lekin ko'p fanli yondashuv uni ilmiy tahlil qilish imkonini beradi.

3. Huquqiy jihatdan kibermakon an'anaviy suverenitet tushunchasini qayta ko'rib chiqishni talab qiladi; u milliy qonunlar, xalqaro huquq, bozor mexanizmlari va texnologik arxitektura orqali tartibga solinadi.

4. Inson huquqlari, xususan shaxsiy ma'lumotlarni himoya qilish, kibermakonning falsafiy-huquqiy talqinida markaziy o'rinni egallaydi.

Shunday qilib, kibermakonni faqat texnologik tizim sifatida

emas, balki falsafiy borliq, epistemologik obyekt va huquqiy makon sifatida ko'rish zarur. Bu yondashuv kibermakon xavfsizligini ta'minlash va davlatlar tajribasini tahlil qilish uchun nazariy poydevor yaratadi.

1.2. Kibermakon xavfsizlik paradigmasi va ilmiy konsepsiyalar

Kibermakon xavfsizligi — bu nafaqat texnik muammolar, balki davlat, jamiyat va shaxs manfaatlarini himoya qilishga qaratilgan kompleks fenomendir. National Institute of Standards and Technology (NIST) shunday ta'rif beradi: «Cybersecurity is the ability to protect or defend the use of cyberspace from cyber attacks»¹. Ushbu ta'rifda kibermakon xavfsizligi hujumlardan himoya qilishga qaratilgan funksional jarayon sifatida ko'riladi.

Biroq boshqa olimlar kibermakon xavfsizligini kengroq kontekstdan talqin qilishadi. Masalan, Singer va Friedman ta'kidlaydilar: «Cybersecurity is not just about technology, but also about people, organizations, and processes»². Demak, kibermakon xavfsizligi texnologik yechimlar bilan chegaralanmaydi, balki sotsiologik va tashkiliy omillarni ham qamrab oladi.

Realistik paradigma. Xalqaro munosabatlar nazariyasida kibermakon xavfsizligi ko'pincha realistik paradigma asosida tahlil qilinadi. Bu yondashuvga ko'ra, davlatlar kibermakonda ham raqobat olib boradi va milliy manfaatlarini himoya qiladi. Nye shunday deydi: «Cyber power is the ability to obtain preferred outcomes through the use of the electronically

¹ National Institute of Standards and Technology (NIST), Cybersecurity Framework, 2018. «Cybersecurity is the ability to protect or defend the use of cyberspace from cyber attacks».

² P.W. Singer, Allan Friedman, Cybersecurity and Cyberwar: What Everyone Needs to Know, Oxford University Press, 2014, bet: 29. «Cybersecurity is not just about technology, but also about people, organizations, and processes».

interconnected information resources of the cyber domain»¹. Bu ta'rif kibermakon xavfsizligini geosiyosiy kuch sifatida talqin qiladi.

Liberal paradigma. Liberal paradigma kibermakonni xalqaro hamkorlik va qo'shma boshqaruv maydoni sifatida ko'radi. Muellerning "Networks and States" asarida bu yondashuv quyidagicha ifodalanadi: «The governance of the Internet is a complex interplay between states, private actors, and international institutions»². Demak, xavfsizlik faqat davlatlararo raqobat emas, balki hamkorlik asosida ham ta'minlanishi mumkin.

Konstruktivistik paradigma. Konstruktivistlar kibermakonda xavfsizlikni ijtimoiy konstruksiya sifatida tushuntiradi. Hansen va Nissenbaumning ta'rificha: «Cybersecurity is what states and societies make of it»³. Boshqacha qilib aytganda, kibermakonda xavfsizlik ob'ektiv hodisa emas, balki sub'ektiv qabul qilingan xavf-xatarlar asosida shakllanadi.

Texnotsentrik paradigma. Texnologiya markaziy rol o'ynaydigan yondashuvda kibermakon xavfsizligi ko'proq texnik vositalar va algoritmik himoya tizimlariga bog'liqdir. Bruce Schneier bu haqda shunday yozadi: «Security is a process, not a product»⁴. Demak, xavfsizlikni ta'minlash doimiy ravishda takomillashtiriladigan jarayon sifatida tushunilishi kerak deb quyidagilarni xulosa qilamiz:

1. Kibermakon xavfsizligi tor ma'noda hujumlardan himoya

¹ Joseph S. Nye, *The Future of Power*, PublicAffairs, New York, 2011, bet: 123. «Cyber power is the ability to obtain preferred outcomes through the use of the electronically interconnected information resources of the cyber domain».

² Milton Mueller, *Networks and States: The Global Politics of Internet Governance*, MIT Press, 2010, bet: 45. «The governance of the Internet is a complex interplay between states, private actors, and international institutions».

³ Lene Hansen, Helen Nissenbaum, *Digital Disaster, Cyber Security, and the Copenhagen School*, *International Studies Quarterly*, Vol. 53, 2009, bet: 1155. «Cybersecurity is what states and societies make of it».

⁴ Bruce Schneier, *Secrets and Lies: Digital Security in a Networked World*, Wiley, 2000, bet: 21. «Security is a process, not a product».

qilish, keng ma'noda esa ijtimoiy, siyosiy va iqtisodiy barqarorlikni ta'minlash jarayonidir.

2. Realistik paradigma xavfsizlikni milliy manfaatlar asosida, liberal paradigma esa xalqaro hamkorlik asosida tushuntiradi.

3. Konstruktivistik yondashuv kibermakonda xavfsizlikni ijtimoiy konstruksiya sifatida ko'radi.

4. Texnotsentrik yondashuv texnologiyalarni xavfsizlikning asosiy manbai sifatida talqin qiladi.

So'nggi yillarda kibermakon xavfsizligini ilmiy asosda o'rganishga qaratilgan yangi yo'nalish – Cybersecurity Dynamics paydo bo'ldi. Shouhuai Xu ta'rificha: «Cybersecurity dynamics is about modeling, analysis, quantification, and management of cybersecurity from a holistic perspective»¹. Ushbu konsepsiya kibermakon xavfsizligini matematik va tizimli modellar orqali tushuntirishga intiladi.

Xu'ning fikricha, kiberhujumlar biologik epidemiyalar kabi tarqaladi va ularni tushunish uchun murakkab tizimlarni modellashtirish zarur. Shu bois, bu yondashuv kibermakon xavfsizligini faqat hujum va himoya sifatida emas, balki dinamik muvozanat jarayoni sifatida ko'radi.

Infosfera nazariyasi. Luciano Floridi tomonidan ilgari surilgan Infosfera nazariyasi kibermakonni global axborot makoni sifatida tushuntiradi. Floridi yozadi: «the infosphere is the totality of informational entities, their properties, interactions, processes and mutual relations»².

Bu konsepsiya kibermakonda xavfsizlik masalasini nafaqat texnik tizimlarga, balki axborot mavjudotlarining ontologik maqomiga ham bog'laydi. Masalan, foydalanuvchining shaxsiy ma'lumotlari oddiy texnik resurs emas, balki axborot mavjudot sifatida muhofazaga muhtojdir. Shu sababli infosferayondashuvi

¹ Shouhuai Xu, Cybersecurity Dynamics: A Foundation for the Science of Cybersecurity, arXiv preprint, 2020. «Cybersecurity dynamics is about modeling, analysis, quantification, and management of cybersecurity from a holistic perspective».

² Luciano Floridi, The Philosophy of Information, Oxford University Press, 2011, bet: 53. «the infosphere is the totality of informational entities, their properties, interactions, processes and mutual relations».

kiberxavfsizlikni axborot etikasi bilan chambarchas bog'laydi.

Kibersuverenitet modeli. Kibermakonda xavfsizlikning yana bir muhim ilmiy konsepsiyasi – bu kibersuverenitet tushunchasidir. Xitoy davlatining rasmiy hujjatlarida shunday ta'kidlanadi: «each state has the right to regulate the Internet within its territory according to its own laws»¹. Bu modelga ko'ra, kibermakon hududiy suverenitet tamoyiliga asoslangan holda boshqarilishi lozim.

Biroq GCSC (Global Commission on the Stability of Cyberspace) bunday yondashuvni tanqid qiladi va global barqarorlik uchun xalqaro qoidalar zarurligini ta'kidlaydi: «cyberspace must remain open, secure, stable, accessible and peaceful»². Demak, kibersuverenitet modeli milliy manfaatlarni ilgari sursa, xalqaro boshqaruv modeli transchegaraviy barqarorlikni asosiy tamoyil sifatida ko'radi.

Xalqaro boshqaruv konsepsiyalari. Milton Mueller Internet boshqaruvi haqidagi kitobida yozadi: «The governance of the Internet is a complex interplay between states, private actors, and international institutions»³. Bu konsepsiyaga ko'ra, kibermakon xavfsizligini ta'minlash nafaqat davlatlar, balki xususiy kompaniyalar (Google, Meta, Microsoft) va xalqaro tashkilotlar (BMT, ITU, ICANN) hamkorligida amalga oshiriladi.

Shuningdek, NATO o'zining 2016-yildagi Varshava sammitida kibermakonni alohida operatsion domen deb tan oldi⁴. Bu qaror kibermakonni quruqlik, dengiz, havo va kosmos

¹ Cyberspace Administration of China, White Paper on Internet Sovereignty, Beijing, 2010. «each state has the right to regulate the Internet within its territory according to its own laws».

² Global Commission on the Stability of Cyberspace (GCSC), Norm Package, The Hague, 2018. «cyberspace must remain open, secure, stable, accessible and peaceful».

³ Milton Mueller, Networks and States: The Global Politics of Internet Governance, MIT Press, 2010, bet: 45. «The governance of the Internet is a complex interplay between states, private actors, and international institutions».

⁴ NATO, Warsaw Summit Communiqué, 2016. Kibermakonni alohida operatsion domen sifatida tan olgan qaror.

qatorida harbiy strategik makon sifatida belgilab berdi. Bu yondashuv kibermakon xavfsizligini xalqaro siyosatning eng yuqori darajasiga olib chiqdi.

Yuqoridagi ilmiy konsepsiyalarni umumlashtirgan holda quyidagi xulosalarga kelamiz:

1. Cybersecurity Dynamics kibermakon xavfsizligini tizimli va matematik asosda modellashtiradi.

2. Infosfera nazariyasi axborotni ontologik mavjudot sifatida himoya qilish zarurligini ta'kidlaydi.

3. Kibersuverenitet modeli milliy qonunlarga asoslangan boshqaruvni ilgari suradi, ammo bu xalqaro erkinlik bilan to'qnash kelishi mumkin.

4. Xalqaro boshqaruv konsepsiyalari kibermakon xavfsizligini davlat, xususiy sektor va xalqaro institutlarning hamkorligi asosida tashkil etadi.

So'nggi yillarda kibermakon xavfsizligida AI va ML texnologiyalari muhim rol o'ynay boshladi. Shakarian va boshqalar shunday deydi: «AI-based cybersecurity systems can detect novel threats faster than traditional signature-based systems»¹. Bu shuni anglatadiki, AI nafaqat mavjud tahdidlarni aniqlash, balki ilgari noma'lum bo'lgan hujum turlarini ham tezda sezishi mumkin.

Biroq, AI texnologiyalari o'zi ham xavf manbaiga aylanadi. Brundage va boshqalar "The Malicious Use of Artificial Intelligence" hisobotida shunday yozishadi: «AI will expand the range of actors who can carry out attacks, the scale of attacks, and the speed at which they can be executed»². Demak, AI xavfsizlikni mustahkamlashi bilan birga, yangi turdagi xavflarni ham yuzaga keltiradi.

¹ Paulo Shakarian, Jana Shakarian, Andrew Ruef, Introduction to Cyber-Warfare: A Multidisciplinary Approach, Syngress, 2013, bet: 210. «AI-based cybersecurity systems can detect novel threats faster than traditional signature-based systems».

² Miles Brundage va boshqalar, The Malicious Use of Artificial Intelligence: Forecasting, Prevention, and Mitigation, Oxford, 2018, bet: 15. «AI will expand the range of actors who can carry out attacks, the scale of attacks, and the speed at which they can be executed».

Kiberetika va axborot etikasi. Kibermakon xavfsizligini tushuntiruvchi konsepsiyalardan biri — bu kiberetikadir. Floridi va Taddeo yozadilar: «Information ethics provides a macroethical framework for addressing the moral challenges posed by ICTs and the infosphere»¹. Bu yondashuvga ko'ra, kibermakonda xavfsizlik faqat texnik masala emas, balki axloqiy masala hamdir.

Masalan, foydalanuvchilarning shaxsiy ma'lumotlarini himoya qilish faqat texnik xavfsizlik chorasidir emas, balki axloqiy majburiyat hamdir. Shu sababli, kibermakon xavfsizligi paradigmasida «axborot etikasi» markaziy o'rin tutadi.

Xalqaro huquqiy innovatsiyalar. Kibermakon xavfsizligi paradigmasiga so'nggi yillarda xalqaro huquqiy mexanizmlar ham jadal kirib kelmoqda. BMTning 2021-yilgi Open-Ended Working Group (OEWG) hisobotida shunday deyiladi: «international law, in particular the UN Charter, applies to the use of ICTs by states»². Bu xalqaro huquq tamoyillari kibermakonda ham amal qilishini tasdiqlaydi.

Bundan tashqari, Tallinn qo'llanmasi (Tallinn Manual) kiberooperatsiyalarni xalqaro huquq nuqtai nazaridan tartibga solishga uringan ilk fundamental asarlardan biridir. Schmitt yozadi: «cyber operations that constitute a use of force are prohibited under Article 2(4) of the UN Charter»³. Bu normativ yondashuv kibermakon xavfsizlik paradigmasini xalqaro tinchlik va xavfsizlik tizimi bilan bog'laydi.

¹ Luciano Floridi, Mariarosaria Taddeo, *Information Ethics and the Infosphere*, Springer Handbook of Information Technology, 2016, bet: 5. «Information ethics provides a macroethical framework for addressing the moral challenges posed by ICTs and the infosphere».

² United Nations, *Report of the Open-Ended Working Group on Developments in the Field of ICTs in the Context of International Security*, 2021, bet: 12. «international law, in particular the UN Charter, applies to the use of ICTs by states».

³ Michael N. Schmitt (ed.), *Tallinn Manual on the International Law Applicable to Cyber Warfare*, Cambridge University Press, 2013, bet: 45. «cyber operations that constitute a use of force are prohibited under Article 2(4) of the UN Charter».

Zamonaviy paradigmalarning uyg'unligi. Bugungi kunda kibermakon xavfsizlik paradigmasi AI, kiberetika va xalqaro huquqiy mexanizmlar uyg'unlashgan gibrid modelga aylanmoqda. Bu modelda:

- AI va ML texnologiyalari tahdidlarni tezda aniqlaydi va bashorat qiladi;
- Kiberetika inson huquqlarini va axloqiy me'yorlarni muhofaza qiladi;
- Xalqaro huquqiy innovatsiyalar davlatlararo barqarorlikni ta'minlaydi.

Kibermakon xavfsizligini tushunish va ta'minlash bugungi globallashuv jarayonida davlatlar, xalqaro tashkilotlar va jamiyat oldidagi eng katta sinovlardan biridir. Bu borada olib borilgan ilmiy tahlillar shuni ko'rsatadiki, kibermakon xavfsizlik paradigmasi bir qator nazariy va amaliy yondashuvlarning uyg'unlashuvi asosida shakllanmoqda. Yuqoridagi tadqiqot tahlillari asosida quyidagi xulosalarga kelamiz:

1. Kibermakon xavfsizligi paradigmasi bir yoqlama emas, balki ko'p qirrali — realistik, liberal, konstruktivistik va texnotsentrikyondashuvlarning sintezi sifatida shakllanmoqda.

2. Ilmiy konsepsiyalar (Cybersecurity Dynamics, Infosfera, Kibersuverenitet, Xalqaro boshqaruv) kibermakon xavfsizligini chuqurroq anglash va tartibga solish uchun nazariy poydevor yaratadi.

3. Zamonaviy modellar (AI, ML, kiberetika, xalqaro huquqiy innovatsiyalar) kibermakon xavfsizligini yangi bosqichga olib chiqmoqda, bu esa global hamkorlikni yanada dolzarb qiladi.

4. Davlatlar uchun asosiy vazifa — milliy manfaatlar bilan xalqaro barqarorlik, texnologik taraqqiyot bilan inson huquqlari o'rtasidagi muvozanatni topishdir.

Shunday qilib, kibermakon xavfsizlik paradigmasi XXI asrda global siyosat, texnologiya va huquqning eng muhim chorrahasi sifatida namoyon bo'lmoqda.

1.3. Zamonaviy kiberxavf va tahdidlarning turlari: kiberterrorizm, kiberjinoyat va kiberpropaganda

Kibermakon taraqqiyoti bilan birga yangi turdagi xavflar paydo bo'ldi. ENISA (European Union Agency for Cybersecurity) ta'rificha: «Cyber threat means any potential circumstance or event with the capability to adversely impact organizational operations, assets, individuals, other organizations, or the Nation»¹. Demak, kiberxavf — bu tashkilotlar, davlatlar yoki shaxslar faoliyatiga zarar yetkazish imkoniyatiga ega bo'lgan hodisa yoki sharoitdir. Kiberxavflarning xususiyatlari an'anaviy xavflardan farq qiladi: ular ko'rinmas, tez tarqaluvchi, transchegaraviy va ko'pincha noma'lum manbadan kelib chiqadi. Shu sababdan, ularni aniqlash va oldini olish o'ta murakkab jarayon hisoblanadi.

Kiberterrorizm atamasi 1980-yillarda Dorothy Denning tomonidan ilmiy muomalaga kiritilgan. U shunday yozadi: «Cyberterrorism is the convergence of cyberspace and terrorism. It is generally understood to mean unlawful attacks and threats of attack against computers, networks, and the information stored therein»².

Bu ta'rifga ko'ra, kiberterrorizm — bu kompyuter tarmoqlari va ma'lumotlarga qarshi noqonuniy hujumlar bo'lib, jamiyatda qo'rquv, siyosiy bosim yoki iqtisodiy zarar keltirish maqsadida amalga oshiriladi. Kiberterrorizmning asosiy ko'rinishlari quyidagilardan iborat:

1. Infratuzilmaga hujumlar – elektr tarmoqlari, transport tizimlari, sog'liqni saqlash va boshqa strategik obyektlarga qarshi kiberhujumlar. Masalan, 2015-yilda Ukrainada elektr tarmoqlariga qilingan kiberhujum millionlab odamlarni

¹ ENISA, Threat Landscape Report 2020, European Union Agency for Cybersecurity, Athens, 2020. «Cyber threat means any potential circumstance or event with the capability to adversely impact organizational operations...».

² Dorothy Denning, Cyberterrorism: Testimony before the Special Oversight Panel on Terrorism, U.S. House of Representatives, 2000. «Cyberterrorism is the convergence of cyberspace and terrorism...».

elektrsiz qoldirgan edi¹.

2. Ma'lumotlarni yo'q qilish yoki o'zgartirish – davlat yoki korporativ axborot tizimlaridagi muhim hujjatlarni o'chirib tashlash yoki manipulyatsiya qilish.

3. Propaganda va qo'rqitish – terrorchi guruhlarining internet va ijtimoiy tarmoqlar orqali qo'rquv uyg'otuvchi materiallarni tarqatishi.

BMTning 2002-yildagi hisobotida shunday deyiladi: «Acts of cyberterrorism may have the same intended impact as conventional terrorism, namely to intimidate a population or compel a government»². Demak, kiberterrorizm an'anaviy terrorizm kabi xalqaro tinchlik va xavfsizlikka bevosita tahdid soladi.

Shuningdek, NATO o'zining 2010-yilgi Strategik Konsepsiyasida kiberhujumlarni kollektiv mudofaa tamoyiliga kiritgan. Ya'ni, agar bir a'zo davlatga nisbatan kiberhujum amalga oshirilsa, bu barcha a'zolarga qilingan hujum sifatida talqin qilinadi³. Yuqoridagilardan kelib chiqib quyidagi xulosalarni berish mumkin.

1. Kiberxavf — bu raqamli makondagi zararli hodisalar majmui bo'lib, ular transchegaraviy va ko'pincha noma'lum manbadan kelib chiqadi.

2. Kiberterrorizm an'anaviy terrorizmning yangi shakli bo'lib, kompyuter tarmoqlari va ma'lumotlarga hujumlar orqali jamiyatni qo'rqitishga qaratilgan.

3. Kiberterrorizm xalqaro tinchlik va xavfsizlikka jiddiy tahdid soladi, shu bois BMT va NATO uni global xavfsizlik siyosatining markaziga qo'ygan.

Kiberjinoyat tushunchasi

Interpol ta'rifiga ko'ra: «Cybercrime is a fast-growing area

¹ Kim Zetter, Inside the Cunning, Unprecedented Hack of Ukraine's Power Grid, Wired Magazine, March 2016.

² United Nations, Report of the Counter-Terrorism Committee on Cyberterrorism, New York, 2002. «Acts of cyberterrorism may have the same intended impact as conventional terrorism...».

³ NATO, Strategic Concept for the Defence and Security of the Members of the North Atlantic Treaty Organization, Lisbon, 2010.

of crime. It includes any illegal activity that uses a computer either as a tool, a target or both»¹. Demak, kiberjinoyat — bu kompyuter va tarmoqlar vositasida sodir etiladigan yoki ularga qarshi qaratilgan barcha noqonuniy faoliyatdir.

Yana bir ta'rifni Budapest Konvensiyasi (2001) beradi: «Offences against the confidentiality, integrity and availability of computer data and systems shall be criminal offences». Bu xalqaro hujjat kiberjinoyatni shaxsiy va davlat xavfsizligiga qarshi qaratilgan jinoiy faoliyat sifatida huquqiy jihatdan belgilab berdi.

Kiberjinoyatning asosiy turlari:

1. Ma'lumotlarga ruxsatsiz kirish (hacking) – davlat yoki korporativ tizimlarga noqonuniy kirish.

2. Fishing va ijtimoiy muhandislik – foydalanuvchilardan maxfiy ma'lumotlarni aldamchilik yo'li bilan olish.

3. Moliyaviy kiberjinoyatlar – bank hisoblarini buzish, kriptovalyuta o'g'riligi, onlayn firibgarlik. Masalan, 2016-yilda Bangladesh Bankidan 81 million dollar o'g'irlangan edi².

4. Ransomware (dasturiy tovlamachilik) – tizimni bloklash va uni qayta ochish uchun to'lov talab qilish. WannaCry (2017) hujumi dunyo bo'ylab 150 mamlakatda 200 mingdan ortiq kompyuterni zararlagan³.

5. Bolalar pornografiyasi va noqonuniy kontent tarqatish – xalqaro miqyosda eng og'ir kiberjinoyatlardan biri sifatida baholanadi.

Budapest Konvensiyasi (2001) kiberjinoyatlarga qarshi kurash bo'yicha birinchi universal xalqaro shartnoma bo'ldi. U quyidagi tamoyillarni belgilaydi:

- Kompyuter tizimlariga noqonuniy kirishni jinoyat deb belgilash;

¹ Interpol, Cybercrime, rasmiy sayt, 2020. «Cybercrime is a fast-growing area of crime. It includes any illegal activity that uses a computer either as a tool, a target or both».

² Joseph Menn, How hackers stole \$81 million from Bangladesh Bank, Reuters, 2016.

³ Europol, WannaCry ransomware outbreak, Press Release, 2017.

- Ma'lumotlarni noqonuniy ushlab qolish va o'zgartirishni taqiqlash;
- Transchegaraviy tergov va xalqaro hamkorlik mexanizmlarini ishlab chiqish¹.

Shuningdek, Yevropa Kengashi kiberjinoyatga qarshi qo'shimcha protokollarni qabul qilgan bo'lib, ularda irqchilik va ksenofobiya mazmunidagi onlayn jinoyatlar ham qamrab olingan².

Kiberjinoyatga qarshi kurashda asosiy muammo — bu yurisdiksiya masalasidir. Masalan, bir jinoyat Xitoyda amalga oshirilishi, ammo uning qurboni Germaniyada bo'lishi mumkin. Bunday hollarda qaysi davlat qonunchiligi ustuvor bo'lishi masalasi yuzaga chiqadi.

Interpolning ta'kidlashicha: «Effective investigation and prosecution of cybercrime require close international cooperation»³. Demak, yagona davlatning sa'y-harakatlari yetarli emas, balki global miqyosda hamkorlik zarur.

Kiberpropaganda tushunchasi

Kiberpropaganda — bu internet va raqamli platformalar orqali amalga oshiriladigan siyosiy, mafkuraviy yoki psixologik ta'sir shaklidir. Rid va boshqalar ta'kidlaganidek: «Cyber propaganda refers to the deliberate use of information and communication technologies to manipulate perceptions and influence public opinion»⁴.

¹ Council of Europe, Convention on Cybercrime (Budapest Convention), 2001, Article 2–4. «Offences against the confidentiality, integrity and availability of computer data and systems shall be criminal offences».

² Council of Europe, Additional Protocol to the Convention on Cybercrime, 2003.

³ Interpol, Cybercrime, rasmiy sayt, 2020. «Cybercrime is a fast-growing area of crime. It includes any illegal activity that uses a computer either as a tool, a target or both».

⁴ Thomas J. Rid, Cyber War Will Not Take Place, Oxford University Press, 2013, bet: 56. «Cyber propaganda refers to the deliberate use of information and communication technologies to manipulate perceptions and influence public opinion».

Ushbu ta'rif shuni ko'rsatadiki, kiberpropaganda shunchaki axborot tarqatish emas, balki ommaviy ongni manipulyatsiya qilish va siyosiy qarorlarni o'zgartirishga qaratilgan strategik faoliyatdir.

Kiberpropaganda jarayonida quyidagi asosiy usullar qo'llaniladi:

1. Soxta axborot (disinformation) – yolg'on yoki noto'g'ri ma'lumotlarni tarqatish orqali jamiyatni chalg'itish.
2. Troll fabrikalari – siyosiy mavzularni ijtimoiy tarmoqlarda muhokama qilish va jamoatchilikni bo'lish uchun uyushtirilgan foydalanuvchilar tarmog'i.
3. Bot tarmoqlari – avtomatlashtirilgan akkauntlar orqali ma'lum xabarlarini tez va keng miqyosda tarqatish.
4. Deepfake texnologiyalari – siyosiy yetakchilar yoki mashhur shaxslarning soxta videolarini yaratish va ularni targ'ibot vositasi sifatida ishlatish.

Kiberpropagandaga biz quyidagi amaliy misollarni keltirishimiz mumkin:

- 2016-yilgi AQSh prezidentlik saylovi – Mueller hisobotida ta'kidlanishicha, «Russian operatives used social media platforms to sow discord and influence the election outcome»¹. Bu holat kiberpropagandaning real siyosiy jarayonlarga ta'sir ko'rsatishini isbotladi.
- COVID-19 pandemiyasi davrida – Jahon sog'liqni saqlash tashkiloti qayd etganidek: «an infodemic spread faster than the virus itself, undermining trust in health measures»². Bu kiberpropagandaning salomatlik sohasida ham xavfli oqibatlarga olib kelishini ko'rsatdi.
- Yevropadagi siyosiy jarayonlar – Yevropa Komissiyasi

¹ U.S. Department of Justice, Report on the Investigation into Russian Interference in the 2016 Presidential Election (Mueller Report), Washington, 2019. «Russian operatives used social media platforms to sow discord and influence the election outcome».

² World Health Organization, Managing the COVID-19 Infodemic: Promoting Healthy Behaviors and Mitigating the Harm from Misinformation and Disinformation, Geneva, 2020. «an infodemic spread faster than the virus itself, undermining trust in health measures».

2018-yilda e'lon qilgan hisobotida: «Disinformation campaigns are a major threat to democratic processes in the EU»¹.

Kiberpropaganda demokratik jamiyatlarga, davlat xavfsizligiga va fuqarolik institutlariga jiddiy xavf tug'diradi:

- Demokratiyaga tahdid – yolg'on axborot saylovchilar qaroriga ta'sir qilishi mumkin.
- Jamiyatning bo'linishi – ekstremistik yoki millatchilik ruhidagi axborot oqimi ijtimoiy kelishmovchiliklarni kuchaytiradi.
- Davlatlararo munosabatlarga ta'sir – kiberpropaganda ko'pincha boshqa davlatlarning siyosiy barqarorligini izdan chiqarish maqsadida ishlatiladi.
- Axborot ishonchliligining pasayishi – odamlar axborot manbalariga ishonmay qo'yadi, bu esa ijtimoiy beqarorlikka olib keladi.

BMTning 2020-yildagi hisobotida shunday deyilgan: «The weaponization of information undermines international peace and security»². Shu sababli, xalqaro hamjamiyat kiberpropaganda va dezinformatsiyaga qarshi kurashni global xavfsizlik siyosatining bir qismi sifatida ko'rib chiqmoqda.

Yevropa Ittifoqi esa 2015-yildan beri East StratCom Task Force tashabbusini amalga oshirib, soxta axborotga qarshi maxsus monitoring tizimlarini yo'lga qo'ydi³.

¹ European Commission, Tackling Online Disinformation: A European Approach, Brussels, 2018. «Disinformation campaigns are a major threat to democratic processes in the EU».

² United Nations, Report of the Secretary-General on Disinformation in the Context of International Peace and Security, New York, 2020. «The weaponization of information undermines international peace and security».

³ European External Action Service (EEAS), East StratCom Task Force: Addressing Disinformation, Brussels, 2015.

1.4. Sun'iy intellekt va kibermakon xavfsizligi: yangi xavf va imkoniyatlar.

AI texnologiyalari kiberxavfsizlikni mustahkamlashda yangi imkoniyatlarni taqdim etmoqda. Shakarian va hamkorlari ta'kidlaganidek: «AI-based cybersecurity systems can detect novel threats faster than traditional signature-based systems»¹. Demak, AI yordamida xavf-xatarlarni tezda aniqlash, ilgari noma'lum bo'lgan hujum turlarini ko'rish va ularga qarshi choralarini avtomatlashtirish mumkin.

AI asosidagi tizimlar quyidagi yo'nalishlarda qo'llanmoqda:

1. Tahdidlarni erta aniqlash – kiberhujumlar boshlanishidan oldin ularni bashorat qilish.
2. Avtomatlashtirilgan javob – tizim zararni kamaytirish uchun tezkor javob choralari o'zi amalga oshiradi.
3. Ma'lumotlarni tahlil qilish – katta hajmdagi log va trafik ma'lumotlarini real vaqt rejimida o'rganib, hujum alomatlarini ajratib olish.

Mashinaviy o'rganish (ML) va kiberxavfsizlik

ML algoritmlari kiberxavfsizlikda an'anaviy usullardan samaraliroq natijalar bermoqda. Sommer va Paxson shunday yozadi: «Machine learning holds great promise for intrusion detection, but it must overcome issues of data quality and adversarial manipulation»². Ya'ni, ML intruziyani aniqlashda katta imkoniyat beradi, ammo u ma'lumot sifati va dushmanona manipulyatsiya kabi muammolarga duch keladi.

ML asosidagi tizimlar, masalan, anomal faoliyatni aniqlash (anomaly detection), fishing xabarlarini filtr qilish, spamni bloklash va zararli dasturlarni tasniflashda keng qo'llanmoqda.

¹ Paulo Shakarian, Jana Shakarian, Andrew Ruef, Introduction to Cyber-Warfare: A Multidisciplinary Approach, Syngress, 2013, bet: 210. «AI-based cybersecurity systems can detect novel threats faster than traditional signature-based systems».

² Robin Sommer, Vern Paxson, Outside the Closed World: On Using Machine Learning For Network Intrusion Detection, IEEE Symposium on Security and Privacy, 2010. «Machine learning holds great promise for intrusion detection, but it must overcome issues of data quality and adversarial manipulation».

AI va tahdidlarni bashorat qilish

AI asosidagi bashorat tizimlari kiberhujumlarni vaqtida oldindan ko'ra olish imkonini beradi. Symantec'ning 2019-yilgi hisobotida ta'kidlanadi: «Predictive analytics powered by AI can forecast attack patterns and help organizations prepare in advance»¹. Bu, xususan, moliya va sog'liqni saqlash kabi sohalarda katta ahamiyatga ega, chunki bu sohalarda tahdidlarning oldini olish zararni keskin kamaytiradi.

AI va katta ma'lumotlar (Big Data)

AI texnologiyalari katta hajmdagi ma'lumotlarni tahlil qilish orqali xavfsizlikni kuchaytiradi. Xu va boshqalar yozadilar: «Big data analytics integrated with AI enhances the capacity to identify sophisticated cyber threats in real time»². Bu esa davlat va korporatsiyalarga nafaqat hujumlardan himoyalanish, balki ularni tezkor aniqlash imkonini beradi.

AI texnologiyalari xavfsizlikni kuchaytirish imkonini bersa-da, ular hujumchilarning ham qo'lida kuchli vositaga aylanmoqda. Brundage va hamkorlari shunday deydilar: «AI will expand the range of actors who can carry out attacks, the scale of attacks, and the speed at which they can be executed»³. Bu shuni anglatadiki, ilgari faqat yirik resurslarga ega tashkilotlar qila oladigan hujumlar endi kichik guruhlar yoki hatto individual shaxslar tomonidan amalga oshirilishi mumkin.

¹ Symantec, Internet Security Threat Report, Mountain View, 2019. «Predictive analytics powered by AI can forecast attack patterns and help organizations prepare in advance».

² Xiaohui Xu, Lei Wu, Big Data Analytics for Cybersecurity: A Survey, Journal of Computer Science and Technology, Vol. 34, No. 1, 2019, bet: 1–28. «Big data analytics integrated with AI enhances the capacity to identify sophisticated cyber threats in real time».

³ Miles Brundage va boshqalar, Sun'iy intellektidan zararli foydalanish: prognozlash, oldini olish va yumshatish, Oksford, 2018, tikish: 15. «AI hujumlarni amalga oshirishi mumkin bo'lgan aktyorlar doirasini, hujumlar ko'lamini va ularni amalga oshirish tezligini kengaytiradi.»

Masalan:

- Avtomatlashtirilgan fishing – AI yordamida juda ishonarli soxta xabarlar yaratish mumkin.
- Deepfake hujumlari – siyosiy yetakchilar yoki biznes rahbarlari nomidan soxta videolar tayyorlash orqali manipulyatsiya qilish.
- AI-dasturlashtirilgan botnetlar – kiberhujumlarni avtonom boshqaradigan tarmoqlar.

AI kibermakonda faqat texnik emas, balki axloqiy muammolarni ham yuzaga keltiradi. Floridi va Taddeo ta'kidlaganidek: «Information ethics provides a macroethical framework for addressing the moral challenges posed by ICTs and the infosphere»¹. Bu degani, AI vositalaridan foydalanishda inson huquqlari, shaxsiy daxlsizlik va erkinlik masalalari hisobga olinishi shart. Asosiy axloqiy xavflar:

1. Maxfiylikni buzish – yuzni tanish tizimlari va kuzatuv algoritmlari fuqarolarning shaxsiy hayotini cheklashi mumkin.
2. Diskriminatsiya – noto'g'ri yoki tarafkash ma'lumotlar asosida mashinaviy o'rganish algoritmlari ayrim guruhlariga nisbatan adolatsiz qarorlar qabul qilishi mumkin.
3. Avtonom qarorlar – AI asosida ishlab chiqilgan qurollar yoki xavfsizlik tizimlari inson aralashuvisiz qaror qabul qilishi xavfli oqibatlariga olib kelishi mumkin.

Xalqaro huquqda AI bilan bog'liq xavfsizlik masalalari hali to'liq tartibga solinmagan. BMTning 2021-yilgi OEWG hisobotida ta'kidlanganidek: «international law, including the UN Charter, applies to the use of ICTs by states, but further clarification is needed regarding AI-driven cyber operations»².

¹ Luciano Floridi, Mariarosaria Taddeo, Axborot etikasi va Infosfera, Springer, 2016, tikish: 5. "Axborot etikasi AKT va infosfera tomonidan qo'yiladigan axloqiy muammolarni hal qilish uchun makroetik asosni ta'minlaydi".

² Birlashgan Millatlar Tashkiloti, Xalqaro xavfsizlik kontekstida AKT sohasidagi rivojlanishlar bo'yicha ochiq ishchi guruhining hisoboti, Nyu-York, 2021 yil, bet: 12. "Xalqaro huquq, jumladan, BMT Nizomi davlatlar tomonidan AKTdan foydalanishga nisbatan qo'llaniladi, ammo sun'iy intellektga asoslangan kiberoperatsiyalar bo'yicha qo'shimcha tushuntirishlar zarur."

Ta'lim qo'llanmasida ham AI bilan bog'liq masalalar bilvosita yoritilgan bo'lib, u yerda «cyber operations that constitute a use of force are prohibited under Article 2(4) of the UN Charter»¹ deyilgan. Biroq AI asosida amalga oshiriladigan hujumlar qaysi chegarada “kuch ishlatish” sifatida baholanishi masalasi ochiq qolmoqda.

Shuningdek, Yevropa Ittifoqi 2021-yilda «Artificial Intelligence Act» loyihasini ishlab chiqdi va unda «high-risk AI systems» uchun qat'iy qoidalar belgilashni taklif qildi². Bu huquqiy tashabbus AI vositalaridan xavfsiz va mas'uliyatli foydalanish yo'lida muhim qadamdir.

AI texnologiyalari kibermakonda xavfsizlikni ta'minlashning yangi darajasini shakllantirishi mumkin. Gartner 2022-yilgi hisobotida shunday deyilgan: «By 2030, AI-driven security operations will become the backbone of cyber defense, enabling autonomous detection and response»³. Bu shuni anglatadiki, kelajakda xavfsizlik tizimlari ko'proq avtonom bo'ladi, inson aralashuviga ehtiyoj kamayadi. Kelajak imkoniyatlari quyidagilarda ko'rinadi:

1. Avtonom mudofaa tizimlari – AI real vaqt rejimida hujumlarni aniqlab, zarur choralarni o'zi ko'radi.

2. Kiberintellektual tarmoqlar – turli tizimlar o'zaro hamkorlik qilib, global darajada kiberxavfsizlikni ta'minlaydi.

3. Predictive defense – AI yordamida hujum naqshlari oldindan taxmin qilinadi va oldini olish imkoniyati oshadi.

Sun'iy intellektning kiberxavfsizlikdagi o'rni xalqaro boshqaruv mexanizmlarini qayta ko'rib chiqishni talab qiladi.

¹ Maykl N. Shmitt (tahr.), Kiber urushga taalluqli xalqaro huquq bo'yicha Tallin qo'llanmasi, Kembrij universiteti nashriyoti, 2013 yil, garov: 45. “Kuch ishlatishni tashkil etuvchi kiberoperatsiyalar BMT Nizomining 2(4) moddasiga muvofiq taqiqlangan.”

² European Commission, Proposal for a Regulation Laying Down Harmonised Rules on Artificial Intelligence (Artificial Intelligence Act), Brussels, 2021.

³ Gartner, Predicts 2022: Cybersecurity Industry, Stamford, 2022. «By 2030, AI-driven security operations will become the backbone of cyber defense, enabling autonomous detection and response».

OECD 2021-yilgi hisobotida ta'kidlanganidek: «AI governance must integrate cybersecurity to ensure trust, resilience, and accountability»¹. Bu yondashuv AI boshqaruvini kiberxavfsizlik bilan uyg'unlashtirish zarurligini ko'rsatadi.

Global boshqaruv istiqbollari:

- Yagona xalqaro standartlar – AI asosida xavfsizlik tizimlari uchun global qoidalar ishlab chiqilishi kerak.
- Davlatlararo hamkorlik – AI xavfsizlikdagi muvaffaqiyat faqat transchegaraviy hamkorlik orqali mumkin.
- Xususiylar sektori ishtiroki – Microsoft, Google, IBM kabi kompaniyalar xalqaro standartlarni ishlab chiqishda muhim rol o'ynaydi.

AI asosidagi xavfsizlik tizimlari imkoniyatlar bilan birga xavflarni ham keltiradi. Amnesty Internationalning 2021-yilgi hisobotida shunday deyiladi: «AI surveillance systems risk eroding privacy and fundamental freedoms if not regulated properly»². Shu sababli, kelajakda AI xavfsizlik paradigmasida inson huquqlarini muhofaza qilish birlamchi vazifa bo'lib qoladi.

AI integratsiyasining istiqbollari

1. Davlat siyosatida – AI kiberxavfsizlik strategiyalarining ajralmas qismi bo'ladi. AQShning 2021-yilgi *National AI Initiative Act* hujjati bunga dalildir³.

2. Xalqaro huquqda – BMT va Yevropa Ittifoqi darajasida AI xavfsizlik standartlarini ishlab chiqish tendensiyasi kuchaymoqda.

3. Ilmiy tadqiqotlarda – AI va kiberxavfsizlik integratsiyasi “cyber defense science” sifatida yangi ilmiy sohaga aylanmoqda.

Sun'iy intellekt (AI) texnologiyalarining kibermakondagi rivoji xavfsizlik paradigmasini tubdan o'zgartirdi. AI endilikda faqat himoya vositasi emas, balki yangi turdagi hujumlar

¹ OECD, *AI in Society: Governance and Security*, Paris, 2021. «AI governance must integrate cybersecurity to ensure trust, resilience, and accountability».

² Amnesty International, *Surveillance Giants: The Human Rights Dimensions of AI Security Systems*, London, 2021. «AI surveillance systems risk eroding privacy and fundamental freedoms if not regulated properly».

³ U.S. Congress, *National Artificial Intelligence Initiative Act*, Washington D.C., 2021.

manbai sifatida ham qaralmoqda. Shu bois bu fenomen falsafiy va huquqiy nuqtai nazardan chuqur tahlil etilishi zarur.

Falsafiy yondashuvga ko'ra, AI kibermakonning ontologiyasini murakkablashtiradi. Floridi ta'kidlaganidek, «the infosphere is the totality of informational entities...» — endi bu infosferada faqat inson emas, balki mashina intellekti ham faol ishtirok etmoqda. Demak, AI kibermakonni inson-mashina hamkorligi asosida yangi “borliq” darajasiga ko'taradi.

Biroq Baudrillard nazariyasidan kelib chiqib aytish mumkinki, AI asosidagi deepfake va manipulyatsiyalar «simulyakr» sifatida yangi “soxta haqiqat”larni yaratmoqda. Bu esa haqiqat va virtual o'rtasidagi chegaralarni yo'qotib, axloqiy muammolarni kuchaytiradi.

Xalqaro huquq AI asosidagi kiberhujumlarga hali to'liq tayyor emas. BMT OEWG hisobotida qayd etilganidek: «international law... applies to the use of ICTs by states, but further clarification is needed regarding AI-driven cyber operations». Bu AI kiberoperatsiyalarining xalqaro huquqiy maqomi hali aniqlashtirilmaganini ko'rsatadi.

Yevropa Ittifoqi AI Act orqali «high-risk AI systems»ni qat'iy tartibga solishni taklif qildi. Bu inson huquqlarini himoya qilish yo'lidagi muhim huquqiy tashabbusdir. Shu bilan birga, Ta'lim qo'llanmasida «cyber operations that constitute a use of force are prohibited...» deya qayd etilgan bo'lsa-da, AI asosidagi hujumlarning qaysi biri kuch ishlatishga tenglashtirilishi masalasi ochiq qolmoqda.

AI kibermakonda inson huquqlari bilan bog'liq yangi xavflarni keltirmoqda. Amnesty International shunday ogohlantiradi: «AI surveillance systems risk eroding privacy and fundamental freedoms if not regulated properly». Demak, AI xavfsizlikni mustahkamlash bilan birga, shaxsiy daxlsizlik va erkinlikka putur yetkazishi mumkin.

Shu nuqtai nazardan, AI xavfsizlik paradigmasida inson huquqlarini markaziy mezon sifatida belgilash zarur. Aks holda, texnologik taraqqiyot demokratik qadriyatlar va axloqiy me'yorlarni yemirishi ehtimoli mavjud.

I BOB BO'YICHA XULOSALAR

XXI asrda insoniyat yangi davrga – raqamli sivilizatsiya davriga qadam qo'ydi. Bu davrning eng muhim belgilaridan biri sifatida kibermakon tushunchasi paydo bo'lib, u tobora keng qamrovli ijtimoiy-falsafiy, siyosiy va huquqiy kategoriya-ga aylandi. Ushbu bobda kibermakonning mazmun-mohiyati, uning falsafiy va huquqiy talqinlari, xavfsizlik paradigmalari hamda zamonaviy tahdidlar tizimi atroflicha o'rganildi. Endi bu tadqiqotlardan kelib chiqib asosiy umumiy xulosalarni quy-idagicha taqdim etish mumkin.

Birinchidan, kibermakon nafaqat texnologik infratuzilma yoki internet tarmoqlarining yig'indisi, balki insoniyat tajrib-asining yangi “borliq o'lchovi” sifatida namoyon bo'ladi. Manu-el Castellsning “space of flows” nazariyasi asosida kibermakon ijtimoiy amaliyotlarning vaqt va makondan mustaqil ravishda qayta tashkil etilgan shakli sifatida tushuniladi. Luciano Floridining “infosfera” konsepsiyasi esa uni barcha axborot mavjudotlari va ularning o'zaro aloqalari jamuljamidan iborat bor-liq sifatida talqin qiladi.

Biroq falsafiy bahslarda baholi-qudrat ikki qutb kuzatiladi: bir tomonda kibermakon “haqiqiy borliq” sifatida tan olinadi, ikkinchi tomonda esa u “simulyakr”, ya'ni haqiqiylikni soxta nusxalar orqali yo'qotadigan hodisa sifatida baholanadi (Baudrillard). Shu sababli kibermakon ontologiyasi doimo bahsli va dinamik bo'lib qoladi.

Epistemologik jihatdan esa kibermakonni bilish doimo chegaralangan va fragmentar. Chunki u tez o'zgaruvchan, transchegaraviy va ko'p qirrali makon bo'lib, uni faqat ko'p fanli yon-dashuvlar orqali anglash mumkin.

Ikkinchidan, kibermakon an'anaviy huquqiy tartibotlarni tubdan o'zgartirdi. John Perry Barlowning “Cyberspace Declaration”i kibermakonni davlatlardan mustaqil hudud sifatida e'lon qilgan bo'lsa, xalqaro huquqiy hujjatlar (Budapest Konvensiyasi, BMT OEWG, Tallinn qo'llanmasi) uni davlatlar va xalqaro tashkilotlarning yurisdiksiyasiga bog'lashga intiladi.

Bu holat shuni ko'rsatadiki, kibermakon huquqiy pluralizm

tamoyiliga asoslanadi. Lawrence Lessig ta'kidlaganidek, kibermakonda huquqni nafaqat qonunlar, balki ijtimoiy me'yorlar, bozor mexanizmlari va texnologik "arxitektura" ham tartibga soladi. Shu bois kibermakon faqat huquqiy emas, balki normativ jihatdan ko'p qatlamli tizimdir.

Xalqaro tajriba ham shuni ko'rsatmoqdaki, davlat suvereniteti bilan inson huquqlari o'rtasida muvozanatni topish zarur. Masalan, Yevropa Ittifoqining GDPR qonuni shaxsiy ma'lumotlarni himoya qilishni milliy manfaatlardan ustun qo'ygan. Bu esa kibermakonni tartibga solishda demokratik qadriyatlarni saqlash muhimligini anglatadi.

Uchinchidan, kibermakon xavfsizligi paradigmalari turlicha talqin qilinmoqda:

- Realistik paradigma xavfsizlikni milliy manfaatlarini himoya qilish vositasi sifatida ko'radi. Davlatlar kibermakonni geosiyosiy raqobat maydoni sifatida baholaydi.
- Liberal paradigma kibermakon xavfsizligini xalqaro hamkorlik va ko'p tomonlama boshqaruv orqali ta'minlashni ilgari suradi.
- Konstruktivistik paradigma xavfsizlikni ijtimoiy konstruksiya sifatida, ya'ni jamiyat va davlatlar qanday xavfni sezsalar, shunga mos ravishda siyosiy qarorlar shakllanishini ta'kidlaydi.
- Texnotsentrik paradigma texnologiyani xavfsizlikning asosiy manbai sifatida talqin qiladi, AI va ML texnologiyalarini markaziy rolga qo'yadi.

Ilmiy konsepsiyalar (Cybersecurity Dynamics, Infosfera nazariyasi, Kibersuverenitet modeli, Xalqaro boshqaruv mexanizmlari) esa bu paradigmalarning nazariy asoslarini kengaytiradi.

To'rtinchidan, zamonaviy tahdidlar uch asosiy toifada tahlil qilindi:

- Kiberterrorizm – jamiyatni qo'rquvga soluvchi, infratuzilmalarga hujum qiluvchi va siyosiy bosim vositasiga aylangan hodisa. Uning oqibatlari an'anaviy terrorizmga teng darajada xavfli.

- Kiberjinoyat – moliyaviy firibgarlik, fishing, ransomware, noqonuniy kontent tarqatish kabi transchegaraviy jinoyatlarni o'z ichiga oladi. Budapest Konvensiyasi bu jinoyatlarga qarshi xalqaro huquqiy mexanizm sifatida qabul qilingan.

- Kiberpropaganda – ommaviy ongni manipulyatsiya qilish, siyosiy jarayonlarga aralashish va jamiyatni bo'lishga qaratilgan faoliyat. 2016-yilgi AQSh saylovlari, COVID-19 davridagi "infodemiya" va Yevropadagi dezinformatsiya kampaniyalari bu tahdidning real misollaridir.

Bu tahdidlarning barchasi shuni ko'rsatadiki, kibermakon xavfsizligi milliy, mintaqaviy va global darajada dolzarb vazifaga aylangan.

Beshinchidan, AI texnologiyalari kibermakon xavfsizligiga ikki tomonlama ta'sir ko'rsatmoqda. Bir tomondan, AI tahdidlarni erta aniqlash, avtomatlashtirilgan javob va bashorat tizimlari orqali xavfsizlikni kuchaytiradi. Ikkinchi tomondan, AI asosidagi hujumlar (deepfake, avtomatlashtirilgan fishing, AI-botnetlar) yangi xavf-xatarlarni yuzaga keltirmoqda.

Axloqiy jihatdan AI kuzatuv tizimlari shaxsiy daxlsizlikni buzishi, diskriminatsion algoritmlar ijtimoiy adolatsizlikni kuchaytirishi mumkin. Huquqiy jihatdan esa AI asosidagi kiberoperatsiyalarning maqomi hali aniq belgilanmagan. BMT OEWG, Tallinn qo'llanmasi va Yevropa Ittifoqi AI Act bu borada ilk normativ asoslarni taklif etmoqda.

Kelajak istiqbollari shuni ko'rsatadiki, AI kibermakon xavfsizligida avtonom mudofaa, global boshqaruv va kiberetika asosida rivojlanadi. Biroq inson huquqlari va demokratik qadriyatlar bu jarayonda asosiy mezon bo'lib qolishi zarur.

Ushbu bobdan kelib chiqadigan asosiy xulosalarni quyidagicha umumlashtirishimiz mumkin:

1. Kibermakon ko'p qatlamli fenomen bo'lib, uni faqat texnologik emas, balki falsafiy va huquqiy nuqtai nazardan ham o'rganish zarur.

2. Kibermakondagi huquqiy pluralizm davlat qonunlari, xalqaro huquqiy mexanizmlar, ijtimoiy me'yorlar va texnologik arxitektura uyg'unligi asosida shakllanadi.

3. Zamonaviy xavfsizlik paradigmalari va ilmiy konsepsiyalar kibermakonni chuqurroq anglash uchun nazariy poydevor yaratadi.

4. Kiberterrorizm, kiberjinoyat va kiberpropaganda kabi tahdidlar global barqarorlikka jiddiy xavf tug'diradi.

5. AI kibermakon xavfsizligida imkoniyatlar va xavflarni uyg'unlashtirib, yangi paradigmalarning shakllanishiga olib kelmoqda.

II-BOB. XALQARO DAVLATLAR TAJRIBASI

Kibermakon zamonaviy dunyoning ajralmas tarkibiy qismiga aylangan bo'lib, davlatlar uchun milliy xavfsizlik, iqtisodiy taraqqiyot va jamiyat barqarorligining muhim omili sifatida namoyon bo'lmoqda. Har bir davlat o'zining tarixiy, siyosiy va huquqiy tajribasidan kelib chiqib, kibermakon xavfsizligini ta'minlashda turlicha yondashuvlarni ishlab chiqqan. Shu sababli ham kibermakonni falsafiy-huquqiy talqin qilish, turli mamlakatlar tajribasini qiyosiy tahlil etish va ular asosida O'zbekiston uchun amaliy saboqlar chiqarish bugungi kunda dolzarb masalalardan biridir.

Mazkur bobda dunyoning turli mintaqalarida shakllangan kiberxavfsizlik modellari o'rganiladi. Avvalo, AQSh tajribasi ko'rib chiqiladi. AQSh kiberxavfsizlikni texnologik ustunlik, davlat–xususiy sektor hamkorligi va xalqaro diplomatik faoliyat bilan uyg'unlashtirgan. Uning modeli kibermakonni geosiyosiy kuch maydoni sifatida talqin qiladi. Shu bilan birga, maxfiylik va inson huquqlariga oid jiddiy tanqidlar mavjud bo'lib, bu modelning zaif tomonlarini ko'rsatadi.

Yevropa Ittifoqi tajribasi esa butunlay boshqa yo'nalishni ifodalaydi. Bu yerda shaxsiy ma'lumotlarni himoya qilish, inson huquqlariga ustuvorlik va fuqarolik jamiyatining faol ishtiroki asosiy tamoyil sifatida qaraladi. GDPR va boshqa normativ hujjatlar global standartga aylangan. Yevropa modeli falsafiy jihatdan inson sha'ni va erkinligini kibermakon siyosatining markaziga qo'yadi. Shu bilan birga, byurokratik murakkablik va texnologik qaramlik uning zaif tomonlari sifatida namoyon bo'ladi.

Rossiya tajribasi kiberxavfsizlikni davlat suvereniteti va markazlashgan nazorat asosida shakllantiradi. “Yarovaya paketi” va “Suveren internet” qonunlari orqali internet ustidan to'liq nazorat o'rnatildi. FSB va Roskomnadzor kabi institutlar markaziy rol o'ynaydi. Falsafiy jihatdan bu yondashuv realizm paradigmasiga yaqin bo'lib, kibermakonni milliy kuchni mustahkamlash vositasi sifatida talqin qiladi. Shu bilan birga,

inson huquqlarining cheklanishi va izolyatsiya xavfi Rossiya modelining muhim kamchiliklaridan biridir.

Xitoy tajribasi esa “kibersuverenitet” g’oyasi asosida shakllangan. Buyuk Xitoy devori, milliy IT-gigantlarning faoliyati va sun’iy intellektga asoslangan kuzatuv tizimlari orqali davlat internet ustidan to’liq nazoratni amalga oshirmoqda. Falsafiy jihatdan bu model konfutsiychilik qadriyatlari va davlat markazchiligiga tayanadi. Kuchli tomoni – texnologik mustaqillik va global tashabbuslarni ilgari surishi; zaif tomoni esa inson huquqlari va so’z erkinligining keskin cheklanishidir.

Koreya va Yaponiya tajribasi texnologik innovatsiyalar va xalqaro hamkorlik asosida shakllangan. Koreya Respublikasi Shimoliy Koreyadan kelayotgan kiberxavflar fonida milliy strategiyasini ishlab chiqib, KISA kabi institutlar orqali samarali boshqaruvni yo’lga qo’ydi. Yaponiya esa Cybersecurity Basic Act (2014) va NISC faoliyati orqali kiberxavfsizlikni muntazam strategik asosda rivojlantirib kelmoqda. Bu ikki davlatning o’ziga xosligi – sun’iy intellekt, 5G va IoT xavfsizligini milliy siyosatga kiritgani, xalqaro hamkorlikda faol ishtirok etgani va innovatsion yondashuvni falsafiy asos sifatida ko’rganidir.

Mazkur bobda, shuningdek, Isroil, Germaniya va boshqa davlatlarning tajribasi ham ko’rib chiqiladi. Isroilning o’ziga xosligi – kibermakon xavfsizligini startap ekotizimi va harbiy texnologiyalar sinergiyasi orqali shakllantirganida. Germaniya esa Yevropa Ittifoqi doirasida shaxsiy ma’lumotlarni himoya qilish va demokratik qadriyatlarni kiberxavfsizlik siyosatiga integratsiya qilishga e’tibor qaratmoqda.

Umuman olganda, turli davlatlar tajribasi kibermakon xavfsizligigabo’lganyondashuvlarningxilma-xilligini ko’rsatadi. AQSh va Rossiya tajribalari kuch va nazorat paradigmasiga yaqinlashsa, Yevropa Ittifoqi va Germaniya inson huquqlari va demokratik qadriyatlarni ustuvor qo’yadi. Xitoy modeli esa kibersuverenitet va davlat nazoratiga asoslanadi. Koreya va Yaponiya esa texnologik innovatsiyalar va xalqaro hamkorlik orqali kibermakon xavfsizligini mustahkamlashga intiladi.

Shu bois 2-bobning maqsadi – turli davlatlar tajribasini tahlil

qilish orqali kibermakon xavfsizligini ta'minlashdagi falsafiy va huquqiy asoslarni ochib berish, ularning kuchli va zaif tomonlarini ko'rsatish hamda O'zbekiston uchun mos saboqlar chiqarishdir. Chunki O'zbekiston ham raqamli transformatsiya jarayonida kibermakon xavfsizligini ta'minlash, milliy suverenitetni himoya qilish va fuqarolarning huquq hamda erkinliklarini asrash masalalarini dolzarb vazifa sifatida ko'rib chiqmoqda.

2.1. AQSh tajribasi: kiberxavfsizlik siyosati, huquqiy asoslari va strategiyasi

AQSh kibermakonni xavfsizlikning alohida sohasi sifatida birinchi tan olgan davlatlardan biridir. 1990-yillarda internetning tez sur'atlarda kengayishi va davlat infratuzilmasining raqamlashtirilishi natijasida AQSh hukumatida yangi xavfsizlik paradigmasini ishlab chiqish zarurati tug'ildi. 1998-yilda Prezident Bill Klinton tomonidan e'lon qilingan Presidential Decision Directive 63 (PDD-63) hujjatida shunday deyiladi: «Protecting America's critical infrastructures is essential to the Nation's security, economy, and public health»¹. Bu hujjat kibermakonni milliy xavfsizlik strategiyasiga integratsiya qilishning dastlabki bosqichi bo'ldi.

Shundan so'ng, 2001-yil 11-sentabr teraktlaridan keyin AQSh hukumati kiberxavfsizlikni terrorizmga qarshi kurashning ajralmas qismi sifatida ko'ra boshladi. Bu davrdan boshlab kibermakon "yangi front" sifatida milliy mudofaa doktrinasiga kiritildi.

AQShda kibermakon xavfsizligining asosiy institutsional poydevori National Security Agency (NSA) tomonidan qo'yildi. NSAning kiberoperatsiyalari ko'pincha maxfiy bo'lsa-da, uning

¹ White House, Presidential Decision Directive 63: Critical Infrastructure Protection, Washington D.C., 1998. «Protecting America's critical infrastructures is essential to the Nation's security, economy, and public health».

asosiy vazifasi davlat sirlarini himoya qilish va xorijiy axborot oqimlarini kuzatishdan iborat.

2009-yilda esa AQSh Mudofaa vazirligi tarkibida United States Cyber Command (USCYBERCOM) tashkil etildi. Rasmiy ta'rifda u shunday belgilangan: «The mission of USCYBERCOM is to direct, synchronize, and coordinate cyberspace planning and operations to defend and advance national interests»¹. Shu tariqa, kibermakon AQSh armiyasining quruqlik, havo, dengiz va kosmos qatorida beshinchi operatsion domen sifatida tan olindi.

AQSh kibermakon xavfsizligini faqat harbiy sohada emas, balki fuqarolik infratuzilmasida ham ta'minlashga intildi. 2002-yilda tashkil etilgan Department of Homeland Security (DHS) bu borada markaziy rol o'ynadi. DHS o'zining Cybersecurity and Infrastructure Security Agency (CISA) orqali davlat idoralari va xususiy sektor o'rtasida hamkorlikni muvofiqlashtiradi. DHS hisobotida shunday deyiladi: «CISA leads the national effort to understand, manage, and reduce risk to our cyber and physical infrastructure»².

Bu yondashuv AQSh modelining muhim jihatini ko'rsatadi: davlat kiberxavfsizlikni faqat hukumat doirasida emas, balki xususiy sektor bilan hamkorlik asosida ko'rmoqda.

Kibermakon xavfsizligi masalalari AQSh Kongressida muntazam ravishda muhokama qilinib kelmoqda. 2002-yilda qabul qilingan Federal Information Security Management Act (FISMA) davlat idoralarini axborot xavfsizligi bo'yicha qat'iy standartlarni joriy etishga majbur qildi. 2015-yilda esa Cybersecurity Information Sharing Act (CISA) qabul qilinib, davlat va xususiy kompaniyalar o'rtasida kiberxavflar haqidagi

¹ U.S. Cyber Command, Mission Statement, Department of Defense, 2010. «The mission of USCYBERCOM is to direct, synchronize, and coordinate cyberspace planning and operations to defend and advance national interests».

² Department of Homeland Security, Cybersecurity and Infrastructure Security Agency Overview, Washington, 2019. «CISA leads the national effort to understand, manage, and reduce risk to our cyber and physical infrastructure».

ma'lumot almashinuviga huquqiy asos yaratildi¹.

Prezident qarorlari ham bu jarayonda hal qiluvchi rol o'ynadi. Masalan, 2017-yilda Prezident Donald Tramp tomonidan e'lon qilingan Executive Order 13800 hujjatida shunday deyiladi: «The President will hold heads of executive departments and agencies accountable for managing cybersecurity risk to their enterprises»². Bu orqali kibermakon xavfsizligi davlat boshqaruvi tizimining markaziga chiqarildi. AQSH da kibermakon tushunchasiga yondashuv haqida quyidagi xulosalarga kelishimiz mumkin:

1. AQSh kibermakonni milliy xavfsizlikning alohida sohasi sifatida eng erta tan olgan davlatlardan biridir.

2. NSA va USCYBERCOM kibermakonni harbiy strategiyaning ajralmas qismiga aylantirdi.

3. DHS va CISA esa fuqarolik infratuzilmasini himoya qilish va davlat-xususiy sektor hamkorligini kuchaytirishga yo'naltirildi.

4. AQSh Kongressi va Prezident qarorlari kiberxavfsizlikni qonuniy va institutsional darajada mustahkamladi.

AQShda kibermakon tushunchasi tarixan milliy xavfsizlik paradigmasi asosida shakllangan va bu yondashuv uni xalqaro miqyosda ham lider davlatga aylantirgan. AQShda kiberxavfsizlik strategiyalari rivojlanishini 4 bosqichga bo'lishimiz mumkin:

1-bosqich – dastlabki strategiyalar (2003-yil). AQSh kibermakon xavfsizligi bo'yicha birinchi rasmiy hujjatini 2003-yilda qabul qildi. "The National Strategy to Secure Cyberspace" nomli hujjatda shunday deyiladi: «Securing cyberspace is an extraordinarily difficult strategic challenge that requires a coordinated and focused effort from our entire

¹ U.S. Congress, Cybersecurity Information Sharing Act (CISA), Washington D.C., 2015.

² The White House, Executive Order 13800: Strengthening the Cybersecurity of Federal Networks and Critical Infrastructure, Washington D.C., 2017.

society»¹. Bu strategiya uch asosiy tamoyilga asoslangan edi: milliy infratuzilmani himoya qilish, hukumat va xususiy sektor hamkorligi, fuqarolarni kiberhujumlardan xabardor qilish.

Shu davrdan boshlab AQSh kibermakon xavfsizligini milliy mudofaa va iqtisodiy barqarorlik bilan bevosita bog'lab kelmoqda.

2-bosqich – yangilanish(2015-yil). Barak Obama davrida 2015-yilda “Cybersecurity Strategy and Implementation Plan (CSIP)” qabul qilindi. Hujjatda: «We must improve the protection of Federal information and assets against cyber threats by modernizing our systems and improving incident response»², – deya qayd etildi. Ushbu strategiya federal hukumat tizimlarini zamonaviylashtirish va hujumlarga tezkor javob berish mexanizmlarini kuchaytirishga qaratildi.

Obama ma'muriyati, shuningdek, NIST Cybersecurity Framework (2014)ni ishlab chiqdi. Bu ramka xususiy kompaniyalar va davlat idoralarida xavfsizlik standartlarini joriy qilish uchun universal qo'llanma sifatida xizmat qildi.

3-bosqich – Milliy kiberxavfsizlik strategiyasi(2018-yil). Donald Tramp davrida 2018-yilda yangilangan National Cyber Strategy e'lon qilindi. Unda quyidagi tamoyillar belgilandi:

1. Milliy infratuzilmani himoya qilish – energetika, transport, sog'liqni saqlash kabi strategik tarmoqlarni kiberhujumlardan himoyalash.

2. Davlat-xususiy sektor hamkorligini kuchaytirish – korporatsiyalarni milliy xavfsizlik tizimiga jalb qilish.

3. Xalqaro hamkorlik – AQShni global kibermakon siyosatida lider sifatida mustahkamlash. Hujjatda shunday deyilgan: «The United States will use all instruments of national

¹ The White House, The National Strategy to Secure Cyberspace, Washington D.C., 2003. «Securing cyberspace is an extraordinarily difficult strategic challenge...».

² The White House, *Cybersecurity Strategy and Implementation Plan (CSIP)*, Washington D.C., 2015. «We must improve the protection of Federal information and assets...».

power to deter, respond to, and defeat cyber threats»¹.

Bu strategiya AQShning yanada faol va "hujumkor mudofaa" siyosatini belgilab berdi.

4-bosqich – Milliy kiberxavfsizlik strategiyasi(2023). Jozef Bayden ma'muriyati 2023-yilda yangi National Cybersecurity Strategyni qabul qildi. Hujjatda asosiy urg'u davlatning mas'uliyatini oshirishga qaratilgan: «We must rebalance the responsibility for cybersecurity to be more effective, ensuring that the most capable and best-positioned actors bear the greatest burden»².

Bu strategiya quyidagi yangiliklarni o'z ichiga oladi:

- Kiberxavfsizlikni ta'minlashda xususiy kompaniyalar emas, balki davlatning o'zi yetakchi rolni bajarishi kerak.
- AQSh kibermakonni xalqaro hamkorlik orqali global barqarorlik maydoniga aylantirishni maqsad qilmoqda.
- Sun'iy intellekt va kvant texnologiyalari kabi yangi texnologik xavflarga qarshi huquqiy bazani yaratish belgilangan.

AQSh modelining eng muhim xususiyati — bu davlat va xususiy sektorning yaqin hamkorligidir. Chunki AQShda kibermakon infratuzilmasining katta qismi (internet provayderlari, moliyaviy tizimlar, energetika tarmoqlari) xususiy qo'llarda. Shu sababli NIST Cybersecurity Framework va CISA dasturlari orqali korporatsiyalar milliy xavfsizlik tizimiga jalb qilinmoqda.

AQSh kibermakon xavfsizligi masalasida NATOning asosiy drayveri hisoblanadi. 2016-yilgi Varshava sammitida NATO kibermakonni rasmiy ravishda harbiy operatsion domen sifatida tan oldi. NATO rasmiy hujjatida shunday deyilgan: «Cyber defence is part of NATO's core task of collective defence»³. Bu qaror asosan AQSh tashabbusi bilan qabul

¹ The White House, National Cyber Strategy of the United States of America, Washington D.C., 2018. «The United States will use all instruments of national power to deter, respond to, and defeat cyber threats».

² The White House, National Cybersecurity Strategy, Washington D.C., 2023. «We must rebalance the responsibility for cybersecurity...».

³ NATO, *Warsaw Summit Communiqué*, Warsaw, 2016. «Cyber defence is part of NATO's core task of collective defence».

qilingan bo'lib, kibermakonni quruqlik, havo, dengiz va kosmos qatorida strategik maydon sifatida e'tirof etdi.

Shundan beri AQSh NATO davlatlari o'rtasida kiberxavfsizlik bo'yicha mashg'ulotlar, qo'shma mashqlar va bilim almashuv dasturlarini faol qo'llab-quvvatlab kelmoqda. AQShning estoniyalik hamkorlari bilan tashkil etgan NATO Cooperative Cyber Defence Centre of Excellence (CCDCOE) markazi bu borada eng muhim platformalardan biridir.

AQSh va Yevropa Ittifoqi o'rtasidagi kiberxavfsizlik hamkorligi "cyber diplomacy" siyosatining markaziy qismi hisoblanadi. 2018-yilda AQSh Davlat departamenti shunday bayonot bergan: «The United States and the European Union are committed to promoting an open, interoperable, reliable, and secure cyberspace»¹.

Hamkorlik quyidagi yo'nalishlarda rivojlanmoqda:

- Transatlantik infratuzilmani (energetika, transport, moliya) himoya qilish;
- Dezinformatsiya va kiberpropagandaga qarshi qo'shma dasturlar;
- Yevropa Ittifoqining GDPR qonuni va AQShdagi shaxsiy ma'lumotlarni himoya qilish mexanizmlarini muvofiqlashtirish.

AQSh BMT doirasida ham kibermakon xavfsizligi bo'yicha faol ishtirokchi hisoblanadi. 2021-yilda BMTning Open-Ended Working Group (OEWG) yig'ilishida AQSh delegatsiyasi shunday ta'kidlagan: «International law, including the UN Charter, applies in cyberspace»².

AQSh xalqaro huquqda uch tamoyilni ilgari surmoqda:

1. Kibermakon xalqaro huquqning amaldagi normalari bilan tartibga solinadi.
2. Davlatlar kiberhujumlarni amalga oshirganda BMT

¹ U.S. Department of State, U.S.-EU Cyber Dialogue Joint Statement, Washington/Brussels, 2018. «The United States and the European Union are committed to promoting an open, interoperable, reliable, and secure cyberspace».

² United Nations, Open-Ended Working Group on Developments in the Field of ICTs in the Context of International Security, New York, 2021. «International law, including the UN Charter, applies in cyberspace».

Nizomining 2(4)-moddasidagi "kuch ishlatmaslik" tamoyiliga rioya etishlari shart.

3. Xalqaro hamjamiyat kiberxavfsizlik bo'yicha normativ kelishuvlarni kengaytirishi zarur.

AQShning bu pozitsiyasi Tallinn qo'llanmasidagi huquqiy talqinlar bilan hamohangdir.

AQSh "cyber diplomacy" siyosatini ishlab chiqib, kibermakonni tashqi siyosatning asosiy vositalaridan biriga aylantirdi. AQSh Davlat departamentining 2022-yilgi hujjatida shunday deyiladi: «Cyber diplomacy is essential to advancing U.S. foreign policy goals and securing an open, secure, and stable cyberspace»¹.

Bu doirada AQSh:

- Boshqa davlatlar bilan kiberxavfsizlik bo'yicha ikki tomonlama bitimlar tuzadi;
- Xususiy kompaniyalar (Microsoft, Google, IBM) bilan global xavfsizlik tashabbuslarini amalga oshiradi;
- Demokratiya va inson huquqlarini kiberxavfsizlikning ajralmas qismi sifatida targ'ib qiladi.

AQSh kibermakon xavfsizligini tashkil etishda bir necha ustunliklarga ega:

1. Ilmiy va texnologik yetakchilik. AQSh sun'iy intellekt, kvant hisoblash va kibertexnologiyalar sohasida dunyo bo'yicha ilg'or davlatlardan biri hisoblanadi. Bu ustunlik kibermakon xavfsizligini ta'minlashda katta strategik imkoniyatlar yaratadi.

2. Davlat-xususiy sektor hamkorligi. AQSh modeli xususiy kompaniyalarni (Microsoft, Google, IBM, Cisco va boshqalar) milliy xavfsizlik strategiyasiga jalb qilish orqali samaradorlikka erishgan. NIST Cybersecurity Framework hamkorlik mexanizmining yorqin misolidir².

¹ U.S. Department of State, Bureau of Cyberspace and Digital Policy Strategic Plan, Washington D.C., 2022. «Cyber diplomacy is essential to advancing U.S. foreign policy goals and securing an open, secure, and stable cyberspace».

² National Institute of Standards and Technology (NIST), Cybersecurity Framework, Gaithersburg, 2014.

3. Xalqaro liderlik. AQSh NATO va BMT doirasida kibermakonni xalqaro huquqiy tartibotlarga bog'lashda yetakchi rol o'ynab kelmoqda. "Cyber diplomacy" siyosati orqali u kiberxavfsizlikni tashqi siyosatning markaziy yo'nalishiga aylantirgan¹.

4. Normativ barqarorlik. AQSh Kongressi muntazam ravishda kiberxavfsizlik bo'yicha qonunlar qabul qilib, Prezident qarorlari bilan strategik siyosatni doimiy yangilab boradi. Bu kibermakon siyosatining izchilligini ta'minlaydi.

Shu bilan birga, AQSh tajribasi ayrim kamchiliklardan ham holi emas:

1. Maxfiylik va inson huquqlari muammosi. NSA tomonidan olib borilgan kuzatuv amaliyotlari global miqyosda tanqidga uchragan. Edward Snowden fosh etgan ma'lumotlarda «the U.S. surveillance programs collected vast amounts of data from citizens and foreign leaders»² deyilgan. Bu inson huquqlariga putur yetkazuvchi siyosat sifatida baholangan.

2. Kibermakonni militarizatsiya qilish. USCYBERCOM faoliyati kibermakonni asosan harbiy strategiya sifatida talqin qiladi. Bu esa xalqaro barqarorlik o'rniga qurollanish poygasini kuchaytirishi mumkin.

3. Yurisdiksiya va xalqaro nizolar. AQSh texnologik kompaniyalari dunyo bo'ylab faoliyat yuritgani sababli, boshqa davlatlar bilan huquqiy to'qnashuvlar yuzaga kelmoqda. Masalan, Yevropa Ittifoqi GDPR doirasida AQSh kompaniyalarining faoliyatini cheklagan.

Falsafiy nuqtai nazardan, AQSh modeli kibermakonni "qudrat maydoni" sifatida talqin qiladi. Joseph Nye ta'kidlaganidek: «Cyber power is the ability to obtain preferred outcomes through the use of the electronically interconnected

¹ U.S. Department of State, Bureau of Cyberspace and Digital Policy Strategic Plan, Washington, 2022.

² Edward Snowden, Permanent Record, Metropolitan Books, New York, 2019. «the U.S. surveillance programs collected vast amounts of data from citizens and foreign leaders».

information resources of the cyber domain»¹. Demak, AQSh kibermakonni faqat texnik infratuzilma emas, balki geosiyosiy kuch manbai sifatida ko'radi.

Shu bilan birga, konstruktivistlar ta'kidlaganidek, xavfsizlik ijtimoiy konstruksiya bo'lib, jamiyat va davlatlarning xatti-harakatlariga bog'liq. Bu jihatdan AQSh modeli xavfni ko'proq milliy manfaatlar doirasida talqin qiladi, inson huquqlari va axborot erkinligi esa ko'pincha ikkinchi darajaga tushib qoladi.

Huquqiy jihatdan AQSh modeli xalqaro huquq tamoyillariga tayanadi, biroq ularni o'z manfaatlari yo'lida talqin qiladi. Masalan, BMT OEWG doirasida AQSh "xalqaro huquq kibermakonga ham tatbiq etiladi" degan pozitsiyani qo'llab-quvvatlasa-da², amaliyotda NSA kuzatuv dasturlari bu tamoyillarga zid bo'lgan.

Biroq AQShning normativ hujjatlarni muntazam ishlab chiqishi va yangilashi boshqa davlatlar uchun ham amaliy ahamiyatga ega.

AQSh tajribasidan O'zbekiston uchun bir necha muhim saboqlarni olish mumkin:

1. Davlat-xususiy sektor hamkorligini kuchaytirish – chunki O'zbekistonda ham internet provayderlari va axborot texnologiyalari kompaniyalari milliy infratuzilmaning muhim qismi hisoblanadi.

2. Milliy kiberxavfsizlik strategiyasini muntazam yangilab borish – AQSh tajribasida strategiyalar 5–7 yilda qayta ko'rib chiqiladi.

3. Kiberxavfsizlikda xalqaro hamkorlikni kengaytirish – O'zbekiston ham BMT va boshqa xalqaro platformalarda faol ishtirok etishi kerak.

4. Shu bilan birga, inson huquqlari va axborot erkinligi

¹ Joseph S. Nye, *The Future of Power*, PublicAffairs, New York, 2011. «Cyber power is the ability to obtain preferred outcomes through the use of the electronically interconnected information resources of the cyber domain».

² United Nations, *Report of the OEWG on ICTs in the Context of International Security*, New York, 2021.

masalalariga alohida e'tibor qaratish zarur, aks holda kibermakon siyosati jamiyatda ishonchsizlikka olib kelishi mumkin.

2.2. Yevropa Ittifoqi: GDPR va xalqaro standartlar asosida xavfsizlikni ta'minlash.

Yevropa Ittifoqida kibermakon xavfsizligi tushunchasi 2000-yillardan boshlab shakllana boshladi. Internet va raqamli texnologiyalarning tez rivojlanishi Yevropa davlatlarini axborot infratuzilmasini himoya qilish zarurati oldida qoldirdi. 2001-yilda Yevropa Komissiyasi ilk bor "Network and Information Security" bo'yicha maxsus direktivani ishlab chiqdi. Hujjatda: «The security of networks and information systems is essential for the functioning of our societies and economies»¹, – deya ta'kidlangan.

Bu davrda kibermakon masalalari asosan iqtisodiy barqarorlik va raqamli bozor xavfsizligi bilan bog'liq tarzda ko'rilgan bo'lsa, keyinchalik ular milliy va mintaqaviy xavfsizlikning ajralmas qismiga aylandi.

2009-yilda kuchga kirgan Lissabon shartnomasi Yevropa Ittifoqining umumiy xavfsizlik siyosatiga yangi qoidalarni kiritdi. Shu jumladan, kibermakon xavfsizligi ham umumiy tashqi va xavfsizlik siyosati (CFSP) doirasiga qo'shildi. Yevropa Parlamenti hujjatida shunday deyilgan: «The Lisbon Treaty provides the EU with new instruments to face cyber threats as part of the Common Security and Defence Policy»².

Bu huquqiy yangilik Yevropa Ittifoqiga kibermakonni nafaqat iqtisodiy, balki siyosiy va mudofaa sohasida ham strategik

¹ European Commission, Network and Information Security: Proposal for a European Policy Approach, Brussels, 2001. «The security of networks and information systems is essential for the functioning of our societies and economies».

² European Parliament, The Lisbon Treaty and EU Security Policy, Strasbourg, 2009. «The Lisbon Treaty provides the EU with new instruments to face cyber threats as part of the Common Security and Defence Policy».

ustuvor yo'nalish sifatida belgilash imkonini berdi.

2004-yilda tashkil etilgan ENISA (European Union Agency for Cybersecurity) Yevropa Ittifoqida kiberxavfsizlikni muvofiq-lashtiruvchi asosiy agentlikdir. ENISAning asosiy vazifalari:

1. Kibermakon xavfsizligi bo'yicha siyosiy tavsiyalar ishlab chiqish;
2. A'zo davlatlarga huquqiy va texnik yordam ko'rsatish;
3. Kiberxavfsizlik bo'yicha ilmiy tadqiqotlarni qo'llab-quvvatlash;
4. Fuqarolarni xabardor qilish va kiberhujumlarga qarshi tayyorlash.

ENISA hisobotida shunday deyilgan: «ENISA works with Members States and the private sector to develop and implement effective cybersecurity policies»¹. Demak, agentlik faqat davlat organlari bilan emas, balki xususiy sektor bilan hamkorlikda faoliyat yuritadi.

Yevropa Ittifoqi kibermakon xavfsizligini tartibga solishda uchta tamoyilga asoslanadi:

1. Ko'p darajali boshqaruv – Yevropa Komissiyasi, Yevropa Parlamenti, ENISA va milliy hukumatlarning birgalikdagi faoliyati.
2. Fuqarolik huquqlariga ustuvorlik – kiberxavfsizlik inson huquqlari, maxfiylik va erkinlik bilan uyg'unlashishi shart.
3. Davlat–xususiy sektor hamkorligi – infratuzilmaning katta qismi xususiy qo'llarda bo'lgani uchun, ular xavfsizlik tizimiga faol jalb qilinadi.

Yevropa Ittifoqida shaxsiy ma'lumotlarni himoya qilish masalasi 1995-yilda qabul qilingan Data Protection Directive (95/46/EC) bilan huquqiy asosga ega bo'ldi. Bu hujjatda shunday deyiladi: «Member States shall protect the fundamental rights and freedoms of natural persons, and in particular their right to privacy with respect to the processing of personal

¹ ENISA, About ENISA, Athens, 2020. «ENISA works with Members States and the private sector to develop and implement effective cybersecurity policies».

data»¹.

Mazkur direktiva Yevropa davlatlari uchun birinchi marta yagona standart yaratdi. Asosiy tamoyillar shundan iborat edi:

- Shaxsiy ma'lumotlarni faqat qonuniy va adolatli yo'lda yig'ish;
- Ularni faqat aniq ko'zlangan maqsadlarda qayta ishlash;
- Ma'lumotlarning maxfiyligi va yaxlitligini saqlash.

Biroq bu direktiva texnologiyalar tez rivojlangan sharoitda eskirib qoldi va turli davlatlarda turlicha talqin qilina boshladi.

2016-yilda Yevropa Parlamenti tomonidan qabul qilingan va 2018-yildan kuchga kirgan General Data Protection Regulation (GDPR) butun dunyo uchun ma'lumotlarni himoya qilishning yangi standartini belgiladi. GDPR matnida shunday deyiladi: «The protection of natural persons in relation to the processing of personal data is a fundamental right»².

GDPRning asosiy tamoyillari:

1. Rozilik tamoyili – shaxsiy ma'lumotlar faqat ma'lumot egasining ochiq roziligi bilan qayta ishlanishi mumkin.
2. Ma'lumot sub'ektining huquqlari – har bir shaxs o'z ma'lumotlarini ko'rish, tuzatish yoki butunlay o'chirish ("right to be forgotten") huquqiga ega.
3. Ma'lumotlarni himoya qilish by design – dasturiy va texnologik tizimlarda ma'lumotlarni himoya qilish mexanizmlari oldindan joriy etilishi kerak.
4. Xalqaro tatbiq – GDPR nafaqat Yevropa ichida, balki Yevropa fuqarolari bilan ishlovchi barcha xorijiy kompaniyalarga ham tatbiq etiladi.

GDPRning global ahamiyati uning transchegaraviy kuchida namoyon bo'ldi. Masalan, AQShning Google va Facebook kabi kompaniyalari ham Yevropa fuqarolarining ma'lumotlarini

¹ European Parliament, Directive 95/46/EC on the Protection of Individuals with Regard to the Processing of Personal Data, Brussels, 1995. «Member States shall protect the fundamental rights and freedoms of natural persons...».

² European Parliament, General Data Protection Regulation (GDPR), Brussels, 2016. «The protection of natural persons in relation to the processing of personal data is a fundamental right».

qayta ishlashda GDPR talablariga bo'ysunishga majbur bo'ldi. Shu bois ko'plab tadqiqotchilar GDPRni «the global gold standard for data protection»¹ deb atashmoqda.

GDPR boshqa davlatlarga ham ta'sir qildi. Masalan:

- Braziliya LGPD (Lei Geral de Proteção de Dados) qonunini qabul qildi (2020).
- Yaponiya o'zining APPI (Act on the Protection of Personal Information) qonunini Yevropa talablariga moslashtirdi.
- Janubiy Koreya va Avstraliya ham shunga o'xshash qonunlarni qabul qildilar.

GDPRdan tashqari Yevropa Ittifoqi quyidagi tashabbuslarni ham amalga oshirmoqda:

- ePrivacy Regulation – elektron aloqa orqali uzatiladigan ma'lumotlarni himoya qilish uchun maxsus huquqiy mexanizm.
- Data Governance Act (2020) – ma'lumotlardan foydalanish va ularni boshqarishda shaffoflikni oshirish.
- Digital Services Act (2022) – onlayn platformalar faoliyatini tartibga solish va foydalanuvchilarning huquqlarini himoya qilish.

Yevropa Ittifoqi o'zining birinchi keng qamrovli kiberxavfsizlik strategiyasini 2013-yilda qabul qildi. Hujjatda shunday deyiladi: «The EU's digital future depends on trust and security»². Ushbu strategiya besh asosiy ustuvor yo'nalishga ega edi:

1. Kibermakonda erkinlik va ochiqlikni saqlash.
2. Yevropa Ittifoqining chidamliligini oshirish.
3. Kibermakonda samarali jinoyatga qarshi kurash.
4. Mudofaa siyosatini kuchaytirish.
5. Xalqaro hamkorlikni rivojlantirish.

Bu strategiya kibermakon xavfsizligini nafaqat texnik, balki

¹ Graham Greenleaf, Global Data Privacy Laws 2019: 132 National Laws and Many Bills, Privacy Laws & Business International Report, 2019. «GDPR is the global gold standard for data protection».

² European Commission, Cybersecurity Strategy of the European Union: An Open, Safe and Secure Cyberspace, Brussels, 2013. «The EU's digital future depends on trust and security».

siyosiy va ijtimoiy hodisa sifatida ham talqin qildi.

2020-yilda Yevropa Komissiyasi yangi EU Cybersecurity Strategy for the Digital Decade hujjatini e'lon qildi. Unda: «Cybersecurity is a cornerstone of the digital and green transition»¹, – deb ta'kidlangan.

Asosiy yangiliklar quyidagilardan iborat:

- 5G va yangi texnologiyalar xavfsizligi: 5G tarmoqlarini kiberhujumlardan himoya qilish bo'yicha "EU 5G Toolbox" ishlab chiqildi.

- Kiberkrisisga qarshi tayyorgarlik: a'zo davlatlar o'rtasida tezkor axborot almashish va qo'shma javob tizimlari yaratildi.

- Kiberxavfsizlikni mudofaa siyosatiga integratsiya qilish: NATO bilan hamkorlik yanada mustahkamlandi.

- Xalqaro diplomatiya: Yevropa Ittifoqi "cyber diplomacy toolbox" orqali dezinformatsiya va kiberhujumlarga qarshi sanksiyalar qo'llash huquqiga ega bo'ldi.

Yevropa Ittifoqi 2021–2027-yillarga mo'ljallangan Digital Europe Programmeni qabul qildi. Unda kiberxavfsizlikni mustahkamlash uchun 1,9 milliard yevro mablag' ajratilgan. Hujjatda shunday deyiladi: «The programme will strengthen Europe's digital capacities, including cybersecurity and trust»².

Bu dastur nafaqat texnologik infratuzilmani, balki mutaxassislarni tayyorlash va ilmiy tadqiqotlarni qo'llab-quvvatlashga qaratilgan.

2023-yilda Yevropa Komissiyasi Cyber Solidarity Actni taklif qildi. Uning maqsadi – Yevropada birgalikdagi mudofaa mexanizmini kuchaytirish. Unda quyidagilar nazarda tutiladi:

- Kiberhujumlar yuzaga kelganda a'zo davlatlar o'rtasida o'zaro yordam mexanizmi.

¹ European Commission, EU Cybersecurity Strategy for the Digital Decade, Brussels, 2020. «Cybersecurity is a cornerstone of the digital and green transition».

² European Commission, Digital Europe Programme 2021–2027, Brussels, 2021. «The programme will strengthen Europe's digital capacities, including cybersecurity and trust».

- Pan-Yevropa kiberxavfsizlik testlash markazlari.
- Kiberhujumlarni kuzatish va prognozlash uchun Yevropa darajasida monitoring tizimi.

Bu tashabbus Yevropa Ittifoqining kibermakonda “strategik avtonomiya”ga erishish intilishini ifodalaydi.

Yevropa Ittifoqining yana bir xususiyati — bu xususiy sektor bilan yaqin hamkorlik. ENISA va NIS2 direktivasi orqali telekommunikatsiya, energetika, sogʻliqni saqlash va transport kabi infratuzilma egalariga majburiy xavfsizlik standartlari yuklatilgan.

Yevropa Ittifoqi kibermakon xavfsizligini ta'minlashda bir qator ustunliklarga ega:

1. Inson huquqlariga ustuvorlik. Yevropa modeli kibermakon xavfsizligini shaxsiy huquqlar va erkinliklar bilan uyg'unlashtirishga intiladi. GDPR shunday deyadi: «The protection of natural persons in relation to the processing of personal data is a fundamental right»¹. Bu kibermakon siyosatida huquqiy asoslarni inson sha'ni va daxlsizligiga bog'lashni ko'rsatadi.

2. Huquqiy barqarorlik. 1995-yildan boshlab qabul qilingan direktiva va reglamentlar orqali Yevropa Ittifoqi kibermakonni huquqiy tartibga solishda izchil tizim yaratdi. GDPR, ePrivacy Regulation va Data Governance Act Yevropaning normativ kuchini ko'rsatadi.

3. Davlat–xususiy sektor hamkorligi. ENISA, NIS2 direktivasi va Digital Europe dasturi davlat bilan xususiy kompaniyalarni umumiy xavfsizlik mexanizmiga jalb qilmoqda.

4. Xalqaro ta'sir. GDPR va boshqa normativ hujjatlar nafaqat Yevropa ichida, balki global miqyosda ham qo'llanmoqda. Shu bois ko'plab davlatlar Yevropa modelini “oltin standart” sifatida qabul qilmoqda.

Shu bilan birga, Yevropa modelida ayrim cheklovlar ham mavjud:

¹ European Parliament, General Data Protection Regulation (GDPR), Brussels, 2016. «The protection of natural persons in relation to the processing of personal data is a fundamental right».

1. Byurokratik murakkablik. Yevropa Ittifoqi 27 a'zo davlatdan iborat bo'lgani sababli, normativ hujjatlarni amalda bir xilda tatbiq qilish qiyin. Bu esa samaradorlikni pasaytirishi mumkin.

2. Texnologik qaramlik. Yevropa kompaniyalari (masalan, telekommunikatsiya va bulutli xizmatlar) ko'pincha AQSh yoki Xitoy texnologiyalaridan foydalanadi. Bu Yevropaning "strategik avtonomiya" sini zaiflashtiradi.

3. Sanksiyalar va biznesga yuklama. GDPR juda qat'iy talablarni joriy qilgani sababli, kichik va o'rta korxonalar uchun huquqiy yuklama ortib ketgan.

Falsafiy nuqtai nazardan, Yevropa modeli kibermakonni "inson markazli makon" sifatida talqin qiladi. Luciano Floridi aytganidek: «The infosphere must be shaped in ways that respect human dignity and autonomy»¹. Yevropa modeli texnologiyani inson sha'ni, daxlsizligi va axloqiy me'yorlar bilan uyg'unlashtirishni maqsad qiladi.

Biroq, Baudrillard nazariyasi nuqtai nazaridan qaralsa, Yevropa modelining ham muammosi bor: kiberpropaganda va soxta axborot oqimlari real haqiqatni simulyatsiya bilan almashtirib qo'ymoqda. Bu esa inson erkinligi va demokratiya uchun xavf tug'diradi.

Huquqiy jihatdan Yevropa modeli inson huquqlariga asoslangan yondashuvdir. BMTning inson huquqlari bo'yicha maxsus ma'ruzachisi ham GDPRni yuqori baholab: «GDPR represents a landmark in aligning data protection with international human rights law»², – deb ta'kidlagan.

Shu bilan birga, Yevropa Ittifoqining "Cyber Diplomacy Toolbox" tashabbusi kibermakonni xalqaro huquqiy tartibotga bog'lashda muhim qadamdir.

¹ Luciano Floridi, *The Ethics of Information*, Oxford University Press, 2013, p. 121. «The infosphere must be shaped in ways that respect human dignity and autonomy».

² United Nations Human Rights Council, *Report of the Special Rapporteur on the right to privacy*, Geneva, 2018. «GDPR represents a landmark in aligning data protection with international human rights law».

Yevropa Ittifoqi tajribasidan O'zbekiston uchun bir nechta saboqlar mavjud:

- Shaxsiy ma'lumotlarni himoya qilish qonunchiligini kuchaytirish – Yevropa modelidan o'rganib, O'zbekistonda ham shaxsiy ma'lumotlarni qayta ishlashni qat'iy tartibga soluvchi huquqiy baza yaratish zarur.
- Inson huquqlariga asoslangan yondashuv – kibermakon siyosatida texnologik xavfsizlik bilan bir qatorda axloqiy va huquqiy me'yorlarni ham hisobga olish.
- Davlat-xususiy sektor hamkorligi – O'zbekistonda telekommunikatsiya va IT-kompaniyalarni milliy kiberxavfsizlik tizimiga faol jalb qilish.
- Xalqaro integratsiya – O'zbekiston Yevropa tajribasidan foydalanib, mintaqaviy va global hamkorlikda o'z o'rnini mustahkamlashi mumkin.

2.3. Rossiya Federatsiyasi: milliy xavfsizlik konsepsiyasi va kibermakonni nazorat qilish yondashuvlari

Rossiyada kibermakon xavfsizligi tushunchasi 2000-yillarning boshlarida milliy xavfsizlik siyosatiga kiritila boshladi. 2000-yilda qabul qilingan Rossiya Federatsiyasining Milliy xavfsizlik konsepsiyasida axborot xavfsizligi davlat xavfsizligining muhim elementi sifatida belgilandi. Hujjatda shunday deyilgan: «Обеспечение информационной безопасности является одним из важнейших направлений национальной безопасности Российской Федерации»¹. Bu davrda Rossiya axborot xavfsizligini nafaqat texnik jihatdan, balki mafkuraviy va siyosiy jihatdan ham ko'rdi. Chunki internet Rossiyada tez ommalashib, davlat suverenitetiga yangi chaqiriqlar tug'dirayotgan edi.

¹ Rossiya Federatsiyasi, Концепция национальной безопасности Российской Федерации, Москва, 2000. «Обеспечение информационной безопасности является одним из важнейших направлений национальной безопасности Российской Федерации».

Rossiyada “axborot xavfsizligi” atamasi kibermakondan kengroq ma’noga ega bo’lib, u axborot oqimlari ustidan nazorat, davlat sirlarini himoya qilish, axborot-kommunikatsiya texnologiyalaridan noqonuniy foydalanishga qarshi choralarni o’z ichiga oladi. 2000-yilda qabul qilingan Rossiya Federatsiyasining Axborot xavfsizligi doktrinasida shunday deyiladi: «Информационная безопасность понимается как состояние защищенности личности, общества и государства от внутренних и внешних информационных угроз»¹.

Demak, Rossiyada kibermakon tushunchasi ilk bosqichdan boshlab siyosiy va mafkuraviy kontekstda talqin qilingan.

Rossiya Federatsiyasida kibermakon xavfsizligini ta'minlashning asosiy instituti Federal Xavfsizlik Xizmati (FSB) hisoblanadi. FSB internetdagi axborot oqimlarini nazorat qilish, kiberjinoyatlarga qarshi kurashish va davlat infratuzilmasini himoya qilish bilan shug’ullanadi.

Shuningdek, Rossiya Mudofaa vazirligi ham o’zining maxsus kiberqo’shinlarini tuzganini 2013-yilda e’lon qilgan. Ularning asosiy vazifasi – davlat infratuzilmasini himoya qilish va hujumkor kiberoperatsiyalarni amalga oshirish.

Rossiya kibermakonni davlat suverenitetining ajralmas qismi sifatida ko’radi. Prezident Vladimir Putin 2012-yilda shunday degan edi: «Цифровое пространство — это сфера, где мы должны обеспечить такой же уровень суверенитета, как и на суше, в воздухе и на море»².

Shu bois Rossiyada kibermakon xavfsizligi nafaqat texnik himoya, balki siyosiy nazorat vositasi sifatida ham shakllandi. Bu yondashuv keyinchalik “suveren internet” konsepsiyasining paydevorini yaratdi.

¹ Rossiya Federatsiyasi, Доктрина информационной безопасности Российской Федерации, Москва, 2000. «Информационная безопасность понимается как состояние защищенности личности, общества и государства от внутренних и внешних информационных угроз».

² Vladimir Putin, Выступление на заседании Совета безопасности Российской Федерации, Москва, 2012. «Цифровое пространство — это сфера, где мы должны обеспечить такой же уровень суверенитета, как и на суше, в воздухе и на море».

Rossiyada kiberxavfsizlik bo'yicha eng muhim qonunlardan biri – 2016-yilda qabul qilingan “Yarovaya paketi” (Федеральный закон №374-ФЗ va №375-ФЗ) hisoblanadi. Ushbu qonunlar terrorizmga qarshi kurash bahonasida qabul qilingan bo'lib, internet va telekommunikatsiya xizmat ko'rsatuvchi kompaniyalarni ma'lumotlarni saqlash va xavfsizlik xizmatlariga taqdim etishga majbur qiladi. Hujjatda shunday deyiladi: «Операторы связи обязаны хранить содержание сообщений пользователей до шести месяцев и предоставлять доступ к ним уполномоченным органам»¹.

Bu qonun Rossiyada internet ustidan davlat nazoratini keskin kuchaytirdi. Tanqidchilarning fikricha, u fuqarolarning shaxsiy hayoti daxlsizligiga tahdid soladi.

2019-yilda Rossiya “Suveren internet to'g'risida”gi qonunni qabul qildi (Федеральный закон №90-ФЗ). Ushbu hujjat Rossiya internet segmentini (RuNet) tashqi tarmoqlardan mustaqil ishlashga tayyorlashni maqsad qilgan. Qonunda shunday deyilgan: «Функционирование сети Интернет на территории Российской Федерации должно обеспечивать устойчивость, безопасность и целостность RuNet»².

Qonun asosida Roskomnadzor davlat idorasi internet trafigini markazlashtirilgan boshqaruv ostiga oldi. Shuningdek, davlat maxsus hollarda xalqaro internet aloqasini to'sib qo'yish huquqiga ega bo'ldi.

Rossiyada kiberxavfsizlik masalalari strategik hujjatlar orqali ham tartibga solinadi. 2016-yilda Prezident Vladimir Putintomonidan imzolangan Rossiya Federatsiyasining Axborot xavfsizligi doktrinasida shunday deyilgan: «Основными угрозами информационной безопасности являются

¹ Rossiya Federatsiyasi, Федеральный закон №374-ФЗ и №375-ФЗ (“пакет Яровой”), Moskva, 2016. «Операторы связи обязаны хранить содержание сообщений пользователей до шести месяцев и предоставлять доступ к ним уполномоченным органам».

² Rossiya Federatsiyasi, Федеральный закон №90-ФЗ “О суверенном Интернете”, Moskva, 2019. «Функционирование сети Интернет на территории Российской Федерации должно обеспечивать устойчивость, безопасность и целостность RuNet».

использование ИКТ в военных целях, киберпреступность и информационные воздействия на общественное сознание»¹.

Bu doktrinada nafaqat texnik hujumlar, balki “axborot urushi” va “ommaviy ongini manipulyatsiya qilish” ham xavf sifatida belgilangan. Bu Rossiya modelining mafkuraviy jihatdan ham o'ziga xosligini ko'rsatadi.

Rossiya kibermakon xavfsizligini tartibga solishda bir nechta strategik hujjatlarni qabul qilgan:

- Milliy xavfsizlik strategiyasi (2021) – unda kiberxavfsizlik Rossiya suverenitetining asosiy omillaridan biri sifatida belgilangan.

- Raqamli iqtisodiyot dasturi (2017) – raqamlashtirish bilan birga kiberxavfsizlikni milliy ustuvor yo'nalish sifatida belgilaydi.

- Mudofaa vazirligi kiberstrategiyasi – Rossiyaning kiberqo'shinlari faoliyatini huquqiy asoslash uchun ishlab chiqilgan.

Rossiya kibermakon siyosatining eng muhim jihatlaridan biri – bu internet ustidan markazlashgan davlat nazoratini o'rnatishdir. Bu jarayonda asosiy rolni Roskomnadzor – aloqa va axborot sohasini nazorat qiluvchi federal idora bajaradi. Roskomnadzor vakolatlari kengaytirilgan bo'lib, u “qonungazid” deb topilgan saytlarni bloklash, ijtimoiy tarmoqlarni tartibga solish va axborot oqimlarini nazorat qilish huquqiga ega. 2020-yilda Rossiya qonunida shunday deyilgan: «Интернет-платформы обязаны удалять запрещённый контент и предоставлять отчётность в Роскомнадзор»². Bu amaliyot

¹ Rossiya Federatsiyasi, Доктрина информационной безопасности Российской Федерации, Москва, 2016. «Основными угрозами информационной безопасности являются использование ИКТ в военных целях, киберпреступность и информационные воздействия на общественное сознание».

² Rossiya Federatsiyasi, Федеральный закон о регулировании деятельности интернет-платформ, Москва, 2020. «Интернет-платформы обязаны удалять запрещённый контент и предоставлять отчётность в Роскомнадзор».

fuqarolarning axborot erkinligi va senzura masalalariga oid xalqaro bahslarni kuchaytirgan.

2019-yilda qabul qilingan “Suveren internet” qonunidan keyin Rossiya oʻzining milliy internet segmenti – RuNetni rivojlantirishga kirishdi. Ushbu tizim asosiy ikki funksiyani bajaradi:

1. Tashqi aloqalardan mustaqil ishlash – Rossiya xalqaro internet tarmoqlaridan ajralib, ichki infratuzilma asosida faoliyat yurita oladi.

2. Markazlashgan trafik boshqaruvi – barcha internet trafigi maxsus davlat tugunlari orqali oʻtadi.

Rossiya hukumati bu yondashuvni milliy xavfsizlikni mustahkamlash deb izohlaydi. Biroq tanqidchilarning fikricha, bu usul internetni davlat nazoratiga toʻliq berib, jamiyatni tashqi dunyodan ajratib qoʻyishi mumkin.

Rossiyada dezinformatsiyaga qarshi kurash ham kiberxavfsizlik siyosatining muhim qismidir. 2019-yilda qabul qilingan qonunga koʻra, “soxta yangiliklar” (fake news) tarqatgan shaxslar yoki OAV jarimaga tortilishi mumkin. Qonunda shunday deyilgan: «Распространение недостоверной общественно значимой информации влечёт административную ответственность»¹.

Bu qonun dezinformatsiyaga qarshi kurash vositasi sifatida joriy etilgan boʻlsa-da, xalqaro tashkilotlar uni soʻz erkinligini cheklash vositasi sifatida tanqid qilmoqda. Masalan, Reporters Without Borders tashkiloti shunday degan: «The Russian fake news law provides authorities with excessive power to silence dissent»².

Rossiya oʻzini kiberhujumlardan himoya qilishni ustuvor deb biladi. Shu bilan birga, koʻplab xalqaro manbalar Rossiyaning

¹ Rossiya Federatsiyasi, Федеральный закон о недостоверной информации (fake news law), Moskva, 2019. «Распространение недостоверной общественно значимой информации влечёт административную ответственность».

² Reporters Without Borders, Russia: Fake News Law as a Weapon Against Free Press, Paris, 2019. «The Russian fake news law provides authorities with excessive power to silence dissent».

o'zi ham hujumkor kiberoperatsiyalarni amalga oshirayotganini qayd etgan. Masalan, NATO 2021-yilda Rossiyaning bir nechta G'arb davlatlariga qarshi yirik kiberhujumlarda ayblagan¹. Rossiya esa bu ayblovlarni inkor etib, o'zining "mudofaa xarakteridagi kiberstrategiya"ni himoya qilib kelmoqda.

Rossiya tajribasi kibermakon xavfsizligi bo'yicha bir qator ustunliklarga ega:

1. Milliy suverenitetni ustuvor qo'yish. Rossiya kibermakonni davlat suverenitetining muhim elementi sifatida ko'radi. "Suveren internet" konsepsiyasi davlatni tashqi tahdidlardan himoya qilish uchun mustaqil infratuzilma yaratishga qaratilgan².

2. Davlat institutlarining markazlashgan roli. FSB, Roskomnadzor va Mudofaa vazirligi kabi organlarning faoliyati davlat siyosatini izchil amalga oshirishga imkon beradi.

3. Axborot urushlariga tayyorgarlik. Axborot xavfsizligi doktrinasida "ommaviy ongning manipulyatsiya qilish" xavf sifatida belgilanishi Rossiyaning kibermakonda mafkuraviy barqarorlikni ham muhofaza qilishga intilayotganini ko'rsatadi³.

Biroq bu model bir qator cheklovlardan ham holi emas:

1. So'z erkinligi va inson huquqlari cheklanishi. Yarovaya paketi va "fake news law" kabi qonunlar fuqarolarning shaxsiy hayoti va erkinliklariga tahdid sifatida baholangan. Reporters Without Borders ta'kidlaganidek: «The Russian fake news law provides authorities with excessive power to silence dissent»⁴.

2. Izolyatsiya xavfi. RuNet tashqi internetdan ajralib ishlashga tayyorlansa-da, bu Rossiyaning global axborot oqimlaridan uzib qo'yish xavfini tug'diradi.

¹ NATO, Statement on Malicious Cyber Activities Attributed to Russia, Brussels, 2021.

² Rossiya Federatsiyasi, Федеральный закон №90-ФЗ "О суверенном Интернете", Moskva, 2019.

³ Rossiya Federatsiyasi, Доктрина информационной безопасности Российской Федерации, Moskva, 2016.

⁴ Reporters Without Borders, Russia: Fake News Law as a Weapon Against Free Press, Paris, 2019.

3. Xalqaro tanqid va sanksiyalar. Rossiyaning hujumkor kiberoperatsiyalarda ayblanishi (masalan, NATO bayonotlari) uning xalqaro obro'siga putur yetkazmoqda¹.

Falsafiy jihatdan Rossiya modeli kibermakonni "geosiyosiy jang maydoni" sifatida talqin qiladi. Vladimir Putin ta'kidlaganidek: «Цифровое пространство — это сфера, где мы должны обеспечить такой же уровень суверенитета, как и на суше, в воздухе и на море»². Bu yondashuv realizm paradigmasiga yaqin bo'lib, kibermakon xavfsizligini milliy kuchni mustahkamlash vositasi sifatida ko'radi. Biroq liberal va konstruktivistik nazariyalar nuqtai nazaridan, bu yondashuv hamkorlik va axborot erkinligini cheklaydi.

Huquqiy jihatdan Rossiya modeli "davlat markazli kiber-xavfsizlik" yondashuviga asoslanadi. Suveren internet va Yarovaya qonunlari orqali davlat internet trafigini to'liq nazorat qiladi. Bu esa milliy xavfsizlikni mustahkamlasa-da, xalqaro huquq normalarida belgilangan inson huquqlari bilan ziddiyatga kirishadi.

2.4. Xitoy Xalq Respublikasi: davlat nazorati va milliy modelning xususiyatlari.

Xitoy kibermakon xavfsizligida o'ziga xos konsepsiyani ishlab chiqdi. Bu konsepsiya "kibersuverenitet" deb ataladi. Uning mazmuni shundaki, har bir davlat o'z hududi va xalqida internet ustidan to'liq nazoratga ega bo'lishi kerak. Xitoy yetakchisi Si Szinpin 2014-yilda o'tkazilgan World Internet Conferenceda shunday degan edi: «Each country has the right

¹ NATO, Statement on Malicious Cyber Activities Attributed to Russia, Brussels, 2021.

² Vladimir Putin, Выступление на заседании Совета безопасности Российской Федерации, Moskva, 2012.

to choose its own path of cyber development, model of cyber regulation, and public policies on cyberspace»¹.

Bu yondashuv g'arbiy modeldan keskin farq qiladi, chunki Yevropa va AQSh kibermakonni erkin va ochiq global maydon sifatida tasavvur qiladi. Xitoy esa kibermakonni davlat suverenitetining ajralmas qismi sifatida ko'radi.

2000-yillarda Xitoy hukumati internetni tez kengayishi bilan birga, u orqali mamlakat ichki barqarorligiga xavf tug'ilishini anglab yetdi. Shu bois "Buyuk Xitoy devori" (Great Firewall of China) tizimi yaratildi. Bu tizim xalqaro saytlar va ijtimoiy tarmoqlarga (Google, Facebook, Twitter) kirishni cheklab, Xitoy internetini tashqi ta'sirlardan himoya qildi.

Xitoy hukumatining qarashiga ko'ra, bu choralar davlat suverenitetini himoya qilish va milliy xavfsizlikni ta'minlash uchun zarur. Rasmiy Pekin buni "barqarorlik siyosati" deb ataydi.

Xitoy rahbarlari kibermakonga doimiy ravishda siyosiy e'tibor qaratib keladi. Si Zinpin 2016-yilda shunday degan edi: «Without cybersecurity, there is no national security; without informatization, there is no modernization»². Bu fikr Xitoy siyosatida kibermakonni milliy xavfsizlik va taraqqiyotning ajralmas qismi sifatida ko'rsatadi.

Shuningdek, Xitoy hukumati kibermakonni mafkuraviy maydon sifatida ham talqin qiladi. Bu borada "axborot xavfsizligi" tushunchasi nafaqat texnik himoyani, balki jamiyatda "to'g'ri" mafkuraviy yo'nalishni shakllantirishni ham o'z ichiga oladi.

Xitoy nafaqat ichki siyosatda, balki xalqaro miqyosda ham "kibersuverenitet"ni faol targ'ib qilmoqda. BMT doirasida Xitoy delegatsiyasi bir necha bor shunday fikr bildirgan: «Cyber

¹ Xi Jinping, Speech at the World Internet Conference, Wuzhen, 2014. «Each country has the right to choose its own path of cyber development, model of cyber regulation, and public policies on cyberspace».

² Xi Jinping, Address at the National Cybersecurity and Informatization Work Conference, Beijing, 2016. «Without cybersecurity, there is no national security; without informatization, there is no modernization».

sovereignty is the foundation for building a community with a shared future in cyberspace»¹.

Bu yondashuv Xitoyning internetni global boshqaruvda davlatlararo tamoyil asosida tartibga solish tarafdori ekanligini ko'rsatadi.

Xitoyda kibermakonni tartibga soluvchi asosiy huquqiy hujjat — 2017-yilda qabul qilingan Kiberxavfsizlik to'g'risidagi qonun (Cybersecurity Law of the People's Republic of China) hisoblanadi. Ushbu qonunda shunday deyilgan: «The state shall safeguard cyberspace sovereignty, national security, and the rights and interests of citizens in cyberspace»².

Asosiy talablar:

- Internet xizmat ko'rsatuvchi kompaniyalar foydalanuvchilar ma'lumotlarini Xitoy hududida saqlashi shart;
- Kompaniyalar davlat organlariga kiberxavflarni aniqlash va tekshirishda yordam berishi lozim;
- “Zarur texnik choralar” orqali siyosiy jihatdan nomaqbul deb topilgan kontentni bloklash.

Bu qonun Xitoyning internet ustidan to'liq nazoratini huquqiy jihatdan mustahkamladi.

Xitoy 2021-yilda ikkita muhim qonunni qabul qildi:

1. Data Security Law (DSL) – ma'lumotlarni milliy xavfsizlikning asosiy resursi sifatida belgilaydi. Unda: «Data is a basic strategic resource of the state»³, – deb yozilgan. Bu hujjat strategik ahamiyatga ega ma'lumotlarni xorijga chiqarishni qat'iy tartibga soldi.

2. Personal Information Protection Law (PIPL) – shaxsiy ma'lumotlarni himoya qilish bo'yicha Xitoyning ilk keng

¹ United Nations, Statement by the Chinese Delegation on Cyber Sovereignty, New York, 2019. «Cyber sovereignty is the foundation for building a community with a shared future in cyberspace».

² National People's Congress of China, Cybersecurity Law of the People's Republic of China, Beijing, 2017. «The state shall safeguard cyberspace sovereignty, national security, and the rights and interests of citizens in cyberspace».

³ National People's Congress of China, Data Security Law, Beijing, 2021. «Data is a basic strategic resource of the state».

qamrovli qonuni bo'lib, u Yevropa Ittifoqining GDPRiga yaqin tamoyillarga asoslanadi. Qonunda: «The processing of personal information shall be lawful, justified, necessary, and with the individual's consent»¹.

Bu ikki qonun Xitoyning ma'lumotlar ustidan suverenitetini mustahkamlash bilan birga, uni xalqaro hamjamiyat oldida "ma'lumotlarni tartibga soluvchi davlat" sifatida ko'rsatdi.

Xitoyning kibermakon siyosati bir necha doktrinalarga asoslanadi:

- "Kibersuverenitet" – internet davlat hududi va suverenitetining ajralmas qismi.
- "Barqarorlik birinchi o'rinda" – internet mafkuraviy va siyosiy barqarorlikni ta'minlash uchun nazorat qilinadi.
- "MahalliyLashtirish" siyosati – xorijiy texnologiyalar o'rniga milliy IT-gigantlarni rivojlantirish.

Xitoy BMT va boshqa xalqaro tashkilotlarda "kibersuverenitet" konsepsiyasini targ'ib qiladi. 2019-yilda BMT minbarida Xitoy vakillari shunday bayonot bergan: «Every country has the right to regulate its cyberspace according to its national laws, traditions, and culture»².

Bu yondashuv global internetni davlatlararo boshqaruvga bo'ysundirish tarafdori bo'lsa-da, ko'plab g'arb davlatlari uni "internetni fragmentatsiyalash" xavfi sifatida baholaydi.

Xitoy kibermakon siyosatining eng mashhur elementi – bu Buyuk Xitoy devori (Great Firewall of China) hisoblanadi. Ushbu tizim orqali hukumat xalqaro internet resurslariga kirishni cheklaydi. Google, Facebook, Twitter, YouTube kabi platformalarga Xitoy ichidan to'g'ridan-to'g'ri kirish mumkin emas. Rasmiy Pekin bu siyosatni "axborot xavfsizligi" va "milliy barqarorlik"ni ta'minlash vositasi deb ataydi.

¹ National People's Congress of China, Personal Information Protection Law (PIPL), Beijing, 2021. «The processing of personal information shall be lawful, justified, necessary, and with the individual's consent».

² United Nations, Statement by the Chinese Delegation on Cyber Sovereignty, New York, 2019. «Every country has the right to regulate its cyberspace according to its national laws, traditions, and culture».

Buyuk devor nafaqat cheklash, balki muqobil milliy xizmatlarni rivojlantirishga ham turtki bo'ldi. Masalan, Baidu (Google o'rnida), WeChat (WhatsApp va Facebook o'rnida), Youku (YouTube o'rnida) kabi platformalar aynan shu sharoitda rivojlandi.

Xitoy kibermakon xavfsizligida milliy kompaniyalarning roli beqiyos. Huawei, Alibaba, Tencent, Baidu kabi gigantlar hukumat siyosatini qo'llab-quvvatlabgina qolmay, balki milliy xavfsizlik infratuzilmasiga integratsiyalashgan.

Masalan:

- Huawei – 5G tarmoqlarida global yetakchi, biroq AQSh va Yevropa uni “milliy xavfsizlik uchun xavf” deb hisoblab, cheklovlar joriy qilgan¹.
- Alibaba Cloud – Xitoyning milliy bulutli infratuzilmasini boshqaradi va hukumat bilan yaqin hamkorlik qiladi.
- Tencent – WeChat orqali nafaqat ijtimoiy muloqot, balki to'lov tizimlari va elektron hukumat xizmatlarini ham qamrab olgan.

Bu kompaniyalar hukumat nazoratida bo'lib, kibermakonni “suveren va mustaqil” saqlashga xizmat qilmoqda.

Xitoy amaliyotida sun'iy intellekt (AI) keng miqyosda qo'llanilmoqda. Eng ko'p tanqid qilinadigan yo'nalishlardan biri — bu ommaviy kuzatuv tizimlaridir. Xitoydagi “Skynet” loyihasi millionlab videokameralarni sun'iy intellekt asosida boshqarib, fuqarolarning harakatlarini kuzatish imkonini beradi. Rasmiy Pekin bu tizimni “jinoyatchilikka qarshi kurash va ijtimoiy tartibni ta'minlash” vositasi sifatida talqin qiladi.

Bundan tashqari, ijtimoiy reyting tizimi (Social Credit System) ham kibermakon nazoratining bir qismi sifatida shakllangan. Fuqarolarning onlayn faoliyati, to'lov intizomi va ijtimoiy xulqi reyting orqali baholanadi. Past reytingga ega shaxslar turli cheklovlarga duch keladi (masalan, kredit olish yoki sayohat qilish huquqi).

Xitoy amalda nafaqat ichki nazoratni kuchaytirgan, balki

¹ European Commission, EU Statement on Security Risks of 5G Networks, Brussels, 2020.

xalqaro miqyosda ham faol rol o'ynamoqda. Masalan, Xitoy Afrikada raqamli infratuzilma qurilishida (Huawei orqali) yetakchi o'rin egallab, o'z modelini eksport qilmoqda. Bu ko'plab tadqiqotchilar tomonidan "Digital Silk Road" (Raqamli Ipak yo'li) deb atalmoqda¹.

Xitoyning kibermakon siyosati konfutsiychilik qadriyatlari va davlat markazchiligiga asoslanadi. Si Szinpin ta'kidlaganidek: «Without cybersecurity, there is no national security»². Bu fikr kibermakonni milliy xavfsizlik va barqarorlikning asosi sifatida ko'rsatadi.

Falsafiy jihatdan Xitoy yondashuvi realizm paradigmasiga yaqin: kuch va suverenitet birinchi o'rinda turadi. Liberal va konstruktivist yondashuvlardan farqli ravishda, Xitoy modeli fuqarolik jamiyati va inson huquqlariga ikkinchi darajali ahamiyat beradi.

Huquqiy jihatdan Xitoy modeli "davlat markazli kiberhuquq"ka asoslanadi. Cybersecurity Law (2017), Data Security Law va Personal Information Protection Law (2021) internet ustidan markazlashgan nazoratni mustahkamladi. Shu bilan birga, bu qonunlar xalqaro hamjamiyat tomonidan inson huquqlari tamoyillariga zid deb baholanmoqda.

2.5. Janubiy Koreya va Yaponiya: texnologik taraqqiyot va kiberxavfsizlik integratsiyasi.

Janubiy Koreya kibermakon xavfsizligini milliy siyosat darajasiga olib chiqqan davlatlardan biridir. Bunga sabab – mamlakatning yuqori darajada raqamlashtirilgani va Shimoliy Koreyadan kelayotgan muntazam kiberxavflardir. Masalan, 2009-yildagi "7/7 DDoShujumi" Koreyaning hukumat saytlarini falaj qilgan edi. Hukumat hisobotida shunday deyiladi: «The

¹ Chinese Academy of Cyberspace Studies, White Paper on China's Digital Silk Road, Beijing, 2019.

² Xi Jinping, Address at the National Cybersecurity and Informatization Work Conference, Beijing, 2016.

July 7 cyber attacks revealed the vulnerability of the nation's critical information infrastructure»¹.

Shundan so'ng Seul kiberxavfsizlikni milliy mudofaa va iqtisodiy xavfsizlik bilan bevosita bog'lashga kirishdi.

2009-yilda Janubiy Koreya hukumat tomonidan KISA (Korea Internet & Security Agency) tashkil etildi. Uning asosiy vazifalari quyidagilar:

- Kiberxavfsizlik siyosatini ishlab chiqish va muvofiq-lashtirish;
- Kiberhujumlarni monitoring qilish va ularga javob berish;
- Internet sohasida standartlarni ishlab chiqish;
- Fuqarolarni xabardor qilish va kiberhujumlarga qarshi tayyorlash.

KISA rasmiy hisobotida shunday deyiladi: «KISA plays a central role in building a safe and trusted digital environment in Korea»².

Janubiy Koreya modelining asosiy ustunligi – bu hukumat va xususiy sektor o'rtasidagi yaqin hamkorlikdir. Chunki mamlakatdagi axborot infratuzilmasining katta qismi xususiy kompaniyalarga tegishli. Samsung, LG, SK Telecom kabi yirik kompaniyalar kiberxavfsizlik siyosatiga faol jalb etilgan.

Bundan tashqari, Janubiy Koreya NATO, AQSh va ASEAN davlatlari bilan kiberxavfsizlik bo'yicha hamkorlik dasturlarini amalga oshirmoqda. Bu xalqaro integratsiya Koreya modelining barqarorligini ta'minlaydi.

Seul kibermakon siyosatini ishlab chiqishda Shimoliy Koreya bilan bog'liq xavflarni ham hisobga oladi. Shimoliy Koreyaning Lazarus Group kabi xakerlik guruhlar Janubiy Koreya moliya sektori va hukumat idoralariga ko'plab hujumlar uyushtirgan. Bu hujumlar Janubiy Koreya uchun "kiber mudofaa" konseps-

¹ «The July 7 cyber attacks revealed the vulnerability of the nation's critical information infrastructure».

² Korea Internet & Security Agency (KISA), Annual Report, Seoul, 2018. «KISA plays a central role in building a safe and trusted digital environment in Korea».

siyasini ustuvor qilish zaruratini kuchaytirdi.

Yaponiya 2000-yillarning boshlaridan boshlab kibermakon xavfsizligini milliy siyosatning ajralmas qismi sifatida ko'ra boshladi. 2000-yilda qabul qilingan Basic Act on the Formation of an Advanced Information and Telecommunications Network Society (IT Basic Law) mamlakatda raqamli infratuzilma va axborot xavfsizligini tartibga soluvchi huquqiy asos bo'ldi. Unda shunday deyiladi: «The government shall take necessary measures to ensure the security and reliability of advanced information and telecommunications networks»¹.

Yaponiyada kibermakon xavfsizligini alohida tartibga soluvchi birinchi muhim hujjat — Cybersecurity Basic Act bo'lib, u 2014-yilda qabul qilingan. Ushbu qonun Yaponiyaning kibermakon xavfsizlik siyosatini belgilovchi asosiy hujjatdir. Unda: «Cybersecurity is essential for the realization of a safe and secure cyberspace and the sustainable development of the national economy»².

Bu qonun quyidagi tamoyillarni belgiladi:

1. Milliy kiberxavfsizlik siyosatini hukumat darajasida muvofiqlashtirish.
2. Davlat organlari va xususiy sektorning hamkorligini kuchaytirish.
3. Xalqaro hamkorlikni kengaytirish.
4. Kiberxavfsizlik bo'yicha ilmiy tadqiqotlarni rivojlantirish.

2015-yilda Yaponiya hukumati **NISC (National center of Incident readiness and Strategy for Cybersecurity)**ni tashkil etdi. Bu markaz hukumat darajasida kiberxavfsizlik siyosatini muvofiqlashtiruvchi va favqulodda holatlarda tezkor javob beruvchi institutdir. NISC hisobotida shunday deyiladi: «NISC

¹ Government of Japan, IT Basic Law, Tokyo, 2000. «The government shall take necessary measures to ensure the security and reliability of advanced information and telecommunications networks».

² Government of Japan, Cybersecurity Basic Act, Tokyo, 2014. «Cybersecurity is essential for the realization of a safe and secure cyberspace and the sustainable development of the national economy».

leads Japan's cybersecurity strategy, incident readiness, and international cooperation»¹.

Yaponiya muntazam ravishda milliy kiberxavfsizlik strategiyalarini yangilab boradi:

- 2013-yilgi Strategiya – milliy infratuzilmani himoya qilishga qaratilgan.
- 2018-yilgi Strategiya – Tokio Olimpiadasi oldidan kiberxavfsizlikni kuchaytirish choralari belgilagan.
- 2021-yilgi Strategiya – 5G, IoT va sun'iy intellekt xavfsizligiga alohida e'tibor qaratadi.

Yaponiya, shuningdek, AQSh, ASEAN va Yevropa Ittifoqi bilan kibermakon xavfsizligi bo'yicha yaqin hamkorlik o'rnatgan.

Koreya va Yaponiyaning kibermakon xavfsizligiga yondashuvi falsafiy jihatdan pragmatizm va innovatsion modernizm paradigmalari bilan bog'liq. Yaponiyaning "Society 5.0" konsepsiyasida keltirilganidek: «Cyberspace and physical space must be fully integrated to create a super-smart society»². Bu qarash kibermakonni inson taraqqiyotining yangi bosqichi sifatida ko'rsatadi. Koreya esa sun'iy intellekt va tezkor axborot tizimlarini milliy farovonlikning ajralmas qismi sifatida talqin qiladi.

Har ikkala davlatda huquqiy bazalar texnologik taraqqiyotga mos ravishda muntazam yangilanib boriladi. Masalan, Yaponiyada 2014-yildagi Cybersecurity Basic Act, Koreyada esa KISA tomonidan ishlab chiqilgan huquqiy mexanizmlar mavjud. Bu ularning kiberxavfsizlik siyosatini qonuniy asosda barqaror olib borishini ta'minlaydi.

Koreya va Yaponiya kibermakon xavfsizligida innovation, pragmatik va xalqaro hamkorlikka asoslangan modelni shakllantirgan. Ularning kuchli tomonlari – ilg'or texnolo-

¹ NISC (National center of Incident readiness and Strategy for Cybersecurity), Annual Report, Tokyo, 2019. «NISC leads Japan's cybersecurity strategy, incident readiness, and international cooperation».

² Government of Japan, Society 5.0: A People-centric Super-smart Society, Tokyo, 2016. «Cyberspace and physical space must be fully integrated to create a super-smart society».

giyalar va global integratsiya, zaif tomonlari esa tashqi tahdidlarga qaramlikdir. O'zbekiston uchun eng asosiy saboq shuki, kibermakon xavfsizligi nafaqat mudofaa yoki nazorat, balki taraqqiyot, hamkorlik va ishonch tamoyillari bilan uyg'unlashganda samarali bo'ladi.

II BOB BO'YICHA XULOSA

Kibermakon xavfsizligini ta'minlash masalasi har bir mamlakatda o'ziga xos sharoit, siyosiy tuzum va huquqiy an'analarga asoslanib shakllanadi. 2-bob davomida tahlil qilingan davlatlar tajribasi shuni ko'rsatadiki, kiberxavfsizlik endi faqat texnik muammo emas, balki falsafiy-huquqiy, siyosiy va ijtimoiy masalalar majmuasidir.

AQSh modeli kibermakonni geosiyosiy kuch maydoni sifatida talqin qiladi. Bu yerda texnologik innovatsiyalar, davlat-xususiy sektor hamkorligi va xalqaro diplomatiya birlashgan. AQShning Milliy kiberxavfsizlik strategiyalari (2003, 2015, 2018, 2023) davlat siyosatini izchil shakllantirgan bo'lsa-da, maxfiylik va inson huquqlari bo'yicha jiddiy bahslarni yuzaga keltirgan.

Yevropa Ittifoqi tajribasi butunlay boshqacha. Bu modelning asosiy tamoyili — inson huquqlariga ustuvorlik, shaxsiy ma'lumotlarni himoya qilish va demokratik qadriyatlar. GDPR (2016) global standart sifatida qabul qilingan va boshqa mamlakatlarga ham ta'sir ko'rsatgan. Shu bilan birga, byurokratik jarayonlarning murakkabligi va texnologik qaramlik uning zaif tomonidir.

Rossiya esa kibermakon xavfsizligini davlat nazorati va milliy suverenitet bilan uyg'unlashtiradi. Yarovaya paketi (2016), Suveren internet qonuni (2019) va Axborot xavfsizligi doktrinalari (2000, 2016) orqali Rossiya o'z milliy segmentini (RuNet) yaratishga intildi. Kuchli tomoni — markazlashgan boshqaruv va mafkuraviy barqarorlikni ta'minlashga intilish; zaif tomoni esa inson huquqlarini cheklash va xalqaro izolyatsiya xavfidir.

Xitoy modeli “kibersuverenitet” konsepsiyasi asosida shakllangan. Buyuk Xitoy devori, milliy IT-gigantlar (Huawei, Tencent, Alibaba) va sun’iy intellekt asosidagi kuzatuv tizimlari orqali davlat internet ustidan to’liq nazoratni amalga oshiradi. Kuchli tomoni — texnologik mustaqillik va global tashabbuslar (Digital Silk Road); zaif tomoni — inson huquqlari va erkinliklarining cheklanishi.

Koreya va Yaponiya tajribasi innovatsion va pragmatik yondashuvni ifodalaydi. Koreya Respublikasi KISA orqali davlat va xususiy sektor hamkorligini kuchaytirib, Shimoliy Koreyadan kelayotgan tahdidlarga qarshi samarali tizim yaratgan. Yaponiya esa Cybersecurity Basic Act (2014) va NISC faoliyati orqali milliy strategiyani muntazam yangilab boradi. Kuchli tomoni — innovatsiyalarni milliy strategiyaga kiritish va xalqaro hamkorlik; zaif tomoni esa tashqi xavflarga yuqori darajada bog’liq bo’lish.

Davlatlarning kibermakon xavfsizligiga bo’lgan yondashuvlarini falsafiy jihatdan quyidagicha tasniflash mumkin:

1. *Realizm paradigmasi* — Rossiya va Xitoy tajribasida yaqqol namoyon bo’ladi. Bu yondashuv kibermakonni geosiyosiy jang maydoni va suverenitetning yangi hududi sifatida talqin qiladi.

2. *Liberal paradigmasi* — Yevropa Ittifoqi modeliga mos keladi. Bu yerda inson huquqlari, axborot erkinligi va xalqaro hamkorlik ustuvorlik qiladi.

3. *Pragmatizm va innovatsion modernizm* — AQSh, Koreya va Yaponiya tajribasida yaqqol ko’rinadi. Ular kibermakon xavfsizligini milliy taraqqiyot va iqtisodiy raqobatbardoshlikning ajralmas qismi sifatida ko’rmoqda.

Huquqiy jihatdan esa davlatlar uch xil modelni shakllantirgan:

- *Davlat markazli model* (Rossiya, Xitoy) — internetni to’liq nazorat qilish va milliy segment yaratish.
- *Huquqiy-demokratik model* (Yevropa Ittifoqi, Germaniya) — fuqarolik huquqlarini markazga qo’yish.
- *Aralash model* (AQSh, Koreya, Yaponiya) — xavfsizlik va

erkinlikni muvozanatlash, davlat–xususiy sektor hamkorligi.

Davlatlarning kiberxavfsizlik tizimini tahlil qilgan qolda kuchli va zaif jihatlarini quyidagicha belgilaymiz:

- *AQSh* — kuchli: innovatsiya va global liderlik; zaif: fuqarolik huquqlarining ikkinchi planga surilishi.
- *Yevropa Ittifoqi* — kuchli: inson huquqlariga ustuvorlik; zaif: texnologik qaramlik.
- *Rossiya* — kuchli: suverenitet va mafkuraviy barqarorlik; zaif: izolyatsiya xavfi.
- *Xitoy* — kuchli: texnologik mustaqillik; zaif: inson huquqlarining keskin cheklanishi.
- *Koreya va Yaponiya* — kuchli: innovatsion texnologiyalar va xalqaro hamkorlik; zaif: tashqi xavflarga qaramlik.

2-bob tahlillaridan kelib chiqib, O'zbekiston uchun quyidagi saboqlarni ajratib ko'rsatish mumkin:

1. *Milliy suverenitetni mustahkamlash* — Rossiya va Xitoy tajribasidan kelib chiqib, milliy internet infratuzilmasini rivojlantirish zarur.

2. *Inson huquqlarini himoya qilish* — Yevropa Ittifoqi tajribasidan foydalanib, shaxsiy ma'lumotlarni himoya qilish bo'yicha mustahkam huquqiy asos yaratish.

3. *Innovatsion texnologiyalarni integratsiya qilish* — Koreya va Yaponiyaning AI, IoT, 5G xavfsizligi bo'yicha tajribasidan foydalanish.

4. *Xalqaro hamkorlikni kuchaytirish* — AQSh, Yevropa va Osiyo davlatlari bilan kibermakon xavfsizligi bo'yicha qo'shma dasturlarni yo'lga qo'yish.

5. *Balansni saqlash* — milliy xavfsizlik va inson huquqlari o'rtasida muvozanatni topish, nazorat va erkinlikni uyg'unlashtirish.

Xulosa qilib aytganda, dunyo davlatlari kibermakon xavfsizligini ta'minlashda turli strategiyalarni qo'llamoqda. Kimdir nazorat va suverenitetga urg'u beradi (Rossiya, Xitoy), kimdir inson huquqlarini markazga qo'yadi (Yevropa Ittifoqi), yana boshqalar innovatsion texnologiyalar va pragmatik hamkorlik orqali xavfsizlikni ta'minlaydi (AQSh, Koreya, Yaponiya).

Bu xilma-xillik kibermakonning o'ziga xos tabiatidan dalolat beradi: u nafaqat texnik, balki ijtimoiy-falsafiy, huquqiy va siyosiy makondir. O'zbekiston uchun esa eng to'g'ri yo'l — turli modellarning eng samarali jihatlarini uyg'unlashtirib, milliy an'analar va xalqaro standartlarga mos kiberxavfsizlik siyosatini shakllantirishdir.

III-BOB. MINTAQAVIY TAJRIBA VA O'ZBEKISTON

Kibermakonning globallashuvi zamonaviy jamiyat taraqqiyotining eng muhim xususiyatlaridan biridir. Bugungi kunda axborot-kommunikatsiya texnologiyalari nafaqat alohida inson hayotiga, balki butun davlatlararo munosabatlarga, milliy xavfsizlik strategiyalariga, iqtisodiy va ijtimoiy barqarorlikka ham bevosita ta'sir ko'rsatmoqda. Shu nuqtai nazardan, kibermakon xavfsizligini ta'minlash masalasi mintaqaviy va milliy darajada dolzarb bo'lib qolmoqda. Chunki axborot oqimlari chegaralarni bilmaydi, kiberjinoiyatlar transc chegaraviy xususiyatga ega va ularning oqibatlari ko'pincha davlat hududiy suverenitetini ham chetlab o'tadi.

Markaziy Osiyo davlatlari, jumladan O'zbekiston ham bu jarayondan mustasno emas. So'nggi yillarda mintaqada raqamli transformatsiya siyosati jadal amalga oshirilmoqda. Elektron hukumat tizimlari, elektron tijorat, onlayn ta'lim, moliya va bank xizmatlari keng joriy qilinmoqda. Shu bilan birga, mazkur sohalar kiberjinoiyatchilar uchun yangi imkoniyatlarni ham yuzaga keltirmoqda. Natijada, davlatlar oldida ikki tomonlama vazifa paydo bo'lmoqda: bir tomondan, raqamli taraqqiyotni jadallashtirish, ikkinchi tomondan esa, uni barqaror va xavfsiz qilish.

Ayniqsa, Markaziy Osiyo mamlakatlarida kiberxavfsizlik masalalari o'ziga xos qiyinchiliklarga duch kelmoqda. Buning sabablari bir nechta: texnologik infratuzilmaning turlicha rivojlanish darajasi, kiberxavfsizlik bo'yicha malakali kadrlar yetishmovchiligi, huquqiy bazaning to'liq shakllanmaganligi, xalqaro tajribadan foydalanish imkoniyatlarining cheklanganligi. Shu bilan birga, mintaqada davlatlari umumiy tarixiy, madaniy va siyosiy kontekstga ega bo'lgani uchun, ularning kibermakon xavfsizligi borasidagi yondashuvlari ko'plab o'xshash jihatlarga ega.

O'zbekiston Respublikasi uchun esa kibermakon xavfsizligi masalasi strategik milliy manfaatlardan biri sifatida qaralmoqda. So'nggi yillarda qabul qilingan bir qator muhim

hujjatlar — “Raqamli O‘zbekiston – 2030” davlat dasturi (2020), “Axborot xavfsizligi to‘g‘risida”gi Qonun (2022), “Sun’iy intellektni rivojlantirish strategiyasi” (2024) mamlakatning bu sohadagi siyosatini huquqiy va institutsional asos bilan mustahkamladi. Bu hujjatlarda kiberxavfsizlik masalasi faqat texnik yoki huquqiy emas, balki keng ijtimoiy va falsafiy muammo sifatida ham talqin qilinmoqda.

Ushbu bobning metodologik asosi — qiyosiy tahlil va falsafiy-huquqiy umumlashtirishdir. Qiyosiy tahlil orqali O‘zbekistonning tajribasi mintaqadagi boshqa davlatlar bilan solishtiriladi, falsafiy-huquqiy umumlashtirish orqali esa kiberxavfsizlik masalalarining chuqur mohiyati ochib beriladi. Shu yo‘sinda, bob nafaqat amaliy, balki nazariy jihatdan ham ilmiy ahamiyatga ega bo‘ladi.

Shuningdek, ushbu bobda kibermakon xavfsizligi masalalariga ijtimoiy-falsafiy yondashuv ham beriladi. Chunki texnik vositalar va huquqiy me‘yorlar qanchalik mukammal bo‘lmasin, ular jamiyat ongida shakllangan kiberxavfsizlik madaniyatisiz samarali ishlamaydi. Demak, kiberxavfsizlik masalasi ijtimoiy ong, ta’lim, ilmiy tadqiqot va milliy qadriyatlar bilan chambarchas bog‘liqdir.

3.1. Markaziy Osiyo davlatlarida kibermakon xavfsizligi: umumiy muammolar va imkoniyatlar

Markaziy Osiyo davlatlari mustaqillikka erishgach, ular uchun raqamli texnologiyalarni joriy etish va internet infratuzilmasini rivojlantirish masalasi strategik ahamiyat kasb eta boshladi. Dastlabki yillarda davlatlar asosan iqtisodiy islohotlar, siyosiy barqarorlik va huquqiy tizimni shakllantirish bilan band bo‘lgani bois, axborot texnologiyalariga ikkinchi darajali vazifa sifatida qaraldi. Ammo 2000-yillardan boshlab internetning keng tarqalishi, mobil aloqa xizmatlarining rivojlanishi va global tarmoqlarga integratsiya ehtiyoji kiberxavfsizlikni ham yangi milliy xavfsizlik yo‘nalishi sifatida shakllantira boshladi.

Xalqaro Telekommunikatsiya Ittifoqi (ITU) ma'lumotlariga ko'ra, Markaziy Osiyo davlatlarida internet foydalanuvchilar soni 2000-yilda jami aholining 1 foizidan ham kam bo'lgan bo'lsa, 2020-yilga kelib bu ko'rsatkich Qozog'istonda 80 foizdan oshdi, Qirg'iziston va O'zbekistonda 60 foizga yetdi, Tojikiston va Turkmanistonda esa 30–40 foiz atrofida bo'ldi. «Digital transformation in Central Asia is progressing unevenly, with Kazakhstan leading, while other countries face infrastructural and political challenges»¹. Bu notekislik kibermakon xavfsizligini ta'minlash infratuzilmasi ham turlicha shakllanishiga olib keldi.

Kibermakon xavfsizligining infratuzilmasi deganda, nafaqat texnik tizimlar (serverlar, ma'lumot markazlari, dasturiy ta'minot), balki huquqiy baza, institutsional mexanizmlar va mutaxassislar tayyorlash tizimi ham nazarda tutiladi. Shu nuqtai nazardan qaraganda, Qozog'iston mintaqada yetakchi bo'lib, milliy darajada keng qamrovli dasturlar ishlab chiqdi. Qirg'iziston va Tojikiston asta-sekin huquqiy asoslarni yaratdi, Turkmaniston esa yopiq modelni tanladi.

Shu sababli, Markaziy Osiyo davlatlarining kibermakon xavfsizligi infratuzilmasini o'rganish nafaqat texnik, balki falsafiy-huquqiy yondashuvni ham talab qiladi. Chunki bu masalada erkinlik va nazorat, suverenitet va integratsiya, xavfsizlik va inson huquqlari o'rtasidagi dialektika yaqqol namoyon bo'ladi.

Qozog'iston tajribasi

Qozog'iston Markaziy Osiyoda kiberxavfsizlik infratuzilmasini eng tizimli shaklda yo'lga qo'yan davlat hisoblanadi. 2017-yilda hukumat “Kibershield of Kazakhstan” konsepsiyasini qabul qildi. Unda shunday deyilgan: «Cybersecurity is the cornerstone of Kazakhstan's digital transformation and a prerequisite for the country's

¹ International Telecommunication Union (ITU). Measuring the Information Society Report 2020. Geneva: ITU Publications, 2020. – P. 145–152. URL: <https://www.itu.int/en/ITU-D/Statistics/Pages/publications/mis2020.aspx>

technological sovereignty»¹. Ushbu konsepsiya asosida milliy darajada huquqiy va texnik infratuzilma yaratildi.

Birinchidan, Qozog'istonda milliy CERT-KZ (*Computer Emergency Response Team*) tashkil etildi. Bu markaz kiberhujumlarni aniqlash, ularni oldini olish va davlat organlari hamda xususiy sektorga maslahat berish bilan shug'ullanadi. CERT-KZ hisobotida qayd etilishicha: «In 2020, more than 20,000 cyber incidents were detected, including phishing, malware, and DDoS attacks»². Bu raqamlar kibermakon tahdidlarining real miqyosini ko'rsatadi.

Ikkinchidan, Qozog'iston kiberxavfsizlikni davlat-xususiy sektor hamkorligida rivojlantirishga e'tibor qaratdi. Masalan, "Kazakhtelecom", "Beeline Kazakhstan" kabi yirik kompaniyalar hukumat bilan birgalikda tarmoqlarni himoya qilish bo'yicha qo'shma loyihalar amalga oshirmoqda. Shu asosda hukumat "National Information Security Technical Service"ni ham yo'lga qo'ygan.

Uchinchidan, Qozog'iston xalqaro hamkorlikda ham faol. 2018-yilda bu davlat *ITU Global Cybersecurity Index* reytingida 40-o'rinni egalladi, mintaqada esa birinchi o'rinda bo'ldi. Hisobotda ta'kidlanishicha: «Kazakhstan has demonstrated strong commitment to cybersecurity through comprehensive policy frameworks and regional leadership»³.

To'rtinchidan, Qozog'istonda ta'lim va ilmiy tadqiqot yo'nalishida ham kiberxavfsizlik bo'yicha alohida dasturlar ishlab chiqilgan. Masalan, Nazarboyev universiteti va boshqa oliy o'quv yurtlarida kiberxavfsizlik magistratura va doktorantura dasturlari joriy etildi. Bu mutaxassislar milliy infratuzilmani yanada kuchaytirishga xizmat qilmoqda.

Qozog'iston tajribasida kibermakon xavfsizligi infratuzil-

¹ Government of Kazakhstan. Cybersecurity Concept "Cyber Shield of Kazakhstan". Astana: Government Press, 2017. – P. 3–15.

² CERT-KZ. Annual Cybersecurity Report 2020. Astana: National Information Security Technical Service, 2020. – P. 27–39.

³ International Telecommunication Union (ITU). Global Cybersecurity Index 2018. Geneva: ITU Publications, 2018. – P. 51–56. URL: <https://www.itu.int/en/ITU-D/Cybersecurity/Pages/GCI-2018.aspx>

masi davlat suvereniteti va innovatsion rivojlanish o'rtasidagi muvozanatga asoslangan. Davlat nazorati kuchli bo'lsa-da, inson huquqlari va xalqaro integratsiya ham e'tibordan chetda qolmaydi. Shu bois, bu modelni "aralash model" deb atash mumkin: unda ham realistik, ham liberal elementlar mavjud.

Qirg'iziston tajribasi

Qirg'iziston kibermakon xavfsizligini davlat siyosatining ustuvor yo'nalishlari qatoriga kechroq kiritgan davlatlardan biridir. 2019-yilda qabul qilingan *"Axborot xavfsizligi konsepsiyasi"* mamlakatda ushbu sohada birinchi muhim hujjat bo'ldi. Unda shunday deyilgan: «Кибербезопасность является неотъемлемой частью национальной безопасности Кыргызской Республики»¹. Bu hujjatning qabul qilinishi Qirg'iziston uchun muhim bosqich bo'ldi, chunki u kibermakonni milliy xavfsizlik konsepsiyasi doirasida tan oldi.

Birinchidan, Qirg'izistonning infratuzilmasi Qozog'istonga qaraganda ancha zaif. ITU ma'lumotlariga ko'ra, «Kyrgyzstan faces significant challenges in developing a robust cybersecurity infrastructure due to limited financial and technical resources»². Bu holat davlatning internet infratuzilmasi tez rivojlanayotganiga qaramay, uni himoya qilish vositalari yetarli emasligini ko'rsatadi.

Ikkinchidan, Qirg'izistonning bank tizimi va davlat portallari ko'plab kiberhujumlarga uchramoqda. 2021-yilda Bishkekda bir nechta banklarning xizmatlari vaqtincha ishdan chiqqan. Mahalliy nashr shunday yozgan: «Cyberattack temporarily paralyzed several Kyrgyz banks' services, exposing the vulnerability of financial infrastructure»³. Bu voqea Qirg'iziston infratuzilmasining zaif tomonlarini fosh etdi.

Uchinchidan, Qirg'iziston xalqaro hamkorlik orqali o'z

¹ Government of Kyrgyz Republic. Information Security Concept. Bishkek: Government Press, 2019. – P. 4–12.

² International Telecommunication Union (ITU). Cybersecurity Country Profile: Kyrgyzstan. Geneva: ITU, 2020. – P. 10–16.

³ 24.kg News Agency. Cyberattack on Kyrgyz Banks. Bishkek: 24.kg, 2021. – URL: <https://24.kg/english/>

infratuzilmasini kuchaytirishga intilmoqda. Xususan, BMT va Yevropa Ittifoqi bilan hamkorlikda kiberjinoyatchilikka qarshi kurash bo'yicha bir nechta loyihalar amalga oshirilgan. 2020-yilda Yevropa Ittifoqi hisobotida qayd etilishicha: «Kyrgyzstan has taken first steps to align its legislation with the Budapest Convention on Cybercrime»¹. Bu jarayon hali yakuniga yetmagan bo'lsa-da, xalqaro me'yorlarga moslashish yo'lida muhim qadamdir.

To'rtinchidan, Qirg'izistonda kibermakon xavfsizligi bo'yicha mutaxassislar yetishmovchiligi muammosi dolzarb. Mamlakatdagi ko'plab universitetlarda IT sohasi bo'yicha kadrlar tayyorlanadi, ammo kiberxavfsizlik mutaxassisligi alohida yo'nalish sifatida rivojlanmagan. Shu bois, davlat ko'proq xalqaro grantlar va treninglarga tayanishga majbur.

Qirg'iziston tajribasi "zaif infratuzilma – kuchli tashqi hamkorlik" modeliga misol bo'la oladi. Davlatning ichki imkoniyatlari cheklangan bo'lsa-da, xalqaro hamjamiyat bilan integratsiya unga yangi imkoniyatlar yaratmoqda. Shu bilan birga, bu holat Qirg'izistonning suverenitet masalalarini ham o'rta qo'yadi: kibermakon xavfsizligini haddan tashqari tashqi resurslarga bog'lash uning mustaqil siyosatini cheklab qo'yishi mumkin.

Tojikiston tajribasi

Tojikiston kibermakon xavfsizligi masalasini asosan *milliy xavfsizlik va terrorizmga qarshi kurash* kontekstida ko'rib kelmoqda. 2018-yilda qabul qilingan "Axborot xavfsizligi konsepsiyasi"da shunday deyilgan: «Интернет-пространство становится площадкой для распространения экстремистских идей, что представляет угрозу национальной и общественной безопасности»². Ushbu hujjat kibermakonni nafaqat texnologik rivojlanish maydoni, balki mafkuraviy xavflarning ham manbai sifatida talqin qiladi.

¹ European Union External Action Service. EU Support to Kyrgyzstan in Cybersecurity Reform. Brussels: EU Publications, 2020. – P. 6–18.

² Government of Tajikistan. Concept of Information Security. Dushanbe: Government Press, 2018. – P. 5–11.

*Birinchi*dan, Tojikiston infratuzilmasi iqtisodiy imkoniyatlar va texnik resurslar yetishmovchiligi sababli sust rivojlangan. ITU hisobotida qayd etilishicha: «Tajikistan has one of the lowest ICT penetration rates in the region, making cybersecurity both less urgent and more difficult to implement effectively»¹. Ya'ni, internet foydalanuvchilari sonining nisbatan kamligi kiberxavfsizlik muammosini biroz orqaga suradi, biroq ayni paytda zaif infratuzilma tashqi tahdidlarga ochiq bo'lib qoladi.

*Ikkinchi*dan, Tojikiston hukumati kibermakonni asosan diniy ekstremizmga qarshi kurash doirasida nazorat qiladi. Masalan, 2019-yilda Milliy xavfsizlik qo'mitasi internet orqali tarqatilgan ekstremistik materiallar uchun bir nechta shaxsni javobgarlikka tortganini ma'lum qilgan: «Over 300 extremist materials were removed from social media platforms in 2019 as part of the government's counter-terrorism policy»². Bu amaliyot kiberxavfsizlikni ko'proq mafkuraviy nazorat vositasi sifatida qo'llanayotganini ko'rsatadi.

*Uchinchi*dan, xalqaro hamkorlik sohasida Tojikiston MDH va SHHT doirasida faol ishtirok etmoqda. Ayniqsa, SHHT doirasidagi kelishuvlarda “axborot terrorizmi” tushunchasini qo'llash Tojikiston uchun ham muhim huquqiy asos bo'lib xizmat qilmoqda³. Biroq, Yevropa Ittifoqi yoki BMT bilan hamkorlik Qozog'iston va Qirg'izistonga qaraganda sustroq.

*To'rtinchi*dan, Tojikistonda mutaxassislar yetishmovchiligi muammosi dolzarb. Universitetlarda IT mutaxassisliklari mavjud bo'lsa-da, kiberxavfsizlik bo'yicha maxsus fakultet yoki ilmiy markazlar deyarli shakllanmagan. Shu sababli, kadrlar tayyorlashda ko'proq Rossiya yoki Xitoydagi ta'lim dasturlariga tayaniladi.

Tojikiston tajribasi “xavfsizlikni mafkuraviy nazorat bilan

¹ International Telecommunication Union (ITU). Cybersecurity Country Profile: Tajikistan. Geneva: ITU, 2020. – P. 12–17.

² State Committee for National Security of Tajikistan. Annual Report on Countering Extremism in Cyberspace. Dushanbe: SCNS, 2019. – P. 9–14.

³ Government of Tajikistan. Concept of Information Security. Dushanbe: Government Press, 2018. – P. 5–11.

ta'minlash" modelini ifodalaydi. Davlat kiberxavfsizlikni erkinlik va innovatsiya bilan emas, balki xavfsizlik va barqarorlik bilan bog'liq tarzda talqin qiladi. Bu model falsafiy jihatdan realizm paradigmasiga yaqin bo'lib, suverenitet va xavfsizlikni inson huquqlaridan ustun qo'yadi. Shu bois, Tojikiston tajribasi texnologik rivojlanishdan ko'ra ko'proq siyosiy barqarorlikni saqlashga qaratilgan.

Turkmaniston tajribasi

Turkmaniston Markaziy Osiyoda kibermakon xavfsizligini ta'minlashda o'ziga xos, ammo ancha yopiq modelni shakllantirgan davlatdir. Xalqaro tashkilotlarning ta'kidlashicha, «Turkmenistan has one of the world's most restrictive environments for internet freedom, with pervasive censorship and surveillance»¹. Bu shuni anglatadiki, davlat internet infratuzilmasini nafaqat rivojlantirish, balki uni qat'iy nazorat ostida saqlash orqali xavfsizlikni ta'minlashni afzal ko'rmoqda.

Birinchidan, Turkmanistonning internet infratuzilmasi davlat monopoliyasi ostida. "Turkmentelecom" milliy operatori barcha internet xizmatlarini nazorat qiladi. Shu sababli, internet tezligi va xizmat sifati past bo'lib qolmoqda. 2021-yilgi "Freedom on the Net" hisobotida shunday qayd etiladi: «Internet access remains slow and expensive, while many global websites and social media platforms are blocked»². Bu holat mamlakat infratuzilmasining rivojlanishini keskin cheklamoqda.

Ikkinchidan, Turkmaniston hukumati kibermakon xavfsizligini asosan "milliy axborot makonini yopiq shaklda saqlash" orqali ta'minlaydi. Masalan, ko'plab xalqaro ijtimoiy tarmoqlar (Facebook, Twitter, YouTube) mamlakatda ochilmaydi. Bu amaliyot bir tomondan milliy suverenitetni mustahkamlashga xizmat qilsa, ikkinchi tomondan xalqaro integratsiyani

¹ Freedom House. Freedom on the Net: Turkmenistan Report. Washington: Freedom House, 2021. – P. 3–8. URL: <https://freedomhouse.org/country/turkmenistan/freedom-net>

² Reporters Without Borders. Internet Censorship in Turkmenistan. Paris: RSF Publications, 2021. – P. 2–7.

murakkablashtiradi.

Uchinchidan, Turkmaniston o'zining milliy axborot platformalarini rivojlantirishga urinmoqda. Masalan, "Altyn Asyr" mobil aloqa operatori milliy messenger va elektron pochta xizmatlarini joriy qilgan. Ammo ekspertlarning fikricha, «these local platforms cannot replace global services in terms of functionality and trust»¹. Ya'ni, milliy alternativalarining xalqaro darajada samaradorligi past.

To'rtinchidan, xalqaro hamkorlik jihatidan Turkmaniston deyarli izolyatsion yondashuvni tanlagan. BMT yoki ITU doirasida formal ishtiroki mavjud bo'lsa-da, amalda bu davlat kiberxavfsizlik bo'yicha qo'shma dasturlarda faol emas. Bu esa mamlakatni xalqaro tajriba va texnologiyalardan uzoqlashtiradi.

Turkmaniston tajribasini "izolyatsion model" deb atash mumkin. Bu modelda kibermakon xavfsizligi mutlaq nazorat va yopiq infratuzilma orqali ta'minlanadi. Falsafiy jihatdan bu yondashuv suverenitetni inson huquqlaridan ustun qo'yadi, huquqiy jihatdan esa xalqaro normalar bilan keskin ziddiyatga kirishadi. Shu bois, Turkmaniston tajribasi xavfsizlikni kuchaytirgan holda, innovatsiya va erkinlikni qurbon qilayotgan model sifatida baholanishi mumkin.

Yuqoridagi tahlillardan kelib chiqib quyidagi xulosalarga kelamiz: Markaziy Osiyo davlatlarida kibermakon xavfsizligi infratuzilmasi turlicha shakllangan bo'lsa-da, ularning rivojlanişida umumiy jihatlar ham, keskin tafovutlar ham mavjud.

Qozog'iston eng rivojlangan modelni shakllantirgan. "Kiber-shield" konsepsiyasi, CERT-KZ faoliyati va xalqaro reytinglardagi yuqori o'zni Qozog'istonning mintaqaviy yetakchi ekanini ko'rsatadi. Bu davlatning tajribasi davlat-xususiy sektor hamkorligiga asoslanadi va xalqaro hamkorlik bilan uyg'unlashadi.

1 Human Rights Watch. *Turkmenistan: Tightening Control over Cyberspace*. New York: HRW, 2020. – P. 4–9.

Qirg'izistonning zaif infratuzilmasi uni xalqaro hamkorlikka ko'proq bog'laydi. Bank tizimlariga qilingan hujumlar va 2019-yildagi "Axborot xavfsizligi konsepsiyasi" qabul qilinishi bu yo'nalishdagi birinchi qadamlar bo'ldi. Shunga qaramay, mutaxassislar yetishmovchiligi Qirg'izistonning eng katta muammosi bo'lib qolmoqda.

Tojikiston kibermakon xavfsizligini asosan terrorizm va ekstremizmga qarshi kurash bilan bog'lab, mafkuraviy nazoratga urg'u beradi. 2018-yilda qabul qilingan konsepsiya bu yondashuvni mustahkamladi. Natijada, texnologik rivojlanishdan ko'ra siyosiy barqarorlikni saqlashga ko'proq e'tibor qaratilmoqda.

Turkmaniston esa izolyatsion modelni tanlab, internet ustidan to'liq nazorat o'rnatdi. Davlat monopoliyasi, xalqaro platformalarning bloklanishi va milliy alternativalarining samarador emasligi bu mamlakatni global raqamli tizimlardan ajratib qo'ymoqda.

Umumiy muammolar

1. Texnologik imkoniyatlarning cheklanganligi. Qozog'iston bundan qisman xoli bo'lsa-da, qolgan davlatlarda zaif infratuzilma katta xavf tug'diradi.

2. Mutaxassislar yetishmovchiligi. Qirg'iziston va Tojikistonda bu muammo dolzarb, Turkmanistonda esa yopiq siyosat kadrlar rivojlanishini ham to'sib qo'yadi.

3. Xalqaro hamkorlikdagi tafovut. Qozog'iston va Qirg'iziston faol, Tojikiston qisman, Turkmaniston esa passiv ishtirok etmoqda.

4. Inson huquqlari muammosi. Turkmaniston va Tojikiston modelida erkinliklar cheklangan, Qozog'iston va Qirg'izistonda esa nisbatan liberal yondashuv mavjud.

Imkoniyatlar

1. Qozog'istonning ilg'or tajribasi mintaqa uchun namunaviy model bo'lishi mumkin.

2. Qirg'izistonning xalqaro integratsiyasi boshqa davlatlarga ham global standartlarga yaqinlashish imkonini beradi.

3. Tojikistonning mafkuraviy barqarorlik tajribasi terro-

rizmga qarshi kurashda muhim ahamiyat kasb etadi.

4. Turkmanistonning milliy suverenitetni ustuvor qo'yishi mintaqada mustaqillikni ta'minlash bo'yicha saboq bo'lishi mumkin, biroq u muvozanatni talab qiladi.

Kibermakon xavfsizligi Markaziy Osiyo davlatlari uchun "erkinlik va nazorat" dialektikasida shakllanmoqda.

- Qozog'iston modeli – muvozanatli va pragmatik: xavfsizlik va integratsiya uyg'unlashgan.

- Qirg'iziston modeli – tashqi hamkorlikka bog'liq, suverenitet masalalarini murakkablashtiradi.

- Tojikiston modeli – realizm paradigmasi asosida xavfsizlikni huquqlardan ustun qo'yadi.

- Turkmaniston modeli – izolyatsion va qat'iy nazoratga asoslangan.

Huquqiy jihatdan bu tajribalar uch turdagi yondashuvni ifodalaydi:

1. Aralash model (Qozog'iston) – xavfsizlik va huquqlar muvozanati.

2. Zaif-hamkorlik modeli (Qirg'iziston) – xalqaro yordamga tayanish.

3. Nazorat modeli (Tojikiston va Turkmaniston) – barqarorlikni huquqlardan ustun qo'yish.

Markaziy Osiyo davlatlarida kibermakon xavfsizligi infratuzilmasi notekis rivojlangan bo'lsa-da, umumiy tendensiya – milliy xavfsizlikni ustuvor qo'yishdir. Qozog'istonning tajribasi mintaqa uchun ilg'or yo'lni ko'rsatsa, Qirg'iziston xalqaro hamkorlik orqali o'z zaifliklarini yengishga intilmoqda. Tojikiston va Turkmaniston esa xavfsizlikni mafkuraviy va izolyatsion nazorat orqali ta'minlashni tanlagan.

Falsafiy-huquqiy nuqtai nazardan, bu jarayon milliy suverenitet va global integratsiya, xavfsizlik va inson huquqlari, erkinlik va nazorat o'rtasidagi muvozanatni topishga qaratilgan murakkab jarayondir.

3.2. O'zbekiston Respublikasida kibermakon xavfsizligini ta'minlashning huquqiy asoslari

O'zbekiston Respublikasida kibermakon xavfsizligini ta'minlash masalasi huquqiy jihatdan eng avvalo Konstitutsiyaga asoslanadi. Konstitutsiya mamlakatdagi barcha huquqiy me'yorlarning asosi bo'lib, unda inson huquqlari, shaxsiy erkinliklar, axborot olish va tarqatish huquqi, shuningdek, davlatning milliy xavfsizlikni ta'minlash majburiyatlari belgilab qo'yilgan. Shundan kelib chiqib, kibermakon xavfsizligi masalalari ham Konstitutsiyada mustahkamlangan prinsiplar asosida rivojlantirilmoqda.

O'zbekiston Respublikasining yangi tahrirdagi Konstitutsiyasida axborot xavfsizligi bilan bog'liq bir qator muhim normalar mavjud. Masalan, 29-moddada shunday deyilgan: «Har kim fikrlash, so'z va e'tiqod erkinligiga ega. Har kim axborotni izlash, olish, uzatish va tarqatish huquqiga ega».

Shuningdek, 30-moddada quyidagicha norma mavjud: «Davlat organlari, jamoat birlashmalari va mansabdor shaxslar fuqarolarga axborot berishi shart. Axborotning yashirilishi qonunda nazarda tutilgan hollardagina ruxsat etiladi»¹.

Biroq Konstitutsiyada axborot erkinligi bilan bir qatorda, milliy xavfsizlikni ta'minlashga doir majburiyatlar ham belgilangan. 55-moddada davlatning vazifalaridan biri sifatida «milliy xavfsizlik va jamoat tartibini ta'minlash» ko'rsatilgan. Shu bois, kibermakon xavfsizligi masalasi Konstitutsiyada inson huquqlari va davlat suverenitetini ta'minlash o'rtasidagi muvozanat nuqtai nazaridan talqin qilinadi.

Konstitutsiyaviy normalardan kelib chiqib, O'zbekistonda axborot xavfsizligi va kibermakonni tartibga soluvchi bir qator umumiy qonunlar qabul qilingan. Ulardan eng muhimlari:

- “Axborotlashtirish to'g'risida”²gi Qonun (2003-yil, yangi

¹ O'zbekiston Respublikasi Konstitutsiyasi (yangi tahrir). – Toshkent: O'zbekiston, 2023. URL: <https://lex.uz/docs/6788457>

² O'zbekiston Respublikasi Qonuni. “Axborotlashtirish to'g'risida” (yangi tahrir). – Toshkent: LexUZ, 2019. URL: <https://lex.uz/docs/4314861>

tahrir 2019-yil) – unda axborot resurslarini himoya qilish va ulardan foydalanish qoidolari belgilangan;

- “Telekommunikatsiyalar to'g'risida”¹gi Qonun (1999-yil, yangi tahrir 2018-yil) – unda davlatning tarmoqlar ustidan nazorati, litsenziyalash tartibi ko'rsatilgan;
- “Davlat sirlarini saqlash to'g'risida”²gi Qonun (1993-yil, tahrirlar bilan) – unda maxfiy axborotlarni himoya qilish mexanizmlari belgilangan.

Bu qonunlar umumiy infratuzilmani belgilab, kibermakon xavfsizligiga doir maxsus qonunlarning qabul qilinishi uchun huquqiy zamin yaratgan.

Konstitutsiya va umumiy qonunlarda belgilangan me'yorlar shuni ko'rsatadiki, O'zbekistonda kibermakon xavfsizligi erkinlik va nazorat dialektikasi asosida rivojlanmoqda. Bir tomondan, fuqaroning axborot olish va tarqatish huquqi kafolatlanadi, ikkinchi tomondan, davlat milliy xavfsizlik va jamoat tartibini ta'minlash majburiyatini zimmasiga oladi.

Falsafiy jihatdan bu jarayon “liberal-demokratik qadriyatlar” bilan “realistik davlat suvereniteti” o'rtasida muvozanat izlash sifatida talqin qilinadi. Huquqiy nuqtai nazardan esa, Konstitutsiya va umumiy qonunlar kibermakon xavfsizligi sohasidagi maxsus normativ-huquqiy hujjatlar uchun asosiy me'yoriy poydevor hisoblanadi.

O'zbekiston Konstitutsiyasi kibermakon xavfsizligini ta'minlash uchun zarur bo'lgan ikki muhim tamoyilni belgilaydi:

1. Axborot erkinligi – fuqarolarning axborotga egalik qilish va uni tarqatish huquqi.
2. Milliy xavfsizlikni ta'minlash – davlatning majburiyati sifatida internet va axborot tizimlarini himoya qilish.

O'zbekistonda kibermakon xavfsizligini huquqiy asosda rivojlantirish jarayonida Konstitutsiya markaziy rol o'ynaydi.

O'zbekistonda kibermakon xavfsizligini ta'minlash bo'yicha

¹ O'zbekiston Respublikasi Qonuni. “Telekommunikatsiyalar to'g'risida” (yangi tahrir). – Toshkent: LexUZ, 2018. URL: <https://lex.uz/docs/35869>

² O'zbekiston Respublikasi Qonuni. “Davlat sirlarini saqlash to'g'risida”. – Toshkent: LexUZ, 1993. URL: <https://lex.uz/docs/16112>

maxsus qonunlarning qabul qilinishi so'nggi yillarda davlat siyosatining eng muhim yo'nalishlaridan biri bo'ldi. Chunki axborot erkinligi va milliy xavfsizlik o'rtasidagi muvozanatni aniq belgilab beruvchi huquqiy mexanizmlarsiz kibermakon xavfsizligini samarali boshqarib bo'lmaydi. Shu maqsadda qabul qilingan eng muhim hujjatlar "Axborot xavfsizligi to'g'risida"gi Qonun (2022-yil) hamda "Shaxsiy ma'lumotlar to'g'risida"gi Qonun (2019-yil)dir.

2022-yilda qabul qilingan ushbu qonun O'zbekistonda kiberoxavfsizlikni huquqiy tartibga soluvchi asosiy normativ-huquqiy hujjatlardan biridir. Qonunda quyidagi ta'rif keltirilgan: «Axborot xavfsizligi — axborot resurslari va tizimlarining yaxlitligini, maxfiylikni va mavjudligini ta'minlashga qaratilgan davlat va jamiyat faoliyati majmui»¹.

Qonun quyidagi asosiy yo'nalishlarni belgilaydi:

- davlat organlari va tashkilotlarning axborot xavfsizligini ta'minlash bo'yicha majburiyatlari;
- milliy axborot tizimlarini sertifikatlashtirish va monitoring qilish tartibi;
- kibermakon xavfsizligini buzgan shaxslarning huquqiy javobgarligi;
- davlat-xususiy sektor hamkorligi asosida axborot xavfsizligini mustahkamlash.

Bu qonunning qabul qilinishi bilan O'zbekistonda axborot xavfsizligi masalalari alohida huquqiy asosga ega bo'ldi. Falsafiy jihatdan, bu hujjat milliy xavfsizlikni ustuvor qo'yadi, ammo inson huquqlari bilan muvofiqlashtirilgan tarzda ishlab chiqilgan.

2019-yilda qabul qilingan ushbu qonun O'zbekistonda kibermakon xavfsizligi va inson huquqlarini muhofaza qilish sohasida yangi bosqichni boshlab berdi. Qonunda shunday deyilgan:

«Shaxsiy ma'lumotlar — bu aniq jismoniy shaxsga oid, uni

¹ O'zbekiston Respublikasi Qonuni. "Axborot xavfsizligi to'g'risida". – Toshkent: LexUZ, 2022. URL: <https://lex.uz/docs/6003766>

identifikatsiya qilishga imkon beradigan ma'lumotlar majmui»¹.

Qonunning asosiy jihatlari:

- shaxsiy ma'lumotlarni yig'ish, saqlash va qayta ishlash tartibini belgilash;
- ma'lumot egasining rozilgisiz ularni tarqatishni taqiqlash;
- ma'lumotlarni himoyalash bo'yicha texnik va tashkiliy chora-tadbirlarni joriy etish;
- xalqaro axborot almashinuvida milliy suverenitetni ta'minlash.

Shu bilan birga, qonun joriy etilgandan keyin muhokamalarga sabab bo'ldi. Xususan, "Data localization" talabi, ya'ni O'zbekiston fuqarolarining shaxsiy ma'lumotlari faqat mamlakat hududida joylashgan serverlarda saqlanishi shartligi xalqaro IT-kompaniyalar uchun muayyan qiyinchiliklar tug'dirdi. Bu borada mutaxassislar shunday baho berishadi: «Data localization laws strengthen national sovereignty but may restrict global digital integration»².

- Kuchli tomonlari:
 - o Shaxsiy ma'lumotlarni huquqiy himoya qilishning milliy asoslari yaratildi;
 - o Axborot xavfsizligi bo'yicha davlat organlari va xususiy sektor majburiyatlari belgilandi;
 - o Kibermakon xavfsizligi buzilishlari uchun aniq javobgarlik mexanizmlari joriy etildi.
- Zaif tomonlari:
 - o "Data localization" talabi xalqaro hamkorlikni cheklashi mumkin;
 - o Qonunlarni amalga oshirish uchun yetarli texnik infratuzilma va mutaxassislar hali yetarli emas;
 - o Huquqiy normalarning xalqaro standartlarga to'liq integratsiyasi jarayoni davom etmoqda.

¹ O'zbekiston Respublikasi Qonuni. "Shaxsiy ma'lumotlar to'g'risida". – Toshkent: LexUZ, 2019. URL: <https://lex.uz/docs/4396428>

² Kuner, C. Data Localization and Human Rights. – International Data Privacy Law, Vol. 6, No. 4, Oxford University Press, 2016. – P. 253–268.

Ushbu ikki qonun kibermakon xavfsizligida davlat suvereniteti va inson huquqlari o'rtasidagi murakkab muvozanatni ifodalaydi. "Axborot xavfsizligi to'g'risida"gi qonun milliy xavfsizlikni ustuvor qo'ygan bo'lsa, "Shaxsiy ma'lumotlar to'g'risida"gi qonun insonning daxlsizligini markazga oladi. Shu bois, bu qonunlarni uyg'unlashtirish falsafiy jihatdan "nazorat va erkinlik dialektikasi"ni huquqiy me'yorlar orqali hal qilishga qaratilgan yondashuv sifatida baholash mumkin.

O'zbekistonda kibermakon xavfsizligini ta'minlash bo'yicha normativ-huquqiy asos faqat umumiy qonunlar va maxsus qonunlar bilan chegaralanmagan. Bu borada Prezident farmonlari va qarorlari davlat siyosatini belgilashda markaziy ahamiyat kasb etadi. Chunki ular strategik yo'nalishlarni aniqlab beradi, davlat organlarining faoliyatini muvofiqlashtiradi hamda milliy rivojlanish dasturlariga huquqiy kuch beradi.

Eng muhim hujjatlardan biri bu — O'zbekiston Respublikasi Prezidentining "Sun'iy intellekt texnologiyalarini 2030-yilgacha rivojlantirish strategiyasini tasdiqlash to'g'risida"gi PQ-358-son qaroridir. Qarorda shunday deyiladi: «Sun'iy intellekt texnologiyalarini rivojlantirish, ularni amaliyotga joriy etish va ularning xavfsiz qo'llanilishini ta'minlash davlat siyosatining ustuvor yo'nalishlaridan biridir»¹.

Bu hujjat kibermakon xavfsizligi bilan bevosita bog'liq, chunki sun'iy intellekt texnologiyalarining joriy etilishi yangi kiberxavflar va axloqiy-huquqiy muammolarni yuzaga keltiradi. Shu bois, qaror asosida AI va kibermakon xavfsizligi integratsiyalashgan holda ko'rilmogda.

Prezident qarorlari ichida eng keng qamrovlisi bu — "Raqamli O'zbekiston – 2030" strategiyasidir (PQ-6079-son, 2020-yil). Hujjatda shunday ta'kidlangan: «Axborot texnologiyalarini rivojlantirish, raqamli iqtisodiyotni shakllantirish va kiberxavfsizlikni mustahkamlash O'zbekistonning ustuvor yo'nalish-

¹ O'zbekiston Respublikasi Prezidentining PQ-358-son qarori, 14.10.2024-y. "Sun'iy intellekt texnologiyalarini 2030-yilgacha rivojlantirish strategiyasini tasdiqlash to'g'risida". – URL: <https://lex.uz/docs/7158604>

laridan biridir»¹.

Ushbu strategiyaning asosiy maqsadlari:

- davlat xizmatlarini to'liq raqamlashtirish;
- elektron hukumat tizimini rivojlantirish;
- milliy kiberxavfsizlik infratuzilmasini mustahkamlash;
- axborot xavfsizligi bo'yicha milliy monitoring tizimini

yaratish.

Shuningdek, hujjatda xalqaro reytinglarda (Global Cyber-security Index, E-Government Index) O'zbekistonning o'rnini yaxshilash maqsad qilib qo'yilgan.

O'zbekistonda kiberxavfsizlikni ta'minlashda quyidagi normativ-huquqiy hujjatlar ham muhim ahamiyat kasb etadi:

- PQ-3832-son qaror (2018-yil) – “Kiberxavfsizlik sohasida davlat boshqaruvini takomillashtirish chora-tadbirlari to'g'risida”². Bu qaror asosida maxsus kiberxavfsizlik bo'linmalari tashkil etildi.

- PQ-6079-son qaror (2020-yil) – “Raqamli O'zbekiston – 2030” davlat dasturini tasdiqlash.

- PF-60-son Farmon (2022-yil) – “Yangi O'zbekiston taraqqiyot strategiyasi”³ doirasida kiberxavfsizlikni kuchaytirish bo'yicha maxsus topshiriqlar berilgan.

Prezident qarorlari O'zbekistonda kibermakon xavfsizligini ta'minlashda strategik huquqiy mexanizm sifatida xizmat qilmoqda. Ular falsafiy jihatdan “taraqqiyot va xavfsizlik uyg'unligi” konsepsiyasiga asoslanadi.

- “Raqamli O'zbekiston – 2030” – innovatsion taraqqiyot va inson huquqlariga asoslangan model;

- PQ-358 – texnologik suverenitet va xavfsizlikni ustuvor

¹ O'zbekiston Respublikasi Prezidentining PQ-6079-son qarori, 05.10.2020-y. “Raqamli O'zbekiston – 2030” davlat dasturi. – URL: <https://lex.uz/docs/5031048>

² O'zbekiston Respublikasi Prezidentining PQ-3832-son qarori, 03.07.2018-y. “Kiberxavfsizlik sohasida davlat boshqaruvini takomillashtirish chora-tadbirlari to'g'risida”. – URL: <https://lex.uz/docs/3827636>

³ O'zbekiston Respublikasi Prezidentining PF-60-son Farmoni, 28.01.2022-y. “2022–2026-yillarga mo'ljallangan Yangi O'zbekiston taraqqiyot strategiyasi to'g'risida”. – URL: <https://lex.uz/docs/5841063>

qo'rgan hujjat;

- PQ-3832 – davlat nazoratini kuchaytiruvchi qaror.

Huquqiy jihatdan bu qarorlar milliy strategiyani huquqiy kuch bilan mustahkamlab, qonunlar va xalqaro shartnomalar bilan uyg'unlikda ishlaydi.

O'zbekistonda kibermakon xavfsizligi huquqiy bazasini falsafiy-huquqiy jihatdan baholashda uch asosiy nuqtaga e'tibor qaratish mumkin:

1. Erkinlik va nazorat dialektikasi. Konstitutsiya va maxsus qonunlar axborot erkinligini kafolatlaydi, biroq milliy xavfsizlikni ta'minlash zaruriyati davlat nazoratini kuchaytiradi. Bu "liberalizm" va "realizm" paradigmalari o'rtasidagi muvozanatni topish vazifasini qo'yadi.

2. Suverenitet va global integratsiya. "Shaxsiy ma'lumotlar to'g'risida"gi qonundagi data localization talabi milliy suverenitetni mustahkamlasa-da, global integratsiyani qisman cheklaydi. Shu bois, falsafiy nuqtai nazardan bu milliy manfaatlar bilan global hamkorlik o'rtasidagi ziddiyatni aks ettiradi.

3. Taraqqiyot va xavfsizlik uyg'unligi. Prezident qarorlari taraqqiyot (raqamli iqtisodiyot, AI) va xavfsizlikni birgalikda rivojlantirishga qaratilgan. Bu "barqaror taraqqiyot falsafasi"ga mos yondashuvdir.

O'zbekistonning kibermakon xavfsizligini ta'minlashga oid huquqiy bazasi kuchli tamoyillar asosida shakllangan: Konstitutsiyaviy kafolatlar, maxsus qonunlar va Prezident qarorlari mavjud. Ammo zaif tomonlari — infratuzilma cheklovlari, huquqiy moslashuvdagi muammolar va inson huquqlari bilan bog'liq masalalar — hali ham dolzarb.

Falsafiy-huquqiy nuqtai nazardan bu baza erkinlik va nazorat, suverenitet va global integratsiya, taraqqiyot va xavfsizlik o'rtasida muvozanat izlashning huquqiy ifodasidir.

O'zbekiston Respublikasida kibermakon xavfsizligini ta'minlash huquqiy bazasining shakllanishi bir necha bosqichlarda kechdi.

1. Dastlabki bosqich (1990–2000-yillar). Mustaqillikdan keyingi yillarda O'zbekistonda "Axborotlashtirish to'g'risida"

(2003) va “Telekommunikatsiyalar to‘g‘risida” (1999) kabi umumiy qonunlar qabul qilindi. Ularning asosiy maqsadi internet infratuzilmasini rivojlantirish va davlat nazoratini belgilash edi. Bu davrda kiberxavfsizlik maxsus huquqiy sohaga ajratilmagan bo‘lsa-da, huquqiy poydevor qo‘yildi.

2. Ikkinchi bosqich (2010–2020-yillar). Axborot texnologiyalarining tez sur‘atlarda kirib kelishi bilan kiberxavfsizlik mustaqil huquqiy yo‘nalishga aylandi. Bu davrda “Shaxsiy ma‘lumotlar to‘g‘risida” (2019) qonuni qabul qilinib, fuqarolarning axborot xavfsizligi huquqiy jihatdan kafolatlandi. Shu bilan birga, Prezidentning PQ-3832 (2018) qarori asosida davlat organlarida maxsus kiberxavfsizlik bo‘linmalari tashkil qilindi.

3. Uchinchi bosqich (2020-yildan hozirgacha). “Raqamli O‘zbekiston – 2030” dasturi (2020) va PQ-358 (2024) kabi hujjatlar qabul qilinib, kiberxavfsizlik strategik davlat siyosatining markaziy qismiga aylandi. Endi kibermakon xavfsizligi nafaqat texnik himoya, balki milliy xavfsizlik, sun‘iy intellektni tartibga solish va xalqaro hamkorlik bilan uzviy bog‘liq huquqiy yo‘nalish sifatida shakllandi.

Huquqiy bazaning kuchli jihatlari shundaki, u Konstitutsiyadan tortib maxsus qonunlarga izchil tizimni tashkil etadi. Konstitutsiya inson huquqlari va erkinliklarini kafolatlaydi, “Axborot xavfsizligi to‘g‘risida”gi qonun esa milliy kiberxavfsizlikni ta‘minlash mexanizmlarini belgilaydi. “Shaxsiy ma‘lumotlar to‘g‘risida”gi qonun esa insonning shaxsiy daxlsizligini himoya qiladi. Prezident qarorlarida esa strategik maqsadlar, davlat-xususiy sektor hamkorligi va xalqaro reytinglarda O‘zbekistonning o‘rnini mustahkamlash vazifasi qo‘yilgan.

Shu bilan birga, huquqiy bazaning ba‘zi kamchiliklari ham mavjud:

1. Texnik infratuzilma va kadrlar muammosi. Qonunlarda belgilangan talablarni bajarish uchun yetarli texnologik resurslar va malakali mutaxassislar hamon yetarli emas. Masalan, data localization talabi xalqaro kompaniyalar bilan

hamkorlikni qiyinlashtirmoqda.

2. Xalqaro standartlarga moslashuvdagi tafovutlar. Ayrim normalar Yevropa Ittifoqi yoki BMT standartlariga to'liq mos kelmaydi. Bu esa O'zbekistonning global kiberxavfsizlik tashabbuslarida faolligini cheklaydi.

3. Amaliyotdagi muammolar. Qonunlar mukammal bo'lsa-da, ayrim hollarda internet erkinligi vaqtincha cheklanadi, saytlar bloklanadi. Bu inson huquqlari bilan bog'liq bahslarni keltirib chiqarmoqda.

Agar O'zbekistonning huquqiy bazasini Markaziy Osiyo davlatlari bilan qiyoslasak, quyidagi natijani ko'ramiz:

- Qozog'iston – keng qamrovli “Kibershield” konsepsiyasi bilan huquqiy bazani tizimli shakllantirgan.
- Qirg'iziston – huquqiy hujjatlar bor, ammo resurslar va infratuzilma zaif.
- Tojikiston va Turkmaniston – asosan mafkuraviy nazorat va izolyatsiya orqali xavfsizlikni ta'minlashga urinmoqda.
- O'zbekiston – huquqiy baza va strategik qarorlar jihatidan Qozog'istondan keyingi yetakchi o'rinda.

Bu qiyosiy tahlil shuni ko'rsatadiki, O'zbekiston o'z huquqiy bazasini global standartlarga moslashtirish va milliy manfaatlarini himoya qilish o'rtasida muvozanatni izlayapti.

O'zbekiston tajribasi kibermakon xavfsizligini ta'minlashda uchta asosiy falsafiy-huquqiy tamoyilga tayanadi:

1. Erkinlik va nazorat dialektikasi. Konstitutsiya axborot erkinligini kafolatlaydi, maxsus qonunlar esa uni nazorat bilan uyg'unlashtiradi. Bu demokratik jamiyat va xavfsizlik davlatining o'zaro muvozanatini ifodalaydi.

2. Suverenitet va global integratsiya. Data localization kabi normalar milliy suverenitetni mustahkamlasa, xalqaro shartnomalarga qo'shilish esa global integratsiyani ta'minlaydi. Bu ikki tamoyil o'rtasida muvozanat zarur.

3. Taraqqiyot va xavfsizlik uyg'unligi. Prezident qarorlarida raqamli taraqqiyot va kiberxavfsizlik parallel ravishda rivojlantirilmoqda. Bu “barqaror taraqqiyot” falsafasining huquqiy ko'rinishi hisoblanadi.

O'zbekiston Respublikasida kibermakon xavfsizligini ta'minlash huquqiy bazasi Konstitutsiya, maxsus qonunlar va Prezident qarorlari orqali shakllangan izchil tizimdir. Bu tizimning kuchli tomonlari — strategik yondashuv, xalqaro me'yorlarga yaqinlashuv va inson huquqlarini huquqiy kafolatlash. Zaif tomonlari esa — infratuzilma cheklovlari, amaliy muammolar va xalqaro integratsiyadagi tafovutlar.

Falsafiy-huquqiy nuqtai nazardan, bu huquqiy baza milliy xavfsizlik va inson huquqlari, suverenitet va global integratsiya, taraqqiyot va xavfsizlik o'rtasida muvozanat izlashga asoslangan. Shu bois, O'zbekiston tajribasi kibermakon xavfsizligi sohasida nafaqat milliy, balki mintaqaviy model sifatida ham o'rganilishi mumkin.

3.3. O'zbekistonning milliy strategiyasi va xalqaro hamkorlikdagi ishtiroki

O'zbekiston Respublikasida kiberxavfsizlik strategiyasi davlatning keng qamrovli raqamli rivojlanish siyosati bilan uzviy bog'liq. 2020-yilda qabul qilingan "Raqamli O'zbekiston – 2030" dasturi mamlakatni raqamli transformatsiya qilish bo'yicha asosiy hujjat sifatida xizmat qilmoqda. Unda kiberxavfsizlik masalasi alohida yo'nalish sifatida belgilangan: «Axborot xavfsizligi, shaxsiy ma'lumotlarning himoyasi va kiberxavfsizlik davlat siyosatining ustuvor yo'nalishlari qatoriga kiradi»¹.

Dasturda kiberxavfsizlik bo'yicha quyidagi maqsadlar belgilangan:

1. Davlat xizmatlarini to'liq raqamlashtirish va ularni kiberxavfsizlik talablari asosida himoyalash.
2. Milliy kiberxavfsizlik tizimini yaratish – davlat organlari, bank-moliya sektori va strategik infratuzilmalarni himoya

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

qiluvchi yagona markazlashtirilgan tizim.

3. Axborot xavfsizligini monitoring qilish markazlarini tashkil etish va muntazam ravishda kiberhujumlar xavfini baholash.

4. Shaxsiy ma'lumotlarni himoya qilish bo'yicha xalqaro standartlarga mos mexanizmlarni joriy etish.

5. Kadrlar tayyorlash – oliy o'quv yurtlarida kiberxavfsizlik yo'nalishini rivojlantirish, xalqaro tajribalarni tatbiq qilish.

Shu yo'nalishlar O'zbekistonni 2030-yilgacha global kiberxavfsizlik tizimining faol ishtirokchisiga aylantirishni ko'zda tutadi.

2020–2023-yillar davomida dastur doirasida bir qancha muhim tashabbuslar amalga oshirildi:

- Milliy CERT (UZ-CERT) faoliyati kengaytirildi va xalqaro hamkorlik aloqalari mustahkamlandi.
- Davlat xizmatlari portal (my.gov.uz) kiberxavfsizlik sertifikatsiyasidan o'tkazildi.
- 2022-yilda Axborot xavfsizligi bo'yicha Respublika Kengashi faoliyati yo'lga qo'yildi.
- ITU Global Cybersecurity Index reytingida O'zbekiston 2020-yilda 86-o'ringa, 2022-yilda 64-o'ringa ko'tarildi¹.

Bu natijalar kiberxavfsizlikni mustahkamlash borasida amaliy qadamlar qo'yilayotganini ko'rsatadi.

“Raqamli O'zbekiston – 2030” dasturida kibermakon xavfsizligi ikki asosiy falsafiy tamoyil asosida talqin qilinadi:

1. Taraqqiyot va xavfsizlik uyg'unligi. Dastur raqamli transformatsiyani xavfsizlik bilan amalga oshirib bo'lmavligini ta'kidlaydi. Shu bois, kiberxavfsizlik innovatsion taraqqiyotning tarkibiy qismi sifatida qaraladi.

2. Inson huquqlari va davlat suvereniteti muvozanati. Strategiyada shaxsiy ma'lumotlarni himoya qilish inson huquqlarining kafolati sifatida talqin qilinsa-da, data localization kabi talablar davlat suverenitetini mustahkamlashga qaratilgan. Bu esa huquqiy jihatdan ikki tamoyilni uyg'unlashtirishga

¹ International Telecommunication Union (ITU). Global Cybersecurity Index 2020–2022. Geneva: ITU Publications, 2022. – P. 84–90.

urinayotganini ko'rsatadi.

“Raqamli O‘zbekiston – 2030” dasturi kiberxavfsizlikni:

- raqamli davlat boshqaruvi va iqtisodiyotning poydevori,
- xalqaro reytinglarda mamlakat o‘rnini mustahkamlovchi

mezon,

- inson huquqlari va davlat suvereniteti o‘rtasidagi muvozanat mexanizmi sifatida talqin qiladi.

Shujihatdan, bu hujjat nafaqat texnik rivojlanish dasturi, balki kiberxavfsizlik falsafasini huquqiy darajada shakllantiruvchi strategik konsepsiya sifatida qaraladi.

Kibermakon xavfsizligini ta'minlash nafaqat huquqiy hujjatlar orqali, balki amaliy institutlar faoliyati orqali ham amalga oshiriladi. O‘zbekistonda so‘nggi yillarda milliy kiberxavfsizlik markazlari tashkil etildi va ular davlat organlari hamda xususiy sektor bilan hamkorlikda ishlashni boshladi. Bu yondashuv «davlatning asosiy vazifasi milliy xavfsizlikni ta'minlash bo'lsa, xususiy sektor innovatsiya va texnologiyalarni joriy etishda asosiy hamkor bo'lishi kerak»¹ degan prinsip asosida shakllandi.

O‘zbekistonda faoliyat olib borayotgan milliy markazlar faoliyati:

1. UZ-CERT (Computer Emergency Response Team of Uzbekistan). Ushbu markaz O‘zbekistonning kiberxavfsizlik infratuzilmasida asosiy institut hisoblanadi. UZ-CERTning asosiy vazifalari: kiberhujumlarni monitoring qilish, ularni tezkor aniqlash va bartaraf etish, davlat organlariga maslahat berish, xalqaro CERT tarmoqlari bilan hamkorlik qilish. 2021-yilda markaz tomonidan 15 mingdan ortiq kiberinsident qayd etilgan².

2. Axborot xavfsizligini ta'minlash bo'yicha Respublika Kengashi. 2022-yilda tashkil etilgan bu kengash hukumat darajasida kiberxavfsizlik siyosatini muvofiqlashtirish

¹ OECD Report. Public-Private Partnerships in Cybersecurity. Paris: OECD Publishing, 2019. – P. 12–18.

² UZ-CERT. Annual Report 2021. Tashkent: National Cybersecurity Center of Uzbekistan, 2022. – P. 5–14.

vazifasini bajaradi. Uning qarorlari majburiy kuchga ega bo'lib, davlat organlari faoliyatini uyg'unlashtirishga xizmat qiladi.

3. Davlat xizmatlari markazlari va "my.gov.uz" portali xavfsizligi bo'yicha bo'linmalar. Bulo'linmalar elektron hukumat tizimini himoya qilish bilan shug'ullanadi. Chunki fuqarolarga taqdim etiladigan davlat xizmatlari kiberhujumlarning asosiy nishoniga aylangan.

O'zbekistonda kiberxavfsizlik sohasida davlat va xususiy sektor hamkorligi tobora kuchayib bormoqda.

- Bank-moliya sektori. Markaziy bank va yirik tijorat banklari (masalan, "Xalq banki", "Asaka bank") UZ-CERT bilan hamkorlikda moliyaviy tranzaksiyalar xavfsizligini ta'minlash bo'yicha qo'shma loyihalarni amalga oshirmoqda.

- Telekommunikatsiya kompaniyalari. "Uztelecom", "Ucell" va "Beeline Uzbekistan" kabi operatorlar davlat bilan hamkorlikda tarmoqlar xavfsizligini kuchaytirish bo'yicha kelishuvlar imzolagan.

- Xalqaro IT kompaniyalari. Microsoft, Kaspersky Lab va Huawei O'zbekistonda kiberxavfsizlik bo'yicha treninglar va qo'shma loyihalar o'tkazmoqda¹.

Bu hamkorlik davlatning nazorat funksiyasi va xususiy sektorning innovatsion imkoniyatlarini birlashtirishga xizmat qilmoqda.

O'zbekistonda kiberxavfsizlik institutlari faoliyati falsafiy jihatdan "ijtimoiy kontrakt" tamoyiliga asoslanadi. Davlat milliy xavfsizlikni ta'minlaydi, xususiy sektor esa texnologik yechimlar va xizmatlarni taqdim etadi.

Huquqiy nuqtai nazardan, bu hamkorlik davlat-xususiy sheriklik to'g'risidagi qonunlar va Prezident qarorlari asosida yo'lga qo'yilgan. Shu bois, kibermakon xavfsizligi masalasi nafaqat davlat siyosati, balki iqtisodiy hamkorlik sohasi sifatida ham qaralmoqda.

Milliy kiberxavfsizlik markazlari va davlat-xususiy sektor hamkorligi O'zbekistonda kibermakon xavfsizligini ta'min-

¹ Microsoft Uzbekistan. Cybersecurity Training Programs 2020–2022. Tashkent: Microsoft Press, 2022. – P. 7–11.

lashning asosiy mexanizmlaridan biridir. Ularning faoliyati:

1. Kiberhujumlarni tezkor aniqlash va bartaraf etish;
2. Davlat organlari va xususiy kompaniyalar o'rtasidagi hamkorlikni mustahkamlash;
3. Xalqaro tajribani milliy tizimga tatbiq etish;
4. Fuqarolarning raqamli xizmatlarga bo'lgan ishonchini oshirishga qaratilgan.

Shu sababli, bu yondashuv falsafiy-huquqiy jihatdan kibermakon xavfsizligini milliy xavfsizlik va innovatsion taraqqiyot uyg'unligi sifatida talqin qilish imkonini beradi.

O'zbekiston Respublikasi kibermakon xavfsizligini faqat milliy darajada emas, balki xalqaro hamkorlik orqali ham ta'minlash zarurligini anglab yetgan. Chunki kiberjinoyatlar va kiberxavflar transchegaraviy xarakterga ega bo'lib, ular bilan samarali kurashish uchun xalqaro huquqiy mexanizmlar va kooperatsiya zarur. Shu bois, O'zbekiston BMT, ITU, SHHT, MDH va OSCE kabi tashkilotlar doirasida faol ishtirok etib kelmoqda.

O'zbekiston BMTning kibermakon xavfsizligiga oid rezolyutsiyalarini muntazam qo'llab-quvvatlab keladi. 2015-yilda qabul qilingan *BMT Bosh Assambleyasi rezolyutsiyasida* shunday deyilgan: «All states have the right to control ICT within their territory while respecting international obligations and human rights»¹.

O'zbekiston bu tamoyilni o'z siyosatida qo'llab, milliy suverenitet va inson huquqlarini uyg'unlashtirish zarurligini ta'kidlaydi. Bundan tashqari, O'zbekiston BMTning *“Open-ended Working Group on ICT Security”* ishida qatnashib, xalqaro xavfsizlik tizimlarini ishlab chiqishda o'z takliflarini ilgari surmoqda. O'zbekiston ITUning faol a'zosi sifatida global kiberxavfsizlik tashabbuslarida muntazam qatnashadi. ITU tomonidan tuziladigan *Global Cybersecurity Index (GCI)* reytingida O'zbekiston 2020-yilda 86-o'rinda bo'lsa, 2022-yilda 64-o'ringa ko'tarildi.

¹ United Nations General Assembly. Resolution on International Cooperation in Information Security. New York: UN, 2015. – URL: <https://digitallibrary.un.org/record/807879>

ITU ekspertlari ta'kidlaganidek: «Uzbekistan has made significant progress in creating a national cybersecurity strategy and establishing a national CERT»¹. Bu ishtirok mam-lakatning xalqaro reytinglardagi o'rnini mustahkamlash bilan birga, xalqaro tajribalarni milliy tizimga tatbiq qilish imkonini berdi.

O'zbekiston SHHT doirasida kiberxavfsizlik masalalariga katta e'tibor qaratmoqda. 2009-yilda qabul qilingan "Axborot xavfsizligi bo'yicha Moskva kelishuvi"da SHHT davlatlari axbo-rot-kommunikatsiya texnologiyalaridan terrorizm va ekstre-mizm maqsadida foydalanishga qarshi kurashishga kelishib olgan².

O'zbekiston bu hujjatni ratifikatsiya qilib, SHHTning *Axbo-rot xavfsizligi bo'yicha mintaqaviy markazi* bilan hamkorlikda faoliyat yuritmoqda. Shu orqali diniy ekstremizm va radi-kalizmga qarshi kurashda mintaqaviy yondashuvni qo'llab-quvvatlamogda.

MDH doirasida 2013-yilda qabul qilingan "*Axborot xavfsizligi konsepsiyasi*" hamkorlik uchun muhim asos bo'ldi. Unda shunday deyilgan: «Сотрудничество государств-участников СНГ направлено на формирование единого информационного пространства и защиту национальных интересов»³.

O'zbekiston bu tashabbusda ishtirok etib, MDH doirasida axborot almashish va kiberjinoyatlarga qarshi kurash bo'yicha qo'shma tadbirlarni qo'llab-quvvatlaydi. Shu bilan birga, MDH hamkorligi mintaqaviy integratsiyaning huquqiy asosini mustahkamlashda muhim ahamiyat kasb etadi.

O'zbekiston OSCE bilan ham kibermakon xavfsizligi bo'yicha hamkorlik qiladi. 2016-yilda OSCE tomonidan qabul qilingan

¹ International Telecommunication Union (ITU). Global Cybersecurity Index 2022. Geneva: ITU Publications, 2022. – P. 84–90.

² Shanghai Cooperation Organisation (SCO). Agreement on Cooperation in the Field of International Information Security. Moscow: SCO Secretariat, 2009. – P. 5–13.

³ СНГ. Концепция сотрудничества государств-участников в области информационной безопасности. Минск: СНГ, 2013. – P. 2–10.

Confidence-Building Measures (CBMs) dasturida O'zbekiston ishtirok etib, milliy kiberxavfsizlik tizimining shaffofligini oshirishga hissa qo'shgan.

OSCE hisobotida qayd etilganidek: «Uzbekistan has actively supported the development of confidence-building measures in cyberspace to prevent conflicts and enhance transparency»¹. Bu tashabbus O'zbekistonning xalqaro huquqiy mexanizmlarda ishonchli hamkor sifatida e'tirof etilishiga xizmat qilmoqda.

O'zbekistonning xalqaro tashkilotlardagi ishtiroki falsafiy jihatdan uch asosiy tamoyilga asoslanadi:

1. *Suverenitet va hamkorlik dialektikasi*. O'zbekiston milliy manfaatlarni ustuvor qo'yadi, lekin xalqaro tashkilotlar orqali hamkorlikni ham kengaytiradi.

2. *Xavfsizlik va inson huquqlari muvozanati*. BMT va OSCE doirasida inson huquqlarini ta'minlash, SHHT va MDH doirasida esa xavfsizlikni kuchaytirish yondashuvi qo'llaniladi.

3. *Mintaqaviy va global uyg'unlik*. ITU va BMT global standartlarni taklif qilsa, SHHT va MDH mintaqaviy hamkorlikni mustahkamlaydi. O'zbekiston bu ikki yo'nalishni uyg'unlashtirishga intilmoqda.

O'zbekistonning xalqaro tashkilotlardagi ishtiroki kibermakon xavfsizligini ta'minlashda quyidagi vazifalarni bajaradi:

- xalqaro standartlarni milliy tizimga integratsiya qilish;
- kiberjinoyatlarga qarshi transchegaraviy mexanizmlarni yaratish;
- inson huquqlari va milliy xavfsizlikni uyg'unlashtirish;
- mamlakatning xalqaro maydondagi obro'sini mustahkamlash.

Shunday qilib, O'zbekiston xalqaro hamkorlik orqali kibermakon xavfsizligini ta'minlashda faol o'rin egallamoqda va bu jarayon falsafiy-huquqiy jihatdan "milliy manfaatlar va global hamkorlik muvozanati" tamoyiliga asoslanadi.

O'zbekiston Respublikasining kibermakon xavfsizligi bo'yicha milliy strategiyasi so'nggi yillarda sezilarli yutuqlarga

¹ OSCE. Confidence-Building Measures in Cyberspace. Vienna: OSCE Publications, 2016. – P. 11–17.

erishdi. Avvalo, *“Raqamli O‘zbekiston – 2030”* dasturi mamlakatda raqamli transformatsiya siyosatining markaziy hujjatiga aylandi. Unda kiberxavfsizlik nafaqat qo‘shimcha yo‘nalish, balki raqamli taraqqiyotning asosi sifatida belgilandi. Shuning uchun ham davlat xizmatlarining raqamlashtirilishi, elektron hukumat tizimining shakllanishi va bank-moliya sektorining modernizatsiyasi kiberxavfsizlikni ta‘minlamasdan turib amalga oshirilishi mumkin emas.

Shu bilan birga, milliy *UZ-CERT* markazi, *Axborot xavfsizligi bo‘yicha Respublika Kengashi* kabi institutlar tashkil etildi¹. Bu institutlar kiberinsidentlarni monitoring qilish, xalqaro hamkorlikni yo‘lga qo‘yish va milliy strategiyani amalga oshirishda muhim ahamiyat kasb etmoqda.

Natijada, O‘zbekiston *ITU Global Cybersecurity Index* reytingida qisqa muddat ichida yuqorilab, 2020-yildagi 86-o‘rindan 2022-yilda 64-o‘ringa chiqdi. Bu xalqaro maydonda mamlakatning kibermakon xavfsizligiga e‘tiborining ortganini ko‘rsatadi.

O‘zbekiston kibermakon xavfsizligini faqat milliy darajada emas, balki xalqaro hamkorlik orqali ham mustahkamlashga intilmoqda. Bu borada:

- *BMT* doirasida — xalqaro rezolyutsiyalarni qo‘llab-quvvatlash, “Open-ended Working Group” ishida qatnashish²;
- *ITU*da — global reytinglarda ishtirok etish va milliy siyosatni xalqaro standartlarga yaqinlashtirish³;
- *SHHT*da — “axborot terrorizmi”ga qarshi mintaqaviy kelishuvlarda faol qatnashish⁴;

¹ UZ-CERT. Annual Report 2021. – Tashkent: National Cybersecurity Center of Uzbekistan, 2022. – P. 5–14.

² United Nations General Assembly. Resolution on International Cooperation in Information Security. – New York: UN, 2015. – URL: <https://digitallibrary.un.org/record/807879>

³ Shanghai Cooperation Organisation (SCO). Agreement on Cooperation in the Field of International Information Security. – Moscow: SCO Secretariat, 2009. – P. 5–13.

⁴ СНГ (MDH). Концепция сотрудничества государств-участников в области информационной безопасности. – Минск: Исполнительный комитет СНГ, 2013. – P. 2–10.

- *MDH*da — axborot xavfsizligi konsepsiyasini qo'llab-quvvatlash¹;

- *OSCE*da — kiberxavfsizlik bo'yicha ishonchni mustahkamlash choralari amalga oshirish².

Shu orqali O'zbekiston xalqaro hamjamiyat oldida o'zini mas'uliyatli hamkor sifatida ko'rsatmoqda.

O'zbekistonning milliy strategiyasi va xalqaro hamkorligining kuchli tomonlarini quyidagicha sanab o'tish mumkin:

1. *Huquqiy asosning mustahkamligi*. PQ-6079 ("Raqamli O'zbekiston – 2030"), PQ-358 ("AI strategiyasi") kabi hujjatlar kiberxavfsizlik siyosatini aniq huquqiy poydevorga qo'ydi.

2. *Milliy institutlarning mavjudligi*. UZ-CERT, Respublika Kengashi va sohaviy markazlar muntazam faoliyat yuritmoqda.

3. *Davlat-xususiy sheriklik modeli*. Banklar, telekom operatorlari va IT kompaniyalari davlat bilan hamkorlikda tizimni mustahkamlashda faol qatnashmoqda.

4. *Xalqaro hamkorlik*. O'zbekiston mintaqaviy va global darajada faol integratsiya qilmoqda.

5. *Xalqaro reytinglarda o'sish*. ITU indeksida yuqorilash bu siyosatning samaradorligini ko'rsatmoqda.

Yuqoridagilardan kelib chiqib quyidagilarni xulosa qilamiz:

- O'zbekistonning milliy strategiyasi kibermakon xavfsizligini davlat taraqqiyotining ajralmas qismi sifatida belgiladi.

- Milliy markazlar va davlat-xususiy sheriklik kibermakon xavfsizligini amalda ta'minlashga xizmat qilmoqda.

- Xalqaro hamkorlik orqali O'zbekiston global kiberxavfsizlik tizimining faol ishtirokchisiga aylanmoqda.

- Kuchli tomonlar (huquqiy asos, institutlar, xalqaro hamkorlik) zaif tomonlardan (infratuzilma, kadrlar, xalqaro

¹ OSCE. Confidence-Building Measures in Cyberspace. – Vienna: OSCE Publications, 2016. – P. 11–17.

² O'zbekiston Respublikasi Prezidentining PQ-358-son qarori, 14.10.2024-y. "Sun'iy intellekt texnologiyalarini 2030-yilgacha rivojlantirish strategiyasi to'g'risida". – Toshkent: Prezident Administratsiyasi, 2024. – URL: <https://lex.uz/docs/7158604>

standartlarga moslashuvdagi muammolar) ustun.

- Falsafiy-huquqiy jihatdan O'zbekiston tajribasi milliy manfaatlar va global hamkorlik, erkinlik va nazorat, taraqqiyot va xavfsizlik o'rtasidagi muvozanatni topishga qaratilgan.

O'zbekistonning milliy strategiyasi va xalqaro hamkorligi kibermakon xavfsizligi sohasida nafaqat milliy, balki mintaqaviy miqyosda ham yetakchi model sifatida qaralishi mumkin.

Raqamli transformatsiya sharoitida insoniyat hayoti tobora axborot-kommunikatsiya texnologiyalari bilan chambarchas bog'lanib bormoqda. Shu bilan birga, texnologiyalar rivoji yangi imkoniyatlar bilan bir qatorda, yangi tahdidlarni ham yuzaga keltirmoqda. Ayniqsa, kibermakon orqali amalga oshiriladigan jinoyatlar, firibgarliklar, axborot urushlari, ekstremistik targ'ibotlar inson va jamiyat xavfsizligiga jiddiy tahdid tug'dirmoqda. Shu sababli, faqat texnik choralar yoki huquqiy mexanizmlar emas, balki keng ijtimoiy ong va madaniyat darajasida kiberxavfsizlik madaniyatini shakllantirish dolzarb masalaga aylanmoqda.

“Kiberxavfsizlik madaniyati” tushunchasi xalqaro adabiyotlarda keng qo'llanila boshladi. ITU ekspertlari ta'kidlaganidek: «Cybersecurity culture is the knowledge, attitudes and behaviors of people that help to maintain the security of the information environment»¹.

Demak, bu tushuncha ikki jihatni o'z ichiga oladi:

1. Bilim va ko'nikmalar – kiberxavfsizlik bo'yicha texnik va huquqiy tushunchalarni egallash.

2. Qadriyatlar va odatlar – kundalik hayotda xavfsizlikni ta'minlash uchun ongli ravishda amal qilish.

Kiberxavfsizlik madaniyati shaxsiy darajada – oddiy foydalanuvchining parolni murakkab qo'yishi, noma'lum fayllarni ochmasligi; jamiyat darajasida – ta'lim va axborot siyosatining xavfsizlikni ustuvor qo'yishi; davlat darajasida esa – milliy strategiya va qonunlarning samarali ishlashi orqali namoyon bo'ladi.

¹ International Telecommunication Union (ITU). Building a Culture of Cybersecurity. – Geneva: ITU Publications, 2018. – P. 7–14.

Kiberxavfsizlik madaniyatining jamiyat rivojlanishidagi o'rnini uchta asosiy yo'nalishda ko'rinadi:

1. Ijtimoiy barqarorlikni ta'minlash. Kiberhujumlar nafaqat alohida shaxslarga, balki butun jamiyatga salbiy ta'sir ko'rsatishi mumkin. Masalan, bank tizimiga qilingan hujumlar iqtisodiy beqarorlikka olib keladi. Shu sababli, fuqarolarning axborot madaniyatini oshirish ijtimoiy barqarorlikning kafo-latidir.

2. Inson huquqlarini himoya qilish. Shaxsiy ma'lumotlar-ni noqonuniy tarqalishi, onlayn kuzatuvlar yoki kiberfi-ribgarliklar inson huquqlarini buzadi. Kiberxavfsizlik mada-niyati esa fuqarolarning huquq va erkinliklarini muhofaza qilishga xizmat qiladi.

3. Innovatsion rivojlanishni rag'batlantirish. ITU ma'lu-motiga ko'ra, «Countries with strong cybersecurity culture have higher rates of digital innovation and economic growth»¹. Ya'ni, odamlar o'zini xavfsiz his qilganida, onlayn xizmatlardan kengroq foydalanadi va iqtisodiy faoliyat kuchayadi.

O'zbekistonda kiberxavfsizlik madaniyati masalasi so'nggi yillarda davlat siyosatining muhim qismiga aylanmoqda. 2020-yilda qabul qilingan "Raqamli O'zbekiston – 2030" dasturida axborot xavfsizligi masalasi alohida yo'nalish sifatida belgilangan². Bundan tashqari, 2022-yilgi "Axborot xavfsizligi to'g'risida"gi Qonun ham fuqarolarning ongini oshirish, axborot muhitida xavfsiz xatti-harakatlarni shakllantirish zarurligini ko'rsatadi³.

Maktablarda "Axborot texnologiyalari" fanida kiberxavfsizlik elementlari o'qitilmoqda, oliy ta'lim muassasalarida esa maxsus "Kiberxavfsizlik" yo'nalishlari ochildi. Shu orqali, yoshlarning raqamli savodxonligi va axborot madaniyati

¹ International Telecommunication Union (ITU). Global Cybersecurity Index 2020. – Geneva: ITU Publications, 2020. – P. 33–40.

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>

³ O'zbekiston Respublikasi Qonuni. "Axborot xavfsizligi to'g'risida". – Toshkent: LexUZ, 2022. – URL: <https://lex.uz/docs/6003766>

bosqichma-bosqich rivojlanmoqda.

Kiberxavfsizlik madaniyatining falsafiy mohiyati — bu inson va texnologiya o'rtasidagi uyg'unlikni saqlashdir. Texnologiyalar jamiyat hayotini yengillashtiradi, lekin ular xavfsiz bo'lmasa, taraqqiyot xavf ostida qoladi. Shu sababli, falsafiy nuqtai nazardan kiberxavfsizlik madaniyati jamiyat taraqqiyotining "ma'naviy immuniteti" sifatida qaralishi mumkin.

Huquqiy nuqtai nazardan esa, kiberxavfsizlik madaniyati Konstitutsiyada belgilangan axborot erkinligi va milliy xavfsizlik o'rtasidagi muvozanatni amaliy hayotda ta'minlash mexanizmi hisoblanadi.

Kiberxavfsizlik madaniyati nafaqat texnik himoya, balki keng ijtimoiy jarayondir. U shaxsiy xulq-atvor, ta'lim, ilmiy tadqiqotlar va davlat siyosati orqali shakllanadi. Jamiyat taraqqiyotida uning ahamiyati shundaki:

- ijtimoiy barqarorlikni ta'minlaydi;
- inson huquqlarini himoya qiladi;
- innovatsion rivojlanishni rag'batlantiradi.

O'zbekiston tajribasi shuni ko'rsatadiki, kiberxavfsizlik madaniyatini shakllantirish — bu uzoq muddatli strategik vazifa bo'lib, u milliy xavfsizlik va taraqqiyotning ajralmas qismi sifatida talqin qilinishi lozim.

Kiberxavfsizlik sohasida barqaror tizim yaratishning eng muhim sharti — yuqori malakali mutaxassislarni tayyorlashdir. Chunki texnologik infratuzilma va huquqiy baza qanchalik mukammal bo'lmasin, agar yetarli bilim va ko'nikmaga ega kadrlar bo'lmasa, milliy xavfsizlik tizimi samarali ishlay olmaydi. Shuning uchun ham BMT va ITU ekspertlari ta'kidlaganidek: «Cybersecurity is not only about technology, it is also about people, skills and education»¹.

O'zbekiston sharoitida ham oliy ta'lim tizimida kiberxavfsizlik bo'yicha mutaxassislar tayyorlash masalasi so'nggi yillarda davlat siyosatining ustuvor yo'nalishiga aylandi.

2018-yildan boshlab O'zbekistonda axborot xavfsizligi

¹ United Nations. Cybersecurity Skills and Education Report. – New York: UN, 2019. – P. 14–19.

bo'yicha maxsus ta'lim yo'nalishlari joriy qilindi. 2020-yilda "Raqamli O'zbekiston – 2030" dasturi doirasida barcha yirik texnika universitetlarida kiberxavfsizlik kafedralari tashkil etildi [6].

Hozirda quyidagi oliy ta'lim muassasalarida kiberxavfsizlik yo'nalishlari faoliyat yuritmoqda:

- Toshkent axborot texnologiyalari universiteti (TATU) – "Axborot xavfsizligi" bakalavr va magistr dasturlari;
- Toshkent davlat texnika universiteti – "Kiberxavfsizlik injiniringi" yo'nalishi;
- Inha universiteti (Toshkent) – xalqaro standartlar asosidagi "Information Security" dasturi;
- Qarshi, Farg'ona, Samarqand filiallari – hududiy kadrlar tayyorlash markazlari sifatida.

Bu yo'nalishlarda talabalar tarmoq xavfsizligi, kriptografiya, ma'lumotlar bazasini himoyalash, axborot xavfsizligi siyosati va huquqiy asoslar kabi fanlarni o'rganadilar.

O'zbekiston hukumati kiberxavfsizlik sohasida kadrlar tayyorlashni qo'llab-quvvatlash maqsadida bir qator normativ-huquqiy hujjatlarni qabul qilgan:

- PQ-3832 (2018) – "Kiberxavfsizlik sohasida davlat boshqaruvini takomillashtirish chora-tadbirlari" qarorida maxsus ta'lim yo'nalishlarini rivojlantirish vazifasi belgilangan¹.
- PQ-6079 (2020) – "Raqamli O'zbekiston – 2030" dasturida har yili 5000 dan ortiq IT-mutaxassis, jumladan, kiberxavfsizlik bo'yicha mutaxassis tayyorlash maqsadi qo'yilgan².
- PF-60 (2022) – "Yangi O'zbekiston taraqqiyot strategiyasi"da kiberxavfsizlik sohasi bo'yicha ilmiy-tadqiqot va innovatsion faoliyatni rivojlantirish zaruriyati ko'rsatib

¹ O'zbekiston Respublikasi Prezidentining PQ-3832-son qarori, 03.07.2018-y. "Kiberxavfsizlik sohasida davlat boshqaruvini takomillashtirish chora-tadbirlari to'g'risida". – Toshkent, 2018. – URL: <https://lex.uz/docs/3827636>

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>

o'tilgan¹.

Shuningdek, ta'lim grantlari, davlat buyurtmalari va xalqaro loyihalar orqali yosh mutaxassislarni tayyorlash ko'lamini kengaytirish rejalashtirilgan.

O'zbekiston oliy ta'lim muassasalari kiberxavfsizlik sohasida xalqaro hamkorlikni ham kengaytirmoqda:

- Inha universiteti (Toshkent) Janubiy Koreya bilan qo'shma dasturlarni amalga oshirmoqda.
- TATU Yevropa Ittifoqining Erasmus+ dasturi doirasida axborotxavfsizligi bo'yicha qo'shma loyihalarda qatnashmoqda.
- Microsoft, Kaspersky Lab va Huawei kompaniyalari O'zbekiston talabalari uchun treninglar va sertifikatlash dasturlarini taklif etmoqda².

Bunday hamkorlik natijasida talabalarga nafaqat nazariy bilim, balki amaliy ko'nikmalar ham berilmoqda.

Shunga qaramay, oliy ta'lim tizimida bir qator muammolar mavjud:

1. Kadrlar yetishmovchiligi. Professor-o'qituvchilarning aksariyati nazariy bilimlarga ega, amaliy tajriba esa yetarli emas.

2. Texnik baza cheklangan. Ko'plab laboratoriyalar zamonaviy kiberxavfsizlik vositalari bilan to'liq jihozlanmagan.

3. Xalqaro sertifikatsiya kamligi. CISSP, CEH, CompTIA Security+ kabi xalqaro sertifikatlarni olgan mutaxassislar juda oz.

4. Hududiy nomutanosiblik. Poytaxtdagi universitetlarda imkoniyat ko'proq, viloyatlarda esa bu yo'nalish endigina shakllanmoqda.

Kiberxavfsizlik sohasida kadrlar tayyorlash masalasi falsafiy jihatdan "ilm va amaliyot birligi" tamoyiliga asoslanadi. Texnologiyalar tez sur'atlarda rivojlanayotgan bir paytda,

¹ O'zbekiston Respublikasi Prezidentining PF-60-son Farmoni, 28.01.2022-y. "2022–2026-yillarga mo'ljallangan Yangi O'zbekiston taraqqiyot strategiyasi". – Toshkent, 2022. – URL: <https://lex.uz/docs/5841063>

² Microsoft Uzbekistan. Cybersecurity Training Programs 2020–2022. – Tashkent: Microsoft Press, 2022. – P. 7–11.

nazariy bilimlar amaliy tajriba bilan uyg'unlashmasa, ta'lim samarasi past bo'ladi.

Huquqiy nuqtai nazardan, oliy ta'lim tizimi "Axborot xavfsizligi to'g'risida"gi Qonun va "Ta'lim to'g'risida"gi Qonun¹ asosida faoliyat yuritib, davlatning kiberxavfsizlik sohasidagi majburiyatlarini amalga oshirishga xizmat qiladi.

O'zbekistonda oliy ta'lim tizimida kiberxavfsizlik bo'yicha kadrlar tayyorlash jarayoni bosqichma-bosqich shakllanmoqda. Kuchli tomonlari: maxsus yo'nalishlarning ochilishi, davlat siyosatining qo'llab-quvvatlashi, xalqaro hamkorlik. Zaif tomonlari: kadrlar va texnik baza yetishmovchiligi, hududiy nomutanosiblik.

Falsafiy-huquqiy jihatdan, bu jarayon milliy xavfsizlik va ta'lim, nazariya va amaliyot, suverenitet va global integratsiya o'rtasida muvozanat izlashni anglatadi.

Kiberxavfsizlikni ta'minlashda faqat ta'lim va huquqiy mexanizmlar emas, balki ilmiy tadqiqotlar ham hal qiluvchi ahamiyatga ega. Chunki kiberjinoyatlar, yangi tahdidlar va ularni bartaraf etish usullari texnologiyalar kabi tez rivojlanadi. Shu sababli, davlatlarning milliy kiberxavfsizlik salohiyati ilmiy izlanishlar, innovatsiyalar va ilmiy-tadqiqot institutlarining faoliyatiga bevosita bog'liqdir. ITU ekspertlari qayd etganidek: «Innovation in cybersecurity is not a luxury, but a necessity for national resilience»².

O'zbekiston uchun ham bu masala dolzarb bo'lib, ilmiy tadqiqotlar kiberxavfsizlik strategiyasining ajralmas qismi sifatida qaralmoqda.

Ilmiy tadqiqotlar kibermakon xavfsizligini ta'minlashda quyidagi vazifalarni bajaradi:

1. Tahdidlarni prognozlash. Yangi turdagi viruslar, xakerlik usullari va ijtimoiy muhandislik sxemalarini oldindan aniqlash.
2. Texnik yechimlar ishlab chiqish. Mahalliy antivirus

¹ O'zbekiston Respublikasi Qonuni. "Ta'lim to'g'risida". – Toshkent: LexUZ, 2020. – URL: <https://lex.uz/docs/5013007>

² International Telecommunication Union (ITU). Cybersecurity Innovation Report. – Geneva: ITU Publications, 2019. – P. 5–12.

tizimlari, shifrlash algoritmlari, xavfsiz dasturiy platformalar yaratish.

3. Huquqiy mexanizmlarni takomillashtirish. Ilmiy izlanishlar asosida yangi qonunlar va normativ hujjatlarni ishlab chiqish.

4. Xalqaro tajribani moslashtirish. Ilmiy tahlillar orqali global tajribani milliy sharoitga moslashtirish.

So'nggi yillarda O'zbekiston ilmiy jamoatchiligi kiberxavfsizlik bo'yicha bir qator yo'nalishlarda tadqiqotlar olib bormoqda:

- Kriptografiya va ma'lumotlarni shifrlash. Toshkent axborot texnologiyalari universiteti va O'zbekiston Fanlar akademiyasi huzuridagi laboratoriyalarda milliy kriptografik algoritmlar ishlab chiqilmoqda.

- Kiberjinoyatchilikka qarshi kurash. Ichki ishlar vazirligi va prokuratura organlari bilan hamkorlikda ilmiy izlanishlar amalga oshirilmoqda.

- Sun'iy intellekt va kiberxavfsizlik. 2024-yilda qabul qilingan PQ-358 qarorida sun'iy intellekt asosida kiberxavfsizlik monitoringini joriy etish vazifasi belgilangan¹.

- Inson omili va kiberxavfsizlik madaniyati. Ijtimoiy-falsafiy tadqiqotlar orqali foydalanuvchilarning axborotga bo'lgan munosabati o'rganilmoqda.

So'nggi yillarda kiberxavfsizlik sohasida bir qator innovatsion startaplar ham paydo bo'ldi. Masalan:

- Cyber Academy Uzbekistan – yoshlar uchun amaliy treninglar va simulyatsiya platformalari;

- UZSOC (Uzbekistan Security Operations Center) – milliy darajadagi xavfsizlik monitoring markazi;

- Startap loyihalar – mobil ilovalar va antivirus dasturlarini ishlab chiqishga yo'naltirilgan kichik korxonalar.

Bunday tashabbuslar davlat grantlari, IT-park rezidentlari va

¹ O'zbekiston Respublikasi Prezidentining PQ-358-son qarori, 14.10.2024-y. "Sun'iy intellekt texnologiyalarini 2030-yilgacha rivojlantirish strategiyasi". – Toshkent: Prezident Administratsiyasi, 2024. – URL: <https://lex.uz/docs/7158604>

xalqaro hamkorlik dasturlari orqali qo'llab-quvvatlanmoqda.

Ilmiy tadqiqotlarni rivojlantirishda xalqaro hamkorlik alohida o'rin tutadi. O'zbekiston quyidagi tashkilotlar bilan ilmiy almashinuv olib bormoqda:

- ITU va UNDP – kiberxavfsizlik bo'yicha qo'shma tadqiqot loyihalari;
- SHHT – "Axborot xavfsizligi bo'yicha ilmiy markazlar" tarmog'ida ishtirok;
- Yevropa Ittifoqi – Erasmus+ va Horizon Europe dasturlari orqali ilmiy almashinuv;
- Rossiya va Koreya – kriptografiya va axborot xavfsizligi bo'yicha qo'shma ilmiy izlanishlar.

O'zbekistonda kiberxavfsizlik bo'yicha ilmiy tadqiqotlar rivojlanayotgan bo'lsa-da, bir qator muammolar mavjud:

1. Moliyalashtirishning yetarli emasligi. Ilmiy grantlar ko'proq fundamental yo'nalishlarga ajratilmoqda, amaliy tadqiqotlar esa kamroq qo'llab-quvvatlanmoqda.

2. Kadrlar yetishmovchiligi. Yuqori malakali ilmiy tadqiqotchilar soni cheklangan.

3. Xalqaro integratsiya pastligi. O'zbekiston olimlarining xalqaro indeksatsiyadagi jurnallarda maqolalari hali kam.

4. Natijalarni amaliyotga tatbiq qilishdagi uzilishlar. Ilmiy ishlanmalar ko'pincha real sektorga yetib bormaydi.

Ilmiy tadqiqotlar va innovatsiyalarni rivojlantirish falsafiy nuqtai nazardan "bilim va xavfsizlik dialektikasi" sifatida talqin qilinadi. Jamiyat taraqqiyoti yangi bilimlarsiz mumkin emas, biroq bu bilimlar xavfsizlik bilan uyg'unlashmasa, taraqqiyot xavfga aylanadi.

Huquqiy nuqtai nazardan esa, ilmiy tadqiqotlar davlatning konstitutsiyaviy majburiyatlariga asoslanadi. Konstitutsiyada «ilm-fan va innovatsiyalar davlat tomonidan qo'llab-quvvatlanadi»¹ deyilgan. Shu bois, ilmiy izlanishlar kiberxavfsizlik sohasida ham huquqiy kafolatga ega.

¹ O'zbekiston Respublikasi Konstitutsiyasi (yangi tahrir). – Toshkent: O'zbekiston, 2023. – URL: <https://lex.uz/docs/6788457>

Ilmiy tadqiqotlar va innovatsiyalar O'zbekistonning milliy kiberxavfsizlik salohiyatini mustahkamlashda hal qiluvchi omil hisoblanadi. Ularning asosiy vazifalari tahdidlarni prognozlash, texnik yechimlar ishlab chiqish, huquqiy mexanizmlarni takomillashtirish va xalqaro tajribani moslashtirishdir.

Kuchli tomonlari — davlatning e'tibori, maxsus yo'nalishlarning mavjudligi, xalqaro hamkorlik. Zaif tomonlari — moliyaviy va kadrlar cheklovi, ilmiy natijalarning amaliyotga tatbiq etilishidagi muammolar.

Falsafiy-huquqiy nuqtai nazardan, bu jarayon ilm-fan va xavfsizlik uyg'unligi, milliy manfaatlar va global hamkorlik muvozanati sifatida talqin qilinadi.

Kibermakon xavfsizligi masalalari tobora murakkablashib, nafaqat texnik yoki huquqiy, balki falsafiy jihatdan ham tahlilni talab etmoqda. Chunki inson va texnologiya, erkinlik va nazorat, milliy suverenitet va global integratsiya o'rtasidagi murakkab muvozanat aynan shu sohada yaqqol namoyon bo'ladi. Ta'lim va ilmiy tadqiqotlar orqali shakllanadigan kiberxavfsizlik madaniyati esa bu muvozanatni ta'minlashda hal qiluvchi rol o'ynaydi. Kiberxavfsizlik madaniyatini shakllantirish falsafiy jihatdan quyidagi natijalarni beradi:

Birinchidan, erkinlik va nazorat dialektikasi. Falsafada erkinlik insonning rivojlanish omili sifatida qaralsa, nazorat esa barqarorlik va xavfsizlikning kafolati sifatida talqin qilinadi. Kibermakon xavfsizligida bu ikki tamoyil to'qnash keladi: bir tomondan, fuqaro erkin internetdan foydalanishni istaydi, ikkinchi tomondan, davlat milliy xavfsizlikni ta'minlash uchun nazoratni kuchaytirishga majbur bo'ladi. Shu sababli, ta'lim tizimida erkinlik va nazoratni uyg'unlashtiruvchi ong shakllanishi zarur.

Ikkinchidan, bilim va xavfsizlik uyg'unligi. Insoniyat tarixida bilim doimo taraqqiyotning kaliti bo'lgan. Lekin bilim xavfsizliksiz qo'llansa, jamiyatga tahdid tug'diradi. Kibermakonda ham bilim — yangi texnologiyalarni yaratadi, xavfsizlik esa ularni jamiyat foydasiga yo'naltiradi. Shu bois, ilmiy tadqiqotlar kiberxavfsizlikni rivojlantirish bilan birga, uni

falsafiy-huquqiy asosda to'g'ri yo'naltirish vazifasini bajaradi.

Uchinchidan, Suverenitet va global integratsiya. O'zbekiston "Shaxsiy ma'lumotlar to'g'risida"gi qonun orqali milliy suverenitetni mustahkamladi. Shu bilan birga, BMT, ITU, SHHT, OSCE kabi tashkilotlar bilan hamkorlik qilishi orqali global integratsiyani kuchaytirmoqda. Bu ikki tamoyilni uyg'unlashtirish falsafiy nuqtai nazardan "milliy manfaatlar va jahon taraqqiyoti muvozanati" sifatida qaraladi.

Beshinchidan, taraqqiyot va xavfsizlikning ajralmasligi. "Raqamli O'zbekiston – 2030" dasturi taraqqiyot va xavfsizlikni bir-biridan ajratmasdanki¹. Chunki xavfsizliksiz taraqqiyot zaif, taraqqiyotsiz xavfsizlik esa ma'nosizdir. Falsafiy jihatdan bu "insoniyat taraqqiyotining barqarorlik paradigmasi"dir.

Kiberxavfsizlik madaniyatini shakllantirish huquqiy jihatdan asoslar quyidagilardan iborat:

Birinchidan, Konstitutsiyaviy asoslar. 2023-yilgi yangi Konstitutsiyada «Har kim axborotni izlash, olish va tarqatish huquqiga ega»² degan norma mavjud. Shu bilan birga, davlat milliy xavfsizlikni ta'minlash majburiyatini zimmasiga olgan. Demak, huquqiy jihatdan axborot erkinligi va milliy xavfsizlik o'zaro uyg'unlikda talqin qilinadi.

Ikkinchidan, Maxsus qonunlar. "Axborot xavfsizligi to'g'risida" (2022) va "Shaxsiy ma'lumotlar to'g'risida" (2019) qonunlari milliy kiberxavfsizlikni huquqiy asos bilan mustahkamladi³. Biroq, ularni amalda qo'llash jarayonida xalqaro standartlarga moslashuv jarayoni davom etmoqda.

Uchinchidan, Prezident qarorlari va strategiyalar. PQ-6079 ("Raqamli O'zbekiston – 2030") va PQ-358 (AI strategiyasi) qarorlari kiberxavfsizlikni strategik davlat siyosatiga

¹ 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>

² O'zbekiston Respublikasi Konstitutsiyasi (yangi tahrir). – Toshkent: O'zbekiston, 2023. – URL: <https://lex.uz/docs/6788457>

³ O'zbekiston Respublikasi Qonuni. "Axborot xavfsizligi to'g'risida". – Toshkent: LexUZ, 2022. – URL: <https://lex.uz/docs/6003766>

aylantirdi¹. Bu hujjatlar huquqiy tizimni global standartlarga yaqinlashtirdi.

To'rtinchidan, Xalqaro huquqiy mexanizmlar. O'zbekiston xalqaro tashkilotlar doirasida qabul qilingan hujjatlarni qo'llab-quvvatlash orqali milliy qonunchilikni xalqaro me'yorlarga uyg'unlashtirmoqda. Masalan, OSCEning "Confidence-Building Measures" dasturi milliy tizimning shaffofligini oshirdi².

Ta'lim va ilmiy tadqiqotlar orqali kiberxavfsizlik madaniyatini shakllantirish O'zbekistonning milliy xavfsizligi va taraqqiyotida markaziy o'rin tutadi. Falsafiy jihatdan bu jarayon inson va texnologiya, erkinlik va nazorat, suverenitet va global integratsiya, taraqqiyot va xavfsizlik o'rtasidagi muvozanatni ta'minlashga qaratilgan. Huquqiy jihatdan esa, Konstitutsiya, maxsus qonunlar va Prezident qarorlari bu muvozanatni kafolatlaydi.

Istiqbolda O'zbekistonning kiberxavfsizlik siyosati milliy manfaatlarni himoya qilish bilan birga global hamkorlikni rivojlantirish, inson huquqlarini ta'minlash bilan birga milliy xavfsizlikni mustahkamlash, ta'lim va ilm-fan orqali yangi avlodni kiberxavfsizlik madaniyatiga tayyorlash kabi ustuvor yo'nalishlarga tayanadi.

Yuqoridagi tahlillarni umumlashtirgan holda ta'lim va ilmiy tadqiqotlar orqali kiberxavfsizlik madaniyatini shakllantirish masalasi quyidagi xulosalarni bildiramiz:

Birinchidan, kibermakon xavfsizligini ta'minlash nafaqat texnik va huquqiy vositalarga, balki keng ijtimoiy ong va madaniyatga ham bog'liq. O'zbekiston tajribasi shuni ko'rsatadiki, kiberxavfsizlik madaniyati tushunchasi jamiyat taraqqiyotining ajralmas qismiga aylangan. Chunki axborot muhitida ongli, mas'uliyatli xatti-harakatlarni shakllantir-

¹ O'zbekiston Respublikasi Prezidentining PQ-358-son qarori, 14.10.2024-y. "Sun'iy intellekt texnologiyalarini 2030-yilgacha rivojlantirish strategiyasi". – Toshkent: Prezident Administratsiyasi, 2024. – URL: <https://lex.uz/docs/7158604>

² OSCE. Confidence-Building Measures in Cyberspace. – Vienna: OSCE Publications, 2016. – P. 11–17.

masdan turib, texnik vositalar samarasi cheklangan bo'ladi. Shu ma'noda, ta'lim tizimida kiberxavfsizlik asoslarini o'qitish, yoshlarni axborot savodxonligi va xavfsiz xatti-harakatlarga o'rgatish strategik vazifaga aylandi. Bu jarayon jamiyatni raqamli transformatsiya sharoitida "ma'naviy immunitet" bilan ta'minlaydi.

Ikkinchidan, Oliy ta'lim tizimida kiberxavfsizlik yo'nalishlarining joriy etilishi O'zbekistonning muhim yutug'idir. Toshkent axborot texnologiyalari universiteti, Inha universiteti, boshqa texnika oliygohlarida maxsus fakultetlar ochilishi mutaxassislar tayyorlashni yangi bosqichga olib chiqdi. Ammo, bu jarayon hali ham kamchiliklardan holi emas: professor-o'qituvchilar tarkibida amaliy tajriba yetarli emas, laboratoriyalar zamonaviy texnik vositalar bilan to'liq jihozlanmagan, xalqaro sertifikatlashga ega mutaxassislar soni kam. Shu sababli, istiqbolda davlat siyosati kadrlar tayyorlashning sifat jihatidan oshishiga qaratilishi zarur.

Uchinchidan, Kiberxavfsizlik bo'yicha ilmiy tadqiqotlar O'zbekistonning milliy salohiyatini mustahkamlashda hal qiluvchi ahamiyatga ega. Kriptografiya, sun'iy intellekt asosidagi xavfsizlik, kiberjinoyatchilikka qarshi kurash yo'nalishlari bo'yicha izlanishlar olib borilmoqda. Shu bilan birga, startaplar va IT-park rezidentlari ham bu jarayonga qo'shilmoqda. Masalan, Cyber Academy Uzbekistan va UZSOC kabi loyihalar milliy innovatsion salohiyatni oshirishga xizmat qilmoqda. Lekin moliyalashtirish va xalqaro integratsiya borasida muammolar mavjud. Bu esa ilmiy ishlanmalarni amaliyotga tatbiq etishni qiyinlashtirmoqda.

III BOB BO'YICHA XULOSALAR

"Kibermakonda xavfsiz muhitni ta'minlash davlatlar tajribasi" monografiyasining uchinchi bobi mintaqaviy tajriba va O'zbekiston tajribasiga bag'ishlandi. Bobni o'rganish davomida quyidagi xulosalarga keldik:

Birinchidan, Markaziy Osiyo mintaqasida kibermakon xavfsizligi muammolari umumiy xususiyatlarga ega. Bu davlatlar:

- texnologik infratuzilmada rivojlanish sur'atlari turlicha bo'lsa-da, umumiy xavf – kiberjinoyatlar va axborot urushlariga qarshi kurashish;
- huquqiy bazada ayrim tafovutlarga ega bo'lsa-da, xalqaro standartlarga moslashishga intilmoqda;
- xalqaro tashkilotlarda (BMT, SHHT, MDH) ko'proq mintaqaviy yondashuvni qo'llamoqda.

O'zbekiston tajribasi Qozog'iston bilan bir qatorda yetakchi o'rinda bo'lib, huquqiy va institutsional tizimi rivojlangan, strategik qarorlar bilan mustahkamlangan.

Ikkinchidan, O'zbekistonning huquqiy bazasi quyidagilardan tashkil topadi:

- *Konstitutsiya* – axborot erkinligi va milliy xavfsizlikni kafolatlaydi.
- *Maxsus qonunlar* – “Axborot xavfsizligi to'g'risida” (2022) va “Shaxsiy ma'lumotlar to'g'risida” (2019) qonunlari milliy huquqiy tizimni shakllantirdi.
- *Prezident qarorlari* – PQ-6079 (“Raqamli O'zbekiston – 2030”), PQ-358 (AI strategiyasi), PQ-3832 kabi hujjatlar strategik vazifalarni belgilab berdi.

Kuchli tomonlari — huquqiy asosning mavjudligi, xalqaro me'yorlarga yaqinlashuv, institutsional mexanizmlar. Zaif tomonlari — texnik infratuzilmaning cheklanganligi, kadrlar yetishmasligi va amaliyotdagi ayrim huquqiy tafovutlar.

Uchinchidan, O'zbekiston milliy strategiyasida kiberxavfsizlik davlat siyosatining ajralmas qismi sifatida qaralmoqda. “Raqamli O'zbekiston – 2030” dasturi doirasida:

- davlat xizmatlarini raqamlashtirish,
- milliy kiberxavfsizlik tizimini yaratish,
- xalqaro reytinglarda o'rinni mustahkamlash maqsad qilingan.

To'rtinchidan, Xalqaro maydonda esa O'zbekiston:

- BMTda – xalqaro rezolyutsiyalarni qo'llab-quvvatlaydi;
- ITUda – GCI reytingida o'z o'rnini yaxshilamoqda;

- SHHT va MDHda – axborot xavfsizligi bo'yicha mintaqaviy hamkorlikni rivojlantirmoqda;
- OSCEda – ishonchni mustahkamlash mexanizmlarida qatnashmoqda.

Bu ishtirok O'zbekistonni xalqaro hamjamiyatda mas'uliyatli hamkor sifatida tanitmoqda.

Beshinchidan, Kiberxavfsizlik madaniyatini shakllantirishning asosi — ta'lim va ilmiy tadqiqotlar.

- *Oliy ta'lim* – TATU, Inha universiteti va boshqa texnika oliygohlarida kiberxavfsizlik yo'nalishlari ochilgan.

- *Ilmiy tadqiqotlar* – kriptografiya, sun'iy intellekt asosida xavfsizlik, kiberjinoyatchilikka qarshi kurash yo'nalishlari rivojlanmoqda.

- *Innovatsiyalar* – UZSOC, Cyber Academy kabi startaplar milliy salohiyatni oshirmoqda.

Muammolar: moliyaviy ta'minot yetarli emas, xalqaro integratsiya past, laboratoriya bazalari cheklangan. Shu sababli istiqbolda davlat-xususiy sheriklik va xalqaro hamkorlik asosida ta'lim va ilmiy faoliyatni kengaytirish zarur.

Oltinchidan, falsafiy-huquqiy nuqtai nazardan quyidagi uch asosiy xulosa chiqadi:

1. *Erkinlik va nazorat uyg'unligi.* Fuqarolar uchun axborot erkinligi kafolatlangan, lekin davlat milliy xavfsizlikni ta'minlash maqsadida nazoratni ham kuchaytiradi. Bu — kibermakonda ijtimoiy barqarorlikni ta'minlashga xizmat qiluvchi dialektika.

2. *Suverenitet va global integratsiya muvozanati.* O'zbekiston milliy qonunlar orqali suverenitetni mustahkamlab, xalqaro tashkilotlarda faol ishtiroki orqali integratsiyani ta'minlamoqda.

3. *Taraqqiyot va xavfsizlik birligi.* "Raqamli O'zbekiston – 2030" dasturi taraqqiyot va xavfsizlikni ajralmas hodisa sifatida talqin qiladi. Bu falsafiy jihatdan barqaror taraqqiyot paradigmasini ifodalaydi.

"Mintaqaviy tajriba va O'zbekiston" nomli bobimizning eng umumiy natijalari sifatida quyidagilarni bayon qilamiz:

- Markaziy Osiyo davlatlari umumiy xavf va imkoniyatlarga ega, O'zbekiston esa huquqiy va strategik bazasi bilan yetakchi o'rinda.
- Huquqiy asoslar mukammal, lekin amaliyotda texnik va kadrlar bilan bog'liq muammolar mavjud.
- Milliy strategiya xalqaro reytinglarda O'zbekiston o'rnini mustahkamladi va xalqaro hamkorlik orqali tajribani boyitdi.
- Ta'lim va ilmiy tadqiqotlar orqali yangi avlodni kiberxavfsizlik madaniyatiga tayyorlash jarayoni bosqichma-bosqich amalga oshmoqda.

O'zbekiston tajribasi kibermakon xavfsizligi sohasida milliy va mintaqaviy yetakchi model bo'lib, falsafiy-huquqiy jihatdan inson huquqlari va davlat suvereniteti, erkinlik va nazorat, taraqqiyot va xavfsizlik o'rtasidagi muvozanatni topishga asoslanadi. Bu tajriba kelajakda O'zbekistonning global kiberxavfsizlik tizimidagi rolini kuchaytirishi va barqaror rivojlanish modelini shakllantirishiga xizmat qiladi.

IV-BOB. GLOBAL HAMKORLIK VA KELAJAK ISTIQBOLLARI

Mazkur bobda kibermakon xavfsizligini ta'minlashda global hamkorlik va kelajak istiqbollari falsafiy-huquqiy hamda amaliy jihatdan tahlil qilinadi. Kibermakonning transmilliy xususiyati bir davlatning o'z kuchi bilan xavfsizlikni to'liq kafolatlashi mumkin emasligini ko'rsatmoqda. Shu sababli, BMT, NATO, SHHT, OSCE va boshqa xalqaro tashkilotlarning faoliyati, ularning axborot xavfsizligi sohasidagi tashabbuslari hamda hamkorlik mexanizmlarining ahamiyati yoritiladi. Shuningdek, kibermakon faqat texnik infratuzilma emas, balki inson huquqlari, shaxsiy hayot daxlsizligi va axborot etikasi bilan bog'liq ijtimoiy-falsafiy muhit sifatida talqin qilinadi. UNESCO, Yevropa Ittifoqi va BMT tomonidan ishlab chiqilgan axborot etikasi tamoyillari – haqqoniylik, shaffoflik, mas'uliyat va shaxsiy ma'lumotlarni himoya qilish – global miqyosda kiberxavfsizlik siyosatining asosiy poydevori sifatida baholalanadi. Shu bilan birga, sun'iy intellekt, kvant hisoblash va katta ma'lumotlar kabi yangi texnologiyalar kiberxavfsizlikni mustahkamlash bilan birga yangi xavf-xatarlarni ham yuzaga keltirishi alohida tahlil qilinadi. Budapest konvensiyasi va boshqa xalqaro huquqiy hujjatlar mavjud bo'lsa-da, kelajakda yangi universal konvensiyalar qabul qilish zarurati ta'kidlanadi. Falsafiy-huquqiy umumlashtirishda inson huquqlari, xavfsizlik va barqarorlik uyg'unligi kelajak kiberxavfsizlik siyosatining markaziy paradigmasi sifatida ko'riladi. O'zbekiston tajribasi misolida milliy manfaatlar va global tamoyillar uyg'unligiga intilish, shaxsiy ma'lumotlar himoyasi, xalqaro tashkilotlarda faol ishtirok va "Raqamli O'zbekiston – 2030" dasturi doirasida texnologik mustaqillikka erishish yo'lidagi sa'y-harakatlar yoritiladi.

4.1. Davlatlararo hamkorlik: BMT, NATO, SCO va boshqa tashkilotlarning roli

Birlashgan Millatlar Tashkiloti (BMT) xalqaro xavfsizlikning barcha sohalarida yetakchi institut bo'lgani kabi, kibermakon xavfsizligi masalalarida ham markaziy platforma hisoblanadi. Zero, kiberjinoyatlar va kiberhujumlar milliy chegaralarni tan olmaydi. Shu sababli ularni faqat davlatlarning o'z kuchi bilan emas, balki xalqaro miqyosdagi hamkorlik orqali bartaraf etish mumkin. BMT doirasidagi tashabbuslar nafaqat huquqiy me'yorlarni belgilash, balki davlatlar o'rtasida ishonchni mustahkamlash, axborot texnologiyalaridan tinchlik va taraqqiyot maqsadida foydalanishni kafolatlashga qaratilgan.

BMT Bosh Assambleyasi so'nggi yigirma yil davomida kiberoxavfsizlikka oid qator rezolyutsiyalar qabul qildi. Masalan, 2015-yilda qabul qilingan "Developments in the field of information and telecommunications in the context of international security" rezolyutsiyasida shunday deyiladi: «All states have the right to control ICT within their territory while respecting international obligations and human rights»¹.

Mazkur tamoyil ikki asosiy g'oyani mujassam etadi:

1. Davlatlarning milliy suvereniteti va kibermakon ustidan nazorat huquqi.

2. Shu bilan birga, xalqaro majburiyatlar va inson huquqlariga rioya qilish zarurati.

Bu rezolyutsiya O'zbekiston tomonidan ham qo'llab-quvvatlangan bo'lib, mamlakatimiz kiberoxavfsizlik siyosatida ham milliy manfaatlarni himoya qilish, ham xalqaro huquqiy me'yorlarga moslashishga intilib kelmoqda.

BMT doirasida kiberoxavfsizlik bo'yicha eng muhim mexanizmlar — Governmental Group of Experts (GGE) va Open-ended Working Group (OEWG) hisoblanadi.

¹ United Nations General Assembly. Resolution on Developments in the Field of Information and Telecommunications in the Context of International Security. – New York: UN, 2015. – URL: <https://digitallibrary.un.org/record/807879>

- GGE (Ekspertlar guruhi). 2004-yildan buyon faoliyat yuritayotgan bu guruh kiberxavfsizlik bo'yicha xalqaro huquq normalarini ishlab chiqish bilan shug'ullanadi. Masalan, 2013-yildagi hisobotda xalqaro huquq, jumladan, BMT Nizomi kibermakonda ham amal qilishi qayd etilgan.

- OEWG (Ochiq ishchi guruh). 2019-yildan boshlab barcha BMT a'zo davlatlari uchun ochiq bo'lgan bu guruh kiber-makon xavfsizligini mustahkamlash bo'yicha keng qamrovli muzokaralar maydoniga aylandi. OEWG doirasida davlatlar o'z pozitsiyalarini erkin bildirish imkoniyatiga ega bo'ldi.

O'zbekiston OEWG majlislarida faol ishtirok etib, kiber-makon xavfsizligida mintaqaviy hamkorlik va xalqaro standart-larning milliy qonunchilikka integratsiyasini qo'llab-quvvatlab kelmoqda.

Kiberxavfsizlik masalalari BMTning Barqaror rivojlanish maqsadlari (SDGs) bilan ham bevosita bog'liq. Masalan:

- 9-maqсад (Sanoat, innovatsiya va infratuzilma) – raqamli infratuzilma xavfsiz bo'lmasa, innovatsiya samarali bo'lmaydi.

- 16-maqсад (Tinchlik, adolat va samarali institutlar) – kiberjinoyatlarga qarshi kurash samarali institutlarni talab qiladi.

- 17-maqсад (Hamkorlik) – kiberxavfsizlik global ham-korliksiz ta'minlanmaydi.

Shu sababli, BMT kiberxavfsizlikni nafaqat xavfsizlik, balki barqaror rivojlanishning ham ajralmas qismi sifatida ko'radi¹.

BMT doirasida bir qator maxsus agentliklar ham kiber-xavfsizlik masalalarida faoliyat yuritmoqda:

- ITU (Xalqaro telekommunikatsiya ittifoqi) – Global Cybersecurity Index (GCI) orqali davlatlarning kiberxavfsizlik salohiyatini baholaydi.

- UNODC (BMTning giyohvandlik va jinoyatlarga qarshi idorasi) – kiberjinoyatchilikka qarshi kurash bo'yicha xalqaro hamkorlikni muvofiqlashtiradi.

¹ United Nations. Sustainable Development Goals and Cybersecurity. – New York: UN, 2020. – P. 22–30.

- UNESCO – axborot erkinligi va shaxsiy hayot daxlsizligi bo'yicha normativ hujjatlar ishlab chiqishda ishtirok etadi.

O'zbekiston ushbu agentliklar bilan hamkorlikni yo'lga qo'ygan. Masalan, ITUning GCI reytingida mamlakatimizning ko'rsatkichlari 2020–2022 yillarda sezilarli darajada yaxshilangan¹.

BMT tashabbuslarini falsafiy nuqtai nazardan tahlil qilar ekanmiz, quyidagi dialektikani ko'ramiz:

1. Milliy suverenitet va global hamkorlik. Davlatlar o'z hududida axborotni nazorat qilish huquqiga ega, ammo ular xalqaro hamjamiyat bilan hamkorlik qilmasdan turib xavfsizlikni ta'minlay olmaydi.

2. Xavfsizlik va inson huquqlari. BMT rezolyutsiyalari xavfsizlikni kuchaytirishni talab qiladi, lekin shu bilan birga, inson huquqlari buzilmasligi shartini ham qo'yadi.

3. Taraqqiyot va xavfsizlik uyg'unligi. BMT kiberxavfsizlikni barqaror rivojlanishning sharti sifatida ko'radi.

Huquqiy nuqtai nazardan esa, BMT tashabbuslari kiberma-konda xalqaro huquq normalarining amal qilishini kafolatlashga xizmat qiladi. Bu esa davlatlarning milliy qonunchiligiga moslashtirilishi zarur bo'lgan asosiy yo'nalishlardan biridir.

BMT doirasidagi kiberxavfsizlik tashabbuslari quyidagi asosiy natijalarga olib keldi:

- kibermakonda xalqaro huquq normalari amal qilishini tasdiqladi;
- davlatlararo ishonchni mustahkamlash uchun platforma yaratdi;
- inson huquqlari va milliy xavfsizlik o'rtasida muvozanat tamoyilini belgiladi;
- barqaror rivojlanish maqsadlariga erishishda kiberxavfsizlikni ustuvor yo'nalish sifatida e'tirof etdi.

BMT tashabbuslari global kiberxavfsizlik siyosatida hal qiluvchi o'rin tutadi va O'zbekiston uchun ham huquqiy, ham falsafiy jihatdan muhim yo'nalish hisoblanadi.

¹ International Telecommunication Union (ITU). Global Cybersecurity Index 2022. – Geneva: ITU Publications, 2022. – P. 84–90.

Shimoliy Atlantika Shartnomasi Tashkiloti (NATO) XXI asrda nafaqat harbiy-siyosiy blok, balki global xavfsizlikning keng ko'lamli yo'nalishlarini qamrab oluvchi institutga aylandi. Raqamli texnologiyalar va kibermakonning rivojlanishi NATO oldiga yangi xavflar va vazifalarni qo'ydi. Agar XX asrda asosiy e'tibor yadroviy xavfsizlik va harbiy bloklar o'rtasidagi muvozanatga qaratilgan bo'lsa, XXI asrda kiberhujumlar davlatlarning mudofaa va iqtisodiy salohiyatiga jiddiy xavf tug'diruvchi omilga aylandi.

NATO bu vaziyatni inobatga olib, kiberxavfsizlikni o'zining kollektiv mudofaa konsepsiyasining ajralmas qismi sifatida belgiladi. Shu tariqa, tashkilot "kiberhujum"ni harbiy hujum bilan tenglashtirib, unga qarshi 5-modda (kollektiv mudofaa prinsipi)ni qo'llash imkoniyatini ochdi.

NAToning rasmiy hujjatlarida kiberxavfsizlik

1. 2008-yil, Bucharest Summit. NATO ilk bor kiber-xavfsizlikni mudofaa siyosatining ustuvor yo'nalishi sifatida tan oldi.

2. 2010-yil, Lisbon Summit. NAToning yangi strategik konsepsiyasida kiberxavfsizlik rasmiy ravishda tashkilotning asosiy faoliyat yo'nalishiga kiritildi.

3. 2014-yil, Wales Summit. Kiberhujumlarni harbiy hujum bilan tenglashtirish qarori qabul qilindi. NATO Bosh kotibi shunday degan edi: «A cyberattack can trigger Article 5, just like a conventional armed attack»¹.

4. 2016-yil, Warsaw Summit. Kibermakon NAToning alohida operatsion domeni sifatida tan olindi (quruqlik, dengiz, havo bilan bir qatorda).

5. 2021-yil, Brussels Summit. NAToning yangi kiber-xavfsizlik siyosati qabul qilinib, unda davlat-xususiy sheriklik,

¹ NATO. Wales Summit Declaration on Cyber Defence. – Cardiff: NATO Press, 2014. – URL: https://www.nato.int/cps/en/natohq/official_texts_112964.htm

innovatsiyalar va sun'iy intellektning xavfsizlikdagi roli alohida qayd etildi¹.

NATOning amaliy mexanizmlari

1. NATO Cooperative Cyber Defence Centre of Excellence (CCDCOE). Estoniya poytaxti Tallinn shahrida joylashgan ushbu markaz NATO davlatlari va hamkorlari uchun kiberxavfsizlik bo'yicha tadqiqot va treninglarni amalga oshiradi. Har yili o'tkaziladigan Locked Shields mashg'ulotlari dunyodagi eng yirik kiber-harbiy o'yinlardan biri hisoblanadi.

2. NATO Cyber Rapid Reaction Teams (CRRTs). Favqulodda vaziyatlarda NATOga a'zo davlatlarga yordam berish uchun tuzilgan tezkor guruhlar. Ular 24/7 rejimida faoliyat yuritadi va real vaqt rejimida kiberhujumlarga qarshi javob qaytaradi.

3. NATO Industry Cyber Partnership (NICP). Davlat-xususiy sheriklik mexanizmi bo'lib, unda IT kompaniyalar, startaplar va ilmiy markazlar ishtirok etadi. Maqsad: xususiy sektor innovatsiyalarini harbiy va davlat infratuzilmasiga tatbiq qilish.

NATOning xalqaro hamkorlik siyosati

NATO nafaqat a'zolari, balki hamkor davlatlar bilan ham kiberxavfsizlik bo'yicha faol hamkorlik qiladi. Masalan:

- Gruziya va Ukraina bilan kiberxavfsizlik bo'yicha qo'shma markazlar tashkil etilgan.

- MDH davlatlari, jumladan O'zbekiston uchun ham NATOning tajribasi xalqaro muloqot va treninglarda muhim manba hisoblanadi.

- NATOning BMT, Yevropa Ittifoqi va OSCE bilan hamkorligi kiberxavfsizlikning global tizimini shakllantirishga xizmat qilmoqda.

NATOning kiberxavfsizlik siyosati ham qator muammolardan xoli emas:

1. Kollektiv mudofaa tamoyili. Kiberhujumlarni aniq davlatga nisbat berish qiyin bo'lgani uchun 5-moddaning amalda

¹ NATO. Brussels Summit Communiqué. – Brussels: NATO Publications, 2021. – P. 7–12. – URL: https://www.nato.int/cps/en/natohq/news_185000.htm

qo'llanishi murakkab.

2. A'zo davlatlar o'rtasidagi tafovutlar. Raqamli infrazuzilma darajasi turlicha bo'lgani uchun hamma davlatlar teng darajada himoyalangan emas.

3. Xususiy sektor roli. NATOning muvaffaqiyati ko'p jihatdan Microsoft, Google, Cisco kabi kompaniyalar bilan hamkorlikka bog'liq, bu esa siyosiy mustaqillikka ta'sir qilishi mumkin.

NATOning kiberxavfsizlik strategiyasi quyidagi xususiyatlarga ega:

- kiberhujumlarni harbiy hujum bilan tenglashtiradi;
- kibermakonni alohida operatsion domen sifatida tan oladi;
- tezkor javob berish kuchlarini va trening markazlarini yaratgan;
- davlat-xususiy sheriklikni rivojlantiradi;
- xalqaro hamkorlikni kengaytiradi.

Shu bois, NATO tajribasi kibermakon xavfsizligi bo'yicha global siyosatda yetakchi model hisoblanadi. O'zbekiston va boshqa Markaziy Osiyo davlatlari uchun NATOning amaliy mexanizmlari, xususan ta'lim, trening va hamkorlik dasturlari foydali bo'lishi mumkin.

Shanxay Hamkorlik Tashkiloti (SHHT) XXI asrda nafaqat siyosiy-iqtisodiy, balki axborot va kiberxavfsizlik sohalarida ham muhim xalqaro maydonga aylandi. 2001-yilda tashkil topgan SHHT dastlab mintaqaviy xavfsizlik, terrorizm va separatizmga qarshi kurash masalalariga e'tibor qaratgan bo'lsa, keyinchalik u kibermakon xavfsizligini ham o'z kun tartibiga kiritdi. Buning sababi aniq: SHHTga a'zo davlatlarning barchasi raqamli transformatsiya jarayonini boshdan kechirmoqda va bu jarayon kiberjinoyatlar, axborot tahdidlari va kiberterrorizm xavfini kuchaytirmoqda.

SHHT hujjatlarida kiberxavfsizlik quyidagilardan iborat:

1. 2009-yilgi Moskva bitimi. "Axborot xavfsizligi sohasida hamkorlik to'g'risida"gi hujjat qabul qilinib, unda a'zo davlatlar kiberjinoyatchilikka qarshi qo'shma mexanizmlar ishlab

chiqishi belgilandi.

2. 2017-yilgi Ostona sammiti. SHHT deklaratsiyasida «axborot xavfsizligini ta'minlash mintaqaviy barqarorlikning ajralmas qismidir» deb qayd etildi.

3. 2018-yilgi Qingdao deklaratsiyasi. SHHT kiberterrorizmga qarshi kurashni ustuvor yo'nalishlardan biri sifatida e'lon qildi.

4. 2021-yil Dushanbe sammiti. Sun'iy intellekt, katta ma'lumotlar va kiberxavfsizlikni integratsiyalashgan holda rivojlantirish haqida kelishuvga erishildi.

Bu hujjatlar SHHTning kiberxavfsizlik masalalariga tobora ko'proq e'tibor qaratayotganini ko'rsatadi.

SHHTning kiberxavfsizlik bo'yicha amaliy mexanizmlari

1. Mintaqaviy aksilterror tuzilmasi (RATS). – Toshkentda joylashgan bu markaz SHHTning eng muhim institutlaridan biri bo'lib, kiberterrorizm va axborot hujumlariga qarshi ham faoliyat yuritadi. – RATS doirasida ma'lumot almashish, qo'shma mashg'ulotlar va kiberjinoyatchilar haqida yagona bazalar shakllantirilmoqda.

2. Qo'shma mashg'ulotlar: "Xitoy–Rossiya–Markaziy Osiyo" formatida o'tkaziladigan mashg'ulotlarda kiberhujumlarga qarshi himoya va javob berish usullari sinovdan o'tkaziladi. – 2019-yildan beri SHHT doirasida muntazam "Cyber Shield" mashg'ulotlari o'tkazib kelinmoqda.

3. Ilmiy-tadqiqot hamkorligi. SHHT universitetlari tarmog'i doirasida kiberxavfsizlik yo'nalishida ilmiy izlanishlar olib borilmoqda. – Toshkent, Moskva va Pekin universitetlari bu sohada qo'shma loyihalarda qatnashmoqda.

O'zbekiston SHHTga asoschilaridan biri sifatida tashkilotning kiberxavfsizlik tashabbuslarida faol qatnashmoqda. Toshkentda joylashgan RATS markazi bu boradagi ishtirokni yanada kuchaytiradi. O'zbekiston quyidagi yo'nalishlarda faol:

- RATS orqali mintaqaviy ma'lumot almashish tizimiga hissa qo'shmoqda.

- SHHT doirasida qabul qilingan barcha axborot xavfsizligi hujjatlarini qo'llab-quvvatlagan.

- “Raqamli O‘zbekiston – 2030” dasturida SHHT bilan hamkorlik alohida ustuvor yo‘nalish sifatida belgilangan¹.

SHHTning kiberxavfsizlik bo‘yicha faoliyati quyidagi natijalarni berdi:

- mintaqaviy darajada hamkorlik mexanizmlari shakllandi;
- RATS markazi samarali faoliyat yuritmoqda;
- qo‘shma mashg‘ulotlar orqali amaliy hamkorlik rivojlanmoqda;
- ilmiy-tadqiqot hamkorligi kengaymoqda.

Shu bilan birga, yagona huquqiy baza yo‘qligi, texnologik nomutanosiblik va xalqaro standartlarga integratsiya sustligi SHHTning asosiy muammolaridan bo‘lib qolmoqda.

O‘zbekiston uchun esa SHHT mintaqaviy xavfsizlik siyosatining ajralmas qismi sifatida nafaqat milliy, balki global kiberxavfsizlik tizimida ham ishtirokini kuchaytirishga xizmat qilmoqda.

Kibermakon xavfsizligi bugungi global siyosatda davlatlarning milliy manfaatlarini himoya qilish bilan birga, xalqaro hamkorlikni ham talab etadigan murakkab jarayon hisoblanadi. NATO va SHHT kabi yirik harbiy-siyosiy bloklardan tashqari, boshqa ko‘plab xalqaro tashkilotlar ham bu borada faoliyat yuritmoqda. Ulardan eng muhimlari — Yevropada xavfsizlik va hamkorlik tashkiloti (OSCE), Xalqaro telekommunikatsiya ittifoqi (ITU) va Mustaqil Davlatlar Hamdo‘stligi (MDH) hisoblanadi. Ularning har biri kibermakon xavfsizligini ta‘minlashda o‘ziga xos rol o‘ynaydi.

OSCE (Organization for Security and Co-operation in Europe) dunyodagi eng yirik mintaqaviy xavfsizlik tashkiloti bo‘lib, 57 ta davlatni qamrab oladi. Kibermakon masalalari OSCE kun tartibiga 2010-yillardan boshlab kiritildi.

1. Ishonchni mustahkamlash choralari (CBMs). 2013-yilda OSCE kibermakonda ishonchni mustahkamlash bo‘yicha

¹ 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>

birinchi choralar paketini qabul qildi. Bu choralar davlatlar o'rtasida axborot almashish, milliy siyosatni ochiq e'lon qilish va favqulodda vaziyatlarda tezkor muloqotni ta'minlashni o'z ichiga oladi¹.

2. Huquqiy asoslar. OSCE xalqaro huquqning amaldagi normalari kibermakon uchun ham tatbiq etilishi zarurligini ta'kidlaydi. Ayniqsa, inson huquqlari, axborot erkinligi va shaxsiy hayot daxlsizligi OSCEning ustuvor tamoyillaridan biridir.

3. Amaliy mexanizmlar. OSCE davlatlar o'rtasida muntazam seminarlar va treninglar tashkil etadi. O'zbekiston ham OSCE doirasidagi kibermakon bo'yicha treninglarda qatnashib kelmoqda.

Xalqaro telekommunikatsiya ittifoqi (ITU) BMTning maxsus agentligi bo'lib, global miqyosda axborot-kommunikatsiya texnologiyalari sohasini muvofiqlashtiradi. ITUning kiberxavfsizlik bo'yicha faoliyati quyidagilardan iborat:

1. Global Cybersecurity Index (GCI). Har ikki yilda e'lon qilinadigan bu indeks davlatlarning milliy kiberxavfsizlik salohiyatini baholaydi. O'zbekiston 2020-yilda 86-o'rinda bo'lgan bo'lsa, 2022-yilda 64-o'ringa ko'tarildi².

2. Technical Assistance. ITU rivojlanayotgan davlatlarga texnik yordam va maslahatlar beradi. O'zbekiston ham ITU orqali milliy strategiyalarini xalqaro standartlarga moslashtirish imkoniyatiga ega.

3. Global hamkorlik platformalari. ITU "Global Cyberdrill" mashg'ulotlarini o'tkazadi. Unda yuzlab davlatlar ishtirok etib, kiberhujumlarga qarshi tezkor javob berishni mashq qiladi.

Mustaqil Davlatlar Hamdo'stligi (MDH) ham mintaqaviy darajada kiberxavfsizlik masalalariga e'tibor qaratmoqda.

1. 2013-yilgi Konsepsiya. MDH davlatlari "Axborot xavf-

¹ OSCE. Confidence-Building Measures in Cyberspace. – Vienna: OSCE Publications, 2016. – P. 11–17.

² International Telecommunication Union (ITU). Global Cybersecurity Index 2022. – Geneva: ITU Publications, 2022. – P. 84–90.

sizligi sohasida hamkorlik konsepsiyasi”ni qabul qildi¹. Unda umumiy xavflarga qarshi birgalikda kurashish, ma'lumot almashish va qo'shma dasturlar ishlab chiqish belgilangan.

2. Qo'shma mashg'ulotlar. MDH davlatlari muntazam ravishda “Cyber Commonwealth” mashg'ulotlarini o'tkazib kelmoqda. Bu mashg'ulotlar kiberjinoyatlarga qarshi amaliy hamkorlikni kuchaytiradi.

3. Huquqiy moslashuv. MDH doirasida qabul qilingan hujjatlar ko'plab a'zo davlatlarning milliy qonunchiligiga moslashtirilgan. O'zbekiston ham mazkur konsepsiyani qo'llab-quvvatlab, uni milliy qonunchilikka integratsiya qilmoqda.

OSCE, ITU va MDH kibermakon xavfsizligini ta'minlashda quyidagi rolni bajaradi:

- OSCE – ishonchni mustahkamlash, inson huquqlarini kafolatlash;
- ITU – texnik standartlar, global baholash va texnik yordam;
- MDH – mintaqaviy hamkorlik va qo'shma mashg'ulotlar.

Bu tashkilotlarning tajribasi bir-birini to'ldiradi. O'zbekiston uchun ularning barchasi muhim: OSCE – inson huquqlari kontekstida, ITU – xalqaro reytinglar va texnik yordam nuqtai nazaridan, MDH esa mintaqaviy hamkorlik jihatidan ahamiyatli.

Yuqoridagilardan kelib chiqib O'zbekiston va global kibermakon xavfsizligi uchun qanday falsafiy-huquqiy ahamiyat kasb etishini ko'rib chiqamiz:

BMT tashabbuslari kibermakon xavfsizligi bo'yicha xalqaro huquqiy maydonni shakllantirdi. Bosh Assambleya rezolyutsiyalari davlatlarning suverenitetini hurmat qilish va shu bilan birga inson huquqlarini kafolatlash zarurligini belgilab berdi. GGE va OEWG mexanizmlari orqali xalqaro huquq kibermakonga tatbiq etildi; BMTning o'ziga xosligi shundaki, u global darajadagi tamoyillarni ishlab chiqadi. Bu tamoyillar har bir davlatning milliy qonunchiligiga integratsiya qilinishi lozim.

¹ СНГ (MDH). Концепция сотрудничества государств-участников в области информационной безопасности. – Минск: Исполнительный комитет СНГ, 2013. – Р. 2–10.

O'zbekiston ham BMT rezolyutsiyalarini qo'llab-quvvatlab, ularni milliy strategiyalarda hisobga olmoqda.

NATO kiberxavfsizlikni harbiy mudofaaning ajralmas qis-miga aylantirdi. Kibermakon alohida operatsion domen sifatida tan olindi va kiberhujumlar 5-modda (kollektiv mudofaa) doirasiga kiritildi. NATOning CCDCOE markazi va Locked Shields mashg'ulotlari global miqyosda eng ilg'or tajribani yaratmoqda. Bu modelning falsafiy mohiyati shundaki, NATO a'zolari suverenitetlarini kollektiv mudofaa foydasiga bo'lishadi. Bu esa xalqaro hamkorlikning yuqori darajasini anglatadi. O'zbekiston NATO a'zosi bo'lmasa-da, uning trening va hamkorlik dasturlari biz uchun ham foydali bo'lishi mumkin;

SHHT kiberxavfsizlikni mintaqaviy barqarorlikning ajralmas qismi sifatida ko'radi. Toshkentda joylashgan RATS markazi SHHTning asosiy amaliy instituti hisoblanadi. SHHT davlatlari o'rtasida qo'shma mashg'ulotlar, hujjatlar va ilmiy hamkorlik orqali birdamlik mustahkamlanmoqda. Bu modelning falsafiy ahamiyati – umumiy tarixiy va hududiy manfaatlarga asoslangan birdamlikdir. Shu bois SHHT tajribasi O'zbekiston uchun nafaqat amaliy, balki strategik jihatdan ham muhim;

OSCE kibermakon xavfsizligida davlatlar o'rtasida ishonchni mustahkamlash choralarini (CBMs) ishlab chiqdi. Bu mexanizmlar axborot almashish, siyosiy ochiqlik va tezkor muloqotni ta'minlashga qaratilgan. Falsafiy jihatdan OSCE modeli inson huquqlari va ishonchni ustuvor qo'yadi. Bu yondashuv erkinlik va xavfsizlik o'rtasidagi muvozanatni global miqyosda topishga xizmat qiladi. O'zbekiston ham OSCE treninglarida qatnashib, bu tajribadan foyda ko'rmoqda;

ITU davlatlarning milliy salohiyatini Global Cybersecurity Index (GCI) orqali baholaydi. Shuningdek, u texnik yordam ko'r-satadi va global mashg'ulotlarni tashkil etadi. ITUning afzalligi shundaki, u siyosiy emas, balki texnik hamkorlik platfor-masidir. O'zbekiston uchun ITUning GCI reytingida yuqorilash — xalqaro maydonda obro'ni oshirish va milliy strategiyaning samaradorligini ko'rsatish vositasidir;

MDH doirasida "Axborot xavfsizligi konsepsiyasi" qabul

qilingan. U umumiy xavflarga qarshi birgalikda kurashish va ma'lumot almashishga asoslangan. Qo'shma mashg'ulotlar va huquqiy moslashuv mexanizmlari mintaqaviy birdamlikni mustahkamlaydi. MDH modelining falsafiy mohiyati – umumiy tarix va til asosidagi integratsiyadir. O'zbekiston uchun MDH tajribasi milliy qonunchilikni qo'shni davlatlar bilan uyg'unlashtirishda muhim.

Xalqaro tashkilotlarning kiberxavfsizlik sohasidagi tajribasi bir-birini to'ldiradi va global xavfsizlik tizimini mustahkamlashga xizmat qiladi. O'zbekiston uchun bu tajribalar milliy strategiyani takomillashtirish, xalqaro maydonda ishonchni oshirish va mintaqaviy barqarorlikni mustahkamlashda beqiyos ahamiyatga ega.

4.2. Kiberxavfsizlikda axborot etikasi va inson huquqlarini himoya qilish

Axborot texnologiyalari insoniyat hayotining barcha jabhalariga chuqur kirib borgan hozirgi davrda "axborot etikasi" tushunchasi tobora muhim ahamiyat kasb etmoqda. Chunki kibermakon — bu nafaqat texnik infratuzilma va dasturiy ta'minotlar majmui, balki insonlarning ongli xatti-harakatlari, qadriyatlari va madaniy munosabatlari namoyon bo'ladigan ijtimoiy maydondir. Agar kibermakonda huquqiy me'yorlar davlat tomonidan belgilansa, axborot etikasi insonlarning axloqiy tanlovi va mas'uliyatini belgilaydi.

Shu sababli, axborot etikasi kibermakon xavfsizligini ta'minlashda nafaqat qo'shimcha, balki asosiy omillardan biri sifatida qaralishi lozim. Global miqyosda BMT, UNESCO, OSCE kabi tashkilotlar bu masalani ko'tarib chiqib, umumiy tamoyillarni ishlab chiqmoqda.

"Axborot etikasi" atamasi ilmiy adabiyotlarda turli talqin qilinadi. Ba'zi olimlar uni "axborotning yaratilishi, tarqatilishi va iste'mol qilinishida axloqiy me'yorlar tizimi" deb ta'riflaydi. UNESCOning 2019-yilgi hisobotida esa quyidagicha

ta'kidlanadi: «Information ethics is concerned with the moral dimensions of the creation, dissemination, and use of information in all forms»¹.

Shunday qilib, axborot etikasi quyidagi uch elementni qamrab oladi:

1. Axborot yaratish etikasi — haqiqat, haqqoniylik va ilmiylik tamoyillariga asoslanadi.

2. Axborot tarqatish etikasi — adolat, shaffoflik, senzura va manipulyatsiyadan voz kechishni talab qiladi.

3. Axborot iste'moli etikasi — foydalanuvchilarning mas'uliyati, shaxsiy ma'lumotlardan to'g'ri foydalanish va zararli kontentdan saqlanishni anglatadi.

Axborot etikasining global tamoyillari sifatida quyidagilarni sanab o'tishimiz mumkin:

1. Haqqoniylik (Truthfulness). Yolg'on ma'lumot tarqatish, dezinformatsiya va manipulyatsiya axborot etikasi tamoyillariga zid. Bu global muammo, chunki "feyk yangiliklar" kiberjinoyatlarning asosiy vositasiga aylangan.

2. Shaffoflik (Transparency). Axborot tarqatishda manba va metodlarning ochiqligi. Masalan, Yevropa Ittifoqi GDPR qonuni shaxsiy ma'lumotlarni yig'ishda shaffoflikni talab qiladi.

3. Mas'uliyat (Responsibility). Axborot yaratgan va tarqatgan shaxs yoki tashkilot uning oqibatlari uchun javobgar bo'lishi kerak. UNESCO deklaratsiyasida: «Each information actor must bear responsibility for the impact of their actions on society»².

4. Adolat (Justice). Axborot texnologiyalaridan foydalanishda teng imkoniyat yaratish. "Digital divide" (raqamli tafovut) axborot etikasi tamoyillariga zid.

5. Shaxsiy hayot daxlsizligi (Privacy). Shaxsiy ma'lumotlar himoyasi axborot etikasi va inson huquqlarining markaziy tamoyili hisoblanadi.

¹ UNESCO. Information Ethics Report. – Paris: UNESCO Publishing, 2019. – P. 8–12.

² UNESCO. *Universal Declaration on Information Ethics*. – Paris: UNESCO, 2015. – P. 4–9.

6. Madaniy xilma-xillikka hurmat (Respect for cultural diversity). Har bir davlatning milliy qadriyatlari va madaniyati kibermakonda inobatga olinishi zarur.

Axborot etikasi falsafiy nuqtai nazardan “axborot erkinligi va mas’uliyati” o’rtasidagi dialektikani ifodalaydi. Erkinlik — inson huquqi, ammo mas’uliyat — ijtimoiy barqarorlikning kafolati. Huquqiy nuqtai nazardan esa, axborot etikasi maxsus qonunlar bilan mustahkamlanishi zarur. Masalan, O’zbekistonda “Shaxsiy ma’lumotlar to’g’risida”gi qonun¹ axborot etikasi tamoyillarini huquqiy shaklga keltiradi.

O’zbekiston axborot etikasi masalalarini ta’lim va huquqiy siyosatda bosqichma-bosqich rivojlantirmoqda:

- “Axborot xavfsizligi to’g’risida”gi Qonunda axloqiy me’yorlarga asoslangan xavfsiz foydalanish talablari belgilangan².

- Oliy ta’lim muassasalarida “Axborot madaniyati” va “Axborot xavfsizligi asoslari” fanlari o’qitilmoqda.

- Internetda yolg’on xabarlar va zararli kontentga qarshi kurashish bo’yicha targ’ibot ishlari kuchaytirilmoqda.

Axborot etikasi kibermakon xavfsizligining falsafiy-huquqiy asosini tashkil etadi. U quyidagi xulosalarni beradi:

- Axborot yaratish, tarqatish va iste’mol qilishda axloqiy mas’uliyat muhim;

- Global tamoyillar — haqqoniylik, shaffoflik, mas’uliyat, adolat, shaxsiy hayot daxlsizligi va madaniy xilma-xillikka hurmat;

- Axborot etikasi huquqiy mexanizmlar bilan uyg’unlashganda samarali ishlaydi;

- O’zbekiston tajribasi ham bu tamoyillarga bosqichma-bosqich integratsiyalashmoqda.

Demak, axborot etikasi nafaqat texnik, balki ijtimoiy va falsafiy jihatdan ham kibermakon xavfsizligining poydevoridir.

¹ O’zbekiston Respublikasi Qonuni. “Shaxsiy ma’lumotlar to’g’risida”. – Toshkent: LexUZ, 2019. – URL: <https://lex.uz/docs/4396428>

² O’zbekiston Respublikasi Qonuni. “Axborot xavfsizligi to’g’risida”. – Toshkent: LexUZ, 2022. – URL: <https://lex.uz/docs/6003766>

Kibermakon xavfsizligini ta'minlash masalasi har doim insonning asosiy huquqlari bilan, xususan, shaxsiy hayot daxlsizligi bilan chambarchas bog'liqdir. Raqamli texnologiyalar tobora chuqur hayotimizga kirib borgani sari shaxsiy ma'lumotlar, xatti-harakatlar va kommunikatsiyalar to'g'risidagi axborot global iqtisodiyotning eng qimmatli resursiga aylanmoqda. Shu sababli, kiberxavfsizlik siyosatida ikki tamoyil o'zaro muvozanatda bo'lishi zarur: milliy xavfsizlikni ta'minlash va shaxsiy hayotni himoya qilish.

Agar davlat xavfsizlikni ustuvor qo'yib, fuqarolarning shaxsiy hayotiga haddan tashqari aralashsa, bu inson huquqlarining buzilishiga olib keladi. Aksincha, agar shaxsiy hayot daxlsizligi to'liq ustuvorlik qilsa, milliy xavfsizlik zaiflashishi mumkin. Shu sababli, kiberxavfsizlik va shaxsiy hayot daxlsizligi o'rtasida falsafiy, huquqiy va ijtimoiy muvozanat zarur.

Shaxsiy hayot daxlsizligi xalqaro huquqda asosiy inson huquqlaridan biri sifatida mustahkamlangan. BMTning Inson huquqlari umumjahon deklaratsiyasida: «Hech kimning shaxsiy hayoti, oilasi, uyi yoki yozishmalariga o'zboshimchalik bilan aralashishga yo'l qo'yilmasligi kerak»¹.

Kibermakon kontekstida bu tushuncha quyidagilarni qamrab oladi:

1. Shaxsiy ma'lumotlar himoyasi (ism, telefon raqami, biometrik ma'lumotlar).
2. Kommunikatsiya daxlsizligi (telefon qo'ng'iroqlari, elektron pochta, ijtimoiy tarmoq yozishmalari).
3. Raqamli xatti-harakatlar himoyasi (onlayn xaridlar, qidiruv tarixlari, geolokatsiya ma'lumotlari).

Kiberxavfsizlik va shaxsiy hayot daxlsizligi bo'yicha global yondashuvlar

1. Yevropa Ittifoqi – GDPR. 2018-yilda kuchga kirgan General Data Protection Regulation (GDPR) dunyodagi eng qat'iy shaxsiy ma'lumotlarni himoya qilish qonuni hisoblanadi. Unda quyidagilar belgilangan:

¹ United Nations. Universal Declaration of Human Rights. – New York: UN, 1948. – Article 12.

o fuqarolarning ma'lumotlari ularning roziligisiz qayta ishlanmasligi;

o "unutish huquqi" (right to be forgotten);

o ma'lumotlar faqat belgilangan maqsadda saqlanishi va ishlatilishi¹.

2. AQSh yondashuvi. AQShda yagona federal qonun yo'q, ammo sohalar bo'yicha maxsus qonunlar mavjud (masalan, HIPAA – tibbiy ma'lumotlar, COPPA – bolalar onlayn himoyasi). Bu yondashuv ko'proq sektorli va pragmatik xususiyatga ega.

3. BMT tashabbuslari. 2013-yilda BMT Bosh Assambleyasi "The Right to Privacy in the Digital Age" rezolyutsiyasini qabul qildi. Unda davlatlar shaxsiy hayotni himoya qilishda xalqaro majburiyatlarga amal qilishi ta'kidlangan².

O'zbekiston Konstitutsiyasining 27-moddasida: «Har kimning shaxsiy hayoti, yozishmalari, telefon orqali so'zlashuvlari, pochta, telegraf va boshqa xabarlar sir tutilishi kafolatlanadi».

Bundan tashqari:

- "Shaxsiy ma'lumotlar to'g'risida"gi Qonun (2019) – shaxsiy ma'lumotlarni yig'ish, saqlash va qayta ishlash tartibini belgilaydi³.

- "Axborot xavfsizligi to'g'risida"gi Qonun (2022) – shaxsiy hayotni himoya qilishni kiberxavfsizlikning ustuvor yo'nalishlaridan biri sifatida qayd etadi⁴.

- Prezidentning "Raqamli O'zbekiston – 2030" dasturi (2020) shaxsiy ma'lumotlarni himoya qilishni milliy siyosat darajasiga ko'tardi.

Shaxsiy hayot daxlsizligi kiberxavfsizlikning asosiy falsafiy va huquqiy tayanchi hisoblanadi. Agar kiberxavfsizlik tizimi inson huquqlarini hisobga olmasa, u barqaror bo'la olmaydi.

¹ European Union. General Data Protection Regulation (GDPR). – Brussels: EU, 2016. – URL: <https://gdpr-info.eu>

² United Nations General Assembly. The Right to Privacy in the Digital Age. – New York: UN, 2013. – A/RES/68/167.

³ O'zbekiston Respublikasi Qonuni. "Shaxsiy ma'lumotlar to'g'risida". – Toshkent: LexUZ, 2019. – URL: <https://lex.uz/docs/4396428>

⁴ O'zbekiston Respublikasi Qonuni. "Axborot xavfsizligi to'g'risida". – Toshkent: LexUZ, 2022. – URL: <https://lex.uz/docs/6003766>

Aksincha, shaxsiy hayotni himoya qilmagan tizim milliy xavfsizlikni ham zaiflashtiradi.

O'zbekiston tajribasi shuni ko'rsatmoqdaki, huquqiy bazaning mavjudligi bilan birga, uni amaliyotda qo'llash va xalqaro tajriba bilan uyg'unlashtirish dolzarb masaladir. Shu bois, kelajakda shaxsiy hayotni himoya qilish masalasi O'zbekistonning kiberxavfsizlik siyosatida strategik yo'nalish sifatida qolishi lozim.

Kibermakon xavfsizligi va axborot etikasi masalalarini o'rganish faqat texnik yoki yuridik yondashuvlar bilan cheklanib qolmaydi. Bu jarayon aslida falsafiy-huquqiy mohiyatga ega, chunki unda inson erkinligi, jamiyat barqarorligi, davlat suvereniteti va global qadriyatlar o'zaro bog'liq. Falsafa bu masalani "erkinlik va mas'uliyat dialektikasi" orqali tushuntirsa, huquqiy fan "konstitutsiyaviy kafolatlar va xalqaro normalar uyg'unligi"ni ko'rsatadi. Shu sababli, kiberxavfsizlik siyosati va axborot etikasi falsafiy-huquqiy umumlashmalar asosida barqaror modelga aylanishi mumkin.

Falsafada erkinlik — insonning tabiiy huquqi, xavfsizlik esa ijtimoiy zarurat sifatida talqin qilinadi. Kibermakonda bu ikki tushuncha o'zaro qarama-qarshi, lekin bir-birini to'ldiruvchi hodisadir.

- Erkinliksiz xavfsizlik – bu avtoritar nazorat, senzura va axborot oqimining cheklanishi.
- Xavfsizliksiz erkinlik – bu kiberjinoyatlar, dezinformatsiya va terrorizm xavfining kuchayishi.

Demak, kibermakon siyosati erkinlik va xavfsizlikning muvozanatli uyg'unligini ta'minlashi kerak. O'zbekiston Konstitutsiyasida (29-modda) so'z erkinligi kafolatlangan, biroq bu huquq milliy xavfsizlik va ijtimoiy tartibni saqlash sharti bilan chegaralanadi¹.

Huquqiy nuqtai nazardan, inson huquqlari va davlat suvereniteti o'rtasidagi muvozanat dolzarb. BMTning "The Right to Privacy in the Digital Age" rezolyutsiyasida davlatlar milliy

¹ United Nations General Assembly. The Right to Privacy in the Digital Age. – New York: UN, 2013. – A/RES/68/167.

xavfsizlikni ta'minlashda inson huquqlarini cheklamasligi kerakligi qayd etilgan.

Falsafiy talqinda bu muammo “shaxs va davlat” dialektikasi sifatida qaraladi. Shaxs o'z erkinligini himoya qiladi, davlat esa umumiy xavfsizlikni. Kiberxavfsizlik siyosati shu ikki manfaatni uyg'unlashtiruvchi mexanizmlarga tayanishi lozim.

Axborot etikasi texnologiyalarni axloqiy mezonlarga moslashni talab qiladi. Sun'iy intellekt, biometrik kuzatuv tizimlari, “big data” texnologiyalari xavfsizlikni kuchaytirishi mumkin, ammo ular inson huquqlarini buzishi ehtimoli ham mavjud.

UNESCOning 2019-yilgi hisobotida shunday deyilgan: «Emerging technologies must be governed by ethical principles that protect human dignity and rights»¹.

Bu yondashuvning falsafiy mohiyati shundaki, texnologiyalarni inson uchun vosita sifatida talqin qilish zarur, ularning maqsadga aylanishiga yo'l qo'yilmasligi kerak.

Huquqiy tizimlarda global tamoyillar (masalan, BMT rezolyutsiyalari, Yevropa Ittifoqi GDPR) va milliy qonunlar o'zaro uyg'unlashishi kerak. Aks holda, “raqamli kolonializm” xavfi tug'iladi, ya'ni kuchli davlatlar o'z standartlarini boshqalarga majburan joriy etadi.

Falsafiy tahlilda bu muammo “universallik va partikulyarlik” qarama-qarshiligini eslatadi. Universallik — umumiy insoniyat qadriyatlarini, partikulyarlik — milliy qadriyatlar. O'zbekiston tajribasida bu ikki tamoyilni uyg'unlashtirishga intilish kuzatilmoqda: milliy qonunlar qabul qilinmoqda, ammo ular xalqaro me'yorlar bilan muvofiqlashtirilmoqda.

Falsafiy-huquqiy tahlil shuni ko'rsatadiki, kibermakon xavfsizligi va axborot etikasi masalalarida quyidagi dialektik tamoyillar hal qiluvchi ahamiyatga ega:

- Erkinlik ↔ Xavfsizlik
- Inson huquqlari ↔ Davlat suvereniteti
- Texnologiya ↔ Axloq
- Global qadriyatlar ↔ Milliy qadriyatlar

¹ UNESCO. Information Ethics Report. – Paris: UNESCO Publishing, 2019. – P. 8–12.

Bu dialektik uyg'unlikni topmagan jamiyatda kiberxavfsizlik siyosati barqaror bo'la olmaydi. Shu bois, O'zbekistonning milliy strategiyasi ham xalqaro huquqiy tamoyillar bilan uyg'unlashgan holda, falsafiy-huquqiy asoslarni chuqur hisobga olishi zarur.

Yuqoridagilardan xulosa qilib kibermakonda axborot etikasi va inson huquqlarini himoya qilish masalalarini quyidagicha talqin qilamiz:

- axloqiy tamoyillar (haqqoniylik, shaffoflik, mas'uliyat, adolat, shaxsiy hayot daxlsizligi)ni;
- huquqiy kafolatlar (konstitutsiya, maxsus qonunlar, xalqaro rezolyutsiyalar)ni;
- falsafiy dialektikalar (erkinlik ↔ xavfsizlik, huquqlar ↔ suverenitet, texnologiya ↔ axloq, global ↔ milliy qadriyatlar)ni;
- amaliy mexanizmlar (GDPR, BMT rezolyutsiyalari, milliy dasturlar)ni o'z ichiga oladi.

O'zbekiston va jahon tajribasi shuni ko'rsatadiki, kiberxavfsizlik siyosati inson huquqlari va axborot etikasi tamoyillariga tayangandagina barqaror bo'lishi mumkin. Bu — zamonaviy kibermakonning nafaqat huquqiy, balki falsafiy asosidir.

4.3. Kiberxavfsizlikning kelajak paradigmalari va global boshqaruv muammolari

XXI asrda kibermakon davlatlar suverenitetining yangi o'lchoviga aylandi. Agar avvallari suverenitet hudud, havo va suv hududi bilan belgilanar edi, hozirgi davrda raqamli suverenitet tushunchasi oldingi o'ringa chiqmoqda. Raqamli suverenitet — bu davlatning o'z hududidagi raqamli infratuzilma, axborot oqimlari va shaxsiy ma'lumotlar ustidan nazorat qilish huquqi. Biroq bu nazorat global boshqaruv mexanizmlari bilan to'qnash kelmoqda. Internet va kibertexnologiyalar tabiatan transmilliy bo'lgani uchun ular ustidan faqat milliy darajadagi nazorat yetarli emas. Shu bois, raqamli suverenitet va global boshqaruv

o'rtasida ziddiyatlar paydo bo'lmoqda.

“Raqamli suverenitet” atamasi dastlab Yevropa Ittifoqi siyosiy hujjatlarida qo'llanila boshladi. Masalan, Fransiya prezidenti Emmanuel Makron 2018-yilgi nutqida shunday degan edi: «Without digital sovereignty, there is no political sovereignty»¹.

Bu tushunchaning asosiy elementlari quyidagilar:

1. Infratuzilma nazorati – davlat o'z hududidagi internet tarmoqlari va data-markazlar ustidan to'liq boshqaruvga ega bo'lishi.

2. Ma'lumotlar ustidan nazorat – fuqarolarning shaxsiy ma'lumotlari xorijiy serverlarda emas, milliy serverlarda saqlanishi.

3. Texnologik mustaqillik – mahalliy dasturiy ta'minot va apparat vositalarini rivojlantirish.

4. Huquqiy suverenitet – milliy qonunlarning kiber-makonda ustuvor bo'lishi.

Hozirgi kunda internet va kibermakonni boshqarish bir qator xalqaro tashkilotlar qo'lida:

1. ICANN (Internet Corporation for Assigned Names and Numbers). Domen nomlari va IP-manzillarni boshqaradi. AQSh huquqiy hududida joylashgani sababli, ko'plab davlatlarda “internetning bir davlat qo'lida jamlanganligi” haqidagi xavotir mavjud.

2. ITU (Xalqaro telekommunikatsiya ittifoqi). Global telekommunikatsiya standartlarini belgilaydi. BMT tizimiga kirgani sababli nisbatan neytral tuzilma hisoblanadi.

3. WTO (Jahon savdo tashkiloti). Elektron savdo va raqamli xizmatlarni tartibga soladi.

4. Big Tech kompaniyalari. Google, Meta, Amazon, Microsoft kabi gigantlar amalda milliy davlatlardan kuchliroq ta'sirga ega bo'lib, ular “nodavlat global boshqaruv aktorlari”ga aylangan.

Raqamli suverenitet va global boshqaruv o'rtasidagi ziddiyat

¹ Macron, E. Speech on Digital Sovereignty. – Paris: Élysée Palace, 2018. – URL: <https://www.elysee.fr>

uch asosiy yo'nalishda ko'rinadi:

1. Milliy qonunlar ↔ Xalqaro normalar. Masalan, Yevropa Ittifoqining GDPR qonuni global kompaniyalardan ham amal qilishni talab qiladi. Bu esa transmilliy korporatsiyalar va ayrim davlatlar o'rtasida huquqiy to'qnashuvlarga sabab bo'lmoqda.

2. Davlat nazorati ↔ Internet erkinligi. Ba'zi davlatlar (Xitoy, Rossiya) internet ustidan qat'iy nazorat o'rnatmoqda. BMT va OSCE esa internet erkinligini inson huquqlarining ajralmas qismi sifatida talqin qiladi.

3. Mahalliy texnologiyalar ↔ Global bozor. Milliy dasturlarni rivojlantirish harakati global IT kompaniyalarning monopoliyasiga qarshi turadi. Shu bilan birga, bu jarayon iqtisodiy raqobatni kuchaytiradi.

Bu ziddiyatlar falsafiy-huquqiy nuqtai nazardan quyidagicha talqin qilinadi:

1. Suverenitetning yangi paradigmasi. Klassik suverenitet hududiy chegaralarga asoslangan bo'lsa, raqamli suverenitet ma'lumotlar oqimi va texnologik mustaqillik bilan belgilanadi.

2. Globalizm va milliylik dialektikasi. Kibermakon tabiatan global, ammo davlatlar milliy nazoratni talab qilmoqda. Bu "universallik va partikulyarlik" qarama-qarshiligini eslatadi.

3. Texnologiya va siyosat uyg'unligi. Texnologiya endilikda siyosiy hokimiyat vositasiga aylangan. Shu sababli, texnologik mustaqillik siyosiy mustaqillikning kafolatiga aylandi.

O'zbekiston raqamli suverenitet masalasini milliy siyosat darajasiga ko'targan:

- "Raqamli O'zbekiston – 2030" dasturida milliy data-markazlar yaratish vazifasi qo'yilgan¹.
- "Shaxsiy ma'lumotlar to'g'risida"gi Qonunga ko'ra, fuqarolarning ma'lumotlari O'zbekiston hududidagi serverlarda saqlanishi shart².

¹ 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>

² O'zbekiston Respublikasi Qonuni. "Shaxsiy ma'lumotlar to'g'risida". – Toshkent: LexUZ, 2019. – URL: <https://lex.uz/docs/4396428>

- O'zbekiston ITU va boshqa global tashkilotlarda faol ishtirok etib, milliy manfaatlarini himoya qilmoqda.

Shu bilan birga, O'zbekiston uchun muammolar ham mavjud: texnologik importga yuqori darajadagi qaramlik, global kompaniyalarga bog'liqlik, xalqaro standartlarga moslashish ehtiyoji.

Raqamli suverenitet va global boshqaruv o'rtasidagi ziddiyat kelajakdagi kiberxavfsizlik siyosatining markaziy masalasi bo'lib qoladi. Asosiy xulosalar:

- Suverenitet endi faqat hududiy emas, balki raqamli o'lchovga ham ega.

- Global boshqaruv mexanizmlari (ICANN, ITU, Big Tech) davlatlarning milliy siyosatiga ta'sir ko'rsatmoqda.

- Ziddiyat falsafiy jihatdan "globalizm ↔ milliylik" dialektikasida, huquqiy jihatdan esa "xalqaro normalar ↔ milliy qonunlar" to'qnashuvida ifodalanmoqda.

- O'zbekiston uchun bu jarayon milliy data-markazlar, shaxsiy ma'lumotlarni himoya qilish va texnologik mustaqillikni rivojlantirish orqali hal qilinishi lozim.

XXI asr kiberxavfsizlik sohasida tub o'zgarishlar davri bo'lib, uning asosiy drayverlari yangi texnologiyalar — sun'iy intellekt (SI), kvant hisoblash va katta ma'lumotlar (Big Data) hisoblanadi. Bu texnologiyalar kibermakon imkoniyatlarini kengaytirishi bilan birga, mutlaqo yangi xavf-xatarlarni ham yuzaga keltirmoqda. Shu sababli, kelajakdagi kiberxavfsizlik siyosati texnologik innovatsiyalarni nazorat qilish va ularni etik-huquqiy asoslarda tartibga solishni talab qiladi.

Sun'iy intellekt bugungi kunda kiberxavfsizlikni ta'minlashning eng kuchli vositalaridan biri sifatida qaralmoqda. U quyidagi yo'nalishlarda qo'llaniladi:

1. Kiberhujumlarni aniqlash va oldini olish. Mashinaviy o'rganish algoritmlari real vaqt rejimida tahdidlarni aniqlay oladi. Masalan, SI asosidagi "intrusion detection systems" an'anaviy tizimlardan ko'ra tezroq ishlaydi.

2. Katta ma'lumotlarni tahlil qilish. SI millionlab log-fayllar va trafik oqimlarini tahlil qilib, yashirin hujum izlarini aniqlaydi.

3. Avtomatlashtirilgan javob berish. SI tizimlari kiber-hujumga javobni inson aralashuvisiz amalga oshira oladi.

Ammo SIning xavfli jihatlari ham mavjud:

- Adversarial attacks – SI tizimlarini aldaydigan maxsus ma'lumotlar yaratish.
- Avtonom qurollar – kibermakonni harbiylashuv xavfi.
- Axloqiy muammolar – qaror qabul qilish jarayonida inson mas'uliyatining pasayishi.

UNESCOning 2021-yilda qabul qilingan “Recommendation on the Ethics of Artificial Intelligence” hujjatida shunday deyilgan: «Artificial Intelligence must remain under human oversight and serve the protection of human rights»¹.

Kvant hisoblash texnologiyalari axborotni qayta ishlash tezligini millionlab barobar oshirishi mumkin. Bu texnologiyaning kiberxavfsizlikka ta'siri ikki tomonlama:

1. Tahdidlar: Kvant kompyuterlari mavjud kriptografik algoritmlarni (RSA, ECC) bir necha daqiqada buzishi mumkin. Bu esa moliya, sog'liqni saqlash va davlat infratuzilmasi uchun jiddiy xavf tug'diradi.

2. Imkoniyatlar: Post-quantum cryptography – yangi matematik algoritmlar asosida yaratilgan shifrlash usullari. Quantum Key Distribution (QKD) – kvant fizikasi qonunlariga asoslangan mutlaq xavfsiz aloqa kanallari.

2019-yilda Xitoy “Micius” sun'iy yo'ldoshi orqali kvant shifrlash texnologiyasini muvaffaqiyatli sinovdan o'tkazdi². Bu texnologiya kelajakdagi kiberxavfsizlik poygasida yangi davrni boshlab berdi.

Big Data texnologiyalari kiberxavfsizlikda “prediktiv” yondashuvni joriy qilmoqda:

- foydalanuvchi xatti-harakatlari tahlil qilinadi;
- statistik modellar asosida potentsial xavf oldindan prognoz qilinadi;

¹ UNESCO. Recommendation on the Ethics of Artificial Intelligence. – Paris: UNESCO Publishing, 2021. – P. 4–12.

² Yin, J. et al. Satellite-based entanglement distribution over 1200 kilometers. – Science, Vol. 356, Issue 6343, 2017. – P. 1140–1144.

- xavf ehtimoli yuqori bo'lgan foydalanuvchilar yoki tizimlar nazoratga olinadi.

Biroq bu jarayon shaxsiy hayot daxlsizligi masalasini keskin qo'yadi. Katta ma'lumotlarni noto'g'ri ishlatish total kuzatuv va nazorat tizimlariga olib kelishi mumkin.

Sun'iy intellekt, kvant hisoblash va katta ma'lumotlar kelajakdagi kiberxavfsizlik siyosatining asosiy belgilovchi omillari bo'ladi. Ularning ijobiy imkoniyatlari:

- hujumlarni tez aniqlash va oldini olish;
- yangi shifrlash tizimlarini yaratish;
- xavflarni oldindan prognoz qilish.

Biroq ular bilan bog'liq xavflar ham mavjud:

- insonning qaror qabul qilishdagi rolini kamaytirish;
- mavjud shifrlash tizimlarining yaroqsiz bo'lib qolishi;
- total kuzatuv xavfi.

Shu sababli, kelajakdagi kiberxavfsizlik siyosati texnologiyalarni falsafiy-huquqiy asoslarda tartibga solishga qaratilishi lozim.

Kibermakon bugungi kunda global xavfsizlikning eng zaif nuqtalaridan biri sifatida qaralmoqda. Internetning transmilliy tabiati shuni ko'rsatadiki, bir davlat hududida yuzaga kelgan kiberhujum boshqa davlatning iqtisodiyoti, infratuzilmasi va ijtimoiy tizimiga bevosita zarar yetkazishi mumkin. Shu bois, xalqaro huquq tizimida kiberxavfsizlikni tartibga soluvchi aniq va majburiy normalar zarur.

Hozircha xalqaro huquqda kiberxavfsizlikni to'liq qamrab oluvchi yagona universal konvensiya mavjud emas. Ayrim tashabbuslar (Budapest konvensiyasi, BMT rezolyutsiyalari) bo'lsa-da, ular global darajada yetarli darajada qabul qilinmagan. Shu sababli, global kiberxavfsizlik siyosatida yangi konvensiyalar zaruriyati tobora ortib bormoqda.

2001-yilda Yevropa Kengashi tomonidan qabul qilingan "Budapest konvensiyasi"¹ kiberjinoyatlarga qarshi kurash

¹ Council of Europe. Convention on Cybercrime (Budapest Convention). – Budapest: CoE, 2001. – URL: <https://www.coe.int/en/web/conventions/full-list>

bo'yicha birinchi xalqaro hujjat hisoblanadi. Unda quyidagilar belgilangan:

- kompyuter tizimlariga noqonuniy kirishni jinoyat deb e'tirof etish;
- ma'lumotlarni noqonuniy egallash va tarqatishga qarshi kurash;
- davlatlar o'rtasida ma'lumot almashish va huquqiy yordam mexanizmlarini yaratish.

Ammo konvensiyaning cheklovlari ham mavjud:

1. Global qamrov yetishmasligi. Ko'plab davlatlar, jumladan, Rossiya, Xitoy va ayrim MDH mamlakatlari uni imzolamagan.
2. Huquqiy tafovutlar. Milliy qonunlar o'rtasidagi farqlar hamkorlikni murakkablashtirmoqda.
3. Texnologik eskirish. 2001-yilda qabul qilingan hujjat bugungi kunda paydo bo'lgan yangi tahdidlarni (sun'iy intellekt, kvant hujumlari) qamrab olmaydi.

BMT xalqaro huquqiy maydonni kengaytirish uchun bir necha mexanizmlar ishlab chiqdi:

- Governmental Group of Experts (GGE). 2004-yildan boshlab muntazam yig'ilishlar o'tkazib, kiberxavfsizlik bo'yicha tamoyillar ishlab chiqmoqda.
- Open-Ended Working Group (OEWG). 2018-yilda tuzilgan ushbu guruh barcha davlatlar ishtirokini ta'minlashga qaratilgan.
- Rezolyutsiyalar. "The Right to Privacy in the Digital Age" (2013) kabi hujjatlar kibermakonning huquqiy chegaralarini kengaytirmoqda.

Ammo BMT tashabbuslari ham majburiy kuchga ega emas, ular ko'proq siyosiy tavsiyalar darajasida qolmoqda.

Global kiberxavfsizlik siyosati uchun yangi xalqaro konvensiyalar ishlab chiqilishi zarur. Ular quyidagilarni qamrab olishi lozim:

1. Kiberhujumlarni huquqiy klassifikatsiya qilish. Hujum turlari (davlatlararo, jinoyatchilik, terroristik) aniq ajratilishi kerak.
2. Davlatlarning majburiyatlari. Har bir davlat o'z hudu-

didan boshqa davlatlarga qarshi kiberhujumlarga yo'l qo'y-maslik majburiyatini olishi kerak.

3. Sun'iy intellekt va yangi texnologiyalar. Yangi konvensiyalar AI, kvant hisoblash va IoT kabi texnologiyalarni huquqiy tartibga solishi zarur.

4. Xalqaro javobgarlik mexanizmlari. Kiberhujum sodir etgan davlat yoki tashkilotga nisbatan sanksiyalar va javobgarlik choralari belgilash.

5. Inson huquqlari va axborot erkinligi. Har qanday konvensiya erkinlik va xavfsizlik muvozanatini saqlashi zarur.

Falsafiy nuqtai nazardan, global kiberxavfsizlik siyosati universallik va partikulyarlik qarama-qarshiligi orqali talqin qilinadi. Universallik — umumiy xalqaro tamoyillar, partikulyarlik — milliy manfaatlar. Shu ikki qutbni uyg'unlashtiruvchi huquqiy mexanizmlar zarur.

Huquqiy jihatdan esa, yangi konvensiyalar xalqaro majburiyatlarni kuchaytirishi kerak. Aks holda, har bir davlat faqat o'z manfaatini ko'zlab harakat qilaveradi va kibermakon anarxiyaga aylanadi.

O'zbekiston global kiberxavfsizlik siyosatida faol ishtirok etmoqda:

- “Raqamli O'zbekiston – 2030” dasturi xalqaro hamkorlikni kuchaytirishni belgilagan.
- O'zbekiston BMTning OEKG jarayonida faol qatnashmoqda.
- Milliy qonunchilik Budapest konvensiyasi tamoyillariga moslashtirilmoqda, ammo xalqaro darajada yangi kelishuvlarda ham ishtirok etish zarur.

O'zbekiston uchun yangi konvensiyalar shuni anglatadiki: milliy qonunchilik global tamoyillar bilan uyg'unlashadi, xalqaro hamkorlik kuchayadi va milliy manfaatlar yaxshiroq himoya qilinadi.

Global kiberxavfsizlik siyosatining kelajagi yangi xalqaro konvensiyalar qabul qilinishiga bog'liq. Hozirgi holatda Budapest konvensiyasi va BMT rezolyutsiyalari yetarli emas. Yangi hujjatlar:

- kiberhujumlarni huquqiy jihatdan tasniflaydi;
- davlatlarning majburiyatlarini aniq belgilaydi;
- yangi texnologiyalarni tartibga soladi;
- xalqaro javobgarlik mexanizmlarini yaratadi;
- inson huquqlarini himoya qilishni davom ettiradi.

Global kiberxavfsizlik siyosati yangi xalqaro huquqiy asoslarsiz barqaror rivojlana olmaydi. Bu nafaqat xalqaro tizim, balki O'zbekiston uchun ham strategik zaruratdir.

Kibermakon xavfsizligi masalalari nafaqat texnikyoki siyosiy, balki chuqur falsafiy-huquqiy mohiyatga ham ega. Chunki kibermakon — bu inson tafakkuri, davlat suvereniteti, jamiyat qadriyatlari va global tizimlar kesishadigan maydon. Unda uch asosiy tamoyil doimo bir-biri bilan dialektik munosabatda: inson huquqlari, xavfsizlik, barqarorlik. Bu tamoyillardan birining mutlaq ustuvorligi boshqalarining zaiflashishiga olib keladi. Shu bois, kelajak kiberxavfsizlik siyosatida ularning uyg'unligi falsafiy va huquqiy asos sifatida qaralishi zarur.

BMTning 2012-yilgi rezolyutsiyasida shunday deyilgan: «Insonlar internetda ham, real dunyoda bo'lgani kabi, o'z huquqlaridan to'liq foydalanishlari lozim»¹.

Bu shuni anglatadiki, kibermakon inson huquqlarining kengayishi uchun yangi imkoniyat yaratadi. Biroq bu huquqlar xavfsizlik va barqarorlikka zid kelmasligi lozim. Misol uchun:

- So'z erkinligi – dezinformatsiya va nafrat targ'iboti bilan chegaralanadi.
- Shaxsiy hayot daxlsizligi – milliy xavfsizlik ehtiyojlari bilan muvozanatda bo'lishi kerak.
- Axborot olish huquqi – davlat suvereniteti va madaniy qadriyatlarni inobatga olishi lozim.

Xavfsizlik tushunchasi kibermakonda davlatlar uchun ham, fuqarolar uchun ham markaziy o'rin tutadi. Davlatlar milliy infratuzilmani himoya qilishni ustuvor qo'yadi, fuqarolar esa shaxsiy ma'lumotlarining xavfsizligini talab qiladi.

¹ United Nations Human Rights Council. Resolution on the Promotion, Protection and Enjoyment of Human Rights on the Internet. – Geneva: UN, 2012. – A/HRC/RES/20/8.

Falsafiy jihatdan xavfsizlik — bu “zarardan xoli bo‘lish holati” emas, balki erkin rivojlanish sharoitidir. Demak, xavfsizlik inson huquqlarini cheklash vositasi emas, balki ularni amalga oshirish kafolatidir.

Barqarorlik kibermakon siyosatining uzoq muddatli maqsadi hisoblanadi. U quyidagilarga tayanadi:

- Texnologik barqarorlik – yangi texnologiyalar (SI, kvant hisoblash) xavf emas, imkoniyatga aylanishi.
- Ijtimoiy barqarorlik – dezinformatsiya va kiberjinoyatlarga qarshi immunitet hosil bo‘lishi.
- Huquqiy barqarorlik – xalqaro normalar va milliy qonunlarning uyg‘unligi.

BMTning “Sustainable Development Goals (SDGs)” dasturida raqamli xavfsizlik global barqaror taraqqiyotning ajralmas qismi sifatida qaralmoqda¹.

IV BOB BO‘YICHA XULOSALAR

Mazkur bobda global hamkorlik va kelajak istiqbollari masalalari kiberxavfsizlik siyosatining markaziy yo‘nalishi sifatida tahlil qilindi. Bob davomida xalqaro tashkilotlarning roli, axborot etikasi va inson huquqlarini himoya qilish tamoyillari, shuningdek, yangi texnologiyalar ta‘sirida kelajakdagi xavf-xatarlar va huquqiy ehtiyojlar falsafiy-huquqiy nuqtai nazardan ko‘rib chiqildi. Endilikda ushbu tadqiqotdan kelib chiqadigan asosiy xulosalarni umumlashtirish mumkin.

Birinchidan, kibermakonning transmilliy xususiyati davlatlarni global hamkorlikka majbur etmoqda. BMT, NATO, SHHT, OSCE va ITU kabi tashkilotlarning tashabbuslari kiberxavfsizlikning umumiy me‘yoriy asoslarini yaratishda hal qiluvchi ahamiyat kasb etmoqda. Shu bilan birga, milliy suverenitet va xalqaro normalar o‘rtasida ziddiyatlar mavjud bo‘lib, ular kelajakda yangi muvozanat mexanizmlarini ishlab chiqishni talab qiladi.

Ikkinchidan, axborot etikasi kibermakon xavfsizligining axloqiy va falsafiy poydevorini tashkil etadi. Haqqoniylik,

¹ United Nations. Sustainable Development Goals Report 2022. – New York: UN, 2022. – P. 33–39.

shaffoflik, mas'uliyat, adolat va shaxsiy hayot daxlsizligi tamoyillari global va milliy siyosatlarida uyg'unlashtirilishi lozim. Inson huquqlarini hisobga olmagan har qanday kiberxavfsizlik siyosati beqaror bo'lib qolishi aniqlandi.

Uchinchidan, yangi texnologiyalar — sun'iy intellekt, kvant hisoblash va katta ma'lumotlar — kiberxavfsizlikni mustahkamlash imkoniyatini yaratadi, ammo ular bilan birga yangi xavflarni ham yuzaga keltiradi. Shu bois, kelajak siyosati texnologiyalarni huquqiy va axloqiy nazorat ostiga olishni talab qiladi.

To'rtinchidan, mavjud xalqaro huquqiy mexanizmlar yetarli emas. Budapest konvensiyasi va BMT rezolyutsiyalari muhim bosqich bo'lsa-da, ular global darajada majburiy kuchga ega emas. Shu sababli, yangi universal konvensiyalar zarur bo'lib, ular davlatlarning majburiyatlarini aniq belgilashi, sun'iy intellekt va kvant texnologiyalarini ham qamrab olishi lozim.

Beshinchidan, falsafiy-huquqiy tahlil shuni ko'rsatadiki, kelajakdagi kiberxavfsizlik siyosati inson huquqlari, xavfsizlik va barqarorlik uyg'unligiga tayanishi kerak. Bu uchlikni muvozanatli uyg'unlashtirmagan jamiyatda barqaror rivojlanish mumkin emas.

Oltinchidan, O'zbekiston tajribasi shuni ko'rsatadiki, milliy manfaatlar va global tamoyillar uyg'unligiga intilish samarali natija beradi. "Raqamli O'zbekiston – 2030" dasturi, shaxsiy ma'lumotlarni himoya qilishga qaratilgan qonunlar va xalqaro hamkorlik tashabbuslari mamlakatni mintaqaviy va global kiberxavfsizlik siyosatida faol ishtirokchiga aylantirmoqda.

Xulosa qilib aytganda, 4-bobning tahlillari shuni ko'rsatadiki, kelajakdagi kiberxavfsizlik siyosati texnik imkoniyatlar, huquqiy mexanizmlar va falsafiy tamoyillar uyg'unligida rivojlanadi. Global hamkorliksiz kibermakon xavfsizligini ta'minlab bo'lmaydi, inson huquqlarisiz xavfsizlik barqaror bo'lmaydi, yangi texnologiyalarni nazoratsiz qo'llash esa xavf-xatarlarni kuchaytiradi. Shu sababli, O'zbekiston va boshqa davlatlar kiberxavfsizlikni ta'minlashda xalqaro hamkorlikni kengaytirishi, milliy manfaatlarni global qadriyatlar bilan uyg'unlashtirishi va falsafiy-huquqiy asoslarni mustahkamlashi zarur.

XULOSA

Mazkur monografiya kibermakon xavfsizligini falsafiy-huquqiy tahlil qilishga, turli davlatlar tajribasini qiyosiy o'rganishga va O'zbekiston uchun amaliy saboqlar ishlab chiqishga bag'ishlandi. Raqamli davrning asosiy xususiyati shundaki, insoniyat hayoti tobora ko'proq virtual maydonga ko'chmoqda va kibermakon jamiyat taraqqiyotining yangi ontologik realligi sifatida shakllanmoqda. Shu jarayonda inson huquqlari, milliy manfaatlar, erkinlik va xavfsizlik muammolari kesishib, murakkab falsafiy va huquqiy savollarni yuzaga keltirmoqda.

Monografiyada keltirilgan tadqiqotlar shuni ko'rsatadiki, kibermakon xavfsizligi masalalari bugungi kunda faqat texnik himoya bilan chegaralanmaydi. U ijtimoiy ong, madaniyat, siyosat va huquq sohalarining kesishma nuqtasida turibdi. Masalan, erkin axborot oqimi demokratik qadriyatlar uchun muhim bo'lsa-da, u bilan birgalikda xabarlar va kiberjinoyatlar xavfi ham ortib bormoqda. Shu bois kibermakon xavfsizligi texnologiya, huquq va falsafaning birgalikdagi harakati orqali ta'minlanishi zarur.

Tadqiqot davomida dunyo miqyosidagi turli yondashuvlar – AQShning milliy xavfsizlikka asoslangan modeli, Yevropa Ittifoqining inson huquqlariga tayangan modeli, Rossiya va Xitoyning suverenitet markazli siyosati, Yaponiya va Koreyaning innovatsion yondashuvlari qiyosiy tahlil qilindi. Shuningdek, Markaziy Osiyo davlatlari va O'zbekiston tajribasi ham atroflicha o'rganildi.

O'zbekiston uchun monografiya natijalarining dolzarbligi shundaki, mamlakatimiz "Raqamli O'zbekiston – 2030" dasturi doirasida keng ko'lamli raqamli transformatsiyani amalga oshirmoqda. Bu esa bir tomondan imkoniyatlarni kengaytirsa, ikkinchi tomondan yangi xavf-xatarlarni yuzaga keltirmoqda. Shu sababli kibermakon xavfsizligini ta'minlash milliy xavfsizlik, davlat suvereniteti va fuqarolarning huquqlarini kafolatlashning eng muhim shartiga aylanmoqda.

Monografiyaning kirish, boblar va tahlillari shuni ko'rsatdiki,

kibermakon xavfsizligi masalasini falsafiy-huquqiy yondashuv asosida tadqiq etish O'zbekiston uchun ham nazariy, ham amaliy jihatdan zarurdir. Endilikda ushbu tadqiqotning asosiy xulosalari sifatida quyidagilarni sanab o'tamiz.

Birinchidan, kibermakon bugungi kunda insoniyat hayotining ajralmas qismi sifatida shakllandi va u endilikda yangi ijtimoiy reallik sifatida qaralmoqda. Turing, Viner va Kastells kabi olimlarning ishlari asosida shuni ko'rish mumkinki, kibermakon faqat texnologik tizim emas, balki ijtimoiy ong, madaniyat va siyosiy jarayonlarning markazida turibdi. Shu bois kibermakon xavfsizligini faqat texnik himoya darajasida emas, balki falsafiy-huquqiy kategoriya sifatida ham tahlil qilish zarur. Bu yondashuv kiberxavfsizlikni jamiyat taraqqiyoti, inson huquqlari, axloqiy qadriyatlar va davlat suvereniteti bilan uyg'unlashtirish imkonini beradi.

Ikkinchidan, kiberxavfsizlik masalalari xalqaro miqyosda turlicha talqin qilinmoqda. AQSh milliy xavfsizlik va mudofaa sohasini ustuvor deb bilsa, Yevropa Ittifoqi inson huquqlari va ma'lumotlarni himoya qilishga asosiy e'tibor qaratadi. Rossiya va Xitoy esa milliy suverenitet va davlat nazoratini markaziy tamoyil sifatida ilgari suradi. Yaponiya va Janubiy Koreya esa innovatsion texnologiyalar orqali kiberxavfsizlikni ta'minlashni asosiy strategiya qilib olgan. Ushbu qiyosiy tahlil shuni ko'rsatadiki, kiberxavfsizlikni ta'minlashda yagona universal model mavjud emas. Har bir davlat o'z siyosiy tizimi, iqtisodiy imkoniyatlari va madaniy qadriyatlariga asoslangan strategiyani tanlaydi. Shu nuqtai nazardan, O'zbekiston uchun ham milliy model ishlab chiqish zarur, biroq u xalqaro tamoyillar bilan uyg'unlashgan bo'lishi lozim.

Uchinchidan, kibermakon xavfsizligi masalalarining markazida inson huquqlari va erkinliklari turadi. Bugungi kunda shaxsiy ma'lumotlarni himoya qilish, so'z erkinligini ta'minlash va axborotdan erkin foydalanish huquqi tobora dolzarb bo'lib bormoqda. Shu bilan birga, kiberjinoyatlar, yolg'on xabarlar va propagandaga qarshi kurashishda davlatlarning xavfsizlik choralarini kuchaytirishi ko'pincha fuqarolik

erkinliklarini cheklab qo'yishi mumkin. Shu bois erkinlik va xavfsizlik o'rtasida muvozanatni topish global hamjamiyat va milliy hukumatlarning eng asosiy vazifasiga aylanmoqda. Monografiyada keltirilgan falsafiy-dialektik yondashuv shuni ko'rsatadiki, inson huquqlarini cheklamagan holda xavfsizlikni ta'minlash mumkin va buning uchun xalqaro hamkorlik, axborot etikasi va normativ-huquqiy mexanizmlar uyg'unlashtirilishi kerak.

To'rtinchidan, kibermakon xavfsizligi masalalarini samarali hal qilishda xalqaro hamkorlik alohida o'rin tutadi. Chunki internet chegaralarni bilmaydi, kiberjinoyatlar va kiberhujumlar esa bir davlat hududi bilan cheklanib qolmaydi. Shuning uchun BMT, NATO, SHHT, Yevropa Ittifoqi, ENISA kabi xalqaro tashkilotlar kiberxavfsizlikka oid tashabbuslarni ilgari surmoqda. Masalan, Budapest konvensiyasi kiberjinoyatlarga qarshi xalqaro miqyosda hamkorlikni kuchaytirishga qaratilgan eng muhim huquqiy hujjat hisoblanadi. NATO va Tallinn qo'llanmasi esa kiberurushning xalqaro huquqiy me'yorlarini belgilashda katta rol o'ynadi. Shuningdek, BMTning GGE va OEWG jarayonlari davlatlarning o'zaro kelishuvlari uchun muhim platformaga aylandi. Bu faktlar shuni ko'rsatadiki, kibermakon xavfsizligini faqat milliy darajada emas, balki xalqaro hamkorlik asosida ta'minlash mumkin. Shu bois O'zbekiston ham xalqaro tashkilotlar bilan faol hamkorlikni davom ettirishi, yangi konvensiyalar ishlab chiqilishida ishtirok etishi lozim.

Beshinchidan, kibermakon xavfsizligini mustahkamlashda ta'lim va ilmiy tadqiqotlarning o'rni beqiyosdir. UNESCO hisobotlariga ko'ra, 2030-yilgacha dunyo bo'ylab 3,5 million kiberxavfsizlik mutaxassisi yetishmasligi prognoz qilinmoqda. Bu raqam kibermakon xavfsizligini ta'minlash uchun inson kapitaliga sarmoya kiritish qanchalik muhimligini ko'rsatadi. Monografiya natijalariga ko'ra, O'zbekistonda oliy ta'lim tizimida kiberxavfsizlikka oid maxsus kurslar va dasturlarni kengaytirish, ilmiy tadqiqot institutlarida bu sohaga oid ilmiy maktablarni shakllantirish zarur. Bu nafaqat texnik

mutaxassislarni tayyorlash, balki kiberfalsafa, axborot etikasi, kiberhuquq kabi sohalarda ham ilmiy salohiyatni kuchaytirishga xizmat qiladi. Zero, kibermakon xavfsizligi masalalarini faqat muhandislik darajasida emas, balki falsafiy-huquqiy kontekstda o'rganish ham zarurdir.

Oltinchidan, O'zbekiston tajribasi shuni ko'rsatadiki, kibermakon xavfsizligi milliy xavfsizlikning ajralmas qismidir. "Raqamli O'zbekiston – 2030" dasturi doirasida davlat xizmatlari, ta'lim va sog'liqni saqlash tizimi, moliya sektori va elektron hukumat jadal raqamlashtirilmoqda. Bu jarayon fuqarolarga qulayliklaryaratish bilan birga, yangi xavf-xatarlarni ham yuzaga keltirmoqda. Shu sababli, milliy qonunchilikni takomillashtirish, xalqaro tajribalarni moslashtirish va texnologik infratuzilmani mustahkamlash zarur. Masalan, shaxsiy ma'lumotlarni himoya qilish, davlat sirlarini muhofaza qilish, kiberjinoyatlarga qarshi kurashish bo'yicha maxsus qonunlar ishlab chiqilishi va amaliyotda samarali qo'llanishi kerak. Shu nuqtai nazardan, O'zbekistonning kibermakon xavfsizligini ta'minlashda falsafiy-huquqiy yondashuvlar, axborot etikasi tamoyillari va xalqaro hamkorlik tajribalaridan foydalanishi alohida ahamiyat kasb etadi.

Yettinchidan, kibermakon xavfsizligi muammolari faqat texnik yoki huquqiy doirada emas, balki axloqiy va falsafiy jihatdan ham ko'rib chiqilishi zarur. Chunki kiberhujumlar oqibatida nafaqat iqtisodiy zarar yetadi, balki inson qadr-qimmati, jamiyatdagi ishonch va axloqiy qadriyatlar ham zararlanadi. Masalan, feyk xabarlar, kiberpropaganda yoki kiberbulling nafaqat xavfsizlikka, balki ijtimoiy barqarorlik va axloqiy muhitga ham putur yetkazadi. Shu bois monografiyada axborot etikasi tamoyillariga alohida e'tibor qaratildi: shaffoflik, mas'uliyat, adolat, inson qadr-qimmatini hurmat qilish. Bu jihatdan kiberxavfsizlik siyosati nafaqat texnologik himoya vositalariga, balki jamiyatda axloqiy qadriyatlarni mustahkamlashga ham asoslanishi kerak.

Sakkizinchidan, kibermakon xavfsizligi masalalarida milliy manfaatlar va global tamoyillar uyg'unligi alohida o'rin

tutadi. Har bir davlat o'zining siyosiy, iqtisodiy va madaniy xususiyatlariga ko'ra milliy strategiya ishlab chiqadi. Shu bilan birga, internetning global tabiati sababli davlatlarning yolg'iz harakati yetarli emas. Masalan, Xitoyning "kiber suverenitet" konsepsiyasi milliy manfaatlarini himoya qilishni nazarda tutsa, Yevropa Ittifoqining GDPR qoidalari global axborot oqimini tartibga solishga qaratilgan. O'zbekiston uchun ham eng maqbul yo'l — milliy manfaatlarini himoya qilgan holda xalqaro standartlarga moslashishdir. Bu uyg'unlik davlat suverenitetini saqlab qolish bilan birga, xalqaro hamkorlik va ishonchni mustahkamlashga xizmat qiladi.

To'qqizinchidan, kibermakon xavfsizligini ta'minlashda texnologik innovatsiyalarning roli ham beqiyosdir. Sun'iy intellekt, blokcheyn, kvant hisoblash kabi yangi texnologiyalar bir tomondan xavfsizlikni mustahkamlash uchun qulay imkoniyatlar bersa, ikkinchi tomondan yangi xavf-xatarlarni ham yuzaga keltiradi. Masalan, sun'iy intellekt yordamida kiberhujumlarni aniqlash va oldini olish mumkin, ammo shu texnologiyaning o'zi ham "deepfake" kabi xavfli vositalar yaratishga xizmat qilishi mumkin. Shu bois monografiyada texnologiyalarni ikki tomonlama tabiatga ega vosita sifatida talqin qilish zarurligi ko'rsatildi. O'zbekiston uchun ham raqamli innovatsiyalarni rivojlantirish jarayonida xavfsizlikni birlamchi shart sifatida belgilash muhimdir. Bu yondashuv texnologik taraqqiyot va milliy xavfsizlik o'rtasidagi muvozanatni ta'minlashga xizmat qiladi.

O'ninchidan, kibermakon xavfsizligini ta'minlashda institutsional mexanizmlar muhim rol o'ynaydi. Faqat qonunlar va xalqaro kelishuvlar emas, balki davlat idoralari, maxsus agentliklar va hukumatga qarashli markazlar faoliyati ham muhimdir. Masalan, AQShda DHS (Department of Homeland Security) va CISA (Cybersecurity and Infrastructure Security Agency), Yevropada ENISA, Rossiyada FSB va boshqa maxsus organlar kiberxavfsizlik siyosatini amalda muvofiqlashtirib kelmoqda. O'zbekistonda esa "Kiberxavfsizlik markazi" tashkil etilib, u davlat organlari faoliyatini muvofiqlashtirish bilan

shug'ullanmoqda. Shu bilan birga, kiberxavfsizlikni samarali ta'minlash uchun faqat markazlashtirilgan nazorat emas, balki xususiy sektor va fuqarolik jamiyati hamkorligi ham zarurdir. Bu integratsiya milliy xavfsizlikni yanada mustahkamlaydi.

O'n birinchidan, kibermakon xavfsizligini mustahkamlashda fuqarolik jamiyati va nodavlat sektorning o'rni ham ortib bormoqda. Chunki internetning asosiy foydalanuvchilari oddiy fuqarolar, tadbirkorlar va ta'lim muassasalaridir. Shu bois kiberxavfsizlik siyosatini faqat davlat idoralari doirasida cheklab qo'yish yetarli emas. Jamoat tashkilotlari, NNTlar, mustaqil ilmiy muassasalar va IT-kompaniyalar ham bu jarayonda faol ishtirok etishi zarur. Masalan, xalqaro tajribada "multi-stakeholder model" — davlat, biznes va jamiyatning hamkorligi asosida kiberxavfsizlikni boshqarish modeli samarali deb topilgan. O'zbekiston sharoitida ham bu tajriba bosqichma-bosqich joriy etilishi mumkin.

O'nikkinchidan, kibermakon xavfsizligi masalalarida madaniy va ma'naviy qadriyatlarni inobatga olish ham muhimdir. Chunki axborot oqimlari milliy madaniyat, urf-odatlar va qadriyatlarga bevosita ta'sir ko'rsatadi. Kiberhujumlar yoki zararli kontent faqat texnik tahdid emas, balki milliy o'zlik va ma'naviy barqarorlik uchun ham xavfdir. Shu sababli, O'zbekistonda kibermakon xavfsizligini mustahkamlash strategiyasi milliy qadriyatlar bilan uyg'un bo'lishi kerak. Ta'lim, OAV va ijtimoiy tarmoqlar orqali yoshlarni milliy va umuminsoniy qadriyatlarga sodiq holda tarbiyalash kiberxavfsizlik siyosatining muhim elementi sifatida qaralishi lozim. Bu yondashuv kibermakon xavfsizligini nafaqat texnologik, balki ma'naviy-ma'rifiy jarayon sifatida ham mustahkamlaydi.

O'n uchinchidan, kibermakon xavfsizligini ta'minlashda iqtisodiy barqarorlik hal qiluvchi omillardan biridir. Jahon iqtisodiy forumining 2023-yilgi hisobotida ta'kidlanganidek, kiberjinoyatlar global iqtisodiyotga milliardlab zarar yetkazmoqda va bu zarar hajmi 2030-yilga borib 10 trillion AQSh dollaridan oshishi mumkin. Demak, iqtisodiy xavfsizlik va kiberxavfsizlik bir-biridan ajralmasdir. O'zbekistonda elektron

tijorat, elektron hukumat va raqamli bank xizmatlarining rivojlanishi bilan bu sohada yangi imkoniyatlar yaratilmoqda, lekin ular bilan bir qatorda kiberxavf-xatarlar ham ortmoqda. Shu bois monografiyada ishlab chiqilgan ilmiy tavsiyalar iqtisodiy barqarorlikni ta'minlash uchun moliyaviy tizimni, elektron to'lovlarni, startaplar va biznes infratuzilmasini kiberhujumlardan himoya qilish mexanizmlarini mustahkamlashga qaratilgan.

O'n to'rtinchidan, kibermakon xavfsizligini mustahkamlashda xalqaro-huquqiy me'yorlarni shakllantirish dolzarbdir. Bugungi kunda kiberhujumlarni xalqaro huquqiy jihatdan urush e'lon qilishga tenglashtirish yoki uni davlatlararo nizolarga sabab bo'lishi mumkinligi haqida bahslar davom etmoqda. "Tallinn qo'llanmasi" muhim hujjat bo'lsa-da, u majburiy kuchga ega emas. Budapest konvensiyasiga esa barcha davlatlar qo'shilmagan. Shu nuqtai nazardan, global darajada majburiy kuchga ega bo'lgan kiberxavfsizlik konvensiyasi ishlab chiqilishi zarur. O'zbekistonning bu jarayonlarda faol ishtiroki nafaqat milliy manfaatlarini himoya qiladi, balki xalqaro maydonda mamlakatimizning pozitsiyasini mustahkamlaydi.

O'n beshinchidan, kibermakon xavfsizligi masalalarida kelajak istiqbollari ham alohida e'tiborni talab qiladi. Sun'iy intellekt, kvant texnologiyalari, metaverse va raqamli platformalarning rivojlanishi bilan birga, yangi xavf-xatarlar yuzaga chiqmoqda. Masalan, kvant hisoblash texnologiyalari mavjud shifrlash tizimlarini eskirtirishi, metaverse esa ijtimoiy nazorat va virtual jinoyatlarning yangi shakllarini paydo qilishi mumkin. Shu bois kelajakdagi kiberxavfsizlik siyosati oldindan rejalashtirish, ehtimoliy tahdidlarni prognoz qilish va ularni falsafiy-huquqiy asosda tartibga solishga tayyor bo'lishi kerak. Monografiya natijalariga ko'ra, O'zbekiston uchun ham ilmiy-tadqiqotlarni kelajak xavflarini hisobga olgan holda olib borish, xalqaro hamkorlikni kengaytirish va innovatsion texnologiyalarni xavfsiz joriy etish eng muhim vazifalardan biridir.

Kibermakon insoniyat taraqqiyotining eng muhim bosqich-

laridan biri sifatida yangi imkoniyatlar va yangi xavflarni bir vaqtda olib keldi. Ushbu monografiyada olib borilgan falsafiy-huquqiy tahlillar, xalqaro tajriba va O'zbekiston sharoitida amalga oshirilgan tadqiqotlar bir necha asosiy natijalarga olib keldi.

Birinchidan, kibermakon xavfsizligi masalasi endilikda milliy yoki texnik masala sifatida emas, balki global va falsafiy-huquqiy muammo sifatida qaralishi zarur. Chunki internetning chegarasiz tabiati, texnologiyalarning jadal rivojlanishi va axborot oqimlarining global tus olishi uni xalqaro siyosat, inson huquqlari va ijtimoiy ong bilan chambarchas bog'liq qiladi.

Ikkinchidan, dunyo davlatlari tajribasi shuni ko'rsatdiki, yagona universal kiberxavfsizlik modeli mavjud emas. AQShning milliy xavfsizlikka yo'naltirilgan strategiyasi, Yevropaning inson huquqlariga asoslangan yondashuvi, Rossiya va Xitoyning suverenitet markazli siyosati, Yaponiya va Koreyaning innovatsion modeli — barchasi o'ziga xos ustuvorliklarga ega. O'zbekiston uchun esa eng maqbul yo'l — milliy manfaatlarni himoya qilgan holda xalqaro tamoyillar bilan uyg'unlashgan milliy modelni ishlab chiqishdir.

Uchinchidan, kibermakon xavfsizligi masalalarini hal qilishda inson huquqlari, axborot etikasi va ijtimoiy barqarorlik tamoyillari alohida ahamiyatga ega. Chunki xavfsizlikni kuchaytirish bahonasida erkinliklarni cheklash jamiyatda norozilik va ijtimoiy beqarorlikni yuzaga keltirishi mumkin. Shu bois xavfsizlik va erkinlik o'rtasidagi muvozanatni topish kibermakon siyosatining asosiy falsafiy tamoyillaridan biri bo'lishi lozim.

To'rtinchidan, O'zbekiston sharoitida kibermakon xavfsizligini ta'minlash "Raqamli O'zbekiston – 2030" dasturi, milliy qonunchilik va xalqaro hamkorlik asosida shakllanmoqda. Shu bilan birga, ta'lim tizimi, ilmiy tadqiqotlar va fuqarolik jamiyatining faol ishtiroki orqali kiberxavfsizlik madaniyatini rivojlantirish dolzarb vazifa sifatida turibdi. Monografiyada ishlab chiqilgan ilmiy tavsiyalar davlat siyosatini takomillashtirish, huquqiy mexanizmlarni mustahkamlash va jamiyatda

axborot madaniyatini shakllantirishga hissa qo'shishi mumkin.

Beshinchidan, kelajak istiqbollari nuqtai nazaridan sun'iy intellekt, kvant texnologiyalari, metaverse va boshqa innovation jarayonlar yangi imkoniyatlar bilan bir qatorda yangi xavflarni ham keltirib chiqaradi. Shu bois O'zbekiston va boshqa davlatlar kelajakdagi tahdidlarni prognoz qilish, ularga tayyor turish va xavfsizlik strategiyalarini oldindan ishlab chiqish zarur.

Shunday qilib, ushbu monografiyaning yakuniy natijasi shundan iboratki: kibermakon xavfsizligi insoniyat taraqqiyo-tining ajralmas qismi sifatida kompleks yondashuvni talab qiladi. Texnik, huquqiy, falsafiy va ijtimoiy omillar uyg'unligida shakllangan strategiyalar barqaror xavfsizlikni ta'minlashi mumkin. O'zbekiston uchun esa bu yo'lda xalqaro tajribani chuqur o'rganish, milliy modelni ishlab chiqish va jamiyatda kiberxavfsizlik madaniyatini keng targ'ib qilish eng muhim vazifalar qatoriga kiradi.

Monografiyaning natijalari nafaqat ilmiy hamjamiyat uchun, balki siyosatchilar, huquqshunoslar, IT-mutaxassislar va keng jamoatchilik uchun ham amaliy ahamiyatga ega bo'lib, kibermakon xavfsizligini mustahkamlash yo'lida nazariy asos va amaliy tavsiyalar majmuasini taqdim etadi.

FOYDALANILGAN ADABIYOTLAR

I. Normativ-huquqiy hujjatlar

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

2. European Parliament. Directive 95/46/EC on the Protection of Individuals with Regard to the Processing of Personal Data. – Brussels: EU, 1995.

3. European Parliament. General Data Protection Regulation (GDPR). – Brussels: EU, 2016. – URL: <https://gdpr-info.eu>

4. NATO. Wales Summit Declaration on Cyber Defence. – Cardiff: NATO Press, 2014. – URL: https://www.nato.int/cps/en/natohq/official_texts_112964.htm

5. O'zbekiston Respublikasi Konstitutsiyasi (yangi tahrir). – Toshkent: O'zbekiston, 2023. – URL: <https://lex.uz/docs/6788457>

6. O'zbekiston Respublikasi Prezidentining PF-60-son Farmoni, 28.01.2022-y. "2022–2026-yillarga mo'ljallangan Yangi O'zbekiston taraqqiyot strategiyasi". – Toshkent: Prezident Administratsiyasi, 2022. – URL: <https://lex.uz/docs/5841063>

7. O'zbekiston Respublikasi Prezidentining PQ-358-son qarori, 14.10.2024-y. "Sun'iy intellekt texnologiyalarini 2030-yilgacha rivojlantirish strategiyasi". – Toshkent: Prezident Administratsiyasi, 2024. – URL: <https://lex.uz/docs/7158604>

8. O'zbekiston Respublikasi Prezidentining PQ-3832-son qarori, 03.07.2018-y. "Kiberxavfsizlik sohasida davlat boshqaruvini takomillashtirish chora-tadbirlari to'g'risida". – Toshkent: Prezident Administratsiyasi, 2018. – URL: <https://lex.uz/docs/3827636>

9. 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>

10. O'zbekiston Respublikasi Qonuni. "Axborot xavfsizligi to'g'risida". – Toshkent: LexUZ, 2022. – URL: <https://lex.uz/>

docs/6003766

11. O'zbekiston Respublikasi Qonuni. "Axborotlashtirish to'g'risida". – Toshkent: LexUZ, 2019. – URL: <https://lex.uz/docs/4314861>

12. O'zbekiston Respublikasi Qonuni. "Davlat sirlarini saqlash to'g'risida". – Toshkent: LexUZ, 1993. – URL: <https://lex.uz/docs/16112>

13. O'zbekiston Respublikasi Qonuni. "Shaxsiy ma'lumotlar to'g'risida". – Toshkent: LexUZ, 2019. – URL: <https://lex.uz/docs/4396428>

14. O'zbekiston Respublikasi Qonuni. "Ta'lim to'g'risida". – Toshkent: LexUZ, 2020. – URL: <https://lex.uz/docs/5013007>

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

16. United Nations. Universal Declaration of Human Rights. – New York: UN, 1948.

17. United Nations General Assembly. The Right to Privacy in the Digital Age. – New York: UN, 2013. – A/RES/68/167.

18. United Nations General Assembly. Report of the Group of Governmental Experts on ICTs in the Context of International Security. – New York: UN, 2015. – A/70/174.

II. Asosiy adabiyotlar

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

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

3. Floridi, L. The Ethics of Information. – Oxford: Oxford University Press, 2013.

4. Floridi, L., Moor, J., Weckert, J. Information Ethics: On the Philosophical Foundations of Computer Ethics. – Ethics and Information Technology, Vol. 1, 1999.

5. Nye, J. Cyber Power. – Harvard Kennedy School, Belfer Center Report, 2010.

6. Ohlin, J. D. The Ethics of Cybersecurity. – Oxford: Oxford

University Press, 2019.

7. Rid, T. Rise of the Machines: A Cybernetic History. – New York: W. W. Norton, 2016.

8. Turing, A. Computing Machinery and Intelligence. // Mind. – 1950. – Vol. LIX, №236.

9. Voynova, I. O. Kiberprostranstvo kak novaya sotsial'naya real'nost'. – Moskva: Nauka, 2018.

10. Wiener, N. Cybernetics: Or Control and Communication in the Animal and the Machine. – Cambridge: MIT Press, 1948.

III. Qo'shimcha adabiyotlar

1. Abdurahmonov, I. Raqamli iqtisodiyotda huquqiy muhofaza. – Toshkent: TDYUI nashriyoti, 2021.

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

3. Bartosh, A. V. Kiberugrozy i mezhdunarodnaya bezopasnost'. – Moskva: Aspekt Press, 2012.

4. Beisenov, A. Informatsionnaya bezopasnost' Kazakhstana. – Almaty: KazNU, 2020.

5. Gibson, W. Neuromancer. – New York: Ace Books, 1984.

6. Ivanova, K. A., Myltykbaev, M., Shtodina, D. D. The Concept of Cyberspace in International Law. – Law Enforcement Review, 2022.

7. Knyazev, V. A. Informatsionnaya bezopasnost' gosudarstva. – Moskva: Yurayt, 2015.

8. Lessig, L. Code and Other Laws of Cyberspace. – New York: Basic Books, 1999.

9. Mueller, M. Networks and States: The Global Politics of Internet Governance. – MIT Press, 2010.

10. Nurmatov, A. Kiberxavfsizlik falsafasi: ijtimoiy va huquqiy muammolar. – Toshkent: Iqtisodiyot, 2022.

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

12. Qarshiyeva, N. T. O'zbekistonda kiberxavfsizlik: raqamli

iqtisodiyotni himoya qilish. – Iqtisodiy integratsiya va mintaqaviy raqobatbardoshlik xalqaro jurnali, Vol. 1, №6, 2024.

13. Schneier, B. *Secrets and Lies: Digital Security in a Networked World*. – Wiley, 2000.

14. Smolyan, G. L. *Tsifrovaya transformatsiya obshchestva i bezopasnost'*. – Moskva: ROSSPEN, 2019.

IV. Internet resurslari

1. Cybersecurity Ventures. *2023 Cybercrime Report*. – New York: Cybersecurity Ventures, 2023. – URL: <https://cybersecurityventures.com>

2. ENISA. *Threat Landscape Report 2021*. – Athens: European Union Agency for Cybersecurity, 2021. – URL: <https://www.enisa.europa.eu>

3. Europol. *Internet Organised Crime Threat Assessment 2018*. – The Hague: Europol, 2018.

4. Interpol. *Cybercrime*. – Official website, 2020. – URL: <https://www.interpol.int/en/Crimes/Cybercrime>

5. ITU. *Global Cybersecurity Index 2020–2022*. – Geneva: ITU Publications, 2022. – URL: <https://www.itu.int>

6. Microsoft Uzbekistan. *Cybersecurity Training Programs 2020–2022*. – Tashkent: Microsoft Press, 2022.

7. OECD. *Public-Private Partnerships in Cybersecurity*. – Paris: OECD Publishing, 2019.

8. UNESCO. *Cybersecurity Skills Gap Report 2022*. – Paris: UNESCO Publishing, 2022.

9. UZ-CERT. *Annual Report 2021*. – Tashkent: National Cybersecurity Center of Uzbekistan, 2022.

10. United Nations. *Sustainable Development Goals and Cybersecurity*. – New York: UN, 2020.

MUNDARIJA

KIRISH	3
I-BOB KIBERMAKON XAVFSIZLIGINI TA'MINLASHNING NAZARIY VA METODOLOGIK ASOSLARI.....	25
1.1. Kibermakon tushunchasi va uning falsafiy-huquqiy talqini.....	26
1.2. Kibermakon xavfsizlik paradigmasi va ilmiy konsepsiyalar.....	35
1.3. Zamonaviy kiberxavf va tahdidlarning turlari: kiberterrorizm, kiberjinoyat va kiberpropaganda	42
1.4. Sun'iy intellekt va kibermakon xavfsizligi: yangi xavf va imkoniyatlar.....	48
II-BOB. XALQARO DAVLATLAR TAJRIBASI.....	58
2.1. AQSh tajribasi: kiberxavfsizlik siyosati, huquqiy asoslari va strategiyasi.....	60
2.2. Yevropa Ittifoqi: GDPR va xalqaro standartlar asosida xavfsizlikni ta'minlash.....	70
2.3. Rossiya Federatsiyasi: milliy xavfsizlik konsepsiyasi va kibermakonni nazorat qilish yondashuvlari	77
2.4. Xitoy Xalq Respublikasi: davlat nazorati va milliy modelning xususiyatlari.....	83
2.5. Janubiy Koreya va Yaponiya: texnologik taraqqiyot va kiberxavfsizlik integratsiyasi.....	88
III-BOB. MINTAQAVIY TAJRIBA VA O'ZBEKISTON	96
3.1. Markaziy Osiyo davlatlarida kibermakon xavfsizligi: umumiy muammolar va imkoniyatlar	97
3.2. O'zbekiston Respublikasida kibermakon xavfsizligini ta'minlashning huquqiy asoslari	107
3.3. O'zbekistonning milliy strategiyasi va xalqaro hamkorlikdagi ishtiroki.....	116
IV-BOB. GLOBAL HAMKORLIK VA KELAJAK ISTIQBOLLARI	140
4.1. Davlatlararo hamkorlik: BMT, NATO, SCO va boshqa tashkilotlarning roli	141

4.2. Kiberxavfsizlikda axborot etikasi va inson huquqlarini himoya qilish.....	152
4.3. Kiberxavfsizlikning kelajak paradigmalari va global boshqaruv muammolari.....	159
XULOSA.....	170
FOYDALANILGAN ADABIYOTLAR.....	179

BERKINOV OYBEK TOXIR O'G'LI

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

Monografiya

Muharrir: X. Tahirov

Texnik muharrir: S. Meliqo'ziyeva

Musaxxih: M. Yunusova

Sahifalovchi: A. Muxammad

Nashr. lits № 2244. 25.08.2020.

Bosishga ruxsat etildi 13.11.2025.

Bichimi 60x84 1/16. Ofset qog'ozi.

“Times New Roman” garniturası.

Xisob-nashr tabogi. 11,5.

Adadi 100 dona. Buyurtma № 68.

«Sarbon LLS» MChJ bosmaxonasida chop etildi.

**Nashriyot tel. raqami +998 (97) 017-01-01
+998 (94) 673-66-56**

QAYDLAR UCHUN