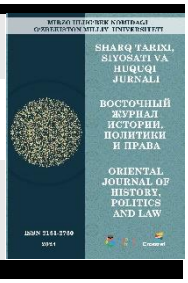
DOI: https://doi.org/10.37547/supsci-ojhpl-06-09-29 **Pages: 259-271**

Oriental Journal of History, Politics and Law

SUPPORT SCIENCE

ORIENTAL JOURNAL OF HISTORY, POLITICS AND LAW

journal homepage:
https://www.supportscience.uz/index.php/ojhpl



PRIORITY AREAS AND PROSPECTS FOR STRENGTHENING CYBERSECURITY IN NEW UZBEKISTAN

Shukurullo Khamidov
Farg'ona davlat universiteti tadqiqotchisi
shukurulloxamidov2695@gmail.com
Science ID: MFR-0526-0026
Fergana, Uzbekistan

ABOUT ARTICLE

Key words: cybersecurity, New Uzbekistan, digital transformation, information society, information security, national security.

Received: 09.09.26
Accepted: 10.09.26
Published: 11.09.26

Abstract: This article examines the priority directions and prospects of strengthening cybersecurity in New Uzbekistan from a socio-philosophical perspective. The study aims to provide scientific grounding for cybersecurity within the context of harmonizing the interests of the state, society, and the individual. The methodological framework relies on systemic-structural and comparative-historical methods together with content analysis of normative-legal documents and theoretical sources. The results reveal the legal, socio-philosophical, cultural, and institutional dimensions of cybersecurity. The conclusion assesses strengthening cybersecurity as a strategic task requiring harmonious cooperation among the state, society, and the individual.

YANGI O'ZBEKISTONDA KIBERXAVFSIZLIKNI MUSTAHKAMLASHNING USTUVOR YO'NALISHLARI VA ISTIQBOLLARI

Shukurullo Xamidov
Farg'ona davlat universiteti tadqiqotchisi
shukurulloxamidov2695@gmail.com
Ilmiy identifikatsiya raqami: MFR-0526-0026
Farg'ona, O'zbekiston

MAQOLA HAQIDA

Kalit so'zlar: kiberxavfsizlik, Yangi O'zbekiston, raqamli transformatsiya,

Annotatsiya: Mazkur maqolada Yangi O'zbekistonda kiberxavfsizlikni

axborotlashgan jamiyat, axborot xavfsizligi, milliy xavfsizlik.

mustahkamlashning ustuvor yo‘nalishlari ijtimoiy-falsafiy nuqtai nazardan tahlil qilingan. Tadqiqotning maqsadi kiberxavfsizlikni davlat, jamiyat va shaxs manfaatlari uyg‘unligi kontekstida ilmiy asoslashdan iborat. Metodologik asos sifatida tizimli-strukturaviy, qiyosiy-tarixiy va kontent-tahlil metodlaridan foydalanilgan holda normativ-huquqiy hujjatlar va nazariy manbalar tahlil qilindi. Natijalar kiberxavfsizlikning huquqiy, ijtimoiy-falsafiy, madaniy va institutsional jihatlarini ochib berdi va uni davlat, jamiyat hamda shaxs manfaatlari uyg‘unligini ta’minlovchi strategik vazifa sifatida baholash zarurligini asoslab berdi.

ПРИОРИТЕТНЫЕ НАПРАВЛЕНИЯ И ПЕРСПЕКТИВЫ УКРЕПЛЕНИЯ КИБЕРБЕЗОПАСНОСТИ В НОВОМ УЗБЕКИСТАНЕ

Шукурилло Хамидов
Исследователь Ферганского государственного университета
shukurulloxamidov2695@gmail.com
Научный идентификационный номер: MFR-0526-0026
Фергана, Узбекистан

О СТАТЬЕ

Ключевые слова: кибербезопасность, Новый Узбекистан, цифровая трансформация, информационное общество, информационная безопасность, национальная безопасность.

Аннотация: В данной статье приоритетные направления и перспективы укрепления кибербезопасности в Новом Узбекистане рассматриваются с социально-философской точки зрения. Целью исследования является научное обоснование кибербезопасности в контексте гармонии интересов государства, общества и личности. В качестве методологической основы использованы системно-структурный, сравнительно-исторический методы и контент-анализ нормативно-правовых документов и теоретических источников. Результаты раскрывают правовые, социально-философские, культурные и институциональные аспекты кибербезопасности. В заключение делается вывод, что укрепление кибербезопасности оценивается как стратегическая задача, требующая гармоничного сотрудничества государства, общества и личности.

Kirish. XXI asr axborot-kommunikatsiya inqilobi insoniyat tamaddunini yangi bosqichga olib chiqdi va jamiyat taraqqiyotining barcha jabhalarini tubdan o‘zgartirmoqda. Zamonaviy dunyoda axborot va bilim nafaqat ijtimoiy munosabatlarning, balki iqtisodiy raqobatning ham asosiy resursiga aylandi. Daniel Bell postindustrial jamiyat nazariyasida bilim va axborotning ishlab chiqarish vositalaridan ustunlik qiluvchi omilga aylanishini asoslab bergan bo‘lsa,[4] Manuel Kastels tarmoq jamiyati kontseptsiyasida axborot-kommunikatsiya texnologiyalarining ijtimoiy tuzilmani tubdan qayta shakllantiruvchi kuchga ega ekanligini ko‘rsatib bergan edi.[5] Ushbu nazariy yondashuvlar zamonaviy davlatlarning raqobatbardoshligi bevosita ularning raqamli salohiyati bilan bog‘liqligini tasdiqlaydi. Shu nuqtai nazardan O‘zbekiston ham jahon hamjamiyati qatorida raqamli transformatsiya jarayonlariga faol kirishmoqda. Yangi O‘zbekistonda amalga oshirilayotgan keng ko‘lamli islohotlar doirasida raqamli iqtisodiyotni rivojlantirish, elektron hukumat tizimini takomillashtirish, sun’iy intellekt texnologiyalarini joriy etish va zamonaviy axborot infratuzilmasini yaratish ustuvor vazifalar sifatida belgilangan. Mazkur jarayonlar davlat boshqaruvi samaradorligini oshirish, aholiga qulay elektron xizmatlar ko‘rsatish hamda iqtisodiy taraqqiyotni jadallashtirish uchun keng imkoniyatlar yaratmoqda. Biroq raqamli texnologiyalarning jadal sur’atlarda joriy etilishi bilan bir qatorda kiber tahdidlar, ma’lumot va tizimlarga qaratilgan ruxsatsiz ta’sirlar (axborot xurujlari), kiberjinoyatchilik ko‘rinishlari va shaxsiy ma’lumotlar xavfsizligiga oid muammolar ham tobora dolzarblashib bormoqda. Elvin Toffler o‘zining “uchinchi to‘lqin” nazariyasida jamiyatning industrial bosqichdan axborot bosqichiga o‘tishi nafaqat yangi imkoniyatlar, balki yangi turdagi ijtimoiy zaifliklarni ham keltirib chiqarishini alohida ta’kidlagan edi.[6] Ana shu ziddiyatli holat — raqamlashtirishning ijobiy salohiyati va undan kelib chiqadigan yangi xavf-xatarlar o‘rtasidagi dialektik bog‘liqlik — kiberxavfsizlik muammosini nafaqat texnik, balki ijtimoiy-falsafiy tahlil predmetiga ham aylantiradi. Chunki kiberxavfsizlik, mohiyatan, texnologik hodisa bo‘lishi bilan birga, insonning raqamli muhitdagi xulq-atvori, qadriyatlar tizimi va ijtimoiy mas’uliyati bilan chambarchas bog‘liq murakkab ijtimoiy hodisadir. Mazkur muammoning ko‘p qirraliligi uni yaxlit ilmiy-falsafiy nuqtai nazardan tahlil qilishni obyektiv zaruratga aylantiradi. Bundan tashqari, raqamli iqtisodiyotning jadal rivojlanishi elektron tijorat, masofaviy bank xizmatlari va davlat xizmatlarining raqamli platformalarga faol ko‘chish jarayonini tezlashtirmoqda, bu esa fuqarolarning shaxsiy va moliyaviy ma’lumotlari xavfsizligini ta’minlash zaruratini yanada kuchaytirmoqda. Xalqaro tajriba shuni ko‘rsatadiki, raqamli transformatsiya sur’ati bilan kiberxavfsizlik salohiyati o‘rtasidagi nomutanosiblik ko‘plab mamlakatlarda jiddiy institutsional

muammolarga sabab bo‘lmoqda, shu bois O‘zbekiston ushbu jarayonlarni parallel va muvozanatli tarzda olib borishga alohida e’tibor qaratmoqda.

Bugungi kunda kiberxavfsizlik masalasi milliy xavfsizlikning ajralmas tarkibiy qismi sifatida namoyon bo‘lmoqda. Davlat boshqaruvi, moliya-bank tizimi, transport, energetika, sog‘liqni saqlash va ta’lim sohalarining barchasi bosqichma-bosqich raqamlashtirilishi natijasida ularning kiber makonga bog‘liqligi tobora kuchaymoqda. Bu esa, o‘z navbatida, kiber tahdidlarning oldini olish, axborot resurslarini himoya qilish va xavfsiz raqamli muhitni shakllantirish masalasini strategik ahamiyat kasb etuvchi vazifaga aylantirmoqda. Ulrix Bek o‘zining “xavf-xatar jamiyati” nazariyasida zamonaviy jamiyatning rivojlanishi yangi turdagi, ko‘pincha ko‘zga ko‘rinmas va global xarakterga ega xavflarni keltirib chiqarishini asoslab bergan edi; kiber tahdidlar aynan shunday xavflar toifasiga mansub bo‘lib, ular an’anaviy davlat chegaralarini tanimaydi va butun ijtimoiy tizimga ta’sir ko‘rsatish salohiyatiga ega.[9] Shu bois 2022–2026-yillarga mo‘ljallangan Yangi O‘zbekistonning taraqqiyot strategiyasida (Prezidentning 2022-yil 28-yanvardagi PF-60-son Farmoni) raqamli texnologiyalarni rivojlantirish, axborot xavfsizligini ta’minlash va milliy kiberxavfsizlik tizimini takomillashtirish ustuvor vazifalar qatorida belgilangan.[1] Mazkur ilmiy tadqiqotning maqsadi — Yangi O‘zbekistonda kiberxavfsizlikni mustahkamlashning ustuvor yo‘nalishlari va istiqbollarini ijtimoiy-falsafiy nuqtai nazardan tahlil qilish, ushbu jarayonning davlat, jamiyat va shaxs manfaatlari uyg‘unligi kontekstidagi o‘rnini aniqlash hamda kelgusi rivojlanish tendensiyalarini ilmiy asoslashdan iborat. Tadqiqot vazifalari quyidagilardan iborat:

birinchidan, kiberxavfsizlikning ijtimoiy-falsafiy mohiyatini axborotlashgan jamiyat nazariyalari asosida ochib berish;

ikkinchidan, O‘zbekistonda kiberxavfsizlikni ta’minlashning normativ-huquqiy asoslarini tahlil qilish;

uchinchidan, kiberxavfsizlik madaniyatini shakllantirishda inson omilining o‘rnini aniqlash;

to‘rtinchidan, davlat, fuqarolik jamiyati va ta’lim institutlarining hamkorlik modelini tavsiflash;

beshinchidan, kelgusi rivojlanishning ustuvor yo‘nalishlarini ishlab chiqish.

Tadqiqotning ilmiy yangiligi shundaki, unda kiberxavfsizlik muammosi Yangi O‘zbekistonning taraqqiyot strategiyasi kontekstida yaxlit ijtimoiy-falsafiy tizim sifatida, ya’ni huquqiy, institutsional va ma’naviy-madaniy jihatlarning uzviy birligida ko‘rib chiqiladi. Tadqiqotning nazariy ahamiyati kiberxavfsizlik muammosini axborotlashgan jamiyat va xavf-xatar jamiyati kontseptsiyalari asosida yaxlit kontseptual modelga birlashtirishda namoyon

bo‘ladi. Tadqiqotning amaliy ahamiyati esa uning natijalaridan davlat organlari, ta’lim muassasalari hamda fuqarolik jamiyati institutlari faoliyatida foydalanish mumkinligi bilan belgilanadi. Shuningdek, tadqiqot doirasida gipoteza sifatida quyidagi taxmin ilgari surildi: kiberxavfsizlikning barqaror tizimi faqat huquqiy-institutsional choralar orqali emas, balki jamiyatda maxsus kiberxavfsizlik madaniyatini shakllantirish orqaligina samarali natija berishi mumkin. Ushbu gipoteza tadqiqot davomida to‘plangan normativ va nazariy manbalar asosida tekshirildi.

Materiallar va metodlar. Tadqiqotning metodologik asosini ijtimoiy-falsafiy tahlilning tizimli-strukturaviy yondashuvi tashkil etadi,[15] bu yondashuv kiberxavfsizlik hodisasini alohida texnik muammo sifatida emas, balki davlat, jamiyat va shaxs manfaatlarining o‘zaro bog‘liq tizimi doirasida o‘rganish imkonini beradi. Tadqiqot obyekti sifatida Yangi O‘zbekistonda kiberxavfsizlikni mustahkamlashga qaratilgan ijtimoiy-siyosiy jarayonlar, tadqiqot predmeti sifatida esa ushbu jarayonlarning ijtimoiy-falsafiy jihatlari, ya’ni ularning qadriyatlar tizimi, institutsional munosabatlar va inson omili bilan bog‘liqligi belgilab olindi.

Empirik-normativ manba bazasini O‘zbekiston Respublikasining 2022-yil 15-apreldagi ЎРҚ-764-son “Kiberxavfsizlik to‘g‘risida”gi Qonuni,[3] 2020-yil 5-oktabrdagi PF-6079-son “Raqamli O‘zbekiston — 2030” strategiyasi to‘g‘risidagi Farmoni[2] hamda tegishli davlat dasturlari tashkil etdi. Nazariy-kontseptual manba bazasiga esa axborotlashgan jamiyat nazariyotchilari — Daniel Bell, Manuel Kastels, Elvin Toffler, Entoni Giddens, Zigmunt Bauman va Ulrix Bekning fundamental asarlari, shuningdek mahalliy faylasuflarning ushbu muammoga bag‘ishlangan tadqiqotlari kiritildi. Xalqaro tashkilotlarning tegishli hisobotlari, xususan Xalqaro elektraloqa ittifoqining Global kiberxavfsizlik indeksi[12] hamda Yevropa Ittifoqi Kiberxavfsizlik agentligining tahdidlar landshafti bo‘yicha hisoboti[13] qiyosiy tahlil uchun qo‘shimcha manba sifatida jalb qilindi. Manbalarni tanlashda ularning ilmiy dolzarbligi, rasmiy maqomi va tadqiqot mavzusiga bevosita aloqadorligi mezon sifatida qo‘llanildi, bu esa tahlil natijalarining ishonchliligini ta’minlashga xizmat qildi. Ushbu tadqiqotda “kiberxavfsizlik” tushunchasi asosan raqamli infratuzilma, tizim va tarmoqlarni ruxsatsiz ta’sirlardan texnik-institutsional himoya qilish jarayoni sifatida, “axborot xavfsizligi” esa kengroq — axborotning maxfiyligi, yaxlitligi va foydalanuvchanligini ta’minlovchi tushuncha sifatida farqlanadi; “raqamli xavfsizlik” mazkur ikki tushunchani birlashtiruvchi umumiyroq kategoriya sifatida qo‘llanildi. Tadqiqot mavhum falsafiy mulohaza yuritishdan emas, balki aniq normativ-huquqiy va institutsional ma’lumotlarni ijtimoiy-falsafiy tafakkur prizmasidan o‘tkazib tahlil qilishdan iborat bo‘lgan aralash-kontseptual dizaynga asoslandi. Bu, o‘z navbatida, olingan xulosalarning nazariy asoslanganligi bilan bir qatorda amaliy dolzarbligini ham ta’minlashga xizmat qildi. Tadqiqot uch bosqichda — manbalarni yig‘ish va

tizimlashtirish, ularni tahlil qilish hamda natijalarni umumlashtirish va kontseptuallashtirish tartibida amalga oshirildi. Manbalarni tanlashda so‘nggi o‘n yil ichida nashr etilgan yoki qabul qilingan hujjatlarga ustuvorlik berildi, bundan tadqiqotning nazariy-kontseptual asosini tashkil etuvchi klassik falsafiy-sotsiologik manbalar (Bell, Toffler, Giddens, Bauman, Bek asarlari) mustasno, chunki ular sohaning fundamental nazariy tushunchalarini ifodalaydi, bu esa tahlilning dolzarbligini ta’minladi.

Tadqiqot jarayonida bir qator ilmiy metodlardan kompleks tarzda foydalanildi. Qiyosiy-tarixiy metod yordamida O‘zbekistonda kiberxavfsizlik sohasidagi institutsional rivojlanish bosqichlari xalqaro tajriba bilan qiyoslangan holda o‘rganildi, bu esa milliy modelning o‘ziga xos va umumiy jihatlarini ajratib ko‘rsatish imkonini berdi. Kontent-tahlil metodi normativ-huquqiy hujjatlar, xususan “Kiberxavfsizlik to‘g‘risida”gi Qonun va “Raqamli O‘zbekiston — 2030’ strategiyasining matnini tizimli tahlil qilish, ulardagi ustuvor yo‘nalishlarni aniqlash uchun qo‘llanildi. Sintez va abstraktlashtirish metodlari turli manbalardan olingan nazariy va empirik ma’lumotlarni yaxlit kontseptual modelga birlashtirish imkonini berdi. Deduktiv-induktiv mulohaza yuritish usuli umumiy nazariy qoidalardan (axborotlashgan jamiyat, xavf-xatar jamiyati kontseptsiyalari) O‘zbekiston sharoitidagi xususiy xulosalarga o‘tishda, shuningdek amaliy kuzatishlardan umumlashtirilgan tendensiyalarni chiqarishda qo‘llanildi. Institutsional tahlil metodi davlat, fuqarolik jamiyati va ta’lim institutlarining kiberxavfsizlikni ta’minlashdagi o‘zaro munosabatlarini o‘rganishga xizmat qildi. Terminologik tahlil metodi esa “kiberxavfsizlik”, “raqamli madaniyat” va “axborot xavfsizligi” kabi tayanch tushunchalarning ijtimoiy-falsafiy mazmunini aniqlashtirishda qo‘llanildi. Tadqiqotning metodologik cheklovlari sifatida shuni ta’kidlash lozimki, mazkur ish empirik-sotsiologik so‘rovnoma yoki statistik model yaratishga emas, balki mavjud normativ va nazariy manbalarning ikkilamchi tahliliga asoslangan kontseptual-nazariy tadqiqot xarakteriga ega. Shu sababli olingan natijalar miqdoriy ko‘rsatkichlar emas, balki sifat jihatidan umumlashtirilgan ilmiy-nazariy xulosalar shaklida taqdim etiladi. Kelgusi tadqiqotlarda ushbu kontseptual modelni empirik so‘rovnoma ma’lumotlari, xususan fuqarolarning raqamli xavfsizlik xatti-harakatlarini o‘rganuvchi sotsiologik tadqiqotlar bilan boyitish istiqbolli yo‘nalish sifatida belgilab qo‘yildi. Tahlil jarayonida olingan barcha xulosalar manba-triangulyatsiyasi tamoyili asosida, ya’ni normativ-huquqiy hujjatlar, nazariy-falsafiy adabiyotlar va xalqaro tashkilotlar hisobotlaridan olingan ma’lumotlarni bir-biri bilan qiyoslash yo‘li bilan bir necha manba orqali o‘zaro tekshirilib, faqat takroran tasdiqlangan qarashlar yakuniy natijalar tarkibiga kiritildi, bu esa tadqiqotning ilmiy obyektivligini oshirishga xizmat qildi.

Natijalar. Normativ-huquqiy hujjatlarni tahlil qilish natijasida O‘zbekistonda kiberxavfsizlikni ta’minlashning institutsional-huquqiy asosi izchil shakllantirilayotgani kuzatildi.

“Raqamli O‘zbekiston — 2030” strategiyasi mamlakat iqtisodiyoti va ijtimoiy hayotining barcha sohalarini raqamlashtirishni nazarda tutadi, bu esa kiberxavfsizlik darajasini strategiyaning muvaffaqiyatli amalga oshirilishini belgilovchi asosiy shartlardan biriga aylantiradi. Chunki elektron hukumat tizimlari, davlat axborot resurslari va raqamli xizmatlarning barqaror faoliyati ishonchli himoya mexanizmlarisiz mumkin emas. Tahlil shuni ko‘rsatadiki, “Kiberxavfsizlik to‘g‘risida”gi Qonunning qabul qilinishi mamlakatda ushbu sohani tartibga solishning muhim huquqiy poydevorini yaratdi, unda davlat organlari, tashkilotlar va fuqarolarning kiberxavfsizlik sohasidagi huquq va majburiyatlari aniq belgilab berildi. Shuningdek, muhim axborot infratuzilmasi obyektlarini himoya qilish, kiber hodisalarni monitoring qilish hamda ularga tezkor javob qaytarish tizimlarini yaratishga qaratilgan amaliy choralar ko‘rilayotgani kuzatildi. Bu institutsional yondashuv Xalqaro elektraloqa ittifoqining Global kiberxavfsizlik indeksi (GCI) 2024 metodologiyasidagi besh asosiy ustunga — huquqiy, texnik, tashkiliy, salohiyatni oshirish va hamkorlik o‘lchamlariga — mos kelishini ko‘rsatadi; xususan, GCI 2024 hisobotiga ko‘ra O‘zbekiston 100 balldan 89,2 ball to‘plab, T2 — “Advancing” (faol rivojlanayotgan) toifasiga kiritilgan (2020-yilgi 71,11 balldan o‘sish),[12] bu esa institutsional yondashuvning xalqaro amaliyot bilan muayyan darajada uyg‘unligini tasdiqlaydi. Shu bilan birga, tahlil normativ bazaning mavjudligi o‘zi kifoya emasligini, uning amaliyotda samarali qo‘llanilishi va muntazam yangilanib borishi zarurligini ham ko‘rsatdi, chunki kiber tahdidlarning tabiati doimiy o‘zgaruvchan xarakterga ega bo‘lib, huquqiy tartibga solish shu dinamikaga hamqadam bo‘lishi lozim. Shuningdek, tahlil davlat dasturlarida kiberxavfsizlik bo‘yicha maqsadli ko‘rsatkichlarning izchil belgilanishi ularning bajarilishini nazorat qilish mexanizmlarini ham talab etishini ko‘rsatdi, aks holda normativ-huquqiy hujjatlarning deklarativ xususiyat kasb etish xavfi saqlanib qoladi. Bundan tashqari, davlat organlari o‘rtasida kiber hodisalar yuzasidan axborot almashish tartibining takomillashtirilishi ham institutsional tizimning muhim yutug‘i sifatida baholandi, chunki tezkor axborot almashinuvi kiber tahdidlarga birlashgan javob berish imkonini yaratadi.

Ijtimoiy-falsafiy tahlil natijasida kiberxavfsizlikning iqtisodiy xavfsizlik, siyosiy barqarorlik va ma’naviy taraqqiyot bilan uzviy dialektik bog‘liqligi yana bir bor tasdiqlandi. Tahlil shuni ko‘rsatadiki, raqamli tizimlarning ishonchli faoliyati jamiyatdagi ijtimoiy munosabatlarning barqarorligini ta’minlovchi muhim omil hisoblanadi, aksincha, kiber tahdidlar iqtisodiy yo‘qotishlar, axborot manipulyatsiyasi va ijtimoiy beqarorlikka sabab bo‘lishi mumkin. Bu xulosa Ulrix Bekning xavf-xatar jamiyati kontseptsiyasi bilan uyg‘un bo‘lib, unga ko‘ra zamonaviy jamiyat rivojlanishi bilan bog‘liq xavflar nafaqat texnik, balki chuqur ijtimoiy-institutsional oqibatlarga ham ega bo‘ladi. Tahlil shuni ko‘rsatdiki, zamonaviy davlatning raqobatbardoshligi endilikda nafaqat iqtisodiy yoki harbiy salohiyat bilan, balki uning axborot resurslarini ishonchli

himoya qilish qobiliyati bilan ham belgilanadi, bu esa kiberxavfsizlikni milliy rivojlanish siyosatining ajralmas tarkibiy qismiga aylantirmoqda. Shuningdek, Entoni Giddensning “modernlik oqibatlari” nazariyasidagi ishonch va xavf-xatar o‘rtasidagi dialektik munosabat g‘oyasini tasdiqlaydi: raqamli institutlarga bo‘lgan ijtimoiy ishonch faqat ularning xavfsizligi kafolatlanganda barqaror bo‘lib qoladi.[7] Zigmunt Baumanning “suyuq modernlik” kontseptsiyasi nuqtai nazaridan qaraganda, raqamli makonning beqaror va tez o‘zgaruvchan tabiati kiberxavfsizlikni statik emas, balki doimiy moslashuvchan jarayon sifatida talqin qilishni taqozo etadi.[8] Shu bilan birga, tahlil kiberxavfsizlik va ma’naviy taraqqiyot o‘rtasidagi bog‘liqlikni ham ochib berdi: axborot xurujlari — ya’ni axborot tizimlariga yoki jamoatchilik ongiga qaratilgan ruxsatsiz, maqsadli ta’sir ko‘rsatish harakatlari — ko‘pincha nafaqat texnik tizimlarga, balki jamoatchilik ongiga, milliy qadriyatlarga va ijtimoiy ishonchga ham qaratilishi mumkin, bu esa kiberxavfsizlikni jamiyatning ma’naviy-madaniy barqarorligi va milliy qadriyatlar tizimini himoya qilish jarayoni sifatida talqin qilinadigan ma’naviy xavfsizlik bilan uzviy bog‘liq hodisaga aylantiradi. Shu tariqa, tadqiqot natijalari kiberxavfsizlikni faqat texnik-muhandislik muammosi emas, balki jamiyatning ma’naviy-institutsional barqarorligini belgilovchi strategik ijtimoiy-falsafiy kategoriya sifatida baholash zarurligini asoslab berdi. Shu bilan birga, kiberxavfsizlikni ta’minlashda ortiqcha nazorat choralarining shaxsiy erkinliklarga ta’sirini muvozanatlash masalasi ham ijtimoiy-falsafiy tahlilning muhim yo‘nalishi sifatida aniqlandi; bu masala zamonaviy demokratik davlatlar amaliyotida keng muhokama qilinayotgan xavfsizlik va erkinlik o‘rtasidagi muvozanat muammosi bilan bog‘liq bo‘lib, uning aniq nisbati har bir mamlakatning o‘ziga xos ijtimoiy-huquqiy konteksti asosida belgilanadi.

Tahlil natijalari kiberxavfsizlikni ta’minlashda texnologik vositalar bilan bir qatorda inson omilining hal qiluvchi ahamiyatga ega ekanligini yana bir bor ko‘rsatdi. Xalqaro tadqiqotlar shuni ko‘rsatadiki, kiber insidentlarning muhim qismi inson omili, jumladan axborot xavfsizligi qoidalariga rioya qilmaslik bilan bog‘liq bo‘lishi mumkin, texnik nosozliklar esa nisbatan kamroq uchraydigan sabab sifatida qayd etiladi.[10] Shu sababli Yangi O‘zbekistonda kiberxavfsizlik madaniyatini shakllantirish ustuvor ijtimoiy vazifalardan biri sifatida belgilandi. Tadqiqot doirasida “kiberxavfsizlik madaniyati” tushunchasi fuqarolarning axborot bilan ishlash, raqamli texnologiyalardan foydalanish hamda kiber tahdidlarga nisbatan mas’uliyatli munosabatda bo‘lish ko‘nikmalari majmuasi sifatida kontseptuallashtirildi. Ijtimoiy-falsafiy jihatdan bu madaniyat axborotlashgan jamiyatning ma’naviy asoslaridan biri sifatida namoyon bo‘ladi, chunki axborot xavfsizligi nafaqat texnik himoya vositalari, balki insonlarning ongli faoliyati va mas’uliyatli xulq-atvori bilan ham ta’minlanadi. Tahlil shuni ko‘rsatdiki, bugungi kunda yoshlar internet va ijtimoiy tarmoqlarning eng faol foydalanuvchilari hisoblanadi, shu bois ta’lim tizimida raqamli

savodxonlik va axborot madaniyatini rivojlantirishga alohida e’tibor qaratish zarurati mavjud. Yevropa Kengashining raqamli fuqarolik ta’limi bo‘yicha qo‘llanmasida ta’kidlanganidek, raqamli kompetentlik nafaqat texnik ko‘nikmalarni, balki tanqidiy fikrlash, axborotni tanqidiy baholash va onlayn muhitda axloqiy mas’uliyatni ham o‘z ichiga oladi.[11] Shu nuqtai nazardan, maktablar, oliy ta’lim muassasalari va ilmiy-tadqiqot markazlarining ushbu jarayondagi faol ishtiroki kiberxavfsizlik madaniyatini keng jamoatchilik miqyosida shakllantirishning muhim sharti sifatida belgilandi. Shuningdek, oilaviy tarbiya va mahalla institutining raqamli savodxonlikni oshirishdagi o‘rni ham inkor etib bo‘lmaydigan ahamiyatga ega ekanligi, chunki kiberxavfsizlik madaniyati faqat rasmiy ta’lim orqali emas, balki kundalik ijtimoiy muhit orqali ham shakllanishi tahlil davomida yana bir bor ta’kidlandi.

Institutsional tahlil natijasida kiberxavfsizlikning barqaror tizimi davlat, jamiyat va shaxs manfaatlari uyg‘unligiga asoslangan tadqiqot muallifi tomonidan taklif etilayotgan uch tomonlama hamkorlik modeliga tayanishi lozimligi xulosa qilindi. Zamonaviy demokratik jamiyatda axborot xavfsizligini ta’minlash birgina davlatning vazifasi bo‘lmay, balki barcha ijtimoiy institutlarning umumiy mas’uliyati ekanligi ta’kidlandi. Tahlil natijalariga ko‘ra, davlat ushbu tizimda normativ-huquqiy bazani yaratish va muhim infratuzilmalarni himoya qilish funksiyasini bajaradi; fuqarolik jamiyati institutlari axborot madaniyatini rivojlantirish va jamoatchilik nazoratini amalga oshirish vazifasini o‘z zimmasiga oladi; ta’lim tizimi esa fuqarolarning raqamli kompetensiyalarini shakllantirish vazifasini bajaradi. Ushbu uchta institutning o‘zaro uyg‘un hamkorligi kiberxavfsizlikning samarali va barqaror modelini yaratishning zaruriy sharti sifatida belgilandi. Yevropa Ittifoqi Kiberxavfsizlik agentligining tahdidlar landshafti bo‘yicha hisobotida ham ko‘p tomonlama hamkorlik modelining samaradorligi ta’kidlangani inobatga olinadi,[13] bu esa O‘zbekiston tajribasining xalqaro amaliyot bilan muayyan darajada uyg‘unligini ko‘rsatadi. Tahlil, shuningdek, Yangi O‘zbekistonda amalga oshirilayotgan islohotlarning aynan mana shu integratsion yondashuvga asoslanayotganini, ya’ni davlat, biznes sektori, ilmiy-ta’lim muassasalari va fuqarolik jamiyati institutlarining hamkorligi kiberxavfsizlikning barqaror tizimini shakllantirish uchun muhim shart sifatida ko‘rilayotganini ko‘rsatdi. Bu natija axborotlashgan jamiyatda davlat, fuqarolik jamiyati va ta’lim institutlarining hamkorligi kiberxavfsizlikning muhim omili ekanligini ko‘rsatadigan zamonaviy ilmiy qarashlar bilan hamohang ekanligini yana bir bor tasdiqladi. Shu bilan birga, xususiy sektor, xususan raqamli xizmatlar va moliyaviy texnologiyalar sohasidagi kompaniyalarning ushbu uch tomonlama modelga to‘rtinchi institutsional bo‘g‘in sifatida qo‘shilishi zarurligi ham tahlil davomida alohida ta’kidlab o‘tildi, bu — davlat-xususiy sheriklik nazariyasida keng qo‘llaniladigan yondashuvga mos ravishda — aynan xususiy sektor raqamli infratuzilmaning katta qismini boshqarishi bilan

izohlanadi. Bundan tashqari, mintaqaviy va mahalliy darajadagi davlat organlarining kiberxavfsizlik siyosatini amalga oshirishdagi roli ham markaziy institutlar bilan bir qatorda muhim ahamiyat kasb etishi, chunki kiber tahdidlarning oldini olish ko‘p jihatdan mahalliy darajadagi tayyorgarlikka bog‘liqligi tahlil natijasida kuzatildi.

Muhokama. Olingan natijalarni umumlashtirish shuni ko‘rsatadiki, Yangi O‘zbekistonda kiberxavfsizlikni mustahkamlash jarayoni nazariy jihatdan axborotlashgan jamiyat va xavf-xatar jamiyati kontseptsiyalarining amaliy tasdig‘i sifatida talqin qilinishi mumkin. Bell va Kastelsning axborot resurslari zamonaviy taraqqiyotning asosiy omili ekanligi haqidagi qarashlari, Bekning xavf-xatarlarning global va institutsional xususiyatga ega ekanligi haqidagi kontseptsiyasi bilan uyg‘unlashib, kiberxavfsizlikni yaxlit ijtimoiy-falsafiy tizim sifatida tushunish uchun mustahkam nazariy asos yaratadi. Shu bilan birga, tadqiqot natijalarini xalqaro tajriba bilan qiyoslash O‘zbekiston modelining o‘ziga xos xususiyatlarini ham ochib berdi. Xususan, ko‘plab rivojlangan davlatlarda kiberxavfsizlik siyosati asosan texnik-institutsional yo‘nalishga tayangan bo‘lsa, O‘zbekiston tajribasida raqamli madaniyat va ma’naviy-axloqiy tarbiya masalalariga alohida urg‘u berilishi milliy ta’lim-tarbiya an’analari bilan bog‘liq o‘ziga xoslikni namoyon etadi, biroq bu xulosa hozircha umumlashtiruvchi kuzatish darajasida bo‘lib, uni tasdiqlovchi qiyosiy-institutsional manba sifatida mahalliy falsafiy adabiyot[14] bilvosita dalil vazifasini o‘taydi. Bu holat kiberxavfsizlik muammosini universal texnik yechim sifatida emas, balki har bir mamlakatning ijtimoiy-madaniy konteksti bilan uyg‘un holda shakllantirilishi zarur bo‘lgan murakkab ijtimoiy jarayon sifatida talqin qilish zarurligini ko‘rsatadi. Ayni paytda, tahlil natijalari ba’zi cheklovlarni ham ochib berdi: normativ-huquqiy bazaning mavjudligi amaliy natijadorlikning avtomatik kafolati emas, balki uning ijrosi, monitoringi va davriy yangilanishi alohida institutsional mexanizmlarni talab etadi. Bundan tashqari, tadqiqot davomida aniqlanishicha, kiberxavfsizlik siyosatini shakllantirishda nazariy-kontseptual yondashuv bilan amaliy-texnik yondashuv o‘rtasidagi muvozanatni saqlash muhim metodologik muammo bo‘lib qolmoqda, chunki ortiqcha texnokratik yondashuv inson omilini, ortiqcha falsafiy-mavhum yondashuv esa amaliy samaradorlikni e’tibordan chetda qoldirishi mumkin; mazkur tadqiqot aynan ushbu ikki yondashuv o‘rtasida muvozanat saqlashga — normativ-huquqiy tahlilni ijtimoiy-falsafiy talqin bilan uyg‘unlashtirishga — harakat qildi. Shu bois kelgusi tadqiqotlarda ushbu normativ mexanizmlarning amaliy samaradorligini baholovchi empirik ko‘rsatkichlarni ishlab chiqish dolzarb vazifa bo‘lib qolmoqda.

Tadqiqot natijalari asosida kelajakda O‘zbekistonda kiberxavfsizlikni mustahkamlashning bir qator ustuvor yo‘nalishlarini belgilash mumkin. Birinchidan, sun’iy intellekt texnologiyalaridan foydalangan holda kiber tahdidlarni aniqlash va prognozlash tizimlarini

rivojlantirish zarur, bu tahdidlarga tezkor javob berish imkoniyatlarini sezilarli darajada kengaytiradi;

shu bilan birga, bunday tizimlarni joriy etishda ma’lumotlar maxfiyligi, algoritmik xatolik (noto‘g‘ri signalizatsiya) xavfi va ushbu texnologiyalarni suiiste’mol qilish ehtimoli kabi cheklovlar ham alohida hisobga olinishi lozim.

Ikkinchidan, milliy kiberxavfsizlik sohasida malakali kadrlar tayyorlash tizimini takomillashtirish, oliy ta’lim muassasalarida zamonaviy kiberxavfsizlik mutaxassisliklarini rivojlantirish dolzarb vazifa hisoblanadi. Uchinchidan, xalqaro hamkorlikni kengaytirish va ilg‘or xorijiy tajribalarni joriy etish muhim ahamiyat kasb etadi, chunki kiber tahdidlarning transmilliy xarakteri davlatlar o‘rtasida yaqin hamkorlikni obyektiv zaruratga aylantiradi. To‘rtinchidan, jamiyatda raqamli madaniyat va kiberxavfsizlik madaniyatini shakllantirish bo‘yicha uzluksiz ta’lim tizimini yaratish zarur, bu jarayon maktabgacha ta’limdan tortib oliy ta’limgacha bo‘lgan barcha bosqichlarni qamrab olishi lozim. Beshinchidan, milliy dasturiy mahsulotlar va himoya vositalarini ishlab chiqish orqali texnologik mustaqillikni mustahkamlash maqsadga muvofiqdir, bu esa amalda soliq va investitsiya imtiyozlari, davlat buyurtmalari hamda raqamli texnologiyalar sohasidagi startap ekotizimini rivojlantirish kabi iqtisodiy rag‘batlantirish mexanizmlarini talab qiladi. Ushbu yo‘nalishlarning barchasi, tadqiqot natijalarida ko‘rsatilganidek, alohida-alohida emas, balki yaxlit tizim sifatida, davlat, jamiyat va shaxs manfaatlari uyg‘unligi kontekstida amalga oshirilgandagina kutilgan samarani berishi mumkin. Shu bilan birga, ushbu yo‘nalishlarning amalga oshirilish sur’ati va samaradorligini vaqt o‘tishi bilan baholash uchun kelgusida tegishli monitoring va empirik baholash mexanizmlarini ishlab chiqish alohida ilmiy-amaliy ahamiyat kasb etadi.

Xulosa. Xulosa qilib aytganda, o‘tkazilgan tadqiqot Yangi O‘zbekistonda kiberxavfsizlikni mustahkamlash mamlakatning barqaror taraqqiyoti va milliy xavfsizligini ta’minlashning muhim shartlaridan biri ekanligini ijtimoiy-falsafiy nuqtai nazardan asoslab berdi. Tadqiqot natijalari raqamli transformatsiya jarayonlarining jadallashuvi kiberxavfsizlik masalasining strategik ahamiyatini yanada oshirayotganini, ushbu jarayon esa faqat texnik emas, balki chuqur ijtimoiy-institutsional va ma’naviy-axloqiy xarakterga ega ekanligini ko‘rsatdi. Tadqiqot davomida qo‘yilgan barcha vazifalar izchil hal etildi, kiberxavfsizlikning ijtimoiy-falsafiy mohiyati axborotlashgan jamiyat nazariyalari asosida ochib berildi, normativ-huquqiy asoslar tahlil qilindi, inson omilining o‘rni aniqlandi, institutsional hamkorlik modeli tavsiflandi va kelgusi rivojlanishning beshta ustuvor yo‘nalishi ishlab chiqildi. Kiberxavfsizlikni rivojlantirishning ustuvor yo‘nalishlari sifatida milliy huquqiy bazani takomillashtirish, muhim axborot infratuzilmalarini himoya qilish, raqamli savodxonlikni oshirish, kiberxavfsizlik

madaniyatini shakllantirish va xalqaro hamkorlikni rivojlantirish alohida ahamiyat kasb etishi xulosa qilindi. Kelgusida sun’iy intellekt, innovatsion texnologiyalar va inson kapitaliga asoslangan kiberxavfsizlik modeli Yangi O‘zbekistonning raqamli taraqqiyotini ta’minlovchi muhim omillardan biriga aylanishi kutilmoqda. Shuningdek, tadqiqot natijalari kiberxavfsizlikni davlat organlari bilan bir qatorda fuqarolik jamiyati, ta’lim tizimi va xususiy sektorni ham qamrab oluvchi umummilliy vazifa sifatida tushunish zarurligini asoslab berdi. Yakun sifatida ta’kidlash joizki, mazkur tadqiqotda ilgari surilgan gipoteza — kiberxavfsizlikning barqaror tizimi huquqiy-institutsional choralar bilan bir qatorda ijtimoiy-madaniy omillarni ham qamrab olishi zarurligi haqidagi taxmin — to‘plangan manbalar tahlili asosida qo‘llab-quvvatlandi.

Foydalanilgan adabiyotlar ro‘yxati:

1. O‘zbekiston Respublikasi Prezidentining 2022-yil 28-yanvardagi PF-60-son "2022–2026-yillarga mo‘ljallangan Yangi O‘zbekistonning taraqqiyot strategiyasi to‘g‘risida"gi Farmoni. – Toshkent, 2022.

2. O‘zbekiston Respublikasi Prezidentining 2020-yil 5-oktabrdagi PF-6079-son "Raqamli O‘zbekiston — 2030" strategiyasi to‘g‘risidagi Farmoni. – Toshkent, 2020.

3. O‘zbekiston Respublikasining 2022-yil 15-apreldagi ЎРҚ-764-son "Kiberxavfsizlik to‘g‘risida"gi Qonuni. – Toshkent, 2022.

4. Bell D. The Coming of Post-Industrial Society. – New York: Basic Books, 1973. – 616 p.

5. Castells M. The Rise of the Network Society. 2nd ed., with a new preface. – Malden, MA: Wiley-Blackwell, 2010. – 656 p.

6. Toffler A. The Third Wave. – New York: Bantam Books, 1980. – 544 p.

7. Giddens A. The Consequences of Modernity. – Stanford: Stanford University Press, 1990. – 186 p.

8. Bauman Z. Liquid Modernity. – Cambridge: Polity Press, 2000. – 228 p.

9. Beck U. Risk Society: Towards a New Modernity. – London: Sage Publications, 1992. – 260 p.

10. Singer P.W., Friedman A. Cybersecurity and Cyberwar: What Everyone Needs to Know. – Oxford: Oxford University Press, 2014. – 320 p.

11. Council of Europe. Digital Citizenship Education Handbook: Being Online, Well-being Online, Rights Online. – Strasbourg: Council of Europe Publishing, 2019. – 336 p.

12. International Telecommunication Union. Global Cybersecurity Index 2024. – Geneva: ITU, 2024. – 96 p.

13. European Union Agency for Cybersecurity (ENISA). Threat Landscape Report. – Brussels: ENISA, 2023. – 158 p.

14. Назаров Қ.Ғ., Шермуҳамедова Н.А. Фалсафа асослари. – Тошкент: Ўзбекистон, 2018. – 400 б.

15. Туленов Ж.Т., Ғофуров З. Фалсафа. – Тошкент: Ўқитувчи, 2016. – 352 б.