O‘ZBEKISTON MILLIY UNIVERSITETI HUZURIDAGI ILMIY DARAJALAR BERUVCHI DSc.03/30.12.2019.Ss.01.08 RAQAMLI ILMIY KENGASH

O‘ZBEKISTON MILLIY UNIVERSITETI

TURDIYEV UYG‘UN RAXMATULLAYEVICH

MARKAZIY OSIYO MINTAQASIDA KIBERXAVFSIZLIKNI TA’MINLASHNING IJTIMOIY-SIYOSIY JIHATLARI

23.00.02 - Siyosiy institutlar, jarayonlar va texnologiyalar

Siyosiy fanlar bo‘yicha falsafa doktori (PhD) dissertatsiyasi AVTOREFERATI

Toshkent – 2023

UDK: 329.71:004.056(584.4)

**Siyosiy fanlar bo‘yicha falsafa doktori (PhD)
dissertatsiyasi avtoreferati mundarijasi**

**Оглавление автореферата диссертации
доктора философии (PhD) по политическим наукам**

**Contents of Dissertation Abstract
the Doctor of Philosophy (PhD) in political Sciences**

Turdiyev Uyg‘un Raxmatullayevich
Markaziy Osiyo mintaqasida kiberxavfsizlikni ta’minlashning ijtimoiy-siyosiy jihatlari.....3

Турдиев Уйгун Рахматуллаевич
Социально-политические аспекты обеспечения кибербезопасности в Центральноазиатском регионе.....29

Turdiyev Uygun Rakhmatullaevich
The political system of the society of Uzbekistan in ensuring the dynamics of national interests …….....57

E’lon qilingan ishlar ro`yxati
Список опубликованных работ
List of publications 62

O‘ZBEKISTON MILLIY UNIVERSITETI HUZURIDAGI ILMIY DARAJALAR BERUVCHI DSc.03/30.12.2019.Ss.01.08 RAQAMLI ILMIY KENGASH

O‘ZBEKISTON MILLIY UNIVERSITETI

TURDIYEV UYG‘UN RAXMATULLAYEVICH

MARKAZIY OSIYO MINTAQASIDA KIBERXAVFSIZLIKNI TA’MINLASHNING IJTIMOIY-SIYOSIY JIHATLARI

23.00.02 - Siyosiy institutlar, jarayonlar va texnologiyalar

Siyosiy fanlar bo‘yicha falsafa doktori (PhD) dissertatsiyasi AVTOREFERATI

Toshkent – 2023

Falsafa doktori (PhD) dissertatsiyasi mavzusi O‘zbekiston Respublikasi Vazirlar Mahkamasi huzuridagi Oliy attestatsiya komissiyasida B2022.4.PhD/Ss373 raqam bilan ro‘yxatga olingan.

Falsafa doktori (PhD) dissertatsiyasi O‘zbekiston Milliy universitetida bajarilgan.

Dissertatsiya avtoreferati uch tilda (o‘zbek, rus, ingliz (rezyume)) O‘zbekiston Milliy universiteti veb-sahifasida (http://nuu.uz) hamda «ZiyoNet» axborot ta’lim portalining www.ziyonet.uz manziliga joylashtirilgan.

Ilmiy rahbar:	**Paxrutdinov Shukritdin Ilyasovich** siyosiy fanlar doktori, professor
Rasmiy opponentlar:	**Kuchkarov Vaxob Xashimovich** siyosiy fanlar doktori, professor
	G‘oyibnazarov Shuxrat G‘oyibnazarovich siyosiy fanlar doktori, professor
Yetakchi tashkilot:	**Toshkent davlat sharqshunoslik universiteti**

Dissertatsiya himoyasi O‘zbekiston Milliy universiteti huzuridagi ilmiy darajalar beruvchi DSc.03/30.12.2019.S.01.08 raqamli Ilmiy kengashning 2023 yil « » oktabr soat 10:00 dagi majlisida bo‘lib o‘tadi (Manzil: 100174, Toshkent shahri, Universitet ko‘chasi, 4-uy. O‘zbekiston Milliy universiteti Ijtimoiy fanlar fakulteti binosi, 5-qavat, 511-xona. Tel.: 246-02-24 faks: (99871) 246-02-24; e-ma l: nauka@nuu.uz).

Dissertatsiya bilan O‘zbekiston Milliy universitetining Axborot-resurs markazida tanishish mumkin (- raqam bilan ro‘yxatga olingan). Manzil: 100174, Toshkent shahri, Universitet ko‘chasi, 4-uy, O‘zMU Ma’muriy binosi, 2-qavat, 4-xona. Tel.: (99871) 246-02-24; faks: (99871) 246-02-24.

Dissertatsiya avtoreferati 2023 yil «___»_____kuni tarqatildi.
(2023 yil «___» _____ da _____ - raqamli reestr bayonnomasi).

A.G. Muminov
Ilmiy darajalar beruvchi ilmiy kengash raisi o‘rinbosari, siyosiy fanlar doktori, professor

G.T. Isanova
Ilmiy darajalar beruvchi ilmiy kengash ilmiy kotibi, siyosiy fanlar bo‘yicha falsafa doktori (PhD), dotsent

A.G. Muminov
Ilmiy darajalar beruvchi ilmiy kengash qoshidagi Ilmiy seminar raisi, siyosiy fanlar doktori, professor

KIRISH

Dissertatsiya mavzusining dolzarbligi va zaruriyati. Jahonda sodir bo‘layotgan ko‘p formatli siyosiy transformatsiya natijasida yuzaga kelayotgan kiber xujum va gibrid ko‘rinishdagi tahdidlar inson, jamiyat va davlat manfaatlariga, siyosiy tizimning dinamik barqarorligiga o‘zining salbiy ta’sirini ko‘rsatmoqda. Turli axborot texnologiyalari orqali davlat va uning boshqaruv organlari faoliyati tizimiga hamda yoshlar qatlamiga g‘arazli maqsadlar, usullar orqali salbiy ta’sir o‘tkazish yo‘li bilan yoshlar ongini zabt etish, ularda submadaniyat ko‘rinishlarini shakllantirish, davlat va jamiyat islohotlariga qarama-qarshi bo‘lgan g‘oyalarni shakllantirish ommalashmoqda. Hozirgi sharoitda g‘arazli mafkuraviy kuchlarning strategik maqsadlarini bartaraf etish, yoshlar genafondini saqlash, turli xavf-xatar omillariga, tahdidli holatlarga samarali preventiv chora-tadbirlarni ko‘rish, davlatlararo barqaror hamkorlik muhitini yuzaga keltirish orqali milliy manfaatlar ustuvorligini ta’minlash va himoya qilish dolzarblashib bormoqda.

Markaziy Osiyo mintaqasida kiberxavfsizlikni ijtimoiy-siyosiy asoslarini shakllantirish, davlatlararo milliy-hududiy, milliy-madaniy aloqadorlikni saqlab qolishning fundamental asoslarini yaratishga qaratilgan kiber makonda turli xavf va tahdidlarga qarshi kurashuvchi immunitetni shakllantirish orqali inson, jamiyat va davlat o‘zining xavfsizligini ta’minlab borishi, geosiyosiy makonda kuchlar muvozanatining izdan chiqishi, beqaror va xavfli tahdidlarning yuzaga kelishini oldini olishga qaratilgan salmoqli ilmiy izlanishlar amalga oshirilmoqda. Amalga oshirilayotgan tadqiqotlarda kiberxavfsizlikni davlat tomonidan tartibga solish, huquqiy, tashkiliy, ilmiy-texnik va me’yoriy uslubiy ta’minot tizimini takomillashtirish, axborot tizimlari va resurslarining yaxlitligini ta’minlash, jumladan Markaziy Osiyo mintaqasida kiberxavf va xatar omillarini aniqlash, ularni oldini olish va bartaraf etish mexanizmlarini hamda xavfsizlik sohasi istiqbolini aniq prognozlash imkonini oshirish, transchegaraviy tahdidlarning kuchayishi sharoitida xavfsizlik sohasida mintaqaviy institutlar, norma va qoidalar ijrosining samaradorligini oshirish dolzarb ahamiyat kasb etmoqda.

O’zbekistonda amalga oshirilayotgan keng qamrovli islohotlar sharoitida axborot sohasida davlat siyosatining isloh etish, sohaga oid normativ-huquqiy bazani tubdan takomillashuviga, mintqaviy va xalqaro darajada kiberxujumlarga qarshi javob beruvchi xavfsiz makonni qaror toptirish kabilarga alohida e’tibor qaratilmoqda. “O’zbekiston o‘zining tashqi siyosatida Markaziy Osiyo mintaqasiga ustuvor ahamiyat qaratmoqda. Bu – har tomonlama chuqur o‘ylab tanlangan yo‘ldir. Markaziy Osiyoning qoq markazida joylashgan O’zbekiston ushbu mintaqa barqarorlik, izchil taraqqiyot va yaxshi qo‘shnichilik hududiga aylanishidan bevosita manfaatdordir”[1]. Markaziy Osiyo davlatlarida milliy davlatchilikni mustahkamlash, xavfsizlik tizimini rivojlantirishning siyosiy,

[1] Мирзиёев Ш.М. Халқимизнинг розилиги бизнинг фаолиятимизга берилган энг олий баҳодир. 2-жилд . -Т.: Ўзбекистон. 2018. – Б.248.

tarixiy, g‘oyaviy-mafkuraviy negizlari, mintaqaviy xavfsizlikni ta’minlashda O’zbekistonning tashabbusi va uning milliy manfaatlar doirasida tadqiq etish dolzarb vazifalar sirasiga kiradi.

O’zbekiston Respublikasi Prezidentining 2017 yil 7 fevraldagi PF-4947-son «O’zbekiston Respublikasini yanada rivojlantirish bo‘yicha Harakatlar strategiyasi to‘g‘risida», 2022 yil 28 yanvardagi PF-60-son «2022–2026 yillarga mo‘ljallangan Yangi O’zbekistonning taraqqiyot strategiyasi to‘g‘risida»gi farmonlari, 2021 yil 1 iyuldagi O’zbekiston Respublikasining ekstremizm va terrorizmga qarshi kurashish bo‘yicha 2021-2026 yillarga mo‘ljallangan strategiyasi, O’zbekiston Respublikasining 2022 yil 15 apreldagi “Kiberxavfsizlik to‘g‘risida”gi Qonuni hamda sohaga tegishli boshqa normativ-huquqiy hujjatlarda belgilangan vazifalarni amalga oshirishda mazkur dissertatsiya ishi muayyan darajada xizmat qiladi.

Tadqiqotning respublika fan va texnologiyalari rivojlanishining ustuvor yo‘nalishlariga mosligi. Dissertatsiya tadqiqoti respublika fan va texnologiyalar rivojlanishining respublika ilm-fan va texnologiyalarini rivojlantirishning I. «Axborotlashgan jamiyat va demokratik davlatni ijtimoiy, huquqiy, iqtisodiy, madaniy, ma’naviy-ma’rifiy rivojlantirishda innovatsion g‘oyalar tizimini shakllantirish va ularni amalga oshirish yo‘llari» ustuvor yo‘nalishi doirasida bajarilgan.

Muammoning o‘rganilganlik darajasi. Dissertatsiyada qo‘yilgan vazifalarni tahlil etishda jahon va o‘zbek siyosatshunoslik ilmida amalga oshirilgan tadqiqotlarga tayanildi.

“Kiberxavfsizlik”, “kibermakon”, “kiber terrorizm va ekstremizm” oid bo‘lgan nazariy ilmiy tadqiqotlar va asarlar keng ko‘lamli bo‘lib, ular masalaning u yoki bu jihatlarini qamrab oladi. Bunday ilmiy tadqiqotlarni uch guruhga ajratish mumkin:

birinchi guruhga g‘arb olimlari: M.Dyuverje Sh.Eyzenshtadt, G.Almond, D.Iston, R.Aron, T.Parsons, R.Dal, A.Toynbi, D.Ikeda, V.Edvardlar[2]ning ilmiy ishlarini kiritish mumkin. Ushbu olimlar tadqiqotlarida asosiy e’tibor jamiyat va uning siyosiy tizimi to‘g‘risidagi qarashlar, uning ichki strukturaviy tuzilishlarini o‘rganishga qaratilgan;

ikkinchi guruhga rus olimlari; Ye.Primakov, V.Gumelyov, V.Fedotova, V.Kolpakov, A.Nьısanbayev, A.Guseynova, Ye.Agoshkovoy, N.Gubanov, B. Isayev, V.Belolikov kabi olimlarning ishlari kiradi. Mazkur tadqiqotchilar tomonidan global o‘zgarishlar sharoitida partiyaviy tizimlarni yangi qarashlar asosida yangicha kontekstda tahlil etilib, yoritib berilgan. Yuqorida qayd etilgan xorijiy tadqiqotlar fundamental xususiyatga ega bo‘lib, tadqiqotda nazariy muammolarning yechimini topishda alohida ahamiyat kasb etadi;

uchinchi guruhga mahalliy tadqiqotchilardan; I.Ergashev, S.Atamuratov, R.Jumayev, S.Jo‘rayev, Sh.Paxrutdinov, A.Mo‘minov, Sh.G’oibnazarov,

[2] Qayd etilgan mahalliy va xorijiy olimlarning asarlari dissertatsiyada batafsil keltirilgan.

J.Mavlonov, O.Sirojov, I.Boboqulov, X.Umarov, U.Bo‘tayev, K.Avazov, O.Allayarov va boshqa tadqiqotchilar milliy manfaatlarni ta’minlashda xavfsizlik va barqarorlik masalasi, dinning siyosiylashuvi, xalqaro terrorizmning huquqiy, siyosiy va falsafiy tahlili hamda davlat va jamiyatni rivojlantirishda AKTning roli va ahamiyati bilan bog‘liq jihatlarni ochib bergan.

Xususan, o‘rganilayotgan muammoning diniy aspektlari bo‘yicha Abdullayeva Moxira Zaxidjanovnaning “Kibermakon va islom bilan bog‘liq diniy-ma’naviy jarayonlar”, huquqiy jihatlarini Ibrohimov Jamshid Abdug‘ofur o‘g‘lining «Terrorizm bilan bog‘liq jinoyatlarga qarshi kurashishning jinoiy-xuquqiy va kriminologik jihatlari», matematik-texnik jihatlari bo‘yicha Kuryazov Davlatyor Matyakubovichning “Bardoshli kriptografik algoritmlar yaratish usullarini ishlab chiqish” mavzusidagi ilmiy-tadqiqot ishlarida kiberxavfsizlikning nazariy va amaliy masalalari tadqiq etilgan.

Hozirgi murakkab davrda jahon hamjamiyatida o‘z o‘rni, pozitsiyasi va obro‘sini tobora mustahkamlab borayotgan Yangi O’zbekiston uchun ilm-fanga raqamli texnologiyalar va zamonaviy usullarni joriy etish, oliy ta’lim muassasalarida ilmiy-tadqiqot ishlari natijadorligini oshirish davlat siyosatning eng muhim yo‘nalish va usullaridan biriga aylandi. Xususan, siyosiy fanlar sohasida kadrlar tayyorlash samaradorligini oshirish, fuqarolik jamiyati, milliy davlatchilikning siyosiy asoslarining shakllanishi va rivojlantirish sohasida kompleks tizimli tadqiqotlar olib borish, globallashuv sharoitida davlatning ichki va tashqi siyosatini shakllantirish va amalga oshirish, shu asosda ijtimoiy-siyosiy islohotlarni chuqurlashtirish bo‘yicha ilmiy asoslangan tavsiyalar va dasturlarni ishlab chiqish dolzarb masala sifatida qaralayotganini alohida qayd etish joiz.

Shu nuqtai nazardan, Markaziy Osiyo mintaqasida kiberxavfsizlikni ta’minlashning ijtimoiy-siyosiy jihatlarini milliy manfaatlar kontekstida o‘rganish uning konsentual asoslarini alohida tadqiqot ob’ekti sifatida o‘rganish jarayonida erishgan yutuqlari va kamchiliklarini hamda istiqboldagi maqsadlarini aniq, puxta belgilab olish va ularga erishish uchun amalga oshirilishi lozim bo‘lgan vazifalarni ishlab chiqish hamda taklif va tavsiyalar berish ushbu tadqiqot mavzuining dolzarbligini belgilaydi.

Dissertatsiya mavzusining dissertatsiya bajarilgan oliy ta’lim muassasasi ilmiy-tadqiqot ishlari rejalari bilan bog‘liqligi. Dissertatsiya tadqiqoti O’zbekiston Milliy universiteti ilmiy-tadqiqot ishlar rejasiga muvofiq I. «Demokratik islohotlarni yanada chuqurlashtirish va fuqarolik jamiyatini rivojlantirishda ijtimoiy-siyosiy, sotsial-iqtisodiy islohotlarning mushtarakligi» mavzusi doirasida bajarilgan.

Tadqiqotning maqsadi Markaziy Osiyo mintaqasida kiberxavfsizlikning ijtimoiy-siyosiy ta’minoti bo‘yicha taklif va tavsiyalar ishlab chiqishdan iborat.

Tadqiqotning vazifalari:

siyosiy fanlarda xavfsizlik kategoriyasi bo‘yicha dastlabki nazariy tushunchalar, ularning tadrijiy taraqqiyoti borasidagi ilmiy-nazariy tadqiqotlarni tizimlashtirish;

kiberxafsizlikni rivojlanish bosqichlarini qiyosiy tahlil qilish hamda kiberxavfsizlik tushunchasi va uning ijtimoiy-siyosiy fenomen sifatida nazariy-amaliy jihatlarini yoritish;

Markaziy Osiyo kiberxavfsizligi tizimi va uning o‘ziga xos xususiyatlarini hamda xorijiy davlatlarining kiberterrorizm va ekstremizmga qarshi kurash yo‘nalishidagi tajribasi va uni mintaqaviy hamkorlikka ta’sirini ko‘rsatib berish;

O’zbekistonning kiberxavfsizlikni ta’minlashda borasidagi tajribasi asoslab berish asosida mintaqada kiberxavfsizlikni ta’minlashning takomillashtirish mexanizmlari takomillashtirishga qaratilgan xulosa, taklif va tavsiyalar ishlab chiqish.

Tadqiqotning ob’ektini Markaziy Osiyo mintaqasida kiberxavfsizlikni ta’minlashning ijtimoiy-siyosiy va mafkuraviy jarayonlari tashkil etadi.

Tadqiqotning predmetini Markaziy Osiyo mintaqasida kiberxavfsizlikni ta’minlashning ijtimoiy-siyosiy jihatlariga priventiv yondashuvlar bo‘lib hisoblanadi.

Tadqiqotning usullari. Tadqiqotda tsivilizatsion, kuzatuv, analiz va sintez, reduksiya, retrospektiv tahlil, komporativ metod, kontent-tahlil, vaziyatli tahlil, futurologik tahlil, ekspert baholash va siyosiy prognozlash kabi usullardan foydalanilgan.

Tadqiqotning ilmiy yangiligi quyidagilarda ko‘rinadi:

xavfsizlik tizimining sub’ektiv (inson, jamiyat, davlat) va ob’ektiv (xalqaro munosabatlar) institutsional tuzilmasini ichki va tashqi tahdidlardan samarali muhofaza qilish va barqaror taraqqiyotini ta’minlashning muhim asosini davlat organlari, tashkilotlar faoliyatiga hamda yoshlar ma’naviy kamolatiga tahdid qiluvchi ijtimoiy, siyosiy, mafkuraviy, xarbiy, diniy ko‘rinishdagi kiberxuruj hamda kiberxujumlardan samarali himoya qilishga bog‘liqligi asoslangan;

ijtimoiy hayotning barcha sohalariga qaratilgan milliy rivojlanish strategiyasini amalga oshirishda axborot resurslari barqarorligi va ishonchliligini ta’minlash, davlat hokimiyati organlarining fuqarolar bilan samarali elektron muloqotida xushyorlik va ogoh bo‘lishga qaratilgan kiberxavfsizlikni priventiv vosita sifatida ta’minlash davlat va jamiyat o‘rtasidagi yuqori legitimlik darajasiga xizmat qilishi isbotlangan;

markaziy Osiyo davlatlarining milliy xavfsizligi, suverenitetining barqarorlik darajasi mintaqaviy strategik va ijtimoiy-iqtisodiy ahamiyatga ega bo‘lgan axborot texnologiyalari vositalarining har qanday ichki va tashqi kibertahdidlaridan himoyalanish qobiliyatiga to‘g‘ri proporsional bo‘lib, ularning institutsional va funksional jihatdan qonuniy asosga ega bo‘lishi jamiyat barqaror taraqqiyotining muhim asosi ekanligi asoslangan;

markaziy Osiyo mintaqasida kompleks xavfsizlik tizimining muhim komponenti bo‘lib tahdidlardan himoyalanish mexanizmlarining zaifligi, zararli axborot dasturlari oqimining mavjudligi transchegaraviy va transmilliy xarakterga ega bo‘lib, unga qarshi kurashish bo‘yicha davlatlararo hamkorlik bosqichlarining o‘zaro ta’siri hamda strategik sheriklikning regional va ko‘p qirrali konstruktiv

yo‘nalishi kiberxavfsizlik tizimini shakllanganlik darajasiga bog‘liqligi asoslangan.

Tadqiqotning amaliy natijalari quyidagilardan iborat:

Xavfsizlikka erishish kafolatlarini ta’minlashning mintaqaviy muammolarini yechish kontekstida kiberxavfsizlik, kiberterrorizm va ekstremizmga qarshi kurash, kiberxavfsizlikni ta’minlashning ijtimoiy-siyosiy jihatlari, xavf-xatar omillarini aniqlash, ularni oldini olish va bartaraf etish mexanizmlarini kompleks va tizimli tarzda o‘rganish yuzasidan konseptual ilmiy xulosa va takliflar ishlab chiqilgan;

zamonaviy xorijiy va milliy tajribani qiyosiy jihatdan o‘rganish asosida O’zbekistonning Markaziy Osiyo mintaqasida olib borilayotgan xavfsizlikka qaratilgan islohotlarning natijadorligi, samaradorligini oshirish, mazkur faoliyat shakli avvalo, inson manfaatlariga xizmat qilishi va siyosiy jarayonlarda fuqarolik jamiyati institutlarining keng ishtirokini ta’minlashga qaratilgan amaliy tavsiyalar berib o‘tilgan.

Tadqiqot natijalarining ishonchliligi. Tadqiqot natijalarining ishonchliligi ma’lumotlarning rasmiy manbaalardan olingani, yondashuv va usullarning maqsadga muvofiqligi, respublika va xalqaro miqyosdagi ilmiy-uslubiy va ilmiy-amaliy konferensiya materiallari to‘plamlari, OAK ro‘yxatidagi maxsus hamda xorijiy ilmiy jurnallarda chop etilgan maqolalar, xulosa, amaliy taklif va tavsiyalarning amaliyotga joriy etilgani, olingan natijalarning vakolatli tashkilotlar tomonidan tasdiqlangani bilan izohlanadi.

Tadqiqotning ilmiy va amaliy ahamiyati. Tadqiqot natijalarining ilmiy ahamiyati olingan natijalardan Markaziy Osiyoda kiberxavfsizlikni ta’minlash masalalarida milliy manfaatlarni siyosiy tadqiq etish asosida mintaqadagi xavfsizlikni ta’minlash borasidagi siyosat asoslarini, ushbu yo‘nalishdagi nazariy-ilmiy va nazariy-fundamental tadqiqotlar hamda metodologik yondashuvlarni takomillashtirishda foydalanish mumkinligi bilan izohlanadi.

Tadqiqot natijalarining amaliy ahamiyati O’zbekistonning Markaziy Osiyoda kiberxavfsizlikni ta’minlash borasidagi siyosati va bu boradagi islohotlarga bag‘ishlangan maqsadli davlat dasturlarining bajarilishi va takomillashtirilishida muhim manba sifatida xizmat qilishi bilan izohlanadi.

Tadqiqot natijalarining joriy qilinishi Markaziy Osiyo mintaqasida kiberxavfsizlikni ta’minlashning ijtimoiy-siyosiy jihatlarini o‘rganish natijasida:

xavfsizlik tizimining sub’ektiv (inson, jamiyat, davlat) va ob’ektiv (xalqaro munosabatlar) omillarini ichki va tashqi tahdidlardan samarali muhofaza qilish va barqaror taraqqiyotini ta’minlashning muhim asosini davlat organlari, tashkilotlar faoliyatiga hamda yoshlar ma’naviy kamolatiga tahdid qiluvchi ijtimoiy, siyosiy, mafkuraviy, xarbiy ko‘rinishdagi kiberxuruj hamda kiberxujumlardan samarali himoya qilishga bog‘liqligi borasidagi ilmiy yangiligi Respublika ma’naviyat va ma’rifat markazi 2023 yil uchun chora tadbirlar dasturining VIII yo‘nalishida belgilangan “Milliy qadriyatlar, ma’naviy fazilatlar va ijtimoiy odoblar targ‘iboti” 43-bandi “Internetda milliylikni targ‘ib etuvchi, mentalitetimiz, azaliy qadriyat va ezgu an’nalarimizni saqlab qolish bo‘yicha o‘zaro muloqot maydoni uchun platforma va mobil ilovalar yaratish” mavzusidagi ilmiy loyihada foydalanilgan

(Respublika ma’naviyat va ma’rifat markazining 2023 yil 22 sentyabrdagi 02-22/1008-son dalolatnomasi). Natijada, dissertatsiyada ilgari surilgan takliflar, tavsiya va xulosalar O’zbekistonning ichki xavfsizligi va barqaror taraqqiyotini ta’minlashning dolzarb masalalari hamda Markaziy Osiyoda xavfsizlik masalalari, mintaqaviy va xalqaro hamkorlik istiqbollari borasida qo‘shma tadqiqotlar olib borishga xizmat qilgan;

ijtimoiy hayotning barcha sohalariga qaratilgan milliy rivojlanish strategiyasini amalga oshirishda axborot resurslari barqarorligi va ishonchliligini ta’minlash, davlat hokimiyati organlarining fuqarolar bilan samarali elektron muloqotida xushyorlik va ogoh bo‘lishga qaratilgan kiberxavfsizlikni priventiv vosita sifatida ta’minlash davlat va jamiyat o‘rtasidagi yuqori legitimlik darajasiga xizmat qilishi bilan bog‘liq xulosalardan Respublika ma’naviyat va ma’rifat markazi 2023 yil uchun chora tadbirlar dasturining VIII yo‘nalishida belgilangan “Milliy qadriyatlar, ma’naviy fazilatlar va ijtimoiy odoblar targ‘iboti” 43-bandi “Internetda milliylikni targ‘ib etuvchi, mentalitetimiz, azaliy qadriyat va ezgu an’nalarimizni saqlab qolish bo‘yicha o‘zaro muloqot maydoni uchun platforma va mobil ilovalar yaratish” mavzusidagi ilmiy loyihada foydalanilgan (Respublika ma’naviyat va ma’rifat markazining 2023 yil 22 sentyabrdagi 02-22/1008-son dalolatnomasi). Natijada, teleradioeshittirishlar uchun tayyorlangan materiallar mazmunini mukammal va ilmiy dalillarga boy bo‘lishida, aholining siyosiy ongi va madaniyatini oshirish borasidagi bilim, ko‘nikma va tajribalarini mustahkamlashga xizmat qilgan;

Markaziy Osiyo davlatlarining milliy xavfsizligi, suverenitetining barqarorlik darajasi mintaqaviy strategik va ijtimoiy-iqtisodiy ahamiyatga ega bo‘lgan axborot texnologiyalari vositalarining har qanday ichki va tashqi kibertahdidlaridan himoyalanish qobiliyatiga to‘g‘ri proporsional bo‘lib, ularning institutsional va funksional jihatdan qonuniy asosga ega bo‘lishi jamiyat barqaror taraqqiyotining muhim asosi ekanligi borasidagi xulosalaridan Respublika ma’naviyat va ma’rifat markazi 2023 yil uchun chora tadbirlar dasturining VIII yo‘nalishida belgilangan “Milliy qadriyatlar, ma’naviy fazilatlar va ijtimoiy odoblar targ‘iboti” 43-bandi “Internetda milliylikni targ‘ib etuvchi, mentalitetimiz, azaliy qadriyat va ezgu an’nalarimizni saqlab qolish bo‘yicha o‘zaro muloqot maydoni uchun platforma va mobil ilovalar yaratish” mavzusidagi ilmiy loyihada foydalanilgan (Respublika ma’naviyat va ma’rifat markazining 2023 yil 22 sentyabrdagi 02-22/1008-son dalolatnomasi). Natijada, jamoatchilik tashkilotlari, xududlardagi nodavlat notijorat tashkilotlari va siyosiy partiyalarning xududiy filiallari bilan o‘zaro hamkorlikda inson xavfsiligi va barqarorligi yo‘nalishlaridagi yo‘l xaritalari, dasturlar va tarmoq sohalarning ustuvor vazifalarini ishlab chiqilishiga asos sifatida xizmat qilgan.

Markaziy Osiyo mintaqasida kompleks xavfsizlik tizimining muhim komponenti bo‘lib tahdidlardan himoyalanish mexanizmlarining zaifligi, zararli axborot dasturlari oqimining mavjudligi transchegaraviy va transmilliy xarakterga ega bo‘lib, unga qarshi kurashish bo‘yicha davlatlararo hamkorlik bosqichlarining

o‘zaro ta’siri hamda strategik sheriklikning regional va ko‘p qirrali konstruktiv yo‘nalishi kiberxavfsizlik tizimini shakllanganlik darajasiga bog‘liqligi yuzasidan ilgari surilgan yangiliklaridan Respublika ma’naviyat va ma’rifat markazi 2023 yil uchun chora tadbirlar dasturining VIII yo‘nalishida belgilangan “Milliy qadriyatlar, ma’naviy fazilatlar va ijtimoiy odoblar targ‘iboti” 43-bandi “Internetda milliylikni targ‘ib etuvchi, mentalitetimiz, azaliy qadriyat va ezgu an’nalarimizni saqlab qolish bo‘yicha o‘zaro muloqot maydoni uchun platforma va mobil ilovalar yaratish” mavzusidagi ilmiy loyihada foydalanilgan (Respublika ma’naviyat va ma’rifat markazining 2023 yil 22 sentyabrdagi 02-22/1008-son dalolatnomasi). Natijada, markaz tomonidan o‘tkaziladigan sotsiologik ilmiy-tadqiqotlarni hamda ijtimoiy mezonlar metodologiyasini takomillashtirishga xizmat qilgan.

Tadqiqot natijalarining aprobatsiyasi Mazkur tadqiqot natijalari 9 ta ilmiy-nazariy va ilmiy-amaliy konferensiyalarda jumladan, 3 ta xalqaro va 6 ta respublika konferensiyalarida muhokamadan o‘tkazilgan.

Tadqiqot natijalarining e’lon qilinishi Dissertatsiya mavzusi bo‘yicha jami 19 ta ilmiy ish, jumladan Oliy attestatsiya komissiyasining doktorlik dissertatsiyalari asosiy ilmiy natijalarini chop etishi tavsiya etilgan ilmiy nashrlarda 10 ta ilmiy maqola, jumladan 3 tasi xorijiy, 7 tasi respublika miqyosidagi jurnallarda, konferensiya materiallari to‘plamlarida 9 ta (xalqaro konferensiyalarda 3 ta, mahalliy konferensiyalarda 6 ta) maqola chop etilgan.

Dissertatsiyaning tuzilishi va hajmi. Dissertatsiya tarkibi kirish, uchta bob, sakkizta paragraf, xulosa va foydalanilgan adabiyotlar ro‘yxatidan iborat. Dissertatsiyaning hajmi 130 sahifani tashkil etadi.

DISSERTATSIYANING ASOSIY MAZMUNI

Kirish qismida tadqiqot mavzusining dolzarbligi va zarurati asoslangan, mavzuning respublika fan va texnologiyalari rivojlanishining asosiy ustuvor yo‘nalishlariga mosligi ko‘rsatilgan, muammoning o‘rganilganlik darajasi yoritilgan, tadqiqot ishining maqsad va vazifalari, ob’ekti va predmeti aniqlangan.

Tadqiqot usullari, ilmiy yangiligi va amaliy natijalari bayon qilingan. Olingan natijalarning ishonchliligi, ilmiy va amaliy ahamiyati asoslab berilgan. Tadqiqot natijalarining amaliyotga joriy etilganligi, e’lon qilinganligi, dissertatsiyaning tuzilishi va hajmi bo‘yicha ma’lumotlar berilgan.

Dessertatsiyaning birinchi bobi **“Markaziy Osiyo mintaqasida kiberxavfsizlikni tadqiq etishning nazariy – metodologik asoslari”** deb nomlanib, unda “Kiberxavfsizlik tushunchasi va uning ijtimoiy-siyosiy talqini”, “Kiberxafsizlikni ta’minlashni rivojlanish bosqichlari”, “Markaziy Osiyo kiberxavfsizligi tizimi va uning o‘ziga xos xususiyatlari” kabi masalalar tadqiq qilingan.

Umuman kiberxavfsizlik muammosi zamonaviy axborat kommunikatsiya texnologiyalarining rivojlanishi barobarida paydo bo‘lgan va bugungi zamonaviy

dunyoning ajralmas qismi, bo‘lagi sifatida qaralib kelinmoqda. Kiberxavfsizlikning jamiyat ijtimoiy – siyosiy hayotiga ahamiyati toboro oshib borayotganligini kuzatishimiz mumkin.

Dissertatsiyaning mazkur bobida kiberxafsizlik tushunchasiga ta’rif berilib, uning paydo bo‘lishi, rivojlanishi haqidagi nazariyalar ochib berilgan. Xususan, zamonaviy siyosiy-harbiy fanlarda “kiberxavfsizlik”, “kibermakon”[3], “kibermadaniyat”[4], “Proxy war”, “gibrid urushlar” kabi kategoriyalar kirib keldi. Bu kategoriyalarni tushunishga bo‘lgan talabning ortishi davlat va jamiyatning nazariy va amaliy ehtiyojlari bilan bog‘liq. Chunki yangi bir sharoitda kiberxavfsizlik muammosi bo‘yicha qaror qabul qilishga bo‘lgan zaruriy ehtiyoj mazkur masalalarni chuqurroq o‘rganishni taqozo etadi.

“Kiberxavfsizlik” kategoriya sifatida – manbalarda turlicha talqin etiladi. Jumladan, kiberxavfsizlik - bu axborot tizimlari, tarmoqlari, va dasturlarini raqamli hujumlardan himoyalashga qaratilgan faoliyatdir. Odatda bunday hujumlardan maqsad maxfiy ma’lumotlarni qo‘lga kiritish, ularni o‘zgartirish yoki yo‘qotish, foydalanuvchilardan pul talab qilish yoki biznes jarayonlarini izdan chiqarishdan iborat[5].

Boshqacha aytganda kiberxavfsizlik bu – tasodifiy va atayin qilingan axboriy hujumlardan himoyalanish demakdir. U ko‘p qirrali faoliyat sohasi bo‘lib, unga faqat tizimli va kompleks yondashuv muvaffaqiyat keltirishi mumkin.

Kiberxavfsizlik – hisoblashga asoslangan bilim sohasi bo‘lib, buzg‘unchilar mavjud bo‘lgan sharoitda amallarni kafolatlash uchun o‘zida texnologiya, inson, axborot va jarayonni mujassamlashtirgan. U xavfsiz kompyuter tizimlarini yaratish, amalga oshirish va tahlil qilishni o‘z ichiga oladi. Shuningdek, konseptual jihatdan kiberxavfsizlik ta’limning mujassamlashgan bilim sohasi hisoblanib, qonuniy jihatlarni, siyosatni, inson omilini, etika va risklarni boshqarishni ham o‘z ichiga oladi.

Mazkur bobda shuningdek, quyidagilarga e’tibor qaratilgan:

O’zbekiston Respublikasining Kiberxavfsizlik to‘g‘risidagi Qonunida kiberxavfsizlik — kibermakonda shaxs, jamiyat va davlat manfaatlarining tashqi va ichki tahdidlardan himoyalanganlik holati deb belgilangan[6].

Qonunda kiberxavfsizlikni ta’minlashning quyidagi: qonuniylik; kibermakonda shaxs, jamiyat va davlat manfaatlarini himoya qilishning ustuvorligi; kiberxavfsizlik sohasini tartibga solishga nisbatan yagona yondashuv; kiberxavfsizlik tizimini yaratishda mahalliy ishlab chiqaruvchilar ishtirokining ustuvorligi; O’zbekiston Respublikasining kiberxavfsizlikni ta’minlashda xalqaro

[3] Bu tushuncha yozuvchi Uilyam Gibson tomonidan 1984 yili “Cyberspace ” (“Kibermakon”) deb nomlangan trilogiyaning birinchi romani “Neuromancer” (“Neyromant”) chop etilishi bilan bog‘liq. U dunyoning barcha kompyuterlaridagi elektron ma’lumotlar aylanib yuradigan virtual makonni ta’riflaydi. Qarang: Axborot kommunikatsiya texnologiyalari izohli lug‘ati. BMTTDning O‘zbekistondagi vakolatxonasi. – 2010. – 573 b

[4] Madaniyatni rivojlantirishdagi texnokrat yangi yo‘nalish. U kompyuter o‘yinlarining imkoniyatlari va virtual voqelik texnologiyalarini ishlatishga asoslangan.

[5] https://www.cisco.com/c/ru_ru/products/security/what-is-cybersecurity.html

[6] Ўзбекистон Республикасининг 2022 йил 15 апрелдаги Киберхавфсизлик тўғрсидаги Қонуни.// https://lex.uz/uz/docs/5960604

hamkorlik uchun ochiqligi kabi asosiy tamoyillari belgilangan.

Kibermakon atamasi - yozuvchi Uilyam Gibson tomonidan 1984 yili “Cyberspace ” (“Kibermakon”) deb nomlangan trilogiyaning birinchi romani “Neuromancer” (“Neyromant”) chop etilishi bilan bog‘liq. U dunyoning barcha kompyuterlaridagi elektron ma’lumotlar aylanib yuradigan virtual makonni ta’riflaydi[7].

Kibermakon kompyuter tarmoqlari orqali amalga oshiriladigan muloqot maydonini hisoblanib, bu 1990 yildan boshlab keng miqyosida rivojlanib, takomillashib kelmoqda. Ijtimoiy nuqtai-nazardan kibermakon - kompyuter tarmog‘i orqali bir-biri bilan bog‘langan va bir vaqtning o‘zida turli geografik nuqtada kesishuvchi har qanday mavjud kompyuterning grafik sifatidagi ma’lumotlar almashuvchi kishilar yoki guruhlar jamoasi tushuniladi.

Bugun mamlakatimizda, diniy sohada amalga oshirilayotgan islohotlar ayrim toifadagi aholi tomonidan noto‘g‘i talqin qilinishi oqibatida yoshlar o‘rtasida diniy mutaassiblashuv jarayonlari avj olmoqda. Bu borada Internet mazkur jarayonni faollashuvi vositasi bo‘lib xizmat qilmoqda.

Diniy ekstremistik va terroristik tashkilotlar a’zolari o‘z saflarini kengaytirish maqsadida ijtimoiy tarmoqlardan unumli foydalanmoqda. Yoshlar ongini zabt etishga qaratilgan mafkuraviy axborot-targ‘ibotlari aynan kibermakonda sodir etilmoqda.

Masalan, ekstremistik guruhlar “Odnoklassniki”, “Facebook”, “Instagram”, “Twitter”, “Vkontakte” ijtimoiy tarmoqlarida “Abdulloh Zufar”, “Sodiq Samarqandiy”, “Mustafo mujohid”, “Abu-Muoviya”, “Ansor-ansor”, “Fulan ibn fulan” kabi soxta profillarini yaratish orqali buzg‘unchilik va yot g‘oyalarni targ‘ib qiluvchi g‘oya va da’vatlarini yoshlar ongiga ruhiy ta’sir o‘tkazib, ularni “hijrat va “jihod” maqsadida jangovar harakatlar ketayotgan dunyoning “o‘choqli hududlariga” chiqib ketishga chorlamoqda.

Dissertatsiyada Markaziy Osiyo mintaqasidagi kiberjinoyatlar uchta asosiy toifaga bo‘linib tahlil etilgan: bezorilik, hakkerlik va kompyuter firibgarligi. Mana shu uchta jihat orqali kibrejinoyatlarning kelib chiqishining ijtimoiy-siyosiy jihatlari tahlil etilgan.

Tahlil natijalari asosida ularning rivojlanish dinamikasi ochib berilgan. Birlashgan Millatlar Tashkilotining 2018 yildagi tadqiqoti natijalariga ko‘ra, **50%** davlatlarning kiberxavfsizlik strategiyasi mavjud emasligi, **25%** davlatda muhim axborot infratuzilmasi uchun xavfsizlik bo‘yicha qonunchilik bazasi mavjud ekanligi ham tadqiqot natijalari bilan uyg‘unlashadi.

Shuningdek, mamlakatlarning atigi **31%**da muhim axborot infratuzilmasi himoyasi bo‘limi kiberxavfsizlik strategiyasiga kiritilgani, faqatgina **109** ta ishtirokchi davlatlarda kiberxavfsizlik bo‘yicha qonun hujjatlari mavjudligi aniqlandi. **141** mamlakatda *(73%)* onlayn maxfiylik qonunlari mavjud.

[7]Қаранг: Ахборот коммуникация технологиялари изоҳли луғати. БМТТДнинг Ўзбекистондаги ваколатхонаси. – 2010. – 573 б.

Tadqiqot natijalariga asosan, kiberxavfsizlik ijtimoiy sohaning ajralmas qismi yohud shaxsning xavfsizligini ta’minlash jarayonida namoyon bo‘ladigan tizimli ko‘rinish hisoblanadi degan xulosaga kelindi.

Qolaversa, kiberxavfsizlik sohaviy jihatdan inson xavfsizligi, ma’lumotlar xavfsizligi, jamoat xavfsizligi, faoliyat xavfsiziligidagi ko‘rinishlarni o‘zida mujassamlaydigan tizim ekanligi isbotlandi.

Masalan, ijtimoiy jihatdan kiberxavfsizlik insonning jamiyat bilan bog‘liq munosabatlarida, ahloqiy munosabatlarida yohud shaxsiy hayot va ularning bir-biri bilan munosabatlarida aks etadi. Tadqiqot ishida kiberxavfsizlikning ijtimoiy jihatlarining elementlari etib – jamiyatdagi mavjud ijtimoiy sohalarning tizim va tizim osti *(ta’lim, tibbiyot, bank, madaniyat va b.)* qismlari sifatida qaralgan va shu kontekstda kiberxurujlarning ijtimoiy ta’sir ko‘rsatkichlari tahlil etilgan.

Dissertatsiyaning mazkur bobida, kiberxavfsizlikning siyosiy jihatlari sifatida muayyan davlatning siyosiy tizimini tashkil etuvchi davlat organlarinining axborot yoki ma’lumotlar xavfsiziligini milliy manfaatlar nuqtai nazaridan himoya qilishga qaratilgan faoliyati yoritib berilgan.

Jumladan, kiberxavfsizlikning siyosiy jihatlari muayyan mamlakatda davlat boshqaruvi organlarining axborot xavfsizligi tizimi, xususan, virus tovlamachilari yoki tarqatuvchilari, zararli dasturiy ta’minot, ijtimoiy muhandislar, veb-serverlar, kibermadaniyat kabi qismlariga salbiy ta’sir etish orqali yuzaga keltiradigan munosabatlar yig‘indisi sifatida qaraladi.

Dissertatsiyaning **“Markaziy Osiyo davlatlari xavfsizligiga kibermakonda vujudga kelayotgan zamonaviy tahdidlar”** deb nomlangan ikkinchi bobida “Destruktiv g‘oyalarning kibermakonda tarqatilishi va uning salbiy jihatlari”, “Xorijiy davlatlarning kiberterorizm va ekstremizmga qarshi kurash yo‘nalishidagi tajribasi va uni mintaqaviy hamkorlikka ta’siri”, “Markaziy Osiyo davlatlarida kiberxavfsizlikni ta’minlashga innovatsion yondashuv va qo‘llash mexanizmlari” kabi masalalar tadqiq qilingan.

Dissertatsiyaning mazkur bobida destruktiv tushunchasi va uning holat sifatidagi falsafiy-siyosiy mazmuni hamda destruktiv g‘oyalarning kibermakonda tarqalashi va uning salbiy jihatlari ochib berilgan. Ularning tarqalish maydoni, yuzaga keluvchi oqibatlar natijalarida yuzaga keladigan masalalar tahlil etilgan.

Destruktiv g‘oyalarning shakllanishi va yuzaga kelishiga diniy ta’limotlarning roli zamonaviy siyosiy jarayonlarda muhim rol o‘ynaydi. Xususan, tarixiy va falsafiy nuqtai-nazardan, tabiat, jamiyat va inson borlig‘idagi destruktiv holatlar to‘g‘risidagi ilk g‘oyalarni diniy manbalarda uchratish mumkin. Masalan, zardushtiylikda olam taraqqiyoti, umuman olganda, ezgulik va yaxshilikka bo‘lgan intilish sifatida tasavvur qilinadi: qachondir ezgulik xudosi Axuramazdaning mutlaq hukmronligi ta’minlanishi, ezgulik va adolat qaror topishi aniq. Lekin ezgulikning ilk shakllari *(osoyishta hayot, bunyodkorlik, obodonchilik va sh. k.)* vujudga kelgani zahoti unga qarama-qarshi o‘laroq yovuzlik shakllari

(qurg‘oqchilik, qurbonliklar, urushlar, kasalliklar va sh.k.) ham paydo bo‘ladi[8]. Zardo‘shtiylikda barcha destruktiv holatlarning muallifi mavjud – bu ruhlantiruvchi kuch Ahriman obrazi bilan bog‘lanadi. Ahriman barcha yovuz kuchlarning manbai, ilhomchisi hisoblanadi: u goho odamlarni yovuzlik bandisiga aylantiradi *(Zahhokni taxtga o‘tqizgani kabi)*, goho ularni to‘g‘ri yo‘ldan chalg‘itadi *(Jamshidni yo‘ldan urgani kabi)*[9]. Dissetatsiyada aynan destruktiv g‘oyaning mazmuni ushbu kontekst orqali ochib berilgan va tegishli xulosalar qilingan.

Barqaror taraqqiyotni ta’minlashda barcha dinlar qatori islom dinining roli ham beqiyos sanaladi. Jumladan islomda yovuzlik ko‘proq insonning salbiy hatti-harakatlari bilan bog‘lab talqin qilinadi. Shu asosida tadqiqotda islom dini aqidalariga ko‘ra, inson hayotining maqsadi Allohga ishonish, uni bilish, unga mehr qo‘yish va ibodat qilish orqali ma’naviy yuksaklikka erishish bilan bog‘liq jihatlar bugungi kunda destruktiv g‘oyalarning oldini olishda samarali usul sifatida tahlil etilgan. Bizga ma’lumki, Qur’oni Karimning “Baqara” surasida: “Balkim, sizlar yoqtirmagan narsa *(aslida)* o‘zlaringiz uchun yaxshi, yoqtirgan narsangiz esa *(aslida)* sizlar uchun yomon bo‘lib chiqar. Alloh bilur, sizlar esa bilmaysizlar”, deb ta’kidlanganligini[10] o‘zi ham insonlarni ezgulik yo‘liga chorashini bildirgan.

Tadqiqotda “destruktivlik” tushunchasi ayniqsa, insonning destruktivlik faoliyatini yetarli darajada o‘rganilmaganligi, bu borada atamalarning bir ma’noli talqini mavjud emasligi unga aniqlik kiritish zaruratini yuzaga keltirish sifatida qaraladi. Chunki, tahdidbardosh jamiyatni shakllantirish jarayonida unga ta’sir o‘tkazuvchi salbiy illatlarning fundamental asoslarini tadqiq etish dolzarb ekanligini anglatmoqda. O’rganligan tadqiqot asosida destruktiv g‘oya – ijtimoiy munosabatlarning buzilishiga sabab bo‘ladigan, nazariyalar, qarashlar, me’yorlar, qadriyatlar va ularni jamiyatda tarqatish usullaridan iborat salbiy destruktiv voqelik degan xulosani berdi.

Tadqiqot ishida destruktiv g‘oya destruktivlik darajasiga qarab aniqlangan. Chunki, barcha destruktiv g‘oyalar ham mutlaq va umumiy mezonlarga tayanmasligi ilmiy jihatlar asoslab beriladi. Fikrimizcha destruktiv g‘oya mavjud ijtimoiy munosabatlarning buzilishiga xizmat qiladi. Mutlaq destruktiv g‘oyalar esa, har qanday ijtimoiy aloqalar va institutlarning buzilishiga xizmat qiladigan, umuman jamiyatning rivojlanishi, hatto, yashashiga imkon qoldirmaydigan g‘oyalardir. “Ular insonparvarlik tamoyiliga zid bo‘lgan, jamiyatni tarafkashlarga ajratib, bo‘lib tashlaydigan, bir millatni boshqasidan ustun qo‘yadigan, oliy irq da’vosida boshqa xalqlarni qirg‘in qilishga chaqiradigan destruktiv g‘oyalardir. Diniy aqidaparastlik va jangari irqchilik *(rasizm)*, buyuk davlatchilik shovinizmi va ashaddiy *(agressiv)* millatchilik, fashizm va bolshevizm mafkuralari ana

[8] Маҳмудов Т. “Авесто” ҳақида.- Т.:Шарқ, 2000.
[9] Қаранг: Фирдавсий А. Шоҳнома.- Т.:А.Навоий номли Ўзб. Миллий кутубх.нашр., 2012.
[10] Қуръони Карим. Бақара сураси. 216-оят.// Қуръони Каримнинг машҳур суралари фазилати./ Нашрга тайёрловчилар А.Аҳмад, И.Нуруллоҳ.- Т.: Ғ.Ғулом номидаги нашр., 2021.- Б.119.

shunday vayronkor g‘oyalar tizimini tashkil etadi”[11].

Yuqorida ko‘rib o‘tganimizdek mazkur bobda destruktiv g‘oyalarga alohida e’tibor qaratilib, tahlillar amalga oshirilgan, jumladan, destruktiv g‘oyalarni turli vaziyatlar, xususiyatlariga qarab ularning turlarini va tasnifini keltirish mumkin. Masalan, asosiy ta’limotlariga qarab, ob’ekti, sub’ekti, yo‘nalishlari, sabablari, oqibatlari, zamon va makon hamda boshqa jihatlari nazarda tutiladi. Bizning fikrimizga ko‘ra, destruktiv g‘oyalarni umumiy ko‘rinishi, manbalariga ko‘ra diniy va dunyoviy hamda aralash shakldagi ko‘rinishga ajratish mumkin.

Dissertatsiyaning asosiy ketegoriyasi bo‘lgan “kibermakon” tushunchasiga ta’rif bizning amaldagi qonunchiligimizda ko‘rsatib o‘tilgan ammo uning mazmuni bugungi kunning talab va tahdidlar darajasini aniqlashda ushbu ta’rifning o‘zi yetarli emas ekanligini zamonaviy siyosiy jarayonlardagi kibertahdidlarning ko‘rinishlari misolida aytish mumkin. Mamalakatimiz qonunchiligida kibermakon — axborot texnologiyalari yordamida yaratilgan virtual muhit[12] sifatida yoritilgan. Tadqiqot ishida kiberxavfsizlikni ta’minlash jaaryonida Markaziy Osiyo mintaqasi davlatlari, rivojlangan xorijiy davlatlar hamda MDH davlatlari misolida tahlil etishni joiz hisoblandi.

Xususan, o‘rganilgan adabiyotlar va materiallar asosida MDH davlatlarida ham mazkur atamaning rasmiy ta’rifi keltirilmagan degan shaxsiy xulosaga kelindi. Biroq, bugungi kundagi Rossiya Federatsiyasida “Kiberxavfsizlik konsepsiyasi” loyihasida mazkur tushuncha izohlangan bo‘lib, unga ko‘ra, kibermakon - inson faoliyati turlari shakllarida *(shaxs, tashkilot, davlat)* foydalanadigan “Internet” va boshqa telekommunikatsiya tarmoqlari hamda ular faoliyatini ta’minlaydigan texnologik infratuzilmalar yig‘indisidan iborat makon, informatsion makonning faoliyat maydoni[13] sifatida qaraladi.

Tadqiqot ishida bugungi kunda kibermakonda tarqalayotgan kiberjinoyatlarning uch muhim xususiyati tahlil etilgan. Bularga:

1) kompyuter - jinoyat maqsadi bo‘lgan jinoyatlar;

2) kompyuter - jinoyatni sodir etish vositasi hisoblangan jinoyatlar;

3) tasodifiylikda undan oddiy jism sifatida foydalanib sodir etilgan jinoyatlar. [14] Mana shu 3 ta jihat mintaqada kibertahdid sifatida mintaqaviy hamkorlik jarayonlariga o‘zining salbiy ta’sirini ko‘rsatmoqda.

Dissertatsiya ishida Markaziy Osiyo mintaqasida kiberxafsizlikni ta’minlash jarayonida ta’sir etuvchi kiberjinoyatlar “kompyuter orqali jinoyat sodir etish”, “elektron jinoyatchilik” va “yuqori texnologiyalar jinoyatchiligi”, “virtual jinoyatchilik” turlari sifatida o‘zining salbiy oqibatlarini keltirib ko‘rsatmoqda. Bu jinoyatlarning ko‘payishi uning global miqyosida ta’sirini o‘tkazmoqda.

---

[11] Назаров К. Ғоялар фалсафаси. –Тошкент: Akademiya, 2011. – 296-301 б.

[12]Ўзбекистон Республикасининг 2022 йил 15 апрелдаги “Киберхавфсизлик тўғрисида”ги Қонуни.// https://lex.uz/uz/docs/5960604

[13]Концепция Стратегии кибербезопасности Российской Федерации. //http://www.council.gov.ru/media/files/41d4b3dfbdb25cea8a73.pdf

[14] Marc D. Why the people don’t care about computer crime?//Harvard Journal of Law and Technology № 10-3.1997. C. 465-494,

Mamlakatimiz misolida kiberjinoyatlarni o‘sish jarayoniga e’tibor qaratadigan bo‘lsak quyidagi raqamlarni o‘zi ham bu borada jinoyatchilik ko‘payib borayotganligini anglatadi. Misol uchun kiberxurujlar mamlakatimizda so‘nggi 3 yilda oshganligini aytish mumkin. Xususan, 2022 yilda Toshkent shahrida axborot texnologiyalari orqali **4332** ta kiberjinoyatlar sodir etilgan. Bu ko‘rsatkich 2021 yilga nisbatan ikki barobarni tashkil etadi. Toshkent shahrida fuqarolarni bank plastik kartalaridan pullarini aldov yo‘llari bilan o‘zlashtirish holatlari keskin ortgan. 2022 yildan buyon kiberjinoyatlar oqibatida Toshkent aholisi kamida **45,2 mlrd so‘m** zarar ko‘rgan. Bu pullarning bor yo‘g‘i **9,2 mlrd.** so‘mi undirib berilgan xolos.

Qolaversa, bugungi kunda Toshkent shahrida axborot-texnologiyalari orqali sodir etilayotgan kiberjinoyatlarni ijara bilan bog‘liq jarayonlarda kupincha firibgarlik kurboni bo‘lmoqda. Ya’ni boshlang‘ich badalni ko‘rmasdan, bilmasdan turib o‘tkazib berish holatlari, yoki OLX platformasidan vosita sifatida foydalanayotgan shaxslarning domiga tushib qolish holatlari kuzatilmoqda. Ya’ni fuqarolarimiz u yoki bu predmetni arzon narxlarda sotib olish yuzasidan qilinayotgan reklamalarda firibgarlik qurboniga aylanmoqda. Ushbu misollar bu kibertahdidlarning borgan sari rivojlanish tendensiyalari ortib borayotganligini ko‘rsatmoqda.

Dissertatsiyada muammoni chuqurroq o‘rganish maqsadida bu borada ko‘plab tajribalarga ega bo‘lgan AQSh, Xitoy, Saudiya Arabistoni, Turkiya, Germaniya kabi mamlakatlar tajribalari ko‘rib chiqilgan.

Tadqiqot ishida AQSh tajribasi quyidagilarga namoyon bo‘ldi. AQSh milliy tadqiqotlar kengashi *(National Research Council)* ma’lumotiga ko‘ra, davlatlar internetni noqonuniy kontentda himoyalashda ikki xil usuldan foydalanmoqda: Bularga davlat darajasida *(provayderlar orqali)* cheklovlar joriy qilish; alohida foydalanuvchilar yoki tashkilotlar darajasida maxsus filtrlash dasturlarini o‘rnatish hisoblanadi.

Shuningdek, AQSh qonunchiligida filtrlash dasturlarini maktab, kutubxona, internet - kafelar va jamoatchilik foydalanadigan joylarda majburiy tarzda o‘rnatiladi. Internetni tashkiliy va texnik jihatdan tartibga solinishi har bir davlat aloqa va axborot infratuzilmasiga javobgar organlari tomonidan olib boriladi. Huquqiy tartibga solish bo‘yicha umumiy ahvol quyidagicha, AQShda Internetda keng qo‘llanadigan filtrlash amaliyoti bo‘lmasada, Internet umuman “tartibga solinmaydi” deb bo‘lmaydi. Hukumatning Internet - kontentni tartibga solish quyidagi to‘rtta muammodan kelib chiqqan. Bularga, bolalarni himoyalash va axloqlilik, milliy xavfsizlik, intelektual mulk hamda kompyuter xavfsizligi masalalari kiradi.

Dissertatsiyada Xitoy Xalq Respublikasining tajribasi quyidagi jihatlada aks ettirilgan. Bu davlatda Internetni nazorat qilish tizimi markazlashgan bo‘lib, nazorat qilish va tozalashning qat’iy usul va chora-tadbirlari qo‘llanilmoqda. Bu borada “Oltin qalqon” loyihasi asosida ishlar olib borilmoqda. Loyiha asosida xavfsizlikni ta’minlash uchun veb-sahifalarni filtrlashda kalit so‘zlar va saytlarning “qora ro‘yxati” tuzilgan. Saytlarga IP-adreslari bo‘yicha cheklovlar o‘rnatilgan.

Xitoyda internet-kafedan foydalanuvchilar uchun majburiy ro‘yxatdan o‘tish yo‘lga qo‘yilgan, shuningdek, qonunga qarshi chop etilgan axborotlarni nazorat qilib turuvchi Internet-politsiyasi ham faoliyat yuritadi. 2009 yilning 1 iyulidan Xitoydagi barcha kompyuterlarga pornografiya va axloqsiz mazmundagi ma’lumotlarga Internet-filtrlar qo‘yilishi ko‘rib chiqildi. Mazkur filtrlar mamlakatda sotuvga chiqarilgan barcha kompyuterlarga ishlab chiqaruvchi korxonaning o‘zida o‘rnatib chiqarilishi belgilab qo‘yildi. Bundan tashqari, hukumat barcha internet-pravayderlarini va internet-kafelarni qat’iy nazorat ostiga oldi. Umuman olganda bugungi kunda Xitoy Internet tarmog‘i tizimi to‘rtta asosiy tarmoqdan iborat bo‘lib ular qo‘yidagilardan iborat: ChinaNet - Axborot sanoati vazirligiga tegishli yetakchi tijoriy tarmoq, Golden Bridge Network - Jitong korparatsiyasiga tegishli kichikroq tijoriy tarmoq, China Science & Technology Network- ilmiy tarmog‘i, China Educational & Research Network - ta’lim maskanlari va akademik institutlarni birlashtiruvchi tarmoqlar hisoblanadi.

Saudiya Arabistoni kiberxavfsizlik masalasini terrorizm xavfi bilan birgalikdagi faoliyat sifatida ko‘radi va shu bo‘yicha strategik mukammal dasturlarni ishlab chiqib, butun jamiyatni qamrab oluvchi usullar bilan omma ongidan ekstremistik kayfiyatni yo‘q qilishga harakat qilmoqda. Saudiyaning bu boradagi xatti-harakatlari ikki bosqichli bo‘lib, u rasman 2005 yildan boshlab ishga tushirildi. Avvaliga shubhali terrorchilarni qamoqqa olish bilan boshlandi. Biroq, faqat bu harakatlar bilan chegaralanib qolinmadi. Qamoqdagi shaxslar bilan tezda muloqot o‘rnatilib, radikallashuvning asosiy sabablari o‘rganildi hamda ularning islom dini bo‘yicha tushunchalari tahlil qilindi. Ushbu tizimli ishlarni asosan uch xil kesimda tashkil qilindi: diniy, ruhiy va madaniy. Saudiya hukumati tomonidan olib borilgan bunday dasturlar ekstremistlar sonini keskin kamaytirgan bo‘lishiga qaramay, ayrim muammolar haligacha saqlanib qolmoqda. Jumladan, so‘nggi yillarda radikal kuchlar tomonidan internet tarmog‘idan g‘oyalarini kengroq tarqatish va shu yo‘l bilan o‘z tarafdorlari sonini orttirishga bo‘lgan urinishlarining ortib borishi sharoitida Saudiya hukumatini jamiyat va undagi yoshlar qatlami radikallashuvining oldini olish borasida profilaktik choralarni kuchaytirishga undamoqda.

Saudiya rasmiylarining ma’lumotlariga ko‘ra, 1998 yilda 15 ta ekstremistik veb-sahifa mavjud bo‘lgan, hozirgi kunda bir necha ming veb-sahifalarni tashkil etadi. Ularning aksariyati o‘z serverlarini Saudiya Arabistonidan tashqarida, AQSh, Yevropa, Xitoy va Janubiy-Sharqiy Osiyo davlatlarida joylashtirgan.

O’zbekistonda ekstremizmga qarshi kurashish, radikallashuv darajasini pasaytirish va jamiyatda bunday salbiy unsurlar ko‘payishining oldini olish uchun kerakli tavsiyalar ishlab chiqildi. Ularni amaliyotga quyidagicha joriy qilish lozim deb hisoblaymiz:

Ekstremistik faoliyatga olib keladigan yoki jamiyatda radikalizm uchun asos bo‘layotgan holatlarni aniqlash;

Yoshlarda dunyoviylik ruhiyatini mustahkamlaydigan ilmiy, ma’naviy tadqiqotlarni ko‘paytirish va ularning xulosalarini amaliyotga joriy qilish;

Mamlakatda obro‘ga ega bo‘lgan diniy arboblar va ulamolarni ekstremizmga va radikalizmga qarshi profilaktik jarayonlarga keng jalb qilish;

Yoshlarda milliy g‘urur, milliy iftixor tuyg‘ularini kuchaytirish orqali zo‘ravonlikka, ekstremizm va radikalizmga qarshi immunitetni mustahkamlash va kuchaytirish;

Ommaviy axborot vositalari va ijtimoiy tarmoqlarda radikalizmning oqibatlari, uning sabablari to‘g‘risida qisqa lo‘nda axborotlarni tarqatishning ta’sirchan uslublari hamda mexanizmlarini ishlab chiqish;

Radikal kayfiyati yoki ekstremistik xulq-atvori aniqlangan toifalar bilan ishlashning ma’rifiy uslublarini joriy qilish, ularni jahon adabiyotining durdona asarlarini o‘qishlari va anglashlari uchun shart-sharoit yaratish;

Radikalizm va zo‘ravon ekstremizm aslida Islom dinini qo‘llab-quvvatlash emas, jamiyatni jaholatga boshlab, taraqqiyotdan ortda qoldiradigan va qoloqlikka yuz tutishiga sabab bo‘ladigan omil ekanligini ilmiy-ma’rifiy isbotlagan tadqiqot namunalarini yaratish hamda turli axborot vositalari orqali maqsadli auditoriyaga yetkazish;

Ekstremizmga qarshi kurashda xotin-qizlarning roli va imkoniyatlariga yetarlicha e’tibor qaratilmayapti. Oila, mahalla, maktablar va shunchaki el orasida mutaassiblikni kamaytirishda ayollardan samarali foydalanish mumkin. Shu sababli, bu mavzuga bag‘ishlangan ilmiy ishlar va tadqiqotlarni, shuningdek, sotsiologik izlanishlarni olib borish maqsadga muvofiq.

Radikalizm va zo‘ravon ekstremizmga qarshi kurashish borasida katta yutuqlarni qo‘lga kiritgan xorijiy mamlakatlar bilan tajriba almashishni yo‘lga qo‘yish, ularning mutaxassislarini ma’lum bir maqsadli vazifalar uchun jalb qilish kabilarni amaliyotga joriy etish o‘z samarasini beradi.

Markaziy Osiyoda ham davlat darajasida, ham xalq hayotida raqamlashtirish jarayoni jadal davom etmoqda. Elektron hujjat aylanishi, davlat xizmatlarini raqamlashtirish, onlayn xaridlar, elektron hamyonlar – bularning barchasi allaqachon mahalliy aholisining urbanizatsiyalashgan hayotiga mustahkam kirib borgan va bu jarayon davom etmoqda.

Ammo, uning salbiy tomoni ham: shaxsiy ma’lumotlarning sizib chiqishi, mablag‘larni hisob raqamidan o‘g‘rilash, turli operatsiyalarda boshqa odamlarning ma’lumotlaridan foydalanish va boshqa shunga o‘xshash xavflar, ortib bormoqda. Dunyodagi kiberjinoyatlar, kiberjosuslik va kiberurushlar Markaziy Osiyo mintaqasiga yetib borgani ham ayni haqiqatdir.

Birlashgan Millatlar Tashkilotining Xalqaro elektraloqa ittifoqi *(International Telecommunication Union, ITU)* Markaziy Osiyo mamlakatlari ekspertlari tomonidan tuzilgan global kiberxavfsizlik indeksida Qozog‘iston 2020-yilda eng yuqori o‘rinlarni egalladi – 192 davlat orasida 38-o‘rin. Keyingi o‘rinlarda O’zbekiston - 78, Qirg‘iziston - 100, Tojikiston bu reytingda 146-o‘rinda.

Markaziy Osiyoning barcha davlatlari raqamli va kiberxavfsizlik sohasida ko‘plab qonun hujjatlari, strategiyalar, konsepsiyalar qabul qildi va zamonaviy

voqelikda bu sohadagi xavf va tahdidlar yanada kuchayishini anglab, o‘z salohiyatini oshirishga intilmoqda. Biroq, hukumatlar kiberhimoyani mustahkamlash va nafaqat o‘z davlat manfaatlarini, balki, o‘z mamlakatlari aholisining ma’lumotlarini ham himoya qilish uchun e’tibor berishlari kerak bo‘lgan ko‘plab jihatlar bor.

Xususan, **Qozog‘iston** o‘z kibermakonini tashqi tahdidlardan himoya qilish uchun allaqachon ko‘p ishlarni amalga oshirgan, shuningdek, mutaxassislar tayyorlashga katta e’tibor qaratmoqda.

Masalan, “Qonunchilik darajasida hozirda xavfsizlikni ta’minlashning yanada amaliy yo‘nalishlarini o‘z ichiga oluvchi Milliy “Kiberqalqon 2.0 (Киберщит 2.0)” siyosatining ikkinchi talqinini ishlab chiqilmoqda.

Bundan tashqari, hozirda davlat idoralari va xususiy sektorni shaxsiy ma’lumotlarni saqlash va qayta ishlash uchun xavfsizroq va mas’uliyatni oshirish maqsadida “Ostona” xalqaro moliya markazi va milliy audit muhiti ishtirokida shaxsiy ma’lumotlarni himoya qilish siyosatini ko‘rib chiqilmoqda.

Qirg‘izistonda ham qator ishlar amalga oshirildi. Masalan, kiberxavfsizlik strategiyasi qabul qilingan bo‘lib, u barcha tomonlarning manfaatlarini hisobga olgan holda ishlab chiqilgan. Xavfsizlik Kengashi, jumladan, davlat idoralari mutaxassislari, iqtisodiy muhit va xususiy sektordan kelib chiqqan holda muvofiqlashtiruvchi kengash tashkil etilgan. Bundan tashqari, “Shaxsiy ma’lumotlar to‘g‘risida”gi qonun yaratilib, qabul qilinganidan 14-13 yil o‘tib, mamlakatda **Shaxsiy ma’lumotlarni himoya qilish agentligi tashkil etilgan**i va hozirda faoliyat yuritib bormoqda.

Tojikistonda kiberxavfsizlik masalasi Tojikiston Respublikasi “Axborot xavfsizligini ta’minlash Konsepsiyasi”da, “Davlati axborot siyosati Konsepsiya”da, bir qator boshqa idoraviy qonunlar bilan bog‘liq kiberjinoyatchilik va zo‘ravon ekstremizmga qarshi onlayn va oflayn rejimda tartibga solinadi.

O’zbekiston Respublikasida ham 2019-yilda “Shaxsga doir ma’lumotlar to‘g‘risida”gi qonun qabul qilindi, unda shaxsiy ma’lumotlar nimadan iboratligi, ular qanday va qayerda saqlanishi belgilab qo‘yildi. Bundan tashqari, 2022-yilda “Kiberxavfsizlik to‘g‘risida”gi O’zbekiston Respublikasining Qonuni qabul qilindi. Qonunga ko‘ra, kibermakonda shaxs, jamiyat va davlat manfaatlarini tashqi va ichki tahdidlardan himoya qilish davlatning kiberxavfsizlik sohasidagi ustuvor vazifasi ekanligi belgilab qo‘yilgan.

Dissertatsiyaning **“Markaziy Osiyo mintaqasida kibexavfsizlikni ta’minlash istiqbollari”** deb nomlangan uchinchi bobida “O’zbekiston Respublikasining kiberxavsizlikni ta’minlashda tajribasi”, “Mintaqada kiberxavfsizlikni ta’minlashning takomillashtirish mexanizmlari” kabi masalalar tadqiq qilingan.

O’zbekistonda oxirgi yillarda axborot sohasiga, xususan, axborot xavfsizligini ta’minlashga oid qonunchilik bazasini mustahkamlash, jurnalist kadrlarni tayyorlash va malakasini oshirish, OAV xodimlarining jamiyatni demokratlashtirish, tub

islohotlarni amalga oshirishdagi ishtirokini faollashtirish yuzasidan muhim tadbirlar bajarildi.

Jumladan, O'zbekiston Respublikasida kiberxavfsizlik sohasiga tegishli bo'lgan **17 ta** qonun hujjati, **9 ta** Prezident Farmon va Qarorlari, **14 ta** Vazirlar Mahkamasining Qarori, shuningdek, tegishli normalar va ko'plab idoralararo me'yoriy-huquqiy hujjatlar qabul qilingan. Ammo, shu bilan birga bu borada ayrim xavf va tahdidlar masalasi saqlanib qolinayotgan edi:

davlat organlari va aloqa operatorlari o'rtasida kiberhujumlarni kuzatish ularning oqibatlarini bartaraf etish bo'yicha o'zaro hamkorlik yetarli darajada yo'lga qo'yilmagan;

davlat axborot-kommunikatsiya infratuzilmasi ob'ektlarini identifikatsiyalash jarayonlarining yakuniga yetkazilmaganligi;

muhim axborot infratuzilmasi ob'ektlarida axborot tizimlari va resurslarining xavfsizlik tizimi mukammal ishlab chiqilmaganligi yoki malakali mutaxassis kadrlarlarga bo'lgan ehtiyojning qolayotgan edi.

Shu sababli, O'zbekiston Respublikasining Prezidenti Sh.Mirziyoyev bu xususida quyidagilarni ta'kidlab o'tganlar: "Mamlakatimizda demokratik islohotlarni yanada chuqurlashtirish va fuqarolik jamiyatini rivojlantirish konsepsiyasini amalga oshirishda biz, ilgarigidek, fuqarolarning o'zini o'zi boshqarish organlari – mahallalar, shuningdek, nodavlat notijorat tashkilotlar, erkin va xolis ommaviy axborot vositalari faol o'rin egallaydi."[15] Shu o'rinda, 2017 yilda "Ijtimoiy fikr" jamoatchilik fikrini o'rganish markazi tomonidan aholi o'rtasida "Fuqarolar davlat boshqaruvi va mahalliy hokimiyat organlari faoliyatining samaradorligi to'g'risida" mavzusida so'rovnoma o'tkazilganligini aytib o'tish joiz. So'rovning ko'rsatishicha, O'zbekistonliklarning 80,6 % fuqarolarning xavfsizligi, huquqlari, erkinliklari va qonuniy manfaatlari ta'minlanganligini yuqori baholaganligini ko'rish mumkin[16].

Mustaqillik yillarida O'zbekistonning kiberxavfsizlikni ta'minlash tajribasining siyosiy-huquqiy asoslarning shakllanishiga ko'ra 4 bosqichga bo'lib o'rganilgan:

Birinchi bosqich, 1991-2001 yillarni o'z ichiga oladi. Ushbu yillar davomida axborot sohasiga doir davlat siyosati ishlab chiqildi hamda huquqiy asoslar yaratildi.

Ikkinchi bosqich, 2002-2012 yillarda axborot sohadagi siyosiy-huquqiy o'zgarishlarni ichiga oladi. Mazkur bosqichda axborot sohasiga doir turli yo'nalishlarining asoslarini mustahkamlashga, institutsional jihatdan takomillashtirishga e'tibor qaratildi.

Uchinchi bosqich, 2013-2016 yillardagi davrni qamrab oladi. Ushbu

[15] Мирзиёев Ш.М. Ўзбекистон Республикаси Президенти лавозимига киришиш тантанали маросимига бағишланган Олий Мажлис палаталарининг қўшма мажлисидаги нутқидан, Тошкент шаҳри, 14.12.2016

[16] O'zbekistonliklarning 80,6 foizi fuqarolarning xavfsizligi va qonuniy manfaatlari ta'minlanganligini yuqori baholaydi. 28.12.2017. www.daryo.uz/k/2017/12/28/ozbekistonliklarning-806-foizifuqarolarning-xavfsizligi-va-qonuniy-manfaatlari-taminlanganligini-yuqori-baholaydi

bosqichda respublikada axborot xavfsizligini ta’minlashga oid davlat siyosatini amalga oshirishga xizmat qiluvchi mutassaddi tashkilotlarni tashkil etish huquqiy me’yorlar bilan mustahkamlandi.

Jumladan, “Aloqa to‘g‘risida”gi *(1992),* “Davlat sirlarini saqlash to‘g‘risida”gi *(1993)*, “Elektron hisoblash mashinalari uchun yaratilgan dasturlar ma’lumotlar bazalarining huquqiy himoyasi to‘g‘risida”gi *(1994)*, “Noshirlik faoliyati to‘g‘risida” *(1996)*, “Axborot olish kafolatlari va erkinliklari to‘g‘risida”gi *(1997)*, “Jurnalistik faoliyatni himoya qilish to‘g‘risida”gi *(1997),* “Ommaviy axborot vositalari to‘g‘risida”gi *(1997)*, “Radiochastota spektri to‘g‘risida”gi *(1998)*, “Reklama to‘g‘risida”gi *(1998)*, “Telekommunikatsiyalar to‘g‘risida”gi *(1999)* qonunlarda axborot sohasiga oid normativ-huquqiy bazani yaratishga asosiy e’tibor qaratilgan. Keyingi yillarda qabul qilingan “Axborot erkinligi va prinsiplari to‘g‘risida”gi *(2002)*, “Pochta aloqasi to‘g‘risida”gi *(2000),* “Axborotlashtirish to‘g‘risida”gi *(2003),* “Elektron raqamli imzo to‘g‘risida”gi *(2003),* “Elektron hujjat aylanishi to‘g‘risida”gi *(2004),* “Elektron tijorat to‘g‘risida”gi *(2004),* “Elektron to‘lovlar to‘g‘risida”gi *(2005),* “Mualliflik huquqi va turdosh huquqlar to‘g‘risida”gi *(2006),* “Davlat hokimiyati va boshqaruvi organlari faoliyatining ochiqligi to‘g‘risida”gi *(2014),* “Jismoniy va yuridik shaxslarning murojaatlari to‘g‘risida”gi *(2014),* “Huquqiy axborotni tarqatish va undan foydalanishni ta’minlash to‘g‘risida”gi *(2017),* “Bolalarni ularning sog‘lig‘iga zarar yetkazuvchi axborotdan himoya qilish to‘g‘risida”gi *(2017)* qonunlarda axborot sohasining turli yo‘nalishlarida axborot munosabatlarini tartibga solish hamda respublikada axborot xavfsizligini ta’minlashga urg‘u berilganligini ko‘rish mumkin.

To‘rtinchi bosqich, 2017-yildan hozirgacha bo‘lgan davrni ichiga oladi. Ushbu davr axborot sohasi xususan, axborot xavfsizligini ta’minlashning siyosiy-huquqiy asoslarini mustahkamlashdagi tub o‘zgarishlar bilan ahamiyatli hisoblanadi. Jumladan, siyosiy yo‘nalishda O’zbekiston Respublikasini rivojlantirishning beshta ustuvor yo‘nalishi bo‘yicha Harakatlar strategiyasida “Xavfsizlik, millatlararo totuvlik va diniy bag‘rikenglikni ta’minlash, chuqur o‘ylangan, o‘zaro manfaatli va amaliy ruhdagi tashqi siyosat yuritish” deb nomlangan beshinchi yo‘nalish doirasida mamlakatning konstitutsiyaviy tuzumini, suverenitetini, hududiy yaxlitligini himoya qilishga doir chora-tadbirlarni ro‘yobga chiqarish, kiberxavfsizlik sohasining normativ-huquqiy asoslarini takomillashtirish belgilangan edi. Aynan mazkur davrlarda mamlakatimizda kiberxavfsizlikning huquqiy, ma’naviy-etik, texnologik, tashkiliy, fizik, texnik *(qurilmaviy va dasturiy)* himoya choralari ko‘rildi.

Ushbu davrda O’zbekiston Respublikasi kibermakonida kiberxavfsizlik masalalariga yagona yondashuvni belgilash maqsadida O’zbekiston Respublikasi Davlat xavfsizlik xizmati tomonidan «Kiberxavfsizlik to‘g‘risida»gi O’zbekiston Respublikasi qonuni loyihasi ishlab chiqildi. Ushbu qonun loyihasini tayyorlash jarayonida kiberxavfsizlik sohasida rivojlangan xorijiy davlatlar Rossiya, Xitoy, AQSh, Qozog‘iston, va Singapur tajribalari o‘rganilib, tahlil qilindi. O’zbekiston

Respublikasi “Kiberxavfsizlik to‘g‘risida”gi qonun loyihasi ishlab chiqish jarayonida manfaatdor vazirlik va idoralarining ekspertlarini jalb qilgan holda ishchi guruh tashkil etilgan bo‘lib, bahslar, uchrashuvlar, seminarlar va videokonferensiyalar o‘tkazildi.

Ushbu **8 ta** bob, **40 ta** moddadan iborat mazkur Qonun Qonunchilik palatasi tomonidan 2022 yil 25 fevral kuni qabul qilingan. Senat tomonidan 2022 yil 17 mart kuni ma’qullagan. 2022 yil 15 aprel kuni Prezident tomonidan imzolangan[17]. 2022 yil 17 iyuldan qonuniy kuchga kirdi. O’zbekistonda kiberxavfsizlik sohasidagi yagona davlat siyosatini Prezident belgilaydi; Davlat xavfsizlik xizmati esa kiberxavfsizlik sohasidagi vakolatli davlat organi hisoblanadi.

Tadqiqot ishida mintaqada kiberxavfsizlikni ta’minlashning takomillashtirish borasida yutuqlar bilan birga, o‘zini yechimini kutayotgan masalalar bor ekanligini ko‘rsatdi.

Markaziy Osiyo mintqasining kiber maydoni to‘liq chegaralangan yo‘q. Ammo so‘nggi o‘n yillikda u sezilarli darajada o‘sdi deb aytish mumkin. Qozog‘iston, Qirg‘iziston va Tojikistonning mobil telekommunikatsiya bozorlarida deyarli "bir odam uchun bir telefon" ko‘rsatkichiga erishildi, O’zbekiston va Turkmanistonda ham ushbu ko‘rsatgich bo‘yicha ijobiy natijalarga erishdi.

Ammo shu bilan birga Markaziy Osiyo ikki qo‘shni davlat Rossiya va Xitoyning kiberjinoyatchiligi yuqori bo‘lgan kibermakonning bir qismiga aylanib borayotganligi ham tahdidlar sonini reallashib borayotganligini ko‘rsatmoqda. Masalan, 2011 yilda butun dunyo bo‘lab amalga oshirilgan va 12,5 milliard AQSh dollar zarar keltirgan kiberhujumlarning uchdan bir qismidan ko‘prog‘i rus tilida so‘zashuvchi mamlakatlar vakillari tomonidan amalga oshirilgan.

Rossiya kiberjinoyatchilik olamida ayniqsa onlayn firibgarlik, spam, va internet tizimlariga foydalanuvchilarning kirishlarini to‘xtatib qo‘yadigan hujumlar bo‘yicha yetakchi davlat hisoblanadi. Ushbu faoliyatga jalb qilingan guruhlar uyushgan jinoiy elementlar tomonidan tobora ko‘proq nazorat qilinmoqda. Markaziy Osiyo kibermadaniyati rus tilida shakllangan va mahalliy kiberjinoyatchilik tarmoqlari Rossiyadagi shunday tarmoqlar bilan aloqador deb hisoblanadi. Shuningdek, Xitoy ham iqtisodiy jinoyatlar bilan shug‘ullanadiganlar kiber jinoyatchilar uchun boshpana hisoblanadi.

2011-yilda chop etilgan AQSh hisobotida ikkala davlat ham o‘z rivojlanishi uchun yuqori texnologiyalar orqali josuslik qilganlikda ayblangan va Xitoy "iqtisodiy josuslikning eng faol va kuchli jinoyatchilari" yashaydigan joy deb e’tirof etilgan.[18] Qolaversa, 2011 yilda, Siandagi Yevroosiyo iqtisodiy forumi sammitida Qozog‘iston rasmiylari davlat tarmoqlariga 500,000ga yaqin hujumlarga duch kelganliklarini haqida bayonot berdi. Xususan, 2011 yil yozida Qozog‘iston hukumatidagi va chet eldagi diplomatik vakolatxonalardagi yuzlab kompyuterlarga xakerlarga kompyuter nazorati va maxfiy ma’lumotlarni olish

[17] Ўзбекистон Республикасининг “Киберхавфсизлик тўғрсида”ги Қонуни. https://lex.uz/uz/docs/5960604

[18] Аналитический обзор по Центральной Азии. №2, июнь, 2012.; Автор благодарит сотрудников компании AESMA за помощь в написании данного обзора, см. www.aesma-group.com.

imkoniyatini beradigan virus tarqatildi.

Aynan bu turdagi kiberjinoyatlar asosan foydali moliyaviy va sanoat ma’lumotlarini olishga intilayotgan mahalliy uyushgan jinoiy guruhlar deb aytish mumkin.

Shundan kelib chiqib, kibertahdidlar tobora ortib borayotgan shiddatli davrda Markaziy Osiyo mintaqasi davlatlari ushbu muammolarni bartaraf etishda quyidagilarga e’tibor qaratishi maqsadga muvofiq deb hisoblanadi:

Birinchidan, kiberxavfsizlik sohasida mintqada yagona yechim bo‘ladigan institutsional tuzilmalar faoliyatida yagona qarash va fikrlar uyg‘unligini ta’minlash lozim. Bunda, Markaziy Osiyo davlatlari kiberxavfsizlik sohasidagi xalqaro hamkorlikka munosabatini aniqlashtirib olishi kerak. Bu munosabatlar mintaqa davlatlarining bu boradagi milliy manfaatlarini aniqlab olishi, ularni qanday va qaysi mexanizmlar asosida ta’minlashi ustuvor vazifaga hamda harakatga aylanishi bilan ro‘yobga chiqadi.

Ikkinchidan, Markaziy Osiyo mintaqasi davlatlari kiberxavfsizlik sohasida ichki o‘zro integratsiyani amalga oshirishi lozim. Tadqiqot doirasida to‘plangan ma’lumotlar tahlili shuni ko‘rsatadi-ki, mintqada Qozog‘iston Respublikasi mintaqadagi boshqa davlatlari orasida o‘zining kiber himoya siyosati bilan ancha amaliy ishlarni olib borilayotganiligini ko‘rsatmoqda. Xususan, Baykonur kosmodromidagi Kazkosmos agentligi kabi davlat tashkilotlari yordamida mamlakat o‘zining kosmik dasturini rivojlantirmoqda, uning asosiy maqsadi sun’iy aloqa yo‘ldoshlarini uchirishni nazorat qilish hisoblanadi.

Qozog‘istonning 2011 yildan beri orbitada bo‘lgan "KazSat 2" sun’iy yo‘ldoshi hozirda mamlakat hududidagi raqamli ma’lumotlarni nazorat qilishga yordam berib kelmoqda. Qolaversa, bu istiqbolda Qozog‘iston harbiylarini aerokosmik sohada, shuningdek Kaspiy dengiz flotida-dengiz konlarini, neft tankerlari o‘tadigan yuk tashish yo‘llarini, ekologik xavflarni kuzatish uchun elektron yechimlarni ishlab chiqishni rejalashtirayotganligini anglatadi. Bunda Markaziy Osiyoda ichki xavfsizlik raqamlashtirish masalasi kun tartibiga chiqadi.

Uchinchidan, Markaziy Osiyoda kiberxavfsizlikni kuchaytirish ko‘plab mamlakatlarda bo‘lgani kabi moliyalashtirish va texnologiyalarni ekspluatatsiya qilishdagi qiyinchiliklar tufayli sekin suratlarda amalga oshirilmoqda. Kiberxavfsizlik bo‘yicha mablag‘larning yetishmasligi sababli, hatto mintaqadagi Qozog‘iston ham o‘zining markaziy va mahalliy tashkilotlari uchun antivirus uskunalari va dasturiy ta’minot bilan ta’minlashda ancha orqada qolmoqda.

Shuningdek, mintaqada kiberxavfsizlikning ushbu yo‘nalishining yetarli darajada rivojlanmayotganligining boshqa sabablaridan biri Markaziy Osiyo siyosiy rejimlarining o‘ziga xosligidadir. Ya’ni mintaqa davlatlarining axborot siyosatidagi o‘ziga xos jihatlar, o‘zining milliy manfaatlariga asoslanishi ekanligi bilan ajralib turadi.

Jumladan, "Tojikiston Respublikasi axborot xavfsizligi konsepsiyasiga ko‘ra, axborot xavfsizligi axborot makonida, shuningdek, internetda milliy

manfaatlarni himoya qilish tushiniladi[19].

To‘rtinchidan, Markaziy Osiyo davlatlarining sa’y-harakatlariga qaramay, axborot xavfsizligiga tahdidlar kuchaymoqda, jumladan, virtual makonda ekstremistik va terroristik guruhlarning faolligi oshmoqda. Ekstremistlar "ijtimoiy tarmoqlardagi shubhali saytlar"dan o‘z tarafdorlari safini to‘ldirishning eng samarali usuli deb bilishmoqda.

Virtual tahdidlarning yana bir ko‘rinishi yoshlar o‘rtasida “onlayn qimor”ning avj olishi bilan bog‘liq. Xususan, onlayn qimor o‘yinlari bilan bog‘liq jinoyatlar 2019 yilda **55 ta**, 2020 yilda **86 ta**, 2021 yilda **103 ta**, 2022 yilda **146 ta**ni tashkil etgan. Mamlakatimizda onlayn qimor o‘yinlari bilan bog‘liq jinoyatlarning harbiy xizmatchilar o‘rtasida sodir etilishi ham muammoning naqadar jiddiy ekanligini ko‘rsatmoqda.

Bu borada, mintaqada kiberxavfsizlikni ta’minlashning takomillashtirish mexanizmlari borasida mintaqada davlatlari oldida turgan bir qator ustuvor vazifalarga yanada e’tibor qaratishi joiz. Jumladan,

ushbu makonda xalqaro huquqning umume’tirof etilgan tamoyillariga rioya qilish;

kompyuter xavfsizligi sohasidagi tadqiqotlar va ishlanmalarni muvofiqlashtirish va qayta yo‘naltirish;

mavjud kompyuter xavfsizligi markazlarining vaziyatli xabardorligini oshirish;

maxfiy ma’lumotlar bilan ishlashda foydalaniladigan kompyuter tarmoqlarining xavfsizlik darajasini oshirish;

kompyuter xavfsizligi bo‘yicha ta’lim dasturlarini joylashtirish;

strategiyalar, texnologiyalar va kompyuter xavfsizligi dasturlari sohasida "oldinga sakrash" ni amalga oshirish bo‘yicha harakatlar rejasini ishlab chiqish.

1. Markaziy Osiyo mamlakatlaridagi axborot xavfsizlikning bugungi holati, kibermakonda ekstremizm va radikalizmning tashviq qilinishi amaliyotlari va oqibatlariga qarshi kurash olib borish siyosatining normativ-huquqiy bazasini takomillashtirish;

2. Ekstremistik va terroristik tashkilotlarning faoliyati bilan postsovet makonida tahdidlarning transformatsiyaga uchrashi jarayonining tahlilini o‘rganish va baholash;

3. Tahdidlarni tahlil qilish orqali Markaziy Osiyo mamlakatlaridagi kiberterrorizm va zo‘ravonlikka asoslangan ekstremizmning zamonaviy shakllarini ko‘rib chiqish va ijtimoiy tarmoqlardagi bunday ekstremizm, radikalizm, millatchilik va ksenofobiya tahdidlariga qarshi kurash chora va mexnaizmlarni takomillashtirish;

4. Zamonaviy kibermakonda jihodchilar sub-madaniyatining o‘ziga xos jihatlarini va qanday amal qilishini tushunish va kibermakondagi jinoiy

[19] Ахборот технологиялари ва киберхавфсизлик соҳасидаги минтақавий эксперти Асомиддин Атоев.// https://cabar.asia/en/expert-meeting-what-do-central-asian-countries-do-to-ensure-cybersecurity

tahdidlarning aniqlanishi va ularga qarshi kurashning psixologik jihatlarini aniqlash;

5. Kibermakonda xalqaro terroristik tashkilotlar faoliyatining transformatsiyasi, bugungi kunda qisman Afg‘onistonda in qurgan terroristik to‘dalar tomonidan internet makonlarini o‘zlarining qabih maqsadlari yo‘lida foydalanish shakllari va metodlarini ko‘rib chiqish va takomilashtirish.

Shundan ko‘rish mumkinki, Markaziy Osiyo davlatlarining o‘zaro ishonch, milliy manfaatlariga xizmat qiladigan prinsiplarga asoslangan kiberxavfsizlikni ta’minlovchi *(axborot almashinuvi, hamkorlikda ilmiy tadqiqotlar olib borish, qo‘shma tadbirlar tashkil etish va h.k.)* maxsus ilmiy-amaliy hamkorlik tizimini amalda joriy qilinishi ichki va tashqi tahdidli holatlarni oldini olishda *(priventiv yondashuv)* zarur ekanligini ko‘satadi.

Qolaversa, Markaziy Osiyo davlatlaridagi axborot xavfsizligi bilan bog‘liq muammolarni giyohvand moddalar savdosi, ekstremizm va uyushgan jinoyatchilik muammolari bilan qiyoslash mumkin. Shu sababdan axborot urushlariga qarshi kurash Markaziy Osiyo mamlakatlarining kuchlarini birlashtirishni talab qiladi.

Markaziy Osiyodagi bugungi kun vaziyati nafaqat kompyuter texnologiyalari sohasida yuqori malakali kadrlar tayyorlashni, balki mintaqashunoslik bo‘yicha chuqur bilimlarni egallagan, axborot hurujlariga qarshi tura olish malakasiga ega bo‘lgan entopsixologlar, antropologlar, tarixchilar, siyosatchilar va boshqa kadrlarni yetishtirib chiqarish talab qiladi[20].

Bundan ko‘rinadi-ki, Markaziy Osiyo mintaqasida yangidan yangi xavfsizlikka tahdidlar yuzaga kelayotgan sharoitda davlatlar o‘z kuch va imkoniyatlarini birlashtirishlari hamda o‘zaro hamkorlikdagi pereventiv mexanizmlarni ishlab chiqishi lozim.

XULOSA

Mazkur tadqiqot ishini o‘rganish va unga oid bo‘lgan turli-ko‘rinishdagi nazariy va amaliy manbalarni o‘rganish asosida “Markaziy Osiyo mintaqasida kiberxavfsizlikni ta’minlashning ijtimoiy-siyosiy jihatlari” mavzusidagi tadqiqot ishi davomida quyidagi xulosa va takliflar ilgari suriladi:

1. “Kiberxavfsizlik” tushunchasi murakkab kategoriya sifatida etirof etiladigan jarayon hisoblanadi. Uning tarkibidagi yondosh atamalar kiberxavfsizlik tushunchasini yaxlit holda ifodalashga imkon beradi. Shu sababli ushbu tushunchalarga oid bo‘lgan tushunchalar turkumini o‘zbek tiliga oid bo‘lgan lug‘atlarga kiritishga zaruriyat sezmoqda.

Buning uchun faylasuflar, tilshunoslar, siyosatshunoslar va huquqshunoslardan iborat bo‘lgan olimlar ushbu tushunchalarning ma’no va mazmunini qayta ko‘rib chiqishi ham sohaga tegishli bo‘lgan maxsus lug‘atlarga kiritish taklif etiladi.

[20] Tojikiston geosiyosiy tadqiqotlar markazi direktori, professor G. M. Maytdinova.// http://berlek-nkp.com/analitics/7355-kiberbezopasnost-i-protivodeystvie-kiberterrorizmu-i-ekstremizmu-v-stranah-centralnoy-azii.html

2. Markaziy Osiyo kiberxavfsizligi tizimi va uning o‘ziga xos xususiyatlari to‘liq ravishda institutsionallashmagan. Natijada kiberxavfsizlikni ta’minlash borasida yondoshuv va amaliy harakatlar tizimlashtirilmaganligini ko‘rsatmoqda. Bu o‘z navbatida kiberxavfsizlikni ta’minlashda mintaqada o‘zaro siyosiy islohotlarni yangi bosqichga chiqarish asosida tuzilmaviy-funksional institutlarni yaratishga zaruriyat bor ekanligini ko‘rsatadi.

Qolaversa, tuzilmaviy-funksional institutlar faoliyatini yo‘lga qo‘yish orqali mintaqada siyosiy muloqotni rivojlantirish asosida mintaqa davlatlarining savdo, investitsiyalar, transport, energetika, qishloq xo‘jaligi va ekologiya sohalarida qo‘shma dastur va loyihalarni ilgari surish, madaniy-gumanitar hamda xavfsizlik sohasidagi zamonaviy tahdid va xatarlarga qarshi chora ko‘rish mexanizmlari yaratilishiga erishiladi.

3. Markaziy Osiyo mintqasida kiberxavfsizlikning turli ko‘rinishlari yoshlar qatlamiga jiddiy ta’sir o‘tkazmoqda. Bu esa davlatlarning milliy xavfsiziligina zarur ko‘rsatish darajasini oshirishi mumkin.

Buning uchun rivojlangan xorijiy davalatlarning bu boradagi tajribalarini chuqur tahlil etish asosida, mintaqa yoshlari, ularning yosh xususiyatlari, urf-odatlaridan kelib chiqib, axborotdan foydalanish bo‘yicha maxsus strategik dastur ishlab chiqish maqsadga muvofiq. Aynan bu ta’lim muassasalari, hamda jamoat joylaridagi faoliyatlarini huquqiy tartibga solishga olib keladi.

4. Markaziy Osiyo mintaqasi kiberterrorizm va zo‘ravonlikka asoslangan kiberjinoyatlar sonini oshib borishi mamlakatlarining madaniy-gumanitar tizimini zaiflashib borishiga sabab bo‘lishi mumkin. Shuning uchun “2024-2030 yillarga mo‘ljallangan Markaziy Osiyo mintaqasi davlatlarining kiberxavfsizlikni ta’minlash bo‘yicha strategiyasini” ishlab chiqishi lozim. Strategiyaning asosiy yo‘nalishlari etib mintaqa davlatlarining barchasining milliy manfaatlariga javob beradigan ustuvor yo‘nalishlar aniqlash va ravshan belgilab olinishi kerak. Ayniqsa, strategiyada noyob madaniy-tarixiy va ma’naviy merosimizni xalqaro maydonda keng targ‘ib etishda ommaviy axborot vositalari va nohukumat tashkilotlar, zamonaviy axborot-kommunikatsiya texnologiyalari imkoniyatlaridan faol foydalanish hamda Markaziy Osiyo yoshlari imkoniyatlarini kengaytirish va ularning salohiyatini ro‘yobga chiqarish orqali mintaqaviy tizimni shakllantirishga erishiladi.

5. O’zbekiston taraqqiyotining yangi bosqichida mintaqa davlatlarining rivojlanish jarayonlarini tizimli tahlil qiladigan “aqliy markaz”lar faoliyatini takomillashtirish lozim. Aynan mintaqada kiberxavfsizlik masalalarini fundamental jihatdan o‘rganish uchun Markaziy Osiyo xalqaro instituti qoshida maxsus kiberxavfsizlik masalasini tadqiq etib boruvchi bo‘lim faoliyatini yo‘lga qo‘yish orqali mavjud muammolar va ularning yechimlarini hamda bu boradagi istiqbolli loyihalarni amalga oshirish bo‘yicha takliflarni kiberxavfsizlik bo‘yicha vakolatli davlat organlariga taqdimnoma kiritish kerak.

6. Markaziy Osiyo mintaqasida saqlanib qolayotgan fundamental muammolarni yechishda milliy manfaatlarni hisobga olgan holda, izchil muloqot

va kelishuvlar asosida tartibga solishga intilishi mintaqada do‘stlik, ishonch va o‘zaro manfaatli hamkorlikning yangicha muhitini yanada takomillashtirib borish global muammolarga - global javoblar berishni taqozo etmoqda.

Bunda mintaqa davlatlari ekspertlari tomonidan “Markaziy Osiyo davlatlarida kiberxavfsizlik va kiberterrorizm hamda ekstremizmga qarshi kurashning zamonaviy bosqichi: natijalar, muammolar va istiqbollar” mavzusida mintaqaviy uchrashuvlarni o‘tkazishi kerak. Bu o‘z navbatida O’zbekiston taraqqiyotining yangi bosqichida davlatimizni pragmatizm, mintaqaviy yakdillikni qo‘llab-quvvatlash va keskin masalalarni tezkor hal etishga yo‘naltirilgan faol tashqi siyosati amalga oshirishda xizmat qiladi.

НАУЧНЫЙ СОВЕТ DSc. 03/30.12.2019.S.01.08 ПО ПРИСУЖДЕНИЮ УЧЕНЫХ СТЕПЕНЕЙ ПРИ НАЦИОНАЛЬНОМ УНИВЕРСИТЕТЕ УЗБЕКИСТАНА

НАЦИОНАЛЬНЫЙ УНИВЕРСИТЕТ УЗБЕКИСТАНА

ТУРДИЕВ УЙГУН РАХМАТУЛЛАЕВИЧ

СОЦИАЛЬНО-ПОЛИТИЧЕСКИЕ АСПЕКТЫ ОБЕСПЕЧЕНИЯ КИБЕРБЕЗОПАСНОСТИ В ЦЕНТРАЛЬНОАЗИАТСКОМ РЕГИОНЕ

23.00.02 – Политические институты, процессы и технологии

АВТОРЕФЕРАТ
диссертации доктора философии (PhD) по политическим наукам

Ташкент – 2023

Тема диссертации доктора философии (PhD) зарегистрирована Высшей аттестационной комиссией за № B2022.3.PhD/Ss373.

Диссертация доктора философии (PhD) выполнена в Национальном Университете Узбекистана.

Автореферат диссертации на трёх языках (узбекском, русском, английском (резюме)) размещен на веб-странице Национального Университета Узбекистана (www.nuu.uz) и на информационно-образовательном портале «Ziyonet» (www.ziyonet.uz).

Научный руководитель:	**Пахрутдинов Шукритдин Илясович** доктор политических наук, профессор
Официальные оппоненты:	**Кучкаров Вахоб Хашимович** доктор политических наук, профессор
	Гайибназаров Шухрат Гойибназарович доктор политических наук, профессор
Ведущая организация:	**Ташкентский государственный университет востоковедения**

Защита диссертации состоится ---- 2023 года в --- часов на заседании Научного совета DSc.03/30.12.2019.Ss.01.08 по присуждению ученых степеней при Национальном университете Узбекистана (Адрес: 100174, город Ташкент, улица Университетская, дом 4. Тел.: (99871) 227-12-24, факс: (99871) 246-53-21, e-mail: nauka@nuu.uz. Здание факультета Социальных наук Национального университета Узбекистана, 5-этаж, ауд. 511).

С диссертацией можно ознакомиться в Информационно-ресурсном центре Национального университета Узбекистана (зарегистрирована за номером --). (Адрес: 100174, город Ташкент, улица Университетская, дом 4. Административное здание НУУз, 2-этаж, комната 4. Тел.: (99871) 246-02-24; факс: (99871) 246-02-24.

Автореферат диссертации разослан «_____ »_____ 2023 года.
(реестр протокола рассылки № _____ от «_____» _____ 2023 года).

А.Г.Муминов
Заместитель председателя Ученного совета по присуждению ученых степеней, д.п.н., профессор

Г.Т.Исанова
Ученый секретарь Научного совета по присуждению ученых степеней, доктор философии (PhD) по политическим наукам

А.Г.Муминов
Председатель Научного семинара по присуждению ученых степеней при Научном совете, доктор политических наук, профессор.

ВВЕДЕНИЕ (аннотация диссертации доктора философии (PhD)

Происходящей в мире кибератаки и гибридные угрозы, возникающие в результате многоформатной политической трансформации, оказывают свое негативное влияние на интересы человека, общества и государства, на динамическую устойчивость политической системы. Посредством различных информационных технологий, негативного воздействия на систему функционирования государства и его органов управления, а также на молодежный слой посредством эгоистичных целей, методов, завоевываются умы молодежи, формируются в ней субкультурные проявления, формируются идеи, противоречащие реформам государства и общества. В современных условиях становится актуальным обеспечение и защита приоритета национальных интересов путем преодоления стратегических целей эгоистичных идеологических сил, сохранения генофонда молодежи, принятия эффективных превентивных мер в отношении различных факторов риска, угрожающих ситуаций, создания атмосферы устойчивого межгосударственного сотрудничества.

В мире формирование социально-политических основ кибербезопасности создание фундаментальных основ сохранения межгосударственных национально-территориальных, национально-культурных связей, обеспечение собственной безопасности человека, общества и государства путем формирования иммунитета к различным опасностям и угрозам в киберпространстве, предотвращение нарушения баланса сил в геополитическом пространстве, возникновение нестабильных и опасных угроз ведутся значительные научные исследования. В проводимых исследованиях совершенствуется государственное регулирование кибербезопасности, система правового, организационного, научно-технического и нормативно-методического обеспечения, обеспечивается целостность информационных систем и ресурсов, в том числе выявление факторов киберугрозы и риска в Центральноазиатском регионе, повышение механизмов их предупреждения и устранения, а также возможность точного прогнозирования перспектив сферы безопасности в условиях усиления трансграничных угроз. региональные институты в области безопасности, актуальное значение приобретает повышение эффективности исполнения норм и правил.

В последние годы в Узбекистане в условиях проводимых широкомасштабных реформ особое внимание уделяется реформированию государственной политики в области информации, коренному совершенствованию отраслевой нормативно-правовой базы, созданию безопасного пространства для реагирования на кибератаки на региональном и международном уровнях. "Узбекистан в своей внешней политике уделяет приоритетное внимание Центральноазиатскому региону. Это-путь, выбранный всесторонне, глубоко продуманно. Узбекистан, расположенный в самом центре Центральной Азии, напрямую заинтересован в том, чтобы этот

регион стал регионом стабильности, последовательного развития и добрососедства”[21]. Среди актуальных задач-укрепление национальной государственности в государствах Центральной Азии, политические, исторические, идейно-идеологические основы развития системы безопасности, инициативы Узбекистана в обеспечении региональной безопасности и его исследования в рамках национальных интересов.

Данная диссертационная работа служит в определенной степени в реализации задач, определенных в Указах Президента Республики Узбекистан №ПФ-4947 «О Стратегии действий по дальнейшему развитию Республики Узбекистан» от 7 февраля 2017 года, №ПФ-60 года «О Стратегии развития» Нового Узбекистана на 2022-2026 годы» от 28 января 2022 г., Стратегия Республики Узбекистан по противодействию экстремизму и терроризму на 2021-2026 годы от 1 июля 2021 года, Закон Республики Узбекистан “О кибербезопасности” от 15 апреля 2022 года и других нормативно-правовыех документах, относящихся к данной сфере.

Соответствие исследования приоритетным направлениям развития науки и технологии в республике. Диссертационное исследование выполнено в рамках приоритетного направления развития республиканской науки и технологий «Формирование системы инновационных идей в социально-правовом, экономическом, культурном, духовно-образовательном развитии информационного общества и демократического государства и пути их реализации».

Степень изученности проблемы. При анализе задач, поставленных в диссертации, опирались на исследования, проведенные в мировой и узбекской политологии. Теоретические научные исследования и работы по вопросам «кибербезопасности», «киберпространства», «кибертерроризма и экстремизма» обширны и охватывают тот или иной аспект проблемы. Такие научные исследования можно разделить на три группы:

к первой группе относятся научные труды западных учёных: М. Дюверье, Ш. Айзенштадта, Г. Алмонда, Д. Истона, Р. Арона, Т. Парсонса, Р. Даля, А. Тойнби, Д. Икеда, В. Эдварда[22]. . В исследованиях этих ученых основное внимание уделяется взглядам на общество и его политическую систему, на его внутренние структурные структуры; научные труды российских ученых - ко второй группе; Это Е. Примаков, В. Гумелёв, В. Федотова, В. Колпаков, А. Нысанбаев, А. Гусейнова, Е. Агошковой, Н. Губанов, Б. Включены работы таких ученых, как Исаев, В. Белоликов. Партийные системы в контексте глобальных изменений были проанализированы и освещены в новом контексте на основе новых взглядов этих исследователей. Вышеупомянутые зарубежные исследования носят фундаментальный характер и имеют особое значение в поиске решения теоретических проблем научных исследований; третью группу составляют

[21] Мирзиеев Ш.М. Одобрение нашего народа-высшая оценка нашей деятельности. Том 2 . -Т.: Узбекистан. 2018. – С.248.

[22] В диссертации подробно представлены работы упомянутых отечественных и зарубежных ученых.

местные исследователи И. Эргашев, С. Атамуратов, Р. Джумаев, С. Джораев, Ш. Пахрутдинов, А. Моминов, Ш. Гоибназаров, Ж. Мавлонов, О. Сироджов, И. Бобокулов, Х. Умаров, У. Ботаев, К. Авазов, О.Аллаяров и другие, которые раскрыли аспекты, связанные с проблемой безопасности и стабильности в обеспечении национальных интересов, политизацией религии, правовым, политико-философским анализом международного терроризма, а также ролью и значением ИКТ в развитии государства и общества.

В частности, теоретические и практические вопросы кибербезопасности были исследованы в научно-исследовательских работах Матьякубовича на тему «Разработка методов создания устойчивых криптографических алгоритмов», по религиозным аспектам изучаемой проблемы «Религиозно-духовные процессы, связанные с киберпространством и исламом» - Абдуллаевой Мохиры Захиджановны, по юридическим аспектам «Уголовно-правовые и криминологические аспекты борьбы с преступлениями, связанными с терроризмом» - Иброхимова Джамшида Абдугофур угли.

Для Нового Узбекистана, который в сегодняшнее сложное время все больше укрепляет свое место, положение и репутацию в мировом сообществе, внедрение цифровых технологий и современных методов в науку, повышение эффективности научных исследований в высших учебных заведениях стало одним из важнейших направлений. и методы государственной политики. В частности, научно обоснованные рекомендации по повышению эффективности подготовки кадров в области политических наук, проведению комплексных систематических исследований в области формирования и развития политических основ гражданского общества, национальной государственности, формирования и реализации внутренней и внешней политики. политика государства в условиях глобализации, углубление общественно-политических реформ на этой основе и следует отметить, что разработка программ рассматривается как актуальный вопрос.

С этой точки зрения изучение социально-политических аспектов обеспечения кибербезопасности в Центральноазиатском регионе в контексте национальных интересов, в процессе изучения ее концептуальных основ как отдельного объекта исследования, ее достижений и недостатков, а также своих будущих целей, четко и тщательно определить и разработать задачи, которые следует реализовать для их достижения, а также внесение предложений и рекомендаций определяет актуальность данной темы исследования.

Связь темы диссертации с планом научно-исследовательских работ в высшем образовательном учреждении. Диссертационное исследование выполнено в соответствии с планом научной работы Национального университета Узбекистана «Общность общественно-политических, социально-экономических реформ в углублении демократических реформ и развитии гражданского общества».

Целью исследования является разработка предложений и рекомендаций по социально-политическому обеспечению кибербезопасности в Центральноазиатском регионе.

Задачи исследования:

систематизация научно-теоретических исследований по ранним теоретическим понятиям категории безопасности в политологии, их теоретическому развитию;

сравнительный анализ этапов развития кибербезопасности и освещение теоретико-практических аспектов понятия кибербезопасности и ее социально-политического явления;

показать систему кибербезопасности Центральной Азии и ее особенности, а также опыт зарубежных государств в борьбе с кибертерроризмом и экстремизмом и ее влияние на региональное сотрудничество;

разработка заключений, предложений и рекомендаций, направленных на совершенствование механизмов обеспечения кибербезопасности в регионе на основе обоснования опыта Узбекистана в области обеспечения кибербезопасности.

Объектом исследования является общественно-политические и идеологические процессы обеспечения кибербезопасности в Центральноазиатском регионе.

Предметом исследования являются превентивные подходы к социально-политическим аспектам обеспечения кибербезопасности в Центральноазиатском регионе.

Методы исследования. В исследовании использовались такие методы, как цивилизация, наблюдение, анализ и синтез, редукция, ретроспективный анализ, сравнительный метод, контент-анализ, ситуационный анализ, футурологический анализ, экспертная оценка и политическое прогнозирование.

Научная новизна исследования заключается с следующем:

обосновано, что важной основой обеспечения эффективной защиты и устойчивого развития субъективной (человек, общество, государство) и объективной (международные отношения) институциональной структуры системы безопасности от внутренних и внешних угроз является зависимость от эффективной защиты от кибератак и кибератак социального, политического, идеологического, военного, религиозного характера, угрожающих деятельности государственных органов, организаций и духовному совершенствованию молодежи;

доказано, что при реализации Национальной стратегии развития, ориентированной на все сферы общественной жизни, обеспечение стабильности и надежности информационных ресурсов, обеспечение кибербезопасности в качестве превентивного инструмента, направленного на бдительность и бдительность в эффективном электронном общении органов государственной власти с гражданами, служит высокому уровню

легитимности между государством и обществом;

обосновано, что уровень устойчивости национальной безопасности, суверенитета государств Центральной Азии прямо пропорционален способности региональных стратегически и социально-экономически значимых средств информационных технологий защищаться от любых внутренних и внешних киберугроз, обосновывается тем, что их институционально и функционально правовая основа является важной основой устойчивого развития общества;

обосновано, что слабость механизмов защиты от угроз, являющихся важным компонентом комплексной системы безопасности в Центральноазиатском регионе, наличие потока вредоносных информационных программ носит трансграничный и транснациональный характер, основываясь на взаимодействии этапов межгосударственного сотрудничества по борьбе с ним, а также на зависимости регионального и многостороннего конструктивного направления стратегического партнерства от степени сформированности системы кибербезопасности.

Практические результаты исследования заключаются с следующем**:**

в контексте решения региональных проблем обеспечения безопасности разработаны концептуальные научные выводы и предложения по борьбе с кибербезопасностью, кибертерроризмом и экстремизмом, социально-политическими аспектами кибербезопасности, выявлению факторов риска, механизмам их предотвращения и устранения. комплексным и систематическим образом;

на основе сравнительного изучения современного зарубежного и отечественного опыта даны практические рекомендации, направленные на повышение эффективности и результативности реформ, направленных на безопасность в центральноазиатском регионе Узбекистана, о том, что данная форма деятельности должна, прежде всего, служить интересам человека и обеспечивать широкое участие институтов гражданского общества в политических процессах.

Достоверность результатов исследования. Достоверность результатов исследования заключается в том, что информация получена из официальных источников, адекватности подходов и методов, сборников материалов научно-методических и научно-практических конференций республиканского и международного уровня, статей, опубликованных в специальных и зарубежных научных журналах. журналов в списке ВАК, выводы, практические предложения и рекомендации внедрены в практику, что объясняется подтверждением полученных результатов уполномоченными организациями.

Научная и практическая значимость результатов исследования.

Научная значимость результатов исследования объясняется тем, что полученные результаты могут быть использованы при совершенствовании основ политики обеспечения безопасности в регионе на основе политического исследования национальных интересов в вопросах

обеспечения кибербезопасности в Центральной Азии, теоретико-научных и теоретико-фундаментальных исследований и методологических подходов в этом направлении.

Практическая значимость результатов исследования объясняется тем, что Узбекистан выступает важным ресурсом в реализации и совершенствовании политики в области обеспечения кибербезопасности в Центральной Азии и целевых государственных программ, посвященных реформам в этой области.

Внедрение результатов исследования. По итогам изучения общественно-политических аспектов обеспечения кибербезопасности в Центральноазиатском регионе выявлено:

Новизна по обоснованию важной основой обеспечения эффективной защиты и устойчивого развития субъективной (человек, общество, государство) и объективной (международные отношения) институциональной структуры системы безопасности от внутренних и внешних угроз является зависимость от эффективной защиты от кибератак и кибератак социального, политического, идеологического, военного, религиозного характера, угрожающих деятельности государственных органов, организаций и духовному совершенствованию молодежи был использован в научном проекте на тему “создание платформы и мобильных приложений в Интернете для диалогового пространства, пропагандирующего национальность, сохранение нашего менталитета, вековых ценностей и благородных традиций” по пункту 43 “пропаганда национальных ценностей, духовных добродетелей и социального этикета”, установленный в VIII направлении программы мероприятий Республиканского центра духовности и просвещения на 2023 год (Акт №02-22/1008 Республиканского центра духовности и просвещения от 22 сентября 2023 г.). В результате, выдвинутые в диссертации предложения, рекомендации и выводы послужили проведению совместных исследований по актуальным вопросам обеспечения внутренней безопасности и устойчивого развития Узбекистана, а также по вопросам безопасности в Центральной Азии, перспективам регионального и международного сотрудничества;

Выводы по доказанию реализации Национальной стратегии развития, ориентированной на все сферы общественной жизни, обеспечение стабильности и надежности информационных ресурсов, обеспечение кибербезопасности в качестве превентивного инструмента, направленного на бдительность и бдительность в эффективном электронном общении органов государственной власти с гражданами, служит высокому уровню легитимности между государством и обществом был использован в научном проекте на тему “создание платформы и мобильных приложений в Интернете для диалогового пространства, пропагандирующего национальность, сохранение нашего менталитета, вековых ценностей и благородных традиций” по пункту 43 “пропаганда национальных ценностей, духовных добродетелей и социального этикета”, установленный в VIII направлении

программы мероприятий Республиканского центра духовности и просвещения на 2023 год (Акт №02-22/1008 Республиканского центра духовности и просвещения от 22 сентября 2023 г.). В результате материалы, подготовленные для вещания, служили для закрепления знаний, навыков и опыта населения в области повышения политического сознания и культуры, при этом содержание их было превосходным и богатым научными доказательствами;

выводы по обоснованию уровени устойчивости национальной безопасности, суверенитета государств Центральной Азии прямо пропорционален способности региональных стратегически и социально-экономически значимых средств информационных технологий защищаться от любых внутренних и внешних киберугроз, обосновывается тем, что их институционально и функционально правовая основа является важной основой устойчивого развития общества был использован в научном проекте на тему “создание платформы и мобильных приложений в Интернете для диалогового пространства, пропагандирующего национальность, сохранение нашего менталитета, вековых ценностей и благородных традиций” по пункту 43 “пропаганда национальных ценностей, духовных добродетелей и социального этикета”, установленный в VIII направлении программы мероприятий Республиканского центра духовности и просвещения на 2023 год (Акт №02-22/1008 Республиканского центра духовности и просвещения от 22 сентября 2023 г.). В результате дорожные карты, программы и сеть по направлениям риска и устойчивости человека во взаимодействии с общественными организациями, НПО и региональными отделениями политических партий в регионах послужили основой для разработки приоритетов отраслей;

новизна по обоснованию, того что слабость механизмов защиты от угроз, являющихся важным компонентом комплексной системы безопасности в Центральноазиатском регионе, наличие потока вредоносных информационных программ носит трансграничный и транснациональный характер, основываясь на взаимодействии этапов межгосударственного сотрудничества по борьбе с ним, а также на зависимости регионального и многостороннего конструктивного направления стратегического партнерства от степени сформированности системы кибербезопасности был использован в научном проекте на тему “создание платформы и мобильных приложений в Интернете для диалогового пространства, пропагандирующего национальность, сохранение нашего менталитета, вековых ценностей и благородных традиций” по пункту 43 “пропаганда национальных ценностей, духовных добродетелей и социального этикета”, установленный в VIII направлении программы мероприятий Республиканского центра духовности и просвещения на 2023 год (Акт №02-22/1008 Республиканского центра духовности и просвещения от 22 сентября 2023 г.). В результате это послужило улучшению социологических исследований, проводимых центром, а также методологии социальных критериев.

Апробация результатов исследования. Результаты исследования обсуждались на 9 научно-теоретических и научно-практических конференциях, в том числе 3 международных и 6 республиканских конференциях.

Опубликованность результатов исследования. Всего по теме диссертации выполнено 19 научных работ, в том числе 10 научных статей, 3 из которых в зарубежных научных изданиях, рекомендованных к публикации основных научных результатов докторских диссертаций ВАК, 7 - опубликовано в республиканских журналах, 9 в сборниках материалов конференций (3 на международных конференциях, 6 на местных конференциях).

Структура и объем диссертации. Диссертация состоит из введения, трех глав, восьми параграфов, заключения и списка использованной литературы. Объем диссертации – 130 страниц.

ОСНОВННОЕ СОДЕРЖАНИЕ ДИССЕРТАЦИИ

Во введении обосновывана актуальность и необходимость темы исследования, показано соответствие темы основным приоритетным направлениям развития науки и техники республики, освещена степень изученности проблемы, определены цель, задачи, объект и предмет исследовательской работы.

актуальность и необходимость темы исследования, показано соответствие темы основным приоритетным направлениям развития науки и техники республики, освещена степень изученности проблемы, определены цель, задачи, объект и предмет исследовательской работы.

Описаны методы исследования, научная новизна и практические результаты. Обоснованы достоверность, научная и практическая значимость полученных результатов. Приводятся сведения о внедрении результатов исследования, их публикации, структуре и объеме диссертации.

Первая глава диссертации называется **«Теоретико-методологические основы исследования кибербезопасности в Центральноазиатском регионе».** В ней исследуются такие проблемы, как «Понятие кибербезопасности и ее социально-политическая интерпретация», «Этапы развития кибербезопасности», «Система кибербезопасности Центральной Азии и ее особенности».

В целом проблема кибербезопасности возникла с развитием современных информационно-коммуникационных технологий и рассматривается в качестве неотъемлемой части современного мира. Мы можем наблюдать, что значение кибербезопасности в социальной и политической жизни общества возрастает.

В данной главе диссертации определяется понятие кибербезопасности, раскрываются теории о ее возникновении и развитии. В частности, в современную политическую и военную науку вошли такие категории, как

«кибербезопасность», «киберпространство»[23], «киберкультура»[24], «прокси-война», «гибридные войны». Повышенная потребность в понимании этих категорий связана с теоретическими и практическими потребностями государства и общества. Потому что острая необходимость принятия решения по вопросу кибербезопасности в новых условиях требует более глубокого изучения этих вопросов.

«Кибербезопасность» как категория в источниках трактуется по-разному. В частности, кибербезопасность – это деятельность, направленная на защиту информационных систем, сетей и программ от цифровых атак. Обычно целью таких атак является получение конфиденциальной информации, ее изменение или потеря, требование денег от пользователей или нарушение бизнес-процессов[25].

Другими словами, кибербезопасность означает защиту от случайных и преднамеренных информационных атак. Это многогранная сфера деятельности, и только системный и комплексный подход к ней может дать результат.

Кибербезопасность – это вычислительная наука, которая объединяет технологии, людей, информацию и процессы для обеспечения операций в присутствии злоумышленников. Она включает в себя создание, внедрение и анализ безопасных компьютерных систем. Кроме того, концептуально кибербезопасность представляет собой интегрированную область исследований, которая включает правовые аспекты, политику, человеческий фактор, этику и управление рисками.

В этой главе также уделяется внимание следующему:

Закон Республики Узбекистан «О кибербезопасности» определяет кибербезопасность как состояние защищенности интересов личности, общества и государства от внешних и внутренних угроз в киберпространстве[26].

Закон предусматривает следующие аспекты кибербезопасности: законность; приоритет защиты интересов личности, общества и государства в киберпространстве; единый подход к регулированию кибербезопасности; приоритет участия местных производителей в создании системы кибербезопасности; определены основные принципы Республики Узбекистан в обеспечении кибербезопасности, такие как открытость к международному сотрудничеству.

Термин «киберпространство» связан с публикацией первого романа трилогии под названием «Киберпространство» писателя Уильяма Гибсона «Нейромант» (“Neuromancer”) в 1984 году. Он описывает виртуальное

[23] Это понятие связано с публикацией в 1984 году первого романа трилогии писателя Уильяма Гибсона «Нейромант» под названием «Киберпространство». Он описывает виртуальное пространство, в котором электронные данные циркулируют на всех компьютерах мира. См.: Ахборот коммуникация технологиялари изоҳли луғати. БМТТДнинг Ўзбекистондаги ваколатхонаси. – 2010. – 573 б.

[24] Новое технократическое направление в развитии культуры. Оно основано на возможностях компьютерных игр и использовании технологий виртуальной реальности.

[25] https://www.cisco.com/c/ru_ru/products/security/what-is-cybersecurity.html

[26] Закон Республики Узбекистан «О кибербезопасности» от 15 апреля 2022 года.// https://lex.uz/uz/docs/5960604

пространство, в котором электронные данные циркулируют на всех компьютерах мира[27].

Киберпространство – это область коммуникации, осуществляемая посредством компьютерных сетей, которая широко развивается и совершенствуется с 1990 года. С социальной точки зрения под киберпространством понимают группу людей или групп, которые связаны друг с другом посредством компьютерной сети, пересекаются одновременно в разных географических точках и обмениваются графической информацией с любого имеющегося компьютера,

Сегодня в нашей стране из-за неправильного понимания реформ, проводимых в религиозной сфере, некоторыми категориями населения, набирают силу процессы религиозного фанатизма среди молодежи. В этом отношении Интернет служит средством активизации данного процесса.

Члены религиозных экстремистских и террористических организаций эффективно используют социальные сети для пополнения своих рядов. Идеологическая пропаганда, направленная на завоевание сознания молодежи, осуществляется в киберпространстве.

Например, экстремистские группы в социальных сетях «Одноклассники», «Фейсбук», «Инстаграм», «Твиттер», «Вконтакте», создавая фейковые профили типа «Абдулла Зуфар», «Садык Самарканди», «Мустафа Муджахид», «Абу-Муавия», «Ансар-Ансар», «Фулан ибн Фулан», воздействуют на сознание молодых людей идеями и призывами, пропагандирующими чуждые подрывные идеи, приглашая их отправиться с целью «эмиграции и «джихада» в «горячие точки» мира, где ведутся военные действия.

В диссертации анализируются три основные категории киберпреступлений в Центральноазиатском регионе: хулиганство, хакерство и компьютерное мошенничество. Социально-политические аспекты происхождения киберпреступлений анализируются через эти три категории.

По результатам анализа выявляется динамика их развития. По результатам исследования ООН 2018 года, **50%** стран не имеют стратегии кибербезопасности, а **25%** стран имеют правовую основу для обеспечения безопасности критически важной информационной инфраструктуры.

Также выяснилось, только **31%** стран имеют раздел о защите критически важной информационной инфраструктуры в своей стратегии кибербезопасности, и только **109** стран-участниц имеют законодательство по кибербезопасности. В **141** стране (*73%*) действуют законы о конфиденциальности в Интернете.

По результатам исследования был сделан вывод о том, что кибербезопасность является неотъемлемой частью социальной сферы или системным явлением, проявляющимся в процессе обеспечения безопасности личности.

---

[27] Қаранг: Ахборот коммуникация технологиялари изоҳли луғати. БМТТДнинг Ўзбекистондаги ваколатхонаси. – 2010. – 573 б.

Кроме того, доказано, что кибербезопасность представляет собой систему, сочетающую в себе аспекты безопасности человека, информационной безопасности, общественной безопасности и оперативной безопасности.

Например, с социальной точки зрения кибербезопасность отражается на отношениях человека с обществом, моральных отношениях или личной жизни и их связи друг с другом. В исследовательской работе элементы социальных аспектов кибербезопасности рассматривались как системные и подсистемные части существующих социальных сфер в обществе (образование, медицина, банковское дело, культура и т.д.) и в этом контексте были проанализированы индикаторы социального воздействия кибератак.

В данной главе диссертации в качестве политических аспектов кибербезопасности выделена деятельность государственных органов, составляющих политическую систему конкретного государства, направленная на защиту информации или безопасности данных с точки зрения национальных интересов.

В том числе, политические аспекты кибербезопасности рассматриваются как совокупность отношений, возникающих вследствие отрицательного воздействия вирусов-вымогателей или распространителей вредоносного программного обеспечения на систему информационной безопасности органов государственного управления определенного государства (такие ее части, как социальные инженеры, веб-серверы, киберкультура).

Во второй главе диссертации под названием «**Современные угрозы безопасности стран Центральной Азии в киберпространстве»** изучались такие вопросы, как «Распространение деструктивных идей в киберпространстве и их негативные стороны», «Опыт зарубежных стран в борьбе с кибертерроризмом и экстремизмом и его влияние на региональное сотрудничество», «Инновационный подход к обеспечению кибербезопасности в странах Центральной Азии и механизмы применения».

В данной главе диссертации раскрывается понятие деструктивности и его философско-политическое содержание, а также распространение деструктивных идей в киберпространстве и их негативные аспекты. Анализируется ареал их распространения, вопросы, возникающие впоследствии.

Значение религиозных учений в формировании и возникновении деструктивных идей играет важную роль в современных политических процессах. В частности, с историко-философской точки зрения первые представления о деструктивных ситуациях в природе, обществе и человеческом существовании можно найти в религиозных источниках. Например, в зороастризме развитие мира вообще понимается как стремление к добру и благости: несомненно, что когда-нибудь установится абсолютное правление Ахурамазды, бога добра, и добро и справедливость восторжествуют. Но как только появляются первые формы добра (мирная

жизнь, творчество, благоустройство и т. д.), появляются противоположные формы зла (засуха, жертвоприношения, войны, болезни и т. д.)[28]. В зороастризме есть автор всех деструктивных ситуаций – эта вдохновляющая сила связана с образом Аримана. Ариман считается источником и вдохновителем всех злых сил: иногда он превращает людей в рабов зла (как он посадил Заххока на трон), иногда он сбивает их с правильного пути (как он заставил сбиться с пути Джамшида)[29]. В диссертации через этот контекст раскрывается содержание деструктивной идеи и делаются соответствующие выводы.

Наряду со всеми другими религиями роль ислама в обеспечении устойчивого развития весьма значительна. Например, в исламе зло трактуется преимущественно в связи с негативными действиями человека. Исходя из этого, в исследовании, согласно принципам исламской религии, цель жизни человека – поверить в Бога, познать его, полюбить его и достичь духовных высот посредством молитвы. Мы знаем, что в Священном Коране, в суре «Аль-Бакара» сказано: «Возможно, то, что вам не нравится, будет для вас хорошо, а то, что вам нравится, будет для вас плохо». Аллах знает, а вы не знаете», - сказал он[30], что направляет людей на путь добра.

В исследовании понятие «деструктивность», особенно деструктивная деятельность человека рассматривается как недостаточно изученная, в связи с эти отсутствует однозначная трактовка термина, что порождает необходимость его уточнения. Потому что в процессе формирования устойчивого к угрозам общества становится очевидной актуальность изучения фундаментальных основ пороков, оказывающие на него негативное воздействие. На основе проведенного исследования сделан вывод, что деструктивная идея – это негативная деструктивная реальность, состоящая из теорий, взглядов, норм, ценностей и методов их распространения в обществе, вызывающих нарушение общественных отношений.

В исследовательской работе деструктивная идея определяется по степени деструктивности. Поскольку обосновывается научными аспектами, что все деструктивные идеи не опираются на абсолютные и общие критерии. По нашему мнению, деструктивная идея служит разрушению существующих общественных отношений. Абсолютно деструктивные идеи – это идеи, которые служат разрушению любых социальных отношений и институтов, не позволяют обществу развиваться или даже выживать. «Это деструктивные идеи, которые противоречат принципу гуманности, разделяют и делят общество на фракции, ставят одну нацию выше другой и призывают к истреблению других наций, притязая на высшую расу. Такую систему деструктивных идей составляют религиозный фанатизм и воинствующий

[28] Маҳмудов Т. “Авесто” ҳақида.- Т.:Шарқ, 2000.
[29] См: Фирдавсий А. Шоҳнома.- Т.:А.Навоий номли Ўзб. Миллий кутубх.нашр., 2012.
[30] Қуръони Карим. Бақара сураси. 216-оят.// Қуръони Каримнинг машҳур суралари фазилати./ Нашрга тайёрловчилар А.Аҳмад, И.Нуруллоҳ.- Т.: Ғ.Ғулом номидаги нашр., 2021.- Б.119.

расизм, великодержавный шовинизм и яростный (агрессивный) национализм, идеологии фашизма и большевизма» [31].

Как мы видели выше, в этой главе особое внимание было уделено деструктивным идеям, произведен анализ, в результате которого деструктивные идеи могут быть классифицированы в соответствии с различными ситуациями и характеристиками. Например, в зависимости от основной доктрины подразумеваются объект, предмет, направления, причины, последствия, время и пространство и другие аспекты. По нашему мнению, деструктивные идеи по общему виду и источникам можно разделить на религиозные, светские и смешанные формы.

Определение понятия “киберпространство”, являющееся основной категорией диссертации, дано в действующем законодательстве. Но содержание этого определения не достаточно для раскрытия уровня требований и угроз сегодняшнего дня, что видно на примере киберугроз в рамках современных политических процессов. Киберпространство в законодательстве нашей страны рассматривается как виртуальная среда, созданная с помощью информационных технологий[32]. В исследовании необходимым представляется проведение анализа процессов обеспечения кибербезопасности на примере государств Центрально-Азиатского региона и стран СНГ.

В частности, на основе изученных материалов и научной литературы получен вывод о том, что не представлено формальное определение данного термина также в странах СНГ. Но, в настоящее время в Российской Федерации в рамках проекта “Концепция кибербезопасности” дано толкование термина, в котором киберпространство рассматривает как “сфера деятельности в информационном пространстве, образованная совокупностью коммуникационных каналов Интернета и других телекоммуникационных сетей, технологической инфраструктуры, обеспечивающей их функционирование, и любых форм осуществляемой посредством их использования человеческой активности (личности, организации, государства)”[33]. В исследовании подвергнуты анализу три отличительных признака киберпреступности, распространных в киберпространстве на сегодняшний день. К ним относятся:

1) преступления, целью которых является компьютер;

2) преступления, в которых средством совершения противоправных деяний является компьютер;

3) преступления, в которых компьютер использован в качестве простого предмета по случайности[34].

---

[31] Назаров Қ. Ғоялар фалсафаси. –Тошкент: Akademiya, 2011. – 296-301 б.

[32] Закон Республики Узбекистан от 15 апреля 2022 года “О кибербезопасности”// https://lex.uz/uz/docs/5960604

[33]Концепция Стратегии кибербезопасности Российской Федерации. //http://www.council.gov.ru/media/files/41d4b3dfbdb25cea8a73.pdf

[34] Marc D. Why the people don’t care about computer crime?//Harvard Journal of Law and Technology № 10-3.1997. C. 465-494.

Эти три аспекта оказывают негативное влияние на процессы регионального сотрудничества в качестве региональных киберугроз.

В диссертационной работе представлены негативные последствия таких видов киберпреступлений, оказывающих воздействие на обеспечение кибербезопасности в Центрально-Азиатском регионе, как “совершение преступления посредством компьютера”, “элетронная преступность”, “преступность высоких технологий”, “виртуальная преступность”. Увеличение количества таких преступлений оказывает также воздействие на глобальном уровне.

Если обратить внимание на рост количества киберпреступлений на примере нашей страны, представленные ниже цифры свидетельствуют об увеличении данных видов преступности. Например, можно отметить увеличение киберугроз за последние 3 года. В частности, в 2022 году в городе Ташкенте совершено 4332 киберпреступлений с использованием информационных технологий. Данный показатель в два раза выше относительно 2021 года. Наблюдается стремительный рост случаев обманного усвоения денег жителей города Ташкента с банковских пластиковых карт. С 2022 года в результате киберпреступлений населению Ташкента нанесен урон в размере **45,2 млрд. сум**. Из них взыскано только **9,2 млрд. сум.**

Кроме того, в настоящее время в городе Ташкенте в сфере аренды встречается много жертв мошенников, которые совершают свои киберпреступления с применением информационных технологий, т.е. наблюдаются случаи, когда люди вносят залог удаленно, не знаю и не понимая, куда уходят их деньги, или попадают в сети злоумышленников, которые используют платформу OLX. Наши граждане становятся жертвой рекламы мошенников, обещающей те или другие предметы по дешевым ценам. Это свидетельствует о возрастании тендеций по последовательному развитию киберугроз.

В диссертации в целях более глубокого изучения проблемы рассмотрен опыт таких стран как США, Китай Саудовская Аравия, Турция, Германия.

В исследовании изучение опыта США показало следующее. Согласно данным Совета национальных исследований *(National Research Council)* США государства используют два способа защиты Интернета от незаконного контента: внедрение ограничений на уровне государства (через провайдеров); установка специальных программ фильтрации на уровне отдельных пользователей и организаций.

Кроме того, согласно законодательству США программы фильтрации в обязательном порядке устанавливаются в школах, библиотеках, интернет-кафе и общественных местах. Организационное и техническое регулирование сети Интернет в каждом государстве ведется соответствующими органами, ответственными за связь и информационную инфраструктуру. В целом правовое регулирование выглядит следующим образом: хотя в США нет практики широкого применения фильтрации

Интернета, нельзя сказать, что Интернет “не регулируется”. Регулирование правительством Интернет-контента исходит из следующих четырех проблем. К ним относятся: вопросы защиты детей и нравственности, национальной безопасности, интеллектуальной собственности и компьютерной безопасности.

В диссертации отражены следующие аспекты опыта Китайской Народной Республики в этих вопросах. В этой стране система контроля Интернета имеет централизованный характер, применяются жесткие методы и меры по контролю и очищению контента. В этом плане работы ведутся на основе проекта “Золотой щит”. Для обеспечения безопасности на основе проекта составлен “черный список” сайтов и ключевых слов при фильтрации веб-страниц. Установлены ограничения на сайты по IP-адресам.

В Китае существует обязательная регистрация для пользователей интернет-кафе, кроме того орсуществляет деятельность Интернет-полиция, контролирующая противозаконную информацию, публикующуюся в сети. Рассмотрено размещение Интернет-фильтров с 1 июля 2009 года на информацию порнографического и безнравственного характера. Определено, что данные фильтры непосредственно в производственных предприятиях на компьютеры, реализуемые в стране. Кроме того, правительство взяло под контроль все интернет-провайдеры и интернет-кафе. В целом, в настоящее время сеть Интернет Китая состоит из следующих из четырех основных сетей: ChinaNet – ведущая коммерческая сеть, принадлежащая Министерству информационной индустрии, Golden Bridge Network – коммерческая сеть корпорации Jitong, China Science & Technology Network – национальная сеть, China Educational & Research Network – сети, объединящая образовательные учреждения и академическая институты.

Опыт Саудовской Аравии также имеет свои отличия. В частности, важное значение приобретает соответствующий большой опыт политики данной страны, ведущей борьбу с радикализмом.

Саудовская Аравия рассматривает проблему кибербезопасности как деятельность, связанную с угрозой терроризма, разрабатывает стратегические выверенные программы, стремится устранить экстремистикие настрояния в сознании масс на основе методов, охватывающих все общество. Действия Саудовской Аравии в этом плане осуществляются в два этапа, которые официально начинаются с 2005 года. Вначале были арестованы подозрительные террористы. Но меры в этом направлении не ограничиваются этим. В ходе оперативного общения с лицами в тюрьмах изучены основные причины радикализации и проанализированы их религиозные взгляды. Данная системная работа проводилась в основном в трех аспектах: религиозном, психологическом и культурном. Такого рода программы, осуществляемые правительством Саудовской Аравии, хотя существенно сократили количество экстремистов, но некоторые проблемы все еще не решены. В частности, в условиях роста за последние годы попыток по широкому распространению идей радикальных

сил в сети Интернет и увеличению за счет этого своих сторонников от правительства Саудовской Аравии требуется усиление мер по профилактике радикализации общества, в особенности молодежи.

Согласно сведениям ответственных лиц в Саудовской Аравии в 1998 году было 15 экстремистских веб-страниц, в настоящее время их количество составляет несколько тысяч. Серверы большинства из них размещены за пределеами Саудовской Аравии, в США, Европе, Китае и Юго-Восточной Азии.

Разработаны необходимые рекомендации по борьбе с экстремизмом, снижением уровня радикализации в Узбекистане и предотвращения увеличения количества таких негативных факторов в обществе.

Необходимо внедрить в практику следующие рекомендации:

1. Определение ситуаций, ведущих к экстремистской деятельности и составляющих основ для появления радикализма в обществе;

2. Расширение научных, духовных исследований, укрепляющих дух светскости среди молодежи и внедрение выводов данных исследований в практику;

3. Широкое привлечение религиозных деятелей и улемов, обладающих авторитетом в стране, к профилактическим процессам по противодействию экстремизму и радикализму;

4. Укрепление и усиление иммунитета по отношению к насилию, экстремизму и радикализму посредством укорении в сознаии молодежи чувства национальной гордости;

5. Разработка действенных механизмов и методов распространения в средствах массовой информации и социальных сетях кратких и ясных сведений о последствия, причинах радикализма;

6. Внедрение просветительских методов по работе категориями граждан, у которых выявлены радикальные настроения или экстремистское поведение, создание для них условий для чтения и восприятия лучших образцов мировой литературы;

7. Проведение научно-просветительских исследований, посвященных вопросам того, что радикализм и агрессивный экстремизм на самом деле не поддерживают ислам как религию, а являются причиной невежества и отсталости, а также доводение их до целевой аудитории посредством различных средств информации;

8. Недостаточно уделяется внимание роли и возможностям женщин при противодейтсвию экстремизму. Значимой является роль женщин в снижении фанатизма в семье, махалле, школах и в обществе. В этом связи, целесообразно ведение научных работ и исследования, в частности,Ю социологических изысканий, посвященных данной теме.

9. Внедрение в практику таких мер как налаживание обмена опытом с зарубежными странами, у которых есть большие достижения в деле борьбы с экстремизмом и радикализмом, привлечение их специалистов для решения целевых задач даст определенный эффект.

В Центральной Азии как на уровне государства, так и на уровни жизни народа продолжается процесс цифровизации. Электронный документооборот, цифровизация государственных услуг, онлайн-торговля, электронные кошельки – все это давно и прочно вошло в урбанизированную жизнь местного населения и этот процесс продолжается.

Но вместе с тем, есть и негативные стороны этого явления: повышается риск утери персональных данных, кража средств с личных счетов, использование данных других людей в различных операциях и другие угрозы. Киберпреступления, кибершпионаж и кибервойны, которые есть во всем мире, также стали реальностью в Центрально-Азиатском регионе.

Согласно данным экспертов Международного союза электросвязи (*International Telecommunication Union, ITU*) Организации объединенных наций страны Центральной Азии в индексе глобальной кибербезопасности в 2020 году из 192 стран Казахстан занял 38 место, Узбекистан - 78 место, Кыргызстан - 100 место и Таджикистан - 146 место.

Все страны Центральной Азии приняли множество законов, стратегий, концепций в цифровой отрасли и сфере кибербезопасности. Также понимая усиление угроз и рисков в современных реалиях стремятся повысить свой потенциал. Но, вместе с тем, наряду с укреплением киберзащиты государственных органов и защиты своих интересов, существует также множество вопросов, на которые следует обратить внимание для защиты данных населения собственных стран.

В частности, **Казахстан** давно уже предпринял ряд мер для защиты собственного киберпространства от внешних угроз, а также уделяет большое внимание подготовке специалистов в этой области.

Например, разрабатывается вторая редакция Национальной политики “Киберщит” (Киберщит 2.0), вобравшей в себя практические направления по дальнейшему обеспечению безопасности на законодательном уровне.

Кроме того, в настоящее время в целях повышения ответственности и безопасности для хранения и обработки персональных данных государственных органов и частного сектора рассматривается политика защиты персональных данных с участием Международного финансового центра “Астана” и национального аудиторского сообщества.

И в Кыргызстане был проведен ряд организационных работ. Например, принята стратегия кибербезопасности, которая разработана с учётом интересов всех сторон. В качестве координационного совета был создан Совет Безопасности, в который вошли эксперты государственных органов, экономической среды и частного сектора. Кроме того, спустя 14-13 лет после создания и принятия Закона «О персональных данных», в стране было создано Государственное агентство по защите персональных данных. Данное агентство ведёт свою деятельность и в настоящее время.

Вопрос кибербезопасности в Таджикистане регулируется «Концепцией обеспечения информационной безопасности», «Концепцией государственной информационной политики» Республики Таджикистан и рядом других

ведомственных законов по борьбе с киберпреступностью и насильственным экстремизмом в режиме как онлайн, так и офлайн.

В 2019 году в Республике Узбекистан принят Закон «О персональных данных», в котором определяются, из чего состоят персональные данные, как и где они хранятся. Кроме того, в 2022 году принят Закон Республики Узбекистан «О кибербезопасности». Согласно закону, защита интересов личности, общества и государства от внешних и внутренних угроз в киберпространстве является приоритетной задачей государства в сфере кибербезопасности.

В третьей главе диссертации под названием «Перспективы кибербезопасности в Центрально-Азиатском регионе» рассматриваются такие вопросы, как «Опыт Республики Узбекистан в области кибербезопасности», «Механизмы совершенствования кибербезопасности в регионе».

В Узбекистане за последние годы приняты важные меры по укреплению правовой базы информационной сферы, в частности по обеспечению информационной безопасности, подготовке и повышению квалификации журналистских кадров, активизации участия работников СМИ в демократизации, а также активизация данных работников в реализации коренных реформ.

В частности, в Республике Узбекистан приняты 17 нормативно-правовых документов, 9 указов и постановлений Президента, 14 постановлений Кабинета министров, а также соответствующие нормы и множество межведомственных нормативных правовых документов, связанных со сферой кибербезопасности. Однако при этом оставался нерешённым вопрос о некоторых рисках и угрозах:

- недостаточно налажено сотрудничество между государственными органами и операторами связи по мониторингу кибератак и устранению их последствий;

- невыполнение процессов идентификации объектов государственной информационно-коммуникационной инфраструктуры;

не была разработана в полной мере система безопасности информационных систем и ресурсов на важных объектах информационной инфраструктуры, или существовала потребность в квалифицированных специалистах данной области.

По этой причине Президент Республики Узбекистан Ш.Мирзиёев в этой связи подчеркнул следующее: “Уверен, что активное участие в реализации Концепции дальнейшего углубления демократических реформ и формирования гражданского общества в стране будут принимать, как и ранее, органы самоуправления граждан - махалли, а также негосударственные некоммерческие организации, свободные и объективные средства массовой информации”[35]. Здесь следует отметить, что в 2017 году

[35] Мирзиёев Ш.М. Из выступления на совместном заседании палат Олий Мажлиса, посвященном церемонии инаугурации Президента Республики Узбекистан, Ташкент, 16.12.2016.

Центр изучения общественного мнения «Социальное мнение» провел опрос населения на тему «Граждане об эффективности государственного управления и органов местного самоуправления». По данным опроса видно, что 80,6% узбекистанцев имеют высокую оценку безопасности, прав, свобод и законных интересов граждан[36].

За годы независимости опыт Узбекистана в обеспечении кибербезопасности был разделен на 4 этапа по формированию политико-правовых основ:

Первый этап охватывает 1991-2001 годы. За эти годы была разработана государственная политика в информационной сфере и создана правовая база.

Второй этап включает политико-правовые изменения в информационной сфере в 2002-2012 гг. На этом этапе внимание уделялось укреплению основ различных направлений в информационной сфере, их институциональному совершенствованию.

Третий этап охватывает период 2013-2016 гг. На этом этапе правовыми нормами было закреплено создание официальных организаций, обслуживающих реализацию государственной политики по обеспечению информационной безопасности в республике.

В частности, видно, что в следующих законах особое внимание уделяется регулированию информационных отношений в различных сферах информационной сферы и обеспечению информационной безопасности в республике:

«О связи» (1992 г.), «О сохранении государственной тайны» (1993 г.), «О правовой охране баз данных программ ЭВМ» (1994 г.), «Об издательской деятельности» (1996 г.), «Получении информации о гарантиях и свободах» (1997), «О защите журналистской деятельности» (1997), «О средствах массовой информации» (1997), а также Законы «О радиочастотном спектре» (1998 г.), «О рекламе» (1998 г.), «О телекоммуникациях» (1999 г.) направлены на создание нормативно-правовой базы информационной сферы. Законы, принятые в последующие годы, «О свободе и принципах информации» (2002 г.), «О почтовой связи» (2000 г.), «Об информации» (2003 г.), «Об электронной цифровой подписи» (2003 г.), «Электронном документообороте» (2004 г.), «Об электронной коммерции» (2004 г.), «Об электронных платежах» (2005 г.), «Об авторском праве и смежных правах» (2006 г.), «Об открытости деятельности органов государственной власти и управления» (2014 г.), «Об обращениях физических и юридических лиц» (2014 г.), «О распространении правовой информации и обеспечении ее использования» (2017 г.), «Защита детей от информации, причиняющей вред их здоровью» на защите» (2017).

[36] 80,6 процента узбекистанцев высоко ценят обеспечение безопасности и законных интересов граждан. 28.12.2017. www.daryo.uz/k/2017/12/28/806-percent-of-uzbekists-rate-highly-the-safety-and-legal-interests-of-citizens-are-secureed.

Четвертый этап охватывает период с 2017 года по настоящее время. Этот период знаменателен для принципиальных изменений, в частности, в укреплении политико-правовых основ информационной безопасности.

В частности, в Стратегии действий по пяти приоритетным направлениям развития Республики Узбекистан в политическом направлении «Обеспечение безопасности, межэтнического согласия и религиозной толерантности» глубоко продуманы. В рамках пятого направления под названием «Проведение внешней политики во взаимовыгодном и практическом духе» определяется реализация мер по защите конституционного строя страны, суверенитета, территориальной целостности, а также совершенствование нормативно-правовой базы сферы кибербезопасности. Именно в эти периоды в нашей стране были приняты правовые, морально-этические, технологические, организационные, физические, технические (*аппаратно-программные*) меры защиты кибербезопасности.

В этот период Службой государственной безопасности Республики Узбекистан был разработан проект закона Республики Узбекистан «О кибербезопасности» в целях определения единого подхода к вопросам кибербезопасности в киберпространстве Республики Узбекистан. При подготовке данного законопроекта был изучен и проанализирован опыт развитых зарубежных стран в сфере кибербезопасности – России, Китая, США, Казахстана и Сингапура. В ходе разработки проекта Закона Республики Узбекистан «О кибербезопасности» была создана рабочая группа с привлечением экспертов соответствующих министерств и ведомств, были проведены обсуждения, встречи, семинары и видеоконференции.

Данный Закон, состоящий из 8 глав и 40 статей, был принят Законодательной палатой 25 февраля 2022 года. Одобрено Сенатом 17 марта 2022 года. Подписано Президентом 15 апреля 2022 года [37]. Он вступил в силу 17 июля 2022 года.

Единая государственная политика в сфере кибербезопасности в Узбекистане определяется Президентом; Служба государственной безопасности является компетентным государственным органом в сфере кибербезопасности.

Несмотря на достигнутый прогресс в улучшении кибербезопасности в регионе, исследования показывают, что все еще существуют проблемы, которые необходимо решить.

Киберпространство Центрально-Азиатского региона не полностью разграничено. Но можно сказать, что за последнее десятилетие он значительно вырос. На рынках мобильной связи Казахстана, Кыргызстана и Таджикистана достигнут показатель «один телефон на человека», а Узбекистан и Туркменистан также достигли положительных результатов по этому показателю.

[37] Закон Республики Узбекистан «О кибербезопасности». https://lex.uz/uz/docs/5960604

Но в то же время тот факт, что две соседние страны Центральной Азии, Россия и Китай, становятся частью киберпространства с высоким уровнем киберпреступности, показывает, что количество угроз становится все более реальным. Например, в 2011 году более трети кибератак, произошедших по всему миру и причинивших ущерб в 12,5 млрд долларов США, были осуществлены представителями русскоязычных стран.

Россия является ведущей страной в мире киберпреступности, особенно онлайн-мошенничества, спама и атак, блокирующих доступ пользователей к интернет-системам. Группы, занимающиеся этой деятельностью, все чаще контролируются организованными преступными элементами. Киберкультура Центральной Азии формируется под влиянием русского языка, и считается, что местные сети киберпреступности связаны с такими сетями в России. Китай также является убежищем для киберпреступников, причастных к экономическим преступлениям.

В докладе США за 2011 год обе страны обвиняются в использовании высокотехнологичного шпионажа в целях собственного развития, а Китай является домом для «наиболее активных и могущественных преступников в области экономического шпионажа»[38]. Более того, в 2011 году на саммите Евразийского экономического форума в Сиане казахстанские чиновники заявили, что столкнулись с почти 500.000 атаками на государственные сети. В частности, летом 2011 года на сотни компьютеров в правительстве Казахстана и дипломатических миссиях за рубежом был распространен вирус, который дал хакерам возможность управлять компьютерами и получать секретную информацию.

Можно сказать, что именно этот тип киберпреступности совершается в основном внутригосударственными организованными преступными группировками, стремящимися получить полезную финансовую и промышленную информацию.

Исходя из этого, странам Центрально-Азиатского региона представляется целесообразным обратить внимание на следующее для устранения данных проблем в период интенсивных киберугроз:

Прежде всего, необходимо обеспечить единство взглядов и мнений в деятельности институциональных структур, что будет единственным решением в регионе в сфере кибербезопасности. В связи с этим странам Центральной Азии следует уточнить свое отношение к международному сотрудничеству в сфере кибербезопасности. Эти отношения реализуются тогда, когда государства региона определяют свои национальные интересы в этой связи, как и на основе каких механизмов они будут обеспечиваться в качестве приоритетной задачи и действия.

Во-вторых, государства Центральноазиатского региона должны осуществлять внутреннюю интеграцию в области кибербезопасности. Анализ данных, собранных в рамках исследования, свидетельствует о том, что в

[38] Аналитический обзор по Центральной Азии. №2, июнь, 2012.; Автор благодарит сотрудников компании AESMA за помощь в написании данного обзора, см. www.aesma-group.com.

регионе ведется достаточно практическая работа с политикой кибербезопасности Республики Казахстан среди других государств региона. В частности, с помощью таких государственных организаций, как Казкосмос на космодроме Байконур, страна развивает свою космическую программу, основной целью которой является контроль за запуском спутников связи.

Казахстанский спутник "КазСат 2", находящийся на орбите с 2011 года, в настоящее время помогает контролировать цифровые данные на территории страны. Кроме того, это означает, что в перспективе Казахстан планирует использовать свои военные в аэрокосмической отрасли, а также на Каспийском флоте-для разработки электронных решений для мониторинга морских месторождений, судоходных путей, по которым проходят нефтяные танкеры, экологических рисков. При этом на повестку дня выходит вопрос о цифровизации внутренней безопасности в Центральной Азии.

В-третьих, укрепление кибербезопасности в Центральной Азии осуществляется медленными темпами из-за трудностей с финансированием и использованием технологий, как и во многих странах. Из-за нехватки средств на кибербезопасность даже в своем регионе Казахстан сильно отстает, в обеспечении антивирусным оборудованием и программным обеспечением своих центральных и местных организаций.

Кроме того, одна из других причин, по которой это направление кибербезопасности в регионе развивается недостаточно, заключается в специфике политических режимов Центральной Азии. То есть она отличается тем, что конкретные аспекты в информационной политике государств региона базируются на их национальных интересах.

В частности, "согласно концепции информационной безопасности Республики Таджикистан, под информационной безопасностью понимается информационное пространство, а также защита национальных интересов в сети Интернет[391].

В-четвертых, несмотря на усилия государств Центральной Азии, угрозы информационной безопасности возрастают, в том числе возросшая активность экстремистских и террористических группировок в виртуальном пространстве. Экстремисты считают это наиболее эффективным способом пополнять ряды своих сторонников с помощью "подозрительных сайтов в социальных сетях".

Еще одно проявление виртуальных угроз связано с ростом "онлайн-гемблинга" среди молодежи. В частности, преступлений, связанных с азартными играми в Интернете, было 55 в 2019 году, 86 в 2020 году, 103 в 2021 году и 146 в 2022 году. Тот факт, что преступления, связанные с онлайн-гемблингом в нашей стране, совершаются среди военнослужащих, также показывает, насколько серьезна проблема.

[39] Региональный эксперт в области информационных технологий и кибербезопасности Асомиддин Атоев.// https://cabar.asia/en/expert-meeting-what-do-central-asian-countries-do-to-ensure-cybersecurity

По нашему мнению, для повышения эффективности борьбы с этими угрозами необходимо объединить наши общие действия и скоординировать нашу совместную деятельность.

В связи с этим допустимо уделять дополнительное внимание ряду приоритетов, стоящих перед странами региона с точки зрения механизмов улучшения обеспечения кибербезопасности в регионе.

Включая,

- соблюдение общепринятых принципов международного права в этой сфере;
- координация и переориентация исследований и разработок в области компьютерной безопасности;
- повышение ситуационной осведомленности существующих центров компьютерной безопасности;
- повышение уровня безопасности компьютерных сетей, используемых при работе с конфиденциальной информацией;
- размещение обучающих программ по компьютерной безопасности;
- разработка плана действий по реализации "скачка вперед" в области стратегий, технологий и программ компьютерной безопасности.

1. Совершенствование нормативно-правовой базы политики противодействия текущему состоянию информационной безопасности в странах Центральной Азии, практике и последствиям пропаганды экстремизма и радикализма в киберпространстве;
2. Изучение и оценка результатов анализа процесса трансформации угроз на постсоветском пространстве, связанных с деятельностью экстремистских и террористических организаций;
3. Рассмотрение современных форм экстремизма на основе кибертерроризма и насилия в странах Центральной Азии путем анализа угроз и совершенствование мер и механизмов противодействия таким угрозам экстремизма, радикализма, национализма и ксенофобии в социальных сетях;
4. Понимание конкретных аспектов субкультуры джихадистов и того, как они действуют в современном киберпространстве, а также выявление преступных угроз в киберпространстве и выявление психологических аспектов борьбы с ними;
5. Трансформация деятельности международных террористических организаций в киберпространстве, рассмотрение и совершенствование форм и методов использования интернет-пространств террористическими бандами, которые сегодня частично построены в Афганистане, для достижения своих гнусных целей.

Из этого видно, что государства Центральной Азии имеют взаимное доверие, которое обеспечивает кибербезопасность, основанную на принципах, служащих их национальным интересам (обмен информацией, совместное проведение научных исследований, организация совместной деятельности и т.д.) показывает, что внедрение на практике специальной системы научно-практического сотрудничества необходимо для

предупреждения внутренних и внешних угрожающих ситуаций (превентивный подход).

Кроме того, проблемы информационной безопасности в странах Центральной Азии можно сравнить с проблемами незаконного оборота наркотиков, экстремизма и организованной преступности. Поэтому борьба с информационными войнами требует консолидации сил стран Центральной Азии.

Сегодняшняя ситуация в Центральной Азии требует не только подготовки высококвалифицированных кадров в области компьютерных технологий, но и подготовки кадров энтопсихологов, антропологов, историков, политиков и других специалистов, обладающих глубокими знаниями в области регионоведения, способных противостоять информационным атакам [40].

Из этого видно, что в условиях новых угроз безопасности в Центральноазиатском регионе страны должны усиливать свои силы., а также разработать перевентивные механизмы взаимодействия.

ЗАКЛЮЧЕНИЕ

В ходе исследовательской работы по теме «Социально-политические аспекты обеспечения кибербезопасности в Центральноазиатском регионе» выдвинуты следующие выводы и предложения на основе изучения данной исследовательской работы и имеющих отношение к ней различных теоретических и практических источников:

1. Понятие "кибербезопасность" - это процесс, который признается сложной категорией. Содержащиеся в нем схожие термины позволяют выразить понятие кибербезопасности в целостном виде. В связи с этим возникает необходимость включения в словари узбекского языка ряда понятий, относящихся к этим понятиям.

Для этого предлагается, чтобы ученые-философы, лингвисты, политологи и юристы, должны пересмотреть значение и содержание этих понятий и включить их в специальные словари, относящиеся к отрасли.

2. Система кибербезопасности Центральной Азии и ее специфика не полностью институционализированы. Результат показывает, что подход и практические действия по обеспечению кибербезопасности не систематизированы. А это, в свою очередь, свидетельствует о необходимости создания структурно-функциональных институтов на основе вывода на новый уровень взаимных политических реформ в области обеспечения кибербезопасности.

[40] Директор Центра геополитических исследований Таджикистана, профессор Г.М. Майтдинова.//http://berlek-nkp.com/analitics/7355-kiberbezopasnost-i-protivodeystvie-kiberterrorizmu-i-ekstremizmu-v-stranah-centralnoy-azii.html

Кроме того, путем налаживания деятельности структурно-функциональных институтов будет достигнуто создание механизмов противодействия современным угрозам и рискам в сфере торговли, инвестиций, транспорта, энергетики, сельского хозяйства и экологии государств региона на основе развития политического диалога в регионе.

3. В Центральноазиатском регионе различные проявления кибербезопасности оказывают серьезное влияние на молодежный слой. Это может только увеличить степень ущерба национальной безопасности государств.

Для этого на основе углубленного анализа опыта развитых зарубежных стран в этом направлении целесообразно разработать специальную стратегическую программу использования информации молодежью региона, исходя из ее возрастных особенностей, традиций. Именно это влечет за собой правовое регулирование деятельности образовательных учреждений, а также их деятельности в общественных местах.

4. Растущее число киберпреступлений, основанных на кибертерроризме и насилии, в Центральноазиатском регионе может стать причиной ослабления культурно-гуманитарной системы его стран. Поэтому необходимо разработать ” Стратегию обеспечения кибербезопасности государств центральноазиатского региона на 2024-2030 годы". Основными направлениями стратегии должны быть определены и четко различены приоритеты, отвечающие национальным интересам всех государств региона. В частности, в стратегии будет достигнуто формирование региональной системы широкого распространения нашего уникального культурно-исторического и духовного наследия на международной арене путем активного использования возможностей СМИ и неправительственных организаций, современных информационно-коммуникационных технологий, а также расширения возможностей и реализации потенциала молодежи Центральной Азии.

5. На новом этапе развития Узбекистана необходимо совершенствовать деятельность “умных центров”, которые проводят системный анализ процессов развития государств региона. Именно для фундаментального изучения вопросов кибербезопасности в регионе, путем создания при центральноазиатском Международном институте специального отдела, занимающегося исследованием проблем кибербезопасности, необходимо представить в уполномоченные государственные органы по кибербезопасности предложения по существующим проблемам и их решениям, а также по реализации перспективных проектов в этой области.

6. Дальнейшее совершенствование новой среды дружбы, доверия и взаимовыгодного сотрудничества в регионе с учетом национальных интересов в решении фундаментальных проблем, сохраняющихся в Центральноазиатском регионе, требует глобальных ответов на глобальные проблемы.

При этом государства региона должны проводить региональные встречи экспертов на тему “кибербезопасность и кибертерроризм в государствах Центральной Азии и современный этап борьбы с экстремизмом: результаты, проблемы и перспективы”. Это, в свою очередь, послужит реализации на новом этапе развития Узбекистана активной внешней политики нашего государства, направленной на прагматизм, поддержку регионального единства и оперативное решение острых вопросов.

SCIENTIFIC COUNCIL AWARDING SCIENTIFIC DEGREE DSc.03/30.12.2019.Ss.01.08 AT THE NATIONAL UNIVERSITY OF UZBEKISTAN

NATIONAL UNIVERSITY OF UZBEKISTAN

TURDIEV UYGUN RAKHMATULLAEVICH

THE POLITICAL SYSTEM OF THE SOCIETY OF UZBEKISTAN IN ENSURING THE DYNAMICS OF NATIONAL INTERESTS

23.00.02 - Political institutions, processes and technologies

ABSTRACT
dissertation of the Doctor of Philosophy (PhD) in political sciences

Tashkent – 2023

The theme of the dissertation of the Doctor of Philosophy (PhD) in political sciences was registered at the Higher Attestation Commission at the Cabinet of Ministers of the Republic of Uzbekistan under number B2022.3.PhD/Ss373.

The dissertation was performed at the National University of Uzbekistan.

Abstract of the dissertation in three languages (Uzbek, Russian, English (summary)) posted on the web page of the National university of Uzbekistan (www.nuu.uz) and educational portal "Ziyonet" (www.ziyonet.uz).

Scientific supervisor:	**Pakhrutdinov Shuritdin Ilyasovich** Doctor of Political Sciences, professor
Official opponents:	**Kuchkarov Vaxob Xashimovich** Doctor of Political Sciences, professor
	Gaibnazarov Shukhrat Gaibnazarovich Doctor of Political Sciences, professor
Leading organisation:	**Tashkent State university of Oriental**

The defense of the dissertation will be held at the meeting of the Scientific Council Awarding Scientific Degree numbered DSc.03/30.12.2019.Ss.01.08 at the National University of Uzbekistan on ----2023 at ---, (Address: 100174, University street, 4, Tashkent city. Tel.: (99871) 227-12-24; fax: (99871) 246-02-24; e-mail: nauka@nuu.uz. Building of the Faculty of Social Sciences of the National University of Uzbekistan, 5th floor, room 511)

The dissertation can be found in the Information Resource Center of the National University of Uzbekistan (registered under the number --). (Address: 100174, Tashkent city, Street Universitet, house 4, Administrative building of the National University of Uzbekistan, 2nd floor, room 4. phone.: (99871) 246-02-24; fax: (99871) 246-02-24.

The abstract of the dissertation was distributed on ----2023.
(Protocol at the registered № -- on ------ 2023).

A.G. Muminov
Deputy chairman of the scientific council council providing academic degrees, Doctor of Political Sciences, professor

G.T.Isanova
Scientific secretary of the scientific council on awarding academic degrees, Doctor of Philosophy, (PhD)

A.G. Muminov
Chairman of the scientific Seminar at the scientific council on awarding academic degrees, Doctor of Political Sciences, professor

INTRODUCTION
(Annotation of the dissertation of the Doctor of Philosophy (PhD)

The aim of the study is to develop proposals and recommendations on socio-political provision of cyber security in the Central Asian region.

The object of the research:

systematisation of scientific and theoretical studies of the initial theoretical concepts of the category of security in political sciences, their gradual development;

clarification of the concept of cyber security, its theoretical and practical aspects as a socio-political phenomenon;

comparative analysis of the stages of cybersecurity development;

Explain the Central Asian cyber security system and its peculiarities;

demonstrate the experience of foreign countries in combating cyber terrorism and extremism and its impact on regional co-operation;

To substantiate Uzbekistan's experience in ensuring cyber security;

Elaborate conclusions, proposals and recommendations aimed at improving mechanisms for ensuring cyber security in the region.

The object of the study is the socio-political and ideological processes of cyber security in the Central Asian region.

The subject of the study is preventive approaches to socio-political aspects of cyber security in the Central Asian region.

Research methods. The study used such methods as civilisational, observational, analysis and synthesis, reduction, retrospective analysis, comparative method, content analysis, situational analysis, futurological analysis, expert assessment and political forecasting.

The novelty of scientific research is as follows:

Social, political, ideological, military, religious cyberattacks are an important basis for effective protection of subjective (human, society, state) and objective (international relations) institutional structure of the security system from internal and external threats and ensuring its stable development. and the dependence on effective protection from cyberattacks is revealed;

It has been proved to ensure the stability and reliability of information resources in the implementation of the national development strategy aimed at all spheres of public life, ensuring cybersecurity as a preventive tool aimed at increasing vigilance and awareness in the effective electronic communication between public authorities and citizens. serve a high level of legitimacy between the state and society;

The level of stability of national security and sovereignty of Central Asian countries is proportional to the ability of information technology means of regional strategic and socio-economic importance to protect against any internal and external cyber threats, and it is revealed that their institutional and functional legal framework is an important basis for sustainable development of society;

An important component of the comprehensive security system in the Central Asian region is the weakness of threat protection mechanisms, the presence of a flow of malicious information programmes of transboundary and transnational nature, the interaction of stages of interstate cooperation to combat it, as well as the regional and multidimensional constructive orientation of strategic partnerships reveal the dependence on the level of formation of the cyber security system.

Implementation of the research results as a result of studying the socio-political aspects of cyber security in the Central Asian region:

Social, political, ideological, military cyberattack threatening the activities of state bodies, organisations, moral maturity of youth is an important basis for effective protection of subjective (individual, society, state) and objective (international) attitude) factors of the security system from internal and external threats and ensuring its sustainable development, as well as its scientific innovations regarding effective protection against cyberattacks. Item 43 "Promotion of national values, moral qualities and social mores" of the Programme of Action for 2023 of the Centre for Spirituality and Enlightenment of the Republic of Uzbekistan "A platform for interaction on the Internet, promoting nationalism, preserving our mentality, age - old values and noble traditions and was used in the organization and conduct of a scientific project and a national scientific-practical conference on the theme "Creation of mobile applications" (Decision No. 02-22/1008 of 22 September 2023 of the Centre for Spirituality and Enlightenment of the Republic of Uzbekistan and the Centre for Enlightenment of the Republic of Uzbekistan).

As a result, the proposals, recommendations and conclusions put forward in the dissertation have served to conduct joint research on topical issues of ensuring internal security and sustainable development of Uzbekistan, security problems in Central Asia, and prospects for regional and international cooperation;

from the conclusions related to ensuring the stability and reliability of information resources in the implementation of the national development strategy aimed at all spheres of public life, ensuring vigilance and awareness in the effective electronic communication of public authorities with citizens as a preventive tool serving a high level of legitimacy between the state and society, the Republic of Spirituality and the Centre of Enlightenment "National Values, propaganda of spiritual virtues and social mores", para. 43, was used in the organisation and conduct of a scientific project and a national scientific-practical conference on the theme "Creation of a platform and mobile applications for the space of mutual communication on the Internet, promoting nationalism, preservation of our mentality, age-old values and noble traditions" (Act No. 02-22/1008 of the Centre for Spirituality and Enlightenment of the Republic of 22 September 2023). As a result, the content of the material produced for television and radio programmes was sophisticated, rich in scientific data and served to strengthen the knowledge, skills and experience of the population in terms of raising political awareness and culture;

The level of stability of national security and sovereignty of Central Asian countries is proportional to the ability of information technology tools of regional strategic and socio-economic importance to protect against any internal and external cyber threats, and their institutional and functional legal framework is an important basis for the sustainable development of society.The Republican Centre for Spirituality and Enlightenment was established under the VIII direction of the programme of measures for 2023 "National Values, propaganda of spiritual virtues and social mores", para. 43, was used in the organisation and conduct of a scientific project and a national scientific-practical conference on the theme "Creation of a platform and mobile applications for the space of mutual communication on the Internet, promoting nationalism, preservation of our mentality, age-old values and noble traditions" (Act No. 02-22/1008 of the Centre for Spirituality and Enlightenment of the Republic of 22 September 2023). As a result, in collaboration with NGOs, regional non-profit organisations and regional branches of political parties, this served as a basis for the development of roadmaps, programmes and network sector priorities in the areas of human risk and stability. An important component of the complex security system in the Central Asian region is the weakness of threat protection mechanisms and the existence of a flow of malicious information programmes of transboundary and transnational nature. Among the innovations put forward in connection with the interaction of the stages of inter-State cooperation and the regional and multidimensional constructive orientation of the strategic partnership to combat it, depending on the level of formation of the cybersecurity system, the Republican Centre for Spirituality and Education was established under the VIII direction of the programme of measures for 2023 "Propaganda of national values, moral qualities and social mores" paragraph 43 "Propaganda of nationalism on the Internet", It was used in the organisation and conduct of a scientific project and a republican scientific-practical conference on the theme "Creation of a platform and mobile applications of the space of mutual communication for the preservation of our mentality, age-old values and noble traditions" (Republican Centre of Spirituality and Enlightenment dated 22 September 2023 (certificate number 02-22/1008). As a result, this has served to improve the Centre's sociological research and social criteria methodology.

The structure and scope of the dissertation. The dissertation consists of an introduction, three chapters, conclusion, and a list of references. The research part of the paper consists of 130 pages.

E’LON QILINGAN ISHLAR RO‘YXATI
СПИСОК ОПУБЛИКОВАННЫХ РАБОТ
LIST OF PUBLISHED WORKS

I bo‘lim (I часть; Part I)

1. Turdiyev U.R. Globallashuv davrida kiberxavfsizlik muammosining ayrim masalalari // ЎзМУ хабарлари. – Toshkent, 2023. – № 1/5. – Б. 172-175 (23.00.00. № 19).

2. Турдиев У.Р. Глобаллашув даврида киберхавфсизлик муаммоси// “XXI аср: фан ва таълим масалалари” илмий электрон журнали. – Toshkent, 2023. – №3. – Б. 1-8 (23.00.00. №).

3. Turdiyev U.R. Globallashuv va kiberxavfsizlik bog‘liqligining ayrim jihatlari // ЎзМУ хабарлари. – Toshkent, 2023. – № 1/5. – Б. 172 (23.00.00. № 19).

4. Турдиев У.Р. Киберхавфсизлик муаммоси: рақамлар, рейтинглар ва янги ғоялар // Фалсафа ва ҳуқуқ – Ташкент, 2023. – № 2. – Б. 143-145 (23.00.00. № 25).

5. Turdiyev U.R. Political and legal foundations of fighting extremism and terrorism in Uzbekistan // Journal of social sciences and humanities research fundamentals. VOL 3. №4. -P. 22-26.

6. Turdiyev U.R. Kiberxavfsizlikni ta’minlash - Markaziy Osiyo mintaqasining ustuvor vazifasi sifatida // ЎзМУ хабарлари. – Toshkent, 2023. – № 1/9. – Б. 160-161 (23.00.00. № 19).

7. Turdiyev U.R. Global o‘zgarishlar kontestida O‘zbekistonda kiberxavfsizlik sohasidagi davlat boshqaruvining roli va ahamiyati // ЎзМУ хабарлари. – Toshkent, 2023. – № 1/9/1. – Б. 238-240 (23.00.00. № 19).

8. Турдиев У.Р. Киберхавфсизлик тушунчасининг концептуал мазмуни ва таҳлили // “Ўзбекистон халқаро рейтингларда: ижтимоий-иқтисодий ислоҳотларнинг самарадорлиги, муаммолар ва ечимлар” мавзусидаги Халқаро илмий-амалий конференция материаллари // Тошкент, 2021 йил 17 июнь. – Б. 306-309.

II bo‘lim (часть II; part II)

9. Турдиев У.Р. Ўзбекистон Республикаси сиёсий тизимида олиб борилаётган ислоҳотларда ёшларнинг ўрни: муаммолар ва ечимлар // Ta`lim tizimidagi islohotlar: olimlar va yoshlar nigohida mavzusidagi ilmiy-amaliy konferensiyasi materiallari to‘plami. – Toshkent, 2021. – B. 521-526.

10. Бўтаев У, Турдиев У. Маънавий ахлоқий тарбия – коррупцияга қарши курашишнинг муҳим омили// Коррупциясиз тараққиётни таъминлаш: муаммо ва ечимлар мавзусидаги Республика илмий-назарий анжуман материаллари to‘plami. – Бухоро, 2023. – Б. 23-28.

11. Turdiyev U.R. Yoshlar mafkuraviy immunitetini kuchaytirishda ijtimoiy-siyosiy institutlarning roli./ “Yangi O‘zbekiston taraqqiyotida yoshlarning o‘rni” mavzusidagi Respublika ilmiy-amaliy konferensiyasi materiallari to‘plami. – Toshkent, 2023. – B. 9-12.

Avtoreferat «O‘zMU xabarlari» jurnali tahririyatida tahrirdan o‘tkazilib,
o‘zbek, rus va ingliz tillaridagi matnlar o‘zaro muvofiqlashtirildi.

Bosmaxona litsenziyasi:

9338

Bichimi: 84x60 $^{1}/_{16}$. «Times New Roman» garniturasi.
Raqamli bosma usulda bosildi.
Shartli bosma tabog‘i: 3,5. Adadi 100 dona. Buyurtma № 50/23.

Guvohnoma № 851684.
«Tipograff» MCHJ bosmaxonasida chop etilgan.
Bosmaxona manzili: 100011, Toshkent sh., Beruniy ko‘chasi, 83-uy.