TOSHKENT DAVLAT SHARQSHUNOSLIK UNIVERSITETI HUZURIDAGI ILMIY DARAJALAR BERUVCHI DSc.03/29.12.2022.Ss.21.02 RAQAMLI ILMIY KENGASH

ANDIJON DAVLAT UNIVERSITETI

ALIYEV OLIMBEK AYBEKOVICH

DAVLAT AXBOROT XAVFSIZLIGI SIYOSATIDA JAMIYAT BARQARORLIGINI TA'MINLASHNING MILLIY VA XORIJIY JIHATLARI

23.00.02 – Siyosiy institutlar, jarayonlar va texnologiyalar

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

Toshkent – 2024

UO‘K: 323:316.77(043.3)

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

Оглавление автореферата диссертации
доктора философии (PhD) по политическим наукам

Contents of Dissertation Abstract
of the Doctor of Philosophy (PhD) on Political Sciences

TOSHKENT DAVLAT SHARQSHUNOSLIK UNIVERSITETI HUZURIDAGI ILMIY DARAJALAR BERUVCHI DSc.03/29.12.2022.Ss.21.02 RAQAMLI ILMIY KENGASH

ANDIJON DAVLAT UNIVERSITETI

ALIYEV OLIMBEK AYBEKOVICH

DAVLAT AXBOROT XAVFSIZLIGI SIYOSATIDA JAMIYAT BARQARORLIGINI TA'MINLASHNING MILLIY VA XORIJIY JIHATLARI

23.00.02 – Siyosiy institutlar, jarayonlar va texnologiyalar

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

Toshkent – 2024

Siyosiy fanlar bo‘yicha falsafa doktori (PhD) dissertatsiyasi mavzusi O‘zbekiston Respublikasi Vazirlar Mahkamasi huzuridagi Oliy attestatsiya komissiyasida №B2020.4.PhD/Ss237 raqam bilan ro‘yxatga olingan.

Dissertatsiya Andijon davlat universitetida bajarilgan.

Dissertatsiya avtoreferati uch tilda (o‘zbek, rus, ingliz (резюме)) Ilmiy kengash veb-sahifasida (https://uzswlu.uz) hamda «Ziyonet» axborot-ta’lim portalida (www.ziyonet.uz) joylashtirilgan.

Ilmiy rahbar:	**Qirg‘izboyev Muqimjon** siyosiy fanlar doktori, professor
Rasmiy opponentlar:	**Jo‘rayev Sayfiddin Axmatovich** siyosiy fanlar doktori, professor
	Yuldashev Anvar Ergashevich tarix fanlar doktori, professor
Yetakchi tashkilot:	O‘zbekiston davlat jahon tillari universiteti

Dissertatsiya himoyasi Toshkent davlat sharqshunoslik universiteti huzuridagi DSc.03/29.12.2022.Ss.21.02 raqamli Ilmiy kengashning 2024-yil “14” dekabr soat 10^{00} dagi majlisida bo‘lib o‘tadi. (Manzil: 100060, Toshkent sh., Amir Temur ko‘chasi, 20-uy. Tel.: (71) 2333424; e-mail: info@tsuos.uz.)

Dissertatsiya bilan Toshkent davlat sharqshunoslik universiteti Axborot-resurs markazida tanishish mumkin (___ raqam bilan ro‘yxatga olingan). Manzil: 100060, Toshkent sh., Amir Temur ko‘chasi, 20-uy. Tel.: (99871) 233-45-21.

Dissertatsiya avtoreferati 2024-yil “____”_____ kuni tarqatildi.
(2024-yil “____” _____ dagi ____ raqamli reyestr bayonnomasi).

D.B.Sayfullayev
Ilmiy darajalar beruvchi ilmiy kengash raisi, tarix fanlari doktori, professor

D.I.Madaminova
Ilmiy darajalar beruvchi ilmiy kengash ilmiy kotibi, siyosiy fanlar doktori, dotsent

E.S. Sultonova
Ilmiy darajalar beruvchi ilmiy kengash huzuridagi Ilmiy seminar raisi, siyosiy fanlar doktori, professor

KIRISH (falsafa doktori (PhD) dissertatsiyasi annotatsiyasi)

Dissertatsiya mavzusining dolzarbligi va zarurati. Jahonda axborot xavfsizligini ta’minlash muammosi inson, jamiyat va davlat manfaatlarini amalga oshirish hamda uni himoya qilishda hayotiy zarurat sifatida namoyon bo‘lmoqda. Axborot xavfsizligiga tahdidlardan biri – bu axborot-kommunikatsiya texnologiyalaridan o‘zlarining buzg‘unchi maqsadlari yo‘lida foydalanayotganliklari insoniyatga nisbatan qaratilgan siyosiy-ijtimoiy hurujdir. Siyosiy maqsadni ko‘zlab tarqatilayotgan axborotlarni soxtalashtirishga urinishlar mamlakatlarning strategik ahamiyat kasb etuvchi infratuzilmalariga zarar yetkazayotganligi tobora oydinlashib bormoqda. Bu esa axborot-mafkuraviy omillarning obyektiv va subyektiv jihatlarini aniqlashga hamda turli xildagi g‘oyaviy xavf-xatarlarning oldini olishning samarali usullari, vositalari va yo‘llarini ishlab chiqishga doir tadqiqotlarni amalga oshirishni taqozo etmoqda.

Axborot makonida vujudga kelayotgan noodatiy chaqiriqlar davlat va jamiyat barqarorligini ta’minlash masalalariga yangicha yondashuvlar ishlab chiqish zaruratini yuzaga keltirmoqda. Natijada dunyoning ilg‘or ilmiy tadqiqot institutlari va xalqaro tahlil markazlarida axborot xavfsizligini ta’minlashga doir muammolarni tadqiq etishga qiziqish ortib bormoqda. Ayniqsa, axborot xavfsizligining milliy, mintaqaviy va global xavfsizlikka ta’sirini inobatga olgan holda, unga tahdid solayotgan xavflarga qarshi kurashishning samarali vositalari va chora-tadbirlarini ishlab chiqish ilmiy tadqiqotlarning obyekti va nazariy-metodologik asosini tashkil etmoqda.

O‘zbekistonda axborot erkinligi va ochiqligini ta’minlash, shuningdek, axborot xurujlariga qarshi kurashishga qaratilgan davlat siyosati dunyodagi murakkab vaziyat, tinchlik va xavfsizlikni mustahkamlash jarayonlari bilan chambarchas bog‘liq. Shu boisdan O‘zbekistonda davlat axborot xavfsizligi siyosatida jamiyat barqarorligini ta’minlash masalalari bugungi kunda O‘zbekistonda amalga oshirilayotgan “O‘zbekiston – 2030” strategiyasida “internet jahon axborot tarmog‘idan to‘siqlarsiz foydalanish uchun zarur shart-sharoitlarni yaratish, milliy internet makonida kiberxavfsizlikni ta’minlash hamda fuqarolarning internetdan foydalanish borasidagi savodxonligini oshirish”ga[1] doir maqsad sifatida belgilangan.

O‘zbekiston Respublikasi Prezidentining “O‘zbekiston Respublikasini yanada rivojlantirish bo‘yicha Harakatlar strategiyasi to‘g‘risida”gi (2017-yil 7-fevral, PF-4947-son), O‘zbekiston Respublikasi Prezidentining “Axborot texnologiyalari va kommunikatsiyalari sohasini yanada takomillashtirish chora-tadbirlari to‘g‘risida”gi (2018-yil 19-fevral, PF-5349-son), O‘zbekiston Respublikasi Prezidentining “2022–2026-yillarga mo‘ljallangan Yangi O‘zbekistonning taraqqiyot strategiyasi” to‘g‘risidagi (2022-yil 28-yanvar, PF-60-son) Farmonlari, “O‘zbekiston taraqqiyotining yangi bosqichida milliy g‘oyani rivojlantirish

[1] Ўзбекистон Республикаси Президентининг 2023-йил 11- сентябрдаги “Ўзбекистон – 2030” стратегияси тўғрисида”ги ПФ-158-сон Фармони// https://lex.uz/docs/6600413

konsepsiyasini ishlab chiqishga doir chora-tadbirlar to‘g‘risida”gi (2019-yil 8-aprel, F-5465-son) Farmoyishi, “Axborot texnologiyalari va kommunikatsiyalarining joriy etilishini nazorat qilish, ularni himoya qilish tizimini takomillashtirish chora-tadbirlari to‘g‘risida”gi (2018-yil 22-noyabr, PQ-4024), O‘zbekiston Respublikasi Prezidentining “O‘zbekiston Respublikasi Prezidenti Administratsiyasi huzuridagi Axborot va ommaviy kommunikatsiyalar agentligi faoliyatini tashkil etish to‘g‘risida”gi (2019-yil 2-fevral, PQ-4151), O‘zbekiston Respublikasi Prezidentining 2023-yil 31-maydagi “O‘zbekiston Respublikasining muhim axborot tuzilmasi obyektlari kiberxavfsizligini ta’minlash tizimini takomillashtirish bo‘yicha qo‘shimcha chora-tadbirlar to‘g‘risida”gi (2023-yil 31-may, PQ-167) Qarorlaridan kelib chiqadigan vazifalarni amalga oshirishga muayyan darajada xizmat qiladi.

Tadqiqotning respublika fan va texnologiyalari rivojlanishining ustuvor yo‘nalishlariga mosligi. Dissertatsiya respublika fan va texnologiyalari rivojlanishining 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‘nalishiga muvofiq bajarilgan.

Muammoning o‘rganilganlik darajasi. O‘zbekiston Respublikasi Prezidenti Sh.M.Mirziyoyevning O‘zbekistonni barqaror va izchil rivojlantirish, jamiyatda barqarorlikni ta’minlashda axborot xavfsizligini saqlashning siyosiy texnologiyalarini yanada takomillashtirish jarayonlariga oid konseptual va strategik g‘oyalari tadqiqotning ilmiy-metodologik asosini tashkil etadi[2].

Zamonaviy tadqiqotchilarning ilmiy ishlarini uch guruhga bo‘lish mumkin:

Birinchi guruh. O‘zbekistonda davlat axborot xavfsizligi siyosatining jamiyat barqarorligiga ta’siriga doir ilmiy tadqiqot ishlarini olib borgan S.K.Ganiyev, Z.T.Xudoykulov, N.B.Nasrullayev, A.E.Yuldashev, I.Islamov, I.M.Karimov, N.A.Turgunov, Sh.Gulomov, F.B.Botirov, Z.I.Azizova, D.Akbarov, D.S.Muitov, U.R.Kushayev N.B.Nasrullayev, N.Qosimova va N.Umarova kabi olimlar aynan bizning mavzuyimizda bo‘lmasa-da, unga yaqin bo‘lgan axborot xavfsizligining AKT, texnologik va texnikaviy jihatlari, axborotning yoshlar ma’naviyatiga ta’siri hamda axborot iste’moli madaniyati bilan bog‘liq tomonlarini tadqiq etganlar. Siyosiy fanlar nuqtayi nazaridan Sh.Murodova, H.Rajabov va M.Q.Yuldashevalar o‘z tadqiqotlarini olib borganlar.

Ikkinchi guruh. MDH mamlakatlari doirasida G.A.Atamanov, O.M.Manjueva, M.Yu.Zaxarov, Ye.Ye.Perchuk, O.I.Nemkina, Yu.A.Kaptyug, O.M.Sidenova, A.V.Polikarpov, V.F.Nitsevich Yu.V.Vovendo Sh.K.Raximzoda, O.A.Melnikova, A.V.Kurilkin, S.N.Fedorchenko, A.B.Romashkina va boshqalar

[2] Mirziyoyev Sh. Qonun ustuvorligi va inson manfaatlarini ta’minlash-yurt taraqqiyoti va xalq farovonligining garovi. – Toshkent:O‘zbekiston, 2017. – 48 b.; Mirziyoyev Sh. Tanqidiy tahlil, qat’iy tartib-intizom va shaxsiy javobgarlik – har bir rahbar faoliyatining kundalik qoidasi bo‘lishi kerak.-Toshkent: O‘zbekiston, 2017. – 104 b.; Mirziyoyev Sh. Buyuk kelajagimizni mard va olijanob xalqimiz bilan birga quramiz. – Toshkent: O‘zbekiston, 2017. – 488 b.; Mirziyoyev Sh. Milliy taraqqiyot yo‘limizni qat’iyat bilan davom ettirib, yangi bosqichga ko‘taramiz. 1-jild.–Toshkent: O‘zbekiston, 2018. – 592 b.; Mirziyoyev Sh. Yangi O‘zbekiston Strategiyasi. – Toshkent: O‘zbekiston, 2021. – 464 b.

axborot urushi, axborot terrorizmi, axborot quroli, axborot xavfsizligini ta’minlashning huquqiy-psixologik mexanizmlari, virtual olam va inson turmush tarzining o‘zaro aloqadorligi hamda axborot xavfsizligi muammolarining kelib chiqishiga oid ilmiy tadqiqotlar olib borganlar.

Uchinchi guruh. Bu sohaga oid muammolar bilan shug‘ullangan xorijlik olimlardan S.Xantington, F.Fukuyama, D.Bell, A.Toffler, M.Kastels, U.Rostou, P.Druker, Dj.Gelbreyt, V.Inozemsev, F.Uebster, A.A.Chyernov, R.F.Abdeev, I.S.Melyuxin[3] kabilarning ishlarini alohida qayd etish kerak. Bu olimlar axborot va axborot xavfsizligiga oid nazariyalarga asos soldilar. Ularning “postindustrial jamiyat” va “axborotlashgan jamiyat” konsepsiyalarida axborot xavfsizligi muammolari tadqiq qilingan.

Shu bilan birga, ularning tadqiqotlari mavzulari va tadqiqot obyektlari bizning dissertatsiyamiz mavzusidan keskin farqlanadi.

Muammoning o‘rganilganlik darajasini tahlil etish shuni ko‘rsatdiki, hozirgi davrga qadar davlat axborot xavfsizligi siyosatida jamiyat barqarorligini ta’minlash masalalari maxsus dissertatsiya sifatida tadqiq etilmagan. Shu tufayli biz o‘z dissertatsiyamizda davlat axborot xavfsizligi siyosatida jamiyat barqarorligini ta’minlash masalalariga oid mavzuni tanladik.

Dissertatsiya tadqiqotining dissertatsiya bajarilayotgan oliy ta’lim muassasasining ilmiy-tadqiqot rejalari bilan bog‘liqligi. Dissertatsiya ishi Andijon davlat universitetining ilmiy tadqiqot ishlari rejasidan o‘rin olgan hamda “Fuqarolik jamiyati nazariyasi” kafedrasining “Fuqarolik jamiyatini rivojlantirish muammolari” mavzusidagi fundamental loyihasi doirasida bajarilgan.

Tadqiqotning maqsadi jamiyat barqarorligini ta’minlash jarayonida davlatning milliy va axborot xavfsizligi siyosatini amalga oshirish hamda uni takomillashtirish bo‘yicha taklif va tavsiyalar ishlab chiqishdan iborat.

Tadqiqotning vazifalari: axborot xavfsizligiga doir tushunchalar tavsifini shakllantirish;

axborot xavfsizligining metodologik jihatlari – kategorial obzor va xalqaro xavfsizlik tizimi evolyutsiyasi, uni jamiyatning barqarorligi omili ekanligini ochib berish;

AQSh, Yevropa Ittifoqi va Xitoy axborot xavfsizligi takomillashishi hamda tajribasini tahlil etish;

O‘zbekistonda davlat axborot xavfsizligi siyosatining huquqiy asoslarining shakllanishi va rivojlanishini tadqiq etish;

O‘zbekiston axborot xavfsizligiga kibertahdidlar va ularga qarshi kurash jarayonini tahlil etish;

O‘zbekistonda axborot xavfsizligi tizimini yanada rivojlantirish jarayoni va uning istiqbollarini ilmiy jihatdan tavsiflab berish;

[3] Mazkur tadqiqotchilarning asarlari dissertasiya asosiy matni havolalari va “Foydalanilgan adabiyotlar ro‘yhati”da berilgan.

O‘zbekistonda axborot xavfsizligini yanada rivojlantirish va samaradorligini oshirishga oid xulosa, taklif va tavsiyalar ishlab chiqish.

Tadqiqotning obyektini O‘zbekistonda jamiyat barqarorligini ta’minlash tizimini mustahkamlashda davlat axborot siyosati o‘rnining oshishi tashkil etadi.

Tadqiqotning predmetini jamiyat barqarorligini ta’minlashda davlatning axborot xavfsizligi sohasidagi siyosatining o‘ziga xos xususiyatlari, qonuniyatlari va mazkur jarayonda vujudga keladigan ijtimoiy-siyosiy munosabatlar tashkil etadi.

Tadqiqotning usullari. Dissertatsiyada kompleks yondashuv, ilmiy bilishning dialektika, tarixiylik, mantiqiylik, analiz va sintez, qiyosiy tahlil, kuzatuv, so‘rov kabi tadqiqot usullari qo‘llanilgan.

Tadqiqotning ilmiy yangiligi quyidagilardan iborat:

Jahonda axborot xavfsizligini ta’minlashining yagona va universal mexanizmi ishlab chiqilmagani, senzura va axborot oqimlarini cheklashga qaratilgan davlat siyosatining kutilgan darajada samara bermasligi hamda davlat va jamiyat barqarorligini ichki va tashqi axborot xurujlaridan muhofaza etishda mamlakatlar o‘z milliy kontentlarini yaratishga asosiy e’tibor qaratayotgani “axborotga qarshi axborot” tamoyilidan foydalanishga asos bo‘lishi dalillangan.

Axborot asrida an’anaviy jamiyat axborotlashgan jamiyatga aylanib, o‘zaro qo‘shilgan holda konvergensiya hosil qilishi, axborot xavfsizligiga qarshi xavf-xatar va tahdidlardan himoyalanish bilan bog‘liq konfidensiallik, axborot resurslariga kirish, metatexnologiyalar hamda AQSh, Xitoy va Yevropa davlatlarining axborot xavfsizligini mustahkamlashga qaratilgan tajribasiga asoslanib, “Uz” domeni orqali ro‘yhatga oluvchi O‘zbekiston axborot milliy tarmog‘i (UZNET) dasturini ishlab chiqish zarurati asoslab berilgan.

Axborot xavfsizligini ta’minlashning asosiga aylangan kiber va gibrid jinoyatchilikka karshi kurashni kuchaytirish, kibertahdidlarning oldini olishga qaratilgan kiberprofilaktika ishlarini uzluksiz davom ettirish, mafkuraviy, diniy va siyosiy adovatni qo‘zg‘atish mazmunidagi buzg‘unchi g‘oyalarning tarqalishiga yo‘l qo‘ymaslik maqsadlaridan kelib chiqib, mahalla institutlarida “Kiberxavfsizlik” jamoatchilik markazlarini tashkil etish taklifi dalillangan.

O‘zbekiston axborot maydonida qonunchilikka rioya etilishini ta’minlash, axborotdan foydalanish savodxonligi va madaniyatini yuksaltirish hamda aholini yot va destruktiv ma’lumotlar ta’siridan himoya qilish, kiberterrorizm va radikallashuvning oldini olish kabi vazifalarni maqsad qilgan davlat axborot xavfsizligi siyosatidan kelib chiqib, milliy axborot xavfsizligini ta’minlashning samarali mexanizmlarini takomillashtirishga xizmat qiluvchi “O‘zbekiston milliy axborot xavfsizlik strategiyasi”ni qabul qilish zarurligi isbotlangan.

Tadqiqotning amaliy natijalari. Axborot xavfsizligi siyosati tushunchasining paydo bo‘lishi hamda takomillashishiga doir qarashlarning mazmun-mohiyati o‘rganildi, jahonning yetakchi olimlarining ilmiy-nazariy qarashlari tahlil qilindi, O‘zbekistonda axborot xavfsizligi siyosatini tashkil etishning asosiy yo‘nalishlari aniqlashtirildi.

O‘zbekistonda axboriy tahdidlarning intellektuallashuvi sharoitida axborot xavfsizligi siyosati uchun ishlab chiqiladigan chora-tadbirlar mazmunini boyitish, axborot xavfsizligi sohasida milliy manfaatlarimizni himoya qilish maqsadida ishlab chiqilgan milliy kontentdan iborat.

Tadqiqot natijalarining ishonchliligi. Tadqiqot natijalarining ishonchliligi xalqaro hamda respublika miqyosidagi ilmiy-amaliy konferensiyalar materiallari to‘plamlari, OAK ro‘yxatiga kirgan maxsus va xorijiy mamlakatlar jurnallarida chop etilgan maqolalar, xulosa, amaliy taklif va tavsiyalarning amaliyotda joriy etilganligi, olingan natijalarning vakolatli tashkilotlar tomonidan tasdiqlanganligi bilan izohlanadi.

Tadqiqot natijalarining ilmiy va amaliy ahamiyati. Tadqiqot natijalarining *ilmiy ahamiyati* axborot xavfsizligi siyosatiga doir ilmiy ta’limotlarning takomillashuvi, siyosiy institutlar, siyosiy jarayonlar va siyosiy texnologiyalarda axborot xavfsizligini ta’minlash kontekstida amalga oshiriladigan tadqiqotlar, yaratiladigan darslik, uslubiy qo‘llanmalar uchun nazariy manba sifatida foydali bo‘lishi mumkinligi bilan izohlanadi.

Shuningdek, tadqiqot natijalari amaliy siyosatshunoslik, amaliy jurnalistika, internet jurnalistikasi, media nazariyasi, OAV nazariyasi, axborot xavfsizligi fanlarini ilmiy-uslubiy jihatdan boyitadi.

Dissertatsiyaning *amaliy ahamiyati* shundaki, oliy ta’lim muassasalarida “Mudofaa va xavfsizlik” hamda “Ochiq tizimlarda axborot-psixologik xavfsizlik” predmetidan ta’lim beruvchi professor-o‘qituvchilarning malaka oshirish amaliyotida, ularning siyosiy kompetensiyasini rivojlantirish uchun o‘quv-treninglarni o‘tkazishda, siyosiy kommunikatsiya modellarini takomillashtirishda foydalanish nazarda tutilgan. Shuningdek, dissertatsiya materiallari OTM ijtimoiy-gumanitar sohada ta’lim olayotgan talabalar uchun o‘qitilayotgan “Axborot xavfsizligi” fani bo‘yicha o‘quv materiallari sifatida xizmat qiladi.

Tadqiqot natijalarining joriy qilinishi. Davlat axborot xavfsizligi siyosatida jamiyat barqarorligini ta’minlash masalalari bo‘yicha olib borilgan tadqiqot natijasida ishlab chiqilgan ilmiy xulosa, tavsiya va takliflar asosida quyidagilarga erishildi:

Jahonda axborot xavfsizligini ta’minlashning yagona va universal mexanizmi ishlab chiqilmagani, senzura va axborot oqimlarini cheklashga qaratilgan davlat siyosatining kutilgan darajada samara bermasligi hamda davlat va jamiyat barqarorligini ichki va tashqi axborot xurujlaridan muhofaza etishda mamlakatlar o‘z milliy kontentlarini yaratishga asosiy e’tibor qaratayotgani “axborotga qarshi axborot” tamoyilidan foydalanishga asos bo‘lishi haqidagi xulosalardan O‘zbekiston Respublikasining 2022-yil 15-apreldagi O‘RQ 764-sonli “Kiberxavfsizlik to‘g‘risida”gi Qonunining “Kiberxavfsizlikni ta’minlashning asosiy prinsiplari” deb nomlangan 4-moddasini ishlab chiqishda foydalanilgan (*O‘zbekiston Respublikasi Oliy Majlis Senatining Mudofaa va xavfsizlik masalalari qo‘mitasining 2023-yil 1-maydagi 13-son ma’lumotnomasi*). Natijada,

kibermakonda shaxs, jamiyat va davlat manfaatlarini himoya qilishning ustuvorligini ta’minlashning huquqiy asoslari yaratilgan.

Axborot asrida an’anaviy jamiyat axborotlashgan jamiyatga aylanib, o‘zaro qo‘shilgan holda konvergensiya hosil qilishi, axborot xavfsizligiga qarshi xavf-xatar va tahdidlardan himoyalanish bilan bog‘liq konfidensiallik, axborot resurslariga kirish, metatexnologiyalar hamda AQSh, Xitoy va Yevropa davlatlarining axborot xavfsizligini mustahkamlashga qaratilgan tajribasiga asoslanib, “Uz” domeni orqali ro‘yhatga oluvchi O‘zbekiston axborot milliy tarmog‘i (UZNET) dasturini ishlab chiqish zarurati haqidagi xulosalardan O‘zbekiston Respublikasining 2022-yil 15-apreldagi O‘RQ 764-sonli “Kiberxavfsizlik to‘g‘risida”gi Qonunining “Kiberxavfsizlikni ta’minlashning asosiy prinsiplari” deb nomlangan 4-moddasini ishlab chiqishda foydalanilgan (*O‘zbekiston Respublikasi Oliy Majlis Senatining Mudofaa va xavfsizlik masalalari qo‘mitasining 2023-yil 12-apreldagi 12-son dalolatnomasi*). Natijada, O‘zbekistonda modernizatsiya va islohotlar amalga oshirilayotgan davrda xavfsizlik tizimining shakllanishi, dinamikasi va istiqbollari bilan bog‘liq bo‘lgan muammolarni to‘g‘ri hal etishga hamda mazkur tizim taraqqiyotiga xizmat qilgan.

Axborot xavfsizligini ta’minlashning asosiga aylangan kiber va gibrid jinoyatchilikka qarshi kurashni kuchaytirish, kibertahdidlarning oldini olishga qaratilgan kiberprofilaktika ishlarini uzluksiz davom ettirish, mafkuraviy, diniy va siyosiy adovatni qo‘zg‘atish mazmunidagi buzg‘unchi g‘oyalarning tarqalishiga yo‘l qo‘ymaslik maqsadlaridan kelib chiqib, mahalla institutlarida “Kiberxavfsizlik” jamoatchilik markazlarini tashkil etish borasidagi takliflardan O‘zbekiston Respublikasi Prezidentining 2019-yil 3-maydagi “Ma’naviy-ma’rifiy ishlar samaradorligini oshirish bo‘yicha qo‘shimcha chora-tadbirlar to‘g‘risida”gi PQ-4307-sonli qaroriga muvofiq ishlab chiqilgan “O‘zbekiston Respublikasida ma’naviy-ma’rifiy ishlar samaradorligini yanada oshirish, aholining intellektual salohiyati va dunyoqarashini yuksaltirishga, mafkuraviy immunitetini mustahkamlashga doir chora-tadbirlar” dasturining “Dunyoda yuz berayotgan murakkab geosiyosiy va g‘oyaviy-mafkuraviy jarayonlarning mazmun-mohiyatini har tomonlama chuqur yoritish, terrorizm, diniy ekstremizm, aqidaparastlik, separatizm, odam savdosi, “ommaviy madaniyat” va boshqa tahdidlarga qarshi samarali g‘oyaviy kurash olib borishga oid tadbirlar” nomli III bandida belgilangan “Axborot hashari” loyihasini amalga oshirish, uning doirasida “internet saytlari va ijtimoiy tarmoqlardagi noxolis axborotlarga qarshi aholi, ayniqsa, yoshlarning mafkuraviy immunitetini mustahkamlash va jamoatchilikda muayyan holatlar haqida haqqoniy fikr shakllanishiga ko‘maklashish”ga bag‘ishlangan vazifalar ijrosini ta’minlashda foydalanilgan *(O‘zbekiston Respublikasi Ma’naviyat va ma’rifat markazi huzuridagi Ijtimoiy-ma’naviy tadqiqotlar markazining 2023-yil 19-iyundagi 228-son dalolatnomasi).* Natijada Yangi O‘zbekiston taraqqiyot strategiyasi asosida olib borilayotgan axborot xavfsizligi siyosatining mazmun-mohiyati haqida yoshlarning chuqur bilimlarga ega bo‘lishlarini ta’minlashga doir zamonaviy targ‘ibot texnologiyalarini ishlab chiqishga xizmat qilgan.

O‘zbekiston axborot maydonida qonunchilikka rioya etilishini ta’minlash, axborotdan foydalanish savodxonligi va madaniyatini yuksaltirish hamda aholini yot va destruktiv ma’lumotlar ta’siridan himoya qilish, kiberterrorizm va radikallashuvning oldini olish kabi vazifalarni maqsad qilgan davlat axborot xavfsizligi siyosatidan kelib chiqib, milliy axborot xavfsizligini ta’minlashning samarali mexanizmlarini takomillashtirishga xizmat qiluvchi “O‘zbekiston milliy axborot xavfsizlik strategiyasi”ni qabul qilish zarurligi bilan bog‘liq xulosalardan “Yangi O‘zbekistonning 2022–2026-yillarga mo‘ljallangan taraqqiyot strategiyasida 2022-yil oktyabrga qadar “2023–2026-yillarga mo‘ljallangan O‘zbekiston Respublikasining kiberxavfsizlik strategiyasi”ni ishlab chiqish vazifasi qo‘yilgan farmon va qarorlarida belgilangan “UZ№ domen zonasi Internet-makonining kiberxavfsizligini ta’minlashning asosiy yo‘nalishlari hamda elektron hukumat, energetika, raqamli iqtisodiyot tizimlari va muhim axborot infratuzilmasiga taalluqli boshqa yo‘nalishlarni himoya qilish bo‘yicha kompleks vazifalar ijrosini ta’minlashga qaratilgan chora-tadbirlar dasturini ishlab chiqishda foydalanilgan *(Yoshlar ishlari agentligi Andijon bo‘limining 2022-yil 18-noyabrdagi dalolatnomasi).* Natijada yoshlar agentligi tizimida faoliyat olib borayotgan xodimlar va yoshlarning axborot xavfsizligi, kiberjinoyatchilik, kiberterrorizm borasidagi siyosiy bilimlari, manaviy-ma’rifiy, huquqiy, siyosiy madaniyatini oshirishga va yoshlar ishlari faoliyatining samaradorligining kuchaytirilishga xizmat qilgan.

Tadqiqot natijalarining aprobatsiyasi. Mazkur tadqiqot natijalari 3 ta xalqaro va 8 ta respublika ilmiy-amaliy konferensiyalarida ma’ruza ko‘rinishida bayon etilgan hamda aprobatsiyadan o‘tgan.

Tadqiqot natijalarining e’lon qilinganligi. Dissertatsiya mavzusi bo‘yicha jami 18 ta ilmiy ish, jumladan, O‘zbekiston Respublikasi Oliy attestatsiya komissiyasi tomonidan doktorlik dissertatsiyalari asosiy ilmiy natijalarini chop etish tavsiya etilgan ilmiy nashrlarda 7 ta maqola, jumladan, 3 ta respublika, 4 ta xorijiy jurnallarda chop etilgan.

Dissertatsiyaning tuzilishi va hajmi. Dissertatsiya kirish, uch bob, to‘qqiz paragraf, xulosa va foydalanilgan adabiyotlar ro‘yxatidan iborat. Dissertatsiyaning hajmi 166 betni tashkil etadi.

DISSERTATSIYANING ASOSIY MAZMUNI

Kirish qismida mavzuning dolzarbligi va zarurati, muammoning o‘rganilganlik darajasi, ilmiy yangiligi, tadqiqotning respublika fan va texnologiyalari rivojlanishining asosiy ustuvor yo‘nalishlariga bog‘liqligi, obyekti, predmeti, metodlari, maqsadi va vazifalari aniqlangan, olingan natijalarning ilmiy va amaliy ahamiyati, amaliyotga joriy qilingani, aprobatsiyasi, nashr etilgan ishlar, dissertatsiyaning tuzilishi bo‘yicha ma’lumotlar keltirilgan.

Dissertatsiyaning “**Jamiyat barqarorligini ta’minlashda axborot xavfsizligi siyosatini tadqiq etishning metodologik jihatlari**” deb nomlangan

birinchi bobida axborot xavfsizligiga doir tushunchalar tavsifi, xalqaro axborot xavfsizligi tizimining shakllanishi va rivojlanishi hamda axborot xavfsizligi – jamiyat barqarorligini ta’minlash omili ekanligi tadqiq etilgan.

Jahon miqyosidagi axborot xavfsizligi muammolari o‘zini tahlikali va tajovuzkorona tarzda namoyon qila boshlaganidan keyin unga doir tushunchalar shakllandi. BMTning xalqaro axborot xavfsizligiga oid qo‘llagan tushunchasi – bu “tahdidlar triadasi” deb ataladigan – terrorchilik, jinoiy va harbiy-siyosiy (harbiy-siyosiy tahdid deganda axborot urushlari va axborotlar o‘zaro kurashi tushuniladi) kabilardan global axborot tizimlarining himoyalanganligini anglatadi.

AQSh va Yevropa Ittifoqi (YI) kiberxavfsizlikka nisbatan eng asosiy tahdidlar sifatida kiberterrorizm va kiberjinoyatchilikni ko‘rsatib, kiberkenglikdagi davlatlararo o‘zaro kurashlarni xalqaro gumanitar huquq doirasida muvofiqlashtirishni tavsiya qiladi[4]. BMT tomonidan 2011-yil 22-sentyabrda qabul qilingan “Xalqaro axborot xavfsizligini ta’minlash” konvensiyasining 2-moddasida “axborot xavfsizligi”ni “shaxs, jamiyat va davlat manfaatlarini axborot kengligida destruktiv tahdidlar va boshqa noxush ta’sirlardan himoyalanganlik holati” deb ta’riflanadi[5].

Xalqaro miqyosda tadqiqot olib borayotgan olimlardan R.Xandli va R.Anderson o‘z tadqiqotlarida AQSh axborot infratuzilmalariga tahdidlarga bog‘liq holda axborot xavfsizligi muammolarining yechimlarini topish jarayonlarida kompyuter, shuningdek, ijtimoiy tarmoqlardagi axborotlarni himoya qilishning texnologik jihatlarini axborot xavfsizligi sifatida ilgari surdi[6].

Axborot xavfsizligini quyidagicha ta’riflash mumkin: bu sotsium holati bo‘lib, bunda davlat, jamiyat va shaxsga nisbatan axborot makonidagi tartibli va stixiyali ravishda vujudga keladigan axborot oqimlari orqali bo‘ladigan tahdidlardir. Axborot xavfsizligi deganda – shaxs, jamiyat va davlatning muhim hayotiy manfaatlarining axborot urushi, intervensiya hamda dezinformatsiya tazyiqlaridan himoyalanganligi tushuniladi. Umuman olganda, olimlar axboriy-siyosiy xavfsizlik deganda fuqarolar, davlat va jamiyatning muhim hayotiy manfaatlarini siyosiy sohada ichki va tashqi axborot tahdidlaridan himoya qilish bilan bog‘liq kompleks muammolar tushuniladi.

Jahon axborot maydoni doirasida 1973-yilda qabul qilingan Xalqaro telekommunikatsiya konvensiyasi dastlabki axborot xavfsizligiga oid rasmiy hujjat edi. Bu Konvensiya axborot qurollarini qo‘llash oqibatlari va bu jarayonning o‘ziga xos xususiyatlariga ega bo‘lgan axborot maydonlarining shakllanishiga bog‘liq holda qabul qilingan.

1998-yil 4-dekabrda BMT tomonidan qabul qilingan “Xalqaro xavfsizlikda axborotlashish va telekommunikatsiya sohalarida yutuqlar” nomli hujjat subyekti

---

[4] Зиновьева Е.С. Международная информационная безопасность. 20.06.2014 г. [Elektron manba]: https://mgimo.ru/ about/ news/ experts/ 256505/.

[5] Конвенция об обеспечении международной информационной безопасности (концепция) ООН. 22 сентября 2011 г. [Elektron manba]: https://www.mid.ru/ mezdunarodnaya informacionnaya bezopasnost/-/asset publisher/UsCUTiw2pO53/ content/ id/ 191666.

[6] Hundley, R.; Anderson, R. Security in Cyberspace: An Emerging Challenge for Society, 1994.

axborot, axborot texnologiyasi va ulardan foydalanish usullari bo‘lgan butunlay yangi xalqaro huquqiy rejimni tashkil etishning rasmiy jihatdan boshlanishi bo‘ldi[7]. BMT Bosh Assambleyasida 2000-yil bu hujjat mavzusi muhokama qilinib, unda “axborot quroli”, “axborot urushi” va “axborot xavfsizligi” kabi tayanch (bazaviy) tushunchalarni aniqlashtirish va shakllantirish tavsiya etildi[8].

2011-yil 22-sentyabrda BMT Bosh Assambleyasi “Xalqaro axborot xavfsizligini ta’minlash to‘g‘risidagi konvensiya”ni qabul qildi. Uning asosiy maqsadi qilib, “xalqaro tinchlik va barqarorlikni buzish uchun foydalanilayotgan AKTga qarshilik qilish, shuningdek, davlatlar axborot maydonidagi faoliyatlariga ko‘maklashishga oid chora-tadbirlarni amalga oshirish belgilandi[9]. 2016-yilda Rossiya Federatsiyasining taklifi bilan 84 ta davlat hammuallifligida “Xalqaro xavfsizlik kontekstidagi axborotlashish va telekommunikatsiyalar sohasidagi yutuqlar” yangi rezolyutsiya loyihasi qabul qilindi.

2018-yil 22-oktyabrda BMT Bosh Assambleyasining 73-sessiyasida BMTning “Xalqaro xavfsizlik kontekstidagi axborotlashish va telekommunikatsiyalar sohasidagi yutuqlar” nomli navbatdagi rezolyutsiyasi qabul qilindi[10]. 2021-yil 12-martda BMT Ochiq tarkibdagi ishchi guruhining “Xalqaro xavfsizlik kontekstidagi axborotlashish va telekommunikatsiyalar sohasidagi yutuqlar” nomli ma’ruzasi qabul qilindi. Ma’ruzani barcha ishtirokchi davlatlar o‘zaro kelishuv asosida qabul qildi.

Xalqaro axborot maydonida keyingi besh yillikda kiberjinoyatchilikning yangidan yangi takomillashgan turlari paydo bo‘la boshladi.

Kiberjinoyatlarning ko‘payishi davlatlarni BMT atrofida hamkorlikda o‘zaro xalqaro axborot xavfsizligini takomillashtirish va rivojlantirishga undadi. Albatta, bu og‘ir va mashaqqatli jarayonlarda rivojlangan mamlakatlar faol ishtirok etdi, ular bu sohada o‘zlarining resurslari va mablag‘larini ayamadi.

So‘nggi o‘n yillikda jahonda xalqaro xavfsizlik tizimi shakllanib, u o‘z ichiga jahondagi aksariyat davlatlarni qamrab oldi. Hozirgi davrga kelib milliy davlatlar terrorizm, ekstremizm, kiberterrorizm, kiberjinoyatchilik, kiberhujumlarga qarshi xalqaro tashkilotlar bilan hamkorlikda kurash tajribasi va usullarini egalladi.

Yapon olimlari bo‘lmish professor Yu.Xayashi va I.Masuda tomonidan kashf etilgan axborot jamiyati konsepsiyasi avvalo iqtisodiy rivojlanish vazifalarini bajarish uchun ishlab chiqilgan edi. Shuning uchun ham u ancha cheklangan, ko‘proq amaliyotga qaratilgan tavsiflarga ega bo‘ldi. Lekin XX asrning 60-yillarida postindustrial jamiyat g‘oyasini amerikalik olim Daniel Bell ishlab

---

[7] Крутских А.В. Информационный вызов безопасности на рубеже XXI века // Международная жизнь. 1999, №2. –С.48.

[8] Информационные вызовы национальной и международной безопасности / Под ред. А.В. Федорова, В.Н. Цыгичко. –М.: ПИР-Центр, 2001. –С.193.

[9] Конвенция об обеспечении международной информационной безопасности. [Elektron manba]: https://pircenter.org/wp-content/uploads/2022/10/Конвенция-об-обеспечении-международной-информационной-безопасности-концепция-РФ.pdf.

[10] Резолюция ООН от 5 декабря 2018 г. A/RES/73/27 «Достижения в сфере информатизации и телекоммуникаций в контексте международной безопасности». [Elektron manba]: https://www.un.org/ga/search/view_ doc.asp? symbol=A/RES/73/27 (Дата обращения: 16.11.2019).

chiqqan bo‘lsa[11], 70-yillarga kelib yangi paydo bo‘lgan ikkita – axborot jamiyati va postindustrial jamiyatni uyg‘unlashtirish, bir-biriga qo‘shish konvergensiyalash jarayonlari boshlandi[12].

YuNESKOning ma’ruzasiga ko‘ra, “axborot jamiyati” tushunchasi texnologiyalar yutuqlariga asoslandi[13]. Albatta, axborot jamiyati va axborot inqilobi noxush siyosiy oqibatlarni keltirib chiqardi: “axborot inqilobi nafaqat sivilizatsiyalar jarayonlarini tezlashtirmoqda, balki yangidan yangi milliy, mintaqaviy va global tahdidlarni ko‘paytirmoqda”[14]. XXI asr boshlariga kelib axborot xavfsizligiga tahdidlardan himoyalanish quyidagilarda ifodalandi:

- axborot resurslariga kirishga (kirishlarning bloklanishi);
- konfidensiallik (axborotga huquqsiz va ruxsatsiz kirish);
- yaxlitlikni buzish (axborotlarni buzib ko‘rsatish);

Shuningdek, axborot xavfsizligiga tahdidning yana quyidagi turlari vujudga keldi:

- “metatexnologiya”larning (ya’ni, turli gadjetlar ishlab chiqaruvchilar tomonidan iste’molchilar haqida axborotlar yig‘ish, ular ustidan nazorat olib borish) paydo bo‘lishi va tarqalishi;
- “elektron-raqamli uzilishlar”, ya’ni AKTga nisbatan davlat ichida va xalqaro darajada chegaralanmagan holda kirish huquqiga ega bo‘lgan, elitaning paydo bo‘lishi. Buning natijasida alohida olingan odamlar, ijtimoiy guruhlar va davlat fikrlari hamda qarashlarini manipulyatsiya qilish imkoniyatlari yildan yilga oshib bormoqda;
- kompyuter militarizatsiyasi, axborot terrorizmi va jinoyatchiligi, ya’ni AKTning ulkan salohiyatidan harbiy-siyosiy ustunlikka erishish, kuchga asoslangan qarama-qarshilik va shantaj, inqirozlar, konfliktlar, harbiy harakatlar taktikalari va strategiyalari haqidagi tasavvurlarni o‘zgartirish, harbiy texnologiyalarni bir-biriga yaqinlashtirish hamda qo‘shish vositasida qurollanish poygasining yangi yo‘nalishlarini tashkil etish.

Axborot tahdidlarining asosiy maqsadlari – bu axborot resurslari – axborot infratuzilmalari, shuningdek, axborotlar va axborot oqimlari[15] (masalan, hujjatlar to‘plamlari, ma’lumotlar banki va bazasi, arxivlar, kutubxonalar, muzeylar fondlari boshqa axborot saqlovchi qurilmalar) kabilarga qarshi qaratiladi.

Bu tahdidlar, bir tomondan, ba’zi davlatlar va siyosiy kuchlarning siyosiy manfaatlari asosida, ikkinchi tomondan, mamlakatimiz xalqaro hamjamiyatning mustaqil, demokratik subyekti sifatida o‘z eshiklarini dunyo uchun keng ochishi

---

[11] Bell D. The Coming of Post-industrial Society. A Venture in Social Forcasting. -N.Y., Basic Books, Inc., 1973.

[12] Классические зарубежные концепции информационного общества. [Elektron manba]: https://studref.com/416484/politologiya/ klassicheskie_zarubezhnye_kontseptsii_informatsionnogo_obschestva.

[13] К обществам знания. Всемирный доклад ЮНЕСКО. – Париж: Издательство ЮНЕСКО, 2005. –С. 19.

[14] O`sha joyda.

[15] Соглашение между правительствами государств-членов Шанхайской организации сотрудничества осотрудничестве в области обеспечения международной информационной безопасности. [Elektron manba]: http://docs.Pravo . ru/document/view/20364925/19329178/.

davrimizning o‘ziga xos ko‘rinishlaridan bo‘lgan globallashuv jarayonining ayrim salbiy ta’sirlari ostida kuchayib bormoqda.

Dissertatsiyaning “**Rivojlangan davlatlarda axborot xavfsizligi siyosatining takomillashish jarayoni**” deb nomlangan ikkinchi bobida AQSh davlat axborot xavfsizligi siyosatining takomillashish jarayoni, Yevropa Ittifoqida axborot xavfsizligi siyosati va uni amalga oshirish shakli hamda Xitoyda axborot xavfsizligi sohasida davlat siyosati evolyutsiyasi va rivojlanishi tadqiq etilgan.

XX asrning ikkinchi yarmidan boshlab AQShda axborot xavfsizligi sohasida tub burilish davri boshlandi. 1958-yilda AQSh Mudofaa vazirligining direktivasi bilan Istiqbolli tadqiqotlar va ishlanmalar Agentligi (ARPA) tashkil etildi. U 1972-yilda qaytadan tashkil etilib, Istiqbolli mudofaa tadqiqotlari va ishlanmalari Agentligi (DARPA) deb nomlandi[16].

1980-yillardan boshlab kompyuter tarmoqlari va tizimlaridagi axborotlar xavfsizligiga nisbatan yondashuvlar jiddiy ravishda o‘zgara boshladi. 1984-yilda “Telekommunikatsiyalar va avtomatlashtirilgan axborot tizimlari milliy siyosati” me’yoriy hujjati qabul qilindi. AQShda kiberterrorizm, kiberjinoyatchilik va davlatlarning AKTdan dushmanlik maqsadlarida foydalanayotganligi kabilar eng katta muammo sifatida e’lon qilindi. Bu sohaga qarshi kurash siyosati 1987-yilda qabul qilingan “Kompyuter xavfsizligi to‘g‘risida”gi qonunda rasmiylashdi. AQSh prezidentining 2001-yil 16-oktyabrdagi (PATRIOT ACT) buyrug‘i hamda 2003-yilda “Kibermaydonni himoya qilishning milliy strategiyasi” to‘g‘risidagi buyrug‘i e’lon qilindi[17].

AQShda kiberxavfsizlik tizimini rivojlantirishning navbatdagi bosqichi 2008-yilda boshlanib, bu davrdan boshlab “Kiberxavfsizlikning umummilliy tashabbusi” hujjati hayotga joriy etila boshlandi. 2009-yilga kelib AQSh prezidenti Barak Obama kibermaydon xavfsizligini ta’minlashni eng muhim davlat vazifasi sifatida e’lon qildi. Shu yili “Kibermaydondagi siyosat obzori” rasmiy hujjati ishlab chiqildi[18]. J.Bush prezidentlik davriga kelib “Kiberxavfsizlikning umummilliy tashabbusi” nomli hujjat qabul qilindi. Prezident B.Obama 2009-yil may oyida “Kibersiyosat obzori”ni (Cyberspace Policy Reviev) e’lon qilib, unda kiberxavfsizlik sohasidagi beshta ustuvor yo‘nalishlarni ko‘rsatib berdi. Ularning ichida eng muhimlari sifatida J.Bush boshlab bergan Amerika axborot-kommunikatsiya tarmoqlarida xavfsizlikni ta’minlashning yangi umumilliy strategiyasini ishlab chiqish ilgari surildi. 2012-yilga kelib AQShda “Axborotlar himoyasi va almashinuvi milliy strategiyasi” qabul qilindi. Mazkur hujjat

---

[16] Department of Defence Directive 5105.15: Department of Defence Advanced Research Projects Agency [issued on 07.02.1958] // ARPA. [Official website] Систем. Требования: Adobe Acrobat Reader. [Elektron manba]: http://www.darpa.mil/Docs/DARP_Original_Directive_1958_200807180942212.pdf. (Дата обращения: 01.05.2014).

[17] National Security Strategy 2010. // National Security Strategy Archive. [Web-source] Систем.требования: AdobecrobatReader. [Elektron manba]: http://nssarchive.us/NSSR/2002.pdf (Дата обращения: 01.12.2014).

[18] Cyberspace Policy Review: Assuring a Trusted and Resilient Information and Communications Infrastructure [issued on 29.05.2009] // The White House. [Official website]. [Elektron manba]: http://www.Whitehouse. gov/assets/documents/ yberspace_Policy_Review_ final.pdf (Дата обращения: 01.05.2014).

AQShning axborot xavfsizligiga doir siyosatining uchta asosiy prinsipini belgilab berdi: axborot milliy boylik sifatida; umumiy xavf-xatarlar taqsimlanishni zarurat qilib qo‘yganligi tufayli axborotlar almashinuvi va himoyalanishi; axborotlar oqimi kuchayishi sababli eng yaxshi qarorlarni qabul qilish.

2015-yil 24-aprelda AQSh Mudofaa vazirligi mamlakat kiberxavfsizligining yangilangan strategiyasini qabul qildi. Unga binoan har qanday kiberhujumlarga qarshi zarbalar berish, AQShni har qanday dushman yoki jinoyatchidan iloji boricha mukammal darajada himoya qilish vazifasi qo‘yildi.

2018-yil 19-yanvarda AQSh Mudofaa vazirligi “Milliy Mudofaa strategiyasi”ning yangilangan variantini e’lon qildi. Shu yilning kuzida Prezident D.Tramp “Kiberxavfsizlik milliy strategiyasi” hujjatini imzoladi. 2021-yilda Jo Bayden Prezident etib saylanganidan keyin kiberxavfsizlik sohasiga e’tibor yanada kuchaydi. U 2021-yil may oyida “Kiberxavfsizlik va federal hukumat tarmoqlarini himoyalashni kuchaytirish to‘g‘risida”gi farmonni imzoladi. Mazkur farmonga muvofiq ravishda mamlakatdagi hokimiyat organlari uchun kiberxavfsizlik sohasidagi hujumlarga qarshi kurashishga oid maxsus standartlashgan yo‘riqnoma ishlab chiqildi, unda qator tavsiyalar joy oldi. Shuningdek, unda xususiy sektorga axborot xavfsizligini ta’minlashga oid qator tavsiyalar berildi[19].

AQSh axborot xavfsizligi sohasiga jahondagi mamlakatlar ichida eng ko‘p sarmoyalar sarfladi. Bu holat uning siyosiy va harbiy qudratini yanada oshirib, dunyo siyosatini belgilaydigan davlat sifatida yashash imkoniyatlarini yanada oshirdi.

XX asrning 90-yillarida ham milliy, ham YI darajalarida telekommunikatsiya va axborotlarni himoyalashga oid qator huquqiy aktlar qabul qilindi. Ularning ichida eng muhimlari – bu Yevropa Komissiyasi tomonidan 2001-yilda e’lon qilingan “Tarmoq va axborot xavfsizligi: Yevropa siyosatiga yondashuvlar uchun takliflar” Xabarnomasi bo‘lib, u YI hayotida muhim o‘zgarishlarni boshlab berdi. Shu bilan birga, 2002-yil 28-yanvarda YI kengashi “Tarmoqlar va axborot xavfsizligi sohasida umumiy yondashuvlar va maxsus choralar”, 2003-yil 18-fevralda “Tarmoqlar va axborot xavfsizligi madaniyatiga nisbatan Yevropa yondashuvi” to‘g‘risidagi qarorlarini qabul qildi.

2004-yil 10-martda tarmoqlar va axborot xavfsizligiga tahdidlarga qarshi kurashish choralarini kuchaytirish maqsadida “Tarmoqlar va axborot xavfsizligi Yevropa agentligi” (European Netvork and Information Security Agency — ENISA) tashkil etildi. Uning asosiy vazifasi “YI hamjamiyati ichida tarmoqlar va axborot xavfsizligini yuqori va samarali darajada ta’minlash va fuqarolar, foydalanuvchilar, ishlab chiqaruvchilar hamda davlat sektori foydasiga tarmoqlar va axborot xavfsizligi madaniyatini rivojlantirish” kabilardan iborat edi.

2010-yillardan boshlab YIda kiberjinoyatlar yanada kuchaydi, axborot tizimlariga yangi turdagi hujumlar yoki fishing (talafot ko‘radigan odam bank hisob raqamiga kirishni ta’minlash maqsadida parollarni so‘rash uchun bank

[19] Байден подписал указ о повышении уровня кибербезопасности в стране. 13 мая 2021 г. [Elektron manba]: https://www.interfax.ru/world/765723.

saytlarini qalbakilashtirish) kabilar paydo bo‘ldi. Bundan tashqari, tovlamachilik va nolegal kontentni tarqatish (bolalarni jinsiy zo‘ravonlikka majburlash yoki Internetda kuch ishlatishni targ‘ib qilishga oid materiallar), kompyuterdan jinoyatni sodir etishda foydalanish kabi an’anaviy bo‘lib qolgan jinoyatlar ham kuchaydi[20].

Stokgolm dasturida (The Stockholm Programme) YIning 2010–2014-yillardagi asosiy e’tibori axborot xavfsizligini ta’minlash va kiberjinoyatchilikka qarshi kurash masalalariga qaratilishi belgilab qo‘yildi.

2020-yil 24-iyulda Yevropa Komissiyasi yangi Ittifoq xavfsizligi strategiyasini qabul qildi. Unda asosan muhim axborot xavfsizligi infratuzilmalarini kiberjinoyatlardan himoya qilishga alohida urg‘u berilib, gibrid tahdidlar va uyushgan jinoyatchilikka qarshi kurashni kuchaytirish vazifalari belgilandi. Ittifoq xavfsizligi strategiyasi so‘nggi 20 yillik strategiyalarni yangiladi.

YIning raqamli rivojlanishining muhim yo‘nalishini muvofiqlashtiruvchi asosiy hujjat bo‘lgan Yevropa raqamli strategiyasi (Shaping Europe’s digital future) 2020-yilning fevral oyida qabul qilindi. Bu strategiyada 2024-yilgacha Yevropa Komissiyasining raqamlashtirish sohasidagi ustuvor yo‘nalishlarini belgilab beradi[21].

Xulosa qilib aytganda, YIning axborot va kiberxavfsizligi AQSh va Xitoy bilan raqobat kurashlarida rivojlanib bormoqda, bu sohada jahonda lider bo‘lish uchun kurashmoqda.

Xitoyning innovatsion rivojlanish davlat strategik dasturida kibermakonni kengaytirish va uning xavfsizligini mustahkamlashga oid muhim vazifalar mujassamlashgan. Xitoy uchun axborot xavfsizligi avvalambor bu innovatsiyalar, shu tufayli ham bu yondashuv kiberxavfsizlikni ta’minlashning o‘ziga xos xususiyati hisoblanadi. Xitoyda Internet dastlab 1987-yil 20-sentyabrda Pekin fizika va yuqori energiyalar instituti professori Syan Tyanbayning CANET (Chinese Academic Netvork) dasturi doirasida Xitoydan birinchi elektron xatni jo‘natishi munosabati bilan o‘z davrini boshladi.

1990-yil oktyabrda Xitoy domen zonasi – “.cn” ro‘yxatga olindi, shu yilning o‘zida bu domen zonasida elektron pochta sayti rasmiy ravishda ochildi[22]. 1994-yilda birinchi marta Internetga Sprint liniyasiga 64 bit/s orqali chiqishga erishildi, bu orqali Xitoy xalqaro hamjamiyat tomonidan rasmiy ravishda Internetning barcha funksiyalariga ega bo‘lgan mamlakat sifatida e’tirof etildi.

---

[20] Cybercrime И European Commission. Home Affairs, http://ec.europa.eu/home-affairs/policies/crime/crime _cybercrime_en.htm/. 2 Communication from the Commission to the European Parliament, the Council and the Com- mittee of the Regions of 22 May 2007 «Towards a general policy on the fight against cyber crime». Brussels, 22.5.2007.COM(2007) 267 final.

[21] Зиновьева Е., Булва В. Цифровой суверенитет Европейского Союза. 27.10.2020.// Современная Европа, 2021, -№ 2. -С. 44-45.

[22] Интернет в Китае. Справка. РИА Новости. 2010, 13 января. [Elektron manba]: http://ria.ru/world/20100113/204310750.html.

Milliy qonunchilikka muvofiq, Xitoyda ikki bosqichli Internet ishlashi lozim: birinchi darajada – foydalanuvchilar global tarmoqlarga faqat magistral aloqalar tugunlari vositasida kirishi mumkin bo‘lgan magistral tarmoqlardan iborat bo‘ldi[23].

Mamlakatda “Oltin qalqon” loyihasi (norasmiy nomi – Buyuk Xitoy fayrvoli) (Xitoy buyuk devoriga o‘xshatma) mamlakat internet tarmoqlariga o‘rnatilgan murakkab filtrlash tizimi doirasida tashkil etilgan edi. Bu loyiha doirasida internet-kanallardagi serverlar tizimi provayderlar va xalqaro tarmoqlarda uzatiladigan axborotlarni filtrlash qobiliyatiga ega edi.

2001-yilda Xitoy Internet tarmoqlaridan foydalanuvchilar jamiyati tashkil etildi, u Internetni rivojlantirishga xizmat qilish uchun mo‘ljallangan bo‘lsa ham, lekin aslida u hukumat tomonidan global tarmoq ustidan nazorat qilish sohasidagi hukumat qarorlarini amalga oshirish maqsadida tashkil etilgan edi.

Xitoyda 2008-yildan boshlab yangi qabul qilingan qoidalarga binoan radioeshittirish yoki onlayn translyatsiya (video) olib borish uchun litsenziya olishga faqat hukumatga qarashli yoki davlat tomonidan nazorat qilinadigan kompaniyalarga ruxsat berildi. 2009-yilda domen nomlarini ro‘yxatdan o‘tkazish uchun qonun kuchga kirib, unga binoan “.cn” zonasida domen nomini ro‘yxatdan o‘tkazish uchun yozma ariza berish, unga ilova tariqasida barcha shaxsiy ma’lumotlar, korxonaning tijorat faoliyatiga berilgan litsenziyani taqdim etish tartibi o‘rnatildi.

Xitoyning axborot xavfsizligi (yoki kiberxavfsizligi) strategiyasi (“Axborotlashishni rivojlantirishni jadallik bilan amalga oshirish va axborot xavfsizligini amalda ta’minlash haqida Davlat kengashining fikri”) 2012-yilda qabul qilindi[24]. 2016-yilda Xitoy kommunistik partiyasi markaziy qo‘mitasi “Innovatsion rivojlanish milliy strategiyasi rejasi”ni e’lon qildi. Unda tarmoqlar xavfsizligi texnologiyalarini tadqiq etish va jadallashtirish orqali Xitoyda iqtisodiy o‘zgarishlarni, modernizatsiya va milliy tarmoqlar xavfsizligini qo‘llab-quvvatlashni himoya qilish ta’minlanadi[25].

2016-yilda Xitoy armiyasida rasmiy ravishda kiberqo‘shin tuzildi. Bu qo‘shinning asosiy vazifasi internet-maydonda harbiy harakatlar olib borish, deb belgilandi. Mamlakat lideri Si Szinpin bayonotiga binoan, qo‘shin tuzilmasi formatini o‘zgartirishdan maqsad – Xitoy armiyasini mintaqaviy mudofaa armiyasidan barcha operatsiyalarni olib borishga qodir qo‘shinga aylantirishdir.

2021-yil 30-iyulda Xitoyda Kiberxavfsizlik milliy markazi – KXMM (National Cybersecurity Center) tashkil etildi. Uxanda tashkil etilgan KXMM

---

[23] Magistral tugunlar (backbone networks) – yuqori tezlikdagi magistral kanallarga qo‘shilib, taqsimlangan tarmoqlar bazaviy tugunlarini ifodalash uchun ishlatiladigan umumiy atama. Korxona miqyosi segmenti, shuningdek, klasterlar va alohida ishlayotgan stansiyalar magistral tarmoqlarga ko‘priklar, marshrutizatorlar va konsentratorlar vositasida ulanadi.

[24] Мнение Государственного совета о форсированном продвижении развития информатизации и о реальном обеспечении информационной безопасности). Официальный сайт Постоянного комитета Всекитайского собрания народных представителей КНР. 17.07.2012. [Elektron manba]: http://www.gov.cn/zwgk/2012-07/17/ content_ 2184979.htm.

[25] *Qarang:* План национальной стратегии инновационного развития). [Elektron manba]: http://www. gov.cn/gongbao/ content/2016 /content_5076961.htm.

kampusi maydoni 40 km.kv. bo‘lib, u bir vaqtning o‘zida maktab, tadqiqotlar laboratoriyasi, inkubator, shu bilan birga, iste’dod egalarini tayyorlash markazi sifatida xizmat qiladi[26].

Tahlillardan ko‘rinib turibdiki, Xitoy davlati internet-texnologiyalariga yirik investitsiyalar ajratish vositasida, xususan, internetda OAVni rivojlantirishni rag‘batlantirish, axborot kanallarini kengaytirish, xorijiy OAVni nisbatan kamaytirish maqsadlarida axborot va kiberxavfsizlikni mustahkamlashni davlat siyosati darajasida amalga oshirmoqda. Lekin AKTlar rivojlanib va takomillashib borgani sari axborot xavfsizligi sohasida yangidan yangi muammolar paydo bo‘lmoqda. Shu bilan birga, axborot xavfsizligiga oid Xitoy tajribasi o‘tish davrini o‘z boshidan kechirayotgan mamlakatlarda bu sohadagi islohotlar uchun nihoyatda muhimdir.

Dissertatsiyaning uchinchi bobi “**O‘zbekistonda ijtimoiy barqarorlikni ta’minlashda axborot xavfsizligi siyosatining rivojlanishi va istiqbollari**” deb nomlanadi. Mazkur bobda O‘zbekistonda axborot xavfsizligi siyosati huquqiy asoslarining shakllanishi va rivojlanishi, kibertahdidlar va ularga qarshi kurash choralari tadqiq etilgan.

1999-yilning 20-avgustida O‘zbekiston Respublikasining “Telekommunikatsiyalar to‘g‘risida”gi Qonuni, 2002-yil 12-dekabrda “Axborot erkinligi prinsiplari va kafolatlari to‘g‘risida”gi Qonuni qabul qilindi. Unda “...urushni va zo‘ravonlikni, shafqatsizlikni targ‘ib qilishni, ijtimoiy, milliy, irqiy va diniy adovat uyg‘otishga qaratilgan terrorizm va diniy ekstremizm g‘oyalarini yoyishni o‘z ichiga olgan axborot tarqatilishiga qarshi harakatlar qilish[27] qoidasi belgilab qo‘yildi. O‘zbekiston Respublikasining 2003-yil 11-dekabrda qabul qilingan “Axborotlashtirish to‘g‘risida”gi Qonunida “shaxs, jamiyat va davlatning axborot xavfsizligini ta’minlash”, “axborot resurslarining tarqalib ketishi, o‘g‘irlanishi, yo‘qotilishi, buzib talqin etilishi, to‘sib qo‘yilishi, qalbakilashtirilishi va ulardan boshqacha tarzda ruxsatsiz erkin foydalanilishining oldini olish” kabi axborot xavfsizligini ta’minlashga oid huquqiy asoslar qabul qilindi.

Axborot xavfsizligi masalalarini muvofiqlashtirish aks etgan yana bir me’yoriy hujjat – bu 2004-yil 29-aprelda qabul qilingan “Elektron hujjat aylanishi to‘g‘risida”gi O‘zbekiston Respublikasi Qonuni bo‘ldi[28]. 2006-yilning 4-aprelida O‘zbekiston Respublikasining “Avtomatlashtirilgan bank tizimida axborotni muhofaza qilish to‘g‘risida”gi qonuni qabul qilindi. Mamlakatda axborot xavfsizligini ta’minlash sohasida 2014-yil 5-mayda qabul qilingan O‘zbekiston

[26] Ларина Е., Овчинский В. Китай готовится стать кибердержавойи создаёт для этого Центр талантов и инноваций в области кибербезопасности. 2 августа 2021 г. [Elektron manba]: https://zavtra.ru/blogs/kitaj_gotovitsya _stat_ kiberderzhavoj.

[27] Ўзбекистон Республикасининг 2002 йил 12 декабрдаги 439-II-сонли “Ахборот эркинлиги принциплари ва кафолатлари тўғрисида”ги Қонуни// Ўзбекистон Республикаси Олий Мажлисининг Ахборотномаси, 2003 й., 1-сон, 2-модда; 2015 й., 52-сон, 645-модда; Қонун ҳужжатлари маълумотлари миллий базаси, 19.04.2018 й., 03/18/476/1087-сон.

[28] Ўзбекистон Республикасининг “Электрон ҳужжат айланиши тўғрисида”ги қонуни. 2004 йил 29 апрель//Ўзбекистон Республикаси қонун ҳужжатлари тўплами", 2004 йил, 20-сон, 230-модда.

Respublikasining “Davlat hokimiyati va boshqaruvi organlari faoliyatining ochiqligi to‘g‘risida”gi Qonuni muhim ahamiyat kasb etdi[29].

2019-yil 2-iyulda O‘zbekiston Respsublikasining “Shaxsga doir ma’lumotlar to‘g‘risida”gi Qonuni qabul qilindi. Mazkur qonunning 28-moddasida “Subyektning roziligisiz yoki boshqa qonuniy asos mavjud bo‘lmagani holda shaxsga doir ma’lumotlarni oshkor etish va tarqatishga yo‘l qo‘yilmasligi to‘g‘risida mulkdor va (yoki) operator yoki shaxsga doir ma’lumotlardan foydalanishga ruxsat olgan boshqa shaxs tomonidan rioya etilishi majburiy bo‘lgan talab shaxsga doir ma’lumotlarning maxfiyligidir”[30] qoidasi mustahkamlab qo‘yildi.

O‘zbekistonda axborot xavfsizligini ta’minlashga oid tub o‘zgarishlar va rivojlanishlar Prezident Sh.M.Mirziyoyev davlat rahbari etib saylanganidan keyin boshlandi. O‘zbekistonning dunyoga ochilishi, rivojlangan davlatlar bilan har tomonlama hamkorlik munosabatlarining yo‘lga qo‘yilishi natijasida mamlakatda AKT va “elektron hukumat”ni rivojlantirish avj oldi. Bu borada mamlakatimiz Prezidenti Sh.M.Mirziyoyev ta’kidlaganlaridek, “taraqqiyotga erishish uchun raqamli bilimlar va zamonaviy axborot texnologiyalarini egallashimiz shart va zarur. Bu bizga rivojlanishning eng qisqa yo‘lidan borish imkonini beradi”[31].

Bundan tashqari, 2017-yil 29-avgustda qabul qilingan O‘zbekiston Respublikasi Prezidentining “Axborot-kommunikatsiya texnologiyalari sohasidagi loyihalarni boshqarish tizimini yanada takomillashtirish chora-tadbirlari to‘g‘risida”gi qarorini bajarish yuzasidan hamda zamonaviy texnologiyalardan foydalangan holda axborot va jamoat xavfsizligi, shuningdek, huquq-tartibotni ta’minlashga qaratilgan chora-tadbirlarni kuchaytirish, “Xavfsiz shahar” yagona apparat-dasturiy kompleksini yaratish loyihasining o‘z vaqtida va sifatli amalga oshirilishini ta’minlash maqsadida 2017-yil 17-oktyabrda O‘zbekiston Respublikasi Vazirlar Mahkamasining “O‘zbekiston Respublikasi axborot texnologiyalari va kommunikatsiyalarini rivojlantirish vazirligining axborot xavfsizligi va jamoat tartibini ta’minlashga ko‘maklashish markazi faoliyatini tashkil etish chora-tadbirlari to‘g‘risida”gi qarori qabul qilindi[32].

O‘zbekiston Respublikasi Prezidentining 2020-yil 5-oktyabrda qabul qilgan PF-6079-sonli “Raqamli O‘zbekiston – 2030” strategiyasini tasdiqlash va uni samarali amalga oshirish chora-tadbirlari to‘g‘risida”gi Farmonida “xalqaro elektron tijorat standartlari va zamonaviy axborot xavfsizligi talablariga rioya

---

[29] Ўзбекистон Республикасининг 2014 йил 5 майда қабул қилинган 369-сонли “Давлат ҳокимияти ва бошқаруви органлари фаолиятининг очиқлиги тўғрисида”ги қонуни. [Elektron manba]: https://lex.uz/docs/2381133.

[30] Ўзбекистон Республикасининг “Шахсга доир маълумотлар тўғрисида”ги қонуни. 2019 йил 2 июль//Қонунчилик маълумотлари миллий базаси, 21.04.2021 й., 03/21/683/0375-сон.

[31] Мирзиёев Ш.М. Янги Ўзбекистон стратегияси. –Т.: “O‘zbekiston” нашриёти, 2021. –Б. 24.

[32] Ўзбекистон Республикаси Вазирлар Маҳкамасининг 2017 йил 17 октябрдаги “Ўзбекистон Республикаси ахборот технологиялари ва коммуникацияларини ривожлантириш вазирлигининг ахборот хавфсизлиги ва жамоат тартибини таъминлашга кўмаклашиш маркази фаолиятини ташкил этиш чора-тадбирлари тўғрисида”ги қарори. //Қонун ҳужжатлари маълумотлари миллий базаси, 18.10.2017 й., 09/17/838/0130-сон, 01.05.2018 й., 09/18/318/1108-сон; 27.03.2019 й., 09/19/254/2839-сон.

qilish uchun elektron tijoratni rivojlantirishning huquqiy asoslarini, shuningdek, mavjud standartlar va elektron tijorat qoidalarini takomillashtirish va yangilash" vazifalari qo‘yildi[33].

2022-yilning 15-aprelida O‘zbekiston Respublikasining "Kiberxavfsizlik to‘g‘risida"gi Qonuni qabul qilindi. Mazkur qonunga binoan O‘zbekiston Respublikasi Davlat xavfsizlik xizmati kiberxavfsizlik sohasidagi vakolatli davlat organi etib belgilandi. Mazkur qonun kiberxavfsizlik subyektlarining huquq va majburiyatlari, ularning kiberxavfsizlik talablariga muvofiqligi yuzasidan ekspertizadan majburiy tartibda yoki kiberxavfsizlik subyektlarining tashabbusiga ko‘ra amalga oshirilishi kabi tartibot o‘rnatildi. Mazkur qonunning qabul qilinishi, dastavval, shaxs, jamiyat va davlat xavfsizligini ta'minlash bilan bir qatorda kiberxavfsizlikni davlat tomonidan tartibga solish, huquqiy, tashkiliy, ilmiy-texnik va me'yoriy uslubiy ta'minot tizimini takomillashtirish, axborot tizimlari va resurslarining yaxlitligini ta'minlash jarayonini huquqiy jihatlardan muvofiqlashtiradi.

O‘zbekiston Respublikasining "Kiberxavfsizlik to‘g‘risida"gi Qonuni, Prezident farmonlarining qabul qilinishi mazkur strategiyani kibermaydonda amalda qo‘llash sohasidagi dastlabki qadamlardan biri bo‘ldi. Mamlakat qisqa davr ichida axborot xavfsizligi sohasida jahondagi rivojlangan davlatlar qatoriga kirishga harakat qila boshladi. Albatta, bu sohadagi rivojlanish Yangi O‘zbekiston poydevorini shakllantirish omillaridan biri hisoblanadi.

Jahon miqyosida axborot texnologiyalarining murakkablashib, takomillashib borishiga monand ravishda ularga qarshi tahdidlar ham ko‘payib va kuchayib bormoqda.

O‘zbekistonda ham so‘nggi uch yilda kiberjinoyatlar 8,3 baravarga ko‘payib, hozirda umumiy jinoyatchilikning qariyb 5 foizini tashkil etmoqda. Xususan, noqonuniy bank-moliya operatsiyalari orqali o‘zgalarning plastik kartadagi mablag‘larini o‘zlashtirish, zararli viruslar tarqatish, qimor va tavakkalchilikka asoslangan onlayn o‘yinlar, diniy aqidaparastlikka qaratilgan axborot xurujlari, onlayn savdo maydonidagi firibgarlik jinoyatlari ko‘payib bormoqda[34].

Kiberhujumlar uchun muayyan chegaraviy to‘siqlar mavjud emasligi, Internet tarmoqlarining globalligi tufayli O‘zbekiston davlati va jamiyatidagi kibermaydonlarga nisbatan hujumlar ham yildan yilga ko‘payib bormoqda. Mazkur masalaga oid eng ko‘p uchraydigan kiberhujumlar va tahdidlar turlari hamda tavsiflari haqida quyidagi tahlillar shakllantirildi. Ularning ichida eng ko‘p uchraydigani quyidagilardir:

Shifratorlar; bloklovchi ekranlar; tarmoq chuvalchang-qurtlari (chervi); moliyaviy fishing hujumlar; DoS/DdoS – hujumlar; botnetlar; kiber-stalking;

---

[33] Ўзбекистон Республикаси Президентининг ПФ-6079-сонли "Рақамли Ўзбекистон - 2030" стратегиясини тасдиқлаш ва уни самарали амалга ошириш чора-тадбирлари тўғрисида"ги Фармони. 2020 йил 5 октябрь//Қонун ҳужжатлари маълумотлари миллий базаси, 06.10.2020 й., 06/20/6079/1349-сон; 02.04.2021 й., 06/21/6198/0269-сон.

[34] Виртуал оламдаги глобал таҳдид. [Elektron manba]: https://uza.uz/uz/posts/virtual-olamdagi-global-tahdid_350549.

kiberterrorizm; kiberfiribgarlik; bulling (ing. “do‘q qilish”, “zo‘ravonlik qilish”); grifing[35].

Shu bilan birga, O‘zbekistonda quyidagi kiberjinoyatchilik turlari keng tarqaldi: virusli dasturiy ta’minotni tarqatish; foydalanuvchining maxfiy ma’lumotlarini o‘g‘irlash; boshqa odamlarning intellektual faoliyat mahsulotlarini o‘g‘irlash; ijtimoiy tarmoqlarda boshqalarning akkauntlarini buzish; yolg‘on ma’lumot tarqatish, tuhmat qilish; millatlararo nizo yoki dinlararo adovatni qo‘zg‘atish; bank plastik kartalari (karta rekvizitlari) bilan noqonuniy operatsiyalar; qimmatli qog‘ozlar bozoridagi Internet-firibgarlik; Internetdagi moliyaviy piramidalar; mobil aloqa bilan bog‘liq jinoyatlar; elektron tijorat sohasidagi boshqa jinoyatlar[36].

O‘zbekistonda kiberxavfsizlik sohasiga tegishli 17 ta qonun hujjati, O‘zbekiston Respublikasi Prezidentining 9 ta farmon va qarori, Vazirlar Mahkamasining 14 ta qarori, shuningdek, tegishli normalar va ko‘plab idoralararo me’yoriy-huquqiy hujjatlar qabul qilindi.

Global kiberxavfsizlik darajasi bo‘yicha 194 mamlakatni o‘z ichiga olgan 2020-yil reytingida O‘zbekiston 70-o‘rinni egalladi. O‘zbekiston mazkur yo‘nalishlar ichida huquqiy choralar bo‘yicha 19.27 ball, hamkorlik bo‘yicha 13.56 ball, salohiyatni rivojlantirishda 15.68 ball, tashkiliy choralar bo‘yicha 10.05 ball hamda texnik choralar bo‘yicha 12.56 ballni qo‘lga kiritgan. Shu tariqa mamlakat jami 71.11 ball olgan. Markaziy Osiyo davlatlari orasida kiberxavfsizlik bo‘yicha Qozog‘iston 31-o‘rin, Qirg‘iziston 92-o‘rin, Tojikiston 138-o‘rin, Turkmaniston 144-o‘rinni egallagan[37].

Jamiyatni tashvishga soladigan holat – bu axborot texnologiyalari yordamida huquqbuzarlik va jinoyatga qo‘l urgan shaxslar orasida yoshlar ko‘pchilikni tashkil etmoqda. Respublikamizda virtual olamdagi qonunbuzilishlarning aksariyati 16-23 yosh oralig‘idagi o‘smir-yoshlar tomonidan sodir qilinmoqda. Bundan ko‘rinib turibdiki, kiberxavfsizlikni ta’minlash masalasi bugun har qachongidan ham dolzarb ahamiyat kasb etmoqda[38].

O‘zbekistonda jamiyat barqarorligini ta’minlashning muhim omili – davlat tomonidan axborot xavfsizligini ta’minlashga oid chora-tadbirlarni amalga oshirish miqyosi ham kengaydi. Shu bilan bir vaqtda, 2020–2022-yillarda axborot-kommunikatsiya vositalari va axborot xavfsizligini ta’minlashga oid texnologiyalarning takomillashib, kengayib va rivojlanib borishiga mutanosib ravishda tashqi kiberhujumlar ham oshib bordi.

---

[35] Бўронов Л. Кибержиноятчиликка қарши курашишда интернет-маданиятнинг аҳамияти. [Elektron manba]: https://ictnews.uz/ uz/15/05/2018/cybercrime/.

[36] Ахборот технологиялари соҳасидаги жиноятлар ва улардан ҳимояланиш усуллари.15 март 2021 й. [Elektron manba]: http://naveconomy.uz/asosiy/yangiliklar/155-ahborot-tehnologiyalari-soasidagi-zhinoyatlar-va-ulardan-imoyalanish-usullari.html.

[37] Ўзбекистоннинг Глобал киберхавфсизлик рейтингидаги ўрни эълон қилинди. [Elektron manba]: https://bugun.uz /2021/10/ 12/ozbekistonning-global-kiberxavfsizlik-reytingidagi-orni-elon-qilindi/.

[38] Кибермаконда содир этилаётган жиноятларга қарши курашиш: муаммолар ва ечимлар. [Elektron manba]: https://iiv.uz/oz/ news/kiber-makonda-sodir-etilayotgan-jinoyatlarga-qarshi-kurashish-muammolar-va-yechimlar.

2022-yilda har kuni o‘rtacha 67 ta dastur-yulg‘ichlarning yangi hujumlari ro‘y berib turdi. Texnikaviy yordam bilan bog‘liq bo‘lgan tovlamachilik hodisalari (fuqarolarga “xorijiy schetlardan pul o‘tkazish”ni taklif qilgan qalloblar) ham ko‘paydi. Bundan ko‘rilgan ziyonlar 347 mln AQSh dollarini tashkil etib, bu ko‘rsatkich 2020-yilga nisbatan 137 foizni tashkil etdi[39]. 2022-yilning birinchi yarmida “UZ” domen hududida 83 ta aniqlangan hujumlar ro‘y berdi. Davlat organlarining veb-saytlarida shu yarim yilda 23 ta axborot xavfsizligiga hamla qilindi[40].

2023-yilning birinchi choragida O‘zbekiston internet tarmog‘i “UZ” segmentida 110 mingdan ortiq veb-sayt domenlari ulangan bo‘lib, shulardan 28 mingdan ortig‘i faol domenlar sifatida ishladi. Ularning 14 mingdan ortig‘i xavfsiz, ya’ni SSL sertifikati bilan himoyalangan domenlar hisoblanadi. Milliy kibermakonda zararli tarmoq bilan bog‘liq 1650000 kibertahdidlar ro‘y berganligi aniqlangan. Shundan 2,1 foizi zaifligi mavjud servislar, 13,1 foizi yopiq bo‘lishi kerak bo‘lgan servislar, 7,3 foizi DdoS hujumiga moyil servislar, 26,4 foizi zararli dasturlar, 51,2 foizi ochiq servislardan iborat bo‘lgan. Internet tarmoqlarining milliy segmentida joylashgan davlat va xo‘jalik organlarining rasmiy veb-saytlarida 249 ta hodisa aniqlangan bo‘lib, buning natijasida davlat idoralarining veb-saytlari umumiy hisobda 417285 daqiqa davomida ishdan chiqishga olib kelgan[41]. Bu shundan dalolat beradiki, kibertahdidlar va hujumlar miqdori yildan yilga oshib bormoqda.

O‘zbekiston Respublikasi Prezidentining 2023-yil 2-iyunda qabul qilgan “O‘zbekiston Respublikasining muhim axborot tuzilmasi obyektlari kiberxavfsizligini ta’minlash tizimini takomillashtirish bo‘yicha qo‘shimcha chora-tadbirlar to‘g‘risida”gi Qarori bilan “O‘zbekiston Respublikasi muhim axborot infratuzilmasi obyektlarining kiberxavfsizligini ta’minlash tartibi to‘g‘risidagi Nizom” tasdiqlanib, unga binoan kiberhujumlarga qarshi kurash shakllari va ularning oldini olish chora-tadbirlari belgilandi[42]. Bu rasmiy hujjatda kiberxavfsizlik sohasida zamonaviy va takomillashgan texnologiyalardan foydalanish va ularni joriy etish masalalarini hal etish ham nazarda tutildi.

Xulosa qilib aytganda, mamlakatda jamiyat barqarorligini ta’minlashning muhim sohasi – axborot xavfsizligini mustahkamlash va takomillashtirish sohasida chuqur islohotlar amalga oshirildi. Bunda avvalo, “Kiberxavfsizlik markazi” davlat unitar korxonasining tashkil etilishi, “Kiberxavfsizlik to‘g‘risida”gi Qonunning qabul qilinishi, axborot xavfsizligiga oid texnologiyalarning yangilanishi va takomillashtirilishi natijasida kiberhujumlar hamlasiga nisbatan to‘siqlar qo‘yildi,

---

[39] Кибербезопасность 2022: обеспечение цифровой безопасности/. 30.06.2022 . [Elektron manba]: https://review.uz/post /kiberbezopasnost-2022-obespechenie-cifrovoy-bezopasnosti/.

[40] Статистика проверок, по состоянию на I- полугодие 2022 года. [Elektron manba]: https://csec.uz/ru/.

[41] “Киберхавфсизлик маркази” давлат унитар корхонаси. 2023 йил 1-чорак якунлари. [Elektron manba]: https://csec.uz/upload/iblock/685/2023%20yil%20I%20chorak%20uchun.pdf.

[42] Ўзбекистон Республикаси Президентининг “Ўзбекистон Республикасининг муҳим ахборот тузилмаси объектлари киберхавфсизлигини таъминлаш тизимини такомиллаштириш бўйича қўшимча чора-тадбирлар тўғрисида”ги қарори. 2023 йил 2 июнь. [Elektron manba]: https://lex.uz/ru/docs/6479190.

jamiyat barqarorligi va xavfsizligi ta’minlandi. Shuningdek, axborot xavfsizligining istiqbollarini yanada yaxshilash maqsadida mazkur soha moddiy-texnika bazasining rivojlantirilishi – bu sohaning yanada rivojlanib borayotganining dalilidir.

XULOSA

“Davlat axborot xavfsizligi siyosatida jamiyat barqarorligini ta’minlashning milliy va xorijiy jihatlari” mavzusida olib borilgan tadqiqotlar asosida quyidagi xulosalar taqdim etiladi:

Birinchidan, XXI asrning ikkinchi o‘n yilligida axborot xavfsizligini ta’minlash jahondagi har bir davlat, jamiyat hayotida ijtimoiy-siyosiy barqarorligini saqlashning asosiy omiliga aylandi. “Axboriy xavfsizlik”, “axboriy muhit”, “axborot xavfsizligi”, “axborot jamiyati”, “shaxs axborot xavfsizligi”, “jamiyatning axborot xavfsizligi”, “davlatning axborot xavfsizligi”, “kommunikatsiyaviy siyosat”, “media siyosati” tushunchalari ta’riflari shakllandi.

Ikkinchidan, xalqaro maydonda axborot almashinuvlarining globallashuvi natijasida xalqaro hamjamiyatda axborot oqimlarining xavfli ta’sirlarini kamaytirishning xalqaro mexanizmlarini topishga zarurat tug‘ildi. Shu tufayli axborot xavfsizligining xalqaro-huquqiy asoslari rivojlana boshladi. Jahon axborot maydoniga oid qonunchilik shakllandi.

Uchinchidan, hozirgi davrga kelib dunyo miqyosida eng xavfli axborot tahdidi terrorchilik va ekstremistik tashkilotlar tomonidan amalga oshirilmoqda. Ayniqsa, Internet ijtimoiy tarmoqlarida terrorchi va ekstremistik tashkilotlarning bir necha minglab saytlarida yoshlarni o‘ziga jalb etuvchi, ularning ongini zaharlovchi materiallar, da’vatlar, soxtalashtirilgan diniy materiallar joylashtirilayotgani tashvishlidir.

To‘rtinchidan, XX asrning 60–70-yillaridan boshlab AQShda axborot xavfsizligi sohasida tub burilish davri boshlandi. Mamlakatda AKTning rivojlanishi va takomillashib borishi, kompyuter tarmoqlarini keng joriy etish oqibatida turli kibertahdidlar kuchaydi. Bu esa axborot xavfsizligini mustahkamlash va kuchaytirish vazifalari 1996-yilda qabul qilingan “Telekommunikatsiyalar to‘g‘risida”gi qonunda mujassamlashdi. 2009-yilga kelib “Kibermaydondagi siyosat obzori” ishlab chiqilib, unda nafaqat kiberxavfsizlik sohasida shakllangan tizim tahlili, balki unda AQSh kiberxavfsizligini har tomonlama rivojlantirish va o‘zgartirish rejasi aks etgan edi. “Kibermaydonda harakat qilishning xalqaro strategiyasi”da kibermaydonda amalga oshiriladigan asosiy prinsiplar, AQShning global darajadagi kibersiyosatining ustuvor yo‘nalishlari mujassamlashtirildi.

Beshinchidan, Yevropa Ittifoqi mamlakatlarida axborot xavfsizligiga oid davlat siyosati eng mukammal va takomillashgan holda amalga oshirilmoqda. Bu sohadagi davlat siyosatining kuchi-qudrati uning avvalambor oddiy fuqarolar manfaatlari asosida qurilganligi bilan xarakterlanadi. Yevropa Ittifoqi axborot xavfsizligi sohasidagi

mavaffaqiyatlarning asosiy sababi – bu demokratik prinsiplarga amal qilishi bilan belgilanadi.

Oltinchidan, Xitoy davlatida Xitoy AKTning salmoqli rolini ifoda etadigan asosiy hujjat – bu Xitoy milliy xavfsizligining keng qamrovli konsepsiyasi hisoblanadi. Unda Xitoy jamiyati, iqtisodiy va harbiy xavfsizligini ta'minlashda, global axborot makonining eng kam nazorat qilinadigan segmenti sifatida Internetga katta e'tibor qaratildi. Xitoyda "Oltin qalqon" loyihasi – Buyuk Xitoy fayrvoli mamlakat internet tarmoqlariga o'rnatilgan murakkab filtrlash tizimi doirasida tashkil etildi. Bu loyiha doirasida internet-kanallardagi serverlar tizimi provayderlar va xalqaro tarmoqlarda uzatiladigan axborotlarni filtrlash qobiliyatiga ega bo'ldi. Natijada, Xitoy axborot xavfsizligi sohasida jahondagi eng kuchli davlatlardan biriga aylandi.

Yettinchidan, O'zbekiston davlati 2017-yildan boshlab kuchayib borayotgan kibertahdidlar, ularga qarshi axborot xavfsizligini ta'minlash maqsadida xalqaro standartlar va milliy manfaatlardan kelib chiqib bir qator qonunlar va boshqa turli me'yoriy hujjatlar shakllantirdi. Axborotlashtirish sohasidagi davlat siyosati axborot resurslari, axborot texnologiyalari va axborot tizimlarini rivojlantirish hamda takomillashtirishning zamonaviy jahon tamoyillari asosida milliy axborot tizimini yaratishga qaratildi.

Shu bilan birga, quyidagi bir qator taklif va tavsiyalarni amaliyotga joriy etish maqsadga muvofiq, deb hisoblaymiz:

- jamiyat barqarorligini ta'minlashda, davlat axborot xavfsizligiga tahdidlarning oldini olishning samarali mexanizmlarini ishlab chiqishda xorijiy tajribalardan foydalangan holda, axborot xavfsizligini ta'minlash Konsepsiyasini ishlab chiqishni Oliy Majlis Qonunchilik palatasiga taklif sifatida kiritish;
- Respublikaning barcha qishloq, tuman, shahar va viloyatlari media makonida axborot xavfsizligini ta'minlash hamda kiberxurujlarga qarshi kurashishda davlat va xususiy sherikchilik asosida yagona UZ domenni yanada transformatsiyalashtirib, axborot hujumlariga qarshi kurashishda zamonaviy texnologiyalar va malakali kadrlar bilan ta'minlash;
- axborot makonidan o'zlarining buzg'unchi siyosiy g'oyalari, shuningdek, ekstremistik radikal mafkuralarini yoyishda foydalanayotgan guruh va tashkilotlar tomonidan olib borilayotgan "kiber" va "gibrid" axborot xurujlarining inson ongiga qilinayotgan g'oyaviy ta'sirlariga qarshi kurashish maqsadida "Intellektual kiberhujumlarga qarshi kurash" guruhlari tashkil etish, ularni zaruriy AKT va boshqa texnologiya vositalari bilan ta'minlash;
- O'zbekiston Respublikasi Maktabgacha va maktab ta'limi vazirligi, Oliy ta'lim, fan va innovatsiyalar vazirligi tarkibidagi tarbiyalanuvchi, o'quvchi va talabalarni hamda yoshlarning uyushmagan qatlamlarini axborot xurujlarining ta'siriga tushib qolishdan saqlash, axborot hujumlariga aks-sado berish, ular tarqatayotgan g'oyalarga qarshi mafkuraviy zarbalar berish maqsadida "Kiberxavfsizlik" nodavlat jamoatchilik markazlarini tashkil etish, ijtimoiy profilaktika ishlarini har bir Oila, mahalla hamda mas'ul mutasaddi tashkilotlar kesimida, birgalikda amalga oshirish bo'yicha ta'sirchan chora-tadbirlar rejasini ishlab chiqish;

- yosh avlodni axborot xurujlari va media siyosiy tahdidlardan saqlash hamda ularda ushbu tahdidlarga qarshi immunitetni shakllantirish, zamonaviy axborot kommunikatsion texnologiyalaridan foydalanishda rivojlangan xorijiy mamlakatlarning amalda sinalgan tajribalarining samarali tomonlarini o‘zlashtirish orqali jamiyatda ijtimoiy-siyosiy barqarorlikni ta’minlash;

- O‘zbekiston Respublikasi maktabgacha va maktab ta’limi vazirligi, Oliy ta’lim, fan va innovatsiyalar vazirligi, Respublika ma’naviyat va ma’rifat markazi, OAV, Yoshlar ishlari agentligi, Yoshlar ittifoqi, jamoat birlashmalari va NNTlar hamda tegishli idoralar bilan hamkorlikda yoshlarning axborot xavfsizligiga oid dunyoqarashini shakllantirishda ularning yosh doirasidan kelib chiqqan holda ilmiy-ommabop, qiziqarli multimedia roliklar, risola va o‘quv qo‘llanmalar, “Axborot xavfsizligi” darsligini yaratish, nashr etish;

- O‘zbekistondagi mavjud oliy ta’lim muassasalarida o‘tilayotgan “Falsafa”, “Sotsiologiya”, “Siyosatshunoslik” fanlari, “Milliy g‘oya va O‘zbekistonning ijtimoiy-iqtisodiy taraqqiyot strategiyasi” kurslarida, qolaversa, umumta’lim maktablarida o‘qitiladigan “Tarbiya”, “Davlat va huquq asoslari” fanlari o‘quv dasturlari va o‘quv qo‘llanmalariga axborot xavfsizligi va “Kiberxavfsizlik” mavzularini kiritish.

- o‘smirlar va bolalar ongini radikal g‘oyalar bilan zararlanishi oldini olish, “Bolalarni ularning sog‘lig‘iga zarar yetkazuvchi axborotdan himoya qilish to‘g‘risida”gi qonunda nazarda tutilgan bolalar psixologiyasiga zarar yetkazuvchi yot va buzg‘unchi g‘oyalarning tarqalishining oldini olishga oid davlat dasturini ishlab chiqish va uni parlamentda qabul qilishga tavsiya etish.

НАУЧНЫЙ СОВЕТ ПО ПРИСУЖДЕНИЮ УЧЁНЫХ СТЕПЕНЕЙ DSc.03/29.12.2022.Ss.21.02 ПРИ ТАШКЕНТСКОМ ГОСУДАРСТВЕННОМ УНИВЕРСИТЕТЕ ВОСТОКОВЕДЕНИЯ

АНДИЖАНСКИЙ ГОСУДАРСТВЕННЫЙ УНИВЕРСИТЕТ

АЛИЕВ ОЛИМБЕК АЙБЕКОВИЧ

НАЦИОНАЛЬНЫЕ И ЗАРУБЕЖНЫЕ АСПЕКТЫ ОБЕСПЕЧЕНИЯ СТАБИЛЬНОСТИ ОБЩЕСТВА В ГОСУДАРСТВЕННОЙ ПОЛИТИКЕ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ

23.00.02 – Политические институты, процессы и технологии

АВТОРЕФЕРАТ
диссертации на соискание ученой степени доктора философии (PhD) по политическим наукам

Ташкент – 2024

Тема диссертации доктора философии (PhD) по политическим наукам зарегистрирована в Высшей аттестационной комиссии при Министерстве высшего образования, науки и инноваций Республики Узбекистан за №B2020.4.PhD/Ss237.

Диссертация выполнена в Андижанском государственном университете.

Автореферат диссертации на трех языках (узбекском, русском, английском (резюме)) размещен на веб-сайте Научного совета (www.namdu.uz) и Информационно-образовательном портале «ZiyoNet» (www.ziyonet.uz).

Научный руководитель:	**Киргизбоев Мукимжон** доктор политических наук, профессор
Официальные оппоненты:	**Жураев Сайфиддин Ахматович** доктор политических наук, профессор
	Юлдашев Анвар Эргашевич доктор исторических наук, профессор
Ведущая организация:	**Узбекский государственный университет мировых языков**

Защита диссертации состоится «14» 2024 года в ____ часов на заседании Научного совета DSc.03/29.04.2022.Ss.27.02 по присуждению ученых степеней при Ташкентском государственном университете востоковедения (Адрес: 100060, город Ташкент, улица Амира Темура, дом 20, Тел.: (71) 2333424; e-mail: info@tsuos.uz).

С диссертацией можно ознакомиться в Информационно-ресурсном центре Ташкентского государственного университета востоковедения (зарегистрирована по № ____). Адрес: 100060, город Ташкент, улица Амира Темура, дом 20. (99871) 233-45-21.

Автореферат диссертации разослан «___» _____ 2024 г.
(протокол реестра рассылки № ___ от «___» _____2024 г.)

Д.Б.Сайфуллаев
Председатель Научного совета по присуждению ученых степеней, доктор исторических наук, профессор

Д.И.Мадаминова
Секретарь Научного совета по присуждению ученых степеней, доктор политических наук, доцент

Э.С.Султанова
Председатель Научного семинара при научном совете по присуждению ученых степеней, доктор политических наук, профессор

ВВЕДЕНИЕ (аннотация диссертации доктора философии (PhD))

Актуальность и необходимость темы диссертации. Во всем мире проблема обеспечения информационной безопасности проявляется как жизненная необходимость в реализации и защите интересов человека, общества и государства. Одной из угроз информационной безопасности являются общественно-политические угрозы, направленные против человечества, использующие информационно-коммуникационные технологии в своих корыстных целях. Становится все более очевидным, что во многих странах происходят попытки фальсификации информации в своих политических целях, и нападения на стратегические инфраструктуры стран наносят вред всему человечеству. Это требует проведения исследований по выявлению объективных и субъективных сторон информационных и идеологических факторов, разработке эффективных методов, инструментов и способов предотвращения различных идеологических рисков.

Появляющиеся в информационном пространстве нетрадиционные призывы обуславливают необходимость разработки новых подходов в вопросах обеспечения стабильности государства и общества. В результате в передовых научно-исследовательских центрах и международных аналитических центрах мира усиливается интерес к исследованию вопросов обеспечения информационной безопасности. Особенно с учетом воздействия информационной безопасности на национальную, региональную и глобальную безопасность, разработка эффективных инструментов и мер борьбы против угрожающих им опасностей составляют объект и теоретико-методологическую основу научных исследований.

Государственная политика в Узбекистане, направленная на обеспечение свободы и открытости информации, а также борьбу против информационных атак, неразрывно связана с процессами укрепления мира и стабильности в мире. В связи с этим, в государственной политике по информационной безопасности в Узбекистане вопросы обеспечения стабильности общества сегодня определены в реализуемой в Узбекистане Стратегии «Узбекистан – 2030» в качестве цели «по созданию необходимых условий для беспрепятственного использования всемирной сети Интернет, обеспечению кибербезопасности в национальном интернет-пространстве и повышению грамотности граждан в деле использования сети Интернет»[43].

Диссертационное исследование в определенной степени послужит реализации задач, вытекающих из Указа Президента Республики Узбекистан от 7 февраля 2017 года № УП–4947 «О Стратегии действий по дальнейшему развитию Республики Узбекистан», Указа Президента Республики Узбекистан от 8 февраля 2018 года № УП–5347 «О мерах по дальнейшему совершенствованию сферы информационных технологий и коммуникаций», Указа Президента

[43] Ўзбекистон Республикаси Президентининг 2023-йил 11- сентябрдаги “Ўзбекистон – 2030” стратегияси тўғрисида”ги ПФ-158-сон Фармони// https://lex.uz/docs/6600413

Республики Узбекистан от 28 января 2022 года № УП–60 «О Стратегии развития Нового Узбекистана на 2022–2026 годы», из распоряжение Президента Республики Узбекистан от 8 апреля 2019 года № Р–5465 «О мерах по разработке Концепции развития национальной идеи на новом этапе развития Узбекистана», из постановления Президента Республики Узбекистан от 22 ноября 2018 года № ПП–4024 «О мерах по совершенствованию системы контроля за внедрением информационных технологий и коммуникаций, организации их защиты», из постановления Президента Республики Узбекистан от 2 февраля 2019 года № ПП–4151 «Об организации деятельности Агентства информации и массовых коммуникаций при Администрации Президента Республики Узбекистан», из постановления Президента Республики Узбекистан от 31 мая 2023 года № ПП–167 «О дополнительных мерах по совершенствованию системы обеспечения кибербезопасности важных объектов критической информационной инфраструктуры Республики Узбекистан».

Соответствие исследования приоритетным направлениям развития науки и технологий в республике. Диссертация выполнена в соответствии с приоритетным направлением республиканского научно-технического развития I.«Формирование системы и пути реализации инновационных идей в социальном, правовом, экономическом, культурном, духовно-образовательном развитии информационного общества и демократического государства».

Степень изученности проблемы. Научно-методическую основу исследования составляют концептуальные и стратегические идеи Президента Республики Узбекистан Ш.М.Мирзиёева относительно процессов дальнейшего совершенствования политических технологий обеспечения информационной безопасности в условиях стабильного и последовательного развития Узбекистана, обеспечения стабильности в обществе[44].

Научные труды современных исследователей можно разделить на три группы: к первой группе относятся ученые, проводившие научно-исследовательскую работу по влиянию государственной политики информационной безопасности Узбекистана на стабильность общества, такие как Ганиев С.К., Худойкулов З.Т., Насруллаев Н.Б., Юлдашев А.Э., Исламов И., Каримов И.М., Тургунов Н.А., Гуломов Ш., Ботиров Ф.Б., Азизова З.И., Акбаров Д., Муитов Д.С., Кушаев У.Р., Насруллаев Н.Б., Касимова Н. и Умарова Н. Они может и не вели исследования именно по нашей теме, но их исследования близки к ИКТ, технологическим и техническим аспектам информационной безопасности, информационным молодежным аспектам. Ряд таких ученых, как

[44] Мирзиёев Ш. Обеспечение верховенства закона и интересов человека является залогом развития страны и благополучия народа. – Ташкент: Узбекистан, 2017. – 48 с.; Мирзиёев Ш. Критический анализ, строгая дисциплина и личная ответственность должны быть повседневным правилом деятельности каждого руководителя. – Ташкент: Узбекистан, 2017. – 104 с.; Мирзиёев Ш. Мы построим наше великое будущее вместе с нашим храбрым и благородным народом. – Ташкент: Узбекистан, 2017. – 488 с.; Мирзиёев Ш. Мы будем решительно продолжать наш путь национального развития и поднимать его на новый уровень. Том 1. – Ташкент: Узбекистан, 2018. – 592 с.; Мирзиёев Ш. Новая стратегия Узбекистана. – Ташкент: Узбекистан, 2021. – 464 с.

Муродова Ш., Раджабов Х. и Юлдашева М.К. провели исследования с точки зрения политических наук.

Ко второй группе относятся исследования ученых стран СНГ, таких как Атаманов Г.А., Манжуева О.М., Захаров М.Ю., Перчук Е.Е., Немкина О.И., Каптюг Ю.А., Сиденова О.М., Поликарпов А.В., Ницэвич В.Ф., Вовендо Ю.В., Рахимзода Ш.К., Мельникова О.А., Курилкин А.В., Федорченко С.Н., Ромашкина А.Б. и других, которые проводили научные исследования по вопросам информационной войны, информационного терроризма, информационного оружия, правовых и психологических механизмов информационной безопасности, взаимосвязи виртуального мира и образа жизни человека, происхождения проблем информационной безопасности.

К третьей группе следует отнести исследования зарубежных ученых, таких как С.Хантингтон, Ф.Фукуяма, Д.Белл, А.Тоффлер, М. Кастельс, У.Ростоу, П.Друкер, Дж.Гэлбрейт, В.Иноземцев, Ф.Вебстер, А.А. Чернов, Р.Ф.Абдеев, И.С.Милюхин[45] и других. Они основали теорию об информации и информационной безопасности, конкретно исследовали проблемы информационной безопасности в концепциях «постиндустриальное общество» и «информационное общество».

При этом тематика их исследований и объекты исследования резко отличаются от темы нашей диссертации.

Анализ степени изученности проблемы показал, что вопросы обеспечения стабильности общества в государственной политике информационной безопасности до сих пор не исследовались в качестве специальной диссертации. В связи с этим в нашей диссертации мы выбрали тему, связанную с вопросами обеспечения стабильности общества в государственной политике информационной безопасности.

Взаимосвязь диссертационного исследования с научно-исследовательскими планами высшего образовательного учреждения, в котором выполняется диссертация. Диссертация была включена в план научно-исследовательских работ Андижанского государственного университета и выполнена в рамках фундаментального проекта кафедры «Теория гражданского общества» на тему «Проблемы развития гражданского общества».

Целью исследования является разработка предложений и рекомендаций по реализации национальной и информационной политики безопасности государства в процессе обеспечения стабильности общества и ее совершенствования.

Задачи исследования:

формирование характеристики понятий информационной безопасности;

раскрытие методологических аспектов информационной безопасности - категориального обзора и эволюции системы международной безопасности в качестве фактора стабильности общества;

[45] Исследования этих и других авторов приведены в списке литературы диссертации.

анализ разработок и опыта США, Европейского Союза и Китая в области информационной безопасности;

исследование формирования и развития правовых основ государственной политики информационной безопасности в Узбекистане;

анализ киберугроз информационной безопасности Узбекистана и процесса борьбы с ними;

научная характеристика процесса дальнейшего развития системы информационной безопасности в Узбекистане и ее перспективы;

разработка выводов, предложений и рекомендаций по дальнейшему развитию и повышению эффективности информационной безопасности в Узбекистане.

Объектом исследования является повышение роли государственной информационной политики в укреплении системы обеспечения стабильности общества в Узбекистане.

Предметом исследования являются особенности политики государства в сфере информационной безопасности, законодательства и общественно-политических отношений, возникающих при этом процессе, в обеспечении стабильности общества.

Методы исследования. В диссертации использованы методы исследования, такие как комплексный подход, диалектика научного познания, историзм, логика, анализ и синтез, сравнительный анализ, наблюдение, опрос.

Научная новизна диссертационного исследования заключается в следующем:

обосновано, что отсутствие единого и универсального механизма обеспечения информационной безопасности в мире, неполучение ожидаемого результата от государственной политики, направленной на ограничение цензуры и информационных потоков, а также уделение странами основного внимания на создание своих национальных контентов в защите стабильности государства и общества от внутренних и внешних информационных атак служат основанием для применения принципа «информация против информации»;

доказана необходимость разработки национальной информационной сети Узбекистана (UzNET), регистрируемой через домен «UZ», основываясь на опыт США, Китая и государств Европы, направленный на укрепление информационной безопасности, исходя из того, что в век информации традиционное общество, превратившись в информационное общество, в синтезе образует конвергенцию, конфиденциальность, связанная с защитой от угроз и вызовов информационной безопасности, доступом в информационные ресурсы, метатехнологиями;

обосновано предложение о создании в институтах махалли общественных центров «Кибербезопасность», исходя из задач по усилению борьбы против кибер и гибридной преступности, как основы обеспечения информационной безопасности, последовательному продолжению работ по

киберпрофилактике, направленных на предотвращение киберугроз, недопущения распространения подрывных идей с целью пробуждения идеологической, религиозной и политической вражды;

доказана необходимость принятия Национальной стратегии информационной безопасности Узбекистана, служащей совершенствованию эффективных механизмов обеспечения национальной информационной безопасности, исходя из государственной политики информационной безопасности, целью которой являются такие задачи, как обеспечение соблюдения законодательства в информационном пространстве Узбекистана, повышение грамотности и культуры использования информации, а также защита населения от воздействия чуждых и деструктивных сведений, предотвращение кибертерроризма и радикализации.

Практические результаты исследования. Изучены суть и значение взглядов на возникновение и совершенствование понятия политики информационной безопасности, проанализированы научно-теоретические взгляды ведущих ученых мира, уточнены основные направления организации политики информационной безопасности в Узбекистане.

В Узбекистане в условиях интеллектуализации информационных угроз задача обогащения содержания мероприятий, разрабатываемых для целей политики информационной безопасности, заключается в национальном контенте, разработанном в целях защиты национальных интересов в сфере информационной безопасности.

Достоверность результатов исследования. Достоверность результатов исследования объясняется статьями, опубликованными в сборниках материалов международных и республиканских научно-практических конференций, специальных и зарубежных журналах, включенных в список ВАК, реализованными на практике выводами, практическими предложениями и рекомендациями, а также подтверждением уполномоченными организациями полученных результатов.

Научная и практическая значимость результатов исследования. *Научная значимость* результатов исследования обусловлена тем, что исследования, проводимые в контексте совершенствования научных учений по политике информационной безопасности, обеспечения информационной безопасности политических институтов, политических процессов и политических технологий, могут быть полезны в качестве теоретического источника для учебников и методических пособий.

Также результаты исследования обогатят науку о прикладной политологии, прикладной журналистике, интернет-журналистике, теории СМИ, теории масс-медиа, информационной безопасности в научно-методическом плане.

Практическая значимость диссертации заключается в том, что ее результаты могут быть использованы в практике повышения квалификации профессоров-преподавателей, преподающих по предметам «Оборона и безопасность», «Информационно-психологическая безопасность в открытых

системах» в высших образовательных учреждениях, при проведении учебных тренингов по развитию их политической компетенции, а также в совершенствовании моделей политической коммуникации. Также материалы диссертации служат учебными материалами по предмету «Информационная безопасность» для студентов, обучающихся по общественно-гуманитарному направлению высших образовательных учреждений.

Внедрение результатов исследования. На основании научного заключения, рекомендаций и предложений, выработанных в результате исследования вопросов обеспечения стабильности общества в государственной политике информационной безопасности, достигнуто следующее:

Выводы диссертации об отсутствии единого и универсального механизма обеспечения информационной безопасности в мире, неполучении ожидаемого результата от государственной политики, направленной на ограничение цензуры и информационных потоков, а также уделении странами основного внимания на создание своих национальных контентов в защите стабильности государства и общества от внутренних и внешних информационных атак служат основанием для применения принципа «информация против информации» использованы при разработке статьи 4 «Основные принципы обеспечения кибербезопасности» Закона Республики Узбекистан «О кибербезопасности» от 15 апреля 2022 года № ЗРУ–764 (*Справка № 13 Комитета по вопросам обороны и безопасности Сената Олий Мажлиса Республики Узбекистан от 1 мая 2023 года*). В результате создана правовая основа для обеспечения приоритета защиты интересов личности, общества и государства в киберпространстве.

Выводы о необходимости разработки национальной информационной сети Узбекистана (UzNET), регистрируемой через домен «UZ», основываясь на опыт США, Китая и государств Европы, направленный на укрепление информационной безопасности, исходя из того, что в век информации традиционное общество, превратившись в информационное общество, в синтезе образует конвергенцию, конфиденциальность, связанная с защитой от угроз и вызовов информационной безопасности, доступом в информационные ресурсы, метатехнологиями использованы при разработке статьи 4 «Основные принципы обеспечения кибербезопасности» Закона Республики Узбекистан «О кибербезопасности» от 15 апреля 2022 года № ЗРУ–764 (*Акт № 12 Комитета по вопросам обороны и безопасности Сената Олий Мажлиса Республики Узбекистан от 12 апреля 2023 года*). В результате в период модернизации и осуществления реформ в Узбекистане это послужило правильному решению проблем, связанных со становлением, динамикой и перспективами системы безопасности, а также развитием этой системы.

Предложения о создании в институтах махалли общественных центров «Кибербезопасность», исходя из задач по усилению борьбы против кибер и гибридной преступности, как основы обеспечения информационной безопасности, последовательному продолжению работ по

киберпрофилактике, направленных на предотвращение киберугроз, недопущения распространения подрывных идей с целью пробуждения идеологической, религиозной и политической вражды были использованы в обеспечении исполнения задач по реализации проекта «Ахборот хашари» и в его рамках – укреплению у населения, особенно у молодежи идеологического иммунитета против необъективной информации на интернет-сайтах и в социальных сетях, а также содействию общественности в формировании правдивого мнения об определенных фактах, которые были намечены в пункте III «Всестороннее глубокое освещение сложных геополитических и идейно-идеологических процессов, происходящих в мире, меры по эффективной идеологической борьбе с терроризмом, религиозным экстремизмом, фанатизмом, сепаратизмом, торговлей людьми, «массовой культурой» и другими угрозами» Программы мер по дальнейшему повышению эффективности духовно-просветительской работы, повышению интеллектуального потенциала и расширению мировоззрения населения, укреплению идеологического иммунитета в Республике Узбекистан, разработанной в соответствии с постановлением Президента Республики Узбекистан от 3 мая 2019 года № ПП–4307 «О дополнительных мерах по повышению эффективности духовно-просветительской работы» (*Акт № 228 Центра социальных и духовных исследований при Центре духовности и просветительства Республики Узбекистан от 19 июня 2023 года*). В результате это послужило разработке современных пропагандистских технологий для обеспечения формирования у молодежи глубоких знаний о сути и содержании политики информационной безопасности, проводимой на основе Стратегии развития Нового Узбекистана.

Выводы о необходимости принятия Национальной стратегии информационной безопасности Узбекистана, служащей совершенствованию эффективных механизмов обеспечения национальной информационной безопасности, исходя из государственной политики информационной безопасности, целью которой являются такие задачи, как обеспечение соблюдения законодательства в информационном пространстве Узбекистана, повышение грамотности и культуры использования информации, а также защита населения от воздействия чуждых и деструктивных сведений, предотвращение кибертерроризма и радикализации, использованы при разработке Основных направлений обеспечения кибербезопасности интернет-пространства зоны UZ домен, а также Программы мер обеспечения комплексных задач по защите других направлений, касающихся электронного правительства, энергетики, систем цифровой экономики, важных информационных инфраструктур (*Акт Андижанского филиала Агентства по делам молодежи от 18 ноября 2022 года*). В результате это послужило повышению политических знаний в области информационной безопасности, киберпреступности, кибертерроризма, духовно-просветительской, правовой, политической культуры молодежи и работников, осуществляющих деятельность в системе Агентства, а также росту эффективности работы в сфере по делам молодежи.

Апробация результатов исследования. Результаты исследования были представлены в виде лекций на 3 международных и 8 республиканских научно-практических конференциях и прошли апробацию.

Опубликованность результатов исследования. Всего по теме диссертации опубликованы 18 научных работ, в том числе 7 статей в научных изданиях, рекомендованных к публикации Высшей аттестационной комиссией Республики Узбекистан, в том числе в 3 республиканских и 4 зарубежных журналах.

Структура и объем диссертации. Диссертация состоит из введения, трех глав, девяти параграфов, заключения и списка использованной литературы. Объем диссертации составляет 166 страниц.

ОСНОВНОЕ СОДЕРЖАНИЕ ДИССЕРТАЦИИ

Во введении указываются актуальность и необходимость темы, уровень изученности проблемы, научная новизна, зависимость исследования от основных приоритетов развития науки и технологий республики, объект, предмет, методы, определены цели и задачи, представлена научная и практическая значимость полученных результатов, их внедрение, апробация, опубликованные работы, информация о структуре диссертации.

В первой главе под названием **«Методологические аспекты исследования политики информационной безопасности в обеспечении стабильности общества»** исследована характеристика понятий информационной безопасности, становления и развития международной системы информационной безопасности, а также факт того, что информационная безопасность является фактором обеспечения стабильности общества.

Представления об информационной безопасности сформировались после того, как глобальные проблемы информационной безопасности стали проявляться опасным и агрессивным образом. Концепция международной информационной безопасности, используемая ООН, подразумевает защиту глобальных информационных систем от так называемой «триады угроз» — терроризма, криминальных и военно-политических угроз (под военно-политическими угрозами подразумеваются информационные войны и информационные конфликты).

США и Европейский Союз (ЕС) указывают на кибертерроризм и киберпреступность как на основные угрозы кибербезопасности и рекомендуют[46] координировать межгосударственные конфликты в киберпространстве в рамках международного гуманитарного права. Статья 2 Конвенции «Обеспечение международной информационной безопасности», принятой ООН 22 сентября 2011 года, определяет «информационную безопасность» как «состояние

[46] Зиновьева Е.С. Международная информационная безопасность. 20.06.2014 г. [Elektron manba]: https://mgimo.ru/ about/ news/ experts/ 256505/.

защищенности интересов личности, общества и государства от деструктивных угроз и иных неблагоприятных воздействий в информационном пространстве»[47].

Р. Хэндли и Р. Андерсон, проводящие исследования в международном масштабе, в своих исследованиях в качестве информационной безопасности выдвинули технологические аспекты защиты информации в компьютерах и социальных сетях в процессе поиска решений проблем информационной безопасности, связанных с угрозами информационным инфраструктурам США.[48]

Информационную безопасность можно определить следующим образом: это состояние социума, при котором возникают угрозы государству, обществу и личности через информационные потоки, которые упорядоченно и стихийно возникают в информационном пространстве. Информационная безопасность означает защиту жизненно важных интересов личности, общества и государства от информационной войны, интервенций и дезинформационного давления. В целом, ученые под информационно-политической безопасностью понимают комплекс проблем, связанных с защитой жизненно важных интересов граждан, государства и общества от внутренних и внешних информационных угроз в политической сфере.

Международная конвенция электросвязи, принятая в 1973 году в рамках мирового информационного пространства, стала первым официальным документом по информационной безопасности. Данная Конвенция была принята в отношении последствий использования информационных средств и формирования информационных полей со специфическими характеристиками этого процесса.

Принятый 4 декабря 1998 года документ ООН под названием «Достижения в области информатизации и телекоммуникаций в сфере международной безопасности» стал официальным началом установления совершенно нового международно-правового режима, субъектом которого являются информация, информационные технологии и способы их использования.[49] Тема этого документа обсуждалась на Генеральной Ассамблее ООН в 2000 году, где было рекомендовано уточнить и сформировать базовые понятия, такие как «информационное оружие», «информационная война» и «информационная безопасность».[50]

22 сентября 2011 года Генеральная Ассамблея ООН приняла Конвенцию об обеспечении международной информационной безопасности. Ее основной целью было «противодействие ИКТ, используемым для нарушения международного мира и стабильности, а также реализация мер по поддержке

---

[47] Конвенция об обеспечении международной информационной безопасности (концепция) ООН. 22 сентября 2011 г. [Elektron manba]: https://www.mid.ru/ mezdunarodnaya informacionnaya bezopasnost/-/asset publisher/UsCUTiw2pO53/ content/ id/ 191666.

[48] Hundley, R.; Anderson, R. Security in Cyberspace: An Emerging Challenge for Society, 1994.

[49] Крутских А.В. Информационный вызов безопасности на рубеже XXI века // Международная жизнь. 1999, №2. –С.48.

[50] Информационные вызовы национальной и международной безопасности / Под ред. А.В. Федорова, В.Н. Цыгичко. –М.: ПИР-Центр, 2001. –С.193.

деятельности государств в информационной сфере»[51]. В 2016 году по предложению Российской Федерации был принят новый проект резолюции «Достижения в сфере информатизации и телекоммуникаций в контексте международной безопасности» при соавторстве 84 стран.

22 октября 2018 года на 73-й сессии Генеральной Ассамблеи ООН была принята очередная резолюция ООН под названием «Достижения в области информатизации и телекоммуникаций в контексте международной безопасности».[52] 12 марта 2021 года был принят доклад Рабочей группы открытого состава ООН под названием «Достижения в сфере информатизации и телекоммуникаций в контексте международной безопасности». Отчет был принят всеми странами-участницами на основе взаимного согласия.

В ближайшие пять лет в международном информационном пространстве стали появляться новые усовершенствованные виды киберпреступности.

Рост киберпреступности побудил страны совершенствовать и развивать взаимную международную информационную безопасность в сотрудничестве с ООН. Конечно, развитые страны приняли активное участие в этих сложных и трудоемких процессах, они не жалели своих ресурсов и средств в этой области.

В последнее десятилетие в мире сформировалась система международной безопасности, в которую вошли большинство государств мира. К настоящему времени национальные государства приобрели опыт и методы борьбы с терроризмом, экстремизмом, кибертерроризмом, киберпреступностью и кибератаками во взаимодействии с международными организациями.

Концепция информационного общества, открытая японскими учеными профессором Ю. Хаяси[53] и И. Масуда, впервые была разработана для решения задач экономического развития. Вот почему оно получило более ограниченные и более ориентированные на практику описания. Однако в 60-е годы XX века идею постиндустриального общества разработал американский ученый Дэниел Белл[54], а к 70-м годам начались процессы конвергенции и объединения двух новых — информационного общества и постиндустриального общества.[55]

Согласно отчету ЮНЕСКО, концепция «информационного общества» основывалась на технологических достижениях.[56] Конечно, информационное общество и информационная революция привели к неприятным политическим последствиям: «информационная революция не только ускоряет цивилизационные процессы, но и увеличивает новые национальные,

---

[51] Конвенция об обеспечении международной информационной безопасности. [Elektron manba]: https://pircenter.org/wp-content/uploads/2022/10/Конвенция-об-обеспечении-международной-информационной-безопасности-концепция-РФ.pdf.

[52] Резолюция ООН от 5 декабря 2018 г. A/RES/73/27 «Достижения в сфере информатизации и телекоммуникаций в контексте международной безопасности». [Elektron manba]: https://www.un.org/ga/search/view_ doc.asp? symbol=A/RES/73/27 (Дата обращения: 16.11.2019).

[53] Masuda Y. The Information Society as Postindustrial Society. -Wash.: World Future Soc.,1983. -P. 29.

[54] Bell D. The Coming of Post-industrial Society. A Venture in Social Forcasting. -N.Y., Basic Books, Inc., 1973.

[55] Классические зарубежные концепции информационного общества. [Elektron manba]: https://studref.com/416484/politologiya/ klassicheskie_zarubezhnye_kontseptsii_informatsionnogo_obschestva.

[56] К обществам знания. Всемирный доклад ЮНЕСКО. – Париж: Издательство ЮНЕСКО, 2005. –С. 19.

региональные и глобальные угрозы».[57] К началу XXI века защита от угроз информационной безопасности выражалась в следующих:

- доступ к информационным ресурсам (блокировка доступов);
- конфиденциальность (бесправный и несанкционированный доступ к информации);
- нарушение целостности (искажение информации).

Также появились следующие виды угроз информационной безопасности:

- появление и распространение «метатехнологий» (то есть сбора информации о потребителях производителями различных гаджетов, контроля над ними);
- «электронно-цифровые разрывы», т.е. появление элиты с неограниченным доступом к ИКТ как внутри страны, так и за рубежом. В результате возможности манипулирования мнениями и взглядами отдельных людей, социальных групп и государства с каждым годом возрастают;
- компьютерная милитаризация, информационный терроризм и преступность, т.е. достижение военно-политического преимущества за счет огромного потенциала ИКТ, конфронтация и шантаж на основе силы, изменение представлений о кризисах, конфликтах, тактике и стратегии военных действий, приближение и объединение военных технологий, тем самым организация новых маршрутов гонок.

Основными целями информационных угроз являются информационные ресурсы – информационные инфраструктуры, а также информация и информационные потоки (например, сборники документов, банки данных и базы данных, архивы, библиотеки, музейные фонды и другие устройства хранения информации).

Эти угрозы усиливаются, с одной стороны, исходя из политических интересов отдельных государств и политических сил, а с другой стороны, в условиях некоторых негативных последствий процесса глобализации, который является уникальным проявлением современности, когда наша страна открывает свои двери в мир, как независимый, демократический субъект международного сообщества.

Во второй главе диссертации **«Процесс совершенствования политики информационной безопасности в развитых государствах»** исследуется процесс совершенствования государственной политики информационной безопасности США, форма политики информационной безопасности и ее реализация в Европейском Союзе, а также эволюция и развитие государственной политики в области информационной безопасности в Китае.

Со второй половины XX века в сфере информационной безопасности США начался период радикальных перемен. В 1958 году по директиве Министерства обороны США было создано Агентство перспективных исследований и

[57] К обществам знания. Всемирный доклад ЮНЕСКО. – Париж: Издательство ЮНЕСКО, 2005. –С. 19.

разработок (ARPA). В 1972 году оно было реорганизовано и переименовано в Агентство перспективных оборонных исследований и разработок (DARPA).[58]

С 80-х годов XX века подходы к обеспечению информационной безопасности в компьютерных сетях и системах начали серьезно меняться. В 1984 году был принят нормативный документ «Национальная политика в области телекоммуникаций и автоматизированных информационных систем». В США самыми большими проблемами объявлены кибертерроризм, киберпреступность и использование ИКТ государствами во враждебных целях. Политика борьбы с этой отраслью была официально закреплена в Законе «О компьютерной безопасности» 1987 года. Были объявлены указ президента США от 16 октября 2001 года (PATRIOT ACT) и приказ 2003 года «Национальная стратегия защиты киберпространства».[59]

Следующий этап развития системы кибербезопасности в США начался в 2008 году, и с этого периода начал реализовываться документ «Общенациональная инициатива кибербезопасности». К 2009 году президент США Барак Обама объявил обеспечение безопасности киберпространства важнейшей государственной задачей. В том же году был разработан официальный документ «Обзор политики в киберпространстве». Ко времени президентства Дж. Буша был принят документ под названием «Общенациональная инициатива кибербезопасности».[60] В мае 2009 года президент Б.Обама анонсировал «Обзор киберполитики» (Cyberspace Policy Review), в котором обозначил пять приоритетных направлений в сфере кибербезопасности. Среди них важнейшим была названа инициированная Дж.Бушем разработка новой Национальной стратегии обеспечения безопасности в американских информационно-коммуникационных сетях. К 2012 году в США была принята «Национальная стратегия защиты и обмена информацией». Этот документ определил три основных принципа политики информационной безопасности США: информация как национальное достояние; обмен информацией и ее защита, поскольку общие риски требуют совместного использования; принятие более эффективных решений благодаря увеличению потока информации.

24 апреля 2015 года Министерство обороны США приняло обновленную Национальную стратегию кибербезопасности, согласно которой была поставлена задача противостоять любым кибератакам, максимально надежно защитить США от любого врага или преступника.

---

[58] Соглашение между правительствами государств-членов Шанхайской организации сотрудничества о сотрудничестве в области обеспечения международной информационной безопасности. [Elektron manba]: http://docs.Pravo . ru/document/view/20364925/19329178/.

[59] Public Law 89-306 (Brooks Act – with amendments) [issued on 30.10.1965] // National Institute of Standards and Technology. [Official website] Систем. требования: Adobe Acrobat Reader. [Elektron manba]: http://itl.nist.gov/History%20 Documents/Brooks%20Act.pdf (Дата обращения: 01.05.2014).

[60] National Security Strategy 2010. // National Security Strategy Archive. [Web-source] Систем.требования: AdobecrobatReader. [Elektron manba]: http://nssarchive.us/NSSR/2002.pdf (Дата обращения: 01.12.2014).

19 января 2018 года Министерство обороны США анонсировало обновленную версию «Национальной оборонной стратегии». Осенью этого года президент Д.Трамп подписал документ «Национальная стратегия кибербезопасности». С избранием Джо Байдена президентом в 2021 году внимание к кибербезопасности еще более усилилось. В мае 2021 года он подписал указ «Усиление кибербезопасности и защиты сетей федерального правительства». В соответствии с этим указом для органов власти страны было разработано специальное стандартизированное руководство по борьбе с атаками в сфере кибербезопасности, которое содержало ряд рекомендаций. Кроме того, частному сектору был дан ряд рекомендаций по обеспечению информационной безопасности.[61]

США вложили больше всех средств в сферу информационной безопасности среди стран мира. Это обстоятельство еще более повысило их политическую и военную мощь, а также шансы существовать как государство, определяющее мировую политику.

В 1990-е годы XX века ряд правовых актов по защите телекоммуникаций и информации был принят как на национальном уровне, так и на уровне ЕС. Важнейшим из них является Сообщение «Сетевая и информационная безопасность: предложения по европейским политическим подходам», опубликованное Европейской комиссией в 2001 году, которое инициировало важные изменения в жизни ЕС. Вместе с тем, 28 января 2002 года Совет ЕС принял решения об «Общих подходах и специальных мерах в области сетевой и информационной безопасности», а 18 февраля 2003 года – о «Европейском подходе к культуре сетевой и информационной безопасности».

10 марта 2004 года было создано «Европейское агентство сетевой и информационной безопасности» (European Network and Information Security Agency - ENISA) с целью усиления мер против угроз сетевой и информационной безопасности. Его основной задачей было «обеспечить высокий и эффективный уровень сетевой и информационной безопасности внутри сообщества ЕС и развивать культуру сетевой и информационной безопасности на благо граждан, пользователей, производителей и государственного сектора».

С 2010-х годов в ЕС возросла киберпреступность: появились новые виды атак на информационные системы или фишинг (подмена банковских веб-сайтов с целью запроса паролей для получения доступа к банковским счетам). Кроме того, возросло количество традиционных преступлений, таких как вымогательство и распространение нелегального контента (материалов, пропагандирующих сексуальное насилие или насилие над детьми в Интернете), а также использование компьютеров для совершения преступлений.[62]

---

[61] Cyberspace Policy Review: Assuring a Trusted and Resilient Information and Communications Infrastructure [issued on 29.05.2009] // The White House. [Official website]. [Elektron manba]: http://www.Whitehouse. gov/assets/documents/ yberspace_Policy_Review_ final.pdf (Дата обращения: 01.05.2014).

[62] Safer Internet Programme: Empowering and Protecting Children Online. [Elektron manba]: http://ec.europa.eu/ information_society /activities/sip/index_en.htm.

В Стокгольмской программе (The Stockholm Programme) основное внимание ЕС в 2010–2014 годах было направлено на вопросы обеспечения информационной безопасности и борьбы с киберпреступностью.

24 июля 2020 года Европейская комиссия приняла новую Стратегию безопасности Союза. В основном она была сосредоточена на защите важных инфраструктур информационной безопасности от киберпреступлений и поставила задачи по усилению борьбы с гибридными угрозами и организованной преступностью. Стратегия безопасности Союза обновила стратегии последних 20 лет.

Цифровая стратегия Европы (Shaping Europe's digital future), являющаяся основным координирующим документом важного направления цифрового развития ЕС, была принята в феврале 2020 года. В этой стратегии определены приоритетные направления деятельности Европейской комиссии до 2024 года в сфере цифровизации[63].

Из этого следует, что информационная безопасность и кибербезопасность ЕС развивается в конкуренции с США и Китаем, которые борются за мировое лидерство в этой области.

Государственная стратегическая программа инновационного развития Китая включает важные задачи, связанные с расширением киберпространства и укреплением его безопасности. Для Китая информационная безопасность – это прежде всего инновации, и поэтому такой подход является уникальной особенностью кибербезопасности. В Китае эра Интернета впервые началась 20 сентября 1987 года, когда профессор Сян Тяньбай из Пекинского института физики и высоких энергий в рамках программы CANET (Китайская академическая сеть) отправил первое электронное письмо из Китая.

В октябре 1990 года была зарегистрирована китайская доменная зона – «.cn», и в этом же году в этой доменной зоне был официально открыт сайт электронной почты. В 1994 году на линии Sprint впервые был обеспечен доступ в Интернет со скоростью 64 бит/с, что сделало Китай официально признанным международным сообществом в качестве страны с полными возможностями Интернета.

Согласно национальному законодательству, в Китае должен работать двухуровневый Интернет: на первом уровне он состоял из магистральных сетей, где пользователи могли получить доступ к глобальным сетям только через магистральные узлы связи.[64]

В стране был создан проект «Золотой щит» (неофициально известный как Великий китайский файрвол (подобно Великой китайской стене) как часть сложной системы фильтрации, установленной в интернет-сетях страны.

---

[63] Зиновьева Е., Булва В. Цифровой суверенитет Европейского Союза. 27.10.2020.// Современная Европа, 2021, -№ 2. -С. 44-45.

[64] Зиновьева Е., Булва В. Цифровой суверенитет Европейского Союза. 27.10.2020.// Современная Европа, 2021, -№ 2. -С. 44-45.

В рамках этого проекта система серверов в интернет-каналах получила возможность фильтровать информацию, передаваемую провайдерами и международными сетями.

В 2001 году была создана Китайская ассоциация интернет-пользователей, хотя она была призвана служить развитию Интернета, но на самом деле она была создана правительством для реализации правительственных решений в сфере контроля над глобальной сетью.

С 2008 года, в соответствии с недавно принятыми правилами, в Китае только государственным или контролируемым государством компаниям разрешено получать лицензии на вещание или онлайн-вещание (видео). В 2009 году вступил в силу закон о регистрации доменных имен, согласно которому предусмотрен порядок подачи письменного заявления на регистрацию доменного имени в зоне «.cn», предоставления всех персональных данных и лицензии на коммерческую деятельность предприятия.

Стратегия информационной безопасности (или кибербезопасности) Китая («Заключение Госсовета об ускорении развития информации и практическом обеспечении информационной безопасности») была принята в 2012 году.[65] В 2016 году центральный комитет Коммунистической партии Китая объявил «План национальной стратегии инновационного развития». Он обеспечивает поддержку экономической трансформации, модернизации и национальной сетевой безопасности Китая путем исследования и ускорения технологий сетевой безопасности.[66]

В 2016 году в Китайской армии было официально создано кибервойско. Основной задачей этого войска было ведение боевых действий на интернет-пространстве. Согласно заявлению лидера страны Си Цзиньпина, цель изменения формата военной структуры — превратить китайскую армию из армии региональной обороны в армию, способную проводить все операции.

30 июля 2021 года в Китае был создан Национальный центр кибербезопасности – НЦК (National Cybersecurity Center). Площадь кампуса НЦК в Ухане составляет 40 кв. км, которая служит как школа, исследовательская лаборатория, инкубатор и в то же время центр подготовки талантов.[67]

Из анализа видно, что китайское государство реализует усиление информационной и кибербезопасности на уровне государственной политики, с целью выделения крупных инвестиций в интернет-технологии, в частности, для стимулирования развития СМИ в Интернете, расширения информационных

---

[65] Интернет в Китае. Справка. РИА Новости. 2010, 13 января. [Электронный источник]: http://ria.ru/world/20100113/204310750.html.

[66] Мнение Государственного совета о форсированном продвижении развития информатизации и о реальном обеспечении информационной безопасности). Официальный сайт Постоянного комитета Всекитайского собрания народных представителей КНР. 17.07.2012. [Elektron manba]: http://www.gov.cn/zwgk/2012-07/17/ content_ 2184979.htm.

[67] Ларина Е., Овчинский В. Китай готовится стать кибердержавойи создаёт для этого Центр талантов и инноваций в области кибербезопасности. 2 августа 2021 г. [Elektron manba]: https://zavtra.ru/blogs/ kitaj_gotovitsya _stat_ kiberderzhavoj.

каналов и сокращения количества иностранных СМИ. Но по мере развития и совершенствования ИКТ возникают новые проблемы в сфере информационной безопасности. В то же время опыт Китая в области информационной безопасности чрезвычайно важен для реформ в этой сфере в странах с переходной экономикой.

В третьей главе под названием **«Развитие и перспективы политики информационной безопасности в обеспечении социальной стабильности в Узбекистане»** изучаются формирование и развитие правовых основ политики информационной безопасности в Узбекистане, киберугрозы и меры борьбы с ними.

20 августа 1999 года был принят Закон Республики Узбекистан «О телекоммуникациях», 12 декабря 2002 года — Закон «О принципах и гарантиях свободы информации». Он установил правила противодействия распространению информации, которые включают «...пропаганду войны и насилия, жестокости, распространение[68] идей терроризма и религиозного экстремизма, направленных на разжигание социальной, национальной, расовой и религиозной вражды. В Законе Республики Узбекистан «Об информатизации», принятом 11 декабря 2003 года, были закреплены правовые основы обеспечения информационной безопасности, определяющие «обеспечение информационной безопасности личности, общества и государства», «предотвращение распространения, хищения, утраты, искажения, блокирования, фальсификации информационных ресурсов и другого несанкционированного их свободного использования».

Еще одним нормативным документом, отражающим координацию вопросов информационной безопасности, является Закон Республики Узбекистан «Об электронном документообороте», принятый 29 апреля 2004 года[69]. 4 апреля 2006 года принят Закон Республики Узбекистан «О защите информации в автоматизированной банковской системе». В сфере обеспечения информационной безопасности в стране важное значение приобрел Закон Республики Узбекистан «Об открытости деятельности органов государственной власти и управления», принятый 5 мая 2014 года[70].

2 июля 2019 года принят Закон Республики Узбекистан «О персональных данных». Статья 28 настоящего Закона гласит: «Конфиденциальностью персональных данных является обязательное для соблюдения собственником и (или) оператором или иным получившим доступ к персональным данным

---

[68] Закон Республики Узбекистан от 12 декабря 2002 года № 439-II «О принципах и гарантиях свободы информации» // Вестник Олий Мажлиса Республики Узбекистан, 2003 г., № 1, статья 2; 2015, № 52, статья 645; Национальная база данных законодательства, 19.04.2018, №18.03.476/1087.

Закон Республики Узбекистан «Об электронном документообороте». 29 апреля 2004 года // Сборник правовых документов Республики Узбекистан», 2004 г., № 20, статья 230.

[69] Закон Республики Узбекистан «Об электронном документообороте». 29 апреля 2004 года // Сборник правовых актов Республики Узбекистан», 2004 г., № 20, статья 230.

[70] Закон Республики Узбекистан № 369 «Об открытости деятельности органов государственной власти и управления», принятый 5 мая 2014 года. [Электронный источник]: https://lex.uz/docs/2381133.

лицом требование о недопустимости их раскрытия и распространения без согласия субъекта или наличия иного законного основания»[71].

Принципиальные изменения и события, связанные с обеспечением информационной безопасности в Узбекистане, начались после избрания Президента Ш.Мирзиёева Главой государства. В результате открытия Узбекистана миру, установления всесторонних отношений сотрудничества с развитыми государствами, в стране ускорилось развитие ИКТ и «электронного правительства». В связи с этим, как заявил Президент нашей страны Ш.М.Мирзиёев, «для достижения прогресса необходимо и обязательно осваивать цифровые знания и современные информационные технологии. Это позволяет нам идти по кратчайшему пути развития»[72].

Кроме того, в связи с реализацией постановления Президента Республики Узбекистан «О мерах по дальнейшему совершенствованию системы управления проектами в области информационно-коммуникационных технологий», принятого 29 августа 2017 года, и обеспечения информационной и общественной безопасности, а также правопорядка с использованием современных технологий в целях усиления мер, направленных на обеспечение своевременной и качественной реализации проекта создания единого аппаратно-программного комплекса «Безопасный город», 17 октября 2017 года принято постановление Кабинета Министров Республики Узбекистан «О мерах по организации деятельности Центра содействия информационной безопасности и общественного порядка Министерства по развитию информационных технологий и коммуникаций Республики Узбекистан».[73]

В Указе Президента Республики Узбекистан от 5 октября 2020 года № УП–6079 «Об утверждении Стратегии «Цифровой Узбекистан – 2030» и мерах по ее эффективной реализации» определены задачи по установлению международных стандартов электронной коммерции и современных требований информационной безопасности, совершенствованию и обновлению правовой основы развития торговли, а также существующих стандартов и правил электронной коммерции»[74].

15 апреля 2022 года был принят Закон Республики Узбекистан «О кибербезопасности». Согласно этому закону Служба государственной безопасности Республики Узбекистан была определена компетентным государственным органом в сфере кибербезопасности. Этот закон устанавливает

[71] Закон Республики Узбекистан «О персональных данных». 2 июля 2019 года//Национальная база данных законодательства, 21.04.2021, №21/03/683/0375.

[72] Мирзиёев Ш.М. Новая стратегия Узбекистана. -Т.: Издательство «Узбекистан», 2021. -Б. 24

[73] Постановление Кабинета Министров Республики Узбекистан от 17 октября 2017 года «О мерах по организации деятельности Центра содействия информационной безопасности и общественного порядка Министерства по развитию информационных технологий и коммуникаций Республики Узбекистан». //Национальная база данных законодательства, 18.10.2017, № 09/17/838/0130, 01.05.2018, № 09/18/318/1108; 27.03.2019, №19.09.254/2839.

[74] Указ Президента Республики Узбекистан № ПФ-6079 «Об утверждении Стратегии «Цифровой Узбекистан – 2030» и мер по ее эффективной реализации. 5 октября 2020//Национальная база данных законодательства, 10.06.2020, №20/06/6079/1349; 04.02.2021, №21.06/6198/0269.

порядок прохождения обязательной экспертизы прав и обязанностей субъектов кибербезопасности, их соответствия требованиям кибербезопасности или по инициативе субъектов кибербезопасности. Принятие данного закона, прежде всего, помимо обеспечения безопасности личности, общества и государства, координирует процесс государственного регулирования кибербезопасности, совершенствования системы правового, организационного, научно-технического и нормативно-методического обеспечения и процесс обеспечения целостности информационных систем и ресурсов с юридической точки зрения.

Принятие Закона Республики Узбекистан «О кибербезопасности» и указов Президента страны стало одним из первых шагов по реализации этой стратегии в киберпространстве. За короткий период страна стала стремиться войти в число развитых стран мира в сфере информационной безопасности. Конечно, развитие в этой сфере является одним из факторов формирования фундамента Нового Узбекистана.

Угрозы информационным технологиям растут и усиливаются по мере усложнения и совершенствования информационных технологий в глобальном масштабе.

В Узбекистане киберпреступность за последние три года выросла в 8,3 раза и сейчас составляет около 5 процентов от общего числа преступлений. В частности, увеличиваются хищения средств с чужих пластиковых карт путем незаконных банковско-финансовых операций, распространение вредоносных вирусов, азартных и рискованных онлайн-игр, информационные атаки, направленные на религиозный фанатизм, мошенничество в сфере интернет-торговли.[75]

В связи с отсутствием конкретных пограничных преград для кибератак и глобальным характером сетей Интернет, атаки на киберпространство государства и общества Узбекистана с каждым годом увеличиваются. Сформирован следующий анализ типов и описаний наиболее распространенных кибератак и угроз, связанных с данной проблемой. Наиболее распространенными из них являются:

шифраторы;
блокировка экранов;
сетевые черви (черви);
финансовые фишинговые атаки;
DoS/DdoS – атаки;
ботнеты;
киберпреследование;
кибертерроризм;
кибермошенничество;
буллинг (англ. «издевательство»);

[75] Глобальная угроза в виртуальном мире. [Электронный источник]: https://uza.uz/uz/posts/virtual-olamdagi-global-tahdid_350549.

гриффинг.[76]

Вместе с тем в Узбекистане получили распространение следующие виды киберпреступлений:

распространение вирусного программного обеспечения;

кража конфиденциальной информации пользователя;

хищение продуктов интеллектуальной деятельности других людей;

взлом чужих аккаунтов в социальных сетях;

распространение ложной информации, клевета;

разжигание межэтнического конфликта или межрелигиозной вражды; незаконные операции с банковскими пластиковыми картами (реквизитами карты);

Интернет-мошенничество на рынке ценных бумаг;

финансовые пирамиды в Интернете;

преступления, связанные с мобильной связью;

иные преступления в сфере электронной коммерции.[77]

В Узбекистане приняты 17 законодательных актов, касающихся сферы кибербезопасности, 9 указов и постановлений Президента Республики Узбекистан, 14 постановлений Кабинета Министров, а также соответствующие нормативы и множество межведомственных нормативно-правовых актов.

Узбекистан занял 70-е место в рейтинге глобальной кибербезопасности 2020 года, в который входят 194 страны. Среди этих направлений Узбекистан набрал 19,27 балла по внутренним правовым мерам, 13,56 балла по сотрудничеству, 15,68 балла по развитию потенциала, 10,05 балла по организационным мерам и 12,56 балла по техническим мерам. Таким образом, страна получила в общей сложности 71,11 балла. Среди стран Центральной Азии Казахстан занимает 31-е место, Кыргызстан – 92-е, Таджикистан – 138-е, Туркменистан – 144-е место.[78]

Вызывает озабоченность общественности тот факт, что молодежь составляет большинство среди людей, совершающих правонарушения и преступления с помощью информационных технологий. Большинство нарушений в виртуальном мире в нашей республике совершают подростки в возрасте 16-23 лет. Очевидно, что вопрос обеспечения кибербезопасности сегодня имеет как никогда актуальное значение.[79]

В Узбекистане также расширился важный фактор обеспечения стабильности общества – масштаб реализации мер, связанных с обеспечением информационной безопасности со стороны государства. При этом в 2020–2022 годах внешние кибератаки увеличились пропорционально совершенствованию,

---

[76] Боронов Л. Важность интернет-культуры в борьбе с киберпреступностью. [Электронный источник]: https://ictnews.uz/uz/15/05/2018/cybercrime/.

[77] Преступления в сфере информационных технологий и способы защиты от них 15 марта 2021. [Электронный источник]: http://naveconomy.uz/asosiy/yangilikar/155-ahborot-tehnologiya-soasidi-zhinoyatlar-va-ulardan-imoyalanish-usullari.html.

[78] Объявлена позиция Узбекистана в Глобальном рейтинге кибербезопасности. [Электронный источник]: https://bugun.uz/2021/10/12/uzbekistonning-global-kiberhafsizlik-reitingadigi-orni-elon-qilindi/.

[79] Борьба с преступностью в киберпространстве: проблемы и решения. [Электронный источник]: https://iiv.uz/oz/news/kiber-makonda-sodir-etilayan-kinoyatlarga-kurishish-muammalar-va-yechimlar.

расширению и развитию информационно-коммуникационных средств и технологий, связанных с информационной безопасностью.

В 2022 году в день происходило в среднем 67 новых вредоносных атак. Участились также случаи вымогательства, связанные с технической поддержкой (мошенники, предлагающие гражданам «перевести деньги с зарубежных счетов»). Ущерб от этого составил 347 млн. долларов США, данный показатель относительно 2020 года равен 137 процентам.[80] За первое полугодие 2022 года на территории домена «UZ» произошло 83 выявленных атаки. За полугодие произошли 23 атаки на информационную безопасность веб-сайтов госорганов.[81]

В первом квартале 2023 года в сегменте «UZ» сети Интернет Узбекистана было подключено более 110 тысяч доменов веб-сайтов, из них более 28 тысяч работали как активные домены. Из них свыше 14 тысяч являются безопасными, то есть доменами, защищенными SSL-сертификатом. В национальном киберпространстве выявлено 1 650 000 киберугроз, связанных с вредоносными сетями. Из них 2,1 процента составили уязвимые сервисы, 13,1 процента — сервисы, которые следует закрыть, 7,3 процента — сервисы, подверженные DDOS-атакам, 26,4 процента — вредоносное ПО и 51,2 процента — открытые сервисы. На официальных сайтах государственных и хозяйственных органов, расположенных в национальном сегменте сетей Интернет, зафиксировано 249 событий, в результате которых сайты госорганов были неактивны в общей сложности 417 285 минут[82]. Это свидетельствует о том, что количество киберугроз и атак увеличивается с каждым годом.

Постановлением Президента Республики Узбекистан от 2 июня 2023 года «О дополнительных мерах по совершенствованию системы обеспечения кибербезопасности важных объектов информационной инфраструктуры Республики Узбекистан» было утверждено «Положение о порядке обеспечения кибербезопасности важных объектов информационной инфраструктуры Республики Узбекистан» и в соответствии с ним определены формы противодействия кибератакам и меры по их предотвращению[83]. В этом официальном документе также предусмотрено решение вопросов использования и внедрения современных и усовершенствованных технологий в сфере кибербезопасности.

Таким образом, реализованы глубокие реформы в сфере укрепления и совершенствования информационной безопасности – важного направления обеспечения стабильности общества в стране. За этот период в результате создания Государственного унитарного предприятия «Центр

[80] Кибербезопасность 2022: обеспечение цифровой безопасности/. 30.06.2022 . [Электронный источник]: https://review.uz/post /kiberbezopasnost-2022-obespechenie-cifrovoy-bezopasnosti/.
[81] Статистика проверок, по состоянию на I- полугодие 2022 года. [Elektron manba]: https://csec.uz/ru/.
[82] Государственное унитарное предприятие «Центр кибербезопасности». Итоги 1 квартала 2023 года. [Электронный источник]: https://csec.uz/upload/iblock/685/2023%20yil%20I%20chorak%20uchun.pdf.
[83] Постановление Президента Республики Узбекистан «О дополнительных мерах по совершенствованию системы обеспечения кибербезопасности важных объектов информационных структур Республики Узбекистан». 2 июня 2023 г. [Электронный источник]: https://lex.uz/ru/docs/6479190.

кибербезопасности», принятия Закона «О кибербезопасности», обновления и совершенствования технологий информационной безопасности созданы барьеры для кибератак, повышена стабильность и безопасность общества. Также развитие материально-технической базы данной сферы в целях дальнейшего улучшения перспектив информационной безопасности является свидетельством дальнейшего продвижения этой области.

ЗАКЛЮЧЕНИЕ

На основе исследования, проведенного по теме «Национальные и зарубежные аспекты обеспечения стабильности общества в государственной политике информационной безопасности» представлены следующие выводы:

Во-первых, во втором десятилетии XXI века обеспечение информационной безопасности стало основным фактором сохранения общественно-политической стабильности в жизни каждого государства, общества. Сформировались понятия «информационная безопасность», «информационная среда», «безопасность информации», «информационное общество», «информационная безопасность личности», «информационная безопасность общества», «информационная безопасность государства», «коммуникационная политика», «медиа-политика».

Во-вторых, в результате глобализации информационного обмена на международной арене возникла необходимость поиска международных механизмов снижения опасного воздействия информационных потоков в международном сообществе. Впоследствии начала развиваться международно-правовая база информационной безопасности. Сформировано законодательство о глобальном информационном пространстве.

В-третьих, в настоящее время наиболее опасную информационную угрозу представляют в мировом масштабе террористические и экстремические организации. Особенно тревожно, что на их многотысячных сайтах все больше размешаются материалы, призывы, фальцифисированные религиозные материалы, привлекающие молодежь и разрушающие ее сознание.

В-четвертых, с 60-70-х годов XX века в США начался период коренных перемен в сфере информационной безопасности. В результате развития и совершенствования ИКТ, а также широкого внедрения компьютерных сетей в стране возросли различные киберугрозы. Впоследствии задачи укрепления и усиления информационной безопасности были отражены в Законе «О телекоммуникациях», принятом в 1996 году. К 2009 году был разработан «Обзор политики на киберпространстве», в котором не только проанализирована существующая система в сфере кибербезопасности, но и отражен план комплексного развития и трансформации кибербезопасности США. В «Международной стратегии действий в киберпространстве» были воплощены основные принципы, реализуемые в киберпространстве, приоритеты глобальной киберполитики США.

В-пятых, в странах ЕС наиболее совершенно и прогрессивно реализуется государственная политика по информационной безопасности. Сила государственной политики в этой сфере характеризуется тем, что она строится, прежде всего, на основе интересов простых граждан. Основная причина успехов Евросоюза в сфере информационной безопасности обусловлена его приверженностью демократическим принципам.

В-шестых, основным документом, отражающим важную роль ИКТ в Китае, является комплексная концепция национальной безопасности Китая. Основное внимание было уделено Интернету как наименее контролируемому сегменту глобального информационного пространства в сфере социальной, экономической и военной безопасности Китая. В Китае проект «Золотой щит» — Великий китайский файрвол — был создан как часть сложной системы фильтрации, установленной в интернет-сетях страны. В рамках этого проекта серверная система интернет-каналов приобрела возможность фильтрации информации, передаваемой провайдерами и международными сетями. В результате Китай стал одной из сильнейших стран мира в сфере информационной безопасности.

В-седьмых, в целях обеспечения информационной безопасности от возрастающих киберугроз с 2017 года Узбекистан сформировал ряд законов и различных других нормативных актов, основанных на международных стандартах и национальных интересах. Государственная политика в сфере информатизации была ориентирована на создание национальной информационной системы, основанной на современных мировых принципах развития и совершенствования информационных ресурсов, информационных технологий и информационных систем.

Вместе с тем, считаем целесообразным реализовать на практике следующие предложения и рекомендации:

- внесение в Законодательную палату Олий Мажлиса в качестве предложения разработку Концепции обеспечения информационной безопасности с использованием зарубежного опыта в обеспечении стабильности общества, разработке эффективных механизмов предотвращения угроз государственной информационной безопасности;

- обеспечение информационной безопасности в медиапространстве всех сел, районов, городов и районов республики, дальнейшая трансформация единого домена UZ на основе государственно-частного партнерства в борьбе против кибератак, обеспечение современными технологиями и квалифицированными кадрами в борьбе с информационными атаками;

- организация групп по борьбе с интеллектуальными кибератаками в целях противодействия идеологическим воздействиям на сознание человека «кибер» и «гибридных» информационных атак, осуществляемых формированиями и организациями, экстремистскими радикальными идеологиями, использующими информационное пространство для распространения своих деструктивных

политических идей, а также обеспечение вышеуказанных групп необходимыми ИКТ и другими технологическими инструментами;

- создание негосударственных общественных центров «Кибербезопасность» в целях ограждения воспитанников, учащихся и студентов образовательных организаций в составе Министерства дошкольного и школьного образования, Министерства высшего образования, науки и инноваций Республики Узбекистан, а также неорганизованной части молодежи от попадания под влияние информационных атак, реагирования на информационные атаки, нанесения идеологических ударов по распространяемым ими идеям, разработка плана действенных мер по совместному осуществлению социально-профилактической работы в разрезе каждой семьи, махалли и ответственных официальных организаций;

- обеспечение общественно-политической стабильности в обществе путем защиты молодого поколения от информационных атак и медиаполитических угроз, формирования у нее иммунитета против этих угроз, освоения эффективных аспектов прошедшего апробацию практического опыта развитых зарубежных стран в использовании современных информационных и коммуникационных технологий;

- в сотрудничестве Министерства дошкольного и школьного образования Республики Узбекистан, Министерства высшего образования, науки и инноваций, Республиканского центра духовности и просветительства, средств массовой информации, Агентства по делам молодежи, Союза молодежи, общественных объединений и ННО, а также профильных ведомств создание и издание научно-популярных, познавательных мультимедийных видеороликов, брошюр и учебных пособий, учебника «Информационная безопасность» в целях формирования мировоззрения молодежи по вопросам информационной безопасности, с учетом их возраста;

- включение тематики информационной безопасности и «Кибербезопасности» на преподаваемых в высших образовательных учреждениях Узбекистана курсах по дисциплинам «Философия», «Социология», «Политология», «Национальная идея и стратегия социально-экономического развития Узбекистана», наконец, в учебные программы и учебные пособия, по которым ведется обучение в общеобразовательных школах, – «Воспитание», «Основы государства и права».

- недопущение нанесения вреда сознанию подростков и детей радикальными идеями, разработка государственной программы о предотвращении распространения чуждых и деструктивных идей, наносящих вред детской психологии, что предусмотрено Законом «О защите детей от информации, наносящей вред их здоровью», рекомендация ее принятия в парламенте.

SCIENTIFIC COUNCIL ON AWARD OF SCIENTIFIC DEGREES DSc.03/29.12.2022.Ss.21.02 AT TASHKENT STATE UNIVERSITY OF ORIENTAN STUDIES

ANDIJAN STATE UNIVERSITY

ALIEV OLIMBEK AYBEKOVICH

NATIONAL AND FOREIGN ASPECTS OF ENSURING THE SOCIETY STABILITY IN THE POLICY OF STATE INFORMATION SECURITY

23.00.02 – Political institutions, processes and technologies

ABSTRACT
The dissertation for the degree of Doctor of Philosophy (PhD) in Political Science

Tashkent – 2024

The topic of the dissertation for the degree of Doctor of Philosophy (PhD) in political science is registered with the Higher Attestation Commission under the Ministry of Higher Education, Science and Innovation of the Republic of Uzbekistan under No. B2020.4.PhD/Ss237.

The dissertation was completed at Andijan State University.

The dissertation abstract in three languages (Uzbek, Russian, English (summary)) is posted on the website of the Scientific Council (www.namdu.uz) and the Information and Educational Portal "ZiyoNet" (www.ziyonet.uz).

Scientific adviser:	**Kirgizboev Mukimjon** doctor of political sciences, professor
Official opponents:	**Juraev Sayfiddin Akhmatovich** doctor of political sciences, professor
	Yuldashev Anvar Ergashevich doctor of historical sciences, professor
Leading organization:	**Uzbekistan State University of World Languages**

The defense of the dissertation will take place on "___ " _____ 2024 at ___ o'clock at the meeting of the Scientific Council DSc.03/29.04.2022.ss.27.02 for awarding academic degrees at the Tashkent State University of Oriental Studies (Address: 100060, Tashkent city, Amir Temur street, house 20, Tel .: (71) 2333424; -mail: info@tsuos.uz.

The dissertation can be found at the Information Resource Center of the Tashkent State University of Oriental Studies (registered under No. ____). Address: 100060, Tashkent, Amir Temur Street, Building 20. Phone: (99871) 233-34-24; fax: (998971) 233-52-24.

The dissertation abstract was sent out on «___» _____ 2024.
(Protocol at the register №____ of «___» _____ 2024).

D.B. Sayfullayev
Chairman of the Scientific Council awarding of scientific degrees, Doctor of Historical Sciences, Professor

D.I.Madaminova
Scientific Secretary of Scientific Council awarding sciences degrees, Doctor of Political Sciences, Dotsent

E.S. Sultanova
Acting Chairman of the Scientific Seminar at the Scientific Council for awarding academic degrees, Doctor of Political Sciences, Professor

INTRODUCTION (annotation of Doctor of Philosophy (PhD) dissertation)

Relevance and necessity of the dissertation topic. The problem of ensuring information security in the world is manifested as a vital necessity in the implementation and protection of the interests of man, society and the state. One of the threats to information security is the use of information and communication technologies for destructive purposes, a political and social attack against humanity. It is becoming more and more clear that attempts to falsify information for political purposes are damaging the strategically important infrastructures of countries. This leads to the implementation of research on the identification of objective and subjective aspects of information-ideological factors and the development of effective methods, tools and ways to prevent various ideological risks.

Unusual challenges arising in the information space create the need to develop new approaches to the issues of ensuring the stability of the state and society. As a result, the world's advanced scientific research institutes and international think tanks are increasingly interested in researching information security issues. Especially taking into account the impact of information security on national, regional and global security, the development of effective means and measures to combat the threats that threaten it is the object and theoretical-methodological basis of scientific research.

The state policy aimed at ensuring freedom and openness of information, as well as combating information attacks in Uzbekistan, is closely related to the complex situation in the world, the processes of strengthening peace and security. Therefore, the issues of ensuring the stability of society in the state information security policy in Uzbekistan today are included in the "Uzbekistan - 2030" strategy, which is being implemented in Uzbekistan, "creating the necessary conditions for the unhindered use of the Internet global information network, national "Ensure cyber security in the Internet space and increase the literacy of citizens in the use of the Internet" as a goal.

The President of the Republic of Uzbekistan "On the Strategy of Actions for the Further Development of the Republic of Uzbekistan" (February 7, 2017, No. PF-4947), President of the Republic of Uzbekistan "On measures to further improve the field of information technologies and communications" (February 8, 2018), President of the Republic of Uzbekistan Decree on "Development Strategy of New Uzbekistan for 2022-2026" (January 28, 2022, No. PD-60) on exit measures (April 8, 2019, Decree No. F-5465, "Information technologies and communication on measures to improve the system of controlling and protecting the introduction of (November 22, 2018, PD-4024), Decree of the President of the Republic of Uzbekistan "On the establishment of the Information and Mass Communications Agency under the Administration of the President of the Republic of Uzbekistan" (February 2, 2019, PD-4151), the President of the

Republic of Uzbekistan dated May 31, 2023 "Additional measures to improve the system of ensuring cyber security of important information structure objects of the Republic of Uzbekistan about". (May 31, 2023, D-167) to a certain extent serves the implementation of tasks.

Compliance of the research with the priorities of the development of science and technology of the republic. The dissertation was carried out in accordance with the priority direction of the republican science and technology development I. "Formation of a system of innovative ideas and ways of their implementation in the social, legal, economic, cultural, spiritual and educational development of the information society and the democratic state" .

Level of study of the problem. The conceptual and strategic ideas of the President of the Republic of Uzbekistan Sh.M. Mirziyoyev regarding the processes of further improvement of the political technologies of maintaining information security in the stable and consistent development of Uzbekistan and ensuring stability in society form the scientific and methodological basis of the research.

The scientific work of modern researchers can be divided into three groups: The first group - scientists S.K.Ganiyev, Z.T.Khudoykulov, N.B.Nasrullayev, A.E.Yuldashev, I.Islamov, who conducted scientific research on the influence of the state information security policy on the stability of society in Uzbekistan. Scientists such as I.M. Karimov, N.A. Turgunov, Sh. Gulomov, F.B. Botirov, Z.I. Azizova, D. Akbarov, D.S. Muitov, U.R. Kushayev, N.B. Nasrullayev, N. Kasimova and N. Umarova are not exactly in our topic, but close to it. ICT, technological and technical aspects of information security, the influence of information on the spirituality of young people, and aspects related to the culture of information consumption were studied. Sh.Murodova, H.Rajabov and M.Q.Yuldasheva conducted their research from the point of view of political science.

The second group - within the CIS countries, G.A. Atamanov, O.M. Manjueva, M.Yu. Zakharov, Ye.Ye. Perchuk, O.I. Nemkina, Yu.A. Kaptyug, O.M. Sidenova, A.V. Polikarpov, V.F. Nitsevich, Yu.V. Vovendo Sh.K. Rakhimzoda, O.A.Melnikova, A.V.Kurilkin, S.N.Fedorchenko, A.B.Romashkina and others on information warfare, information terrorism, information weapons, legal and psychological mechanisms of information security, the interrelationship of the virtual world and human lifestyle, and the origin of information security problems carried out scientific researches.

The third group - S. Huntington, F. Fukuyama, D. Bell, A. Toffler, M. Kastels, U. Rostow, P. Druker, Dj. Galbraith, V. Inozemsev, F. The works of Webster, A.A. Chernov, R.F. Abdeev, I.S. Melyukhin[84] and others should be noted separately. These scientists founded the theories of information and information security, the problems of information security were studied in the concepts of "post-industrial society" and "information society".

[84] The works of these researchers are given in the references of the main text of the dissertation and in the "List of References".

At the same time, the topics and objects of their research differ sharply from the topic of our dissertation.

The analysis of the level of study of the problem showed that the issues of ensuring the stability of the society in the state information security policy have not been studied as a special dissertation until now. Due to this, in our dissertation, we have chosen the topic of ensuring the stability of society in the state information security policy.

The connection of the dissertation research with the research plans of the higher education institution where the dissertation is carried out. The dissertation was included in the plan of scientific research of Andijan State University and was carried out within the framework of the fundamental project of the "Civil Society Theory" department on the topic "Problems of Civil Society Development".

The aim of the study is to develop proposals and recommendations for the implementation of the national and information security policy of the state in the process of ensuring the stability of the society and its improvement.

Tasks of the research: formation of a description of information security concepts;

Methodological aspects of information security - categorical view and evolution of the international security system, revealing that it is a factor of society's stability;

Analysis of US, European Union and China information security improvement and experience;

Researching the formation and development of the legal basis of the state information security policy in Uzbekistan;

Analysis of cyber threats to the information security of Uzbekistan and the process of combating them;

To scientifically describe the process of further development of the information security system in Uzbekistan and its prospects;

Development of conclusions, suggestions and recommendations regarding the further development and efficiency of information security in Uzbekistan.

The object of the study is to increase the role of the state information policy in strengthening the system of ensuring the stability of society in Uzbekistan.

The subject of the study is the specific features of the state's policy in the field of information security in ensuring the stability of the society, laws and socio-political relations that arise in this process.

Research methods. Research methods such as complex approach, dialectics of scientific knowledge, historicity, logic, analysis and synthesis, comparative analysis, observation, survey were used in the dissertation.

The scientific novelty of the research is as follows:

The fact that a single and universal mechanism for ensuring information security in the world has not been developed, that the state policy aimed at censorship and limiting information flows is not as effective as expected, and that

in order to protect the stability of the state and society from internal and external information attacks, countries focus on creating their own national content. it is proved that it is the basis for using the principle of "information against information".

In the age of information, the traditional society has become an information society, convergence is formed in the case of mutual integration, confidentiality, access to information resources, meta-technologies and the information security of the USA, China and European countries. based on the experience aimed at strengthening, the need to develop the program of the national information network of Uzbekistan (UZNET) registered through the "Uz" domain is justified.

Strengthening the fight against cyber and hybrid crime, which has become the basis of ensuring information security, continuing cyber prevention activities aimed at preventing cyber threats, and preventing the spread of destructive ideas that incite ideological, religious and political enmity. based on its goals, the proposal to establish "Cybersecurity" community centers in neighborhood institutions was proved.

Based on the national information security policy, which aims to ensure compliance with the law in the information field of Uzbekistan, increase the literacy and culture of information use, and protect the population from the influence of foreign and destructive information, prevent cyber terrorism and radicalization. It has been proven that it is necessary to adopt the "Uzbekistan National Information Security Strategy", which serves to improve effective mechanisms for ensuring security.

Practical results of the research. The essence of views on the emergence and improvement of the concept of information security policy was studied, the scientific and theoretical views of the world's leading scientists were analyzed, and the main directions of the organization of information security policy in Uzbekistan were clarified.

It consists of national content developed in order to enrich the content of the measures developed for the information security policy in the conditions of the intellectualization of information threats in Uzbekistan, to protect our national interests in the field of information security.

Reliability of research results. The reliability of the research results is explained by the collections of materials of international and national scientific-practical conferences, articles published in special and foreign journals included in the HAC list, the implementation of conclusions, practical suggestions and recommendations, and the confirmation of the obtained results by authorized organizations.

Scientific and practical significance of research results. The scientific significance of the research results is explained by the fact that it can be useful as a theoretical source for the improvement of scientific teachings on information security policy, researches carried out in the context of ensuring information

security in political institutions, political processes and political technologies, textbooks and methodological manuals. .

Also, the results of the research will enrich the sciences of applied political science, applied journalism, internet journalism, media theory, mass media theory, and information security in a scientific and methodological way.

The practical importance of the dissertation is that in the practice of professional development of professors and teachers who teach the subject "Defense and security" and "Information-psychological security in open systems" in higher education institutions, trainings for the development of their political competence It is intended to be used in the implementation and improvement of political communication models. Also, the dissertation materials serve as educational materials for the subject of "Information Security" for students studying in the social and humanitarian field of Higher Education Institution.

Implementation of research results. Based on the scientific conclusion, recommendations and suggestions developed as a result of the research on the issues of ensuring the stability of society in the state information security policy, the following was achieved:

The fact that a single and universal mechanism for ensuring information security in the world has not been developed, that the state policy aimed at censorship and limiting information flows is not as effective as expected, and that in order to protect the stability of the state and society from internal and external information attacks, countries focus on creating their own national content. from the conclusions about the basis for using the principle of "information against information" of the Law of the Republic of Uzbekistan dated April 15, 2022 "On Cyber Security" No. 764, entitled "Basic Principles of Cyber Security" was used in the development of Article (Reference No. 13 of May 1, 2023 of the Committee on Defense and Security of the Senate of the Oliy Majlis of the Republic of Uzbekistan). As a result, the legal basis for ensuring the priority of protecting the interests of the individual, society and the state in cyberspace has been created.

In the age of information, the traditional society has become an information society, convergence is formed in the case of mutual integration, confidentiality, access to information resources, meta-technologies and the information security of the USA, China and European countries. Based on the experience aimed at strengthening, from the conclusions about the need to develop the program of the National Information Network of Uzbekistan (UZNET), which registers through the "Uz" domain, the Decree of the Republic of Uzbekistan dated April 15, 2022 No. 764 "Cybersecurity to was used in the development of Article 4 of the Law entitled "Main principles of ensuring cyber security" (*Deed No. 12 of April 12, 2023 of the Committee on Defense and Security of the Senate of the Oliy Majlis of the Republic of Uzbekistan*). As a result, during the period of modernization and reforms in Uzbekistan, it served to correctly solve the problems related to the formation, dynamics and prospects of the security system and the development of this system.

Strengthening the fight against cyber and hybrid crime, which has become the basis of ensuring information security, continuing cyber prevention activities aimed at preventing cyber threats, and preventing the spread of destructive ideas that incite ideological, religious and political enmity. Based on the goals, proposals for the establishment of "Cybersecurity" community centers in local institutions, the President of the Republic of Uzbekistan on May 3, 2019 "Additional measures to increase the effectiveness of spiritual and educational work" about" "Measures to further increase the effectiveness of spiritual and educational work in the Republic of Uzbekistan, to increase the intellectual potential and worldview of the population, to strengthen their ideological immunity" developed in accordance with the decision PD-4307 "The complex geopolitical and g "Information pest" is defined in paragraph III, "in-depth coverage of the content and essence of ideological and ideological processes, activities related to effective ideological struggle against terrorism, religious extremism, fanaticism, separatism, human trafficking, "mass culture" and other threats" ” project, within which it was used to ensure the execution of tasks dedicated to "strengthening the ideological immunity of the population, especially young people, against biased information on Internet sites and social networks and helping the public to form a true opinion about certain situations" (*Uzbekistan Act No. 228 of June 19, 2023 of the Center for Social and Spiritual Research under the Spirituality and Enlightenment Center of the Republic of Kazakhstan*). As a result, it served to develop modern propaganda technologies to ensure that young people have in-depth knowledge about the content and essence of the information security policy, which is carried out on the basis of the development strategy of New Uzbekistan.

Based on the national information security policy, which aims to ensure compliance with the law in the information field of Uzbekistan, increase the literacy and culture of information use, and protect the population from the influence of foreign and destructive information, prevent cyber terrorism and radicalization. from the conclusions related to the need to adopt the "Uzbekistan National Information Security Strategy", which serves to improve the effective mechanisms for ensuring security, "In the development strategy of New Uzbekistan for 2022-2026, until October 2022, "2023- "The main directions of ensuring the cyber security of the Internet space of the UZ domain zone, as well as electronic government, energy, digital economy systems and used in the development of a program of measures aimed at ensuring the implementation of complex tasks related to the protection of other areas related to important information infrastructure (*deed of the Andijan branch of the Youth Affairs Agency dated November 18, 2022*). As a result, it served to increase the political knowledge, moral-educational, legal and political culture of the employees and young people working in the youth agency system regarding information security, cybercrime, cyberterrorism, and the effectiveness of youth work.

Approval of research results. The results of this research were presented in the form of lectures at 3 international and 8 national scientific-practical conferences and were approved.

Publication of research results. A total of 18 scientific works on the subject of the dissertation, including 7 articles in scientific publications recommended to be published by the Higher Attestation Commission of the Republic of Uzbekistan, including 3 republican and 4 foreign journals.

The structure and scope of the dissertation. The dissertation consists of an introduction, three chapters, nine paragraphs, a conclusion and a list of references. The volume of the dissertation is 166 pages.

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

I бўлим (I част; I part)

1. Aliyev O.A. O‘zbekistonda axborot xavfsizligi siyosatining huquqiy asoslarini shakllanishi va rivojlanishi // SamDU ilmiy tadqiqotlar axborotnomasi. – Samarqand, 2023. – № 2. – B. 21-29 (23.00.00; № 5).
2. Aliyev O.A. Axborot xavfsizligi: kibertahdidlar va ularga qarshi kurash choralari // Ta’lim, fan va innovatsiya. – Toshkent, 2023. – №1. – B. 127-130 (www.esijournal.uz ISSN: 2181-8274) (23.00.00; № 26).
3. Aliyev O.A. O‘zbekistonda axborot xavfsizligini yanada rivojlantirish jarayoni va uning istiqbollari // Экономика и социум. – Российская Федерация, № 4 (107) 2023. – B. 1-6 (11.00.00; № 11).
4. Aliyev O.A. Xalqaro axborot xavfsizligi tizimining shakllanishi va rivojlanishi // NamDU ilmiy axborotnomasi. – Namangan, 2022. № 12. – B. 148-152 (www.journal.namdu.uz ISSN: 2181-0427).
5. Aliyev O.A. Information security policiy and the process of combating cybercrime in Uzbekistan // JOURNALNX A Multidisciplinary Peer Reviewed. ... (USA), 2020. – № 6 (9). – P. 207-210 (JournalNX Septermber 2020 Full PDF.pdf 1 Request PDF (researchgate.net) (ISSN: 2581-4230. ID 20151756. Impact Factor 7.223.).
6. Aliyev O.A. Improvement of the US State Information Security Policy // Spanish jurnal of innovation. – Ispaniya, 2022. – № 8. – P. 98-108 http://siii.indexedresearch.org/index.php/siii/arti cle/view/550/699) (DOI:... ISSN: 2792-8268).
7. Aliyev O.A. Us government information security policy development process // International Journal of Social Science & Interdisciplinary Research. ... (...), 2023. – № 12 (1). – P. 107-116. Impact Factor: 7.429 (DOI:... ISSN: 2777-3630).
8. Aliyev O.A. Aholining kam ta’minlanganlik darajasini pasaytirish hamda oziq-ovqat xavfsizligini mustahkamlashda aholi ro’yxati ma’lumotlaridan foydalanish / Международная конференция Академических наук. – Novosibirsk. (RF). – August 20, 2021. – C. 38-45. (https://doi.org/10.5281/zenodo. 5226096)
9. Aliyev O.A. Axborot xavfsizligi tushunchasiga doir / “Models and methods in modern science”. Materials of the International scientific-onlayn conference. France. – May 25, 2022. – P. 56-62. (https://doi.org/ 10.5281/zenodo.6585584)
10. Aliyev O.A. Ikki palatali parlament sharoitida qonunchilik jarayoni / “Qonun ustuvorligi – hayotimizning asosiy me’zoni” mavzusidagi Respublika

olimlari huquqshunoslari va jamoatchiligi ilmiy-amaliy konferensiyasi materallari. – Toshkent, 2008. – B. 94-96.

II бўлим (II часть; part II)

11. Aliyev O.A. Axborot xavfsizligini ta’minlash muhim vazifa / “Yangi O‘zbekiston - yangi renessans sari!” mavzusidagi Respublika ilmiy-amaliy konferensiya materiallari. – Toshkent, 2021. – B. 276-278.

12. Aliyev O.A. Axborot xavfsizlgi siyosati – inson taraqqiyoti omili sifatida / Materials of the International scientific-onlayn conference on “Innovative achievements in science – 2020”. Ferghana (Uzb), 2020. – S. 416-418.

13. Aliyev O.A. Axborot xavfsizligining inson taraqqiyotidagi o‘rni / “Ilm-fan va ta’limda innovatsion yondashuvlar, muammolar, taklif va yechimlari” mavzusidagi 4-sonli Respublika ko‘p tarmoqli ilmiy-onlayn konferensiyasi materiallari. – Toshkent, 2020-yil 30-sentabr. – B. 47-49. (ISSN (E)-2181-1334).

14. Aliyev O.A. Axborotlashtirish sohasidagi davlat siyosati / “O‘zbekistonda ilm-fan va ta’lim” mavzusidagi konferensiya to`plami. № 3. 11-qism. – Qo‘qon. 26-may 2020-yil. – B.337-339. (http://www.academiascience.uz/)

15. Aliyev O.A. Internet tarmog`i milliy segmentida axborot xavfsizligi / “O`zbekistonda ilm-fan va ta’lim” mavzusidagi konferensiya to`plami. № 3. 11-qism. – Qo‘qon. 26-may 2020-yil. – B.340-341. (http://www.academiascience.uz/)

16. Aliyev O.A. Biznes va hukumatlarga qarshi kiberhujumlar miqyosini kuchayishiga qarshi kurash / “O‘zbekistonda ilm-fan va ta’lim” mavzusidagi konferensiya to`plami. № 3. 11-qism. – Qo‘qon. 26-may 2020-yil. – B. 342-346. (http://oac.dsmi-qf.uz).

17. Aliyev O.A. Davlat axborot xavfsizligi siyosatida jamiyat barqarorligini ta`minlash masalalari / “Zamonaviy dunyoda ijtimoiy fanlar: nazariy va amaliy izlanishlar” nomli 1-son ilmiy, masofaviy, onlayn konferensiyasi. – Toshkent, 2021-yil 20-avgust. – B. 54-57. (doi.org/10.5281 / zenodo.5254692)

18. Aliyev O.A. Axborot xavfsizligini ta’minlash – muhim vazifa / “Yangi O`zbekiston – yangi Renessans sari!” mavzusidagi Respublika ilmiy-amaliy konferensiya mateiallari. – Toshkent: Zarqaynar, 2021. – B. 276-278.

Avtoreferat «Sharqshunoslik. Востоковедение. Oriental Studies» jurnali tahririyatida tahrirdan o‘tkazilib, o‘zbek, rus va ingliz tillaridagi matnlar o‘zaro muvofiqlashtirildi.

Bosishga ruxsat etildi: 25-oktabr 2024-yil.
Bichimi 60x45 $^{1}/_{8}$. «Times New Roman» garnitura raqamli bosma usulida bosildi.
Shartli bosma tabog‘i 4. Adadi 100 nusxa. Buyurtma _____.

O‘zbekiston Respublikasi IIV Akademiyasi,
100197, Toshkent shahri, Intizor ko‘chasi, 68.

«AKADEMIYA NOSHIRLIK MARKAZI» DUK