MARKAZIY OSIYO MINTAQASIDA KIBERXAVFSIZLIK

qoidalar, bosqichlar va mexanizmlar

O'ZBEKISTON RESPUBLIKASI OLIY TA'LIM,
FAN VA INNOVATSIYALAR VAZIRLIGI

MIRZO ULUG'BEK NOMIDAGI
O'ZBEKISTON MILLIY UNIVERSITETI

BO'TAYEV USMONJON XAYRULLAYEVICH
TURDIYEV UYG'UN RAHMATULLAYEVICH

MARKAZIY OSIYO MINTAQASIDA KIBERXAVFSIZLIK

qoidalar, bosqichlar va mexanizmlar

MONOGRAFIYA

TOSHKENT – 2024

UDK: 004.056(58)
KBK: 32.811.4(54)
B 96

Bo‘tayev U.X., Turdiyev U.R.
Markaziy Osiyo mintaqasida kiberxavfsizlik: qoidalar, bosqichlar va mexanizmlar [Matn] Monografiya / Bo‘tayev U.X., Turdiyev U.R.. – Toshkent: “Invest book” nashriyoti, 2024.– 120 b.

Taqrizchilar:

Jurayev Sayfiddin Axmatovich – Toshkent davlat Sharqshunoslik universiteti professori, siyosiy fanlar doktori

Umarov Xayrulla Payzullayevich – O‘zbekiston Milliy universiteti Siyosatshunoslik kafedrasi dotsenti, siyosiy fanlar nomzodi

Ushbu monografiyada kiberxavfsizlik tushunchasi mazmuni, uning ijtimoiy-siyosiy jihatlarining nazariy-konseptual asoslari tahlil etilgan. Shuningdek, monografiyada Markaziy Osiyo mintaqasida kiberxavfsizlikni ta’minlashning ijtimoiy-siyosiy asoslari o‘rganilgan. Tadqiqotda kibermakonda shaxs, jamiyat va davlat manfaatlarini tashqi va ichki tahdidlardan himoya qilishdagi ustuvor vazifalar yoritib berilgan.

Monografiyada keltirilgan xulosa va tavsiyalardan siyosatshunoslik, xalqaro munosabatlar va tizimli tahlil, huquqshunoslik, milliy g‘oya va ma’naviyat asoslari va huquq ta’limi yo‘nalishi talabalari, magistrlar hamda tadqiqotchilar foydalanishi uchun mo‘ljallangan.

Monografiya Mirzo Ulug‘bek nomidagi O‘zbekiston Milliy universitetining Ilmiy-texnikaviy kengashining 2023-yil 24-noyabr 11-son majlis bayonnomasi bilan muhokama qilinib, nashrga tavsiya etilgan.

ISBN 978-9910-9276-6-9

KIRISH

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

Markaziy Osiyo mintaqasida kiberxavfsizlikning ijtimoiy-siyosiy asoslarini shakllantirish, davlatlararo milliy-hududiy, milliy-madaniy aloqadorlikni saqlab qolishning fundamental asoslarini yaratishga qaratilgan kibermakonda turli xavf va tahdidlarga qarshi kurashuvchi immunitetni shakllantirish orqali inson, jamiyat va davlat o‘zining xavfsizligini ta’minlab borishi, geosiyosiy makonda kuchlar muvozanatining izdan chiqishi, beqaror va xavfli tahdidlarning yuzaga kelishining oldini olishga qaratilgan salmoqli ilmiy izlanishlar amalga oshirilmoqda. Amalga oshirilayotgan tadqiqotlarda kiberxavfsizlikni davlat tomonidan tartibga solish, huquqiy, tashkiliy, ilmiy-texnik va me’yoriy uslubiy ta’minot tizimini takomillashtirish, axborot tizimlari va resurslarining yaxlitligini ta’minlash, jumladan, Markaziy Osiyo mintaqasida kiberxavf va xatar omillarini aniqlash, ularning oldini olish va bartaraf etish mexanizmlarini hamda xavfsizlik sohasi istiqbolini

aniq prognozlash, transchegaraviy tahdidlarning kuchayishi sharoitida xavfsizlik sohasida mintaqaviy institutlar, norma va qoidalar ijrosining samaradorligini oshirish dolzarb ahamiyat kasb etmoqda.

O'zbekistonda amalga oshirilayotgan keng qamrovli islohotlar sharoitida axborot sohasida davlat siyosatining isloh etish, sohaga oid normativ-huquqiy bazani tubdan takomillashuviga, mintaqaviy va xalqaro darajada kiberhujumlarga qarshi javob beruvchi xavfsiz makonni qaror toptirish kabilarga alohida e'tibor qaratilmoqda. "O'zbekiston o'zining tashqi siyosatida Markaziy Osiyo mintaqasiga ustuvor ahamiyat qaratmoqda. Bu – har tomonlama chuqur o'ylab tanlangan yo'ldir. Markaziy Osiyoning qoq markazida joylashgan O'zbekiston ushbu mintaqa barqarorlik, izchil taraqqiyot va yaxshi qo'shnichilik hududiga aylanishidan bevosita manfaatdordir".[1] Markaziy Osiyo davlatlarida milliy davlatchilikni mustahkamlash, xavfsizlik tizimini rivojlantirishning siyosiy, tarixiy, g'oyaviy-mafkuraviy negizlari, mintaqaviy xavfsizlikni ta'minlashda O'zbekistonning tashabbusi dolzarb vazifalar sirasiga kiradi.

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

"Kiberxavfsizlik", "kibermakon", "kiberterrorizm va ekstremizm"ga oid bo'lgan nazariy ilmiy-tadqiqotlar va asarlar

[1] Mirziyoyev Sh.M. Xalqimizning roziligi bizning faoliyatimizga berilgan eng oliy bahodir. 2-jild . –T.: "O'zbekiston", 2018. – B.248.

keng ko'lamli bo'lib, ular masalaning u yoki bu jihatlarini qamrab oladi. Bunday ilmiy-tadqiqotlarni uch guruhga ajratish mumkin:

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

– **ikkinchi guruhga** Y.Primakov, V.Gumelyov, V.Fedotova, V.Kolpakov, A.Nisanbayev, A.Guseynova, Y.Agoshkovoy, N.Gubanov, B. Isayev, V.Belolikov[3] kabi olimlarning ishlari kiradi. Mazkur tadqiqotchilar tomonidan global o'zgarishlar sharoitida partiyaviy tizimlarni yangi qarashlar asosida yangicha kontekstda tahlil etilib, yoritib berilgan. Yuqorida qayd etilgan xorijiy

[2] Эйзенштад Ш. Парадокс демократических режимов: хрупкость и изменяемость// Ж.Полис. – 2002; Альмонд Г. Сравнительная политология: концепция развития. – Москва, 1997; Истон Д. Системный анализ политической жизни. – Москва, 1997; Арон Р. Демократия и тоталитаризм. – М., 1993; Парсонс Т. Система современных обществ. – М., 1998; Даль Р. О Демократии. – М.: "Аспект Пресс", 2000; Тойнби А., Икеды Д. Избери жизнь. – М.: 2008; Эдвард В.С. Ориентализм. Западные концепции Востока. – СПб.: "Русский Мир", 2006. – С.637.

3 Примаков Е.М. Ближний Восток на сцене и за кулисами. – М., 2012; Гумилёв Л.Н. Этногенез и биосфера Земли. – М., 2010; Федотова В.Г., Колпаков А.В., Федотова Н.Н. Глобальный капитализм: три трансформации (Социально-философский анализ общества и экономики) – М., 2010; Нысанбаев А. Философия возвращения: опыт казахстанской философии // Вопросы философии, №7 2013; Гусейнов А.А. О чём говорим, когда мы говорим о диалоге цивилизации // Международная жизнь, №3, 2008; Агошкова Е. Категория «система» в современном мышлении // Вопросы философии №4, 2009; Губанов Н.И. Субъективная реальность и пространства // Вопросы философии, №3, 2015; Кокошин А.А. Проблемы обеспечения стратегической стабильности // Социс №3, 2015; Ваджра А. Мифология Украинское идеология. – М.: «Яуза пресс», 2015; Касавин И.Т. Философия науки: политический поворот // Вестник Российской Академии наук. 2015. №12; Громыко А.А. Россия, США, Малая Европа: конкуренция за лидерство в мире полицентричности // Вестник Российской Академии наук, №2, 2016; Петухов В.В. Российская трансформация и общественная мораль//Социс, №12, 2015; Поликарпова Е.А. Понятие «Oriental despotism» как часть европацентризма // История государства и права, №3, 2016; Исаев И.А. Граница и государство в пранстранство. История государства и права, №2, 2016; Исаев И.А. Государство и нация в пространстве // История государства и права, №3, 2016; Иванов С. «Исламское государство» против ислам // Международная жизнь, №3, 2016; Веремчук В.И., Крутилин Д.С. Религиозная ситуация в вооруженных силах// Социс, №4, 2016.

tadqiqotlar fundamental xususiyatga ega bo'lib, tadqiqotda nazariy muammolarning yechimini topishda alohida ahamiyat kasb etadi;

– **uchinchi guruh,** I.Ergashev, S.Atamuratov, R.Jumayev, S.Jo'rayev, Sh.Paxrutdinov, A.Mo'minov, R.Alimov, S.Saidolimov, J.Mavlonov, O.Sirojov, I.Boboqulov, X.Umarov, U.Bo'tayev, O.Allyorov, Z.O'lmasxo'jayev[4] va boshqa tadqiqotchilar milliy manfaatlarni ta'minlashda xavfsizlik va barqarorlik masalasi, dinning siyosiylashuvi, xalqaro terrorizmning huquqiy, siyosiy va falsafiy tahlili hamda davlat va jamiyatni rivojlantirishda AKT ning roli va ahamiyati bilan bog'liq jihatlarni ochib bergan.

[4] Ergashev I. Milliy g'oya va rahbar mas'uliyati. – T.: "Akademiya", 2007; Otamurodov S. "Globallashuv: millatni asrash mas'uliyati". – T., 2018. – B.148; Jumayev R. Davlat va jamiyat: demokratlashtirish yo'lida. – T.: "Sharq", 1998; Жўраев С. Восток запад новое измерение: единая Центральная Азия связаюущее звено// Wschodnioeuropejskie Czasopismo Naukowe (East European Scientific journal) №8 (60), 2020. – С.65–68; Paxrutdinov Sh. Barqaror taraqqiyot va rahbar mas'uliyati. – T.: "Akademiya", 2011; Mo'minov A. Ijtimoiy-iqtisodiy xavfsizlik. O'quv qo'llanma. – T.: "Universitet", 2017; Алимов Р. Проблемы формирования новой архитектуры региональной безопасности в условиях глобализации (на примере Центральной Азии): Автореф. дисс. док. полит. наук. – Ташкент: УМЕД, 2006; Саидолимов С. Проблемы обеспечения безопасности в Центральной Азии. – Т.: "Академия", 2003; Мавлонов Ж. Концептуальные основы исследования демократии и гражданского общества на Востоке // Ж. Credo New, 2015, №2 (82); Sirojov O. Markaziy Osiyodagi chegara muammolari va ularni hal etish imkoniyatlari // "Oriental Journal of History. Politics and Law", 2023, №03; Boboqulov I., Umarov X. Xavfsizlik asoslari. O'quv qo'llanma. – T.: JIDU, 2011; Bo'tayev U. O'zbekiston jamiyati siyosiy tizimining milliy manfaatlarni ta'minlashdagi dinamikasi mavzusidagi (s.f.d. ilmiy darajasini olish uchun dissertatsiya). – T., 2022; Allayorov O. O'zbekiston barqaror taraqqiyotini ta'minlashda internet texnologiyalaridan samarali foydalanish mexanizmlari mavzusidagi (s.f.f.d. ilmiy darajasini olish uchun yozilgan dessertatsiya avtoreferati). – T., 2019; O'lmasxo'jayev Z. Globallashuv sharoitida shaxs ijtimoiy-siyosiy dunyoqarashining shakllanishiga ijtimoiy tarmoqlarning ta'siri mavzusidagi (s.f.f.d. ilmiy darajasini olish uchun yozilgan dessertatsiya avtoreferati). – T.. 2023;

I BOB. MARKAZIY OSIYODA KIBERXAVFSIZLIKNI TADQIQ ETISHNING NAZARIY-METODOLOGIK ASOSLARI

Bugun jahon hamjamiyati oldida turgan ulkan muammolardan biri butun insoniyatni xavotirga solayotgan kiberhujumlar natijasida vujudga kelayotgan diniy ekstremizm va terrorizm tahdidlari bo'lib turibdi. Bu esa, globallashuv vositalaridan kuch olgan bu tahdidlar kundan-kunga avj olib, kuchayib borishiga sabab bo'lmoqda. Dunyoning ko'plab mamlakatlari, mintaqalarida diniy ekstremizm va terrorizm oqibatida qonli to'qnashuvlar va ashaddiy xunrezliklardan yuz minglab odamlar qurbon bo'lmoqda. Natijada tinchlikni ta'minlash uchun ana shu illatlarga qarshi profilaktik ishlar olib borish zarurati tobora katta ahamiyat kasb etmoqda. Xususan, hozirgi vaqtda ekstremizm va terrorizm xalqaro xavfsizlikka, shu jumladan, Markaziy Osiyoda asosiy tahdidlardan biri bo'lib qolmoqda. Ekstremizm va terrorizm xavfi hamda tahdidlariga qarshi kurashish O'zbekiston Respublikasi uchun birinchi navbatdagi vazifalardan biri bo'lib, mintaqa davlatlari va xalqaro hamjamiyatning sa'y-harakatlarini birlashtirishni taqozo etadi. O'zbekiston Respublikasi har tomonlama o'ylangan tinchliksevar, pragmatik va izchil tashqi siyosatni olib borib, ekstremizm va terrorizmning umumiy tahdidlariga qarshi kurashishda barcha davlatlar bilan teng huquqli va o'zaro manfaatli hamkorlik uchun ochiqdir. Mana shu ochiqlik natijasini ilmiy jihatdan o'rganish mamlakatimiz ilm-fani oldida turgan dolzarb muammo. Shu sababli ham mazkur bobning "Markaziy Osiyo mintaqasida kiberxavfsizlikni tadqiq etishning nazariy-metodologik asoslari" deb nomlanishi hamda uning tarkibiy qismi sifatida "Kiberxavfsizlik tushunchasi va uning ijtimoiy-siyosiy talqini"ni, "Kiberxavfsizlikni ta'minlashning rivojlanish bosqichlari"ni hamda "Markaziy Osiyo kiberxavfsizligi tizimi va uning o'ziga xos xususiyatlari"ni tahliliga bag'ishlangan.

1.1. Kiberxavfsizlik tushunchasi va uning ijtimoiy-siyosiy talqini

Bugun "Siyosiy muhitda kuch emas, balki axborot omili tobora katta ahamiyat kasb eta boshladi. Tashqi siyosiy muvaffaqiyatlar nafaqat iqtisodiy va harbiy qudrat bilan, balki jahonda kechayotgan asosiy axborot va madaniy jarayonlar ustidan nazoratni o'rnatishga qaratilgan demokratiya dasturlari va ommaviy demokratiya muvaffaqiyatlari bilan belgilanadi".[5] Darhaqiqat, bugun axborot har bir davlatning "yumshoq kuch"iga aylanib borayotgan bir sharoitda davlatlar o'zlarining axborot xavfsizligini ta'minlashning nazariy-amaliy va konseptual asoslarini yaratishga zaruriyat sezmoqda. Nazariy jihatdan quyidagi holatlar axborot xavfsizligi konseptual modelining komponentlari bo'lishi mumkin. Bularga tahdid obyektlari, tahdidlar, tahdid manbalari, dushman tomonidan uyushtiriladigan tahdid maqsadlari, axborot manbalari, noqonuniy yo'llar orqali maxfiy axborotlarni olish (usullari), axborot muhofazasi yo'nalishlari, axborot himoyalash usullari hamda axborotni himoyalash vositalari.[6] Biz bularni umumiy ma'noda axborot xavfsizligining konseptual modeli deb hisoblasak, bu komponentlarning har biri yangicha ko'rinishda va yangi shaklda paradigma sifatida ilm-fanga kirib kelmoqda.

Kiberhujumlar nafaqat axborotlarga nisbatan, balki rivojlangan davlatlarni geosiyosiy va geoiqtisodiy jihatdan birlashtirdi, desak ham mubolag'a bo'lmaydi. Biz bunga 2008-yilda RF ning kiberhujumlari, o'sha yilning iyul oyida Gruziyaning internet-infratuzilmasining buzishi, 2012-yilda Isroil va AQSh Eronning yadroviy dasturini buzishga urinishi yoki Eronning Pentagonga hujumlarini aytishimiz mumkin.[7]

Ma'lumki, 2020-yili ichki axborot xavfsizligi bozori 25 foizga o'sdi.[8] Boshqacha aytganda, bu o'sishning uchta sababi bor.

[5] Boboqulov I.I., Umarov X.P. Xavfsizlik asoslari. – Toshkent: 2011. – B.83.

[6] O'sha manba. – B.88-89.

[7] Блэквилл Р., Харрис Дж. "Война иными средствами" Геоэкономика и искусство управления государством. Издание на русском языке AST Publishers. 2017. – С.105.

[8] Кибербезопасность 2020–2021. https://www.ptsecurity.com/

Birinchidan, axborot xavfsizligini o'rganishga bo'lgan ilmiy ehtiyoj, ikkinchidan, axborot xavfsizligini tobora dolzarblashib borishi asosida yangi tahdidlar va ularning sonini o'sishi natijasida kiberjinoyatchilik faoliyatining yildan-yilga rivojlanishi. Shunga ko'ra, bugun xalqaro munosabatlarda COVID-9 pandemiyasining kuchayishi oqibatida kiberxavfsizlik bozorida davlatlar, kompaniyalar hamda xalqaro darajadagi TMK alohida o'z hamkorliklari va bizneslarini alohida tavakkalchilikka asoslanib olib borishdan xavotir hissini kuchaytirdi. Ya'ni pandemiya sharotida biznes vakillari, davlat xizmatchilarining masofaviy ish tizimiga o'tishi, banklardagi pullarning muzlatilishi oqibatida kiberjinoyatlarning rivojlanishi avj oldi. Dunyo bo'ylab internetdan foydalanish mumkin bo'lgan korporativ xizmatlarning zaif tomonlariga nisbatan hujumlar soni oshish ko'paydi. Natijada davlat va xususiy sektorlarning dasturiy ta'minotidagi zaifliklar va kamchiliklarga nisbatan hujumlar uyushtirish 2020-yilga kelib 30 foizgacha (birinchi chorakda 9% ni tashkil qilgan) o'sishiga olib keldi. Bu kiberjinoyatchilarning davlat tashkilotchilardan tortib – kompaniyalarning tarmoqlaridagi kiber josuslikkacha bo'lgan masofani egalladi. Bu esa, bugunga kelib kiber xavfsizlik bozorida xavfsiz muhitni yaratishning trend darajasiga olib kelishi bilan birga ilm-fan oldida ham yangi muammolar, konsepsiyalarni yaratish zaruriyatini yuzaga keltirdi. Shundan kelib chiqib, kiberxavfsizlik tushunchasining konseptual mazmuniga chuqurroq e'tibor qaratish joizdir.

Zamonaviy siyosiy-harbiy fanlarga "kiberxavfsizlik", "kibermakon"[9], "kibermadaniyat"[10], "Proxy war", "gibrid urushlar"

[9] Bu tushuncha yozuvchi Uilyam Gibson tomonidan 1984-yili "Cyberspace " ("Kibermakon") deb nomlangan trilogiyaning birinchi romani "Neuromancer" ("Neyromant") chop etilishi bilan bog'liq. U dunyoning barcha kompyuterlaridagi elektron ma'lumotlar aylanib yuradigan virtual makonni ta'riflaydi. Qarang: Axborot kommunikatsiya texnologiyalari izohli lug'ati. BMTTD ning O'zbekistondagi vakolatxonasi, 2010. – B.573.

[10] Madaniyatni rivojlantirishdagi texnokrat yangi yo'nalish. U kompyuter o'yinlarining imkoniyatlari va virtual voqelik texnologiyalarini ishlatishga asoslangan. O'sha manba.

kabi kategoriyalar kirib keldi. Bu kategoriyalarni tushunishga bo'lgan talabning ortishi davlat va jamiyatning nazariy va amaliy ehtiyojlari bilan bog'liq. Chunki yangi bir sharoitda kiberxavfsizlik muammosi bo'yicha qaror qabul qilishga bo'lgan zaruriy ehtiyoj mazkur masalalarni chuqurroq o'rganishni taqozo etadi.

"Kiberxavfsizlik" kategoriya sifatida manbalarda turlicha talqin etiladi. Jumladan, kiberxavfsizlik – bu axborot tizimlari, tarmoqlari, dasturlarini raqamli hujumlardan himoyalashga qaratilgan faoliyatdir. Odatda bunday hujumlardan maqsad maxfiy ma'lumotlarni qo'lga kiritish, ularni o'zgartirish yoki yo'qotish, foydalanuvchilardan pul talab qilish yoki biznes jarayonlarini izdan chiqarishdan iborat.[11] Boshqacha aytganda, kiberxavfsizlik bu – tasodifiy va atayin qilingan axboriy hujumlardan himoyalanish demakdir. U ko'p qirrali faoliyat sohasi bo'lib, unga faqat tizimli va kompleks yondashuv muvaffaqiyat keltirishi mumkin.

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

Texnik nuqtayi nazardan kiberxavfsizlik tizimlarni, tarmoqlarni va dasturlarni raqamli hujumlardan himoyalash amaliyoti tushuniladi.

O'zbekiston Respublikasining Kiberxavfsizlik to'g'risidagi Qonunida kiberxavfsizlik – kibermakonda shaxs, jamiyat va davlat manfaatlarining tashqi va ichki tahdidlardan himoyalanganlik holati deb belgilangan.[12]

Shulardan kelib chiqib aytish mumkinki, kiberxavfsizlik ijtimoiy sohaning ajralmas qismi yoxud shaxsning xavfsizligini ta'minlash

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

[12] O'zbekiston Respublikasining 2022-yil 15-apreldagi Kiberxavfsizlik to'g'risidagi Qonuni.// https://lex.uz/uz/docs/5960604

jarayonida namoyon bo'ladigan tizimli ko'rinish sanaladi. Kiberxavfsizlik sohaviy jihatdan inson xavfsizligi, ma'lumotlar xavfsizligi, jamoat xavfsizligi, faoliyat xavfsiziligidagi ko'rishlarni o'zida mujassamlaydi. Masalan, ijtimoiy jihatdan kiberxavfsizlik "inson xavfsizligi" bilim bilan bog'liq inson xatti-harakatlarini tashkilotlar (masalan, xodim) va shaxsiy hayot sharoitida shaxsiy ma'lumotlarni, shaxsiy hayotni himoya qilishga e'tibor qaratish jarayonida mujassam bo'ladi. Insonning jamiyat bilan bog'liq munosabatlarida, axloqiy munosabatlarida yoxud shaxsiy hayot va ularning bir-biri bilan munosabatlarida aks etadi.

Shundan kelib chiqib aytish mumkinki, bugun kiberxavfsizlikning tahdid turlari sifatida quyidagilarni kiritish mumkin:

Fishing – bu axborot qabul qiluvchilarning xabarlariga o'xshagan yolg'on elektron pochta xabarlarini yuborish tushuniladi. Ushbu jinoyatning maqsadi kredit karta raqamlari va hisobga olish ma'lumotlarining maxfiyligini o'rganish hisoblanadi.

Virus tovlamachilari yoki tarqatuvchilari – foydalanuvchining to'lov to'lash jarayonida kompyuter tizimlariga kirishni blokirovka qilish orqali mablag'larni o'g'irlash tushuniladi.

Zararli dasturiy ta'minot – bu kompyuterga ruxsatsiz kirish yoki zarar yetkazish uchun mo'ljallangan tasturiy ta'minot hisoblanadi.

Ijtimoiy muhandislar – hujumchilar maxfiy ma'lumotlarini oshkor qilish uchun sizni aldash orqali ijtimoiy muhandislardan foydalanadi. Ular sizni pul o'tkazmangiz yoki maxfiy ma'lumotlarga kirishni ta'minlashingizni so'rashlari orqali jonoyatlarni sodir etishlari mumkin.

Veb serverlar – veb dasturlarda ma'lumotlarni ajratib olish va noto'g'ri kodlarni kiritish orqali qilinayotgan hujumlarni ko'rishimiz mumkin. Kiber jinoyatchilar o'zlari rivojlantirayotgan veb serverlar orqali noto'g'ri kodni tarqatadilar. Shuningdek, kodni shifrlash, IPv6: yangi internet protokoli orqali uyujtiriladigan tahdidlarni aytish mumkin.

Kibermakon atamasi – bu tushuncha yozuvchi Uilyam Gibson tomonidan 1984-yili "Cyberspace" ("Kibermakon") deb nomlangan

trilogiyaning birinchi romani "Neuromancer" ("Neyromant") chop etilishi bilan bog'liq. U dunyoning barcha kompyuterlaridagi elektron ma'lumotlar aylanib yuradigan virtual makonni ta'riflaydi.[13] Kibermakon kompyuter tarmoqlari orqali amalga oshiriladigan muloqot maydonini hisoblanib, bu 1990-yildan boshlab keng miqyosda rivojlanib, takomillashib kelmoqda. Ijtimoiy nuqtayi nazardan kibermakon deganimizda – kompyuter tarmog'i orqali bir-biri bilan bog'langan va bir vaqtning o'zida turli geografik nuqtada kesishuvchi har qanday mavjud kompyuterning grafik sifatidagi ma'lumotlariga o'ralashib qolgan kishilar yoki guruhlar jamoasi tushuniladi.

Bugun siyosiy jarayonlarda dinning siyosiylashuvi natijasida kibermakonda din niqobidagi tahdidlar kuchayib bormoqda. Ular din niqobi ostidagi ekstremistik tashkilotlarning saytlarida asosan davlat to'ntarilishi va xunrezlik urushlari haqida diniy rahnamolarning da'vatlariga oid ma'lumotlarni joylaydi. Bu ma'lumotlarni hamda da'vatlar yoshlar ongida kuchli psixologik jihatdan ta'sir ko'rsatish orqali o'zlarining qarmoqlariga ildirib olishga yo'naltirilgan. Masalan, ekstremistik guruhlar tomonidan "Odnoklassniki", "Facebook", "Instagram", "Twitter", "Vkontakte" ijtimoiy tarmoqlarida "Mustafo mujohid" "Abul moviya", "Ansor-ansor", "Abu Ali" kabi o'zlarining soxta profillarini yaratish orqali buzg'unchi, yot g'oyalarni targ'ib qiluvchi da'vatlari bilan yoshlar ongiga ruhiy ta'sir o'tkazib, ularni "jihod" qilish uchun Yaqin Sharq davlatlariga chiqib ketishga chorlamoqda.

Kibermadaniyat – madaniyatni rivojlantirishdagi texnokrat yangi yo'nalish. U kompyuter o'yinlarining imkoniyatlari va virtual voqelik texnologiyalarini ishlatishga asoslangan tushuncha hisoblanadi.[14] Bu atama bugungi global axborot makonida virtual tarmoqdagi ijtimoiy ongga salbiy ta'sir etuvchi, ya'ni vayronkor-buzg'unchi, axloq me'yorlariga to'g'ri kelmaydigan va noxolis

[13] Qarang: Axborot kommunikatsiya texnologiyalari izohli lug'ati. BMTTD ning O'zbekistondagi vakolatxonasi, 2010. – B.573.

[14] Qarang: Axborot kommunikatsiya texnologiyalari izohli lug'ati. BMTTD ning O'zbekistondagi vakolatxonasi, 2010. – B.573.

mazmundagi axborotlardan foydalanishning ongli ravishda cheklanilishi tushuniladi.

Proxy war (ingliz tilidan olingan, vakil yoki vositachilik urushi) – uchinchi tomon donorlarining aralashuvi natijasida resurslardan foydalangan holda jangovar harakatlar orqali o'z maqsadlariga erishish maqsadida, ikki davlat o'rtasidagi mojarolarni saqlab qolish va uni uzaytirish hisoblanadi.[15]

Gibrid urushlar – "Yumshoq kuch" siyosati asosida harbiy kuch va vositalaridan foydalangan holda ta'sir o'tkazish vositasidir. "Gibrid urush" – siyosiy, mafkuraviy va boshqa sohalarda doimiy manipulyatsiya bilan uyg'unlashgan ko'rinishda an'anaviy, tartibsiz va asimmetrik vositalardan foydalanish hisoblanadi.[16]

O'zbekiston Respublikasining 2022-yil 15-aprelida qabul qilingan "Kiberxavfsizlik to'g'risida"gi Qonunida kiberxavfsizlik tushunchasiga oid tushunchalarning mazmuni ochib berilgan.[17] Jumladan, qonunda:

axborotlashtirish obyekti – turli darajadagi va maqsaddagi axborot tizimlari, telekommunikatsiya tarmoqlari, axborotga ishlov berishning texnik vositalari, ushbu vositalar o'rnatilgan va foydalaniladigan xonalar;

kiberjinoyatchilik – axborotni egallash, uni o'zgartirish, yo'q qilish yoki axborot tizimlari va resurslarini ishdan chiqarish maqsadida kibermakonda dasturiy ta'minot va texnik vositalardan foydalanilgan holda amalga oshiriladigan jinoyatlar yig'indisi;

kibermakon – axborot texnologiyalari yordamida yaratilgan virtual muhit;

kibertahdid – kibermakonda shaxs, jamiyat va davlat manfaatlariga tahdid soluvchi shart-sharoitlar va omillar majmuyi;

kiberxavfsizlik – kibermakonda shaxs, jamiyat va davlat manfaatlarining tashqi va ichki tahdidlardan himoyalanganlik holati;

[15] Qarang: Andrew Mumford. Proxy Warfare War and Conflict in the Modern World. Wiley, 2013. – P.13.

[16] Qarang: https://regnum.ru/news/polit/2421809.html

[17] O'zbekiston Respublikasining 2022-yil 15-aprelida qabul qilingan "Kiberxavfsizlik to'g'risida"gi Qonuni.// https://lex.uz/uz/docs/5960604

kiberxavfsizlik hodisasi – kibermakonda axborot tizimlarining ishlashida uzilishlarga va (yoki) ulardagi axborotning ochiqligi, yaxlitligi va undan erkin foydalanilishining buzilishiga olib kelgan hodisa;

kiberxavfsizlik obyekti – axborotning kiberhimoya qilinishini hamda milliy axborot tizimlari va resurslarining kiberxavfsizligini ta'minlashga doir faoliyatda foydalaniladigan axborot tizimlari majmuyi, shu jumladan, muhim axborot infratuzilmasi obyektlari;

kiberxavfsizlik subyekti – milliy axborot resurslariga ega bo'lish, ulardan foydalanish va ularni tasarruf etish bo'yicha elektron axborot xizmatlari ko'rsatish, axborotni himoya qilish hamda kiberxavfsizlik bilan bog'liq muayyan huquqlar va majburiyatlarga ega bo'lgan yuridik shaxs va (yoki) yakka tartibdagi tadbirkor, shu jumladan, muhim axborot infratuzilmasi subyektlari;

kiberhimoya – kiberxavfsizlik hodisalarining oldini olishga, kiberhujumlarni aniqlashga va ulardan himoya qilishga, kiberhujumlarning oqibatlarini bartaraf etishga, telekommunikatsiya tarmoqlari, axborot tizimlari hamda resurslari faoliyatining barqarorligini va ishonchliligini tiklashga qaratilgan huquqiy, tashkiliy, moliyaviy-iqtisodiy, muhandislik-texnik chora-tadbirlar, shuningdek ma'lumotlarni kriptografik va texnik jihatdan himoya qilish chora-tadbirlari majmuyi;

kiberhujum – kibermakonda apparat, apparat-dasturiy va dasturiy vositalardan foydalangan holda qasddan amalga oshiriladigan, kiberxavfsizlikka tahdid soladigan harakat;

muhim axborot infratuzilmasi – muhim strategik va ijtimoiy-iqtisodiy ahamiyatga ega bo'lgan avtomatlashtirilgan boshqaruv tizimlarining, axborot tizimlari hamda tarmoqlar va texnologik jarayonlar resurslarining majmuyi;

muhim axborot infratuzilmasi obyektlari – davlat boshqaruvi va davlat xizmatlari ko'rsatish, mudofaa, davlat xavfsizligi, huquq-tartibotni ta'minlash, yoqilg'i-energetika majmuyi (atom energetikasi), kimyo, neft-kimyo tarmoqlari, metallurgiya, suvdan foydalanish va suv ta'minoti, qishloq xo'jaligi, sog'liqni saqlash, uy-joy kommunal xizmatlar ko'rsatish, bank-moliya tizimi,

transport, axborot-kommunikatsiya texnologiyalari, ekologiya va atrof-muhitni muhofaza qilish, strategik ahamiyatiga ega bo'lgan foydali qazilmalarni qazib olish va qayta ishlash sohasida, ishlab chiqarish sohasida, shuningdek iqtisodiyotning boshqa tarmoqlarida va ijtimoiy sohada qo'llaniladigan axborotlashtirish tizimlari;

muhim axborot infratuzilmasi subyektlari – davlat organlari va tashkilotlari, shuningdek mulk, ijara huquqlari asosida yoki boshqa qonuniy asoslarda muhim axborot infratuzilmasi obyektlariga egalik qiluvchi yuridik shaxslar, shu jumladan, muhim axborot infratuzilmasi obyektlarining ishlashini hamda hamkorligini ta'minlovchi yuridik shaxslar va (yoki) yakka tartibdagi tadbirkorlar.

Kiberjinoyatlarning soni va salmog'i turlicha bo'lganligi sababli ularning turlarini tasniflashda har kim har xil yondashadi. Xususan, Internet firibgarligi moliyaviy ma'lumot yoki bank kartasi ma'lumotlarini o'g'irlash korporativ ma'lumotlarni o'g'irlash va sotish, kibertovlamachilik, kriptodjeking, kiberjosuslik kabi turlarga ega ekanligini, shu sababli ularni ikkita guruhga kompyuterlarning o'ziga qaratilgan kiberjinoyatlar va kompyuterdan foydalanilgan holda amalga oshiriladigan kiberjinoyatlar.[18]

Biz bu borada haqiqatan kiberjinoyatlarning ikkita guruhga ajratish bilan fikrlarga qisman qo'shilish zarur deb hisoblaymiz, sababi kiberjinoyatdan ko'zlangan asosiy maqsad ikkinchi tarafga moddiy va ma'naviy, siyosiy va boshqa turdagi zarar yetkazish hisoblanadi. Bunda kiberjinoyatchi o'zining qabih maqsadiga kibertexnologiyalardan foydalanib, yuqoridagi maqsadiga yetishni ko'zlaydi yoki ikkinchi tarafning kibertexnologiyalarini yo'q qilish orqali uni kuchsizlantirish va shu orqali o'ziga tobe qilishga harakat qiladi, aniqroq aytadigan bo'lsak, kiberqotillik, kibersuitsid, kiberfiribgarlik, kibero'g'rilik, kiberpornografiya, kiberzo'ravonlik, kiberekstremizm va boshqa kiberjinoyatlar orqali kiberjinoyatchi ikkinchi tarafga kibertexnologiyalardan foydalanib jabrlanuvchining axborot-kommunikatsiya texnologiyalarini zararsizlantirishni ko'zlamaydi, balki shaxsni, jamiyatni o'ziga qaratish va tobe qilishga harakat qiladi, kiberterrorizm,

[18] https://www.kaspersky.ru/resource-center/threats/what-is-cybercrime.

kiberagressiya, kompyuter modifikatsiyasi, kompyuter axborotidan qonunga xilof ravishda (ruxsatsiz) foydalanish, kompyuter sabotaji va boshqa kiberjinoyatlarda esa, kiberjinoyatchi ikkinchi tarafning kibertexnologiyalariga zarar keltirish va ularni yo'q qilishni maqsad qilib oladi. "Tadviser" kompaniyasining fikricha, kiberjinoyatlar spam, maqsadli fishing, PDF-hujum, qidiruv tizimini optimallashtirishni zararlash, ishlash qobiliyatini yo'qotish kabi turlarga ega.[19]

Shundan kelib chiqqan holda bugun globallashuv jarayonida yoshlarning internetga ko'p vaqtini sarflashi, hayotining mazmunini AKT orqali deb hisoblashi evaziga kiberxavfsizlik sohasidagi e'tirof etilgan siyosiy tushunchalar bilan birga, unga yonma-yon bo'lgan tushunchalar ijtimoiy hayot sohasiga kirib kelmoqda. Jumladan, **kibersuitsid** hisoblanadi. Ushbu tushuncha kibertexnologiyalar orqali ko'ndirish, aldash yoki boshqa yo'l bilan o'zga shaxsda o'zini o'zi o'ldirish hissini uyg'otish yoki shaxsning o'zini o'zi o'ldirishi nazarda tutiladi.

Navbatdagi kiberxavfsizlik jarayon sifatida tahlil etgan holda unga bevosita va bilvosita aloqador bo'lgan **kiberpornografiya hisoblanadi.** Ushbu tushunchaning ijtimoiy ahamiyati shundaki, pornografik mahsulotni kibertexnologiyalar yordamida tayyorlash, ma'lum bir A yoki B mintaqa hududiga olib kirish yoki olib chiqish, tarqatish, reklama qilish, namoyish etish, foydalanish, targ'ib qilish tushuniladi.

O'rganilgan tadqiqotlarga asoslanib aytish mumkinki, kiberxavfsizlik tushunchasi murakkab tushuncha sifatida qarash kerak ekanligini ko'rsatadi. Xususan, unga yondosh bo'lgan atamalar ham. Bugun ushbu tushunchaga yana bir yondosh atama ham kirib keldiki, ushbu atama ijtimoiy hayot tarzini umuman o'rab olishi natijasida, har bir insondagi qo'rquv, nafrat tuyg'uchini shakllantirib bormoqda. Bu tushuncha **kiberagressiya** deb ataladi. **Kiberagressiya** – kibertexnologiyalar orqali bosqinchilik urushini rejalashtirish yoki unga tayyorgarlik ko'rish, shuningdek shu harakatlarni amalga oshirishga qaratilgan fitnada qatnashishni anglatadi.

[19] Киберпреступность в мире. 2020. http://www.tadviser.ru/index.php

Kibertovlamachilik – jabrlanuvchi yoki uning yaqin kishilariga zo'rlik ishlatish, mulkka shikast yetkazish yoki uni nobud qilish yoxud jabrlanuvchi uchun sir saqlanishi lozim bo'lgan ma'lumotlarni kibertexnologiyalar orqali oshkor qilish bilan qo'rqitib o'zgadan kibertexnologiyalar orqali mulkni yoki mulkiy huquqni topshirishni, mulkiy manfaatlar berishni yoxud mulkiy yo'sindagi harakatlar sodir etishni talab qilish yoxud jabrlanuvchini o'z mulki yoki mulkka bo'lgan huquqini berishga majbur qiladigan sharoitga solib qo'yish hisoblanadi.

Qolaversa, bugun ijtimoiy tarmoqlarda kibero'zlashtirish yoki kiberrastrata qiluvchilar ham paydo bo'lib borayotganligi ham fuqarolarning sha'ni va qadr-qimmatini tushirishga sabab bo'lib bormoqda. Ya'ni bu tushunchalar, aybdorga ishonib topshirilgan yoki uning ixtiyorida bo'lgan o'zganing mulkini kibertexnologiyalar orqali o'zlashtirish, talon-toroj qilishni anglatadi.

Sodir etilgan yoki sodir etilishi rejalashtirilayotgan kiberjinoyatlar haqida aniq tushunchaga ega bo'lish uchun kiberxavfsizlikni turlarga ajratish va ularning mazmun-mohiyatini o'zaro tizimlashtirish maqsadga muvofiqdir. Shuningdek, kiberjinoyatlarning sodir etilish quroli, vositasi bo'lgan axborot-kommunikatsiya texnologiyalarini bugun shu nomda atay olishimiz mumkin. Biroq keyinchalik uni qanday nom bilan aytishimiz mumkin? Bugungi kunda u sohadagi barcha tushunchalarni o'zida qamrab olar, ammo sohaning rivoji ushbu tushunchaning keyinchalik ham o'zgarmasligini hech kim kafolatlay olmaydi. Kiberjinoyatlar kibermuhitda sodir etilishini va barcha axborot-kommunikatsiya texnologiyalarini kiberjinoyatlarning sodir etilish quroli yoki vositasi bo'ladi, deb ayta olmaymiz. Masalan, televideniya yoki radio ham axborot-kommunikatsiya texnologiyasi hisoblanadi. Biroq ulardan foydalanish orqali sodir etilgan jinoyatlarni biz doim ham kiberjinoyatlar deb ayta olmaymiz. Bironta shaxsning jinoyati bilan bog'liq lavhalarni uning yaqinlaridan biri ko'rishi yoki eshitishi orqali ushbu shaxsga yetkazilgan ruhiy zo'riqishni biz jinoyat deb ayta olmaymiz. Sababi bu lavhalarni ko'rsatish orqali lavha tayyorlovchi jinoyatchi deb gumon qilinayotgan shaxsning

yaqiniga ruhiy zo'ravonlik o'tkazishni maqsad qilmagan bo'ladi. Maqsad qilgan taqdirda u kiberzo'ravonlik bo'ladi.[20]

1.2. Kiberxavfsizlikni ta'minlash bosqichlari

Xalqaro tizimda ko'plab davlatlar o'zining kibermudofaa va hujum qobiliyatini oshirish uchun kiberxavfsizlik strategiyasini ilgari sura boshladi va ushbu jarayonlarni davom ettirish uchun bazaviy tuzilmalarni tashkil etdi. 1980-yillar boshida AQSh da dastlabki shaxsiy kompyuterlarni ishlab chiqarish ortidan boshlangan internet-texnologiyalarga asoslangan tijorat sovuq urushdan keyingi davrdagi global miqyosli rivojlanishning ilk xabarchisi bo'ldi. Internetning ommalashuvi va tijoratlashuvidan so'ng, 2000-yillarda mobil telefon texnologiyasi shiddat bilan rivojlanib bordi. Bugungi kunda esa tobora keng tarqalib borayotgan zamonaviy smartfonlar hayotning barcha jabhalariga kirib bordi.

Texnologik rivojlanish bilan parallel ravishda, ayni paytda mamlakatlar "muhim infratuzilma" sifatida ta'riflanuvchi davlat xizmatlarini ko'rsatish tizimlarini tarmoq texnologiyalariga asoslangan innovatsiyalar bilan boshqara boshladilar. Natijada muhim infratuzilmalarning kiberxavfsizligini ta'minlash ularning eng ustuvor vazifalaridan biriga aylandi.

AQSh da axborot-kommunikatsiya texnologiyalarining jadal rivojlanishi natijasida kiberxavfsizlik 1960-yillardan boshlab, to hozirgi kunga qadar bir necha bosqichlarni bosib o'tdi. Xususan:

Birinchi bosqich, 1980-yillarning oxiridan boshlab, 2000-yilga qadar bo'lgan davr hisoblanadi. Ushbu davrning o'ziga xosligi kompyuter texnologiyalari, ularni siyosiy va faol ravishda qo'llash imkonini bergan davr sifatida e'tirof etiladi. Ushbu davrda AKT sohasidagi inqilob jahon iqtisodiyoti, ayrim davlatlar siyosiy tizimi, umuman dunyoning bugungi ko'rinishini o'zgartirayotgan edi. Buning natijasida zamonaviy davlatlarning xarakteri va davlatlararo munosabatlar o'zgara boshlagan edi. Shunday

[20] Anorboyev A.U. Kiberjinoyatchilik, unga qarshi kurashish muammolari va kiberxavfsizlikni ta'minlash istiqbollari. –T., 2020.

sharoitda AKT zamonaviy jamiyatlar transformatsiyasining asosiy omili ekanligi kun tartibiga chiqdi. Natijada AKT globallashuv jarayonining rivojlanishiga olib keldi. Bu jarayonda AQSh ichki va tashqi siyosatda o'zini AKT sohibi sifatidagi maqomini egalladi, deb aytishimiz mumkin. Natijada 1990-yillarning boshidan boshlab AQSh Kongressida kiberxavfsizlik masalasi kun tartibiga chiqdi. Unga oid bo'lgan jarayonlar faol muhokama qilish, shuningdek kiberxavfsizlik faoliyatini tartibga soluvchi strategik hujjatlarni yaratish, uning ijrosi direktivalarini yaratish bo'yicha axborot sohasida davlat xavfsizligiga tahdidlarga qarshi kurashish mexanizmlari mazkur bosqichda ishlab chiqildi.[21] Ushbu rivojlanish bosqichining yana bir xususiyati shunda bo'ldiki, bunda kiberxavfsizlikni AQSh infratuzilmasiga nisbatan turli hujumlar, masalan, Pentagon veb-saytidan o'g'irlashlarga nisbatan xavotir tuyg'usi vujudga kela boshladi. Natijada, AQSh kompaniyalariga, jumladan, Facebook, Twitter va boshqalarga xakerlik hujumlari dunyoning eng yirik kompyuter korporatsiyasi Apple munozaraning boshlanish davri sifatida e'tirof etildi.[22] Natijada AQSh da kiberjinoyatlar masalasi kundan-kunga rivojlanish bosqichiga chiqish holati kuzatildi. Hatto kiberjinoyat dinamik o'sish holatiga chiqishi AQSh Adliya departamenti tomonidan kiberjinoyatlarni 3 ta turga bo'lib klassifikatsiya qilinishiga olib keldi. Unga ko'ra:

– birinchi toifaga subyektiv tomon to'g'ridan-to'g'ri kompyuter yoki kompyuter tarmog'ining ish faoliyatini izdan chiqarish yoki uni buzishga qaratilgan jinoyatlar;

– ikkinchi toifaga kompyuter tizimi va global tarmoq an'anaviy jinoyatlarni sodir etishning vositasi yoxud usuli bo'lgan jinoyatlar;

– uchinchi toifaga kompyuter va Internet tarmog'i boshqa jinoyatlarni sodir etishda asosiy usul bo'lmasa-da, uni sodir etish

[21] Карасев П.А. Новые стратегии США в области кибербезопасности [Электронный ресурс]: URL: http://russiancouncil.ru/analytics-and-comments/analytics/novyestrategii-ssha-v-oblasti-kiberbezopasnosti/(дата обращения: 02.10.2019).

[22] Rogovsky E. Cyber-Washington: Global Ambitions. International Relations. Moscow, 2014. – P.848.

yaqiniga ruhiy zo'ravonlik o'tkazishni maqsad qilmagan bo'ladi. Maqsad qilgan taqdirda u kiberzo'ravonlik bo'ladi.[20]

1.2. Kiberxavfsizlikni ta'minlash bosqichlari

Xalqaro tizimda ko'plab davlatlar o'zining kibermudofaa va hujum qobiliyatini oshirish uchun kiberxavfsizlik strategiyasini ilgari sura boshladi va ushbu jarayonlarni davom ettirish uchun bazaviy tuzilmalarni tashkil etdi. 1980-yillar boshida AQSh da dastlabki shaxsiy kompyuterlarni ishlab chiqarish ortidan boshlangan internet-texnologiyalarga asoslangan tijorat sovuq urushdan keyingi davrdagi global miqyosli rivojlanishning ilk xabarchisi bo'ldi. Internetning ommalashuvi va tijoratlashuvidan so'ng, 2000-yillarda mobil telefon texnologiyasi shiddat bilan rivojlanib bordi. Bugungi kunda esa tobora keng tarqalib borayotgan zamonaviy smartfonlar hayotning barcha jabhalariga kirib bordi.

Texnologik rivojlanish bilan parallel ravishda, ayni paytda mamlakatlar "muhim infratuzilma" sifatida ta'riflanuvchi davlat xizmatlarini ko'rsatish tizimlarini tarmoq texnologiyalariga asoslangan innovatsiyalar bilan boshqara boshladilar. Natijada muhim infratuzilmalarning kiberxavfsizligini ta'minlash ularning eng ustuvor vazifalaridan biriga aylandi.

AQSh da axborot-kommunikatsiya texnologiyalarining jadal rivojlanishi natijasida kiberxavfsizlik 1960-yillardan boshlab, to hozirgi kunga qadar bir necha bosqichlarni bosib o'tdi. Xususan:

Birinchi bosqich, 1980-yillarning oxiridan boshlab, 2000-yilga qadar bo'lgan davr hisoblanadi. Ushbu davrning o'ziga xosligi kompyuter texnologiyalari, ularni siyosiy va faol ravishda qo'llash imkonini bergan davr sifatida e'tirof etiladi. Ushbu davrda AKT sohasidagi inqilob jahon iqtisodiyoti, ayrim davlatlar siyosiy tizimi, umuman dunyoning bugungi ko'rinishini o'zgartirayotgan edi. Buning natijasida zamonaviy davlatlarning xarakteri va davlatlararo munosabatlar o'zgara boshlagan edi. Shunday

[20] Anorboyev A.U. Kiberjinoyatchilik, unga qarshi kurashish muammolari va kiberxavfsizlikni ta'minlash istiqbollari. –T., 2020.

sharoitda AKT zamonaviy jamiyatlar transformatsiyasining asosiy omili ekanligi kun tartibiga chiqdi. Natijada AKT globallashuv jarayonining rivojlanishiga olib keldi. Bu jarayonda AQSh ichki va tashqi siyosatda o'zini AKT sohibi sifatidagi maqomini egalladi, deb aytishimiz mumkin. Natijada 1990-yillarning boshidan boshlab AQSh Kongressida kiberxavfsizlik masalasi kun tartibiga chiqdi. Unga oid bo'lgan jarayonlar faol muhokama qilish, shuningdek kiberxavfsizlik faoliyatini tartibga soluvchi strategik hujjatlarni yaratish, uning ijrosi direktivalarini yaratish bo'yicha axborot sohasida davlat xavfsizligiga tahdidlarga qarshi kurashish mexanizmlari mazkur bosqichda ishlab chiqildi.[21] Ushbu rivojlanish bosqichining yana bir xususiyati shunda bo'ldiki, bunda kiberxavfsizlikni AQSh infratuzilmasiga nisbatan turli hujumlar, masalan, Pentagon veb-saytidan o'g'irlashlarga nisbatan xavotir tuyg'usi vujudga kela boshladi. Natijada, AQSh kompaniyalariga, jumladan, Facebook, Twitter va boshqalarga xakerlik hujumlari dunyoning eng yirik kompyuter korporatsiyasi Apple munozaraning boshlanish davri sifatida e'tirof etildi.[22] Natijada AQSh da kiberjinoyatlar masalasi kundan-kunga rivojlanish bosqichiga chiqish holati kuzatildi. Hatto kiberjinoyat dinamik o'sish holatiga chiqishi AQSh Adliya departamenti tomonidan kiberjinoyatlarni 3 ta turga bo'lib klassifikatsiya qilinishiga olib keldi. Unga ko'ra:

– birinchi toifaga subyektiv tomon to'g'ridan-to'g'ri kompyuter yoki kompyuter tarmog'ining ish faoliyatini izdan chiqarish yoki uni buzishga qaratilgan jinoyatlar;

– ikkinchi toifaga kompyuter tizimi va global tarmoq an'anaviy jinoyatlarni sodir etishning vositasi yoxud usuli bo'lgan jinoyatlar;

– uchinchi toifaga kompyuter va Internet tarmog'i boshqa jinoyatlarni sodir etishda asosiy usul bo'lmasa-da, uni sodir etish

[21] Карасев П.А. Новые стратегии США в области кибербезопасности [Электронный ресурс]: URL: http://russiancouncil.ru/analytics-and-comments/analytics/novyestrategii-ssha-v-oblasti-kiberbezopasnosti/(дата обращения: 02.10.2019).

[22] Rogovsky E. Cyber-Washington: Global Ambitions. International Relations, Moscow, 2014. – P.848.

uchun kerakli axborot bilan ta'minlash manbasi hisoblangan jinoyatlar kiritiladi.[23]

Ikkinchi bosqich, 2000-yildan 2010-yilgacha bo'lgan davr. Ushbu davrda kiberxavfsizlik masalasida dunyo davlatlari yaxlit axborot makonining shakllanish davri sifatida e'tirof etildi. Sababi, ushbu davrda davlatlarning harbiy qudrati yo iqtisodiy qudrati bilan emas, balki AKT texnologiyalar sohasidagi salohiyati, kiberxavfsilik muhitini yaratish qoibiliyati hamda dunyodagi madaniy jarayonlarni boshqarish darajasi bilan belgilanadigan davr sifatida e'tirof etildi. Jumladan, ushbu davrga kelib kiberxavfsizlikning rivojlanishiga nisbatan, ko'pchilik ekspertlar keng ko'lamli kibermojarolarning misli ko'rilmagan darajada o'sganligini e'tirof eta boshlashdi. Xususan, AQSh ning o'sha paytdagi prezidenti Jorj Bush ma'muriyatida ham kiberxavfsizlik muammolari kun tartibiga chiqdi. Natijada, 2001-yilda "AQSh mudofaasini rivojlantirish bo'yicha to'rt yillik dastur" qabul qilinib, unda kiberoperatsiyalarga alohida e'tibor qaratilishi va u harbiy faoliyatning mustaqil turi sifatida e'tirof etildi. Buning eng muhim hujjatlaridan biri 2002-yilgi hamda 2003-yilning fevralidagi AQSh Milliy xavfsizlik strategiyasi bo'ldi.[24] Ushbu strategik hujjatlarda axborot va kiberxavfsizlik ko'lamining ortib borishi va uning siyosiy ahamiyati aks ettirildi. Ushbu hujjatning qabul qilinishi natijasida kompyuter tarmoqlari bo'yicha davlatning yangi siyosatini ishlab chiqish, bu bo'yicha kadrlarni tayyorlashni takomillashtirish masalasi belgilab berildi. AQSh kiberxavfsizlik strategiyasida asosan quyidagi maqsadlarga e'tibor qaratadi:

– Muhim infratuzilmalarni himoya qilish uchun davlat va xususiy sektorlarning birgalikda harakatlanishiga erishish.

– Davlat va xususiy sektorning birgalikda harakat qilishini rivojlantirishga oid rejalarni ishlab chiqish, xususiy sektorni kiber

[23] Computer Crime and Intellectual Property Section, US Department of Justice, The National Information Infrastructure Protection Act of 1996, Legislative Analysis, 1996.

[24] National Security Strategy 2002 [Электронный ресурс]: The W hite House. URL: http://georgewbush-whitehouse.archives.gov/nsc/nss/2002/ (дата обращения: 29.03.2023).

sohadagi vazifalarni bajarishga undash va uni bu yo'lda qo'llab-quvvatlash.

– Ish beruvchilar va biznes sektorining kiberhujumlarga qarshi "immunitet"ini oshirish, federal darajada ta'lim berish va yo'naltirishga ahamiyat qaratish.

– Rossiyaning kiber qudrati ortidan tug'iluvchi tahdidlarni yo'q qilish bo'yicha rejalar ishlab chiqish.

– Xitoyning kiber-josuslik tahdidlarining oldini olish maqsadida texnologik yangiliklarni amaliyotga muttasil joriy qilish va xususiy sektorning tijoriy manfaatlarini himoya qilish uchun zaruriy chora-tadbirlarni ko'rish.

– Qishloq xo'jaligi, oziq-ovqat, ichimlik suvi, aholi sog'lig'ini saqlash va favqulodda vaziyatlarga javob berish tizimlari, ijtimoiy ta'minot, axborot va telekommunikatsiya infratuzilmalari, energetika, transport, bank va moliya, kimyo sohasi, pochta tizimlaridagi barcha rasmiy kompyuter, dasturiy ta'minot va tarmoq texnologiyalarini kiberhujumlardan himoya qilish.

– Tovar va xizmatlar, g'oyalar, tadbirkorlar va kapitalning erkin harakatlanishini ta'minlash.

– AQSh bilan ittifoqdosh mamlakatlarni beqarorlashtirishga qaratilgan kiberhujumlarga qarshi kurashda ushbu davlatlarni qo'llab-quvvatlash.[25] Bularning asosiy maqsadi esa, texnologik rivojlanish bilan parallel ravishda, ayni paytda mamlakatlar "muhim infratuzilma" sifatida ta'riflanuvchi davlat xizmatlarini ko'rsatish tizimlarini tarmoq texnologiyalariga asoslangan innovatsiyalar bilan boshqara boshlashi, natijada muhim infratuzilmalarning kiberxavfsizligini ta'minlash ularning eng ustuvor vazifalaridan biriga aylantirish bo'ldi.

Ushbu davrning yana bir o'ziga xosligi, Yevropa Ittifoqi tomonidan 2001-yilda qabul qilingan "Kiberjinoyatchilik to'g'risida" Konvensiya orqali dunyo hamjamiyatida "kiberjinoyatchilik" tushunchasi shakllantirilganligi rasman tan olinganligi bilan izohlanadi.

[25] AQSh va Xitoyning kiberxavfsizlik strategiyasi: kim nimani ko'zlamoqda? https://kun.uz/28352354?q=%2F28352354#

Uchinchi bosqich, 2010-yildan to hozirgi qadarni o'z ichiga olgan davr hisoblanadi. Bu bosqichda kiberxavfsizlik rivojlanishining uchinchi bosqichi AQSh va Yevropa taraqqiyoti uchun muhim sanaldi. Sababi, AKT ning inqilobi global jarayonlarning barqaror taraqqiyoti uchun yangi imkoniyatlarni ochib berishi, bu imkoniyatlar natijasida kiberxavfsizlik rivojlanishiga "aqlli texnologiya"lar yaratilishi, kiberjinoyatchilik, kiberterrorizm va ekstremizm, gibrid urushlar, moliyaviy, sug'urta bozoridagi kibirxurujlar vujudga kelganligi bilan izohlanadi. Bu o'zgarishlar jarayoni kiberxavfsizlik rivojlanishining yuqori nuqtasi sifatida va dunyo davlatlarining bu boradagi tahdidlarga nisbatan o'zaro axborot integratsiyasi davri sifatida e'tirof etildi.

O'zbekistonda jamiyat va siyosatning barcha sohalarida axborot texnologiyalari rivojlanib borishi bilan mazkur sohani tartibga solish borasidagi ishlar ham parallel ravishda takomillashtirilib borilganligi kuzatiladi. Xususan, O'zbekiston 1996-yilda Internet global tarmog'iga qo'shildi va yilma-yil aholining butunjahon axborot tarmog'idan foydalanish imkoniyati va sharoitlari yaxshilanib bormoqda. Shu bilan birga bu boradagi munosabatlarni normativ huquqiy asosini yaratib beruvchi qonun va qonunosti hujjatlari qabul qilindi hamda bugungi kunga qadar ular izchillik bilan to'ldirilib borilmoqda.

Tadqiqot davomida aniqlanishicha, ko'pgina davlatlarda Internet tarmog'idan foydalanishni huquqiy tartibga solish va uning qonunchilik bilan qo'riqlanadigan ijtimoiy munosabatlarning zarar yetkazuvchi obyektlaridan kelib chiqib, 5 ta:

1) Bolalarni zararli kontentdan himoyalash va axloqlilik;
2) Milliy xavfsizlikka tahdidlar;
3) Intellektual mulk himoyasi;
4) Kompyuter xavfsizligi;
5) Elektron tijorat sohalariga bo'linadi.

O'zbekiston Respublikasida Internet global tarmog'idan foydalanishda o'ziga xos qonunchilik asoslari mavjud. Jumladan, 1993-yilda "Axborotlashtirish to'g'risida", 1994-yilda "Elektron hisoblash mashinalari uchun yaratilgan dasturlar va ma'lumotlar

bazalarining huquqiy himoyasi to'g'risida"gi, 1997-yilda "Axborot olish kafolatlari va erkinligi to'g'risida", 1999-yilda "Telekommunikatsiyalar to'g'risida"gi Qonunlar shaxsning axborotdan foydalanish bilan bog'liq huquqlari, erkinliklari hamda majburiyatlari, bu sohada qonun himoyasidagi obyektlar tavsifi keltirildi hamda ularga qarshi ijtimoiy xavfli qilmishlar uchun javobgarlik mavjudligi kabi prinsiplar o'rnatildi.

Shuningdek, "Telekommunikatsiyalar to'g'risida"gi Qonunga ko'ra (Internet global tarmog'iga ta'rif keltirilmagan bo'lsa-da), telekommunikatsiyalar tarmog'i-uzatishlarning bir yoki bir necha turini: telefon, telegraf, faksimil turlarini, ma'lumotlar uzatish va hujjatli xabarlarning boshqa turlarini, televizion va radioeshittirish dasturlarini translyatsiya qilishni ta'minlovchi telekommunikatsiya vositalarining majmui[26] sifatida talqin etildi. Qolaversa, O'zbekiston Respublikasi Prezidentining 2019-yil 14-sentyabrdagi "Axborot texnologiyalari va kommunikatsiyalarining joriy etilishini nazorat qilish, ularni himoya qilish tizimini takomillashtirishga oid qo'shimcha chora-tadbirlar to'g'risida"gi PQ-4452-sonli qarori[27] ham shular jumlasidandir. Bundan tashqari mazkur sohani tartibga solish maqsadida bir qator xalqaro hujjatlar ham qabul qilingan bo'lib, bulardan, internet va kompyuter tarmoqlari, axborot texnologiyalaridan foydalanib, sodir etilayotgan jinoyatlarga qarshi kurashish bo'yicha Budapesht konvensiyasi (23.11.2001. Budapesht), Mustaqil davlatlar hamdo'stligiga a'zo davlatlarning axborot texnologiyalari sohasidagi jinoyatlarga qarshi kurashishdagi hamkorlik to'g'risidagi kelishuv (28.09.2018. Dushanbe) va boshqalarni sanab o'tish mumkin.

Tahlillar shuni ko'rsatdiki, O'zbekiston Respublikasida kiberxavfsizlik sohasiga tegishli bo'lgan 17 ta qonun hujjati, 9 ta Prezident Farmon va Qarorlari, 14 ta Vazirlar Mahkamasining

[26] O'zbekiston Respublikasining Telekommunikatsiyalar to'g'risida,1999 // O'zbekiston Respublikasi Oliy Majlisining Axborotnomasi, 1999-yil, 9-son, 219-modda.

[27] O'zbekiston Respublikasi Prezidentining 2019-yil 14-sentyabrdagi "Axborot-texnologiyalari va kommunikatsiyalarining joriy etilishini nazorat qilish, ularni himoya qilish tizimini takomillashtirishga oid qo'shimcha chora-tadbirlar to'g'risida"gi PQ-4452-sonli qarori. https://lex.uz/docs/4665548

Qarori, shuningdek tegishli normalar va ko'plab idoralararo me'yoriy-huquqiy hujjatlar qabul qilingan. Xususan, mazkur sohada tadqiqot olib borgan A.Rasulev mamlakatning axborot texnologiyalar borasidagi kiberxavfsizlik bilan bog'liq huquqiy normalar rivojlanish bosqichlarini 3 ga bo'lishni tavsiya etgan. Unga ko'ra:

– birinchi bosqich, 1991–1994-yillarni qamrab olib, bu jarayonda 4 ta qonun, 4 ta Prezident qarorlari va farmonlari hamda 2 ta Vazirlar Mahkamasi qarori qabul qilingan bo'lib, bu sohadagi dastlabki munosabatlar tartibga solingan.

– ikkinchi bosqich, 1994-yildan 2007-yilgacha bo'lgan davrni o'z ichiga olgan va bunda 10 ta qonun, 8 ta Prezident qaror va farmonlari hamda 31 ta Vazirlar Mahkamasi qarorlari qabul qilingan. Ushbu davrda axborot texnologiyalari sohasidagi jinoyatlar uchun jinoiy taqiqlar kiritilgan.

– uchinchi bosqich, 2007-yildan hozirgacha bo'lgan bosqich bo'lib, unda jinoyat kodeksiga axborot texnologiyalari borasidagi jinoyatlar uchun javobgarlik belgilovchi alohida bob kiritildi va ular kengaytirib borilmoqda. So'nggi bosqichda 10 ga yaqin qonun, 24 ta Prezident qaror va farmonlari hamda 40 ga yaqin Vazirlar Mahkamasi qarorlari qabul qilinganligi borasida tadqiqotlar olib borilgan.[28]

Aynan, kiberxavfsizlik rivojlanish jarayoni O'zbekiston Respublikasini rivojlantirishning beshta ustuvor yo'nalishi bo'yicha Harakatlar strategiyasida "Xavfsizlik, millatlararo totuvlik va diniy bag'rikenglikni ta'minlash, chuqur o'ylangan, o'zaro manfaatli va amaliy ruhdagi tashqi siyosat yuritish" deb nomlangan beshinchi yo'nalish doirasida amalga oshirildi, desak mubolag'a bo'lmaydi. Chunki, ushbu yo'nalish doirasida mamlakatning konstitutsiyaviy tuzumi, suvereniteti, hududiy yaxlitligini himoya qilishga doir chora-tadbirlarni ro'yobga chiqarish, kiberxavfsizlik sohasining normativ-huquqiy asoslarini takomillashtirish belgilangan edi.

[28] Расулев А.К. Некоторые вопросы совершенствования уголовно правовых и криминологическихмер борьбы с преступлениями в сфере информационных технологий и безопасности. – Т., 2017. – С.36-37.

Xususan, 2020–2023-yillarga mo'ljallangan kiberxavfsizlikka doir milliy strategiyani, "Kiberxavfsizlik to'g'risida"gi Qonun loyihasini hamda O'zbekiston Respublikasi yagona axborot siyosati konsepsiyasini ishlab chiqish belgilandi. O'zbekiston Respublikasi Prezidentining 2018-yil 21-noyabrdagi "Axborot texnologiyalari va kommunikatsiyalarining joriy etilishini nazorat qilish, ularni himoya qilish tizimini takomillashtirishga oid qo'shimcha chora-tadbirlar to'g'risida"gi Qarori hisoblanadi. Mazkur Qarorga asosan, "Texnik ko'maklashish markazi" davlat unitar korxonasi "Kiberxavfsizlik markazi"ga aylantirildi. Aynan mazkur markazni qayta tashkil etishdan maqsad mamlakatimizda "xavfsiz axborotlashgan jamiyat" muhitini yaratishga qaratilgan ustuvor islohotlar, vazifalar belgilab berilgan.

2019-yil 2-fevralda Prezident Sh.Mirziyoyevning "Axborot sohasi va ommaviy kommunikatsiyalarni yanada rivojlantirishga oid qo'shimcha chora-tadbirlar to'g'risida"gi PF-5653-son Farmoni bilan O'zbekiston matbuot va axborot agentligi negizida O'zbekiston Respublikasi Prezidenti Administratsiyasi huzuridagi Axborot va ommaviy kommunikatsiyalar agentligi, O'zbekiston matbuot va axborot agentligining Ommaviy kommunikatsiyalar sohasida monitoring Markazi negizida O'zbekiston Respublikasi Prezidenti Administratsiyasi huzuridagi Axborot va ommaviy kommunikatsiyalar agentligining Ommaviy kommunikatsiyalar masalalari bo'yicha markazi tashkil etildi. Agentlikning asosiy vazifalari etib fuqarolarning so'z va axborot erkinligiga doir konstitutsiyaviy huquqlarining ro'yobga chiqishini ta'minlash, mamlakatni ijtimoiy-siyosiy va sotsial-iqtisodiy rivojlantirishda ommaviy axborot vositalarining rolini kuchaytirish, media-bozorda ular uchun teng sharoitlar yaratish, shuningdek jurnalistlar huquqlarini himoya qilish;

– respublika axborot xavfsizligini ta'minlashda ishtirok etish hamda axborot sohasidagi xatar va tahdidlarga qarshi o'z vaqtida va munosib ravishda kurashish choralarini ko'rish belgilandi.

– Ommaviy kommunikatsiyalar masalalari bo'yicha markazning muhim vazifalari sifatida milliy axborot makonini hamda ommaviy

axborot vositalari, matbuot, noshirlik-matbaa va axborot-kutubxona faoliyatini rivojlantirishni qo'llab-quvvatlash bo'yicha chora-tadbirlarning amalga oshirilishi samaradorligini monitoring qilish;

– ommaviy axborot vositalarida tarqatilayotgan materiallar mazmunining, shu jumladan, shaxs, jamiyat va davlat manfaatlarining himoyasini ta'minlashga qaratilgan qonun hujjatlari talablariga muvofiqligini tizimli asosda tahlil qilish.[29]

Mazkur Farmon bilan O'zbekiston Respublikasi Axborotlashtirish va telekommunikatsiyalar sohasida nazorat bo'yicha davlat inspeksiyasining fonogrammalar va audiovizual asarlarni tarqatish (sotish, ijaraga berish va omma e'tiboriga yetkazish)da mualliflik huquqlari sohasidagi qonunchilikka va normativ hujjatlarga rioya qilinishi ustidan davlat nazorati bo'yicha vakolatlari Agentlikka berildi.

O'zbekiston Respublikasi Prezidentining 2020-yil 5-oktyabrdagi Farmoni bilan "Raqamli O'zbekiston – 2030" strategiyasi"[30] tasdiqlandi. Mazkur strategiyada ham mamlakatimizda raqamli iqtisodiyotni faol rivojlantirish, barcha tarmoqlar va sohalarda, eng avvalo, davlat boshqaruvi, ta'lim, sog'liqni saqlash va qishloq xo'jaligida zamonaviy axborot-kommunikatsiya texnologiyalarini keng joriy etish belgilab qo'yilgan. Xususan, strategiyada "Raqamli O'zbekiston – 2030" strategiyasining maqsadli ko'rsatkichlari, transformatsiya qilish dasturi, amalga oshirish bo'yicha muvofiqlashtirish komissiyasi, tarmoqlar va hududlarni axborot texnologiyalari sohasida O'zbekiston Respublikasining xorijiy mamlakatlardagi diplomatik vakolatxonalariga biriktirish, amalga oshirish bo'yicha "Yo'l xaritasi" ishlab chiqilgan. Ushbu strategiya doirasida O'zbekistonda kiberxavfsizlikni ta'minlashga hamda rivojlanishiga qaratilgan amaliy islohotlar olib borildi, desak

[29] O'zbekiston Respublikasi Prezidentining 2019-yil 2-fevraldagi "Axborot sohasi va ommaviy kommunikatsiyalarni yanada rivojlantirishga oid qo'shimcha chora-tadbirlar to'g'risida"gi PF-5653-son Farmoni.//Qonun hujjatlari ma'lumotlari milliy bazasi, 04.02.2019-y., 06/19/5653/2568-son.

[30] O'zbekiston Respublikasi Prezidentining 2020-yil 5-oktyabrdagi "Raqamli O'zbekiston – 2030" strategiyasi" va uni samarali amalga oshirish chora-tadbirlari to'g'risida"gi Farmoni / https://lex.uz/docs/5030957

mubolag'a bo'lmaydi. Xususan, 2020–2022-yillarda hududlarni raqamli transformatsiya qilish, 2020–2022-yillarda tarmoqlarni raqamli transformatsiya qilish dasturlari qabul qilindi. Qolaversa, aholi punktlarini Internet tarmog'iga ulash darajasi, shu jumladan, keng polosali ulanish portlarini 2,5 milliongacha ko'paytirish, 20 ming kilometr optik-tolali aloqa liniyalarini qurish va mobil aloqa tarmoqlarini rivojlantirish orqali 78 foizdan 95 foizga yetkazish, hududlarni ijtimoiy-iqtisodiy rivojlantirishning turli sohalarida 400 dan ortiq axborot tizimlari, elektron xizmatlar va boshqa dasturiy mahsulotlar joriy etish, qolaversa, 587 ming nafar kishini, shu jumladan, "Bir million dasturchi" loyihasi doirasida 500 ming nafar yoshlarni qamrab olish orqali kompyuter dasturlash asoslariga o'qitish tashkillashtiriladi. Aynan mazkur strategiya mamlakatimizda bu boradagi faoliyatlarning rivojlanishiga katta xizmat qilmoqda. Shuningdek, mazkur normativ-huquqiy hujjatlar O'zbekistonda raqamli texnologiyalarni rivojlantirish asosida xalqaro imijini oshirishga qaratilgan chora-tadbirlar hisoblanadi.

2022-yil 15-aprelda O'zbekiston Respublikasining "Kiberxavfsizlik to'g'risida"gi O'RQ-764-sonli Qonuni[31] qabul qilindi. Mazkur qonun 40 ta moddadan iborat bo'lib, unda kiberxavfsizlik faoliyatini tartibga soluvchi normalar belgilab qo'yildi. Mazkur Qonunga muvofiq, davlatning kiberxavfsizligini ta'minlashda kibermakonda shaxs, jamiyat va davlat manfaatlarini tashqi va ichki tahdidlardan himoya qilish ustuvor vazifa sifatida qayd etildi. Qonunda kiberjinoyatchilik, kibermakon, kibertahdid, kiberxavfsizlik, kiberhimoya, kiberhujum sohasidagi asosiy tushunchalarga ta'rif berilgan.

Qonunda kiberxavfsizlikni ta'minlashning quyidagi:

- qonuniylik;
- kibermakonda shaxs, jamiyat va davlat manfaatlarini himoya qilishning ustuvorligi;
- kiberxavfsizlik sohasini tartibga solishga nisbatan yagona yondashuv;

[31] 2022-yilning 15-aprel kuni O'zbekiston Respublikasining "Kiberxavfsizlik to'g'risida"gi O'RQ-764-sonli Qonuni.// https://lex.uz/uz/docs/5960604

• kiberxavfsizlik tizimini yaratishda mahalliy ishlab chiqaruvchilar ishtirokining ustuvorligi;

• O'zbekiston Respublikasining kiberxavfsizlikni ta'minlashda xalqaro hamkorlik uchun ochiqligi kabi asosiy tamoyillari belgilangan.

Shuningdek, kiberxavfsizlik sohasidagi yagona davlat siyosatini O'zbekiston Respublikasi Prezidenti belgilashi nazarda tutildi. O'z navbatida, kiberxavfsizlik sohasidagi vakolatli davlat organi etib O'zbekiston Respublikasi Davlat xavfsizlik xizmati belgilandi. Kiberxavfsizlik talablariga muvofiqlik yuzasidan ekspertiza majburiy tartibda yoki kiberxavfsizlik subyektlarining tashabbusiga ko'ra amalga oshirilishi, quyidagilar kiberxavfsizlik talablariga muvofiqlik yuzasidan majburiy tartibda ekspertizadan o'tkazilishi nazarda tutildi:

– davlat organlarining axborot resurslari;

– davlat organlarining axborot tizimlari;

– muhim axborot infratuzilmasi obyektlari toifasiga kiritilgan axborot tizimlari.

Davlat organlari va tashkilotlari axborot tizimlari hamda resurslarining, shuningdek, muhim axborot infratuzilmasi obyektlarining kiberxavfsizligini ta'minlash maqsadida qo'llaniladigan apparat, dasturiy-apparat va dasturiy vositalar majburiy tartibda sertifikatlashtirilishi lozimligi belgilandi. Qonunga ko'ra, kiberxavfsizlik subyektlari tomonidan kiberxavfsizlik hodisalariga nisbatan choralar ko'rish quyidagi shakllarda amalga oshirilishi mumkin ekanligi ko'rsatildi:

• dasturiy ta'minotdagi va qurilmalardagi zaifliklarni hamda xatoliklarni bartaraf etish;

• zararli dasturlarni yo'q qilish, ularning tarqalishini cheklash, kiberhujumlar manbayini texnik jihatdan cheklash;

• axborotlashtirish obyektlarini mavjud kibertahdidlardan ajratib qo'yish;

• huquqni muhofaza qiluvchi organlarga kiberxavfsizlik hodisalari to'g'risida ma'lumotlar taqdim etish.

Xulosa o'rnida, mazkur Qonun davlatning kiberxavfsizligini ta'minlashda kibermakonda shaxs, jamiyat va davlat manfaatlarini

tashqi va ichki tahdidlardan himoya qilishning huquqiy mexanizmi sifatida muhim ahamiyatga egaligini ta'kidlash lozim.

1.3. Markaziy Osiyo kiberxavfsizligi tizimi va uning o'ziga xos xususiyatlari

Kibermakondagi muammolar va xatarlarning ko'payishi, kiberjinoyatchilikning keskin oshishi, onlayn hujumlarning ortishi va dunyoda kibermakon rivojlashinining oldindan aytib bo'lmaydigan dinamikasi O'zbekiston Respublikasida kiberxavfsizlikni ta'minlash uchun me'yoriy-huquqiy bazani ishlab chiqish zarurati borligini ko'rsatdi.

Markaziy Osiyo mintaqaviy xavfsizlik masalalari rivojlanish jarayoni. Mintaqaviy siyosiy jarayonlar va mintaqaviy xavfsizlik mavzulari yangi ilmiy yo'nalishdagi tadqiqotlar obyekti sifatida XX asr boshlarida siyosatshunoslik va mintaqashunoslik kabi fanlar doirasida paydo bo'ldi. Mintaqaviy siyosat konsepsiyasini aniqlashda mavjud yondashuvlarni tahlil qilish ularning nazariy jihatdan yetarli darajada rivojlanmaganligini ko'rsatadi. Xususan, Markaziy Osiyo submintaqasidagi hududiy xavfsizlik muammolari ham butun dunyodagi kabi terrorizm, ekstremizm, ommaviy qirg'in qurollarining tarqalishi, yadro quroli xavfining ortishi, narkobiznes, atrof-muhitning buzilishi, global isish, o'rmonlarning kesilishi, pandemik kasalliklarning avj olishi va boshqa tahdidlar bilan ifodalanmoqda. Suv resurslari taqsimoti bilan bog'liq urushlar xavfi ham tobora o'sib bormoqda. Shuningdek, mazkur mintaqa mamlakatlari ichki, endogen xarakterga ega bo'lgan ko'plab eski va yangi muammolar uchun ham hali munosib javob topa olishayotgani yo'q. Jumladan, ichki siyosiy va ijtimoiy-iqtisodiy beqarorlik, millatlararo ziddiyatlar, mintaqaviy elita va davlatlar boshqaruvidagi tuzilmalar o'rtasida mavjud qarama-qarshiliklar, aholining qashshoqlashishi, aholi daromadlaridagi farqning ortishi va ijtimoiy muvozanatning kuchayishi, yoshlar orasida ishsizlikning yuqori darajaga yetishi, korrupsiyaning avj olishi, davlat tuzilmalarining past samaradorligi, har qanday siyosiy beqarorlik yuz berganda

boshini ko'tarishga tayyor va dunyoviy hukmron boshqaruvlarni obro'sizlantirish uchun ijtimoiy muammolardan faol foydalanuvchi radikal islomizm, giyohvand moddalar savdosi va diniy ekstremizm ta'sirining o'sishi hamda oliy siyosiy hokimiyatning davomiyligi muammosi (chunki Markaziy Osiyoning aksariyat davlatlarida bunday davomiylik uchun aniq belgilangan va o'rnatilgan qoidalar mavjud emas) kabilar bugungi kunda hudud tinchligi uchun asosiy tahdid manbalari sifatida namoyon bo'lmoqda.[32]

1991-yilda mustaqilikka erishgach, O'zbekiston, Qirg'iziston, Tojikiston va Turkmaniston respublikalari milliy xavfsizligi mutlaqo yangi tahdidga duch keldi. So'nggi o'n yillikda mavjud muammolar qatoriga yuqori texnologiyalar va internetdan foydalanib sodir etiladigan jinoyatlar turi qo'shildi. Kiberxavfsizlik Internetning tarqalishi bilan chambarchas bog'liq bo'lib, tarmoqqa ulanish tezligining o'zgarishiga qaramay, Markaziy Osiyoning barcha davlatlarida kuzatilmoqda. Internet tezligini 2014-yil fevraldan buyon har 30 kunda sinovdan o'tkazuvchi "Ookla" kompaniyasi ma'lumotlariga ko'ra, 188 mamlakatlar ichida Qozog'iston 58, Tojikiston 66, Qirg'iziston 81, O'zbekiston 171-o'rinni egallagan. O'sha manbaga ko'ra, Birlashgan Millatlar Tashkilotining xalqaro elektraloqa ittifoqi (International Telecommunication Union) ekspertlari tomonidan Markaziy Osiyo mamlakatlaridan tuzilgan global kiberxavfsizlik indeksida Qozog'iston 2020-yilda eng yuqori o'rin, ya'ni 192 dan 38-o'rinni egalladi. O'zbekiston 78, Qirg'iziston 100 va Tojikiston 146 o'rinni egallagan.

Markaziy Osiyodagi kiberjinoyatlar uchta asosiy toifaga bo'linadi: bezorilik, xakkerlik va kompyuter firibgarligi. Birlashgan Millatlar Tashkilotining 2018-yildagi tadqiqoti natijalariga ko'ra, 50% davlatlarning kiberxavfsizlik strategiyasi mavjud emas, aksincha 25% davlatda muhim axborot infratuzilmasi (keyingi o'rinda MAI) uchun xavfsizlik bo'yicha qonunchilik bazasi mavjud. Shuningdek, mamlakatlarning atigi 31% da MAI himoyasi

[32] Markaziy Osiyoda mushtarak jihatlar, tahdidlar va yangi imkoniyatlar. O'zbekiston Respublikasi Prezidenti huzuridagi Strategik va mintaqalararo tadqiqotlar instituti. 16.02.2019. http://uza.uz/oz/society/markaziy-osiyeda-mushtarak-zhi-atlar-ta-didlar-va-yangi-imko-15-02-2019

bo'limi kiberxavfsizlik strategiyasiga kiritilgani, faqatgina 109 ta ishtirokchi davlatlarda kiberxavfsizlik bo'yicha qonun hujjatlari mavjudligi aniqlandi. 141 mamlakatda (73%) onlayn maxfiylik qonunlari mavjud.

Shundan kelib chiqib, Markaziy Osiyo mintaqasida kiberxavfsizlik tizimi va uning o'ziga xos xususiyatlarini quyidagicha tahlil etamiz.

Qozog'iston Respublikasi

Qozog'iston Respublikasi Markaziy Osiyoda o'z o'rniga ega bo'lgan davlat hisoblanadi. Uning siyosiy tuzumida 1991-yildan so'ng demokratik o'zgarishlar boshlandi.[33] Bu borada ikki bosqichga mo'ljallangan olti yillik Milliy dasturning (2006–2011-yillar) qabul qilinishi bu islohotlarga qattiq kirishilganligidan dalolat beradi. Ammo axborot-kommunikatsiya texnologiyalari yutuqlarini ulardan foydalanish madaniyatini shakllantirish va "axborot jamiyati"ga xos bo'lgan ijtimoiy va ishlab chiqarish munosabatlari, birinchi navbatda, kiberxavfsizlikni ta'minlash masalalarida ildiz otishi so'nggi o'n yilliklarga xos xarakterli ekanligi Qozog'istonda ham o'z tasdig'ini topmoqda. Xususan, Birlashgan Millatlar Tashkilotining global kiberxavfsizlik indeksida Qozog'iston 9 pog'ona ko'tarilib, 31-o'rinni egalladi (ilgari 40-o'rin). Bu haqda Xalqaro elektraloqa ittifoqining 29 iyun kuni bo'lib o'tgan konferensiyasida Global kiberxavfsizlik indeksining 4-nashrining hisobotida ma'lum qilindi. Reyting davlatning qonunchilik bazasi, texnik va tashkiliy choralari, xalqaro maydondagi faoliyati va axborot xavfsizligini rivojlantirish salohiyatiga asoslangan. Shu sababli bo'lsa kerak, Qozog'iston Respublikasining 2017-yilning 30-iyundagi 307-sonli Qarori bilan "Kiberxavfsizlik konsepsiyasi" qabul qilindi. Kiberxavfsizlik konsepsiyasi ("Qozog'iston kiberqalqoni") (keyingi o'rinlarda Konsepsiya deb yuritiladi).[34] Qozog'iston Respublikasi Prezidentining "Qozog'istonning uchinchi modernizatsiyasi: global

[33] Кульжанова Г. Некоторые аспекты проблемы политической модернизации местного государственного управления // Казахстан–Спектр. 20005 № 2. – С.22.

[34] Об утверждении Концепции кибербезопасности ("Киберщит Казахстана") Постановление Правительства Республики Казахстан от 30 июня 2017 года № 407. https://adilet.zan.kz/rus/docs/P1700000407

raqobatbardoshlik" Murojaatiga muvofiq "Qozog'iston-2050" Strategiyasi Qozog'iston dunyoning eng rivojlangan mamlakatlari 30-o'ringa kirishi bo'yicha yondashuvlarini hisobga olgan holda ishlab chiqilgan. Ushbu konsepsiya 6 ta qismni o'z ichiga oladi. Ular: 1.Kirish; 2.Hozirgi vaziyatni tahlil qilish; 3.Xalqaro tajriba; 4.Maqsad, vazifalar, kutilayotgan natijalar va amalga oshirish muddati; 5.Asosiy tamoyillar va yondashuvlar; 6.Konsepsiyani amalga oshirish ko'zda tutilgan normativ-huquqiy hujjatlar ro'yxatidan tashkil topgan. Shundan ko'rinadiki, konsepsiyada davlat organlari faoliyatini axborotlashtirish, davlat xizmatlarini avtomatlashtirish sohasidagi joriy vaziyatni baholash, "raqamli" iqtisodiyotni rivojlantirish istiqbollari va sanoatda ishlab chiqarish jarayonlarini texnologik modernizatsiya qilish, axborot-kommunikatsiya xizmatlari ko'rsatish ko'lamini kengaytirish asosida ishlab chiqilgan. Qolaversa, ushbu konsepsiya Qozog'iston Respublikasi Prezidenti "Uchinchi Qozog'istonni modernizatsiya qilish: global raqobatbardoshligi" va Qozog'istonning kuchli 30 talikka kirishi uchun ishlab chiqilganligini ko'rsatadi.[35] Ushbu konsepsiyani amalga oshirish ikki bosqichda mo'ljallangan bo'lib, bular birinchi bosqich 2017-2018-yillar, ikkinchi bosqich 2019–2022-yillarni o'z ichiga oladi.

Qozog'iston Respublikasida o'tkazilgan ijtimoiy so'rovnoma natijalari ko'rsatadiki, 51,5% aholi internet orqali, 41,6% televizor orqali, 65,4% aholi mobil telefon orqali axborotlarni olishi aniqlangan.[36] Shundan kelib chiqib aytish kerakki, Qozog'iston Respublikasida kiberxavfsizlikni ta'minlash masalasi mamlakatning milliy xavfsizligi uchun tahdid sifatida baholanganligini ko'rish mumkin. Sababi, so'nggi uch yil mobaynida Qozog'iston Respublikasida kiberxavfsizlik quyidagi ko'rinishda tahdid sifatida davlat xavfsizlik tizimiga ta'sir etgan.

[35] Постановление Правительства Республики Казахстан от 30 июня 2017 года № 407 «Об утверждении Концепции кибербезопасности (Киберщит Казахстана)» // adilet.zan.kz/rus/docs/P1700000407.

[36] Вопросы безопасности обеспечения кибербезопасности рекомендации.// https://www.gov.kz/memleket/entities/infsecurity?lang=ru

Qozog'iston Respublikasida kiberxavfsizlikka ta'sir etish holati (2020-2022-yillar)[37]

Tahdid ko'rinishlari	2020-yil	2021-yil	2022-yil
Kompyuter viruslari orqali	32.1%	16.5%	51.7%
Zararli spamlar orqali	13.4%	23.0%	34,5%
Ijtimoiy tarmoqlarni buzish natijasida	3.9%	14.5%	28.4%

Shundan kelib chiqqan holda Qozog'iston hukumati mamlakat aholisini va davlat tuzilmalarini kibertahdidlardan himoya etishning 5 ta asosiy qoidasini ishlab chiqqan. Bularga maxfiylik siyosati, pochta xavfsizligi, antivirus dasturiy ta'minoti, ijtimoiy injeneriya xizmati, internet va ijtimoiy tarmoqlar. Ushbu beshta qoida asosida davlat va aholi orasida kiberxavfsizlikni ta'minlash "yo'riqnoma"sini ishlab chiqqan. Ushbu yo'riqnoma aholi orasida tarqatilgan bo'lib, aholi bevosita ushbu namuna asosida o'zini kiberxurujlardan himoya etadi.

Qirg'iziston Respublikasi

2019-yilga qadar Qirg'izistonda kiberjinoyatchilikka qarshi kurashish bo'yicha davlat dasturi yo'q edi. Qirg'iziston Respublikasida Kiberxavfsizlik strategiyasi faqat 2019-yilda ishlab chiqilgan va tasdiqlangan bo'lib, uning doirasida 2019–2023-yillarda mamlakatda kiberxavfsizlikni ta'minlash uchun asosiy shart-sharoitlar yaratish rejalashtirilgan.

Bundan tashqari, strategiya doirasida kiberjinoyatlar, jumladan, transchegaraviy kompyuter jinoyatlari uchun javobgarlikni qonunchilikka kiritish, AKT dan foydalangan holda dalillarni aniqlash, to'plash va taqdim etish usullarini joriy etish rejalashtirilgan.

Ta'kidlash lozimki, mamlakatda 2008-yildan "Shaxsiy ma'lumotlar to'g'risida", 2009-yildan boshlab "Elektron hujjat va elektron raqamli imzo to'g'risida"gi qonunlar amal qilmoda.

[37] O'sha manba.

Bundan tashqari, Qirg'iziston Respublikasi hukumati huzuridagi Axborot texnologiyalari va kommunikatsiyalari davlat qo'mitasi Qirg'iziston Respublikasida kiberxavfsizlik sohasida muvofiqlashtiruvchi agentlik hisoblanadi. Biroq mamlakatda kiberjinoyatlarni kuzatish uchun aniq ko'rsatkichlar mavjud emas.

Strategiyani amalga oshirish rejasi doirasida mahalliy mutaxassislarning texnik malakasini oshirish ko'zda tutilgan. Bundan tashqari, hodisalarni tasniflash tizimini ishlab chiqish va joriy etish rejalashtirilgan bo'lib, u o'z navbatida kiberxavfsizlik ko'rsatkichlariga asoslanadi, masalan; axborot tizimlarining buzilishi darajasi, tizimlarni tiklash uchun zarur bo'lgan vaqt, ma'lumotlarni o'chirish, voqea oqibatlari va boshqalar. Ushbu ko'rsatkichlar asosida axborot tizimlarini himoya qilishga qo'yiladigan talablar tizimini ishlab chiqishda muhim vosita bo'lgan kiberxavfsizlik hodisalari darajalari shkalasi shakllantiriladi.[38]

2019-yil 31-dekabr kuni Qirg'iziston Respublikasining o'sha paytdagi Jeenbekov Sooronbay Sharipovich o'z xalqiga Yangi yil Murojaatnomasida kirib kelayotgan 2020-yilni "Hududlarni rivojlantirish, mamlakatni raqamlashtirish va bolalarni qo'llab-quvvatlash yili" deb e'lon qildi.[39]

Axborot-kommunikatsiya texnologiyalari sohasi ketma-ket ikkinchi yil respublika rivojlanishining ustuvor yo'nalishiga aylangani ham bu boradagi davlat siyosati faollashganidan, ham bu yerda tez orada hal etilishi lozim bo'lgan ancha jiddiy muammolar mavjudligidan dalolat beradi.

Qirg'iziston Respublikasining raqamli himoyasini ta'minlash masalalari so'nggi yillarda siyosiy va akademik muhokamalar mavzusiga aylandi. Ma'lumki, Birlashgan Millatlar Tashkiloti (BMT) Xalqaro elektraloqa ittifoqining Global kiberxavfsizlik indeksi – tadqiqot loyihasi mavjud bo'lib, u dunyoda raqamli muhit rivojlanishi yo'lidagi to'siqlar (risklar) xavfini aniqlash, tavsiyalar ishlab chiqish, davlatlarning kibermudofaasini kuchaytirish va global

[38] https://elibrary.ru/item.asp?id=44191317

[39] От цифровизации до волонтерства: каким будет 2020 год в странах Центральной Азии // News-Asia. 3 января 2020. URL: news-asia.ru/view/kz/ politics/13202 (дата обращения: 10.01.2020).

raqamli madaniyatni shakllantirish maqsadlariga xizmat qiladi. Qirg'iziston esa, ana shu indeks bo'yicha nisbatan past ballga egadir.

Qirg'iziston 2014-yildan boshlab kiberxavfsizlik darajasi past bo'lgan davlatlar guruhiga kiritildi. U 2017-yilda reyting ko'rsatkichi bo'yicha 96-o'rinda bo'lsa, 2018-yilga kelib, 111-o'ringa tushib qoldi hamda o'z o'rnini yo'qotishda davom etmoqda. Indeksning mintaqaviy taqsimotida Qirg'iston Markaziy Osiyoda 4-o'rinni, MDH da esa 8-o'rinni egallaydi, undan pastda faqat Turkmaniston turadi. Markaziy Osiyo mintaqasida Qozog'iston yetakchi bo'lib qolmoqda; u 2017-yildan 2018-yilgacha bo'lgan qisqa davrda jahon reytingida 82-o'rindan 40-o'ringa, MDH mamlakatlari indeksida esa, 7-o'rindan 2-o'ringa ko'tarildi.[40]

Shu tariqa, Markaziy Osiyoning boshqa mamlakatlari singari, Qirg'iziston ham deyarli darhol axborot tengsizligi muammosiga duch keldi: faqat yirik shaharlar Internetga kirish imkoniga ega edi; Internetga kirish asosan mobil aloqa orqali amalga oshirildi (2010-yillarning boshiga kelib respublika aholisining 90 foizi mobil aloqaga ulangan edi); uyali aloqa operatori xizmatlari narxi nisbatan yuqoriligicha qoldi, Butunjahon Internetning qirg'iz segmentida rus tilidagi kontent ustunlik qildi, mamlakatda rus tilini bilish darajasi esa tez pasayib bordi.

Bundan tashqari, media resurslari huquqiy tartibga solingan, ammo internet saytlari huquqiy tartibga solinmaganligi sababli ular ko'pincha siyosiy muxolifat uchun axborot platformasiga aylanib qoldi. 2010-yilda Qirg'iziston janubida sodir bo'lgan fojiali voqealar raqamli texnologiyalarning ijtimoiy-siyosiy ahamiyati va ularning ziddiyatli salohiyatini namoyish etdi. Buning natijasida Markaziy Osiyo davlatlari hukumatlarida axborot xavfsizligi to'g'risida o'ziga xos tushuncha shakllandi, bu asosan milliy axborot makonini buzg'unchi g'oyalardan himoya qilish, ya'ni hokimiyatni tanqid qilishning oldini olishni anglatardi.[41] Qolaversa, shunday yondashuv

[40] Global Cybersecurity Index 2017. Geneva: International Telecommunication Union (ITU), 2018. – P.66.

[41] Ибрагимова Г. Подходы государств Центральной Азии к вопросам управления интернетом и обеспечения информационной безопасности // Индекс безопасностиб 20136 № 1. – С.103–128.

Mustaqil Davlatlar Hamdo'stligi (MDH), Shanxay hamkorlik tashkiloti (ShHT) va Kollektiv xavfsizlik shartnomasi tashkiloti (KXShT) kabi Markaziy Osiyo respublikalari ishtirokidagi xalqaro tuzilmalarning axborot xavfsizligini ta'minlash bo'yicha asosiy hujjatlarda ham belgilandi. Biroq xalqaro amaliyotda kiberxavfsizlik sohasi "kiberjinoyatlarga qarshi kurashish, shaxsiy, korporativ va davlat ma'lumotlarini himoya qilish, kiberxavfsizlik madaniyatini yuksaltirish va internet xizmatlari operatorlari, tartibga soluvchilar va sohaning boshqa ishtirokchilari o'rtasidagi texnik hamkorlik bo'yicha texnik, huquqiy va tashkiliy chora-tadbirlarni o'z ichiga oladi".[42] Shu tariqa, Qirg'izistonda "Axborot suvereniteti"ni himoya qilishga qaratilgan davlat siyosatining bu tomonga o'zgarishi Markaziy Osiyo davlatlarining texnik va texnologik xavfsizligini ta'minlash mexanizmlarini shakllantirish jarayoniga to'sqinlik qildi, ularning global raqamli makondan kelib chiqadigan tashqi kibertahdidlarga nisbatan obyektiv tarzda zaifligini kuchaytirdi.

Internetning jadal kirib kelishiga javoban hokimiyat organlari maxsus nazorat institutlarini yaratdilar, ijtimoiy-siyosiy sohada an'anaviy ravishda qo'llaniladigan bir qancha cheklovchi amaliyotlardan foydalandilar, ya'ni aloqa kanallarini markazlashtirdilar. Mamlakatda internet-provayderlarini blokirovka qildilar, shubhali mazmunga ega veb-saytlarni buzdilar, global tarmoqlarga ulanish tezligini ataylab pasaytirdilar va h.k. Hatto 2009-yilda Qirg'iziston Respublikasi Ichki ishlar vazirligining to'qqizinchi boshqarmasi tarkibida Kiber tahdidlar masalalari bo'yicha guruh tashkil etildi. Uning vazifalariga Global tarmoqning milliy segmentida radikal ekstremistik islomiy guruhlar mavjudligini aniqlash kiritildi.[43] Bundan tashqari, Qirg'iziston Milliy xavfsizlik davlat qo'mitasi tarkibidagi maxsus bo'limlar, Ichki ishlar vazirligi O'ninchi bo'limi, Axborot texnologiyalari va

[42] Демидов О. Вызовы кибербезопасности в Центральной Азии // Digital Report, 11 августа 2016. УРЛ: дигитал.репорт/олег-демидов-пир-центр-москва-вызовы-кибербезопасности-в-центральной-азии-2/(дата обращения:19.01.2020).

[43] Кутнаева Н. Кибербезопасность в Центральной Азии // Unipath. 20 августа 2015 года. URL: unipath-magazine.com/kiberbezopasnost-v centralnoj-azi/ (data obrashheniya: 25.01.2020).

kommunikatsiyalari Davlat qo'mitasi, I.Razzoqov nomidagi Qirg'iz davlat texnika universiteti Elektronika va telekommunikatsiyalar instituti huzuridagi, Mudofaa kengashi kotibiyati rahbarligida faoliyat yurituvchi AKT tadqiqotlari tahliliy markazi kabi yangi davlat tuzilmalari uchun ham Onlayn muhitda ekstremizmga qarshi kurash, raqamli tahdidlarni aniqlash, mamlakatning kibermudofaasini ta'minlash ustuvor vazifaga aylandi. Ularning barchasi, shuningdek, milliy internet makonini muhofaza qilish sohasida huquqiy normalar va yagona davlat siyosatini ishlab chiqishda ishtirok etdi. 2018-yil iyun oyida Qirg'iziston Prezidenti huzurida tuzilgan Raqamli transformatsiya bo'yicha ekspert kengashiga AKT sohasida qonunchilik va me'yoriy-huquqiy bazani yaratish bo'yicha turli bo'limlar ishini muvofiqlashtirish topshirildi [Qirg'izistonda kiberxavfsizlik. Raqamli transformatsiya masalalari bo'yicha Kengash tashkil etildi.[44]

Qirg'izistonda milliy kiberxavfsizlik tizimini shakllantirishning bunday trayektoriyasi to'g'risida ekspertlar juda qarama-qarshi fikrlarni bildirdilar. Bir tomondan, jarayonning haddan tashqari byurokratlashuvi hokimiyatning yuqori bo'g'inlari haligacha boshqaruvning an'anaviy modeliga sodiq bo'lib qolayotganini ko'rsatadi; bu holda hokimiyat qarorlarni AT sohasining yuqori malakali mutaxassislarini jalb etmasdan, shuningdek, fuqarolik sektori ishtirokisiz, ya'ni jamoat tashkilotlari va umuman mamlakat aholisini jalb etmasdan qabul qiladi.

Boshqa tomondan, Qirg'iziston axborot makonini himoya qilish uchun institutsional va me'yoriy bazaning jadal yaratilishi rivojlanayotgan raqamli sanoatning ahamiyatini davlat tomonidan tan olinishi, hokimiyatning bunday vaziyat bilan muloqotga kirishishga tayyorligi, idoralararo o'zaro hamkorlikni tartibga solish zarurligini ko'rsatdi; ayni paytda, funksiyalarning takrorlanishiga yo'l qo'ymaslik uchun javobgarlik sohalarini aniq belgilash, shuningdek, "axborot xavfsizligi" tushunchasining boshdan-oyoq

[44] Бердибаева А. Как Кыргызстан планирует бороться с киберугрозами? // DigitalReport. 4 апреля 2017. URL: digital.report/kak-kyirgyizstan-planiruetborotsya-s-kiberugrozami/ (дата обращения: 27.01.2020).

siyosiylashtirilgan talqinini qayta ko'rib chiqish zarurati e'tirof etildi.[45]

2019-yil avgust oyida "Qirg'iziston Respublikasining 2019–2023-yillarga mo'ljallangan axborot xavfsizligi konsepsiyasi" va uni amalga oshirish bo'yicha chora-tadbirlar rejasining qabul qilingani ushbu jarayondagi muhim qadam bo'ldi. Mazkur keng ko'lamli hujjat hukumatning o'tgan yillardagi barcha tashabbuslari va kiberxavfsizlik sohasidagi yutuqlarini amalda yagona bir tizimga jamladi. Strategiya mamlakatni axborot jihatidan himoya qilishning quyidagi bir qator yo'nalishlari va usullarini qamrab oldi: kompyuter jinoyatlariga qarshi kurashishning uslubiy yondashuvlari va huquqiy asoslarini belgilash, Qirg'iziston iqtisodiyoti va davlat boshqaruvini raqamlashtirish tamoyillari; texnik standartlashtirish va xalqaro hamkorlik masalalari, kiberxavfsizlik sohasida inson salohiyatini oshirish va h.k. Albatta bu, 2018-yil dekabr oyida Respublika Xavfsizlik Kengashi tomonidan qabul qilingan "Raqamli Qirg'iziston 2019–2023" raqamli transformatsiya dasturi Konsepsiyaning ajralmas qismi bo'ldi. Dastur davlat tilida milliy raqamli kontentni rivojlantirish, fuqarolar va tadbirkorlik subyektlariga elektron davlat xizmatlarini ko'rsatishni joriy etish va yanada yaxshilash, adliya, ta'lim, fan, madaniyat, sanoat va qishloq xo'jaligi va boshqa sohalarida avtomatlashtirilgan axborot tizimlarini yaratishga qaratilgan milliy loyihalar majmuidir.[46] Shu bilan birga alohida ta'kidlash joizki, Qirg'iziston jamiyati hayotining barcha jabhalarida raqamli texnologiyalarni keng joriy etishga qaratilgan keng ko'lamli huquqiy, tashkiliy, texnik va iqtisodiy chora-tadbirlarga qaramay, mamlakatning axborot xavfsizligi, davlat va fuqarolarning ijtimoiy-siyosiy xavfsizligi masalasida respublika hukumati o'zining asosiy yondashuv va tamoyillarini saqlab qoldi. Qirg'izistonning kiberstrategiyasida respublikaning

45 Демидов О. Вызовы кибербезопасности в Центральной Азии // Digital Report. 11 августа 2016. URL: digital.report/oleg-demidov-pir-tsentrmoskva-vyizovyi-kiberbezopasnosti-v-tsentralnoy-azii-2/ (дата обращения: 19.01.2020).

46 Концепция информационной безопасности Кыргызской Республики на 2019–2023 годы (к Постановлению Правительства КР № 209 от 3 мая 2019 года). URL: cbd.minjust.gov.kg/act/view/ru-ru/13652 (дата обращения: 19.02.2020).

AKT sohasidagi milliy manfaatlari "qonuniylik va huquq-tartibot normalariga rioya qilish, konstitutsiyaviy tuzum daxlsizligi, suverenitet va hududiy yaxlitlikni ta'minlash, iqtisodiy o'sishga, siyosiy va ijtimoiy barqarorlikka erishish" sifatida belgilangan deb aytish mumkin.

Boshqacha aytganda, milliy internet makonida ekstremizmga qarshi kurashish Qirg'iziston rasmiylari uchun ustuvor vazifa bo'lib qolmoqda. Shu bilan birga, AKT sohasidagi qonun loyihalarini ko'rib chiqish va qabul qilish algoritmi ularni ekspertlar va fuqarolik jamiyati vakillari bilan dastlabki muhokama qilish tartibini nazarda tutadi. Qirg'izistonning davlat va jamoatchilik o'rtasidagi o'zaro hamkorligi amaliyoti, kuzatuvchilarning fikricha, kiberxavfsizlik masalalarida milliy manfaatlar hamda raqamli muhitda fuqarolarning so'z erkinligi va shaxsiy makon huquqi o'rtasida murosa topish imkoniyatidan dalolat beradi.[47] Strategiyada "bolalar va o'smirlarni ularning sog'lig'i va rivojlanishiga zarar etkazuvchi axborotdan g'ayriqonuniy va ijtimoiy xavfli kontentdan himoya qilish" masalalariga alohida e'tibor qaratilgan, shuningdek, respublikaning yosh avlodi uchun xavfsiz onlayn muhitni yaratish maqsadida fan, ta'lim va madaniyat sohalari bo'yicha chora-tadbirlar kompleksi taklif etilgan. So'nggi yillarda raqamli makonda bolalarni himoya qilish birinchi darajali vazifa sifatida xalqaro kun tartibiga kiritildi. Shu bois Qirg'iziston tajribasini dunyoning ilg'or tajribalari qatoriga kiritish mumkin, chunki bu mamlakatda tegishli milliy loyihalar amalga oshirilmoqda, maktab, o'rta maxsus kasb-hunar va oliy ta'lim tizimiga kiberxavfsizlik, kompyuter savodxonligi va raqamli madaniyat bo'yicha fanlar joriy etilmoqda.

Qirg'iziston Respublikasi kiberxavfsizlikni ta'minlash milliy tizimi hozirgi paytda endi shakllanish bosqichiga qadam qo'ydi. Uning rivojlangan mamlakatlarga nisbatan biroz kechikib boshlanishi (bu 2000-yil oxiriga to'g'ri keladi) SSSR parchalanishi va umuman bipolyar dunyoning barbod bo'lishi natijasida yuzaga

47 Бердибаева А. Как Кыргызстан планирует бороться с киберугрозами? // DigitalReport. 4 апреля 2017. URL: digital.report/kak-kyirgyizstan-planiruetborotsya-s-kiberugrozami/ (дата обращения: 27.01.2020).

kelgan qiyinchiliklar, yosh davlat duch kelgan bir qator iqtisodiy, ijtimoiy-siyosiy, tarixiy va madaniy tahdidlar bilan izohlanadi. Global megatrend sifatida AKT ning jadal o'sishi Markaziy Osiyo mamlakatlarida xuddi shu sabablarga ko'ra o'zini namoyon qildi, ya'ni raqamli texnologiyalar imkoniyatlarining kengayishi tizimga qarshi bo'lgan radikal ekstremistik guruhlarning faollashuvi uchun Internet fazosida qulay zamin yaratdi. Hozirgi vaqtda dunyoning rivojlangan mamlakatlari muhim infratuzilma obyektlariga kiberhujumlar ko'rinishidagi eng yuqori darajadagi kibertahdidlarga duch kelishgan va o'z e'tiborini muammoning sof texnik jihatlariga qaratgan. Qirg'iziston va uning mintaqadagi qo'shnilarining milliy axborot himoyasini qurish yo'li ijtimoiy-siyosiy barqarorlikka putur yetkazish uchun onlayn muhitdan foydalanishga qarshi kurashish, shuningdek, xuddi shunday tahdidlar majmuasiga ega davlatlar bilan sa'y-harakatlarni muvofiqlashtirishdan boshlandi. Ana shunday holatlar tufayli Qirg'iziston va Markaziy Osiyoning boshqa mamlakatlarida axborotni himoya qilish milliy tizimini yaratish tashabbuskori obyektiv ravishda davlat bo'ldi. U esa, an'anaviy tarzda "yuqoridan pastga" qaratilgan sxema bo'yicha harakat qiladi, ya'ni mamlakatning raqamli mudofaa tizimiga avvalo davlat organlari, so'ng huquqiy-me'yoriy baza, milliy strategiya, so'ng xususiy sektor integratsiya qilindi. Markaziy Osiyo mintaqasida radikal islomiy tahdidning sezilarli darajada kamaygani bu yondashuv samaradorligidan dalolat beradi. Shu bilan birga, tan olish lozimki, axborot xavfsizligining ijtimoiy-siyosiy jihatlariga alohida e'tibor qaratilishi institutsional va huquqiy sohani ma'lum darajada "me'yoridan ortiqcha tartibga solish" tendensiyasini keltirib chiqardi. Bu holatda kiberxavfsizlik tizimining boshqa muhim tarkibiy qismlariga, chunonchi texnikaviy, tashkiliy masalalarga yetarli e'tibor berilmaydi. Mamlakatni raqamlashtirishning juda tez sur'atlar bilan borishi pirovardida kibertahdidlar spektrining kengayishiga va yuqori darajaga chiqishiga olib keldi. Bu holat Qirg'iziston hukumatini shunday bo'shliqlarni to'ldirish jarayonini tezlashtirishga majbur qildi. Bugun Qirg'izistonda hokimiyat, xususiy sektor va fuqarolik jamiyati o'rtasida o'zaro hamkorlik

mexanizmlari faol yaratilmoqda. Bu yo'nalishdagi eng muhim qadamlar mamlakat rahbariyati tomonidan so'nggi ikki yil ichida amalga oshirildi. Bu esa qisqa muddatda Global xavfsizlik indeksida Qirg'iziston Respublikasi reyting ko'rsatkichlari bo'yicha yuqori o'rinlarga ko'tarilishiga imkon yaratmoqda.

Tojikiston Respublikasi

Tadqiqotlarga ko'ra, kiberxavfsizlik bo'yicha Tojikiston dunyodagi eng kam himoyalangan mamlakat bo'lib, undan keyin Bangladesh va Xitoy o'rin olgan. Tojikiston bank zararli dasturlari hujumiga uchragan foydalanuvchilar (4,7 foiz), mahalliy zararli dasturlardan kamida bitta hujumga uchragan kompyuterlar (41,16 foiz) va kriptomaynerlarning hujumlari (5,7 foiz) bo'yicha eng yomon ko'rsatkichlarga ega mamlakat bo'ldi. Shuningdek, u tovlamachi-troyan hujumiga uchragan foydalanuvchilar mezonida ham yomon natija qayd etdi (1,35 foiz). Shu bilan birga, u bir nechta mezonlar bo'yicha eng yaxshi natijalarga erishgan mamlakatlardan biri bo'ldi, jumladan, kelib chiqqan mamlakat bo'yicha veb-manbalar orqali hujum qilingan foydalanuvchilar (0,03 foiz), Telnet orqali qilingan hujumlar (0,01 foiz), spam-xabarlar (0,01 foiz), shuningdek, zararli pochta jo'natmalari qamrab olingan mamlakatlar foizi bo'yicha (0,01 foiz). Hech bir foydalanuvchi mobil tovlamachi-troyanlar tomonidan hujumga uchramagan va SSH ga asoslangan hujumlarning hech biri Tojikistondan kelib chiqmagan.[48]

Tojikiston Respublikasi 2003-yil 7-noyabr kuni mintaqa davlatlari ichida birinchi bo'lib Axborot xavfsizligi konsepsiyasini qabul qildi.[49] Aynan mazkur konsepsiya mamlakatda axborot sohasidagi muayyan maqsadlarni aks ettiradi. Axborot xavfsizligini ta'minlash vaziyatlari, yo'nalishlari, davlatning ichki va tashqi siyosat sohasidagi strategik maqsadlarini ifoda etadi.

[48] Dunyo davlatlarining kiberxavfsizlik reytingi.// https://www.xabar.uz/

[49] Указ Президента Республики Таджикистан от 7 ноября 2003 года №1175 «О Концепции информационной безопасности Республики Таджикистан// https: // www.google.ru/url?sa=t&rct=j&q=&esrc=s&source=web&cd=1&ved= 0ahUKEwjPt7S S7rrVAhUIfhoKHfE8AYwQFggmMAA&url=http%3A%2F%2Fnansmit.tj%2F20968-2%2F%3Fid%3D15325&usg=AFQjCNFVPJAoTk-iQvlc9C5P0-jDJPmy6Q

Mazkur konsepsiyada Tojikistonning axborot sohasidagi milliy manfaatlarini, har bir shaxsning muvozanatli manfaatlari majmuyi bilan belgilanishini, jamiyat va davlat uning axborot xavfsizligini ta'minlashi belgilangan.

Shuningdek, 2003-yilda ham qabul qilingan Tojikiston Respublikasining axborot-kommunikatsiya texnologiyalarini rivojlantirish bo'yicha "Tojikiston Respublikasining axborot kommunikatsion texnologiyalarni rivojlantirish" bo'yicha Davlat strategiyasi qabul qilindi.[50] Ushbu davlat strategiyasi Tojikistonning jahon hamjamiyati va axborot maydonidagi integratsiyasini nazarda tutgan edi. Xususan, unda davlatning raqamli tafovutlarni hal etish borasidagi maqsadlari aniq belgilab berilgan edi. Bu nafaqat Markaziy Osiyo mintqasi, balki MDH makonini ham nazarda tutadigan normativ-hujjat hisoblanadi. Undan tashqari mamlakatda kiberxavfsizlikni ta'minlash bo'yicha ham bir qancha normativ-hujjatlar qabul qilingan ediki, ular ham mamlakat milliy xavfsizligini ta'minlashga qaratilgan edi. Tojikiston Respublikasining "Axborot to'g'risida"gi va "Axborotni himoya qilish to'g'risida"gi, "Davlat sirlari to'g'risida"gi, "Tijorat sirlari to'g'risida"gi qonunlari shular jumlasidandir.

2008-yil 30-aprelda Tojikiston Respublikasi Prezidenti Qarori bilan "Davlatning axborot sohasidagi konsepsiyasi"[51] qabul qilindi va tasdiqlandi. Ushbu konsepsiyada mamlakatning kiberxavfsizligini ta'minlash, zamonaviy axborot texnologiyalarini boshqaruv jarayoniga tatbiq etish orqali boshqaruv qarorlarining sifatini oshirish, axborot oqimi xavfsizligini saqlash, iqtisodiyotda barqaror o'sishni ta'minlash, hukumat bilan aholi o'rtasidagi munosabatni barqarorlashtirish hamda axborot siyosatining obyektlarini aniqlash, jamiyat, davlat va manfaatlari yo'lida axborotni targ'ib qilish va qo'llash nazarda tutilgan.

[50] Указ Президента Республики Таджикистан от 5 ноября 2003 г. № 1174 "О Государственной стратегии "Информационно-коммуникационные технологии для развития Республики Таджикистан" // http://cis.rudn.ru/doc/255

[51] Указ Президента РТ "Об утверждении Концепции Государственной информационной политики" от 30 апреля 2008 г. №451 //https://www.google.ru/url?sa=t&rct=j&q=&esrc=s&source=web&cd=3&ved=0ahUKEwiv1aSt8_3RAhVoIJoKHZo8CvgQFgglMAI&url=http%3A%2F%2Ffilial-nic-mkur.tj

Mamlakatning kiberxavfsizligini ta'minlash maqsadida 2016-yil 1-oktayabrdagi "Tojikiston Respublikasining 2030-yilgacha Milliy rivojlanish strategiyasi"[52] ham qabul qilindi. Ushbu srategiya axborot qurilmalari faoliyatini rivojlantirish orqali "Elektron hukumat"ni joriy etishga qaratilganligi bilan ajralib turadi. Bu borada tojikistonlik siyosatshunos A.X. Ibodov takidlaganidek, "Davlatning axborot xavfsizligini ta'minlashga qaratilgan siyosati hayotiy vazifalarni hal etishda asos vazifalarini bajarganlikdan dalolat beradi".[53]

Turkmaniston Respublikasi

Raqamli dunyo maydonining kengayib borishi bilan xavfsizlik sohasida kiberxavfsizlik masalalarini o'rganuvchi yangi yo'nalish paydo bo'ldi. Kiberxavfsizlik turli xalqaro institutlar talqinida yoki neytral qabul qilingan axloqiy me'yorlarga va texnikaviy ifratuzilmalarga asoslangan bilimlarga tayanadi. Kiberxavfsizlik tezda texnik intizomdan strategik dasturga aylandi. Lekin nazariy rivojlanish hali-hamon boshlang'ich bosqichda turibdi. Faqatgina 2013-yilga kelib bu borada dastlabki hujjat qabul qilingan. 2013-yil 4-mayda "Turkmanistonning milliy xavfsizligi to'g'risida"gi Qonuni qabul qilingan.[54] Aynan mazkur hujjatda axborot makoniga hudud sifatida qaralib, uni shakllantirish, yaratish bilan bog'liq faoliyat, o'zgartirish, qayta ishlash, uzatish, foydalanish, saqlash, axborot infratuzilmasiga ta'sir etuvchi ma'lumotlar va jumladan, individual va ijtimoiy ongga ta'siri masalasini himoya qilish vazifalari belgilangan. Aynan shu tartibda belgilanishiga sabab, 1995-yilda qabul qilingan "Davlat sirlari to'g'risida"gi Qonunga

[52] Национальная стратегия развития Республики Таджикистан на период до 2030 года. Утв. Постановлением Правительства РТ от 1 октября 2016 г., № 392 // URL: http://www.tajikngo.tj/en/-mainmenu-51/item/3105-natsionalnaya-strategiya-razvitiya-respubliki-tadzhikistan-na-period-do-2030-goda.html

[53] Ибодов А.Х. Информационная безопасность: новые вызовы и угрозы в процессе перехода к информационному обществу (на материалах Республики Таджикистан): Дис. канд. полит. наук. – Душанбе, 2015. – С.32

[54] Закон Туркменистана "О национальной безопасности Туркменистана" от 4 мая 2013 г. №388-IV (в редакции от 18 июня 2016 г. №414-V) // http://base.spinform.ru/ show_doc.fwx?rgn=65978

ko'ra, aynan mamlakatda axborot uzatish va chiqib ketish masalasi qattiq senzura sifatida taqiqlangan edi. Ya'ni axborot uzatuvchi barcha kanallar nazorat qilib turilgan edi.

Turkmaniston Respublikasining 2012-yil 22-dekabrda qabul qilingan "Ommaviy axborot vositalari to'g'risida"gi Qonunida[55] axborot tarqatuvchi manbalar belgilab berilgan. Shundan so'ng bu boradagi islohotlarda liberallashtirish jarayoni boshlangan.

2016-yil 14-sentyabrda mamlakat siyosiy hayotida yangi konstitutsiya qabul qilingandan so'ng "Har kim erkin axborot olish va izlash huquqiga egaligi, Qonun hujjatlarida taqiqlanmagan tartibda axborotni tarqatish mumkin ekanligi, davlat yoki boshqa qonun bilan himoyalanganlar bundan mustasnoligi"[56] belgilandi. Shu tariqa mamlakat mintaqa va jahon axborot maydonida ochila boshladi.

2019-yil 6-sentyabrda Turkmaniston Prezidenti "Kiberxavfsizlik to'g'risida"gi Qonunni imzolagan va o'sha yilning 9-sentyabrida Kiberxavfsizlik xizmatini tashkil etgan. Shu bilan birga, Turkmanistonda 2022–2025-yillarga mo'ljallangan kiberxavfsizlikni ta'minlash bo'yicha Davlat dasturi tasdiqlangan.

2022-yilda Ashxobodda "Markaziy Osiyo mintaqasida iqlim o'zgarishi, suvdan foydalanish, oziq-ovqat xavfsizligi va axborot-kommunikatsiya texnologiyalari bo'yicha mintaqaviy hamkorlikning dolzarb jihatlari" mavzusida beshinchi Markaziy Osiyo ekspertlar forumi bo'lib o'tdi.[57] Ushbu forumda Turkmaniston tashqi ishlar vazirligi xalqaro aloqalar instituti strategik tadqiqotlar ilmiy markazi tomonidan BMT ning mintaqaviy Preventiv diplomatiya markazi ko'magida tashkil etildi. Mintaqaning yetakchi ekspertlarining bunday keng ko'lamli forumi mamlakatlarni yanada yaqinlashtirish va hamkorlikning barcha jabhalarida mintaqaviy hamkorlikni

[55] Закон Туркменистана "О правовом регулировании развития сети Интернет и оказания интернет-услуг в Туркменистане" от 20 декабря 2014 г., № 159-V// http://www.wipo.int/wipolex/ru/text.jsp?file_id=398876

[56] Конституция Туркменистана (новая редакция). Утверждена Конституционным Законом Туркменистана от 14 сентября 2016 г. №448-V // http://www.base.spinform.ru/ show_doc.fwx?rgn=89543

[57] https://turkmenistan.gov.tm/ru/post/68980/informacionnaya-bezopasnost-prioritetnaya-zadacha-centralnoaziatskogo-regiona

chuqurlashtirishning ilg'or jarayoni mavzusida bo'lib o'tdi. Tadbirdan ko'zlangan maqsad mintaqaviy hamkorlikni ta'minlashning dolzarb masalalarini muhokama qilish, kelishilgan yo'nalishlarda mintaqa davlatlari hukumatlari uchun umumiy strategik yondashuvlar, amaliy taklif va tavsiyalar ishlab chiqishdan iborat bo'ldi.

Ushbu forumda Turkmaniston Respublikasi Prezidenti Serdar Berdimuhamedov so'zga chiqib, Markaziy Osiyo mintaqasi uchun zamonaviy chaqiriq va tahdidlarni, jumladan, jahondagi asosiy muammolardan biri bu xavfsizlik sektori ekanligini belgilab, "axborot texnologiyalaridan noqonuniy ravishda yot g'oyalar yaratish va Markaziy Osiyo xalqlarining tarixiy an'analari, asosiy qadriyatlari va hayotining ko'p asrlik negizlariga zid bo'lgan munosabat"ni alohida ta'kidlagan edi. Shu bilan birga, Turkmaniston rahbari o'z nutqida, jumladan, Markaziy Osiyo barqarorlik va farovonlik muhitida rivojlanishni davom ettirish maqsadida axborot texnologiyalaridan noqonuniy foydalanishga qarshi kurashish uchun birgalikda harakat qilish, besh davlat uchun yaxlit xavfsizlik tizimini barpo etish zarurligini ta'kidladi. Aynan ushbu forumda mintaqa davlatlarining barcha mutaxassislari so'zga chiqib, ushbu masala bo'yicha bir xil prinsipial pozitsiyaga amal qilish masalasida o'z fikrlarini ta'kidlab o'tgan. Xususan, O'zbekiston Respublikasi Prezidenti huzuridagi strategik va mintaqalararo tadqiqotlar instituti direktorining o'rinbosari Akramjon Ne'matov o'z chiqishlarida quyidagilarni ta'kidladi: "Axborot-kommunikatsiya texnologiyalari zamonaviy jamiyat hayotida tizim yaratuvchi omilga aylandi. Ular siyosiy, ijtimoiy, iqtisodiy, harbiy va boshqa xavfsizlik sohalariga ta'sir ko'rsatmoqda".[58] Bu fikrlar mintaqa davlatlari uchun kiberxavfsizlik masalasi jamiyatning barcha sohalariga ta'sir etayotgaligidan dalolat beradi.

2023-yilning yanvarida xavfsizlik Kengashining yakuniy yig'ilishida Turkmaniston Prezidenti "Turkmanistonning kiberxavfsizligini ta'minlash Davlat dasturini tasdiqlash to'g'risida"gi qarorini imzoladi.[59] Turkmaniston poytaxti Ashxobodda joylashgan

[58] https://turkmenistan.gov.tm/ru/post/68980/informacionnaya-bezopasnost-prioritetnaya-zadacha-centralnoaziatskogo-regiona

[59] Об этом сообщает госинформагентство. "Туркменистан сегодня", 2023.

telekommunikatsiya va Informatika institutida kiberxavfsizlik bo'yicha yangi markaz ochildi. Markazning vazifasi Turkmaniston hukumati kiberxavfsizligini takomillashtirish borasidagi sa'y-harakatlarini qo'llab-quvvatlash va institutga kibertahdidlarning oldini olishda ko'mak berishdir. Aynan bu vazifalarni amalga oshirishda asosiy idora Turkmaniston Aloqa vazirligi (Ministry of Communications) bo'lib, u telekommunikatsiyalarni rivojlantirish siyosatini amalga oshiradi va uni rivojlantirish yo'nalishlarini belgilaydi.

Axborot texnologiyalari sohasidagi kiberhujum va noqonuniy tahdidlarga qarshi kurashish bo'yicha aniq takliflar Turkmaniston Prezidenti huzuridagi Davlat boshqaruvi Akademiyasi ijtimoiy Fanlar kafedrasi professori, Sotsiologiya fanlari doktori Ovezberdi Muhametberdiyev tomonidan ham bildirildi. U o'z nutqida, xususan, quyidagilarni ta'kidladi: "Yigirma birinchi asrning boshlariga kelib, ko'plab global xavfsizlik muammolari – tabiiy va texnogen ofatlar, epidemiyalar va qurolli to'qnashuvlar bilan hali to'liq kurasha olmagan insoniyat yana bir tahdid – kibermakondagi barcha turdagi ma'lumotlarni qamrab olgan murakkab hujumlar tahdidiga duch keldi. Leksikonimizda yangi atama paydo bo'ldi, bu – "kiberxavfsizlik" muammosidir, deb ta'kidlagan edi.

Umuman Markaziy Osiyo davlatlari hamkorligida kiberxurujlarga qarshi normativ hujjatlar ishlab chiqilayotgan bo'lsa-da, haligacha kiberhujumlar davom etayotganligi masalaning eng nozik tomoni bo'lib qolmoqda. Masalan, Markaziy Osiyo mamlakatlari kiberjinoyatchilikning kundalik ko'rinishlariga tobora ko'proq duch kelmoqdalar. Jumladan, Qozog'iston Respublikasi dunyoda spamlar soniga ko'ra 18-o'rinda, veb-serverga xavfi bo'yicha 7-o'inda turibdi. 2010-yilda internetdan foydalangan Qozog'iston fuqarolarining deyarli yarmi onlayn hujumlar nishoniga aylangan, bu ko'rsatkich 2011-yilda 47 foizga oshganligini ko'rsatadi. Kasperskiy xavfsizlik tarmog'i ma'lumotlariga ko'ra, Qozog'iston Markaziy Osiyoda Internet hujumlarining 85% nishoniga aylandi, solishtirish uchun O'zbekistonda 8%, Qirg'izistonda 4%, Turkmanistonda 2% va Tojikistonda 1%. Yaqin vaqtlargacha yirik kiberhujumlar asosan moliyaviy ma'lumot olish uchun hukumat saytlariga qaratilgan edi. Ushbu hujumlar raqamli infratuzilmaning

rivojlanishiga mutanosib ravishda o'sdi va Qozog'iston Markaziy Osiyoda bunday hujumlarning asosiy nishoniga aylandi.[60] Bundan ko'rish mumkinki, ushbu kiberhujumlarni uyushtirayotgan xakerlar asosan foydali moliyaviy va sanoat ma'lumotlarini olishga intilayotgan mahalliy uyushgan jinoiy guruhlardir. Shundan ham ko'rish mumkinki, mintaqa davlatlari kiberxavfsizlikni to'liq va yaxlit ta'minlamaganligini ko'rishimiz mumkin. Shu sababli ham bu borada hamkorlikda yechilishi kerak bo'lgan amaliy priventiv choralarga zaruriyat bor, deb o'ylaymiz. Chunki, kiberxavfsizlik vosita sifatida milliy xavfsizlik tizimiga tahdid solayotgan bir pallada mintaqa davlatlari oldida turgan o'zaro ishonch va hamkorlikka asoslangan tizim yaratishga zaruriyat sezilib borayotganligini ko'rsatadi.

Xulosa o'rnida aytish kerakki, Markaziy Osiyo mintaqasi davlatlari kiberxavfsizlik muammosiga birgalikda ahamiyat berishlari lozim:

– ushbu makonda xalqaro huquqning umume'tirof etilgan tamoyillariga rioya qilish;

– kompyuter xavfsizligi sohasidagi tadqiqotlar va ishlanmalarni muvofiqlashtirish va qayta yo'naltirish;

– mavjud kompyuter xavfsizligi markazlarining vaziyatli xabardorligini oshirish;

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

– kompyuter xavfsizligi bo'yicha ta'lim dasturlarini joylashtirish;

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

Ushbu sohadagi xalqaro strategiyaning maqsadlaridan biri – kiberxavfsizlik ishlanmalari samaradorligidan bir necha baravar yuqori bo'lgan va keyingi 5–10 yil ichida amalga oshirilishi mumkin bo'lgan tizimlar bilan ta'minlaydigan texnologiyalarni ishlab chiqishdir.

[60] Марлен Ларюэль. Кибербезопасность в Центральной Азии: реальные угрозы, ложные предлоги? Аналитических обзор.//2012 г. №2. Екатерина Исакова "Хакеры выбирают Казахстан". Kursiv.kz, 21 октября 2010 г., http://www.kursiv.kz/hi-tech/hitechweekly/1195205432-xakery-vybirayutkazaxstan.html.

Birinchi bob bo'yicha xulosalar

Fuqarolarni kiberhujumlardan himoyalash uchun ommaviy axborot vositalarida, axborot tarqatuvchi qurilmalarda va elektron pul o'tkazmalari jarayonlarida himoyalovchi kod (parol)lardan foydalanish zarur. Ushbu kod sir saqlanishi, qurilmalardagi antivirus dasturlari doimiy ravishda faollashtirib borilishi kerak.

O'zbekiston raqamli iqtisodiyotga asta-sekin o'tmoqda. Bunday sharoitda ma'lumotlarni saqlash, yetkazish, qayta ishlashda xavfsizlik va barqarorlik muhim omil hisoblanadi. Bu borada, ayniqsa, davlat organlari xodimlaridan mas'uliyat va e'tibor talab etiladi. Aholi, yoshlar o'rtasida, jamoalarda kiberxavfsizlik mavzusidagi seminarlar tashkil etish lozim. Bu kabi tadbirlar dastur buzuvchi (xaker)larning muntazam kichik hujumlarini bartaraf etishga yordam beradi.

Umuman olganda, O'zbekistonda kiberxavfsizlikni ta'minlash bo'yicha olib borilayotgan tizimli va fundamental yondashuv, yagona normativ-huquqiy hujjatlar bazasini yaratish, ilg'or xorijiy tajribani joriy etish, innovatsion usullardan keng foydalanish davlat axborot siyosatini samarali olib borishga hamda axborot xavfsizligi sohasidagi muammolarni hal etishga xizmat qiladi.

Bu esa axborot kommunikatsiya va texnologiyalari tizimini zamonaviy kibertahdidlardan himoya qilish, turli darajadagi tizimlar uchun kiberxavfsizlik bo'yicha zamonaviy mexanizmlarni joriy etish, mazkur sohada davlat organlari, korxonalar, tashkilotlarning huquqlari va majburiyatlarini belgilash, ularning faoliyatini muvofiqlashtirish kabilarni amalga oshirish orqali belgilanadi. Bu sohadagi normativ-huquqiy hujjatlarni unifikatsiyalash orqali kiberxavfsizlikni ta'minlashni takomillashtirish mumkin.

Yurtimizda olib borilayotgan barcha islohotlar zamirida xalqimizga qulayliklar yaratish maqsadi yotibdi. Kiberxavfsizlikni ta'minlashga alohida e'tibor qaratilishi raqamli imkoniyatlardan ishonchli va xavfsiz tarzda foydalanishga asos bo'ladi.

II BOB. MARKAZIY OSIYO DAVLATLARI XAVFSIZLIGIGA KIBERMAKONDA VUJUDGA KELAYOTGAN ZAMONAVIY TAHDIDLAR

Axborot makonida turli axborot manbalarining bir-biriga qarshi o'zaro kurashi o'z navbatida qaysidir davlatga yoki qaysidir siyosiy jarayonga qarshi axborot xurujini yuzaga keltiradi. Bugungi kunda axborot xuruji bir vaqtning o'zida bir necha yo'nalishlarda: iqtisodiy, siyosiy, harbiy, ijtimoiy sohalarda olib borilmoqda.

Axborot xurujining asl mohiyati inson ongini voqelikdan chalg'itish, qalbi va ongini yemirish, uni o'z asoratiga solish, psixologik qaramlik holatiga keltirishga qaratilgan. Shu ma'noda ushbu hodisa madaniy ekspansiyani amalga oshirishning hozirgi zamonda eng keng tarqalgan va tez ta'sir o'tkazuvchi vositasi, deb aytish mumkin. Zero, XXI asrni bejizga "Axborot asri" deb atashmagan. Shu boisdan ham AQSh axborot-psixologik xurujlar nazariyasi tadqiqotchilaridan biri Uinn Shvartou ochiqchasiga "Zamonaviy jamiyat axborotga asoslanganligi sababli, ertami, kechmi, har kim axborot xurujining qurboniga aylanadi", deb ta'kidlab o'tgan edi. Hozirda barcha davlatlar uchun yoshlar ongini destruktiv g'oyalar ta'siridan asrash va ta'sirini minimallashtirish dolzarbligicha qolmoqda. Mazkur bob "Markaziy Osiyo davlatlari xavfsizligiga kibermakonda vujudga kelayotgan zamonaviy tahdidlar" deb nomlangan bo'lib, unda "Destruktiv g'oyalarning kibermakonda tarqatilishi va uning salbiy jihatlari", "Xorijiy davlatlarning kiberterrorizm va ekstremizmga qarshi kurash yo'nalishidagi tajribasi va uni mintaqaviy hamkorlikka ta'siri" va "Markaziy Osiyo mintaqasining yoshlar qatlamiga ijtimoiy tarmoqlar orqali ta'sir ko'rsatayotgan kiberxurujlar va ularni bartaraf etish texnologiyalari" tahlil etiladi.

2.1. Destruktiv g'oyalarning kibermakonda tarqatilishi va uning salbiy jihatlari

Insoniyat tarixining har bir davridagi kishilik jamiyatida ijtimoiy destruktiv holatlar o'ziga xos shaklda namoyon bo'lgan. Davrlar o'tishi bilan progress, taraqqiyot, pozitivlik, bunyodkorlik naqadar jadallashsa, regress, tanazzul, negativlik, vayronkorlik ham shu qadar ildiz ota bordi. Bugungi kunda vujudga kelayotgan ijtimoiy muammolar va negativ holatlar o'zining o'ta murakkab tabiati, oqibatlari ko'lami bilan jiddiy tashvish tug'dirmoqda. Shu munosabat bilan destruktiv holatlarning shakllanishi qonuniyatlarini aniqlash, buning uchun esa mazkur jarayonlarning mohiyati va sabablariga doir mulohazalarni umumlashtirish zaruriyati yuzaga kelmoqda.

Ushbu paragrafda destruktiv g'oyalarning kibermakonda tarqalashi va uning salbiy jihatlarini ochib berishdan oldin "destruktiv" tushunchasi va uning holat sifatidagi falsafiy-siyosiy mazmuniga e'tibor qaratishni lozim topdik. Sababi, "destruktiv" tushunchasi dastlab diniy qarashlar va manbalar asosida shakllangan va rivojlangan degan konseptni ilgari suramiz.

Ma'lumki, tabiat, jamiyat va inson borlig'idagi destruktiv holatlar to'g'risidagi ilk g'oyalarni diniy manbalarda uchratish mumkin. Masalan, zardo'shtiylikda olam taraqqiyoti, umuman olganda, ezgulik va yaxshilikka bo'lgan intilish sifatida tasavvur qilinadi: qachondir ezgulik xudosi Axuramazdaning mutlaq hukmronligi ta'minlanishi, ezgulik va adolat qaror topishi aniq. Lekin ezgulikning ilk shakllari (osoyishta hayot, bunyodkorlik, obodonchilik va sh.k.) vujudga kelgani zahoti unga qarama-qarshi o'laroq yovuzlik shakllari (qurg'oqchilik, qurbonliklar, urushlar, kasalliklar va sh.k.) ham paydo bo'ladi.[61] Zardo'shtiylikda barcha destruktiv holatlarning muallifi mavjud – bu ruhlantiruvchi kuch Ahriman obrazi bilan bog'lanadi. Ahriman barcha yovuz kuchlarning manbai, ilhomchisi hisoblanadi: u goho odamlarni yovuzlik bandisiga aylantiradi (Zahhokni taxtga o'tqizgani kabi),

[61] Qarang: Mahmudov T. "Avesto" haqida. – T.: "Sharq", 2000.

goho ularni to'g'ri yo'ldan chalg'itadi (Jamshidni yo'ldan urgani kabi).[62]

Xristianlik dinida destruktiv holatlar mustaqil substansiya sifatida emas, turli jarayonlarning buzilishi tarzida tasavvur qilinadi. Xudo materiyani yaratdi, uni turli shakllarga soldi, turfa xususiyatlar bilan to'ldirdi. Uning barcha yaratuvchanlik harakatlari ezgulik bilan yo'g'rilgan, binobarin, uning tomonidan bunyod etilgan borliqning o'zi ham ezgulikdir.

Biroq ushbu ezgulikni yemiruvchi, vayron qiluvchi holatlar, jarayonlar mavjud. Aynan ana shu holat va jarayonlar yovuzlik sifatida talqin qilinmog'i darkor. Yovuzlik ibtidodan yaratilgan mustaqil voqelik emas, u Xudo tomonidan bunyod etilgan narsalarning buzilishi, vayron qilinishidir. Masalan, Xudo odamni o'z qiyofasiga ko'ra erkin mavjudot qilib yaratdi, uni ezgu ishlarga oshno qildi. Lekin odam bolasi gunohga botib, Xudodan yuz o'girdi, yovuzlik sari yuz tutdi. Shu ondan boshlab, xristian dini talqiniga ko'ra, uning barcha qilmishlari destruktiv xarakter kasb qilmoqda.[63]

Islomda yovuzlik ko'proq insonning salbiy xatti-harakatlari bilan bog'lab talqin qilinadi. Islom dini aqidalariga ko'ra, inson hayotining maqsadi Allohga ishonish, Uni bilish, Unga mehr qo'yish va ibodat qilish orqali ma'naviy yuksaklikka erishish bilan bog'liq. Odam bolasini ana shu yo'lda muqim saqlovchi har qanday manba ezgulik, yo'ldan ozdiruvchi har qanday holat esa yovuzlikdir. Yovuzlik mohiyatini bilish birmuncha murakkab, unga yolg'iz Allohgina qodir. Shu bois Qur'oni Karimning "Baqara" surasida: "Balkim, sizlar yoqtirmagan narsa (aslida) o'zlaringiz uchun yaxshi, yoqtirgan narsangiz esa (aslida) sizlar uchun yomon bo'lib chiqar. Alloh bilur, sizlar esa bilmaysizlar", deb ta'kidlanadi.[64] Ko'rinadiki, islom talqinida, Allohni tanishga eltuvchi noxushlik (masalan, kasallik – agar inson uni sabr bilan yengsa) ezgulikka,

[62] Qarang: Firdavsiy A. Shohnoma. – T.: A.Navoiy nomli O'zbekiston Milliy kutubxonasi nashriyoti, 2012.

[63] Qarang: Августин А. О свободе воли. Книга 2.// Антология средневековой мысли. В двух томах. Том 1.- СПб.: РХГИ, 2001. – С.19–112.

[64] Qur'oni Karim. Baqara surasi. 216-oyat // Qur'oni Karimning mashhur suralari fazilati/ Nashrga tayyorlovchilar: A.Ahmad, I.Nurulloh. – T.: G'.G'ulom nomidagi Adabiyot va san'at nashriyoti, 2021. – B.119.

yaxshilik bo'lib ko'ringan holat (masalan, boylik – agar u insonni gunohga yetaklasa) yovuzlikka xizmat qiladi[65].

"Kibermakon" tushunchasiga ta'rif bizning amaldagi qonunchiligimizda ko'rsatib o'tilmagan, MDH davlatlarida ham mazkur atamaning rasmiy ta'rifi keltirilmagan. Rossiya Federatsiyasi "Kiberxavfsizlik konsepsiyasi" loyihasida mazkur tushuncha izohlangan bo'lib, unga ko'ra, kibermakon – Inson faoliyati turlarida (shaxs, tashkilot, davlat) foydalanadigan "Internet" va boshqa telekommunikatsiya tarmoqlari hamda ular faoliyatini ta'minlaydigan texnologik infratuzilmalar yig'indisidan iborat makon, informatsion makonning faoliyat maydoni.[66]

"Virtual makon" termini ham qamroviga ko'ra katta hajmga ega bo'lib, "virtual" so'zi "xayoliy" so'zi bilan sinonim hisoblanadi, u kompyuter texnikasi yordamida yaratilgan makon bilan chegaralanmaydi. "Internet makoni" esa tor ma'noga ega, chunki Internet bilan parallel ravishda kichik, axborot va telekommunikatsiya tarmoqlari ham mavjud ("FidoNet"). Shuningdek, "Internet" – bu nom va ehtimol, kelajakda boshqa global axborot va telekommunikatsiya tarmog'i uning o'rnini egallashi, boshqa nom bilan atalishi mumkin, ammo kibermakon o'zgarmasdan qoladi.

AQSh da ushbu tushunchaga ta'rif 1997-yilda ilk bor rasman Oliy sud qarorida keltirilgan va unda "Internet – jismoniy va yuridik shaxslarning interfaol muloqotiga xizmat qiladigan, egasi hamda foydalanuvchisini aniqlash murakkab bo'lgan axborot resurslari va kompyuter tarmoqlarining global birlashmasi" sifatida talqin etilgan.

Kibermakon esa Internet tarmog'i orqali dunyoning istalgan joyidan har qanday kishi kirish huquqiga ega bo'lgan geografik kenglikda joylashmagan, yagona, o'xshashi bo'lmagan makon sifatida yoritilgan.[67]

[65] Qarang: Благие дела: добро и зло в исламе.// https://www.islam-love.ru.

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

[67] Вылков Р.И. Киберпространство как социокультурный феномен, продукт технологического творчества и проективная идея: дис. канд. фил. наук. – Екатеринбург, 2009. – С.128. 129.

Internet global tarmog'ida yaratilgan kibermakonda foydalanishning qulayligi va tezkorligi, uning keng tarqalganligi hamda anonimligi an'anaviy jinoyatchilikdan yangi jinoyatchilik turi shakllanishiga sharoit yaratib berdi. Global tarmoq jinoyatchiligi tushunchasi unga qadar mavjud bo'lgan "kompyuter jinoyatchiligi" tushunchasi bilan to'la mos kelmaydi va shunga ko'ra, mazkur jinoyatchilik turi bugungi kunda "kiberjinoyatchilik" tushunchasi bilan atalib kelinmoqda.

Xalqaro ilmiy va huquqiy amaliyotda dastlab "kompyuter jinoyatchiligi" tushunchasi, keyinchalik "kompyuter bilan bog'liq jinoyat",[68] "kompyuter orqali jinoyat sodir etish", "elektron jinoyatchilik" va "yuqori texnologiyalar jinoyatchiligi", "virtual jinoyatchilik" tushunchalari ishlatilib, bugungi kunga kelib esa "kiberjinoyatchilik" yoki global tarmoq jinoyatchiligi atamasi qo'llanilmoqda.

Bugungi kunda kibermakonda tarqalayotgan "kompyuter jinoyatchiligi" tushunchasini uning uch muhim xususiyati bilan izohlangan, ya'ni 1) kompyuter – jinoyat maqsadi bo'lgan jinoyatlar, 2) kompyuter – jinoyatni sodir etish vositasi hisoblangan jinoyatlar, 3) tasodifiylikda undan oddiy jism sifatida foydalanib sodir etilgan jinoyatlar.[69]

Xususan, dastlab, Xitoy, AQSh va Singapurda "kompyuter jinoyati" tushunchasi yaratildi va ilk bor 1984-yilda AQSh da "Kompyuter firibgarligi va uni suiiste'mol qilish haqida" Qonun qabul qilindi.[70] Internet jahon axborot tarmog'i inson hayotiga kirib kelganidan so'ng esa "kompyuter jinoyati" tushunchasi o'zgartirilib, ushbu sohaga global tarmoq jinoyatchiligi ham kiritilib, umumiy nom bilan "kiberjinoyatchilik" atamasi yaratildi. Yevropa Ittifoqi tomonidan 2001-yilda qabul qilingan "Kiberjinoyatchilik to'g'risida"gi Konvensiya orqali dunyo hamjamiyatida "kiberjinoyatchilik" tushunchasi shakllantirilganligi

[68] Richard C. Crime by Computer: correlations of software piracy and unauthorised account access // Security Journal. №4–1.1993. –C.2–12.

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

[70] https://www.congress.gov/bill/98th-congress/senate-bill/2864

rasman tan olindi. Oxirgi yillarda mazkur Konvensiya asosida milliy qonunchilikka o'zgartirish kiritayotgan davlatlar soni oshib bormoqda.

Ilmiy adabiyotlarda "destruktiv g'oya" tushunchasiga ta'riflar mavjud, ammo ularda mazkur tushunchani anglashda yakdillik yo'q. Uning o'zagini "destruktivlik" tushunchasi tashkil etadi va belgilari amaliyotda ko'zga tashlanadi. Ammo aynan destruktivlik falsafada yetarli tadqiq etilmagan. Hatto "destruktiv", "destruktivlik", "destruktiv faoliyat" tushunchalari aksariyat lug'atlarda mavjud emas. "Destruktivlik" tushunchasi, ayniqsa, insonning destruktivlik faoliyatini yetarli darajada o'rganilmaganligi, bu borada atamalarning bir ma'noli talqini mavjud emasligi unga aniqlik kiritish zaruratini yuzaga keltirmoqda.

Destruktiv g'oya – ijtimoiy munosabatlarning buzilishiga sabab bo'ladigan nazariyalar, qarashlar, me'yorlar, qadriyatlar va ularni jamiyatda tarqatish usullaridan iborat salbiy destruktiv voqelikdir. Destruktiv g'oya destruktivlik darajasiga qarab aniqlanadi. Hamma destruktiv g'oyalar ham mutlaq va umumiy mezonlarga tayanmaydi. Destruktiv g'oya deganda, keng ma'noda, shunday g'oyalar tushuniladiki, ular mavjud ijtimoiy munosabatlarning buzilishiga xizmat qiladi. Mutlaq destruktiv g'oyalar esa har qanday ijtimoiy aloqalar va institutlarning buzilishiga xizmat qiladigan, umuman jamiyatning rivojlanishi, hatto, yashashiga imkon qoldirmaydigan g'oyalardir. "Ular insonparvarlik tamoyiliga zid bo'lgan, jamiyatni tarafkashlarga ajratib, bo'lib tashlaydigan, bir millatni boshqasidan ustun qo'yadigan, oliy irq da'vosida boshqa xalqlarni qirg'in qilishga chaqiradigan destruktiv g'oyalardir. Diniy aqidaparastlik va jangari irqchilik, buyuk davlatchilik shovinizmi va ashaddiy (agressiv) millatchilik, fashizm va bolshevizm mafkuralari ana shunday vayronkor g'oyalar tizimini tashkil etadi".[71]

Destruktiv g'oya avtoritar shaxslar va minoritar ijtimoiy guruhlarning g'ayriinsoniy ifodalangan manfaatlariga asoslanadi va ushbu manfaatlarni butun jamiyat uchun qo'llab bo'lmaydigan usullarda amalga oshirishni nazariy jihatdan asoslaydi. Destruktiv

[71] Nazarov Q. G'oyalar falsafasi. – Toshkent: "Akademiya", 2011. – B.296–301.

g'oyalarning asosiy tamoyillar, qarashlar, aqidalar, ramzlar va tushunchalarni olishi mumkin bo'lgan eng asosiy manbalarni, ya'ni, asosiy dunyoqarash oqimlarini ajratish, destruktivlikning ta'siri va tajovuz yo'nalishining xarakterini aniqlash, destruktiv harakat obyekti va manfaatlarini amalga oshirishning asosiy doirasini aniqlash tadqiqotlardagi ko'plab chigalliklarni oydinlashtiradi.

Destruktiv g'oyalarning ham subyekt sifatida, ham obyekt sifatida asosini marginal guruhlar tashkil qiladi. Ayni paytda bugungi dunyoda turli vositalar orqali o'z ta'sir doirasini kengaytirishga intilayotgan buyuk davlatchilik shovinizmi, tajovuzkor millatchilik, neofashizm terrorchilik, ekstremizm kabi siyosiy oqimlar faoliyati bunga misol bo'ladi. Pirovardida bunday g'ayriinsoniy, destruktiv g'oyalar xalqlar boshiga so'ngsiz kulfatlar keltirib, insoniyatning tinchligi va osoyishtaligini buzmoqda.

O'zbekistonning Birinchi Prezidenti I.A.Karimov "O'zbekiston XXI asr bo'sag'asida: xavfsizlikka tahdid, barqarorlik shartlari va taraqqiyot kafolatlari" asarida mamlakatimiz taraqqiyotiga xavf soluvchi tahdidlarning bir qanchasini keltirib o'tadi. Ularning aksariyati milliy mentalitetimizga yot bo'lgan mafkuraviy xurujlar hisoblanib, mintaqaviy mojarolar, diniy ekstremizm va fundamentalizm, buyuk davlatchilik shovinizmi va agressiv millatchilik, etnik va millatlararo ziddiyatlar, korrupsiya va jinoyatchilik, mahalliychilik va urug'-aymoqchilik munosabatlari va boshqalardan iboratligi asoslab beriladi.[72] Darhaqiqat, bunday g'oyalar inson tabiatiga zid bo'lib, uni salbiy tomonga o'zgartiradi, unda nosog'lom turmush tarzini shakllantiradi, fikrlar xilma-xilligini cheklaydi, qaramlik, tobelik, mutelik muhitini yaratadi. Milliy tafakkur tarzini o'z negizlaridan begonalashtiradi, begona urf-odat, an'analarni targ'ib qiladi, ularning kirib kelishiga sharoit yaratadi, xalqni o'z milliy qadriyatlaridan, oxir-oqibat o'z taraqqiyot yo'lidan adashtiradi, jamiyatda xalqlar va millatlararo totuvlik, dinlararo bag'rikenglikka raxna solib, ichki ixtiloflar, parokandalikka olib keladi. I.Karimov "Millatni bo'lib tashlashga

[72] Karimov I.A. Xavfsizlik va barqaror taraqqiyot yo'lida. 6-jild. –Toshkent: "O'zbekiston", 1998. – B.429.

asos bo'ladigan g'oya destruktiv g'oyadir", degan edi.[73] Darhaqiqat, destruktiv g'oyalar qayerda va qanday vujudga kelgani, faoliyati xarakteri va boshqa belgilaridan qat'i nazar, ularda ma'lum bir umumiy qonuniyatlar kuzatiladi: umumqabul qilingan qonunlarni, axloqiy me'yorlar, madaniy va ma'naviy qadriyatlarni rad etish, o'z dunyoqarashini, siyosiy xohish-irodasini jamiyatning qolgan qismiga tiqishtirishga intilish, terror, ma'naviy va axborotga oid zo'ravonlik yoki nayrangbozlik usullaridan foydalanish va boshqalar shular jumlasidandir.

Shundan kelib chiqib, destrkutiv g'oyalar tarqalishi, ularning holati, bular bo'yicha yuzaga kelayotgan salbiy jihatlar, ularni ta'minlash bo'yicha normativ-huquqiy bazamizning holati bo'yicha quyidagi tahlillarni keltirish maqsadga muvofiq.

Olib borilgan tadqiqotlar asosida g'oyalarning ijtimoiy ongga ta'siri, oqibatlaridan kelib chiqib, quyidagi destruktivlik mezonlarini ajratish mumkin:

– g'oyaning individga, uning jismoniy, ruhiy va axloqiy sog'ligiga, moddiy manfaatlariga, siyosiy, diniy, madaniy, oilaviy, fuqarolik huquqlariga, majburiyat va talablariga salbiy ta'siri;

– g'oyaning ijtimoiy guruhlar, institutlar va formal belgilar asosida qabul qilingan ijtimoiy-zaruriy aloqalarga munosabati, masalan, milliy, iqtisodiy, diniy, sinfiy, millatlararo va konfessiyalararo munosabatlaridagi salbiy ta'siri;

– g'oyaning jamiyat iqtisodiy, texnologik va ilmiy taraqqiyotiga, demografik jarayonlarga, ijtimoiy muhofaza, transport va aloqa tizimi munosabatiga salbiy ta'siri;

– g'oyaning madaniyat va madaniy qadriyatlarga, ilmiy va texnik yutuqlarga, etnosiyosiy, diniy yoki xalq an'analariga, ijtimoiy ta'minot va mehnat munosabatlari tizimiga salbiy ta'siri;

– g'oyaning davlat va xalqaro tashkilotlarga, hududiy yaxlitlik va milliy xavfsizligiga, ichki institutsional qurilishga salbiy ta'siri;

– g'oyaning ekologik muhitga, sotsiumning mavjudligini ta'minlaydigan zarur unsur va omillarga salbiy ta'siri.

[73] I.Karimov "Millatni bo'lib tashlashga asos bo'ladigan g'oya destruktiv g'oyadir", deydi.

Destruktiv g'oyalarni turli vaziyatlar, xususiyatlariga qarab tasniflash mumkin. Masalan, asosiy ta'limotlariga qarab, obyekti, subyekti, yo'nalishlari, sabablari, oqibatlari, zamon va makon hamda boshqa jihatlari nazarda tutiladi. Bizning fikrimizga ko'ra destruktiv g'oyalarni umumiy ko'rinishi, manbalariga ko'ra diniy va dunyoviy hamda aralash shakldagi ko'rinishga ajratish mumkin.

Birinchisi, Diniy ko'rinishdagi destruktiv g'oyalar.

Din nomidan ish ko'ruvchi yoki diniy manbalarni noto'g'ri talqin qilish oqibatida vujudga kelgan diniy aqidaparastlik yoki dinga nisbat berilgan xristian fundamentalizmi, hinduiylik ekstremizmi, terrorizm kabi destruktiv g'oyalar mavjud. Bunday qarashlar juda qadimiy ildizlarga ega bo'lib, hech qachon chegara bilmagan, din, millat, hududni tan olmagan, barcha dinlar doirasida rivojlangan. Bunday ko'rinishdagi qarashlarni buddizm, xristianlik, yahudiylik, islom, katoliklar, protestantlar, pravoslavlar orasida birday uchratish mumkin. Masalan, diniy ekstremistlar qayerda faoliyat ko'rsatmasin, asosiy maqsadi diniy davlatni barpo qilish bo'lib, bunga o'zaro nizolar, ixtiloflar, qurolli to'qnashuvlar orqali, ya'ni qon to'kish va zo'rlik bilan erishishni ko'zlaydi.

Ikkinchisi, Dunyoviy ko'rinishdagi destruktiv g'oyalar.

Bolshevizm – siyosiy avantyuristlar va hokimiyatparastlarning o'ta reaksion, insoniyat uchun zararli va xavfli bo'lgan siyosiy hokimiyatni egallab olish va davlat boshqaruvining vayronkor shakli. Buyuk davlatchilik shovinizmi – bir davlatning boshqa davlat yoki davlatlar ustidan siyosiy, mafkuraviy, iqtisodiy va harbiy hukmronligini o'rnatishga qaratilgan vayronkor nazariya va amaliyot.

Uchinchidan, Aralash ko'rinishdagi destruktiv g'oyalar.

Aqidaparastlik, ekstremizm, terrorizm, fundamentalizm kabi destruktiv g'oyalar diniy va dunyoviy shakllarda namoyon bo'ladi. I.Karimov aqidaparastlik haqida shunday degan edi: "Aqidaparastlik esa, u qanday qiyofada bo'lishidan qat'i nazar – bu diniy aqidaparastlik bo'ladimi yoki kommunistik aqidaparastlik bo'ladimi – o'z mafkurasiga, hayot qarashlariga mos kelmaydigan

hamma narsani inkor etadi va "kimki biz bilan emas ekan, demak, u bizga qarshi" degan tamoyil asosida ish ko'radi".[74]

Destruktiv g'oyalarning makoniga ko'ra tasnifi o'z g'oyaviy ta'sirni barcha tarafdorlariga yetkazishga imkon beruvchi global, iqtisodiy va axborot tizimining zamonaviy bosqichdagi o'ziga xosliklariga bog'liqdir. Ommaviy kommunikatsiyaning zamonaviy vositalari ham alohida insonning, ham tarixiy shakllangan siyosiy, diniy, milliy va ijtimoiy-madaniy institutlarning butun guruhlari dunyoqarashini shakllantirishga imkon beradi. Shunga bog'liq holda barcha destruktiv mafkuralarni quyidagilarga bo'lish mumkin:

Global (transmilliy) mafkuralar – bularning ta'siri shaxsga ta'sir ko'rsatishning an'anaviy institutlari mazmunini hisobga olmagan holda ayrim insonga tayanuvchi barcha insoniyatga tarqaladi (vesternizm, barcha global sektalar: bahoiylik, sayentologiya, sotsiomadaniy harakatlar, tiklar, xippi, rastamanlar);

Mintaqaviy mafkuralar – muayyan madaniy-geografik makon yoki birgina davlat, etno-milliy hamjamiyat va h.k. bilan cheklangan mafkuralar ("skinxed", "Akromiylar", "Beloye-Bratstvo"), soxta-diniy oqimlar.

Ekspertlarning qayd etishicha, so'nggi yillarda O'zbekistonda Internet tarmog'i orqali sodir etilayotgan ijtimoiy xavfli holatlar ko'payishi kuzatilmoqda. Jumladan, Axborot texnologiyalari va kommunikatsiyalarini rivojlantirish vazirligining ma'lumotlarida 2017-yilning noyabr holatiga ko'ra, milliy UZ domenidagi 548 ta saytlarga buzish/ishdan chiqarish, 321 ta muallif ruxsatisiz tarmoqdagi kontentlarni yuklab olish, 225 ta saytning asosiy sahifasini o'zgartirish va 2 ta fishing materiallarini tarqatish holatlari aniqlangan. Ayrim mutaxassislarning ta'kidlashicha, hozirgi paytda O'zbekiston Internet foydalanuvchilarining 26%i turli darajada kiberhujumga uchramoqda.

So'nggi yillarda O'zbekistonda ham jinoyatchilikning ushbu turiga qarshi kurash borasidagi ishlar jadallashmoqda. Xususan, 2013-yilda O'zbekiston Respublikasi Prezidentining "O'zbekiston Respublikasi Milliy axborot-kommunikatsiya

[74] Karimov I.A. O'zbek xalqi hech qachon, hech kimga qaram bo'lmaydi. 13-jild. – Toshkent: "O'zbekiston", 2005. – B.448.

tizimini yanada rivojlantirish chora-tadbirlari to'g'risida"gi qarori bilan 2013–2020-yillarda O'zbekiston Respublikasi Milliy axborot kommunikatsiya tizimini kopmleks rivojlantirish Dasturi qabul qilindi. Dastur doirasida 2015–2019-yillarda umumiy qiymati 883,7 mln AQSh dollari qiymatidagi 9 loyihaga investitsiya kiritilgan.[75] O'zbekistonda mazkur jinoyatchilikka qarshi kurash mexanizmini takomillashtirish uchun avvalo uning huquqiy bazasini mustahkamlashga urg'u berilayotganligi eng samarali yo'l ekanligini namoyon qilmoqda. Jumladan, bugungi kunga qadar axborot texnologiyalari va xavfsizligini ta'minlashga yo'naltirilgan 22 qonun, 37 ta Prezident qaror va farmonlari, 75 ta Vazirlar Mahkamasi qarorlari qabul qilingan.

Shunga qaramasdan, O'zbekistonda Internet tarmog'i orqali sodir etiladigan jinoyatchilikka qarshi kurash borasida ba'zi jinoiy, huquqiy muammolarning mavjudligi sezilmoqda. Birinchidan, kiberjinoyatchilikning siyosiy maqsadlarga yo'naltirilgan, ya'ni davlatning konstitutsiyaviy tuzumiga qarshi g'oyalarni global tarmoq orqali tarqatib borish bilan katta ommani jamlash va ommaviy namoyishlar, terrorchilik harakatlari sodir etilmoqda. Bu hodisalar mamlakat suvereniteti va yalpi xavfsizligiga katta tahdid tug'dirmoqda. "Arab bahori" hamda Gruziya, Ukraina va Qirg'izistonda bo'lib o'tgan rangli inqiloblar, ommani to'ntarish olib borish g'oyasi ostida birlashtirish uchun Internetdan foydalanilganligi global tarmoqning jinoyatchilar qo'lidagi qanday qurol ekanligini anglatadi.

2.2. Xorijiy davlatlarning kiberterrorizm va ekstremizmga qarshi kurash tajribasi va uning mintaqaviy hamkorlikka ta'siri

Kiberxavfsilik tezda texnik intizomdan strategik dasturga aylandi. Lekin nazariy rivojlanish hali-hamon boshlang'ich bosqichda turibdi. Kiberxavfsizlik metodlari ko'p, ammo

[75] В развитие сетей связи вложат $883,7 млн (К 2020 году скорость передачи данных планируется увеличить в 20 раз) // http:// www.gazeta.uz/2015/12/01/comm/

sohaga tegishli bo'lgan kiberurush. kiberqurol. kiberhujum. kiberjinoyatchilik, kiberterrorizm kabi atamalarning yagona ta'rifi yo'q. AQSh kiberarsenaliga oid so'nggi ma'lumotlar, ayniqsa. Stuxnet dasturining Eron yadro obyektariga qarshi qo'llanilishi kiberurushlar zamonaviy mudofaa strategiyasining bir qismiga aylanganini tasdiqlaydi. Markaziy Osiyo davlatlarida texnologik rivojlanish yuqori bo'lmasa-da, mahalliy OAV larda kiberxavsizlik masalasi haqida bong urilmoqda. Avvalo, bu "axborot urushi", ya'ni dunyoning qudratli davlatlari ommaviy axborot vositalari va kompyuter texnologiyalari orqali mafkuraviy urush olib borishi haqidagi o'z isbotini topmagan munozaralar bilan bog'liq. Kiberxavfsizlik masalalari "kiberterrorizm tahdidlari" ko'rinishida ham talqin qilinmoqda Ushbu yondashuv Markaziy Osiyo hukumatlariga yashirin harakatlarga qarshi repressiyani kuchaytirishni qonuniylashtirish, shuningdek, internet va ijtimoiy tarmoqlar faol foydalanuvchilar ustidan nazorat qilish imkonini beradi. Hozirgacha Markaziy Osiyo hukumatlari duch kelgan yirik kiberhujumlar faqat jinoiy xarakterga ega va birinchi navbatda moliyaviy operatsiyalar bilan bog'liq. Mahalliy davlat axborot tarmoqlari 2007-yilda Estoniyada yoki 2008-yilda Gruziyada sodir bo'lgan kiberhujumlarga o'xshash siyosiy kiberhujumlarga duch kelmagan. Lekin ayni vaqtda Markaziy Osiyo davlatlari iqtisodiyotining muhim tarmoqlari hisoblanadigan energetika va transport sohalarida kiberxavfsizlik bilan bog'liq o'z yechimini kutayotgan muammolarni hal qilishga ko'proq e'tibor qaratishi lozim.

Kiberjinoyatchilikning transchegaraviylik xususiyatidan kelib chiqib, o'tgan asrning 70–80-yilllarida mazkur muammoni bartaraf etishda global darajada e'tibor qaratila boshlandi. Bunga qadar axborot texnologiyalari borasida rivojlangan davlatlarda (Italiya – 1978, Avstraliya – 1979, B.Britaniya – 1981, AQSh – 1980, Daniya va Kanada – 1985, Germaniya – 1986, Avstriya, Yaponiya va Norvegiya – 1987, Fransiya va Gretsiya – 1988-yillarda) kompyuter tizimi bilan bog'liq jinoyatlar uchun ma'muriy va jinoiy javobgarliklar belgilab qo'yilgan edi. Biroq ushbu davlatlar

qonunchiligida mazkur masalaga nisbatan turlicha yondashilgan. Bu esa global ahamiyat kasb etayotgan axborot texnologiyalari jinoyatchiligiga qarshi kurashda qator muammolarni yuzaga keltirdi.

Yuqoridagi fikrlarga asoslanib mazkur paragrafni ikki jihat asosida tahlil etishga harakat qilamiz. Bular – xorijiy davlatlarning kiberterrorizm va ekstremizmga qarshi kurashdagi qonunchilik masalasi hamda rivojlangan davlatlarning bu boradagi institutsional tajribasi asosida yoritiladi.

Xorijiy davlatlarning kiberterrorizm va ekstremizmga qarshi kurash yo'nalishida qonunchilik masalasi o'ziga xos jihatlar bilan ajralib turadi.

Bu boradagi muammolarni bartaraf etish va kiberjinoyatchilikka qarshi yagona yondashuvni yaratish maqsadida Yevropa Ittifoqi vazirlar Qo'mitasi tomonidan 1989-yilda №(89)9-sonli Tavsiyanoma/ko'rsatma qabul qilindi. Unga asosan, a'zo davlatlar milliy qonunchiligida jinoiy taqiq o'rnatilishi lozim bo'lgan kiberjinoyatlar ro'yxati shakllantirildi. Unga ko'ra: kompyuter firibgarligi, kompyuterda qalbakilashtirish (soxtakorlik), kompyuter axboroti va dasturlarini buzish, kompyuter sabotaji, ruxsatsiz (noqonuniy) kompyuter tarmog'iga kirish, ruxsatsiz (noqonuniy) ma'lumotlar muomalasini to'sib qo'yish/ushlab qolish va ruxsatsiz (noqonuniy) himoyalangan kompyuter axborotidan nusxa olish jinoyatlari YeI doirasida taqiqlanishi lozimligi ko'rsatilgan.

Shuningdek, 2002-yilda BMT Bosh Assambleyasining kompyuter jinoyatlariga qarshi kurashni kuchaytirish to'g'risidagi №56/261 Rezolyutsiyasi qabul qilingan. Mazkur jinoyatchilikka qarshi kurash olib boruvchi tashkilotlar/institutlar tashkil etish va ular orqali xalqaro hamkorlik olib borish alohida inobatga olindi. Xususan, 1996-yilda Lion (Fransiya)da "Katta sakkizlik" davlatlarining yig'ilishida global tarmoq jinoyatlarining kriminalizatsiyasi va javobgarligi borasida qonunchilikni qayta ko'rib chiqish va maxsus vakolatli huquq idoralarini tashkil etishga yo'naltirilgan №16 Reglament imzolandi. Unga asosan, Germaniyada Myunxen politsiya boshqarmasida kiberjinoyatlarga qarshi kurash bo'yicha

maxsus guruh, Fransiyada axborot texnologiyalari jinoyatlarga qarshi kurash Xizmati tashkil etildi.

Unga asosan, Germaniyada Myunxen politsiya boshqarmasida kiberjinoyatlarga qarshi kurash bo'yicha maxsus guruh, Fransiyada axborot texnologiyalari jinoyatchiligiga qarshi kurash Xizmati tashkil etildi. 1998-yilda Rossiyada Ichki ishlar vazirligi huzurida "K" boshqarmasi, B.Britaniyada 2001-yilda Milliy bo'linma, 2006-yildan esa Milliy Agentlik, Yaponiyada 2013-yilda kiberjinoyatchilikka qarshi kurash olib boruvchi alohida politsiya tizimi shakllantirildi va bugungi kunda yuqori samara bilan faoliyat yuritmoqda. Yevropa Ittifoqi tarkibida ham mazkur jinoyatchilik tahlilini olib boruvchi, global tarmoq jinoyatlarini aniqlash va fosh qilish hamda bu borada qo'llanmalar tayyorlash bilan shug'ullanuvchi 10 dan ortiq guruhdan iborat "Yevropa kiberjinoyatchilik Markazi" (European cybercrime centre/"YC3") tashkil etildi.

Internet global tarmog'ida axborot xavfsizligiga qarshi qaratilgan jinoyatlar Amerika, Yevropa, Osiyo va MDH a'zo davlatlarida jinoiy qilmish sifatida baholanganligi kuzatiladi. Bu turdagi jinoyatlarga – kibermakonda axborot yaratish, saqlash, egalik qilish, foydalanish va tarqatishdan iborat jinoiy qo'riqlov ostidagi obyektga zarar yetkazuvchi jinoyatlar kiradi. AQSh federal jinoyat kodeksi 18-bo'limida davlatlararo yoki xalqaro savdoga aloqador har qanday himoyalangan kompyuterdan hukumat idoralarining axborotlariga yoki axborot bazasiga ruxsatsiz (noqonuniy) kirish/ foydalanish uchun javobgarlik belgilangan.

Ushbu jinoyatlar Fransiya jinoiy qonunchiligida (3231-modda) "avtomatlashtirilgan axborotni qayta ishlash tizimiga noqonuniy kirish", Ispaniya jinoyat kodeksida (256-modda) "mulk egasining roziligisiz telekommunikatsiyalardan foydalanish", Daniya jinoyat kodeksida (263-modda) "elektron ma'lumotni qayta ishlash uchun mo'ljallangan axborot yoki dasturlarga noqonuniy kirish", Shvetsariya jinoyat kodeksida "ma'lumotlarni qayta ishlash tizimiga noqonuniy kirish" jinoyati (143-modda) deb ko'rsatilgan.

1996-yil 27-dekabrdagi Rossiya Federatsiyasi jinoiy qonunchiligiga asosan. kodeksning "Jamoat va jamoat tartibiga qarshi jinoyatlar" deb nomlangan 28-bo'limida kompyuter ma'lumotlari sohasidagi jinoyatlarga jazo choralari belgilandi. Unda kompyuter tizimi bilan birga kompyuter tarmog'i xavfsizligi ham alohida nazarda tutilgan.

Ozarbayjon Respublikasining jinoyat kodeksida (271-modda) va Gruziya jinoyat kodeksida (284-modda), Turkmaniston Respublikasi jinoyat kodeksida (333-modda) kompyuter ma'lumotlaridan noqonuniy foydalanishga yo'l qo'yganlik uchun jinoiy javobgarlik to'g'risidagi qoida Rossiya Federatsiyasi jinoyat kodeksining (272-moddasi) kompyuter axborotidan noqonuniy (ruxsatsiz) foydalanish normalarini takrorlaydi.

O'zbekiston Respublikasining Jinoyat kodeksida 2782-moddasida "Kompyuter ma'lumotlariga noqonuniy (ruxsatsiz) kirish" jinoyati ko'rsatib o'tilgan.

2. Internet tarmog'ida taqiqlangan kontentni muomalasi bilan bog'liq jinoyatlar tahlili bu boradagi ma'lumotlar aylanmasiga aloqador munosabatlar real makonda qay tarzda tartibga solingan bo'lsa, kibermakonda ham xuddi shu tarzda tartibga solinishi talab qilinadi. Bunga: pornografiya, zo'ravonlikni targ'ib qiluvchi, shaxs sha'nini tahqirlovchi, tuhmat, giyohvandlik va portlovchi moddalar, odam savdosi hamda ekstremistik, separatistik va boshqa shu kabi erkin muomalada bo'lishi taqiqlangan materiallar kiradi.

Qozog'iston JK ning 174-moddasida milliy, irqiy, etnik yoki diniy adovat qo'zg'atishga qaratilgan harakatlarni OAV imkoniyatlaridan yoxud Internet tarmog'idan foydalanib sodir etishlik uchun javobgarlik nazarda tutilgan.

Bundan tashqari, Tojikiston JK ning 167-moddasiga asosan agressiya, urushni targ'ib qilish, shuningdek bunday harakatlarni OAV imkoniyatlaridan foydalanib sodir etganlik uchun va 175-moddasida esa konstitutsiyaviy tuzumni zo'rlik ishlatib o'zgartirishga ommaviy chaqiriq OAV imkoniyatlaridan foydalanib sodir etish uchun javobgarlik mavjud. Xuddi shunday harakatlarni sodir etish, Ukraina JK ning 109-moddasi bilan huquqiy baholanadi.

Navbatdagi jihat rivojlangan davlatlarning bu boradagi institutsional tajribasi.

AQSh ning internetda axborot xavfsizligini ta'minlash tizimi. AQSh milliy tadqiqotlar kengashi (National Research Council) ma'lumotiga ko'ra, davlatlar Internetni noqonuniy kontentda himoyalashda ikki xil usuldan foydalanmoqda. Bularga davlat darajasida (provayderlar orqali) cheklovlar joriy qilish; alohida foydalanuvchilar yoki tashkilotlar darajasida maxsus filtrlash dasturlarini o'rnatish hisoblanadi.

Yuqoridagi usullarni quyidagicha tasniflash va ta'riflash maqsadga muvofiq.

1. Birgalikda tartibga solish rejimi (davlat darajasida) – sanoat subyektlari va davlat o'rtasida majburiyatlarning taqsimlanishidir.

2. Provayder darajasida filtrlash. Bu usulda alohida veb-saytlar faoliyatini to'xtatish davlat darajasida amalga oshiriladi. Bu tartibni faqat Internet xizmatlari soni cheklangan davlatlarda amalga oshirish mumkin.

Shuningdek, AQSh qonunchiligida filtrlash dasturlari maktab, kutubxona, internet-kafelar va jamoatchilik foydalanadigan joylarda majburiy tarzda o'rnatiladi. Internetning tashkiliy va texnik jihatdan tartibga solinishi har bir davlat aloqa va axborot infratuzilmasiga javobgar organlari tomonidan olib boriladi.

2001-yil 11-sentyabrdan boshlab AQSh hukumati terroristik tashkilotlarning internet orqali berayotgan targ'ibot va tashviqot ishlariga katta e'tibor qaratdi va AQSh maxsus xizmati terroristlar saytlarini berkita boshladi. Kamikadzelar e-mail va Internet kafelar orqali o'zaro aloqada bo'lganlardan xabar topgan Prezident Djordj Bush 2001-yilda "Amerikani birlashtirish va mustahkamlash to'g'risida"gi Qonunni imzoladi. Endilikda kompyuterga noqonuniy kirishga olib keluvchi har qanday faoliyat terrorizm sifatida tasniflanib, barcha provayderlar foydalanuvchilari haqidagi ma'lumotlarni maxsus xizmatlarning birinchi talabidayoq taqdim etishi kerakligi majburiyat sifatida belgilandi.

Huquqiy tartibga solish bo'yicha umumiy ahvol quyidagicha, AQSh da internetda keng qo'llanadigan filtrlash amaliyoti bo'lmasa-

da, internet umuman "tartibga solinmaydi", deb bo'lmaydi. Hukumatning internet-kontentni tartibga solishi quyidagi to'rtta muammodan kelib chiqqan. Bularga, bolalarni himoyalash va axloqlilik, milliy xavfsizlik, intellektual mulk hamda kompyuter xavfsizligi masalalari kiradi.

Xitoy Xalq Respublikasining tajribasi. Internet tarmog'ini noqonuniy kontentdan himoyalashda qat'iy chora-tadbirlar ham yetarli samara bermoqda. Xususan, internet milliy segmentini nazorat qilish bo'yicha samarali mexanizmlarni qo'llayotgan davlat Xitoy hisoblanadi. Bu davlatda internetni nazorat qilish tizimi markazlashgan bo'lib, nazorat qilish va tozalashning qat'iy usul va chora-tadbirlari qo'llanilmoqda. Bu borada "Oltin qalqon" loyihasi asosida ishlar olib borilmoqda. Loyiha asosida xavfsizlikni ta'minlash uchun veb-sahifalarni filtrlashda kalit so'zlar va saytlarning "qora ro'yxati" tuzilgan. Saytlarga IP-adreslari bo'yicha cheklovlar o'rnatilgan.

Xitoyda internet-kafedan foydalanuvchilar uchun majburiy ro'yxatdan o'tish yo'lga qo'yilgan, shuningdek, qonunga qarshi chop etilgan axborotlarni nazorat qilib turuvchi internet-politsiyasi ham faoliyat yuritadi.

Qonunga muvofiq, 2005-yilda ish boshlagan yangiliklar saytlari qayta ro'yxatdan o'tishi kerak edi. By tadbir internet saytlarini pornografiya va qonunga qarshi ma'lumotlardan tozalash maqsadida o'tkazilgan. Hozirda barcha internet-provayderlari o'z saytlaridagi barcha ma'lumotlar uchun javobgar hisoblanadi.

2009-yilning 1-iyulidan Xitoydagi barcha kompyuterlarga pornografiya va axloqsiz mazmundagi ma'lumotlarga internet-filtrlar qo'yilishi ko'rib chiqildi. Mazkur filtrlar mamlakatda sotuvga chiqarilgan barcha kompyuterlarga ishlab chiqaruvchi korxonaning o'zida o'rnatib chiqarilishi belgilab qo'yildi. Bundan tashqari, hukumat barcha internet-pravayderlarini va internet-kafelarni qat'iy nazorat ostiga oldi.

Bugungi kunda Xitoy internet tarmog'i tizimi to'rtta asosiy tarmoqdan iborat: ChinaNet – Axborot sanoati vazirligiga tegishli yetakchi tijoriy tarmoq, Golden Bridge Network – Jitong

korparatsiyasiga tegishli kichikroq tijoriy tarmoq. China Science & Technology Network ilmiy tarmog'i. China Educational & Research Network – ta'lim maskanlari va akademik institutlarni birlashtiruvchi tarmoqlar hisoblanadi.

Xitoyda internet-texnologiyalarini tartibga solish davlat siyosati va milliy mafkura bilan bog'liqlikda olib boriladi. Xitoy Kommunistik partiyasi hokimiyatda monopoliyani saqlab qolish maqsadida, an'anaviy OAV ni nazorat qilib kelgan. Internetning paydo bo'lishi bilan o'z nazoratiga xavf sezdi va bu masalada filtrlash texnologiyalari, kiber – militsiya nazorati va targ'ibotni birga qo'llagan holda choralar ko'rib kelmoqda.

O'tgan asrning 90-yillar boshlarida jamoat xavfsizligi organlari barcha bo'g'inlarida axborot xavfsizligi ustidan nazorat o'rnatilgan. Xitoy "militsiya to'g'risida"gi qonun va tegishli qonunlar, qonunosti hujjatlari jamoat tartibi organiga axborot xavfsizligini nazorat qilish vazifasini topshiradi. Jamoat militsiyasining tarkibidagi internet-politsiyasining asosiy vazifalari qilib quyidagilar belgilangan:

- axborot tizimi xavfsizlik darajasi mezonlarini aniqlash va ularni himoyalashning aniq usullarini topish;
- olingan ma'lumotlarni Internet foydalanuvchisiga yetkazish;
- internetda xavfsizlik rejimini o'rnatish;
- elektron ma'lumotlar, hujjatlardan foydalanishda yuzaga kelgan jinoiy ish materiallarini yuritish;
- kompyuter viruslari va boshqa xavfli axborotlardan ogohlantirish mexanizmlarini ishlab chiqish;
- axborot mahsulotlarini sotilishiga davlat ruxsatini berishda aniq usullarini ishlab chiqish;
- axborot xavfsizligini ta'minlashni nazorat qilish va yo'naltirib borish;
- internet tarmog'idagi huquqbuzarliklarning oldini olish bo'yicha choralar ishlab chiqish.

Xitoy o'n minglab kibersenzurachilar va kiberpolitsiya xodimlariga ega bo'lgan dunyodagi yagona davlat hisoblanadi. Ular barcha hududiy jamoat tartibi byurolarida o'z bo'limlariga ega. Ularning oldiga qo'ygan maqsadi davlat sirlarini saqlash bo'lsa-da,

amalda ularning vazifalari internetni hukumatga qarshi qaratilgan destruktiv axborotlardan tozalashga yo'naltirgan. Olingan ma'lumotlarga ko'ra kiberpolitsiya xodimlari tomonidan oxirgi o'n yillikda yuzlab internet qoidabuzarlarini jazoga tortgan.

Bundan tashqari, Xitoyda internetni nazorat qiluvchi organlar qatoriga quyidagilarni kiritish mumkin:

- Davlat Axborot Kengashi boshqarmasi (Internet – targ'ibot ma'muriy byurosi va jamoat fikrini o'rganish markazi);
- Xitoy kommunistik partiyasining markaziy kengashi targ'ibot bo'limi (Internet Byurosi, Axborot va jamoatchilik fikri byurosi);
- Axborot sanoati vazirligi (Internetda noqonuniy va axloqsiz axborotni ro'yxatga olish markazi);
- Jamoat xavfsizligi vazirligi (Kompyuter nazorati va tekshirish byurosi).

Saudiya Arabistoni. Radikalizmga qarshi kurashayotgan shunday davlatlardan biri – Saudiya Arabistoni. Arabiston yarimorolida joylashgan ushbu mamlakat garchi Islom dinining markazi, jamiyatning birmuncha konservativligi bilan ajralib tursa-da, radikalizmga qarshi kurashish bo'yicha juda katta tajribaga egaligi bilan ham alohida e'tiborga molik davlat hisoblanadi. Saudiya Arabistoni terrorizmga qarshi kurash borasida juda mukammal dasturlarni ishlab chiqib, butun jamiyatni qamrab oluvchi usullar bilan omma ongidan ekstremistik kayfiyatni yo'q qila oldi. Saudiyaning bu boradagi xatti-harakatlari ikki bosqichli bo'lib, u rasman 2005-yildan boshlab ishga tushirildi. Avvaliga shubhali terrorchilarni qamoqqa olish bilan boshlandi. Biroq faqat bu harakatlar bilan chegaralanib qolinmadi. Qamoqdagi shaxslar bilan tezda muloqot o'rnatilib, radikallashuvning asosiy sabablari o'rganildi hamda ularning Islom dini bo'yicha tushunchalari tahlil qilindi. Ishlar asosan uch xil kesimda tashkil qilindi: diniy, ruhiy va madaniy.

Dastur qatnashchilariga ijtimoiy tadbirlarda, ayniqsa, oilaviy yig'inlar va sport tadbirlarida qatnashishga ruxsat berildi. Lekin, shu bilan birga, asosiy e'tibor ularning Islom haqidagi "tushunchalari va bilimlariga" qaratildi. Saudiya dasturining yana o'ziga xos

jihati shunda ediki, dastur qatnashchilarining davlat tomonidan berilgan moliyaviy yordam evaziga oila qurish va ta'lim olishlari rag'batlantirildi. Afv so'rab murojaat qilgan sobiq ekstremistlar ish bilan ta'minlanib, ularni jamiyatga qaytadan qo'shish bo'yicha amaliy choralar ko'rildi. Bundan tashqari, dastur qatnashchilari va ularning oila a'zolariga davolanish va sog'liqni tiklash bo'yicha moliyaviy yordam va nafaqalar ajratildi.

Saudiya hukumati tomonidan olib borilgan bunday dasturlar ekstremistlar sonini keskin kamaytirgan bo'lishiga qaramay, ayrim muammolar haligacha saqlanib qolmoqda. Jumladan, so'nggi yillarda radikal kuchlar tomonidan internet tarmog'ida g'oyalarni kengroq tarqatish va shu yo'l bilan o'z tarafdorlari sonini orttirishga bo'lgan urinishlarning ortib borishi Saudiya hukumatini jamiyat va undagi yoshlar qatlami radikallashuvining oldini olish borasida profilaktik choralarni kuchaytirishga undamoqda. Saudiya rasmiylarining ma'lumotlariga ko'ra, 1998-yilda 15 ta ekstremistik veb-sahifa mavjud bo'lgan, hozirgi kunda bir necha ming veb-sahifalar ishlab turibdi. Ularning aksariyati o'z serverlarini Saudiya Arabistonidan tashqarida, jumladan AQSh, Yevropa, Xitoy va Janubiy-Sharqiy Osiyo davlatlarida joylashtirgan.

Kiberterrorizm va ekstremizmga qarshi kurash yo'nalishida **Turkiya davlati** o'ziga xos o'ringa ega.

Zo'ravon ekstremizmga qarshi kurash borasida katta tajribaga ega bo'lgan, texnologik jihatdan tobora taraqqiy etib borayotgan yana bir davlat – Turkiya Respublikasi bo'lib, mamlakatda radikal kuchlarga qarshi kurashish bilan bog'liq juda zalvorli tarix mavjud. Bugungi Turkiya radikalizmga qarshi kurashishning yorqin misoli sifatida ham qayd etiladi. Deyarli 85 millionlik aholiga ega Turkiyada 98 foiz kishilar Islom diniga e'tiqod qilishadi.

Turkiyada deyarli 20 yil davomida mo'tadil islomiy, shuningdek, asosiy mafkurasi "konservativ demokratiya" bo'lgan Adolat va taraqqiyot partiyasi hukmronlik qilayotgan bo'lsa-da, mamlakat radikallashuvga va zo'ravonlikka samarali qarshilik ko'rsata olmoqda. Buning asosiy sababi sifatida biz Islom va dunyoviylik o'rtasida shakllangan muvozanatli munosabatni keltirishimiz

mumkin. Mamlakatda turli siyosiy qarashlarning mavjudligi, ham diniy va ham dunyoviylikning o'zaro "til topishishi" bilan bog'liq jarayonlar tarixiga deyarli 100 yil bo'ldi.

O'z vaqtida Turkiya Respublikasining asoschisi Mustafo Kamol Otaturk ekstremistik kuchlarga qarshi olib borgan murosasiz kurashi tufayli mamlakat butunlay sekulyar jamiyatga aylantirilgan edi. Ammo o'tgan asrning 80-yillarida sodir bo'lgan Islom uyg'onishi bilan bog'liq xalqaro jarayonlar Turkiyaga ham o'z ta'sirini o'tkazdi.

Mamlakatda diniy va dunyoviy tuzum tarafdorlari o'rtasidagi qarashlarda kelishmovchilik bo'lsa-da, dunyoviy hayot tarafdorlari tomonidan Turkiyaning o'z modernizatsiya loyihalari mavjudligi, liberal hayot, demokratiya va fuqarolik institutlarining shiddati kabilar siyosiy jarayonlarning asosini tashkil qiladi.

Bugungi kunda mamlakat miqyosida "Radikalsizlantirish" dasturlari asosan ikki yo'nalishda amalga oshirilmoqda:

Birinchidan, Turkiyaning diniy ishlar bo'yicha "Diyonat" tashkiloti Islomning tinchlikparvarlik dini ekanligini keng targ'ib qilmoqda. Shu maqsadda 2015-yili "Global terror iskanjasidagi Islom" nomli ma'ruza matni tayyorlandi. Turkiyadagi 80 000 va xorijdagi 2 000 ta masjidga tarqatildi.

Ikkinchidan, Turkiyaning Milliy politsiyasi va tegishli xavfsizlik xizmatlari birgalikda radikalizm va ekstremizmga moyil kishilarni aniqlash, ularni bunday harakatlardan qaytarish maqsadida muloqotga kirishib, bu borada tizimli ishlab kelmoqda. Ana shunday tadbirlardan biri 2016-yil Turkiyaning janubida joylashgan Adana shahrida o'tkazildi. Tadbir davomida 333 nafar ekstremistdan 226 nafari "radikalsizlantirilib", ular osuda hayotga qaytarildi.

Misr tajribasi. XX asr oxiri – XXI asr boshida Misr hukumatining islomparastlar bilan muloqotga borilmaydigan, yon bosmaydigan, hukumatning aniq ishlab chiqqan chora-tadbirlari terrorizm, diniy ekstremizm va radikal diniy guruhlar faoliyatini asta-sekin yo'qqa chiqardi. Hukumatning islom fundamentalistlari bilan murosasiz kurashida Misr armiyasi muhim rol o'ynadi. 90-yillarda Misrda yaratilgan ekstremizmga qarshi kurash tizimiga qonun chiqaruvchi va ijro etuvchi hokimiyatlarning ko'p qismi jalb

etildi. Misrda ushbu sohada barcha davlat idoralarining o'zaro aloqalarini o'rnatishga katta ahamiyat berildi. Ushbu maqsadlar uchun hukumat huzurida ichki ishlar idoralari, targ'ibot va ta'lim muassasalari, hukumatning ijtimoiy-iqtisodiy vazirliklari va idoralari faoliyatini muvofiqlashtirish bo'yicha idoralararo ishchi guruhi tuzildi. Ushbu tizimda muhim rol Oliy xavfsizlik sudiga yuklandi, ulardan armiya zobitlari tayinlandi. Sudning hukmlari ustidan shikoyat qilinishi mumkin emas edi. O'zining xatti-harakatlari va vakolatlari tabiati bo'yicha u favqulodda sudga to'g'ri keldi. Terroristik xarakterdagi jinoyatlar uchun asosiy jazo og'ir mehnat yoki o'lim jazosi edi. Misrdagi oppozitsion nashrlardan ma'lumki, 1995-yilda mamlakat qamoqxonalarida 10000 ga yaqin siyosiy mahbuslar saqlangan.

1995-yilda Addis-Abebada Prezident Husni Muborakka qilingan suiqasddan so'ng, Misr terrorizmga qarshi kurash bo'yicha keng qamrovli dastur ishlab chiqdi. Uni amalga oshirish doirasida 1997-yilda islom ekstremizmiga qarshi kurashni kuchaytirish bo'yicha qo'shimcha choralar ko'rildi. Xususan, xodimlar soni ko'paytirildi va o'quv dasturi takomillashtirildi, Ichki ishlar vazirligi Davlat xavfsizligi bosh boshqarmasining vakolatlari kengaytirildi. 1998-yilda ish boshlagan ushbu bo'limning yangi rahbari X.Alberiy Misrda aksilterror faoliyatini sezilarli darajada faollashtirishga muvaffaq bo'ldi. Shunday qilib, uning buyrug'iga binoan, shubhali shaxslarning harakatini cheklash uchun Misr-Liviya chegarasini qo'riqlash kuchaytirildi. Bundan tashqari, AQSh dan sotib olingan portlovchi moddalarni aniqlash uchun uskunalar MAR dengiz portlari va aeroportlariga o'rnatildi.

Suriya tajribasi.

1982-yildan keyin Suriyadagi islomparastlar faolligi keskin pastga tushib ketdi. Hofiz Asad hukumati ular bilan kurashning samarali usulini (keyinchalik bu usulni Tunisda ham qo'llashdi) topdi. U harbiy yurish va maxsus xizmat harakatlarini OAV tashviqoti bilan birgalikda qo'llab, Suriya shaharlarining ijtimoiy "tub"ini yo'qotishga erishdi. Shaharlarda yollanma ishchilardan foydalanadigan shaxslar soni 1970–1984-yillarda 4 marotaba,

qishloqlarda esa 1,5 marotabaga o'sdi. Mayda va o'rta tadbirkorlikni rag'batlantirib. 1965-yildan keyin esa nazorat qilib, iqtisodning asosiy sohalari, davlat har qanaqasiga yirik kapitalning o'sishini chegaraladi. Shu bilan birgalikda milliy biznesni rivojlantirish, chet el investitsiyalari, bandlikni oshirish bo'yicha shart-sharoitlar yaratildi. 70-yillarda iqtisodiyot 10% ga oshdi, qishloq xo'jaligida, qayta ishlash sanoatida (ham davlat sektori, ham xususiy kooperativ sektorlarida), transport sohasi, neft qazib olish va turizm sohalarida salmoqli potensial hosil qilindi. 1970-1983-yillarda aholi jon boshiga foyda olish 480 dollardan 930 dollargacha ko'tarildi. Neft qazib oluvchi Fors ko'rfazi davlatlarining ko'magi, o'n minglab suriyalikning u yerga ish izlab borishi (ayniqsa, Kuvaytga), 1 millionga yaqin suriyalikning Livanda ishlashi (1975–1991-yillardagi fuqarolar urushi davrida buzilgan joylarni tiklash bo'yicha chora-tadbirlar amalga oshirilayotgan edi) shubhasiz, katta madad bo'ldi.

O'zbekiston Respublikasi Prezidenti Sh.M.Mirziyoyev bu kabi xavf-xatarlar va ularga qarshi olib borilishi lozim bo'lgan kurash haqida shunday deydi: "O'zbekiston terrorizm, ekstremizm va radikalizm mafkurasiga qarshi kurash borasida hamisha prinsipial pozitsiyaga ega bo'lib kelgan. Bunday xavf-xatarlarga qarshi faqat kuch ishlatish usullari bilan emas, balki birinchi navbatda, ayniqsa, yoshlar o'rtasida, zo'ravonlikni keltirib chiqaradigan jaholatga qarshi ma'rifat bilan kurashish lozim" ekanligini ta'kidlaydi.

Xorijiy davlatlarning "radikalsizlantirish" dasturlarini o'rganish va tegishli xulosalar chiqarish O'zbekiston uchun ham foydali bo'lishi mumkin. Haqiqatan, ayrim davlatlarda "kuch ishlatmaslik" usullari orqali ko'plab ekstremistlarni zararsizlantirish va ularni osuda hayotga qaytarishga erishildi.

Yuqorida ko'rsatilgan mamlakatlar tajribalarini yetarlicha o'rganish, tadqiq qilish asnosida O'zbekistonda zo'ravon ekstremizmga qarshi kurashish, radikallashuv darajasini pasaytirish va jamiyatda bunday salbiy unsurlar ko'payishining oldini olish uchun kerakli tavsiyalar ishlab chiqildi. Ularni amaliyotga quyidagicha joriy qilish lozim deb hisoblaymiz:

1. Ekstremistik faoliyatga olib keladigan yoki jamiyatda radikalizm uchun asos bo'layotgan holatlarni aniqlash;

2. Yoshlarda dunyoviylik ruhiyatini mustahkamlaydigan ilmiy, ma'naviy tadqiqotlarni ko'paytirish va ularning xulosalarini amaliyotga joriy qilish;

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

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

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

6. Radikal kayfiyati yoki ekstremistik xulq-atvori aniqlangan toifalar bilan ishlashning ma'rifiy uslublarini joriy qilish, ularni jahon adabiyotining durdona asarlarini o'qishlari va anglashlari uchun shart-sharoit yaratish, zarur bo'lsa, bunga majbur qilish;

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

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

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

Qolaversa, 2022-yil 3-4-mart kunlari Toshkent shahrida "BMTning Global aksilterror strategiyasini amalga oshirish bo'yicha Birgalikdagi harakatlar rejasi doirasida Markaziy Osiyo mamlakatlarining mintaqaviy hamkorligi" mavzuida o'tkaziladigan xalqaro konferensiya g'oyat muhim va dolzarb ahamiyatga ega. Ushbu global anjuman mintaqa mamlakatlari va jahon hamjamiyati sa'y-harakatlarini terrorizmga qarshi hamjihatlik bilan kurashishda birlashtirish hamda faollashtirish uchun da'vat etishga qaratilgan.

O'zbekiston Respublikasi Prezidenti BMT Bosh Assambleyasining 75-sessiyasidagi nutqida ta'kidlaganidek, "Hozirgi vaqtda Markaziy Osiyo mintaqasida tub o'zgarishlar yuz bermoqda. Biz mintaqa davlatlari o'rtasida yaxshi qo'shnichilik va o'zaro ishonch, do'stlik va hurmat muhitini yaratishga erishdik. Birlashgan Millatlar Tashkiloti Bosh Assambleyasining 72-sessiyasida ilgari surilgan tashabbusga asosan muntazam o'tkazilayotgan Markaziy Osiyo davlatlari rahbarlarining Maslahat uchrashuvlari umumiy yutug'imiz bo'ldi". Davlatimiz rahbari BMT minbarida so'zlagan ushbu nutqida bugungi kunda Markaziy Osiyoda xavfsizlikni ta'minlash sohasida ham samarali hamkorlik olib borilayotgani haqida so'z yuritar ekan, Birlashgan Millatlar Tashkilotining Global aksilterror strategiyasi muvaffaqiyatli amalga oshirilayotganini e'tirof etdi. O'z navbatida, Prezidentimiz: "Biz ushbu strategiya doirasidagi Mintaqaviy qo'shma rejaning 10-yillik natijalari va kelgusi istiqbollariga bag'ishlangan xalqaro konferensiyani o'tkazish tarafdorimiz", deb ta'kidladi.

Xulosa o'rnida aytish kerakki, bugungi tahlikali davrda diniy ekstremizm, radikalizm va terrorizmga qarshi kurashning xorij tajribasini o'rganish, ibratli jihatlarini o'zlashtirish hamda hayotga tatbiq etish mavjud davlatlarning barchasi uchun bir xilda zarur va foydali. Diniy ekstremizm, radikalizm hamda terrorizmning asosiy o'chog'i bo'lgan Yaqin Sharq mintaqasida joylashgan arab mamlakatlari ushbu muammolarga qarshi kurashda dunyoning boshqa mintaqalari va davlatlariga nisbatan ko'proq tajribaga ega.

Yuqorida keltirilganlardan shunday xulosaga kelish mumkinki, internet global tarmog'i orqali sodir etiladigan jinoyatlar shakli va

turi shiddat bilan o'zgarish xususiyatiga ega bo'lib, so'nggi yillarda jinoiy qonun bilan qo'riqlanadigan ko'plab obyektlarga tahdid solmoqda. Shunga ko'ra, unga qarshi kurashda bu boradagi har bir ijtimoiy xavfli qilmishga individual jinoiy sanksiyalar bilan javob qaytarish samarali chora hisoblanishi xorijiy davlatlar tajribasidan anglanilmoqda.

2.3. Markaziy Osiyo davlatlarida kiberxavfsizlikni ta'minlashga innovatsion yondashuv va qo'llash mexanizmlari

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

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

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

Markaziy Osiyoning barcha davlatlari raqamli va kiberxavfsizlik sohasida ko'plab qonun hujjatlari, strategiyalar, konsepsiyalar qabul qildi va zamonaviy voqelikda bu sohadagi xavf va tahdidlar yanada kuchayishini anglab, o'z salohiyatini oshirishga intilmoqda. Biroq hukumatlar kiberhimoyani mustahkamlash va nafaqat o'z davlat manfaatlarini, balki, o'z mamlakatlari aholisining ma'lumotlarini

ham himoya qilish uchun e'tibor berishlari kerak bo'lgan ko'plab jihatlar bor.

Xususan, Qozog'iston o'z kibermakonini tashqi tahdidlardan himoya qilish uchun allaqachon ko'p ishlarni amalga oshirgan, shuningdek, mutaxassislar tayyorlashga katta e'tibor qaratmoqda. Masalan, "Qonunchilik darajasida hozirda xavfsizlikni ta'minlashning yanada amaliy yo'nalishlarini o'z ichiga oluvchi Milliy "Kiberqalqon 2.0 (Kibershit 2.0)" siyosatining ikkinchi talqini ishlab chiqilmoqda. Bundan tashqari, mas'uliyatni oshirish maqsadida "Ostona" xalqaro moliya markazi va milliy audit muhiti ishtirokida shaxsiy ma'lumotlarni himoya qilish siyosati ko'rib chiqilmoqda.

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

Tojikistonda kiberxavfsizlik masalasi Tojikiston Respublikasi axborot xavfsizligini ta'minlash Konsepsiyasida, Davlat axborot siyosati Konsepsiyada, bir qator boshqa idoraviy qonunlar bilan bog'liq kiberjinoyatchilik va zo'ravon ekstremizmga qarshi onlayn va oflayn rejimda tartibga solinadi.

O'zbekiston Respublikasida ham 2019-yilda "Shaxsga doir ma'lumotlar to'g'risida"gi Qonun qabul qilindi. Unda qanday tuzilma, shaxsiy ma'lumotlar nimadan iboratligi, ular qanday va qayerda saqlanishi belgilab qo'yildi. Bundan tashqari, 2022-yilda "Kiberxavfsizlik to'g'risida"gi O'zbekiston Respublikasining Qonuni qabul qilindi. Qonunga ko'ra, kibermakonda shaxs, jamiyat va davlat manfaatlarini tashqi va ichki tahdidlardan himoya qilish davlatning kiberxavfsizligini ta'minlashda ustuvor hisoblanadi.

Kiberhujumlarga qarshi kurash quvvatini ifodalovchi ko'rsatkichlardan biri, bu kiberxavfsizlik darajasi bo'lib, bu borada MDH ga a'zo ayrim davlatlarning "Global kiberxavfsizlik indeksi 2020" (GGI) hisoboti e'tiborga loyiqdir. Xususan, sobiq ittifoq mamlakatlarining pandemiya bilan bog'liq muammolarga qaramay, ko'plab faoliyat sohalari va ijtimoiy-iqtisodiy xizmatlarning raqamli formatga o'tishi, ushbu davlatlarning kiberxavfsizlik darajasini yaxshilash uchun ish olib borayotganidan dalolatdir.

Jumladan, respublikamizga qo'shni bo'lgan davlatlar Qozog'iston va Qirg'iziston respublikalarida bu borada amalga oshirayotgan ishlari natijasida, zararli kiberhodisalarning o'sishiga qaramasdan, ularning GCI ro'yxatida yuqori pog'onalarga siljishlari qayd etilgan.

Xususan, Qozog'istonda internet jinoyatlari soni 139 foizga o'sgan bo'lsa-da, Xitoy (33-o'rin) va Isroilni (36-o'rin) chetlab o'tib, 31-o'rinni, MDH davlatlari o'rtasida esa 2-o'rinni egallagan. Qirg'iziston Respublikasi davlat organlarida 2019-yildan beri 676 ming 918 ta zararli dasturiy ta'minot bartaraf etilgan, GCI ro'yxati bo'yicha 111-dan 92-pozitsiyasiga ko'tarilgan. Ushbu ro'yxatning 138-o'rnini Tojikiston egallagan. U MDH davlatidagi eng yaqin qo'shnisi Turkmanistondan (144) oldinda hisoblanadi, lekin Markaziy Osiyo mintaqasida Qozog'iston, O'zbekiston va Qirg'izistondan ortda qolgan.

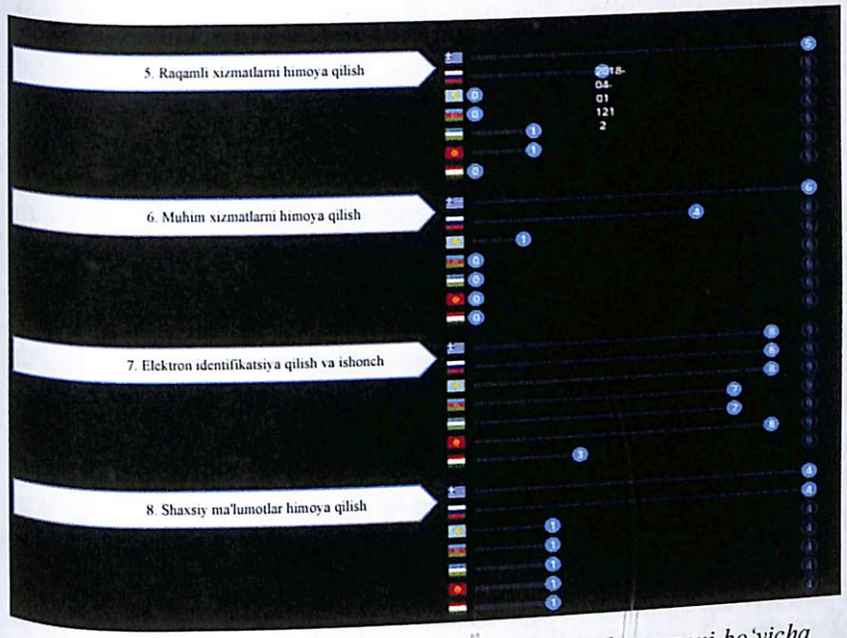
2022-yilda Estoniya Elektron boshqaruv akademiyasi tomonidan nashr etilgan Milliy kiberxavfsizlik indeksida (National cybersecurity index, NCSI) 160 ta davlat ichida O'zbekiston Respublikasi 31,17 reyting ko'rsatkichi bilan 95-o'rinda qayd etildi. Shuningdek, axborot kommunikatsiya texnologiyalarining rivojlanishi ko'rsatkichi bo'yicha 95-o'rinni egallagan.

Ushbu indeks 12 ta asosiy mezonlar kiritilgan 3 ta guruhdan iborat. Bularga:

1) kiberxavfsizlik umumiy mezonlari;
2) xavfsizlikning tayanch mezonlari;
3) mojaro va keskin o'zgarishlarda o'zini tutish mezonlari kiradi.

Har bir 12 mezon o'zaro bog'liq 46 ta ko'rsatkichlardan tashkil topgan. Har bir mezon o'lchovi maksimal 100 foiz etib belgilangan.

O'zbekiston Respublikasining NCSI indeksining har bir mezoni bo'yicha to'plagan baholari quyidagi diagrammada berilgan.



O'zbekiston Respublikasining NCSI indeksining har bir mezoni bo'yicha natijalari solishtirilgan jadval

Natijalardan ko'rinib turibdiki, 4 ta mezon bo'yicha O'zbekiston Respublikasi 50 foizdan ortiq ko'rsatkichga erishgan. Bunda "kibertahdidlarni tahlil qilish" – 60%, "ta'lim va kasbiy rivojlantirish" – 67%, "elektron identifikatsiya qilish va ishonch xizmatlari" – 78% va "kiberhodisalarga javob qaytarish" – 50% ko'rsatkichlarga ega bo'lgan.

Reytingda mavjud 46 ta indikator jami 77 ballni tashkil qilib, O'zbekiston 24 ball yoki 31,17 % ko'rsatkichga erishgan. Agar mutlaq "nol" qiymatdagi ko'rsatkichlarni kamida bitta pog'ona ko'tarishga erishiladigan bo'lsa, umumiy 54 ball yoki 70,13 % ko'rsatkich bilan reytingda 25-o'ringa ko'tarilish imkoniyati mavjud. Bu esa O'zbekistonni Osiyo davlatlari orasida 15-o'rindagi

Singapur (80,52 %) va 21-o'rindagi Malayziyadan (71,43 %) keyingi o'rinlarga olib chiqadi.

Positive Technologies tadqiqotchilarining ta'kidlashicha, kiberhujumlarning o'ziga xos xususiyati shundaki, ular masofadan turib, ko'pincha boshqa mamlakatlar hududidan amalga oshiriladi va dunyodagi biron-bir davlat ularga qarshi yakka o'zi kurashishga qodir emas. Ularning oldini olish uchun eng avvalo qonunchilikni takomillashtirish, shu jumladan, ushbu yo'nalishda xorijiy va xalqaro tashkilotlar bilan yaqin hamkorlikni mustahkamlash lozim.

– Xulosa va takliflar. Yuqoridagilardan kelib chiqib xulosa qilish mumkinki, jahonda, shu jumladan, respublikamizda kiberhujumlar va ular ko'lamining o'sish sur'ati saqlanib qoladi. Respublikamizda raqamlashtirish va axborot texnologiyalari rivojlanishi fonida kiberjinoyatlarning turlari, shakllarining o'zgarishi va takomillashib borishi kuzatiladi. Bu esa, vakolatli davlat organlari oldiga yangi vazifalarni qo'yish barobarida quyidagilarni amalga oshirish lozimligini taqazo etadi. Jumladan:

– Davlat korxona va muassasalari, shuningdek muhim axborot infratuzilmalari xodimlarining kiberxavfsizlik bo'yicha ko'nikma va malakalarini oshirishga qaratilgan tadbirlarni davom ettirish. Xususan, kiberxavfsizlik darajasi yuqori bo'lgan xorijiy mamlakatlar tajribasidan foydalangan holda mahalliy mutaxassislarni tayyorlash va ularning malakasini bugungi kun talabiga mos bo'lishini ta'minlash choralarini ko'rish, shuningdek, bu borada xorijiy va xalqaro tashkilotlar bilan hamkorlikni mustahkamlash;

– kiberxavfsizlik sohasidagi mavjud zaifliklarni minimallashtirish, muhim infratuzilmalarni muhofaza qilishga qaratilgan choratadbirlarni takomillashtirish hamda shaxsiy ma'lumotlarni himoya qilish choralarini ko'rish (shifrlash, antivirus, fayvol, raqamli imzolar va ikki faktorli autentifikatsiya va h.k.);

– zamonaviy voqelikda kibertahdid va kiberhujumlar darajasi va salmog'i, ularning keltirib chiqarishi mumkin bo'lgan talofatlarini inobatga olib, aholining keng qatlamlari orasida ularning savodxonligini oshirishga qaratilgan tushuntiruv-profilaktik tadbirlarni yanada kuchaytirish.

Ikkinchi bob bo'yicha xulosalar

Ilmiy adabiyotlarda "destruktiv g'oya" tushunchasiga ta'riflar mavjud, ammo ularda mazkur tushunchani anglashda yakdillik yo'q. Uning o'zagini "destruktivlik" tushunchasi tashkil etadi va belgilari amaliyotda ko'zga tashlanadi. Ammo aynan destruktivlik falsafada yetarli tadqiq etilmagan. Hatto "destruktiv", "destruktivlik", "destruktiv faoliyat" tushunchalari aksariyat lug'atlarda mavjud emas.

Destruktiv (buzg'unchi) g'oyalar uyushma, oqimlar tomonidan faoliyat yo'nalishi sifatida tanlangan va umuminsoniyat hayotiga xavf soluvchi, ijtimoiy taraqqiyotni tanazzulga olib boruvchi, odamlarning hukmronlikka intiluvchi kuchlarga tobe, qaram bo'lishini ta'minlovchi qarashlar, ta'limotlardir.

Bugun O'zbekiston Respublikasi hamda Markaziy Osiyo mintaqasi uchun xorijiy davlatlarning kiberterrorizm va ekstremizmga qarshi kurash yo'nalishidagi tajribasi, uning mintaqaviy hamkorlikka ta'siri juda muhim hisoblanadi. Buning uchun rivojlangan davlatlarning kiberxavfsizlikni ta'minlash borasidagi strategiyasini o'rganish va uni tahlil etib borish kerak. Shuningdek, AQSh, Xitoy, Hindiston, RF kabi davlatlardan kirib kelayotgan axborot texnologiyalarini olib kirish, ulardan foydalanishdan avval ularni mutaxassislar yordamida tekshiruvlardan o'tkazish lozim. Shuningdek, xorijiy rivojlangan davlatlar kiberxavfsizlik sohasida hamkorlik aloqalarini amalga oshirish jarayonida ularning milliy manfaatlarini nimalardan iborat ekanligi va bu mintaqa davlatlarining milliy manfaatlariga qanchalik javob berish jarayonini o'rganish asosida munosabat bildirish lozim hisoblanadi.

Markaziy Osiyo mintaqasining yoshlar qatlamiga ijtimoiy tarmoqlar orqali ta'sir ko'rsatayotgan kiberxurujlar va ularni bartaraf etish texnologiyalari bugungi zamonaviy siyosiy jarayonlarga qanchalik javob berishi, o'z vaqtida bartaraf etish mexanizmlari yaratilganligi bugungi kun uchun muhim sanaladi. Shu bilan birga mintaqa davlatlari bu borada yaxlit strategiya va priventiv yondashuvlar ishlab chiqishi lozim.

III BOB. MARKAZIY OSIYO MINTAQASIDA KIBERXAVFSIZLIKNI TA'MINLASH ISTIQBOLLARI

Raqamli dunyo maydonining kengayib borishi bilan xavfsizlik sohasida kiberxavfsizlik masalalarini o'rganuvchi yangi yo'nalish paydo bo'ldi. Kiberxavfsizlik turli xalqaro institutlar talqinida yoki neytral qabul qilingan axloqiy me'yorlarga va texnikaviy ifratuzilmalarga asoslangan bilimlarga tayanadi. Kiberxavfsizlik tezda texnik intizomdan strategik dasturga aylandi. Bugun ko'plab nufuzli xalqaro reytinglarda Markaziy Osiyo dunyoning eng xavfsiz mintaqalari qatoridan o'rin egallasa-da, ammo hamon o'zining fundamental yechimini kutayotgan kiberxavfsizlik masalasi bo'yicha amaliy ishlar qilinishi lozim hisoblanmoqda.

Markaziy Osiyo davlatlarida yangidan-yangi xavfsizlikka tahdidlar yuzaga kelayotgan sharoitda mintaqada kiberqurollardan foydalanib, tinchlikka tahdid solish holatlariga yo'l qo'ymaslik uchun davlatlar o'z kuch va imkoniyatlarini birlashtirishlari talab qilinadi. Markaziy Osiyoda axborot kurashi va axborot urushi ketmoqda. Bunday sharoitlarda noxush vaziyatlarning oldini olish uchun moliyaviy xarajatlar talab qilinadi, lekin hech bir Markaziy Osiyo davlati bu muammoni yolg'iz hal qila olmaydi. Shu sababdan ushbu bob "**Markaziy Osiyo mintaqasida kiberxavfsizlikni ta'minlash istiqbollari**" deb nomlandi hamda uning tarkibiy qismi sifatida "O'zbekiston Respublikasining kiberxavfsizlikni ta'minlashda tajribasi" hamda "Mintaqada kiberxavfsizlikni ta'minlashning takomillashtirish mexanizmlari"ni ko'rib chiqish, bu bo'yicha tegishli taklif va tavsiyalarni berish mazkur bobning asosiy maqsadi etib belgilandi.

3.1. O'zbekiston Respublikasining kiberxavfsizlikni ta'minlash tajribasi

Hozirgi kunda axborot sohasida yuz berayotgan o'zgarishlar mazkur sohada axborot xavfsizligini ta'minlovchi mexanizmlarni mustahkamlashga oid chora-tadbirlarni ishlab chiqish mamlakatning rivojlanishiga xizmat qiladi. O'zbekistonda oxirgi yillarda axborot sohasiga, xususan, axborot xavfsizligini ta'minlashga oid qonunchilik bazasini mustahkamlash, jurnalist kadrlarni tayyorlash va malakasini oshirish, OAV xodimlarining jamiyatni demokratlashtirish, tub islohotlarni amalga oshirishdagi ishtirokini faollashtirish yuzasidan muhim tadbirlar bajarildi. Jumladan, O'zbekiston Respublikasida kiberxavfsizlik sohasiga tegishli bo'lgan 17 ta qonun hujjati, 9 ta Prezident Farmon va Qarorlari, 14 ta Vazirlar Mahkamasining Qarori, shuningdek tegishli normalar va ko'plab idoralararo me'yoriy-huquqiy hujjatlar qabul qilingan edi. Ammo shu bilan birga bu borada ayrim xavf va tahdidlar masalasi saqlanib qolinayotgan edi:

– qonunchilikda axborot xavfsizligiga doir huquqiy normalar qisman amalga oshirilganligi;

– davlat organlari va aloqa operatorlari o'rtasida kiberhujumlarni kuzatish ularning oqibatlarini bartaraf etish bo'yicha o'zaro hamkorlik tizimining mavjud emasligi;

– davlat axborot-kommunikatsiya infratuzilmasi obyektlari identifikatsiya qilinmagan va tasdiqlanmagan holda qolayotganligi;

– muhim axborot infratuzilmasi obyektlarida axborot tizimlari va resurslarining xavfsizlik tizimlarining baholash usullari mavjud emasligi saqlanib qolayotgan edi. Shu sababli bo'lsa kerak, O'zbekiston Respublikasining Prezidenti Sh.M.Mirziyoyev bu xususda quyidagilarni ta'kidlab o'tganlar: "Mamlakatimizda demokratik islohotlarni yanada chuqurlashtirish va fuqarolik jamiyatini rivojlantirish konsepsiyasini amalga oshirishda biz, ilgarigidek, fuqarolarning o'zini o'zi boshqarish organlari – mahallalar, shuningdek, nodavlat notijorat tashkilotlar, erkin va xolis ommaviy axborot vositalari faol o'rin egallaydi, deb

ishonamiz".[76] Shu o'rinda, 2017-yilda "Ijtimoiy fikr" jamoatchilik fikrini o'rganish markazi tomonidan aholi o'rtasida "Fuqarolar davlat boshqaruvi va mahalliy hokimiyat organlari faoliyatining samaradorligi to'g'risida" mavzusida so'rovnoma o'tkazilganligini aytib o'tish joiz. So'rovning ko'rsatishicha, o'zbekistonliklarning 80,6 %i fuqarolarning xavfsizligi, huquqlari, erkinliklari va qonuniy manfaatlari ta'minlanganligini yuqori baholaganligini ko'rish mumkin.[77] Ammo bu borada hali o'z yechimini kutayotgan muammolar bor ekanligi ko'rinadi.

Mustaqillik yillarida O'zbekistonning kiberxavfsizlikni ta'minlash tajribasining siyosiy-huquqiy asoslari shakllanishiga ko'ra 4 bosqichga bo'linadi:

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

– ikkinchi bosqich 2002–2012-yillarda axborot sohadagi siyosiy-huquqiy o'zgarishlarni o'z ichiga oladi. Mazkur bosqichda axborot sohasi yo'nalishlarining mustahkamlanishi, institutsional jihatdan takomillashishiga e'tibor qaratildi.

– uchinchi bosqich 2013–2016-yillardagi davrni qamrab oladi. Ushbu bosqichda axborot xavfsizligini ta'minlashga oid davlat siyosatini amalga oshirishga xizmat qiluvchi mutasaddi tashkilotlarni tashkil etish huquqiy me'yorlar bilan mustahkamlandi.

Jumladan, "Aloqa to'g'risida"gi (1992), "Davlat sirlarini saqlash to'g'risida"gi (1993), "Elektron hisoblash mashinalari uchun yaratilgan dasturlar, ma'lumotlar bazalarining huquqiy himoyasi to'g'risida"gi (1994), "Noshirlik faoliyati to'g'risida" (1996), "Axborot olish kafolatlari va erkinliklari to'g'risida"gi (1997), "Jurnalistik faoliyatni himoya qilish to'g'risida"gi (1997),

[76] Mirziyoyev Sh.M. O'zbekiston Respublikasi Prezidenti lavozimiga kirishish tantanali marosimiga bag'ishlangan Oliy Majlis palatalarining qo'shma majlisidagi nutqidan, Toshkent shahri, 14.12.2016.

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

"Ommaviy axborot vositalari to'g'risida"gi (1997), "Radiochastota spektri to'g'risida"gi (1998), "Reklama to'g'risida"gi (1998), "Telekommunikatsiyalar to'g'risida"gi (1999) qonunlarda axborot sohasiga oid normativ-huquqiy bazani yaratishga asosiy e'tibor qaratilgan. Keyingi yillarda qabul qilingan "Axborot erkinligi va prinsiplari to'g'risida"gi (2002), "Pochta aloqasi to'g'risida"gi (2000), "Axborotlashtirish to'g'risida"gi (2003), "Elektron raqamli imzo to'g'risida"gi (2003), "Elektron hujjat aylanishi to'g'risida"gi (2004), "Elektron tijorat to'g'risida"gi (2004), "Elektron to'lovlar to'g'risida"gi (2005), "Mualliflik huquqi va turdosh huquqlar to'g'risida"gi (2006), "Davlat hokimiyati va boshqaruvi organlari faoliyatining ochiqligi to'g'risida"gi (2014), "Jismoniy va yuridik shaxslarning murojaatlari to'g'risida"gi (2014), "Huquqiy axborotni tarqatish va undan foydalanishni ta'minlash to'g'risida"gi (2017), "Bolalarni ularning sog'lig'iga zarar yetkazuvchi axborotdan himoya qilish to'g'risida"gi (2017) qonunlarda axborot sohasining turli yo'nalishlarida axborot munosabatlarini tartibga solish hamda respublikada axborot xavfsizligini ta'minlashga urg'u berilganligini ko'rish mumkin.

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

O'zbekiston Respublikasining 2015-yil 9-dekabrda e'lon qilingan "Elektron hukumat to'g'risida"gi qonunining[78] 112-moddasi "Axborot xavfsizligini ta'minlash prinsipi" deb nomlanadi. Ushbu moddaga binoan elektron davlat xizmatlari ko'rsatuvchi davlat organlari elektron davlat xizmatlari ko'rsatishda foydalaniladigan axborot tizimlari va axborot resurslarining axborot xavfsizligini ta'minlashi shart deb belgilab qo'yildi.

Yuqoridagilarni ro'yobga chiqarish maqsadda, 2017-yildan boshlab Yangi O'zbekiston taraqqiyotida kiberxavfsizlik muammosini yaratishning yangi bir institutsional davri boshlandi, desak mubolag'a bo'lmaydi. Xususan, 2020–2023-yillarga mo'ljallangan kiberxavfsizlikka doir milliy strategiyani, "Kiberxavfsizlik to'g'risida"gi qonun loyihasini hamda O'zbekiston Respublikasi yagona axborot siyosati konsepsiyasi ishlab chiqish belgilandi. O'zbekiston Respublikasi Prezidentining 2018-yil 21-noyabrdagi "Axborot texnologiyalari va kommunikatsiyalarining joriy etilishini nazorat qilish, ularni himoya qilish tizimini takomillashtirishga oid qo'shimcha chora-tadbirlar to'g'risida"gi Qarori hisoblanadi. Mazkur Qarorga asosan, "Texnik ko'maklashish markazi" davlat unitar korxonasi "Kiberxavfsizlik markazi"ga aylantirildi. Aynan mazkur markazni qayta tashkil etishdan ham maqsad mamlakatimizda "xavfsiz axborotlashgan jamiyat" muhitini yaratishga qaratilgan ustuvor islohotlar, vazifalar belgilab berilgan.

Markaz dastlab O'zbekiston Respublikasi Axborot texnologiyalari va kommunikatsiyalarini rivojlantirish vazirligi huzuridagi "Axborot xavfsizligini ta'minlash markazi" davlat muassasasi nomi bilan O'zbekiston Respublikasi Prezidentining 2013-yil 27-iyundagi "O'zbekiston Respublikasining Milliy axborot-kommunikatsiya tizimini yanada rivojlantirish chora-tadbirlari to'g'risida"gi PQ-1989-son Qarori va O'zbekiston Respublikasi Vazirlar Mahkamasining 2013-yil 16-sentyabrdagi "O'zbekiston Respublikasi Aloqa, axborotlashtirish va telekommunikatsiya texnologiyalari davlat qo'mitasi huzuridagi "Elektron hukumat"

[78] O'zbekiston Respublikasining 2015-yil 9-dekabrda e'lon qilingan "Elektron hukumat to'g'risida"gi Qonuni// https://lex.uz/mobileact/2833860

tizimini rivojlantirish markazi hamda Axborot xavfsizligini ta'minlash markazi faoliyatini tashkil etish chora-tadbirlari to'g'risida"gi 250-son qaroriga muvofiq faoliyat yuritadigan davlat muassasasi shaklidagi notijorat tashkiloti sifatida o'z faoliyatini boshlagan.

Keyinchalik O'zbekiston Respublikasi Prezidentining "Axborot-kommunikatsiya texnologiyalari sohasidagi loyihalarni boshqarish tizimini yanada takomillashtirish chora-tadbirlari to'g'risida" 2017-yil 29 avgustdagi PQ-3245-son 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 Vazirlar Mahkamasi qarori bilan O'zbekiston Respublikasi Axborot texnologiyalari va kommunikatsiyalarini rivojlantirish vazirligining Axborot xavfsizligini ta'minlash markazi O'zbekiston Respublikasi Axborot texnologiyalari va kommunikatsiyalarini rivojlantirish vazirligining Axborot xavfsizligi va jamoat tartibini ta'minlashga ko'maklashish markazi etib qayta tashkil etildi.

So'ngra, O'zbekiston Respublikasi Axborotlashtirish va telekommunikatsiyalar sohasida nazorat bo'yicha davlat inspeksiyasining "Texnik ko'maklashish markazi" davlat unitar korxonasi nomi bilan O'zbekiston Respublikasi Prezidentining Axborot texnologiyalari va kommunikatsiyalarining joriy etilishini nazorat qilish, ularni himoya qilish tizimini takomillashtirish chora - tadbirlari to'g'risida"gi 2018-yil 21-noyabrdagi PQ-4024-son qaroriga muvofiq faoliyat yuritadigan davlat unitar korxonasi shaklidagi tashkilot sifatida faoliyat yuritdi.

Hozirda, "Kiberxavfsizlik markazi" davlat unitar korxonasi nomi bilan 14.09.2019-yildagi PQ-4452-son O'zbekiston Respublikasi Prezidentining "Axborot texnologiyalari va kommunikatsiyalarining joriy etilishini nazorat qilish, ularni himoya qilish tizimini takomillashtirishga oid qo'shimcha chora-tadbirlar to'g'risida"gi qaroriga muvofiq faoliyat yuritib kelmoqda.

Markazning asosiy vazifalari quyidagilardan iborat:

Axborot xavfsizligiga hozirgi vaqtdagi tahdidlar to'g'risidagi ma'lumotlarni yig'ish, tahlil qilish va to'plash, davlat organlari va tashkilotlari axborot tizimlari, resurslari va ma'lumotlar bazalariga noqonuniy kirib olish holatlarining oldini olishni ta'minlaydigan samarali tashkiliy va dasturiy-texnik yechimlarni tezkor qabul qilish bo'yicha tavsiyalar va takliflar ishlab chiqish;

Qonun buzuvchilarni, axborotlar makonidagi ruxsatsiz yoxud buzuvchi harakatlarni amalga oshirishda foydalaniladigan metodlar va vositalarni tahlil qilish, identifikatsiyalashda telekommunikatsiyalar tarmoqlarining operatorlari va provayderlari, huquqni muhofaza qilish organlari bilan hamkorlik qilish;

Axborotlashtirish obyektlarida (davlat sirlari bundan mustasno) apparat vositalari va dasturiy mahsulotlarni, axborot-kommunikatsiya texnologiyalari, telekommunikatsiya jihozlari va boshqa texnik vositalarni attestatsiya, ekspertiza va sertifikatsiyadan o'tkazish;

Davlat organlari va tashkilotlari axborot tizimlari va resurslari axborot xavfsizligi siyosatini ishlab chiqish va amalga oshirishda ko'maklashish;

Davlat axborot tizimlari va resurslari, shuningdek, internet tarmog'i milliy segmentining axborot xavfsizligini ta'minlash sohasidagi normativ-huquqiy bazani takomillashtirish bo'yicha takliflar ishlab chiqish;

Internetning milliy foydalanuvchilarini internet tarmog'i milliy segmentida axborot xavfsizligiga paydo bo'layotgan tahdidlar to'g'risida o'z vaqtida xabardor qilish, shuningdek, axborotlarni himoya qilish bo'yicha maslahat xizmatlari ko'rsatish.[79]

Qolaversa, O'zbekiston so'nggi yillarda xalqaro reytinglarda ishtirok etishining normativ-huquqiy asoslari ham belgilab berildi. Bundan maqsad, O'zbekiston Respublikasining iqtisodiy va siyosiy-huquqiy xalqaro reyting va indekslarda o'rnini yaxshilash, bu borada mutasaddi vazirlik va idoralarning faoliyatini samarali muvofiqlashtirish, xalqaro maydonda mamlakatimiz

[79] https://csec.uz/uz/company/

mavqeyini yanada yuksaltirish, xorijiy reyting agentliklari bilan hamkorlikda tizimli ravishda islohotlar amalga oshirilmoqda. Xususan, O'zbekiston Respublikasi Prezidentining O'zbekiston Respublikasi Prezidentining 2019-yil 7-martdagi "Xalqaro reyting va indekslarda O'zbekiston Respublikasining o'rnini yaxshilashga oid chora-tadbirlarni tizimlashtirish to'g'risida"gi[80] PF-5687-sonli hamda 2020-yil 2-iyundagi "O'zbekiston Respublikasining xalqaro reyting va indekslardagi o'rnini yaxshilash hamda davlat organlari va tashkilotlarida ular bilan tizimli ishlashning yangi mexanizmini joriy qilish to'g'risida"gi PF-6003-son farmonlari qabul qilindi.[81] Mazkur farmon bilan O'zbekiston Respublikasi uchun ustuvor bo'lgan xalqaro reyting va indekslar bo'yicha samaradorlikning eng muhim ko'rsatkichlari (keyingi o'rinlarda – KPI) tasdiqlandi. Bu ko'rsatkichlarni tizimli tahlil qilib borish maqsadida Xalqaro reyting va indekslar bilan ishlash bo'yicha respublika kengashi tashkil etildi. Mazkur kengashning asosiy vazifasi etib:

– mamlakatning ijtimoiy-iqtisodiy va siyosiy-huquqiy taraqqiyot darajasini tizimli tahlil qilib borish, turli sohalarda amalga oshirilayotgan tub o'zgarishlarning O'zbekiston Respublikasi uchun ustuvor bo'lgan xalqaro reyting va indekslarda mamlakatning o'rnini yaxshilash maqsadlariga xizmat qilishini ta'minlash, mazkur yo'nalishdagi ishlarning samaradorligiga to'siq bo'layotgan muammolarni bartaraf etish;

– O'zbekiston Respublikasi uchun ustuvor bo'lgan xalqaro reyting va indekslarda mamlakatning o'rnini yaxshilash maqsadida davlat hokimiyati va boshqaruvi tizimini takomillashtirish, jamiyatni demokratlashtirish, ilg'or xalqaro tajribaga asoslangan davlat va jamiyat qurilishi sohasidagi islohotlarni amalga oshirish bo'yicha tashabbuslarni ilgari surish;

[80] O'zbekiston Respublikasi Prezidentining 2019-yil 7-martdagi "Xalqaro reyting va indekslarda O'zbekiston Respublikasining o'rnini yaxshilashga oid chora-tadbirlarni tizimlashtirish to'g'risida"gi PF-5687-sonli Farmoni/ https://lex.uz/docs/4230916

[81] O'zbekiston Respublikasi Prezidentining 2020-yil 2-iyundagi "O'zbekiston Respublikasining xalqaro reyting va indekslardagi o'rnini yaxshilash hamda davlat organlari va tashkilotlarida ular bilan tizimli ishlashning yangi mexanizmini joriy qilish to'g'risida"gi PF-6003-son Farmoni/ https://lex.uz/docs/4838762

– davlat va jamiyat hayotining turli jabhalarini tartibga solishga qaratilgan normativ-huquqiy hujjatlar va ularning loyihalarini O'zbekiston Respublikasi uchun ustuvor bo'lgan xalqaro reyting va indekslardagi mamlakatning o'rniga ta'siri nuqtayi nazaridan kompleks baholab borish belgilab qo'yilgan. Mazkur Kengash o'z faoliyatini ijtimoiy-iqtisodiy va siyosiy-huquqiy reyting va indekslar sohada ishchi guruhlarga bo'lingan holda xalqaro reyting va indekslar bo'yicha olib boradi. Aynan O'zbekistonning xalqaro reyting va indekslarda o'rnini yaxshilash borasida olib borayotgan islohotlarida Elektron hukumatni rivojlantirish indeksi (E-Government Development Index)da:

O'zbekiston Respublikasi Prezidentining 2020-yil 5-oktyabrdagi Farmoni bilan "Raqamli O'zbekiston – 2030" strategiyasi"[82] tasdiqlandi. Mazkur strategiyada ham mamlakatimizda raqamli iqtisodiyotni faol rivojlantirish, barcha tarmoqlar va sohalarda, eng avvalo, davlat boshqaruvi, ta'lim, sog'liqni saqlash va qishloq xo'jaligida zamonaviy axborot-kommunikatsiya texnologiyalarini keng joriy etish belgilab qo'yilgan. Xususan, strategiyada "Raqamli O'zbekiston – 2030" strategiyasining maqsadli ko'rsatkichlari, transformatsiya qilish dasturi, amalga oshirish bo'yicha muvofiqlashtirish komissiyasi, tarmoqlar va hududlarni axborot texnologiyalari sohasida O'zbekiston Respublikasining xorijiy mamlakatlardagi diplomatik vakolatxonalariga biriktirish bo'yicha "Yo'l xaritasi" ishlab chiqilgan. Umuman olganda mazkur normativ-huquqiy hujjatlar O'zbekistonda raqamli texnologiyalarni rivojlantirish asosida xalqaro imijini oshirishga qaratilgan chora-tadbirlar hisoblanadi.

O'zbekiston Respublikasi kibermakonda kiberxavfsizlik masalalariga yagona yondashuvni belgilash maqsadida O'zbekiston Respublikasi Davlat xavfsizlik xizmati tomonidan "Kiberxavfsizlik to'g'risida"gi O'zbekiston Respublikasi qonuni loyihasi ishlab chiqildi.

[82] O'zbekiston Respublikasi Prezidentining 2020-yil 5-oktyabrdagi "Raqamli O'zbekiston – 2030" strategiyasi" va uni samarali amalga oshirish chora-tadbirlari to'g'risida"gi Farmoni / https://lex.uz/docs/5030957

Ushbu qonun loyihasini tayyorlash jarayonida kiberxavfsizlik sohasida rivojlangan xorijiy davlatlar Rossiya, Xitoy, AQSh, Qozog'iston, Singapur tajribalari o'rganilib, tahlil qilindi. O'zbekiston Respublikasi "Kiberxavfsizlik to'g'risida"gi qonun loyihasi ishlab chiqish jarayonida manfaatdor vazirlik va idoralarning ekspertlarini jalb qilgan holda ishchi guruh tashkil etilgan bo'lib, bahslar, uchrashuvlar, seminarlar va videokonferensiyalar o'tkazildi.

"Kiberxavfsizlik to'g'risida"gi qonun loyihasi Qonunchilik palatasi tomonidan 2022-yil 25-fevral kuni qabul qilingan. Senat tomonidan 2022-yil 17-mart kuni ma'qullangan. 2022-yil 15-aprel kuni Prezident tomonidan imzolangan.[83] Qonun 8 ta bob, 40 ta moddadan iborat bo'lib, 2022-yil 17-iyuldan qonuniy kuchga kirgan. O'zbekistonda kiberxavfsizlik sohasidagi yagona davlat siyosatini prezident belgilaydi; Davlat xavfsizlik xizmati esa kiberxavfsizlik sohasidagi vakolatli davlat organi hisoblanadi.

Qonun quyidagilarni ta'minlaydi:

– respublika miqyosida kiberxavfsizlikni ta'minlashga doir davlat siyosatini amalda joriy etilishi;

– davlat tomonidan kiberxavfsizlikni ta'minlashning huquqiy, tashkiliy, ilmiy-texnikaviy va normativ-uslubiy tamoyillarini tartibga solish;

– axborot tizimlari va resurslarining yaxlitligini saqlash;

– axborotni yo'q qilish, o'zgartirish, buzib ko'rsatish, nusxa ko'chirish, bloklash kabi ruxsat etilmagan harakatlarga yo'l qo'ymaslik;

– O'zbekiston Respublikasining axborot tizimlari va tarmoqlariga noqonuniy aralashuvning boshqa shakllariga yo'l qo'ymaslik, tizimni takomillashtirish.

Kiberxavfsizlikni ta'minlashning asosiy prinsiplari

Qonunga ko'ra, kibermakonda shaxs, jamiyat va davlat manfaatlarini tashqi va ichki tahdidlardan himoya qilish davlatning kiberxavfsizligini ta'minlashda ustuvor hisoblanadi. Shuningdek,

[83] O'zbekiston Respublikasining "Kiberxavfsizlik to'g'rsida"gi Qonuni. https://lex.uz/uz/docs/5960604

kiberxavfsizlikni ta'minlashning quyidagi asosiy prinsiplari belgilangan:

– qonuniylik;

– kibermakonda shaxs; jamiyat va davlat manfaatlarini himoya qilishning ustuvorligi;

– kiberxavfsizlik sohasini tartibga solishga nisbatan yagona yondashuv;

– kiberxavfsizlik tizimini yaratishda mahalliy ishlab chiqaruvchilar ishtirokining ustuvorligi;

– O'zbekiston Respublikasining kiberxavfsizlikni ta'minlashda xalqaro hamkorlik uchun ochiqligi.

Yuqoridagilardan kelib chiqib aytish mumkinki, bu tahlillar kiberxavfsizlik masalasining dolzarbligini yana bir bor tasdiqlaydi, boisi dasturiy zaifliklar buzg'unchiga axborot tizimi yoki veb-sayt, shuningdek, fayl va ma'lumotlarga masofadan kirish, fuqarolarning shaxsiy ma'lumotlari chiqib ketishiga sabab bo'lishi mumkin. Kiberxavfsizlik choralari bu kabi holatlarning oldini oladi.

Fuqarolarni kiberhujumlardan himoyalash uchun ommaviy axborot vositalarida, axborot tarqatuvchi qurilmalarda va elektron pul o'tkazmalari jarayonlarida himoyalovchi kod (parol)lardan foydalanish zarur. Ushbu kod sir saqlanishi, qurilmalardagi antivirus dasturlari doimiy ravishda faollashtirib borilishi kerak.

O'zbekiston raqamli iqtisodiyotga asta-sekin o'tmoqda. Bunday sharoitda ma'lumotlarni saqlash, yetkazish va qayta ishlashda xavfsizlik va barqarorlik muhim omil hisoblanadi. Bu borada, ayniqsa, davlat organlari xodimlaridan mas'uliyat va e'tibor talab etiladi. Aholi, yoshlar o'rtasida, jamoalarda kiberxavfsizlik mavzusidagi seminarlar tashkil etish lozim. Bu kabi tadbirlar dastur buzuvchi (xaker)larning muntazam kichik hujumlarini bartaraf etishga yordam beradi.

Umuman olganda, O'zbekistonda kiberxavfsizlikni ta'minlash bo'yicha olib borilayotgan tizimli va fundamental yondashuv, yagona normativ-huquqiy hujjatlar bazasini yaratish, ilg'or xorijiy tajribani joriy etish, innovatsion usullardan keng foydalanish davlat axborot siyosatini samarali olib borishga hamda axborot

xavfsizligi sohasidagi muammolarni hal etishga xizmat qiladi. Bu esa axborot kommunikatsiya va texnologiyalari tizimini zamonaviy kibertahdidlardan himoya qilish, turli darajadagi tizimlar uchun kiberxavfsizlik bo'yicha zamonaviy mexanizmlarni joriy etish, mazkur sohada davlat organlari, korxonalar va tashkilotlarning huquqlari va majburiyatlarini belgilash, ularning faoliyatini muvofiqlashtirish kabilarni amalga oshirish orqali belgilanadi. Bu sohadagi normativ-huquqiy hujjatlarni unifikatsiyalash orqali kiberxavfsizlikni ta'minlashni takomillashtirish mumkin.

"Bugungi kunda raqamli iqtisodiyotning mamlakat yalpi ichki mahsulotidagi ulushi 2,2 foizni tashkil etmoqda. Raqamli iqtisodiyotning O'zbekiston yalpi ichki mahsulotidagi ulushini 2023-yilga qadar ikki barobarga, elektron hukumat xizmatlari ulushini esa 2022-yilga kelib 60 foizgacha oshirish rejalashtirilgan", – deydi Axborotlashtirish va telekommunikatsiyalar sohasida nazorat bo'yicha davlat inspeksiyasi boshlig'i G'olibsher Ziyayev.[84] Shundan ham ko'rish mumkinki, mamlakatimizda kiberxavfsizlik sohasida olib borilayotgan amaliy harakatlarning mintaqada xavfsizlikni ta'minlash uchun yetarli emasligini ko'rsatadi. Bu borada Shavkat Mirziyoyev quyidagilarni ta'kidlaydi: "MDH davlatlari doirasida raqamli iqtisodiyotni rivojlantirish va xavfsizlik masalalariga bag'ishlangan tadbirlar o'zaro hamkorligimiz ifodasidir. Axborot xavfsizligini to'g'ri isloh qilishda bitta davlatning sa'y-harakatlari yetmasligini" e'tirof etadi. Shu sababli ham mintaqa davlatlari bu borada axborot va kiberxavfsizlikni ta'minlash, raqamli iqtisodiyot, shuningdek, ushbu sohada ixtisoslashgan mutaxassislarni tayyorlash bo'yicha izchil hamkorlik aloqalarini olib borishi lozim.

O'zbekiston Respublikasi Prezidenti Shavkat Mirziyoyevning 2022-yil 27-yanvardagi "Hindiston – Markaziy Osiyo" birinchi sammitida ham IT sohasida mintaqaviy hamkorlikni rivojlantirish maqsadida raqamli innovatsiyalar, moliyaviy va blokcheyn texnologiyalarni joriy qilish, kiberxavfsizlikni ta'minlash, mutaxassislar tayyorlash kabi yo'nalishlarda harakatlar dasturini ishlab

[84] https://gov.uz/uz/news/view/31375

chiqishni[85] taklif etganligini o'zi ham kiberxavfsizlik sohasidagi muammolarning naqadar chuqur ekanligini ko'rsatib beradi.

Bugungi kunda ekstremizm va terrorizm alohida mamlakatlarning milliy xavfsizligi va umuman jahon hamjamiyatiga jiddiy tahdid uyg'otayotgan omilga aylandi. Umumbashariy muammoga aylangan ekstremizm va terrorizmni jahon hamjamiyati faqat birgalikda, turli tor geosiyosiy manfaatlardan voz kechgan holda harakat qilibgina yenga olishi mumkinligi aksariyat davlatlar tomonidan tan olingan ayni haqiqatdir. Shu sababli bugun ijtimoiy tarmoqlar orqali yoshlarning turli xil oqimlarga aralashib qolishi oqibatida ekstremistik guruhlar ta'siriga tushib qolmoqda.

O'zbekiston bu borada katta tajribaga ega davlat sifatida o'z tajribasini ko'rsatmoqda. Bu borada juda ko'p normativ-huquqiy hujjatlar qabul qilindi. Hatto, O'zbekiston Respublikasining Birinchi Prezidenti Islom Karimovning: "O'zbekiston XXI asr bo'sag'asida: xavfsizlikka tahdid, barqarorlik shartlari va taraqqiyot kafolatlari" asarida mamlakatimiz tinchligi va suverenitetiga tajovuz etuvchi turli tahdidlarni va ularni bartaraf etish vazifalarini aniq va izchil yoritib berganlar. Ular asosida mamlakatning kuch ishlatar tuzullmalari tarkibida alohida bo'linmalar tashkil etildi. Natijada mamlakatimizda ekstremizm va terrorizmga qarshi kurashish bo'yicha institutsional tizim shakllandi.

So'nggi yillarda O'zbekiston taraqqiyotining yangi bosqichida, xususan, 2018-yil 30-iyulida O'zbekiston Respublikasining "Ekstremizmga qarshi kurashish to'g'risida"gi Qonuni qabul qilindi. Mazkur qonunda ekstremizm faoliyati, ekstremizm bilan shug'ullanuvchi guruh va tashkilot hamda ushbu faoliyatni moliyalashtirishning oqibatlari yuzasidan tushunchalar ochib berildi.

Bu borada Prezidentimiz Sh.M.Mirziyoyev ham bu masala yuzasidan: "Ayni vaqtda dunyoning ba'zi mintaqalarida yuzaga kelgan notinch vaziyat aholi migratsiyasi kuchayishiga, bu esa, o'z navbatida, terrorizm va ekstremizmning tarqalishiga hamda ularning

[85] O'zbekiston Respublikasi Prezidenti Shavkat Mirziyoyevning "Hindiston – Markaziy Osiyo" birinchi sammitidagi nutqi.// https://president.uz/uz/lists/view/4944

global muammolardan biriga aylanishiga olib kelmoqda. Bunday vaziyatda milliy davlatchiligimiz, mustaqilligimiz, aholimizning tinch va osoyishta hayoti va xavfsizligimizni saqlash biz uchun eng ustuvor vazifaga aylanib bormoqda", deb so'zlagani ham muammoning dolzarb ekanligini ko'rsatadi. Chunki kiberterrorizm, kiberekstremizm masalasi "virtual muloqot" turi sifatida rivojlanib bormoqda. Uning ta'sirida yoshlar tushib qolishi masalaning eng yomon jihati sanaladi. Shu sababli muhtaram Prezidentimiz Sh.M.Mirziyoyev jahon hamjamiyati e'tiborini Markaziy Osiyoda xavfsizlik va barqarorlikni ta'minlash maqsadida amaliy hamkorlikni yanada mustahkamlash, terrorizm va ekstremizm, transmilliy jinoyatchilik va narkotrafik tahdidlariga qarshi samarali kurashishni BMT preventiv diplomatiya usullaridan foydalangan holda, shuningdek, MDH, ShHT, YeXHT va boshqa nufuzli xalqaro hamda mintaqaviy tuzilmalar mexanizmlari doirasida ta'minlash mumkin ekaniga, xavfsizlikka tahdidlarni "o'ziniki va o'zgalarniki" deb ajratishdan voz kechish, "yaxlit xavfsizlik" tamoyiliga amalda rioya qilish zarurligiga qaratmoqda.[86]

O'zbekiston ekstremizm va terrorizm tahdidlari, zararlarini boshidan kechirgan mamlakat hisoblanadi. Yurtimizda ushbu illatlarga qarshi kurashish, uning sabablari oldini olish bo'yicha jahon hamjamiyatiga namuna bo'la oladigan darajada o'ziga xos tajriba shakllangan.

Respublikamizda Prezidentimiz boshchiligida hukumatimiz tomonidan ekstremizm va terrorizmga qarshi kurash borasida jahon hamjamiyati uchun namuna bo'lishi mumkin bo'lgan samarali ishlar qatorida quyidagilarni qayd etish mumkin:

To'g'ri yo'ldan adashganlarni ijtimoiy reabilitatsiya qilish va ularni sog'lom hayotga qaytarish maqsadida mazkur shaxslar bilan keng jamoatchilikni jalb etgan holda tushuntirish-profilaktika ishlarini tizimli tashkil qilish, ularni maxsus ro'yxatdan chiqarish bo'yicha mexanizm yaratildi. Mazkur mexanizmning samarasi sifatida aqidaparastlik g'oyalari ta'siriga tushgan 16 mingdan

[86] Ekstremizm va terrorizmga qarshi kurashda O'zbekiston tajribasi.// https://iiv.uz/oz/news/ekstremizm-va-terrorizmga-qarshi-kurashda-ozbekiston-tajribasi

ziyod fuqarolarning ichki ishlar organlarining maxsus hisobidan chiqarilishi jamiyatda katta ijobiy rezonans berdi.

Yoshlarni ilm-ma'rifatga o'rgatish, ularga islom dinining insonparvarlik mohiyati, islom madaniyatining asl qadriyatlarini yetkazish, ma'rifiy islom ta'limoti, buyuk ajdodlarimizning ulkan ma'naviy merosini chuqur o'rganish, jamiyatda diniy va milliy bag'rikenglik va hamkorlikni mustahkam qaror toptirish orqali aholi, ayniqsa, yoshlarda aqidaparast g'oyalarga nisbatan mustahkam ma'naviy himoya qobig'i shakllantirish maqsadida Imom Buxoriy va Imom Termiziy xalqaro ilmiy-tadqiqot markazlari faoliyati yo'lga qo'yildi. Samarqandda hadis va kalom ilmi maktabi, Buxoroda tasavvuf maktabi, Qashqadaryoda aqida maktabi, Farg'onada islom huquqi (fiqhi) ilmiy maktablari ochildi. Shuningdek, Davlat Rahbari darajasida respublikada mavjud diniy konfessiya rahbarlari bilan muloqotlar uyushtirilib, barcha din vakillariga keng imkoniyatlar yaratib berilmoqda.

Har yili O'zbekiston Respublikasi Vazirlar Mahkamasining diniy ekstremizmga qarshi kurash, millatlararo va konfessiyalararo hamkorlikni yanada kuchaytirishga yo'naltirilgan kompleks tadbirlar dasturi qabul qilinadi. Ushbu dastur doirasida davlat va jamoat tashkilotlari, mahalla yig'inlarida, aholining turli qatlamlari orasida ekstremizm va terrorizm bilan bog'liq tahdidlarning oldini olishga qaratilgan seminar, uchrashuv va davra suhbatlari o'tkazish yo'lga qo'yilgan.

Aqidaparastlik g'oyalari tarqalishining oldini olish uchun OAV va boshqa axborot yetkazish vositalaridan samarali foydalanishga urg'u berilmoqda. Xususan, "Diniy ekstremizm – kelajakka tahdid", "Ekstremizm va terrorizm – taraqqiyot kushandasi", "Ogoh bo'ling "Sekta", "Din niqobi ostidagi axborot xurujlari" nomli bukletlar tayyorlanib, mahallalarga, turli vazirlik, tashkilot va idoralar orqali aholiga yetkazilmoqda.

Xorijdagi mehnat migrantlari, talabalar va vaqtincha istiqomat qilayotgan vatandoshlarimizni ekstremistik oqimlar ta'siriga tushib qolishining oldini olish yuzasidan zarur tadbirlar amalga oshirilmoqda. Respublikamizning taniqli ulamolari Rossiya Federatsiyasining Moskva, Sankt-Peterburg, Yekaterinburg,

Novosibirsk va Qozon shaharlari, Chuvash Respublikasi, Sibir o'lkasi, Sverdlovsk va Omsk viloyatlariga Ukrainaning Kiyev shahriga xizmat safariga yuborilib, mazkur tashriflar davomida o'tkazilgan diniy-ma'rifiy uchrashuvlarda ma'rifiy islom ta'limoti hamda hozirda buzg'unchi oqimlar tomonidan noto'g'ri talqin qilinayotgan "hijrat", "jihod", "shahidlik" kabi tushunchalarning asl mohiyati haqida keng tushunchalar berilmoqda.

Prezidentimizning BMT Bosh Assambleyasi 72-sessiyasidagi nutqida xalqaro terrorizm va ekstremizmning ildizini boshqa omillar bilan birga, jaholat va murosasizlik tashkil etishi, shu munosabat bilan odamlar, birinchi navbatda, yoshlarning ong-u tafakkurini ma'rifat asosida shakllantirish va tarbiyalash eng muhim vazifa ekaniga e'tibor qaratildi.

"Ekstremizm g'oyalari ta'siriga tushib qolgan, to'g'ri yo'ldan adashgan fuqarolar ijtimoiy reabilitatsiya qilinmoqda, ularni sog'lom hayotga qaytarish uchun zarur sharoitlar yaratilmoqda.

Dunyoda terrorizm tahdidlari, ayniqsa, so'nggi yillarda kuchayib borayotgani ularga qarshi, asosan, kuch ishlatish yo'li bilan kurashish usuli o'zini oqlamayotganidan dalolat beradi.

Bu borada ko'p hollarda tahdidlarni keltirib chiqarayotgan asosiy sabablar bilan emas, balki ularning oqibatlariga qarshi kurashish bilangina cheklanib qolinmoqda. Shu munosabat bilan odamlar, birinchi navbatda, yoshlarning ong-u tafakkurini ma'rifat asosida shakllantirish va tarbiyalash eng muhim vazifadir.

Shu nuqtayi nazardan, Prezidentimizning ikki global ahamiyatga ega, ya'ni yoshlarga oid siyosatni shakllantirish va amalga oshirishga qaratilgan umumlashtirilgan xalqaro huquqiy hujjat – BMT ning "Yoshlar huquqlari to'g'risidagi xalqaro konvensiya"sini ishlab chiqish hamda BMT Bosh Assambleyasining "Ma'rifat va diniy bag'rikenglik" deb nomlangan maxsus rezolyutsiyasini qabul qilish haqidagi takliflari barcha mamlakatlar tomonidan katta qiziqish bilan qabul qilindi va qo'llab-quvvatlandi.

Qolaversa, O'zbekiston Respublikasi Prezidentining 2021-yil 1-iyuldagi "2021–2026-yillarga mo'ljallangan ekstremizm va terrorizmga qarshi kurashish bo'yicha O'zbekiston Respublikasi

Milliy strategiyasini tasdiqlash to'g'risida"gi Farmoni qabul qilindi.[87] Farmon bilan "2021–2026-yillarga mo'ljallangan ekstremizm va terrorizmga qarshi kurashish bo'yicha O'zbekiston Respublikasi Milliy strategiyasi" va "Milliy strategiyani amalga oshirish yuzasidan "yo'l xaritasi"ga ko'ra, quyidagilar strategiyaning ustuvor yo'nalish va maqsadlari etib belgilandi:

– ekstremizm va terrorizm g'oyalari tarqalishining oldini olish maqsadida vatanparvarlik, an'anaviy qadriyatlar va bag'rikenglik mafkurasini targ'ib qilish;

– voyaga yetmaganlar, yoshlar orasida ekstremizm va terrorizm g'oyalari tarqalishining oldini olish;

– ayollar huquqlarini himoya qilish hamda ularning ekstremizm va terrorizmga qarshi kurashishdagi rolini kuchaytirish;

– uzoq muddat xorijda bo'lgan fuqarolarni ekstremizm va terrorizm g'oyalari ta'siridan himoya qilish;

– Internet jahon axborot tarmog'idan ekstremistik va terrorchilik maqsadlarida foydalanishga qarshi kurashish;

– fuqarolik jamiyati institutlari va ommaviy axborot vositalarini ekstremizm va terrorizmga qarshi kurashishga keng jalb qilish;

– ekstremistik va terrorchilik harakatlarini sodir etganlik hamda ularni moliyalashtirganlik uchun huquqiy ta'qib va javobgarlikka tortish choralarini takomillashtirish;

– ekstremizm va terrorizmga qarshi kurashish sohasidagi normativ-huquqiy bazani takomillashtirish;

– ushbu sohadagi xalqaro va mintaqaviy hamkorlikni rivojlantirish.

Hujjatda ma'lum qilinishicha, hukumat bundan keyin ham diniy sabablarga ko'ra buzg'unchi mafkuralar ta'siridan jabr ko'rgan shaxslarga har tomonlama yordam ko'rsatishda davom etadi. Aynan mazkur strategiyaning qabul qilinishi ham mamlakatimizda kiberxavfsizlik borasidagi jinoyatlarni kamaytirish orqali mamlakatimizda jamiyat barqarorligi va xavfsizligini ta'minlash

[87] O'zbekiston Respublikasi Prezidentining 2021-yil 1-iyuldagi "2021–2026-yillarga mo'ljallangan ekstremizm va terrorizmga qarshi kurashish bo'yicha O'zbekiston Respublikasi Milliy strategiyasini tasdiqlash to'g'risida"gi Farmoni.// https://lex.uz/pdfs/5491626

orqali xalqaro xavfsizlikni ta'minlashda O'zbekistonning ishtirokini qo'shish yo'lidagi amaliy harakat hisoblanadi.

Shuningdek, hujjatda aholining huquqiy madaniyati va ma'rifatini oshirib borish, diniy sohada diniy va dunyoviy bilimlarni egallagan, fuqarolar orasida diniy asosdagi ekstremizm mafkurasiga qarshi immunitetni shakllantira oladigan yuqori malakali kadrlarni tayyorlash va ommaviy axborot vositalarini ekstremizm va terrorizmga qarshi kurashish ishlariga faol jalb etish belgilangan.

Jumladan, 2023-yil 28-fevraldagi O'zbekiston Respublikasi Prezidentining PF-27-son Farmoni bilan tasdiqlangan "2022–2026-yillarga mo'ljallangan Yangi O'zbekistonning taraqqiyot strategiyasini "Insonga e'tibor va sifatli ta'lim yili"da amalga oshirishga oid Davlat Dasturining 82-bandi "Ekstremizm va terrorizmga qarshi kurashishning samarali mexanizmlarini shakllantirish" deb nomlandi. Mazkur yo'nalish doirasida yosh avlodda ekstremizmga qarshi kurashishda qat'iy va barqaror immunitetni shakllantirish yuzasidan tadbirlarni tashkil etish vazifasi manfaatdor idoralar zimmasiga yuklatildi.

Xulosa sifatida ta'kidlash joizki, mintaqa va umuman dunyodagi vaziyatning murakkabligiga qaramay, mamlakatimizning yangi islohotlar va rivojlanish davrida Prezident Shavkat Mirziyoyev rahnamoligida amalga oshirib kelinayotgan oqilona ichki va tashqi siyosat hamda xalqimizning kuchli irodasi, mehnatsevarligi, bag'rikengligi va ma'rifatparvarligi tufayli mamlakatimizda tinchlik va barqarorlik ta'minlab kelinmoqda.

Shunday ekan, yurtimizda hukm surayotgan tinch va osuda hayotni asrash, uning mustaqilligi va barqarorligiga munosib hissamizni qo'shish – har birimizning, shu aziz Vatanda yashayotgan turli millat va din vakillarining eng asosiy vazifalaridan bo'lmog'i lozim.

3.2. Mintaqada kiberxavfsizlikni ta'minlashning takomillashtirish mexanizmlari

Markaziy Osiyo mintaqasi kibermaydoni to'liq chegaralanmaganligini yuqoridagi paragraflardan kelib chiqqan holda aytish mumkin. Ammo so'nggi o'n yillikda u sezilarli darajada o'sdi. Qozog'iston, Qirg'iziston va Tojikistonning mobil telekommunikatsiya bozorlarida deyarli "bir odam uchun bir telefon" ko'rsatkichiga erishildi. Shuningdek, O'zbekiston va Turkmanistonda ham ushbu ko'rsatgich bo'yicha ijobiy natijalarga erishdi, deb aytish mumkin. Ammo shu bilan birga Markaziy Osiyo ikki qo'shni davlat Rossiya va Xitoyning kiberjinoyatchiligi yuqori bo'lgan kibermakonning bir qismiga aylanib borayotganligi ham tahdidlar soni reallashib borayotganligini ko'rsatmoqda. Masalan, 2011-yilda butun dunyo bo'ylab amalga oshirilgan va 12,5 milliard AQSh dollar zarar keltirgan kiberhujumlarning uchdan bir qismidan ko'prog'i rus tilida so'zashuvchi mamlakatlar vakillari tomonidan amalga oshirilgan. Rossiya kiberjinoyatchilik olamida ayniqsa onlayn firibgarlik, spam, va internet tizimlariga foydalanuvchilarning kirishlarini to'xtatib qo'yadigan hujumlar bo'yicha yetakchi davlat hisoblanadi. Ushbu faoliyatga jalb qilingan guruhlar uyushgan jinoiy elementlar tomonidan tobora ko'proq nazorat qilinmoqda. Markaziy Osiyo kibermadaniyati rus tilida shakllangan va mahalliy kiberjinoyatchilik tarmoqlari Rossiyadagi shunday tarmoqlar bilan aloqador hisoblanadi. Shuningdek, Xitoy ham iqtisodiy jinoyatlar bilan shug'ullanadiganlar kiberjinoyatchilar uchun boshpana hisoblanadi. 2011-yilda chop etilgan AQSh hisobotida ikkala davlat ham o'z rivojlanishi uchun yuqori texnologiyalar orqali josuslik qilganlikda ayblangan va Xitoy "iqtisodiy josuslikning eng faol va kuchli jinoyatchilari" yashaydigan joy deb e'tirof etilgan.[88] Qolaversa, 2011-yilda, Siandagi Yevroosiyo iqtisodiy forumi sammitida Qozog'iston rasmiylari davlat tarmoqlariga 500 000 ga yaqin hujumlarga duch kelganliklarini haqida bayonot berdi.

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

Xususan, 2011-yil yozida Qozog'iston hukumatidagi va chet eldagi diplomatik vakolatxonalardagi yuzlab kompyuterlarga xakerlarga kompyuter nazorati va maxfiy ma'lumotlarni olish imkoniyatini beradigan virus tarqatildi. Shuningdek, Rossiyadagi Tojikiston hukumati, Avstriyadagi Qirg'iziston hukumati va Qozog'istondagi Xitoy hukumatiga tegishli kompyuterlar ham hujumga uchraganligini[89] ta'kidlaydi. Aynan bu turdagi kiberjinoyatlar asosan foydali moliyaviy va sanoat ma'lumotlarini olishga intilayotgan mahalliy uyushgan jinoiy guruhlar deb aytish mumkin.

Shundan kelib chiqib aytish lozimki, kibertahdidlar soni oshib borayotgan Markaziy Osiyo mintaqasi davlatlarni ushbu muammolarni bartaraf etish uchun nima qilish lozim degan savol tug'iladi.

Avvalo, birinchidan, kiberxavfsizlik sohasida mintaqada yagona yechim bo'ladigan institutsional tuzilmalar faoliyatida yagona qarash va fikrlar uyg'unligini ta'minlash lozim ekanligi hisoblanadi. Bunda, umuman Markaziy Osiyo davlatlarining kiberxavfsizlik sohasidagi xalqaro hamkorlikka munosabatini aniqlashtirib olish lozim hisoblanadi. Mintaqa davlatlari bu boradagi milliy manfaatlarini aniqlab olishi, ularni qanday va qaysi mexanizmlar asosida ta'minlash lozimligi ustuvor vazifa sanalishi kerak, deb o'ylaymiz. Qolaversa, MDH davlatlari va SHHTga a'zo davlatlar, KXSHT va Yevroosiyo iqtisodiy ittifoqi (YeOI) bilan hamkorlik olib borilayotgan vaqtda 2001-yilda kompyuter jinoyati bo'yicha Budapesht konvensiyasi hamda 2013-yilda qabul qilingan ikkita hujjat AKT dan foydalangan holda sodir etilgan jinoyatlarga qarshi kurashish bo'yicha hamkorlik konsepsiyasi hamda Axborot xavfsizligi sohasida hamkorlik to'g'risidagi bitimni takomillashtish lozim hisoblanadi. Ushbu normativ-huquqiy hujjatlar ekspertlar fikriga ko'ra, cheklangan xarakterga ega ekanligi bilan ajralib turadi.[90] Aynan 2006-yilda Shanxay Hamkorlik Tashkilotiga a'zo

[89] "В Казахстане создана Служба реагирования на компьютерные инциденты". Nur.kz, 21 ноября 2011 г., http://news.nur.kz/200694.html; "Служба реагирования на компьютерные инциденты рассказала о своей работе". Adilsoz.kz, 25 марта 2010 г. http://www.adilsoz.kz/wpcontent/uploads/2012/02/MonitoringZakonodatelstva.pdf.

[90] Эксперты Центральной Азии: кто должен отвечать за кибербезопасность // Digital Report. 29 июля 2016 года. URL: digital. report/ekspertyitsentralnoy-azii-kto-dolzhen-otvechat-za-kiberbezopasnost/ (дата обращения : 19.01.2020).

davlatlar dunyoda birinchilardan bo'lib jahon hamjamiyatini internet makonidagi faoliyatning xalqaro miqyosda tan olingan standartlarini ishlab chiqish va axborot sohasidan kelib chiqadigan tahdidlarga qarshi kurashish borasida sa'y-harakatlarni muvofiqlashtirish masalasi kun tartibiga qo'yilgan edi. Unda "Xavfsiz raqamli muhit uchun" davlatlarning mas'uliyatini oshirish, kibermudofaa masalalari bo'yicha maxsus ekspert guruhi tashkil etish masalalari ham muhokama etilgan edi.[91] Ammo bu boradagi hamkorlik aloqalari ham ko'zlangan natijani bermadi. Natijada Shanxay Hamkorlik Tashkiloti 2011 va 2015-yillarda BMT ga Xalqaro axborot xavfsizligi bo'yicha o'zini tutish qoidalarini yaratish taklifini bergan edi. Ushbu hujjat raqamli muhitda jinoiy, terroristik va ekstremistik faoliyatga qarshi AKT tomonidan vujudga keltiriladigan tahdidlardan uchtasini ajratadi hamda "boshqa mamlakatlarning siyosiy, iqtisodiy va ijtimoiy barqarorligi, madaniyati va ma'naviy dunyosini" asosiy himoya obyektlari sifatida belgilab berishi bilan ajralib turar edi.[92] Ammo ushbu tavsiyalarni ham tahlilchilar ko'proq "yumshoq huquq" sohasiga taalluqli, deb baholadilar. Chunki u faqat tavsiyalarni o'z ichiga olishi bilan birga, internet makonida huquqbuzarliklarga qarshi kurashning texnik yoki huquqiy mexanizmlarini taklif qilmagan deb qaraldi.[93]

Natijada esa, ShHTga a'zo davlatlar tomonidan xalqaro axborot xavfsizligi sohasida hamkorlik to'g'risidagi yagona to'xtamga kelish zaruriyati anglatildi. Natijada 2019-yil noyabr oyida Bishkekda bo'lib o'tgan so'nggi sammitda kiberjinoyatchilikka qarshi birgalikda kurashish va ishtirokchi davlatlarning siyosiy manfaatlariga

[91] Кутнаева Н. Кибербезопасность в Центральной Азии // Unipath. 20 августа 2015 года. URL: unipath-magazine.com/кибербезопасность-в центральной-ази/ (дата обращения: 25.01.2020).

[92] Письмо постоянных представителей Казахстана, Китая, Кыргызстана, Российской Федерации, Таджикистана и Узбекистана при ООН от 9 января 2015 года на имя Генерального секретаря, 13 января 2015 года // ГА ООН. URL: undocs.org/pdf?symbol=ru/a/69/723 (дата обращения: 10.01. 2020).

[93] Segate R. V., Dovgalyuk O. Regional Courts in Regional Organizations: An enhanced judicial cooperation, or the failure of international law? Research Gate. September 6, 2017. 46 p.

potensial zarar yetkazishi mumkin bo'lgan ma'lumotlarni internetda tarqatish bilan bog'liq hujjatlar imzolandi.[94]

Ikkinchisi, Markaziy Osiyo mintaqasi davlatlarida kiberxavfsizlik sohasida o'zaro ichki integratsiyani amalga oshirish ustuvor vazifalar hisoblanadi. Tadqiqot doirasida to'plangan ma'lumotlar tahlili shuni ko'rsatadiki, mintaqada Qozog'iston Respublikasi boshqa mintaqa davlatlari orasida o'zining kiberhimoya siyosati bilan ancha amaliy ishlar olib borayotganini ko'rsatmoqda. Xususan, Baykonur kosmodromidagi Kazkosmos agentligi kabi davlat tashkilotlari yordamida mamlakat o'zining kosmik dasturini rivojlantirmoqda. Uning asosiy maqsadi sun'iy aloqa yo'ldoshlari uchirishni nazorat qilish hisoblanadi. 2011-yildan beri orbitada bo'lgan "KazSat 2" sun'iy yo'ldoshi Qozog'iston hududidagi raqamli ma'lumotlarni nazorat qilishga yordam berib keladi. Qolaversa, bu istiqbolda Qozog'iston harbiylarining aerokosmik sohada, shuningdek Kaspiy dengiz flotida-dengiz konlari, neft tankerlari o'tadigan yuk tashish yo'llari, ekologik xavflarni kuzatish uchun elektron yechimlarni rejalashtirayotganligini anglatadi. Bunda Markaziy Osiyoda ichki xavfsizlikni raqamlashtirish masalasi kun tartibiga chiqadi. Ya'ni Qozog'iston quyidagi yo'llar: shaxsni tasdiqlovchi hujjatlar, videokuzatuv kameralari, gumon qilinuvchilar uchun elektron ishlar, uyali aloqa xabarlarini tekshirish, monitoring va ma'lumot to'plash tizimlari bilan amalga oshirmoqda.

Uchinchidan, Markaziy Osiyoda kiberxavfsizlikni kuchaytirish ko'plab mamlakatlarda bo'lgani kabi moliyalashtirish va texnologiyalarni ekspluatatsiya qilishdagi qiyinchiliklar sabab sekin amalga oshirilmoqda. Kiberxavfsizlik bo'yicha mablag'lar yetishmasligi sababli, hatto Qozog'iston ham markaziy va mahalliy tashkilotlari uchun antivirus uskunalari, dasturiy ta'minot bilan ta'minlashda ancha orqada qolmoqda. Qolaversa, mintaqada kiberxavfsizlik bo'yicha ekspert lavozimlarida bo'sh ish o'rinlari mavjud, lekin bu talabni mavjud taklif qondira olmaydi. Bu borada

[94] Количество интернет пользователей Киргизстана ежегодно растет – Догоев // Kabar. 4 oktjabrja 2019.URL: kabar.kg/news/kolichestvo-internet-pol-zovatelei-kyrgyzstana-ezhegodno-rastet-dogoev/ (дата обращения: 21.01.2020).

davlatlar dunyoda birinchilardan bo'lib jahon hamjamiyatini internet makonidagi faoliyatning xalqaro miqyosda tan olingan standartlarini ishlab chiqish va axborot sohasidan kelib chiqadigan tahdidlarga qarshi kurashish borasida sa'y-harakatlarni muvofiqlashtirish masalasi kun tartibiga qo'yilgan edi. Unda "Xavfsiz raqamli muhit uchun" davlatlarning mas'uliyatini oshirish, kibermudofaa masalalari bo'yicha maxsus ekspert guruhi tashkil etish masalalari ham muhokama etilgan edi.[91] Ammo bu boradagi hamkorlik aloqalari ham ko'zlangan natijani bermadi. Natijada Shanxay Hamkorlik Tashkiloti 2011 va 2015-yillarda BMT ga Xalqaro axborot xavfsizligi bo'yicha o'zini tutish qoidalarini yaratish taklifini bergan edi. Ushbu hujjat raqamli muhitda jinoiy, terroristik va ekstremistik faoliyatga qarshi AKT tomonidan vujudga keltiriladigan tahdidlardan uchtasini ajratadi hamda "boshqa mamlakatlarning siyosiy, iqtisodiy va ijtimoiy barqarorligi, madaniyati va ma'naviy dunyosini" asosiy himoya obyektlari sifatida belgilab berishi bilan ajralib turar edi.[92] Ammo ushbu tavsiyalarni ham tahlilchilar ko'proq "yumshoq huquq" sohasiga taalluqli, deb baholadilar. Chunki u faqat tavsiyalarni o'z ichiga olishi bilan birga, internet makonida huquqbuzarliklarga qarshi kurashning texnik yoki huquqiy mexanizmlarini taklif qilmagan deb qaraldi.[93]

Natijada esa, ShHTga a'zo davlatlar tomonidan xalqaro axborot xavfsizligi sohasida hamkorlik to'g'risidagi yagona to'xtamga kelish zaruriyati anglatildi. Natijada 2019-yil noyabr oyida Bishkekda bo'lib o'tgan so'nggi sammitda kiberjinoyatchilikka qarshi birgalikda kurashish va ishtirokchi davlatlarning siyosiy manfaatlariga

[91] Кутнаева Н. Кибербезопасность в Центральной Азии // Unipath. 20 августа 2015 года. URL: unipath-magazine.com/кибербезопасность-в центральной-ази/ (дата обращения: 25.01.2020).

[92] Письмо постоянных представителей Казахстана, Китая, Кыргызстана, Российской Федерации, Таджикистана и Узбекистана при ООН от 9 января 2015 года на имя Генерального секретаря, 13 января 2015 года // ГА ООН. URL: undocs.org/pdf?symbol=ru/a/69/723 (дата обращения: 10.01. 2020).

[93] Segate R. V., Dovgalyuk O. Regional Courts in Regional Organizations: An enhanced judicial cooperation, or the failure of international law? Research Gate. September 6, 2017. 46 p.

potensial zarar yetkazishi mumkin bo'lgan ma'lumotlarni internetda tarqatish bilan bog'liq hujjatlar imzolandi.[94]

Ikkinchisi, Markaziy Osiyo mintaqasi davlatlarida kiberxavfsizlik sohasida o'zaro ichki integratsiyani amalga oshirish ustuvor vazifalar hisoblanadi. Tadqiqot doirasida to'plangan ma'lumotlar tahlili shuni ko'rsatadiki, mintaqada Qozog'iston Respublikasi boshqa mintaqa davlatlari orasida o'zining kiberhimoya siyosati bilan ancha amaliy ishlar olib borayotganini ko'rsatmoqda. Xususan, Baykonur kosmodromidagi Kazkosmos agentligi kabi davlat tashkilotlari yordamida mamlakat o'zining kosmik dasturini rivojlantirmoqda. Uning asosiy maqsadi sun'iy aloqa yo'ldoshlari uchirishni nazorat qilish hisoblanadi. 2011-yildan beri orbitada bo'lgan "KazSat 2" sun'iy yo'ldoshi Qozog'iston hududidagi raqamli ma'lumotlarni nazorat qilishga yordam berib keladi. Qolaversa, bu istiqbolda Qozog'iston harbiylarining aerokosmik sohada, shuningdek Kaspiy dengiz flotida-dengiz konlari, neft tankerlari o'tadigan yuk tashish yo'llari, ekologik xavflarni kuzatish uchun elektron yechimlarni rejalashtirayotganligini anglatadi. Bunda Markaziy Osiyoda ichki xavfsizlikni raqamlashtirish masalasi kun tartibiga chiqadi. Ya'ni Qozog'iston quyidagi yo'llar: shaxsni tasdiqlovchi hujjatlar, videokuzatuv kameralari, gumon qilinuvchilar uchun elektron ishlar, uyali aloqa xabarlarini tekshirish, monitoring va ma'lumot to'plash tizimlari bilan amalga oshirmoqda.

Uchinchidan, Markaziy Osiyoda kiberxavfsizlikni kuchaytirish ko'plab mamlakatlarda bo'lgani kabi moliyalashtirish va texnologiyalarni ekspluatatsiya qilishdagi qiyinchiliklar sabab sekin amalga oshirilmoqda. Kiberxavfsizlik bo'yicha mablag'lar yetishmasligi sababli, hatto Qozog'iston ham markaziy va mahalliy tashkilotlari uchun antivirus uskunalari, dasturiy ta'minot bilan ta'minlashda ancha orqada qolmoqda. Qolaversa, mintaqada kiberxavfsizlik bo'yicha ekspert lavozimlarida bo'sh ish o'rinlari mavjud, lekin bu talabni mavjud taklif qondira olmaydi. Bu borada

[94] Количество интернет пользователей Киргизстана ежегодно растет – Догоев // Kabar. 4 oktjabrja 2019.URL: kabar.kg/news/kolichestvo-internet-pol-zovatelei-kyrgyzstana-ezhegodno-rastet-dogoev/ (дата обращения: 21.01.2020).

TSARKA kompaniyasi tahlilchisi Al-Aydar Amirseitning so'zlariga ko'ra, Qozog'iston o'z kibermakonini tashqi tahdidlardan himoya qilish uchun ko'plab choralarni ko'rgan va hozirda mutaxassislarni tayyorlashga katta e'tibor qaratmoqda, deb ta'kidlashi ham bejiz emas.[95] Jumladan, "Qonunchilik darajasida biz hozirda xavfsizlikni ta'minlash uchun ko'proq amaliy yo'nalishlarni o'z ichiga olgan "Cyber Shield 2.0" Milliy konsepsiyasining ikkinchi talqinini ishlab chiqmoqdamiz, deydi. Bundan tashqari, hozirda shaxsiy ma'lumotlarni himoya qilish siyosatini Ostona xalqaro Moliya markazi va milliy audit muhiti bilan birgalikda davlat idoralari va xususiy sektorni shaxsiy ma'lumotlarni saqlash va qayta ishlash, shuningdek ulardan foydalanish uchun yanada xavfsizroq va mas'uliyatli qilish uchun hamda sun'iy intellektni o'rganish uchun ko'rib chiqmoqdamiz", dedi Qozog'iston tahlilchisi.

Shuningdek, mintaqada kiberxavfsizlik yetarli darajada rivojlanmayotganligining sabablaridan biri Markaziy Osiyo siyosiy rejimlari o'ziga xos xususiyatlaridan kelib chiqishi bilan bog'liqligidir. Ya'ni mintaqa davlatlarining axborot siyosatidagi o'ziga xos jihatlar, o'z milliy manfaatlariga asoslanishi bilan ajralib turadi. Jumladan, "Tojikiston Respublikasi axborot xavfsizligi konsepsiyasiga ko'ra, axborot xavfsizligi axborot makonida, shuningdek, internetda milliy manfaatlarni himoya qilish tushuniladi, deydi axborot texnologiyalari va kiberxavfsizlik sohasi mintaqaviy eksperti Asomiddin Atoyev.[96]

Ya'ni, mintaqada axborot tarqatish va ulardan samarali foydalanish borasida muammolar mavjud. Jumladan, axborot tarqatuvchi davlat va xususiy tashkilotlar o'rtasidagi hamkorlik tizimi kuchli emas, deb aytish mumkin. Shu sababli ushbu tizimni rivojlantirish lozim hisoblanadi. Shunda mintaqada axborot tarqatish va undan ta'sirli hamkorlik aloqalari shaffoflik muhitini yuzaga keltirishi mumkin. Xususan, Qirg'izistonning "Internet siyosati bo'yicha fuqarolik

[95]https://cabar.asia/en/expert-meeting-what-do-central-asian-countries-do-to-ensure-cybersecurity

[96]https://cabar.asia/en/expert-meeting-what-do-central-asian-countries-do-to-ensure-cybersecurity

tashabbusi" jamoat fondi axborot texnologiyalari bo'yicha direktor o'rinbosari Artem Goryainov fikricha: "Mintaqa mamlakatlarida kiberfazoni himoya qilish bo'yicha huquqiy tashabbuslar va normalar o'rtasidagi farq borligi, ularni amaliy tatbiq etishga alohida e'tibor mavjud ekanligini ta'kidlashi[97] yuqorida keltirlgan tahlillarga asos bo'ladi.

Bugun Qozog'iston Respublikasi bu borada institutsional o'zgarishlarni boshlamoqda. Xususan, Qozog'iston "Parasat" milliy ilmiy-texnologik xoldingi orqali (shu jumladan, Kazsatnet, Kazteleradio, Kazpochta va axborotlashtirish milliy markazi) hukumat (elektron hukumat yaratish) va yirik biznesni tezroq kompyuterlashtirishga harakat qilmoqda. Davlat kiberhujumlarning asosiy qurbonlari bo'lishi mumkin bo'lgan strategik aktivlarini xavf ostiga qo'ymaslik uchun kiberxavfsizlik masalalariga alohida e'tibor qaratmoqda. Bu vazifalarni yechish davlat va xususiy sektorning asosiy vazifasi ekanligi belgilab berilmoqda. Minqtaqaning boshqa davlatlari ham o'zaro ishonch va hamkorlik tamoyiliga asosan mintaqada "axborot tarqatish, undan foydalanish maydoni"ni takomillashtirishi maqsadga muvofiq.

To'rtinchidan, Markaziy Osiyo davlatlarining sa'y-harakatlariga qaramay, axborot xavfsizligiga tahdidlar kuchaymoqda, jumladan, virtual makonda ekstremistik va terroristik guruhlarning faolligi oshmoqda. Bundan tashqari, tahlillar shuni ko'rsatadiki, ekstremistlar "ijtimoiy tarmoqlardagi shubhali saytlar"dan foydalanib, o'z tarafdorlari safini kengaytirmoqda. Fikrimizcha, ushbu hodisaga qarshi kurash samaradorligini oshirish uchun umumiy harakatlarimizni birlashtirish va birgalikdagi harakatlarimizni muvofiqlashtirish zarur, deb o'ylaymiz. Masalan, KXSHT doirasida 2014-yildan buyon kompyuter insident (salbiy hodisalari)ga qarshi kurash guruhi (CERT) hududiy bo'limi faoliyat ko'rsatmoqda. Kiberhujumlardan, jumladan, boshqa davlatlar hududidan kirib keladigan kiberhujumlardan himoya qilish Qozog'istonda 2011-yildan, O'zbekistonda 2013-yildan va Qirg'izistonda

[97]https://cabar.asia/en/expert-meeting-what-do-central-asian-countries-do-to-ensure-cybersecurity

2015-yildan beri faoliyat yurita boshlagan milliy CERT lar tomonidan amalga oshirilmoqda. Biroq xalqaro amaliyotdan farqli o'laroq, Markaziy Osiyo mamlakatlaridagi CERT lar hali mustaqil tuzilmalar emas, ular davlat organlari qoshida tashkil etiladi va hukumat vakolati doirasida faoliyat yuritadi.

Shuningdek, mintaqada kiberxavfsizlikni ta'minlashning takomillashtirish mexanizmlari borasida bir qator ustuvor vazifalarga yanada e'tibor qaratishi joiz. Bularga:

– ushbu makonda xalqaro huquqning umume'tirof etilgan tamoyillariga rioya qilish;

– kompyuter xavfsizligi sohasidagi tadqiqotlar va ishlanmalarni muvofiqlashtirish va qayta yo'naltirish;

– mavjud kompyuter xavfsizligi markazlarining vaziyatli xabardorligini oshirish;

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

– kompyuter xavfsizligi bo'yicha ta'lim dasturlarini joylashtirish;

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

2019-yil 27-fevralda Toshkentda "Markaziy Osiyo davlatlarida kiberxavfsizlik va kiberterrorizm hamda ekstremizmga qarshi kurashning zamonaviy bosqichi: natijalar, muammolar va istiqbollar" mavzusida xalqaro davra suhbati tashkil qilingan edi.[98] Ushbu xalqaro davra suhbati Fridrix Ebert fondining O'zbekistondagi vakilligida tashkil etilgandi. Unda Qozog'iston, Qirg'iziston, Tojikiston, O'zbekiston va Rossiya Federatsiyasidan mutaxassis va ekspertlar: akademik va tahliliy markazlar vakillari, davlat organlari vakillari, huquqni muhofaza qilish xizmatchilari, shuningdek OAV vakillari ishtirok etishdi. Aynan ushbu davra suhbatida ham mintaqada kiberxavfsizlik va kiberterrorizm hamda ekstremizmga qarshi kurash bo'yicha quyidagi jihatlarga e'tibor qaratish va kuchaytirish masalalari tahlil etiladi. Ular:

[98]http://berlek-nkp.com/analitics/7355-kiberbezopasnost-i-protivodeystvie-kiberterrorizmu-i-ekstremizmu-v-stranah-centralnoy-azii.html

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

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

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

4. Zamonaviy kibermakonda jihodchilar sub-madaniyatining o'ziga xos jihatlarini, qanday amal qilishini tushunish va kibermakondagi jinoiy tahdidlarning aniqlanishi va ularga qarshi kurashning psixologik jihatlarini aniqlash;

5. Kibermakonda xalqaro terroristik tashkilotlar faoliyatining transformatsiyasi, bugungi kunda qisman Afg'onistonda in qurgan terroristik to'dalar tomonidan internet makonlarini o'zlarining qabih maqsadlari yo'lida foydalanish shakllari va metodlarini ko'rib chiqish, takomillashtirish. Shundan ko'rish mumkinki, kibermakonda xalqaro terroristik tashkilotlar faoliyatini kamaytirish, Markaziy Osiyo davlatlarining o'zaro ishonch, milliy manfaatlariga xizmat qiladigan prinsiplarga asoslangan kiberxavfsizlikni ta'minlovchi (axborot almashinuvi, hamkorlikda ilmiy tadqiqotlar olib borish, qo'shma tadbirlar tashkil etish va h.k.) maxsus ilmiy-amaliy hamkorlik tizimini amalda joriy qilinishi ichki va tashqi tahdidli holatlar oldini olishda (priventiv yondashuv) zarur ekanligini ko'rsatadi.

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

Markaziy Osiyodagi bugungi kun vaziyati nafaqat kompyuter texnologiyalari sohasida yuqori malakali kadrlar tayyorlashni, balki mintaqashunoslik bo'yicha chuqur bilimlarni egallagan, axborot xurujlariga qarshi tura olish malakasiga ega bo'lgan entopsixologlar, antropologlar, tarixchilar, siyosatchilar va boshqa kadrlarni yetishtirib chiqarishnbi talab qiladi, deb yozadi RTSU geosiyosiy tadqiqotlar markazi direktori, professor Maytdinova G.M. (Tojikiston).[99] Mutaxassis fikriga ko'ra, Markaziy Osiyo davlatlarida yangidan-yangi xavfsizlikka tahdidlar yuzaga kelayotgan sharoitda mintaqada kiberqurollardan foydalangan holda tinchlikka tahdid solish holatlariga yo'l qo'ymaslik uchun davlatlar o'z kuch va imkoniyatlarini birlashtirishlari talab qilinadi, deb ta'kidlaydi. Markaziy Osiyoda axborot kurashi, urushi ketmoqda. Bunday noxush vaziyatlarning oldini olish uchun moliyaviy xarajatlar talab qilinadi, Markaziy Osiyo davlatlari bu muammoni yolg'iz hal qila olmasligini e'tirof etadi. Ekspert fikricha, Markaziy Osiyoda axborot urushlarida muvaffaqiyat qozonish uchun maqsadli kadrlar tayyorlash tizimi yo'lga qo'yilishi kerak. Bunda mintaqada axborot-mafkuraviy kurash sohasida faoliyat yurutuvchi kadrlar tayyorlashga yo'naltirilgan maxsus fan tarmog'i – Markaziy Osiyo axborot xavfsizligi Akademiyasini tuzish lozim ekanligini ta'kidlaydi. Albatta, ushbu ekspertlarning fikrida ham haqiqat bor. Bugun kiberxavfsizlik borasida mintaqada xavfsizlik va barqarorlikka erishishda yangicha yondoshuvlarga ehtiyoj bor. Faqat bu yo'lda o'zaro ishonch, demokratik ochiq jamiyat asosida rivojlanayotgan Markaziy Osiyo davlatlarining milliy xavfsizligi, suvereniteti ta'minlanganlik darajasi kiberxavfsizlik (har qanday ichki va tashqi kiberhujum, kiberxurujlardan himoyalanish qobiliyati) holatlari (davr talablariga mos yoki aksincha) bilan bevosita bog'liq, to'g'ri proporsionaldir. Ularning barqaror taraqqiyotini belgilovchi asosiy muhim omillardan biri – hamkorlikning yangi formatini o'rnatish.

Xulosa qilib aytganda, ushbu yondashuvlardan kelib chiqib, mintaqada kiberxavfsizlikni ta'minlashning takomillashtirish

[99]http://berlek-nkp.com/analitics/7355-kiberbezopasnost-i-protivodeystvie-kiberterrorizmu-i-ekstremizmu-v-stranah-centralnoy-azii.html

mexanizmlari mintaqadagi har bir davlatning milliy manfaatlarga erishish vositasi sifatida qaralishidan kelib chiqadi. Bunda barcha mamlakatlar kiberxavfsizlik davlatning milliy manfaatlariga erishish vositasi ekanligiga ishonadi, chunki ikkala nazariya ham moddiy manfaatga qaratilganligi bilan ajralib turadi. Ayni paytda, ba'zi mamlakatlar kiberxavfsizlikni dushmanlarning idrokiga ta'sir qilish vositasi sifatida ko'radi. Bu holat kiberhujumlarning ulkan halokat kuchiga asoslanishiga olib keladi. Oldingi ikki yondashuvdan farqli o'laroq, milliy xavfsizlik institutlari moddiy manfaatni emas, shaxs, jamiyat, davlatning tinchligi va xavfsizligiga urg'u beradi. Faqatgina ushbu milliy xavfsizlik yondashuvlari o'rtasidagi farq shundaki, ushbu vositadan maqsadlarga erishish uchun foydalaniladi.

Uchinchi bob bo'yicha xulosalar

So'nggi yillarda kibermakon o'zgarishlarga uchrab, takomillashib, harbiy harakatlar olib boriluvchi hududlar uchun yollanma askarlar jalb qilish, terroristik hujumlarni yaratish, jinoiy faoliyatni moliyalashtirish vositasiga aylandi. Bunday sharoit mintaqa davlatlari oldida dolzarb muammolar mavjud ekanligini ko'rsatadi. Xususan, O'zbekistonning kiberxavfsizlikni ta'minlashda nimalarga e'tibor qaratishi, kuchli tahliliy tadqiqotlar o'tkazishi maqsadga muvofiq. Qolaversa, mustaqillik yillarida qo'lga kiritgan imkoniyatlar va tajribalardan tashqari qo'shni davlatlarning bu boradagi tajribalarini o'rganishi kerak. Kiberxavfsizlik sohasida kadrlar tayyorlash tizimini takomillashtirish, qonunchilikka kiberxavfsizlik tushunchasiga oid bo'lgan ijtimoiy tushunchalarning tahlilini kiritishi maqsadga muvofiq. Bu tushunchalar haqida birinchi bobda to'xtalingan.

O'zbekiston yangi taraqqiyot bosqichida kiberxavfsizlik sohasidagi mintaqaviy hamkorlik aloqalarini mustahkamlashda Markaziy Osiyo davlatlarining o'zaro ishonch, milliy manfaatlariga xizmat qiladigan prinsiplarga asoslangan kiberxavfsizlikni ta'minlovchi (axborot almashinuvi, hamkorlikda ilmiy tadqiqotlar olib borish, qo'shma tadbirlar tashkil etish va h.k.) maxsus ilmiy-amaliy hamkorlik tizimining amalda joriy qilinishi ichki va tashqi tahdidli holatlar oldini olishda (priventiv yondashuv), Markaziy Osiyo mintaqasini barqaror, xavfsiz taraqqiy etishining asosiy shartlaridan biri sifatida ko'rishi maqsadga muvofiq.

XULOSA

Mazkur tadqiqot ishi nazariy va amaliy manbalarni o'rganish asosida quyidagi xulosa va takliflarni ilgari suradi:

1. "Kiberxavfsizlik" tushunchasi murakkab kategoriya sifatida e'tirof etiladigan jarayon hisoblanadi. Uning tarkibidagi yondosh atamalar kiberxavfsizlik tushunchasini yaxlit holda ifodalashga imkon beradi. Shu sababli ushbu tushunchalarga oid bo'lgan tushunchalar turkumini o'zbek tiliga oid bo'lgan lug'atlarga kiritishga zaruriyat sezilmoqda.

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

2. Markaziy Osiyo kiberxavfsizligi tizimi va uning o'ziga xos xususiyatlari to'liq ravishda institutsionallashmagan. Natijada kiberxavfsizlikni ta'minlash borasida yondoshuv va amaliy harakatlar tizimlashtirilmagan ekanligini ko'rsatmoqda. Bu o'z navbatida kiberxavfsizlikni ta'minlashda mintaqada o'zaro siyosiy islohotlarni yangi bosqichga chiqarish asosida tuzilmaviy-funksional institutlarni yaratishga zaruriyat bor ekanligini ko'rsatadi. Qolaversa, tuzilmaviy-funksional institutlar faoliyatini yo'lga qo'yish orqali mintaqada siyosiy muloqotni rivojlantirish asosida mintaqa davlatlarining savdo, investitsiyalar, transport, energetika, qishloq xo'jaligi va ekologiya sohalarida qo'shma dastur va loyihalarni ilgari surish, madaniy-gumanitar hamda xavfsizlik sohasidagi zamonaviy tahdid va xatarlarga qarshi chora ko'rish mexanizmlari yaratilishiga erishiladi.

3. Markaziy Osiyo mintaqasida kiberxavfsizlikning turli ko'rinishlari yoshlar qatlamiga jiddiy ta'sir o'tkazmoqda. Bu esa davlatlarning milliy xavfsiziligiga zarar ko'rsatish darajasini oshirishi mumkin.

Buning uchun rivojlangan xorijiy davlatlarning bu boradagi tajribalarini chuqur tahlil etish talab etiladi. Mintaqa yoshlari, ularning yosh xususiyatlari, urf-odatlaridan kelib chiqib, axborotdan

foydalanish bo'yicha maxsus strategik dastur ishlab chiqish maqsadga muvofiq. Aynan bu ta'lim muassasalari hamda jamoat joylaridagi faoliyatlarini huquqiy tartibga solishga olib keladi.

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

5. O'zbekiston taraqqiyotining yangi bosqichida mintaqa davlatlarining rivojlanish jarayonlarini tizimli tahlil qiladigan "aqliy markaz"lar faoliyatini takomillashtirish lozim. Aynan mintaqada kiberxavfsizlik masalalarini fundamental jihatdan o'rganish uchun Markaziy Osiyo xalqaro instituti faoliyatini tubdan takomillashtirib, uning qoshida maxsus kiberxavfsizlik masalasini tadqiq etib boruvchi bo'lim faoliyatini yo'lga qo'yish kerak. Ushbu bo'lim mintaqa davlatlarini kiberxavfsizlikni ta'minlash siyosati borasida olib borayotgan islohotlarini tizimli o'rganish asosida tegishli takliflarni tayyorlash bilan shug'illanishi maqsadga muvofiq bo'lar edi.

6. Markaziy Osiyo mintaqasida to'planib qolgan muammolar, manfaatlarni hisobga olgan holda, izchil muloqot va kelishuvlar asosida tartibga solishga intilishi mintaqada do'stlik, ishonch va o'zaro manfaatli hamkorlikning yangicha muhitini yanada takomillashtirib borish global muammolarga global javoblar berishni taqozo etmoqda. Bunda mintaqa davlatlari ekspertlari tomonidan "Markaziy Osiyo

davlatlarida kiberxavfsizlik va kiberterrorizm hamda ekstremizmga qarshi kurashning zamonaviy bosqichi: natijalar, muammolar va istiqbollar" mavzusida mintaqaviy uchrashuvlarni o'tkazishi kerak. Bu o'z navbatida O'zbekiston taraqqiyotining yangi bosqichida davlatimizni pragmatizm, mintaqaviy yakdillikni qo'llab-quvvatlash va keskin masalalarni tezkor hal etishga yo'naltirilgan faol tashqi siyosatni amalga oshirishda xizmat qiladi.

FOYDALANILGAN ADABIYOTLAR

Normativ-huquqiy hujjatlar va metodologik ahamiyatga molik nashrlar

1. O'zbekiston Respublikasining ekstremizm va terrorizmga qarshi kurashish bo'yicha 2021–2026-yillarga mo'ljallangan strategiyasi.// https://lex.uz/docs/5491626
2. O'zbekiston Respublikasining 2022-yil 15-apreldagi Kiberxavfsizlik to'g'rsidagi Qonuni.// https://lex.uz/uz/docs/5960604
3. O'zbekiston Respublikasining 2015-yil 9-dekabrda e'lon qilingan "Elektron hukumat to'g'risida"gi Qonuni.// https://lex.uz/mobileact/2833860
4. O'zbekiston Respublikasining Telekommunikatsiyalar to'g'risida// O'zbekiston Respublikasi Oliy Majlisining Axborotnomasi, 1999-yil, 9-son, 219-modda.
5. O'zbekiston Respublikasi Prezidentining 2019-yil 14-sentyabrdagi "Axborot texnologiyalari va kommunikatsiyalarining joriy etilishini nazorat qilish, ularni himoya qilish tizimini takomillashtirishga oid qo'shimcha chora-tadbirlar to'g'risida"gi PQ-4452-sonli qarori. https://lex.uz/docs/4665548
6. O'zbekiston Respublikasi Prezidentining 2019-yil 2-fevraldagi "Axborot sohasi va ommaviy kommunikatsiyalarni yanada rivojlantirishga oid qo'shimcha chora-tadbirlar to'g'risida"gi PF-5653-son Farmoni.//Qonun hujjatlari ma'lumotlari milliy bazasi, 04.02.2019-y., 06/19/5653/2568-son.
7. O'zbekiston Respublikasi Prezidentining 2020-yil 5-oktyabrdagi "Raqamli O'zbekiston–2030" strategiyasi" va uni samarali amalga oshirish chora-tadbirlari to'g'risida"gi Farmoni/ https://lex.uz/docs/5030957
8. O'zbekiston Respublikasi Prezidentining 2019-yil 7-martdagi "Xalqaro reyting va indekslarda O'zbekiston Respublikasining o'rnini yaxshilashga oid chora-tadbirlarni tizimlashtirish to'g'risida"gi PF-5687-sonli Farmoni/ https://lex.uz/docs/4230916
9. O'zbekiston Respublikasi Prezidentining 2020-yil 2-iyundagi "O'zbekiston Respublikasining xalqaro reyting va indekslardagi o'rnini yaxshilash hamda davlat organlari va tashkilotlarida ular bilan tizimli ishlashning yangi mexanizmini joriy qilish to'g'risida"gi PF-6003-son Farmoni/ https://lex.uz/docs/4838762
10. O'zbekiston Respublikasi Prezidentining 2021-yil 1-iyuldagi "2021–2026-yillarga mo'ljallangan ekstremizm va terrorizmga qarshi

kurashish bo'yicha O'zbekiston Respublikasi Milliy strategiyasini tasdiqlash to'g'risida"gi Farmoni.// https://lex.uz/pdfs/5491626
11. O'zbekiston Respublikasi Prezidentining 2020-yil 5-oktyabrdagi "Raqamli O'zbekiston–2030" strategiyasi" va uni samarali amalga oshirish chora-tadbirlari to'g'risida"gi Farmoni/ https://lex.uz/docs/5030957
12. Mirziyoyev Sh.M. O'zbekiston Respublikasi Prezidenti lavozimiga kirishish tantanali marosimiga bag'ishlangan Oliy Majlis palatalarining qo'shma majlisidagi nutqidan, Toshkent shahri, 14.12.2016.
13. O'zbekiston Respublikasi Prezidenti Shavkat Mirziyoyevning "Hindiston – Markaziy Osiyo" birinchi sammitidagi nutqi.// https://president.uz/uz/lists/view/4944
14. Karimov I.A. Xavfsizlik va barqaror taraqqiyot yo'lida. 6-jild. – Toshkent: "O'zbekiston", 1998. – B.429.
15. Karimov I.A O'zbek xalqi hech qachon hech kimga qaram bo'lmaydi. 13-jild. – Toshkent: "O'zbekiston", 2005. – B.448.

Kitob, monografiya, darsliklar, disssertatsiya, avtoreferat, davriy nashrlar, statistik to'plamlar

16. Anorboyev A.U. Kiberjinoyatchilik, unga qarshi kurashish muammolari va kiberxavfsizlikni ta'minlash istiqbollari. –T: 2020.
17. Axborot kommunikatsiya texnologiyalari izohli lug'ati. BMTTD ning O'zbekistondagi vakolatxonasi. – 2010. – B.573.
18. Andrew Mumford. Proxy Warfare War and Conflict in the Modern World. Wiley, 2013. – P.13.
19. Расулев А.К. Некоторые вопросы совершенствования уголовно правовых и криминологических мер борбы с преступлениями в сфере информационных технологий и безопасности. – Т. 2017.С.36-37.
20. AQSh va Xitoyning kiberxavfsizlik strategiyasi: kim nimani ko'zlamoqda? https://kun.uz/28352354?q=%2F28352354#
21. Августин А. О свободе воли. Книга 2.// Антология средневековой мысли. В двух томах. Том 1.- SPb.: RXGI, 2001. – С.19–112.
22. Boboqulov I.I., Umarov X.P. Xavfsizlik asoslari. – Toshkent, 2011. – B. 83.
23. Блеквилл Р., Харрис Дж. «Война иными средствами» Геоэкономика и искусство управления государством. Издание на русском языке AST Publishers, 2017. – С.105.

24. Бердибаева А. Как Кыргызстан планирует боротся с киберугрозами? // Digital Report. 4-aprelya 2017. URL: digital.report/kak-kyirgyizstan-planiruetborotsya-s-kiberugrozami/ (дата обращения: 27.01.2020).

25. Бердибаева А. Как Кыргызстан планирует боротся с киберугрозами? // Digital Report. 4-aprelya 2017. URL: digital.report/kak-kyirgyizstan-planiruetborotsya-s-kiberugrozami/ (дата обращения: 27.01.2020).

26. Вылков Р.И. Некоторые вопросы совершенствования уголовно правовых и киберпространство как сотсиокултурный феномен, продукт технологического творчества и проективная идея: дис. канд. фил. наук. – Екатеринбург, 2009. – С.128, 129.

27. Вопросы безопасности обеспечения кибербезопасности рекомендации.// https://www.gov.kz/memleket/entities/infsecurity? lang=ru

28. Dunyo davlatlarining kiberxavfsizlik reytingi.// https://www.xabar.uz/ Кибербезопасност, 2020–2021. https://www.ptsecurity.com/

29. Демидов О. Вызовы кибербезопасности в Сентральной Азии // Digital Report. 11 августа 2016 года. URL: digital.report/oleg-demidov-pir-tsentr-moskva-vyizovyi-kiberbezopasnosti-v-tsentralnoy-azii-2/ (дата обращения: 19.01.2020).

30. Демидов О. Вызовы кибербезопасности в Централной Азии // Digital Report. 11 avgusta 2016 года. URL: digital.report/oleg-demidov-pir-tsentrmoskva-vyizovyi-kiberbezopasnosti-v-tsentralnoy-azii-2/ (дата обращения: 19.01.2020).

31. Закон Туркменистана "О правовом регулировании развития сети Интернет и оказания интернет-услуг в Туркменистане" от 20 декабря 2014 г., № 159-V// http://www.wipo.int/wipolex/ru/text.jsp?file_id=398876

32. Закон Туркменистана "О националной безопасности Туркменистана" от 4 мая 2013 г. №388-IV (в редакции от 18 июня 2016 г. №414-V) // http://base.spinform.ru/ show_doc.fwx?rgn=65978

33. Ибодов А.Х. Информационная безопасност: новые вызовы и угрозы в процессе перехода к информационному обществу (на материалах Республики Таджикистан): Дис. канд. полит. наук. – Душанбе, 2015. –С.32.

34. Ибрагимова Г. Подходы государств Центральной Азии к вопросам управления интернетом и обеспечения информационной безопасности // Индекс безопасности. 2013. № 1. – С.103–128.

35. Конституция Туркменистана (новая редакция). Утверждена Конституционным Законом Туркменистана от 14 центября 2016 г. №448-V // http://www.base.spinform.ru/ show_doc.fwx?rgn=89543

36. Киберпреступность в мире. 2020 г., http://www.tadviser.ru/index.php

37. Карасев П.А. Новые стратегии США в области кибербезопасности [Электронный ресурс]: URL: http://russiancouncil.ru/analytics-and-comments/analytics/novyestrategii-ssha-v-oblasti-kiberbezopasnosti/ (дата обращения: 02.10.2019).

38. Кулжанова Г. Некоторые аспекты проблемы политической модернизации местного государственного управления.// Kazaxstan – Spektr, 20005 № 2. – С.22.

39. Кутнаева Н. Кибербезопасность в Центральной Азии //Unipath. 20 августа 2015 года. URL: unipath-magazine.com/ кибербезопасность в Центральной Азии / (дата обращения: 25.01.2020).

40. Концепция информационной безопасности Кыргызской Республики на 2019–2023 годы (к Постановлению Правительства КР № 209 от 3 мая 2019 года). URL: cbd.minjust.gov.kg/act/view/ru-ru/13652 (дата обращения: 19.02.2020).

41. Количество интернет пользователей Кыргызстана ежегодно растет – Догоев // Кабар. 4 октября 2019. URL: kabar.kg/news/kolichestvo-internet-pol-zovatelei-kyrgyzstana-ezhegodno-rastet-dogoev/ (дата обращения: 21.01.2020).

42. Марлен Ларюел Кибербезопасность в Централной Азии: реалный угрозы, ложные предлоги? Аналитических обзор.//2012 г. №2. Екатерина Исакова "Хакеры выбирают Казахстан," Kursiv.kz, 21 октября 2010 года, http://www.kursiv.kz/hi-tech/hitechweekly/1195205432-xakery-vybirayutkazaxstan.html

43. Markaziy Osiyoda mushtarak jihatlar, tahdidlar va yangi imkoniyatlar. O'zbekiston Respublikasi Prezidenti huzuridagi Strategik va mintaqalararo tadqiqotlar instituti. 16.02.2019. http://uza.uz/oz/society/markaziy-osiyeda-mushtarak-zhi-atlar-ta-didlar-va-yangi-imko-15-02- 2019

44. Mahmudov T. "Avesto" haqida. – T.: "Sharq", 2000.

45. Marc D. Why the people don't care about computer crime?// Harvard Journal of Law and Technology № 10-3.1997. –P. 465–494.

46. National Security Strategy 2002 [Электронный ресурс]: The White House. URL:http://georgewbush-whitehouse.archives.gov/nsc/nss/2002/ (дата обращения: 29.03.2023).

47. Национальная стратегия развития Республики Таджикистан на период до 2030 года. Утв. Постановлением националная-стратегия-развития-республики-таджикистан-на-период-до-2030-года.html

48. Nazarov Q. G'oyalar falsafasi. –Toshkent: "Akademiya", 2011. – B.296–301.

49. Об этом сообщает госинформагентство. "Туркменистан сегодня", 2023.

50. Об утверждении Концепции кибербезопасности ("Киберщит Казахстана") Постановление Правительства Республики Казахстан от 30 июня 2017 года, № 407. https://adilet.zan.kz/rus/docs/P1700000407

51. От цифровизации до волонтерства: каким будет 2020 год в странах Централной Азии // News-Asia, 3 января 2020. URL: news-asia.ru/view/kz/ politics/13202 (дата обращения: 10.01. 2020).

52. Постановление Правительства Республики Казахстан от 30 июня 2017 года № 407 "Об утверждении Концепции кибербезопасности (Киберщит Казахстана)" // adilet.zan.kz/rus/docs/P1700000407.

53. Правительства РТ от 1 октября 2016 г., № 392 // URL: http:// www.tajikngo.tj/en/-mainmenu-51/item/3105-

54. Firdavsiy A. Shohnoma. – T.: A.Navoiy nomli O'zbekiston Milliy kutubxonasi nashriyoti, 2012.

55. Эксперты Централной Азии: кто должен отвечат за кибербезопасность // Digital Report. 29 июля 2016 года. URL: digital. report/ эксперты Централной Азии: кто должен отвечат за кибербезопасность / (дата обращения: 19.01.2020).

56. Указ Президента Республики Таджикистан от 5 ноября 2003 г. № 1174 "О Государственной стратегии "Информационно-коммуникационные технологии для развития Республики Таджикистан"// http://cis.rudn.ru/doc/255

57. Qur'oni Karim. Baqara surasi. 216-oyat.// Qur'oni Karimning mashhur suralari fazilati./ Nashrga tayyorlovchilar A.Ahmad, I.Nurulloh. – T.: G'.G'ulom nomidagi nashr., 2021. – B.119.

58. Rogovsky E. Cyber-Washington: Global Ambitions. International Relations, Moscow, 2014. – P.848.

59. Richard C. Crime by Computer: correlations of software piracy and unauthorised account access // Security Journal. №4-1.1993. – P.2–12.

60. Computer Crime and Intellectual Property Section, US Department of Justice, The National Information Infrastructure Protection Act of 1996, Legislative Analysis, 1996.

61. Global Cybersecurity Index 2017. Geneva: International Telecommunication Union (ITU), 2018. – P.66.

Internet manbalari

62. https://turkmenistan.gov.tm/ru/post/68980/informacionnaya-bezopasnost-prioritetnaya-zadacha-centralnoaziatskogo-regiona

63. https://turkmenistan.gov.tm/ru/post/68980/informacionnaya-bezopasnost-prioritetnaya-zadacha-centralnoaziatskogo-regiona

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

65. https://elibrary.ru/item.asp?id=44191317

66. https://regnum.ru/news/polit/2421809.html

67. https://www.kaspersky.ru/resource-center/threats/what-is-cybercrime.

68. Благие дела: добро и зло в исламе.// https://www.islam-love.ru.

69. Концепция Стратегии кибербезопасности Российской Федерации. //

70. http://www.council.gov.ru/media/files/41d4b3dfbdb25cea8a73.pdf

71. https://www.congress.gov/bill/98th-congress/senate-bill/2864

72. В развитие сетей связи вложат $883,7 млн (К 2020 году скорост передачи данных планируется увеличит в 20 раз) // http:// www.gazeta.uz/2015/12/01/comm/

73. Указ Президента РТ "Об утверждении Концепции Государственной информационной политики" от 30 апреля 2008 г. №451//https://www.google.ru/url?sa=t&rct= j&q=&esrc=s&source=web&cd=3&ved=0ahUKEwiv1a St8_3AhVoIJoKHZo 8CvgQFgglMAI&url=http%3A%2F%2Ffilial-nic-mkur.tj

74. Указ Президента Республики Таджикистан от 7 ноября 2003 года №1175 "О Концепции информационной безопасности Республики Таджикистан//https://www.google.ru/l?sa=t&rct=j&q=&esrc=s&source=web&cd=1&ved=0ahUKEwjPt7SS7rrVAhUIfhoKHfE8AYwQFggmMAA&url=http%3A%2F%2Fnansmit.tj%2F20968-2%2F%3Fid%3D15325&usg=AFQjCNFVPJAoTk-iQylc9C5P0-jDJPmy6Q

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

76. https://csec.uz/uz/company/
77. https://gov.uz/uz/news/view/31375
78. Ekstremizm va terrorizmga qarshi kurashda O'zbekiston tajribasi.// https://iiv.uz/oz/news/ekstremizm-va-terrorizmga-qarshi-kurashda-ozbekiston-tajribasi
79. Аналитический обзор по Централной Азии. №2, июнь, 2012; Автор благодарит сотрудников компании AECMA за помощ в написании данного обзора, sm. www.aesma-group.com.
80. "В Казахстане создана Служба реагирования на компютерные инциденты". Нур.кз, 21 ноября 2011 г., http://news.nur.kz/200694.html; "Служба реагирования на компютерные инциденты рассказала о своей работе", Адилсоз.кз, 25 марта 2010 г., http://www.adilsoz.kz/wpcontent/uploads/2012/02/MonitoringZakonodatelstva.pdf.
81. Кутнаева Н. Кибербезопасность в Централной Азии // Unipath. 20 августа 2015 года. URL: unipath-magazine.com/ кибербезопасност-в централной-азии/ (дата обращения: 25.01.2020).
82. Письмо постоянных представителей Казахстана, Китая, Кыргызстана, Российской Федерации, Таджикистана и Узбекистана при ООН от 9 января 2015 года на имя Генерального секретаря, 13 января 2015 года // ГА ООН. URL: undocs.org/pdf?symbol=ru/a/69/723 (дата обращения: 10.01. 2020).
83. Segate R. V., Dovgalyuk O. Regional Courts in Regional Organizations: An enhanced judicial cooperation, or the failure of international law? Research Gate. September 6, 2017. – P.46.
84. https://cabar.asia/en/expert-meeting-what-do-central-asian-countries-do-to-ensure-cybersecurity
85. https://cabar.asia/en/expert-meeting-what-do-central-asian-countries-do-to-ensure-cybersecurity
86. https://cabar.asia/en/expert-meeting-what-do-central-asian-countries-do-to-ensure-cybersecurity
87. http://berlek-nkp.com/analitics/7355-kiberbezopasnost-i-protivodeystvie-kiberterrorizmu-i-ekstremizmu-v-stranah-centralnoy-azii.html

MUNDARIJA

BO‘TAYEV USMONJON XAYRULLAYEVICH
TURDIYEV UYG‘UN RAHMATULLAYEVICH

MARKAZIY OSIYO MINTAQASIDA
KIBERXAVFSIZLIK

qoidalar, bosqichlar va mexanizmlar

MONOGRAFIYA

Muharrir: U.Radjabova
Dizayner-sahifalovchi: F.Bahodirov

Nashriyot tasdiqnomasi №6260.
Bosishga ruxsat etilgan sana 29.02.2024-y.
Bichimi 60x84/16. Nashr b.t. 7,5. Shartli b.t. 6,98.
«Times New Roman» garniturasi. Adadi 100.
Shartnoma №13, 09.02.2024.

“INVEST BOOK” MCHJ tomonidan tayyorlanib, chop etilgan.
Toshkent sh. Foziltepa ko‘ch., 12-B uy

Ushbu monografiyada kiberxavfsizlik tushunchasi mazmuni, uning ijtimoiy-siyosiy jihatlarining nazariy-konseptual asoslari tahlil etilgan. Shuningdek, monografiyada Markaziy Osiyo mintaqasida kiberxavfsizlikni ta'minlashning ijtimoiy-siyosiy asoslari o'rganilgan. Tadqiqotda kibermakonda shaxs, jamiyat va davlat manfaatlarini tashqi va ichki tahdidlardan himoya qilishdagi ustuvor vazifalar yoritib berilgan. Monografiyada keltirilgan xulosa va tavsiyalardan siyosatshunoslik, xalqaro munosabatlar va tizimli tahlil, huquqshunoslik, milliy g'oya va ma'naviyat asoslari va huquq ta'limi yo'nalishi talabalari, magistrlar hamda tadqiqotchilar foydalanishi uchun mo'ljallangan.

INVEST BOOK

ISBN 978-9910-8276-6-9

9 789910 927669