

O‘ZBEKISTON RESPUBLIKASI ICHKI ISHLAR VAZIRLIGI
MALAKA OSHIRISH INSTITUTI



AXBOROT TEXNOLOGIYALARIDAN FOYDALANGAN
HOLDA SODIR ETILADIGAN HUQUQBUZARLIKLARGA
QARSHI KURASHISHNING DOLZARB MUAMMOLARI VA
YECHIMLARI

Respublika ilmiy-amaliy konferensiya materiallari to‘plami
2025-yil, 26-iyun

Toshkent-2025

UO‘K: 343.97 (575.1)

Axborot texnologiyalaridan foydalangan holda sodir etiladigan huquqbuzarliklarga qarshi kurashishning dolzarb muammolari va yechimlari. Respublika ilmiy-amaliy konferensiya materiallari to‘plami. 2025-yil 26-iyun. – Toshkent: O‘zbekiston Respublikasi Ichki ishlar vazirligi Malaka oshirish instituti. 2025. - 196-bet.

To‘plam “*Axborot texnologiyalaridan foydalangan holda sodir etiladigan huquqbuzarliklarga qarshi kurashishning dolzarb muammolari va yechimlari*” mavzusidagi respublika ilmiy-amaliy konferensiyaning materiallari, olimlarning ilmiy maqolalari asosida tuzildi.

To‘plam professor-o‘qituvchilar, ilmiy izlanishlar olib borayotgan soha mutaxassislari, ilmiy-tadqiqotchilar, doktorantlar, magistrlar, talabalar va tinglovchilar uchun mo‘ljallangan.

Maqolalarda keltirilgan ma’lumotlarning haqqoniyligi uchun mualliflar javobgardir.

Tashkiliy qo‘mita:

U.E. Rasulev O‘zbekiston Respublikasi Ichki ishlar vazirligi
Malaka oshirish instituti boshlig‘ining birinchi
o‘rinbosari, dotsent.

Tashkiliy qo‘mita a‘zolari:

E.E. Marupov - IIV Malaka oshirish instituti Axborot
texnologiyalari sikli boshlig‘i.

Y.B. Tashmanov - IIV Malaka oshirish instituti Axborot
texnologiyalari sikli katta o‘qituvchisi, t.f.f.d.
(PhD) dotsent.

J.D. Risqaliyev - IIV Malaka oshirish instituti Axborot
texnologiyalari sikli katta o‘qituvchisi.

O.M. Boynazarov - IIV Malaka oshirish instituti Axborot
texnologiyalari sikli o‘qituvchisi.

A.A. Abdiraximov - IIV Malaka oshirish instituti Axborot
texnologiyalari sikli o‘qituvchisi.

KIRISH SO‘ZI

Assalomu alaykum, Hurmatli konferensiya qatnashchilari!

XXI asr - axborot texnologiyalari asridir. Chorak asr bo‘lganiga qaramasdan, dasturlash, axborotni uzatish va qabul qilish, katta ma’lumotlar tahlili, axborot xavfsizligi, kiberxavfsizlik hamda sun’iy intellekt texnologiyalari sohasida o‘zgarishlar yaqqol sezilmoqda.

O‘zbekiston Respublikasi Prezidenti Shavkat Miromonovich Mirziyoyev aholiga ko‘rsatilayotgan xizmatlarni raqamlashtirishga alohida e’tibor qaratdilar. Buning natijasida 2025-yilda <https://my.gov.uz> yagona interaktiv davlat xizmatlari portali orqali **766** ta onlayn xizmat joriy qilindi.

Axborot texnologiyalari rivojlanib borgani sari kiberjinoyatlar salmog‘i ham o‘shib bormoqda. O‘zbekiston Respublikasi Ichki ishlar vazirligi Tezkor qidiruv departamenti Kiberxavfsizlik markazi ma’lumotlariga ko‘ra yurtimizda so‘nggi 5 yillikda kiberjinoyatlar **68** baravar, 2024-yilda esa 2023-yildagiga nisbatan **9,1** baravar oshgan. Ushbu davrda kibermakondagi huquqbuzarliklar yuzasidan yuridik va jismoniy shaxslardan kelib tushayotgan murojaatlar soni **34** baravar ko‘paygan. Mazkur sodir etilgan jinoyatlar natijasida fuqarolarning **1 trillion 909 milliard** so‘mdan ortiq mablag‘i talon-taroj qilingan. Bu esa internet yoki ijtimoiy tarmoqlar orqali sodir etilayotgan turli huquqbuzarlik va jinoyatlarga qarshi kurashishning samarali mexanizmlarini taqozo etadi.

Kiberjinoyatlarning umumiy jinoyatchilikdagi ulushi 2023-yilda **6,2** foizni tashkil etgan bo‘lsa, 2024-yilda **44,4** foizga yetib, deyarli har 2 ta jinoyatning biri axborot texnologiyalari orqali sodir etildi. Bu esa muntazam ravishda ularning oldini olish tizimini takomillashtirib borishni taqozo etmoqda.

O‘zbekiston Respublikasining 2022-yil 15-apreldagi “Kiberxavfsizlik to‘g‘risida” O‘RQ-764-son Qonunida “**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” deb ta‘rif berilgan.

Axborot texnologiyalari asrida jinoyatchilar bank plastik kartalaridagi pul mablag‘lari hamda fuqarolarning shaxsiy ma’lumotlarini o‘z shaxsini oshkor qilmasdan olish imkoniyatiga ega. O‘shib borayotgan kiberjinoyatlarni oldini olish, aniqlash va fosh etish uchun huquqni muhofaza qilish organlari jadal kurash olib bormoqda. Bu esa soha mutaxassislaridan yuqori malakani talab qiladi.

O‘zbekiston Respublikasi Ichki ishlar vazirligida kiberxavfsizlikni ta‘minlash, kiberjinoyatlarni oldini olish, aniqlash va fosh etish Axborot texnologiyalari aloqa va axborotni himoyalash boshqarmasi, Tezkor qidiruv departamenti Kiberxavfsizlik markazi hamda uning hududiy bo‘limlari va Ekspert kriminalistika bosh markazining Raqamli axborot-qidiruv tizimlari markazi mutaxassislari tomonidan amalga oshirib kelinmoqda.

O‘zbekiston Respublikasi Prezidentining 2023-yil 30-noyabrdagi “Raqamli mahsulotlar (xizmatlar) iste‘molchilari huquqlarini himoya qilish va raqamli texnologiyalar vositasida sodir etiladigan huquqbuzarliklarga qarshi kurashishni

kuchaytirish choralari to'g'risida" PQ-381-son qaroriga asosan, soha mutaxassislari kiberjinoyatchilikka qarshi kurashishda o'z malakalarini oshirib borishi yo'lga qo'yildi.

O'zbekiston Respublikasi Ichki ishlar vaziri o'rinbosari, general-mayor D.Nazarmuxamedovning 2025-yil 15-yanvar kunidagi 20-son farmoyishiga asosan Ichki ishlar vazirligi Malaka oshirish institutida Toshkent shahar IIBB Tezkor-qidiruv xizmatlari tuzilmasidagi Kiberjinoyatchilikka qarshi kurashish bo'linmalari, Axborot texnologiyalari sohasidagi jinoyatlarni tergov qilish bo'linmalari hamda Huquqbuzarliklar profilaktikasi bo'linmalari tuzilmasidagi Axborot texnologiyalari sohasida jinoyatlarni oldini olish bo'linmalari xodimlari uchun kasbiy qayta tayyorlash va malaka oshirish o'quv kurslari tashkil etib kelinmoqda.

Shuningdek, O'zbekiston Respublikasi Prezidentining 2025-yil 30-apreldagi "Axborot texnologiyalari yordamida sodir etiladigan jinoyatlarga qarshi kurashish faoliyatini yanada kuchaytirishga qaratilgan chora-tadbirlar to'g'risida" PQ-153-son qaroriga asosan, Ichki ishlar vazirligi O'zbekiston Respublikasida kiberjinoyatlarga qarshi kurashish yo'nalishida yagona ishlash amaliyotini yo'lga qo'yish, bu borada barcha mas'ul davlat organlari va muassasalari faoliyatini muvofiqlashtirish hamda manzilli hamkorligini tashkil etish bo'yicha vakolatli organ etib belgilandi.

Mazkur maqsad va vazifalardan kelib chiqqan holda aytishimiz mumkinki, ichki ishlar organlari xodimlari o'z zimmasiga yuklatilgan vazifalarni muvaffaqiyatli bajarishlari uchun axborot texnologiyalari sohasidagi jinoyatlarni aniqlash, kiberjinoyatchilikka qarshi kurashish, axborot texnologiyalari sohasida sodir etilishi mumkin bo'lgan huquqbuzarliklarni barvaqt oldini olish, mamlakatimiz va xorijdagi huquqni muhofaza qilish organlarining axborot texnologiyalari orqali sodir etilayotgan jinoyatlarni oldini olish, ularni fosh etish hamda jamoat xavfsizligini ta'minlashda ilg'or ish tajribalarni o'rganishlari lozim.

Hurmatli konferensiya ishtirokchilari!

Umid qilamanki, bugun o'tkazilayotgan respublika ilmiy-amaliy konferensiyada ko'rib chiqiladigan muammolar, bildiriladigan fikrlar, takliflar va tavsiyalar yurtimizda kiberjinoyatlarni oldini olish, aniqlash va fosh etishda ko'mak bo'ladi.

So'zim yakunida menga berilgan vakolatdan foydalanib, konferensiyani ochiq deb e'lon qilaman hamda barcha ishtirokchilarga muvaffaqiyatlar tilayman!

E'tiboringiz uchun rahmat.

U.E. Rasulev

O'zbekiston Respublikasi Ichki ishlar vazirligi Malaka oshirish instituti boshlig'ining birinchi o'rinbosari, dotsent.

TARMOQ VA DASTURIY TA'MINOT XAVFSIZLIGINI OSHIRISHDA ILG'OR HIMOYA VOSITALARINING TAHLILI

Ulug'bek Erkinovich Rasulev

*O'zbekiston Respublikasi Ichki ishlar vazirligi Malaka oshirish instituti
boshlig'ining birinchi o'rinbosari dotsent*

Axborot texnologiyalarining jadal sur'atlarda rivojlanishi zamonaviy jamiyat hayotining deyarli barcha sohalariga bevosita ta'sir ko'rsatmoqda. Raqamlashtirish jarayonining tezlashuvi, internet xizmatlarining kengayishi va kompyuter tarmoqlarining global tarmoqqa integratsiyalashuvi natijasida turli xil axborot resurslariga bo'lgan talab keskin oshdi. Shu bilan birga, axborotlar oqimi hajmining ortishi va texnologik imkoniyatlarning kengayishi borasida kiberxavfsizlik muammolari tobora dolzarb masalaga aylanmoqda. Dunyo bo'yicha tashkilotlar, korxonalar va davlat muassasalari o'z faoliyatini elektron platformalar orqali yuritmoqda. Masofaviy xizmatlar, onlayn bank operatsiyalari, elektron tijorat, tibbiy ma'lumotlar bazalari, ta'lim tizimlari va boshqa ko'plab sohalarda katta hajmdagi ma'lumotlar tarmoqlar orqali uzatiladi va saqlanadi. Shu sababli, ushbu ma'lumotlarning xavfsizligini ta'minlash eng muhim vazifalardan biriga aylangan. Tarmoq xavfsizligini ta'minlash bugungi kunda axborot texnologiyalarining rivojlanishi bilan bevosita bog'liq bo'lib, bu sohada zamonaviy himoya texnologiyalaridan foydalanish juda muhim hisoblanadi.

No	Himoya texnologiyasi / Yondashuv	Asosiy funksiyasi	Samaradorlik darajasi (%)	Izoh
1	Firewall	Kiruvchi va chiquvchi trafikni filtrlash	85%	Asosiy xavfsizlik devori, barcha tarmoq qatlamlariga mos keladi
2	IDS (Intrusion Detection System)	Noqonuniy faoliyatni aniqlash	75%	Tahdidlarni aniqlaydi, ammo bartaraf eta olmaydi
3	IPS (Intrusion Prevention System)	Aniqlangan tahdidlarni bloklash	80%	IDS bilan integratsiyada samaradorligi oshadi
4	VPN (Virtual Private Network)	Ma'lumotlar uzatishda shifrlash	70%	Uzoqdan xavfsiz ulanishni ta'minlaydi
5	SDLC (Secure Software Development Life Cycle)	Xavfsizlikka yo'naltirilgan dasturiy ishlab chiqish	90%	Tizimli va barqaror xavfsizlikni ta'minlaydi
6	Statik va dinamik kod tahlili vositalari	Dasturiy zaifliklarni aniqlash va bartaraf etish	80%	Avtomatlashtirilgan audit vositasi sifatida ishlatiladi
7	Tashkiliy choralar (o'quv, siyosatlar)	Foydalanuvchi xatti-harakatlarini nazorat qilish, bilim berish	65%	Texnologiyaga emas, inson omiliga asoslangan

O'tkazilgan tadqiqotlar va amaliy tajribalar shuni ko'rsatmoqdaki, zamonaviy himoya texnologiyalaridan foydalangan holda tarmoq xavfsizligini yuqori darajada ta'minlash mumkin. Jumladan, firewall (dastlabki kirishni nazorat

qiluvchi tizim), IDS/IPS (kirishlarni aniqlash va oldini olish tizimlari) hamda VPN (virtual shaxsiy tarmoqlar) texnologiyalari orqali kiberhujumlar xavfini sezilarli darajada kamaytirish mumkin. Firewall tizimlari tarmoqqa kirish va chiqish ma'lumotlarini nazorat qiladi va faqat ruxsat berilgan trafikni o'tkazadi. IDS (Intrusion Detection System) tizimlari esa tarmoqqa noqonuniy kirish harakatlarini aniqlab, ogohlantiradi, IPS (Intrusion Prevention System) esa aniqlangan tahdidlarni avtomatik ravishda bloklaydi. VPN texnologiyasi esa masofaviy kirishlar vaqtida ma'lumotlarning shifrlangan kanal orqali uzatilishini ta'minlab, ularga uchinchi tomonlar aralashuvining oldini oladi. Shuningdek, dasturiy ta'minot xavfsizligini oshirish ham tarmoq xavfsizligining ajralmas qismidir.

Olib borilgan ilmiy-amaliy tadqiqotlar natijasida aniqlanishicha, dasturiy ta'minotni ishlab chiqish jarayonida Secure Software Development Life Cycle (SDLC) — xavfsiz dasturiy ta'minotni ishlab chiqish hayotiy sikli — tamoyillariga qat'iy amal qilish tizimning umumiy xavfsizligini sezilarli darajada oshiradi. Ushbu yondashuv dasturiy ta'minotning har bir bosqichida, ya'ni talablarni aniqlashdan tortib testlash va foydalanishga topshirishgacha bo'lgan jarayonlarda xavfsizlik choralari ko'zda tutadi.

Bundan tashqari, dasturiy kodni avtomatik tarzda skanerlash va xavfsizlik tahlilini o'tkazish vositalari (masalan, statik va dinamik tahlil vositalari) orqali dasturiy zaifliklar erta aniqlanadi va ularni vaqtida bartaraf etish imkoniyati paydo bo'ladi. Bu esa nafaqat tizimni mustahkamlashga, balki kiberxavfsizlik xavf-xatarlarini kamaytirishga ham xizmat qiladi. Kiberhujumlarni oldindan aniqlash uchun sun'iy intellekt va mashinaviy o'rganish asosida ishlovchi xavfsizlik tizimlarini joriy etish. Blockchain texnologiyasi yordamida ma'lumotlar xavfsizligini ta'minlash. Zero Trust Architecture (ZTA) tamoyiliga asoslangan xavfsizlik strategiyalarini ishlab chiqish.

Tarmoq va dasturiy ta'minot xavfsizligini ta'minlashda zamonaviy himoya texnologiyalaridan foydalanish, xavfsizlikka yo'naltirilgan dasturiy ishlab chiqish tamoyillariga amal qilish va xavfsizlikni avtomatik nazorat qilish vositalaridan keng foydalanish orqali axborot tizimlarining himoya darajasini yuqori pog'onaga olib chiqish mumkin. Bu esa o'z navbatida korxonalar, tashkilotlar va yakka foydalanuvchilarning axborot resurslarini ishonchli himoya qilishga xizmat qiladi.

Foydalanilgan adabiyotlar:

1. C.Adelard, O.Penrod. Implementation of Network Security System Using Firewall Technology and Intrusion Detection System (IDS). *Idea: Future Research*, 1(3), 113–121. 2023y.
2. M.Latah, L.Toker. An Efficient Flow-based Multi-level Hybrid Intrusion Detection System for Software-Defined Networks. 2018y.
3. F. Qodirov, Z. Mardonov. Firewall va ids/ips tizimlari: himoya va vositalari. *zdift*, 4(5), 125–130. 2025y.

КИБЕРЖИНОЯТ НИМА ВА УНДАН ҚАНДАЙ ҲИМОЯЛАНИШ КЕРАК

Кудратов Бунёд Бахтиёрович

*Ўзбекистон Республикаси Хуқуқни муҳофаза қилиш академияси
Рақамли криминалистика илмий-тадқиқот институтининг
Кибержиноятларга қарши курашишга ва рақамли терговга қўмаклашиш
маркази бошлиғи bunyodbaxtiyorovichkudratov@mail.ru*

Аннотация: Мақолада замонавий дунёнинг энг долзарб муаммоларидан бири – кибержиноятлар масаласи кенг ёритилган. Кибержиноят тушунчаси, унинг турлари (зарарли дастурлар, фишинг, DDoS-ҳужумлар), субъектлари ва глобал иқтисодиётга етказётган зарарлари таҳлил қилинган. Жаҳон миқёсида йиллик 20 триллион доллар зарар келтираётган бу соҳада Ўзбекистон статистикаси ҳам келтирилган. Мақолада кибержиноятлардан ҳимояланишнинг техник ва ҳуқуқий чоралари, антивирус дастурлари, паролларни ҳимоялаш, шахсий маълумотлардан эҳтиёткорлик билан фойдаланиш бўйича амалий тавсиялар берилган.

Калит сўзлар: кибержиноят, киберхавфсизлик, фишинг, зарарли дастурлар, рақамли ҳимоя, интернет хавфсизлиги, кибер ҳужумлар.

XXI аср ахборот технологиялари ва рақамлаштириш асри бўлиб, инсон фаолиятининг деярли барча соҳалари интернет ва компьютер технологиялари билан чамбарчас боғлиқдир. Лекин технологик тараққиёт билан бирга янги хил жиноятлар – кибержиноятлар ҳам пайдо бўлди. Бугунги кунда бу масала глобал хавфсизлик учун жиддий таҳдид бўлиб қолмоқда.

Сўнгги йилларда мамлакат иқтисодиётининг рақамли сектори кенгайиб, унинг асосий ўсиш омиллари ҳисобланган электрон тижорат платформалари, рақамли сервислар ва уларда амалга ошириладиган тўловларни сифатли ва хавфсиз қайта ишлаш билан боғлиқ молиявий технологиялар шиддат билан ривожланмоқда. Шу билан бирга, кейинги вақтларда банк карталаридан фойдаланган ҳолда ўғрилиқ ёки фирибгарлик ҳолатларининг кўпайиши аҳолининг рақамли молиявий саводхонлиги ҳамда ҳуқуқни муҳофаза қилувчи органлар ходимларининг малакаси етарли эмаслиги, тижорат банклари, тўлов тизими операторлари ва тўлов ташкилотларида ҳуқуқбузарликларнинг олдини олишнинг замонавий тизимлари мавжуд эмаслигидан далолат бермоқда.

Кибержиноятлар оқибатида етказилган жами зарар 2026 йилга қадар 20 триллион доллардан ошиши кутилмоқда. Баъзи ҳисоб-китобларга караганда 2020 йилда кибержиноятлар оқибатида жаҳон иқтисодиётига

1 триллион АҚШ долларидан ортиқ зарар етказилган, 2025 йилга бориб эса бу кўрсаткич 10 триллион АҚШ долларидан зиёдни ташкил этиши тахмин қилинмоқда.

Кибержиноятчилик – бу компьютер тармоқларида ва “Интернет” тармоғида содир этиладиган жиноят қонунчилигининг бузилиши. Ушбу тушунча ҳозирча умумий характерга эга ва ахборот технологиялари ва телекоммуникация тармоқлари соҳасидаги жиноятлар каби аниқ эмас.

Шу билан бирга, кибержиноятчилик – бу жиноят кодексида назарда тутилган жиноятларни содир этиш учун кибермакон, ахборот технологиялари ёки электрон воситалардан фойдаланиш ҳаракати. Бу тушунча ахборот технологиялари ва телекоммуникация тармоқлари соҳасидаги жиноятчилик тушунчасига ўхшаш, аммо бу ҳолда телекоммуникация соҳаси эслатилмайди.

Хорижий давлатлар қонунчилигини кўриб чиқиб, бу турдаги жиноятчилик ўз табиатига кўра ички характерга эга эканлигини кўриш мумкин. Ахборот технологиялари ва телекоммуникация тармоқлари соҳаси бошқа анъанавий жиноятлар каби барча ўша хусусиятларга эга, аммо фарқи қуйидагича.

Жиноят предмети нуқтаи назаридан, энг оддий маънода, компьютерлар ва бошқа телекоммуникация қурилмалари қимматли актив ҳисобланади. Шу муносабат билан улар ўғирлик кўринишидаги жиноят предмети сифатида ҳам иштирок этиши мумкин. Агар уларни мураккаброқ нуқтаи назардан кўриб чиқсак, жиноят предметининг бир қисми сифатида компьютерлар ва телекоммуникация қурилмалари жиноятчилар қандайдир операцияларни тўхтатиш ёки ташувчиларда сақланадиган маълумотларни ўғирлаш мақсадида қасдан ўғирлик содир этишида ҳам намоён бўлади.

Жиноят воситалари нуқтаи назаридан, компьютерлар ва бошқа телекоммуникация қурилмалари уларнинг аъло даражадаги имкониятлари туфайли турли хил жиноятчилар томонидан тобора кўпроқ қўлланилмоқда. Жиноятлар воситалари сифатида компьютерлар ва телекоммуникация қурилмаларидан фойдаланиш икки тоифада кўриб чиқилади: биринчидан, компьютерлар ва телекоммуникация қурилмалари қимор ўйинлари, телекоммуникация хизматларини ўғирлаш билан боғлиқ жиноятлар ва ҳоказолар каби анъанавий жиноятларни содир этиш воситалари сифатида ишлатилади; иккинчидан, компьютерлар ва телекоммуникация қурилмалари ҳамда уларда сақланадиган маълумотлар жиноятчилар томонидан фойдаланувчи ҳисобларини, шахсий маълумотларни ва ҳоказоларни ўғирлаш каби жиноятларни содир этиш учун ишлатилади.

Кибержиноят ҳар доим қуйидагиларнинг камида биттасини назарда тутлади. Биринчиси, компьютерларга ҳужум қилишни мақсад қилган фаолият: компьютерларни зарарли дастурлар билан зарарлаш, тизимларни шикастлаш ёки тўлиқ ишдан чиқариш, маълумотларни ўчириш ёки ўғирлаш, DDoS-ҳужуми (хизматдан бош тортиш турдаги ҳужум). Иккинчиси, бошқа жиноятларни содир қилиш учун компьютерлардан фойдаланиш: зарарли дастурларни тарқатиш, тақиқланган ахборот ёки тасвирларни тарқатиш, фирибгарлик схемаларини амалга ошириш.

Кибержиноятларнинг бошқа асосий турлари қуйидагилардан иборат: электрон почта ва интернет орқали фирибгарлик, шахсий маълумотларни ўғирлаш ва улардан ғараз мақсадларда фойдаланиш, тўлов карталари маълумотлари ва бошқа молиявий ахборотни ўғирлаш, корпоратив маълумотларни ўғирлаш ва қайта сотиш, кибершантаж (ҳужум билан таҳдид қилиб пул талаб қилиш), криптожекинг (бошқаларнинг ресурсларидан фойдаланиб криптовалюта қазиб олиш), кибержосуслик (давлат ёки корпоратив маълумотларга рухсатсиз кириш), муаллифлик ҳуқуқларини бузиш, тақиқланган товарлар билан онлайн савдо қилиш.

Кибержиноятлардан ҳимояланиш учун аввало техник ҳимоя чораларини кўриш лозим. Дастурий таъминот ва операцион тизимни мунтазам янгилаш компьютерингизда долзарб хавфсизлик тузатишларининг мавжудлигини кафолатлайди. Антивирус ёки комплекс интернет хавфсизлиги ечимидан фойдаланиш тизимингизни кибер ҳужумлардан ҳимоялашнинг яхши усули.

Антивирус дастурлари тизимни скан қилиш, таҳдидларни аниқлаш ва улар зарар етказишдан олдин зарарсизлантириш имкониятини беради. Ҳеч ким топа олмайдиган мустаҳкам паролларни қўлланг ва уларни ёзма шаклда сақламанг. Шунингдек, сиз учун тасодикий мустаҳкам паролларни генерация қиладиган ишончли парол менежеридан ҳам фойдаланишингиз мумкин.

Хулқ-атвор чоралари ҳам жуда муҳим. Спам хатлардаги иловалар орқали кибержиноятчилар турли хил ҳужумларни амалга оширадилар, жумладан компьютерни зарарли дастурлар билан юктирадилар. Номалум жўнатувчилардан келган иловаларни ҳеч қачон очманг. Фуқароларимиз кўпинча спам хатлар ва бошқа хабарлардаги ҳаволаларни босиб, номалум веб-сайтларга кириб кибержиноятчилар қурбони бўлмоқдалар. Хавфсизликда қолиш учун бундай ҳаволаларни ҳеч қачон босманг. Алоқаларингизнинг хавфсизлигига тўлиқ ишонч ҳосил қилмагунча шахсий маълумотларингизни телефон ёки электрон почта орқали ҳеч қачон, ҳеч кимга айтманг. Сухбатдошингиз ҳақиқатдан ҳам ўзини кўрсатаётган киши эканлигига ишонч ҳосил қилинг.

Расмий каналлар орқали мулоқот қилиш принципи ҳам жуда муҳим. Агар сизга бирор ташкилотдан қўнғироқ қилиб, суҳбат давомида шахсий маълумотларингизни сўрасалар, телефон гўшагини қўйинг.

Кибержиноятчи билан эмас, балки ҳақиқий ходим билан гаплашаётганлигингизга ишонч ҳосил қилиш учун компаниянинг расмий веб-сайтида кўрсатилган рақамга қайта қўнғироқ қилинг.

Веб-сайтларга кириш пайтида ҳам эҳтиёт бўлиш керак. Босадиган ҳаволаларнинг URL манзилларига эътибор беринг. Манзилнинг ҳақиқийлигига ишонч ҳосил қилинг. URL манзили номаълум ёки спам каби кўринадиган ҳаволаларни босманг. Онлайн тўлов қилишдан олдин антивирус ҳимояси ёқилганлигини текширинг.

Банк операцияларини мунтазам назорат қилиш ҳам муҳим чора. Агар сиз кибержиноят қурбони бўлган бўлсангиз, буни иложи борича тезроқ аниқлаш муҳим. Операциялар тарихини мунтазам кўриб чиқинг ва ҳар қандай шубҳали транзакция бўйича банкдан маълумот сўранг.

Хулоса қилиб айтганда, кибержиноятлар замонавий жамиятда жиддий таҳдид бўлиб, ҳам жисмоний шахслар, ҳам компаниялар учун катта хавф туғдирмоқда. Ер юзида ҳар 39 сонияда киберхавфсизликга қарши ҳужум содир этилади. 2024 йил IV кварталда инцидентлар сони олдинги кварталга нисбатан 5%га ошган. Кибер таҳдидлар доимо ривожланиб, мураккаблашиб бормоқда. Зарарли дастурлар жиноятчиларнинг асосий воситаси бўлиб қолмоқда: улар ташкилотларга қарши муваффақиятли ҳужумларнинг 66% ва жисмоний шахсларга қарши ҳужумларнинг 51% ида қўлланилмоқда. Шунинг учун ҳар бир фойдаланувчи ва ташкилот ўз хавфсизлигини таъминлаш учун профилактика чораларини кўришга, замонавий ҳимоя воситаларидан фойдаланишга ва рақамли саводхонликни ошириши даркор. Кибержиноятлардан ҳимояланиш нафақат техник воситалар, балки рақамли гигиена қоидаларига риоя қилиш, эҳтиёткорлик ва доимий хабардорликни ҳам талаб қилади. Фақат комплекс ёндашув орқали кибермакондаги хавфсизликни таъминлаш мумкин. Сифатли антивирус ечими ва профессионал маслаҳатлар сизни кибер таҳдидлардан ҳимоялашда муҳим роль ўйнайди. Рақамли технологиялардан фойдаланишда доимо эҳтиёткор бўлинг.

Фойдаланилган адабиётлар рўйхати:

1. Шавкат Мирзиёев. Эркин ва фаравон, демократик Ўзбекистон давлатини биргаликда барпо этамиз. // “Ўзбекистон” НМИУ. Тошкент – 2016;
2. Ўзбекистон Республикаси Жиноят кодекси, Ўзбекистон Республикасининг Миллий қонунчилик базаси (lex.uz);

3. Ўзбекистон Республикаси Жиноят процессуал кодекси.
<https://lex.uz/docs/111460>;
4. М.Х.Рустамбаев, “Ўзбекистон Республикаси Жиноят кодексига шархлар”, 2024 йил;
5. Cybersecurity Statistics & Trends For 2025 // Website Rating. – 2025. – URL: <https://www.websiterating.com/blog/research/cybersecurity-statistics-facts/>;
6. Актуальные киберугрозы: IV квартал 2024 года — I квартал 2025 года // Positive Technologies. – 2025. – URL: <https://ptsecurity.com/ru-ru/research/analytics/>;
7. Статистика кибербезопасности, тенденции и факты, имеющие значение на 2022 год // Website Rating. – 2022. – URL: <https://www.websiterating.com/ru/research/cybersecurity-statistics-facts/>;
8. В 2024 году количество атак через подрядчиков выросло в три раза // TAdviser. – 2025. – URL: https://tadviser.ru/index.php/Статья:Число_кибератак_в_России_и_в_мире;
9. Кибербезопасность: занимательная статистика // Стахановец. – 2023. – URL: <https://stakhanovets.ru/blog/kiberbezopasnost-zanimatelnaya-statistika/>;
10. What is Bitcoin? // Kaspersky Resource Center. – URL: <https://www.kaspersky.ru/resource-center/definitions/what-is-bitcoin>;
11. Spam and Phishing // Kaspersky Resource Center. – URL: <https://www.kaspersky.ru/resource-center/threats/spam-phishing>;
12. DDoS Attacks // Kaspersky Resource Center. – URL: <https://www.kaspersky.ru/resource-center/threats/ddos-attacks>.

AXBOROT-TELEKOMMUNIKATSIYA TEXNOLOGIYALARIDAN FOYDALANIB SODIR ETILAYOTGAN JINOYATLARGA QARSHI KURASHNI TASHKIL ETISH

Marupov Erkinjon Elmirovich

*O‘zbekiston Respublikasi Ichki ishlar vazirligi Malaka oshirish instituti
Axborot texnologiyalari sikl boshlig‘i*

Annotatsiya. Ushbu maqolada axborot-telekommunikatsiya texnologiyalari (ATT) yordamida sodir etiladigan jinoyatlarga qarshi kurashni tashkil etishning dolzarb muammolari va yo‘nalishlari muhokama qilinadi. Bunday jinoyatlarni fosh etish va tergov qilish murakkab tizim bo‘lib, kompleks yondashuvni hamda tashkiliy-texnik, tashkiliy-taktik va tashkiliy-uslubiy usullarni samarali qo‘llashni talab etadi. Zamonaviy IT-jinoyatchilik global va transchegaraviy xususiyatga ega bo‘lib, yuqori latentligi bilan ajralib turadi. Huquqni muhofaza qiluvchi organlar

duch kelayotgan asosiy qiyinchiliklarga malakali kadrlar yetishmasligi, tergov usullarining tez eskirishi va raqamli ma'lumotlarni to'plash hamda tahlil qilishning murakkabligi kiradi. Odatiy jarayonlarni avtomatlashtirish, bashorat qilish va qonuniyatlarni aniqlash uchun sun'iy intellekt (SI) va katta hajmli ma'lumotlar kabi ilg'or axborot texnologiyalaridan foydalanish zarurligi ta'kidlanadi. Tadqiqot tuzilmaga ega bo'lmagan matnli ma'lumotlarni tahlil qilish va buzg'unchi kontentni aniqlash uchun sun'iy intellektdan foydalanishni yoritib beradi. Axborotni integratsiyalash, yagona ma'lumotlar bazasini yaratish va mutaxassislar tayyorlashni takomillashtirish masalalariga alohida e'tibor qaratiladi.

Kalit so'zlar: Axborot-telekommunikatsiya texnologiyalari, kiberjinoyatchilik, jinoyatchilikka qarshi kurash, ichki ishlar organlari, sun'iy intellekt, katta ma'lumotlar.

Zamonaviy dunyoda axborot-telekommunikatsiya texnologiyalaridan foydalanib sodir etilayotgan jinoyatlar murakkab va tez rivojlanayotgan muammo hisoblanadi. Bu jinoyatlarning o'ziga xos xususiyatlari yuqori yashirinlik, chegaralararo xususiyat hamda apparat-dasturiy vositalar va aloqa texnologiyalarining faol qo'llanilishidir. Jinoyatchilar doimo yangi va paydo bo'layotgan texnologiyalardan foydalanmoqdalar, bu esa jinoyatchilikning mavjud va shakllanayotgan turlarining oldini olish va ularga qarshi kurashishda misli ko'rilmagan qiyinchiliklarni keltirib chiqarmoqda. Bunday jinoyatlar O'zbekiston Respublikasi Jinoyat kodeksining Maxsus qismida ko'rsatilgan deyarli barcha sohalarda ATTLaridan foydalangan holda sodir etilishi mumkin va uncha og'ir bo'lmagan jinoyatlardan tortib o'ta og'ir jinoyatlargacha bo'lgan turli toifalarga kiradi.

Huquqni muhofaza qilish organlari oldida turgan muammolar

Ichki ishlar organlari (IIO) ITT jinoyatlariga qarshi samarali kurashishda bir qator muhim muammolarga duch kelmoqda:

- Raqamli kriminalistika sohasida malakali kadrlarning yetishmasligi.
- Yangi texnologiyalar paydo bo'lishi sharoitida tergov usullarining tez eskirishi.
- Osongina yo'q qilinishi yoki o'zgartirilishi mumkin bo'lgan kriminalistik ahamiyatga ega raqamli ma'lumotlarni to'plash va tahlil qilishning murakkabligi.
- Transchegaraviy jinoyatlarni tergov qilish uchun tashqi, shu jumladan O'zbekiston Respublikasi yurisdiksiyasidan tashqaridagi subyektlar bilan hamkorlik qilish zarurati.
- Aloqa operatorlaridan ma'lumot olish bilan bog'liq muammolar, ko'pincha ma'lumotlarni taqdim etmaganlik uchun jarimalarning pastligi, bu esa tergov organlarining so'rovlariga javoblarning uzoq vaqt kechikishiga olib keladi.

Texnologik yechimlar va istiqbollar

ITT jinoyatlariga qarshi kurashish samaradorligini oshirish uchun ilg'or texnologiyalarni faol joriy etish va ulardan foydalanish maqsadga muvofiqdir:

- Sun'iy intellekt (SI) va katta ma'lumotlar (Big Data):
 - Loglarni tahlil qilish, tasvirlar va matnlarni aniqlash kabi kundalik jarayonlarni avtomatlashtirish.
 - Foydalanuvchilar xatti-harakatlaridagi qonuniyatlar va g'ayrioddiy holatlarni aniqlash.
 - Jinoyatlarning oldini olish maqsadida ularning sodir etilish ehtimolini bashorat qilish uchun prognozli tahlil.
 - Chuqur neyron tarmoqlari (BERT, GRU, LSTM) yordamida buzg'unchi mazmuni (masalan, ekstremizm, antisemitizm, terrorizmga chaqiriqlar) aniqlash uchun tizimlanmagan matnli ma'lumotlarni tahlil qilish. Bu, ayniqsa, Telegram messenjeridagi ulkan hajmdagi matnli kontentni tahlil qilish uchun dolzarbdir.
 - Tarmoq tahlili uchun ma'lumotlarni qayta ishlash va jinoiy tarmoqlarning noaniq chegaralari muammosini hal etish.
 - Virtual yordamchilar va suhbat-botlarni yaratish uchun tabiiy tilni qayta ishlash.
- Uzluksiz texnologiyalar: Jarayonning barcha tarkibiy qismlarini integratsiyalash.

Raqamli kriminalistika va biometriya:

- Elektron-raqamli izlarni markazlashtirilgan holda yig'ish va tahlil etish.
- DNK asosida insonning tashqi va morfologik xususiyatlarini (yosh, ko'z, soch, teri rangi) bashorat qilish uchun DNK fenotiplash usullarini ishlab chiqish.
- Barmoq izlari, ko'z gavhari va boshqa o'ziga xos xususiyatlarni tahlil qilishga asoslangan biometrik tizimlardan foydalanish.
- Past sifatli tasvirlardagi yuzlarni ham aniqlash, tanib olish va identifikatsiya qilishni takomillashtirish uchun sun'iy intellekt algoritmlaridan foydalangan holda yuz tanish tizimlarini qo'llash.
- Yuz berkitilgan bo'lsa ham, shaxsni aniqlash uchun yurish uslubini tahlil qilish.
 - Axborot integratsiyasi: Yagona ma'lumotlar bazalarini yaratish, masalan, moliyaviy oqimlar haqidagi ma'lumotlar, gumonlanuvchilarning 3D tasvirlari, shuningdek, Rossiya IIV Axborot-tahlil departamenti, ijtimoiy tarmoqlar, kosmik geolokatsiya tizimlaridan olingan ma'lumotlarni birlashtirish.
 - Internet tarmog'idan ma'lumot yig'ish va noqonuniy kontentni yaratish hamda tarqatishga aloqador shaxslarni aniqlash uchun maxsus parser dasturlarini ishlab chiqish.

Tashkiliy va huquqiy chora-tadbirlar

Axborot-telekommunikatsiya texnologiyalari sohasidagi jinoyatchilikka qarshi samarali kurashish, shuningdek, quyidagi tashkiliy va huquqiy jihatlarni takomillashtirishni talab etadi:

- Muloqot, shaxslararo munosabatlar odobi, nizolarni bartaraf etish, shuningdek, IT-texnologiyalar, iqtisodiyot, huquq, boshqaruv va sotsiologiya sohalarida kadrlarning kasbiy va maxsus tayyorgarlik darajasini oshirish.

- Xodimlar o‘rtasida bilim va tajribaning uzluksizligini ta’minlash.

- Raqamli izlarni aniqlash, qayd etish, olish va o‘rganishning zamonaviy usullariga asoslangan holda jinoyatlarni tergov qilishni texnik-kriminalistik ta’minlash sohasida ilmiy asoslangan tavsiyalar ishlab chiqish.

- Boshqaruv qarorlari samaradorligini oshirish uchun ommaviy hokimiyatni cheklash shakllarining yaxlit konsepsiyasini shakllantirish.

- Ishonchli, aniq, xavfsiz, shaffof, hisobdor va axloqiy bo‘lishi lozim bo‘lgan ishonchli innovatsion texnologiyalardan foydalanish tamoyillarini qabul qilish va ularga rioya etish.

- Aktivlarni qidirish va qaytarish uchun ixtisoslashtirilgan moliyaviy razvedka bo‘linmalarini tashkil etish.

- Hisobga olish obyektlarini aniqlashtirish va kriminalistik ahamiyatga ega axborotni hisobga olish tizimini takomillashtirish.

- Terrorizmga qarshi himoyani kuchaytirish uchun sog‘liqni saqlash obyektlarini toifalash mezonlarini aniqlashtirish.

Kriptoalyutalardan foydalanish bilan bog‘liq jinoyatlarga qarshi kurashishga alohida e’tibor qaratilmoqda. Bu sohada qonunchilikni tartibga solish va blokcheyn texnologiyasiga asoslangan tergov qilish metodologiyasini takomillashtirish talab etiladi.

Xulosa

Axborot-telekommunikatsiya texnologiyalaridan foydalangan holda sodir etiladigan jinoyatlarga qarshi samarali kurashish zamonaviy raqamli o‘zgarishlar sharoitida jamoat xavfsizligi va huquq-tartibotni ta’minlashning asosiy vazifasidir. Bu lingvistik, metodologik va ijtimoiy-madaniy kompetensiyalarni birlashtirgan holda yaxlit yondashuvni talab qiladi. Bunday qarshi kurashning eng muhim tarkibiy qismlari axborot texnologiyalarini, shu jumladan katta ma’lumotlarni tahlil qilish usullarini va sun’iy intellektni uzluksiz joriy etish va takomillashtirishdir. Shu bilan birga, mutaxassislarni o‘qitish va malakasini oshirish orqali kadrlar salohiyatini mustahkamlash, kiberjinoyatchilikning transmilliy va murakkab shakllariga qarshi kurashish uchun xalqaro va idoralararo hamkorlikni rivojlantirish zarur. Texnologiyalarning rivojlanish dinamikasi va yangi muammolarni hisobga oladigan bunday keng qamrovli va moslashuvchan

yondashuvgina xavfsizlikni ta'minlash sohasidagi zamonaviy vazifalarni hal qilishga qodir bo'lgan yuqori malakali mutaxassislarni tayyorlashni kafolatlaydi.

Foydalanilgan adabiyotlar:

1. Николаева Анастасия Николаевна Преступления, совершаемые с использованием средств массовой информации и информационно-телекоммуникационных сетей: некоторые ситуационные аспекты раскрытия и расследования // Академическая мысль. 2024. №4 (29). URL: <https://cyberleninka.ru/article/n/prestupleniya-sovershaemye-s-ispolzovaniem-sredstv-massovoy-informatsii-i-informatsionno-telekommunikatsionnyh-setey-nekotorye> (дата обращения: 20.05.2025).

2. Гаврилин Ю. В., Пинкевич Т. В., Мартыненко Н. Э., и др. Организация противодействия преступлениям, совершаемым с использованием информационно-телекоммуникационных технологий : учебник : в 2 ч. / под ред. Ю. В. Гаврилина. - Москва : Академия управления МВД России, 2024. - Ч. 1. - 304 с. ISBN 978-5-907721-62-3.

3. Батоев В.Б. IT-преступность: современное состояние, проблемы противодействия, пути их решения // Криминалистика, уголовный процесс и судебная экспертология в XXI веке: векторы развития (к 70-летию кафедры управления органами расследования преступлений академии управления мвд россии (66-е ежегодные криминалистические чтения). Ч. 1. 220-227. 2025.

4. Залялов И.М., Куфтерин А.Н. К вопросу о цифровой трансформации уголовно-процессуальной деятельности // // Криминалистика, уголовный процесс и судебная экспертология в XXI веке: векторы развития (к 70-летию кафедры управления органами расследования преступлений академии управления мвд россии (66-е ежегодные криминалистические чтения). Ч. 3. 57-65. 2025.

5. Краснов М.А., Попова Ю.К. Цифровая трансформация уголовно-процессуальной и экспертно-криминалистической деятельности // Криминалистика, уголовный процесс и судебная экспертология в XXI веке: векторы развития (к 70-летию кафедры управления органами расследования преступлений академии управления мвд россии (66-е ежегодные криминалистические чтения). Ч. 3. 82-89. 2025.

6. Muxammadqulov, Shohruhbek Erkin O'g'li Axborot texnologiyalaridan foydalanib sodir etiladigan firibgarlik jinoyatini fosh etish bo'yicha ayrim xorijiy mamlakatlar tajribasi // ORIENSS. 2024. №8. URL: <https://cyberleninka.ru/article/n/axborot-texnologiyalaridan-foydalanib-sodir-etiladigan-firibgarlik-jinoyatini-fosh-etish-bo-yicha-ayrim-xorijiy-mamlakatlar> (дата обращения: 20.05.2025).

7. Марупов Эркинжон Эльмирович Киберпреступность и дети: угрозы и профилактика. Материалы vii международной научно-теоретической конференции «права человека и глобализация», посвященной дню прав человека и объявлению «года правового просвещения». 266-271. 2024.

ELLIPTIC ВОСИТАЛАРИДАН КРИПТОВАЛЮТА ТРАНЗАКЦИЯЛАРИНИ ТАҲЛИЛ ҚИЛИШДА ФОЙДАЛАНИШ МАСАЛАСИ

Тухтаматов Х.Р.
СТИБОМ ходими, PhD.

Сўнгги ўн йилликда рақамли иқтисодиётнинг жадал ривожланиши билан параллел равишда криптовалюта бозорида транзакциялар сони ортиб бормоқда. Bitcoin, Ethereum, Tether, USD Coin, Binance Coin ва бошқа криптовалюталар ва стейблкоинлар нафақат молиявий восита, балки ноқонуний фаолиятларни амалга ошириш учун қулай платформага айланиб бормоқда. Бу эса давлатлар, молиявий ташкилотлар ва ҳуқуқни муҳофаза қилувчи идоралар учун жиддий муаммоларни келтириб чиқармоқда.

Ҳозирги кунда дунёнинг аксарият мамлакатлари криптовалютани тўлақонли пул воситаси сифатида қонуний тан олиш бўйича фаол кадамларни қўймаган. Тартибга солувчи органлар томонидан бундай ёндашувнинг асосий сабаби криптовалюталарнинг тез ўсишининг назоратсиз оқибатлари, ўзгарувчанликнинг кучайиши, спекулятив фаолиятнинг кенгайиши, шунингдек, жиноий даромадларни легаллаштириш ва терроризмни молиялаштириш билан боғлиқ ноқонуний фаолият каби таҳдидларнинг мавжудлиги ҳисобланади.

Молиявий институтлар ва ҳуқуқни муҳофаза қилувчи идораларга транзакцияларнинг қонунийлигини таъминлаш ва пул ювишининг олдини олиш учун блокчейнга асосланган операцияларни кузатиш муҳим аҳамият касб этади. Бизга маълумки, криптовалюта биржаларининг муваффақиятли ишлашининг калити фойдаланувчиларнинг юқори ишончи ва транзакцияларнинг шаффофлиги ҳисобланади. Бу борада Elliptic компанияси етакчи ташкилот сифатида тан олинган бўлиб, у криптовалюта блокчейнларини таҳлил қилиш, хавфларни баҳолаш ва жиноий фаолиятларни фош этиш соҳасида юқори технологияларга таянади. Бош қароргоҳи Лондонда жойлашган Elliptic компанияси 100 дан ортиқ мамлакатлардаги давлат идоралари, крипто биржалар, молия институтлари, суғурта компаниялари ва киберхавфсизлик компанияларига дастурий таъминот хизматлари, маълумотларни бошқариш ва тадқиқотлар ўтказишда ўз

хизматларини таклиф қилади¹. Шунингдек, АҚШ молия вазирлиги (FinCEN), Европа Иттифоқининг молия назорати органлари, Европа марказий банки, Буюк Британия молия назорати органи (FCA), йирик криптобиржалар (Binance, Coinbase), FATF ва бошқа халқаро ташкилотлар билан ахборот алмашинувини йўлга қўйган².

Elliptic компанияси ўз фаолиятида сунъий интеллект, машинали ўқитиш, катта маълумотлар таҳлили (big data analytics) ва блокчейн визуализациясидан фойдаланиб турли дастурий воситаларни ишлаб чиққан³:

1. Elliptic Navigator – криптовалюта транзакцияларни визуал таҳлил қилиш учун мўлжалланган платформа бўлиб, блокчейндаги транзакцияларни график кўринишда тақдим этади, улар ўртасидаги боғлиқликларни аниқлашга ёрдам беради. Жиноий фаолиятнинг манбасини, иштирокчи манзилларни ва криптовалюта ҳаракатининг йўналишини таҳлил қилиш имконини беради.

2. Elliptic Lens – крипто-манзилларнинг ишончилигига баҳо беришда қўлланилиб, фойдаланувчига манзилнинг илгариги фаолиятини таҳлил қилиб, унинг жиноий фаолиятга боғлиқ ёки боғлиқ эмаслигини аниқлайди. Пул ювиш ва бошқа шубҳали фаолиятлар билан боғлиқ манзиллар аниқ белгилар билан ажратиб кўрсатилади.

3. Elliptic Discovery – платформаси криптобиржалар тўғрисидаги маълумотлар базасини жамлайди, шунингдек, уларнинг лицензиялари, юрисдикцияси, комплаенс сиёсати ва хавф даражасини баҳолаш имконини беради. Бу восита молиявий регуляторлар ва ташкилотлар учун муҳим восита ҳисобланади.

4. Elliptic Data Set – ҳозирда дунёдаги энг йирик блокчейн маълумотларни ўз ичига олувчи база бўлиб, бир неча млн транзакциялар, шубҳали фаолиятлар, уларнинг манбалари, NFT савдолари ва бошқа маълумотларни ўз ичига олган.

Elliptic технологиялари бир неча босқичли таҳлил ва шу асосда мониторинг қилиш имконини беради. Машинали ўқитиш моделлари (machine learning models) криптовалюта транзакциялари орасидаги паттернларни аниқлаб, фаолиятларнинг хавф даражасини баҳолайди⁴. Бизнинг фикримизча, Elliptic воситаларидан фойдаланишнинг афзалликлари қуйидагилардан иборат:

¹ Elliptic Official Website // <https://www.elliptic.co>

² FATF Guidance on Virtual Assets and VASPs // <https://www.fatf-gafi.org>

³ Elliptic Research Reports, 2021–2024 // <https://www.elliptic.co>

⁴ Solutions for Crypto Compliance and Investigations // <https://www.elliptic.co/>

– аниқлик ва ишончлилик. Elliptic крипто транзакцияларни аниқлаш ва кузатишга ёрдам берадиган маълумотлар базаси ва таҳлилий воситаларга эга;

– фойдаланиш қулайлиги. Elliptic интерфейси соддалиги ва фойдаланувчиларга керакли маълумотларни тезда топишга имкон бериши билан ажралиб туради;

– кенгайтирилган таҳлил хусусиятлари. Elliptic пул ювиш ва терроризмни молиялаштириш схемаларини очишга ёрдам берадиган таҳлил воситаларини, шу жумладан боғланиш графларини ва визуализацияларни таклиф этади;

– ҳуқуқни муҳофаза қилиш соҳасидаги ҳамкорлик. Elliptic дунё бўйлаб ҳуқуқни муҳофаза қилиш идоралари билан фаол ҳамкорлик қилади, уларга тергов ўтказиш учун маълумотлардан ва мавжуд тажрибалардан фойдаланиш имконини беради.

Шунингдек, Elliptic маълум чекланишларга ҳам эга бўлиб, улар жумласига блокчейн ва криптовалюталар билан боғлиқ транзакцияларни таҳлил қилишга ихтисослашганлиги ва бошқа турдаги молиявий операцияларни ўрганиш учун унинг имкониятлари чекланганлигини келтириб ўтиш мумкин. Бундан ташқари, Ellipticдан фойдаланиш хизматлари нарх юқори ҳамда уни бошқа тизимлар билан интеграциялаш имкониятлари мавжуд эмас.

Хулоса сифатида шуни таъкишлаш мумкинки, Elliptic компанияси хизматларидан криптовалюта транзакцияларини таҳлил қилиш ва жиноий фаолиятдан олинган даромадларни легаллаштириш каби ноқонуний ҳатти-ҳаракатларни аниқлаш соҳасида қўллаш молиявий хавфсизликни таъминлаш, шаффофликни ошириш ва комплаенс назорати талабларига риоя қилишда муҳим аҳамият касб этади. Шунингдек, криптовалюталар билан боғлиқ жиноятларга қарши самарали курашишда қуйидаги таклифларни илгари суриш мумкин:

блокчейн операциялари, криптовалюталар транзакциясини мониторинг қилишда турли воситаларни қўллаш. Chainalysis, Elliptic, Coin Metrics кабилардан фойдаланиш халқаро ва миллий қонунчиликка мувофиқ равишда тергов ҳаракатларини олиб бориш, крипто бозорни таҳлил қилиш ва бу орқали жиноий ишларни очишга ёрдам беради ҳамда истеъмолчиларнинг виртуал активларга киришини хавфсиз равишда таъминлаш имконини беради;

криптовалюталар орқали жиноий фаолиятдан олинган даромадларни легаллаштириш, терроризмни молиялаштириш, пул ювиш билан

шуғулланган гуруҳлар ва шахслар тўғрисидаги ахборотни жамловчи электрон маълумотлар базасини яратиш;

халқаро тажрибани эътиборга олган ҳолда крипто-активлар билан боғлиқ транзакциялар ва ҳисоб рақамларини (электрон ҳамён) назоратга олишда Ўзбекистон Республикаси Марказий банки ваколатларини кенгайтириш;

криптовалюталарнинг глобал табиати ва турли мамлакатларда тартибга солишдаги фарқлар туфайли, жиноят олами вакиллари бир юрисдикциядан бошқасига ўтишишига чек қўйиш мақсадида ушбу соҳадаги ёндашувларни уйғунлаштириш, миллий тартибга солувчилар ва халқаро ташкилотлар билан ҳамкорликни такомиллаштириш.

SUN'IY INTELLEKTDAN FOYDALANGAN HOLDA AXBOROT TEKNOLOGIYALARI SOHASIDA HUQUQBUZARLIKLARGA QARSHI KURASHNING DOLZARBLIGI VA ISTIQBOLLARI

Y.B.Tashmanov

IIV Malaka oshirish instituti kata o'qituvchisi, PhD, dotsent.

Xozirgi kunda raqamli texnologiyalarning rivojlanishi kiberjinoyatlar, shaxsiy ma'lumotlarni o'g'irlash va moliyaviy firibgarlik kabi yangi tahdidlarni keltirib chiqarmoqda. Mashinaviy o'rganish, tabiiy tilni qayta ishlash va bashoratli tahlil algoritmlarining kiberxavfsizlikni ta'minlashdagi imkoniyatlari tahlil qilinadi. O'zbekistonning "Raqamli O'zbekiston – 2030" strategiyasi doirasidagi tajribasi, huquqiy asoslari va SI'ni joriy etishdagi muammolar ko'rib chiqilmoqda. SI'ni keng qo'llash orqali davlat va fuqarolar xavfsizligini oshirish bo'yicha takliflar keltiriladi. Raqamli texnologiyalarning jadal rivojlanishi insoniyat hayotini tubdan o'zgartirib, iqtisodiyot, ta'lim, sog'liqni saqlash va boshqa sohalarda yangi imkoniyatlar yaratmoqda. Biroq, bu taraqqiyot bilan birga axborot texnologiyalari sohasida yangi turdagi jinoyat va huquqbuzarliklar xavfi ham ortib bormoqda. Kiberjinoyatlar, masalan, shaxsiy ma'lumotlarni o'g'irlash, moliyaviy firibgarlik, ruxsatsiz kirish va ma'lumotlarni buzish kabi holatlar jiddiy xavf tug'dirmoqda. Ushbu muammolar nafaqat shaxslarning xavfsizligiga, balki davlat va korxonalar faoliyatiga ham tahdid solmoqda.

An'anaviy usullar bu turdagi jinoyatlarga qarshi kurashda tobora samarasiz bo'lib bormoqda, chunki kiberjinoyatchilar ilg'or texnologiyalardan foydalanib, o'z faoliyatlarini doimiy ravishda takomillashtirmoqdalar. Shu sababli, sun'iy intellekt (SI) vositalarini joriy etish kiberxavfsizlikni ta'minlashda muhim ahamiyat kasb etmoqda. Sun'iy intellekt real vaqt rejimida katta hajmdagi

ma'lumotlarni tahlil qilish, xavf-xatarlarni aniqlash va oldini olish imkoniyatiga ega bo'lib, axborot texnologiyalari sohasidagi huquqbuzarliklarga qarshi kurashda innovatsion yechim sifatida ko'rilmogda.

Axborot texnologiyalari sohasidagi jinoyatlar soni global miqyosda yildan-yilga o'sib bormogda. Xalqaro tashkilotlar ma'lumotlariga ko'ra, kiberjinoyatlar iqtisodiyotga milliardlab dollar zarar keltirmogda. O'zbekiston kabi rivojlanayotgan mamlakatlarda raqamlashtirish jarayonining tezlashishi bilan birga kiberxavfsizlikka oid muammolar ham keskinlashmogda. Quyidagi asosiy huquqbuzarlik turlari alohida e'tiborga molik:

Shaxsiy ma'lumotlarni o'g'irlashda foydalanuvchilarning shaxsiy ma'lumotlari, masalan, bank kartasi raqamlari, pasport ma'lumotlari va boshqa maxfiy axborot noqonuniy ravishda qo'lga kiritilmogda.

Moliyaviy firibgarlikda onlayn platformalar orqali amalga oshiriladigan firibgarliklar, masalan, fishing (soxta saytlar orqali ma'lumot o'g'irlash) va boshqa usullar keng tarqalmogda. Ruxsatsiz kirishda tarmoq va axborot tizimlariga ruxsatsiz kirish orqali ma'lumotlarni o'zgartirish yoki yo'q qilish. DDoS hujumlari tizimlarni ishlamay qoldirish maqsadida serverlarga haddan tashqari yuklama keltirish. Ma'lumotlarni shifrlash va tovlamachilikda Ransomware (tovlamachi dasturlar) yordamida ma'lumotlarni shifrlab, foydalanuvchilardan pul talab qilish. Ushbu muammolar fuqarolarning shaxsiy hayotiga, moliyaviy xavfsizligiga va davlat axborot tizimlari ishonchliligiga jiddiy tahdid soladi. An'anaviy kiberxavfsizlik usullari, masalan, antivirus dasturlari yoki oddiy tarmoq monitoringi, bu xavflarga qarshi yetarli darajada samarali emas, chunki jinoyatchilar sun'iy intellekt va boshqa ilg'or texnologiyalarni o'z maqsadlari uchun foydalanmogdalar.

Sun'iy intellekt axborot texnologiyalari sohasida huquqbuzarliklarga qarshi kurashda keng imkoniyatlarga ega. Quyida SI'ning asosiy qo'llanilish yo'nalishlari keltirib o'tsak.

Sun'iy intellekt, xususan, mashinaviy o'rganish algoritmlari real vaqt rejimida tarmoq faoliyatini monitoring qilish orqali g'ayrioddiy xatti-harakatlar va shubhali faoliyatni aniqlay oladi.

Anomaliyalarni aniqlashda tarmoq trafigida odatiy bo'lmagan harakatlar (masalan, katta hajmdagi ma'lumotlar o'tkazilishi yoki noo'rin vaqtda tizimga kirish) SI algoritmlari tomonidan tezda aniqlanadi.

Bot faoliyatini aniqlashda soxta hisoblar yoki botlar tomonidan amalga oshiriladigan hujumlarni aniqlash va bloklash.

SI asosidagi tizimlar xavf tahlilini avtomatlashtirish orqali tizimlarni himoya qilishda muhim rol o'ynaydi.

Parol va autentifikatsiya xavfsizligi biometrik ma'lumotlar (yuzni tanish, barmoq izi) va xatti-harakat tahlili orqali ruxsatsiz kirishlarning oldini olish. Shifrlash va xavfsizlik devorlarida SI algoritmlari tarmoqqa kirish nuqtalarini doimiy ravishda kuzatib, shubhali kirishlarni avtomatik ravishda bloklaydi.

Videokuzatuv tizimlarida SI'ning qo'llanilishi noqonuniy faoliyatni oldindan aniqlashda muhim ahamiyatga ega:

Yuzni tanish texnologiyasida jinoyatchilarni aniqlash yoki shubhali shaxslarni kuzatish uchun SI asosidagi videokuzatuv tizimlari ishlatiladi. Harakat tahlilida omma oldida g'ayrioddiy xatti-harakatlar (masalan, jamoat joylarida shubhali harakatlar) SI algoritmlari tomonidan aniqlanadi.

Sun'iy intellekt ilgari sodir etilgan jinoyatlar ma'lumotlari asosida yangi tahdidlarni bashorat qilish imkonini beradi:

Bashoratli tahlili jinoyatlarning geografik joylashuvi, vaqti va turi bo'yicha ma'lumotlarni tahlil qilib, kelajakdagi xavf-xatarlarni aniqlash.

Resurslarni optimallashtirish orqali huquqni muhofaza qilish organlari faoliyatini samarali boshqarish uchun SI yordamida resurslarni to'g'ri taqsimlash.

O'zbekistonda axborot texnologiyalari sohasidagi huquqbuzarliklarga qarshi kurashda sun'iy intellektni joriy etish bo'yicha dastlabki qadamlar qo'yilmoqda. "Raqqamli O'zbekiston – 2030" strategiyasi doirasida kiberxavfsizlikni ta'minlash va raqqamli infratuzilmani rivojlantirishga alohida e'tibor qaratilmoqda. Quyidagi yo'nalishlar ayniqsa muhim:

Kiberxavfsizlik to'g'risidagi qonunmiz axborot tizimlarini himoya qilish va kiberjinoyatlarga qarshi kurashish uchun huquqiy asoslarni belgilaydi.

Shaxsiy ma'lumotlar to'g'risidagi qonunimiz fuqarolarning shaxsiy ma'lumotlarini himoya qilish va noqonuniy foydalanishning oldini olishga qaratilgan.

Elektron tijorat to'g'risidagi qonunda onlayn platformalarda xavfsiz tranzaksiyalarni ta'minlash uchun normativ baza yaratadi.

Biroq, sun'iy intellektni kiberxavfsizlikda keng miqyosda qo'llash uchun maxsus qonunchilik, masalan, SI algoritmlarining axloqiy me'yorlari va shaffofligini tartibga soluvchi normalar talab etiladi.

Smart shahar loyihalari Toshkent va boshqa yirik shaharlarda videokuzatuv tizimlarida SI'ning yuzni tanish texnologiyasi sinovdan o'tkazilib ishlatib kelinmoqda.

Bank sektorida SI qo'llanilishi: Moliyaviy firibgarliklarni aniqlash uchun ba'zi banklar SI asosidagi tahlil tizimlarini joriy qilmoqda.

Davlat xizmatlari portali: Foydalanuvchilarning xatti-harakatlarini tahlil qilish orqali noqonuniy kirishlarni aniqlash tizimlari sinovdan o'tkazilmoqda.

Sun'iy intellektni kiberxavfsizlikda samarali qo'llash uchun quyidagi muammolarni hal qilish zarur:

Texnik infratuzilmada SI algoritmlarini ishlatish uchun yuqori unumdor serverlar va katta hajmdagi ma'lumotlarni saqlash tizimlari talab qilinadi.

Kadrlar tayyorlashda SI va kiberxavfsizlik sohasida malakali mutaxassislar yetishmasligi jiddiy muammo hisoblanadi.

Axloqiy va huquqiy masalalarda SI tizimlarining shaffofligi va foydalanuvchilarning shaxsiy ma'lumotlarini himoya qilish masalalari hal qilinishi lozim.

Sun'iy intellekt axborot texnologiyalari sohasidagi huquqbuzarliklarga qarshi kurashda inqilobiy yondashuvlarni taqdim etmoqda. Real vaqt rejimida katta hajmdagi ma'lumotlarni tahlil qilish, xavf-xatarlarni aniqlash va oldini olish imkoniyatlari tufayli SI kiberxavfsizlikni ta'minlashda muhim vosita sifatida xizmat qilmoqda. O'zbekiston sharoitida SI'ni huquqni muhofaza qilish organlarining amaliy faoliyatiga tatbiq etish davlat xavfsizligini ta'minlashning muhim omilidir.

Biroq, bu sohada muvaffaqiyatga erishish uchun bir qator choralar ko'rish zarurdir. Qonunchilikni takomillashtirish, xususan, SI algoritmlarining axloqiy me'yorlari va shaffofligini tartibga soluvchi normalarni ishlab chiqish. Texnik infratuzilmani rivojlantirish va SI loyihalarini moliyalashtirishni ko'paytirish.

SI va kiberxavfsizlik sohasida malakali mutaxassislar tayyorlash uchun ta'lim dasturlarini kengaytirish. Xalqaro tajriba va texnologiyalarni o'zlashtirish orqali mahalliy sharoitga moslashtirilgan SI tizimlarini joriy etish. O'zbekistonda sun'iy intellektni kiberxavfsizlik sohasida keng qo'llash nafaqat raqamli iqtisodiyotni rivojlantirishga, balki fuqarolar va davlat manfaatlarini himoya qilishga ham xizmat qiladi. Ushbu yo'nalishdagi islohotlar va investitsiyalar kelajakda mamlakatning global raqamli xavfsizlik tizimidagi o'rnini mustahkamlashga yordam beradi.

Foydalanilgan adabiyotlar ro'yhati:

1. Schneider, B. (2018). Click Here to Kill Everybody: Security and Survival in alanilasi.
2. O'zbekiston Respublikasining "Kiberxavfsizlik to'g'risida"gi Qonuni (2021).
3. Russell, S., & Norvig, P. (2020). Artificial Intelligence: A Modern Approach (4th ed.). Pearson.

MAYNING QURILMALARINING XAVFLARI VA ULARNI ANIQLASH STRATEGIYALARI

Boynazarov Otabek Murot o'g'li

*IIV Malaka oshirish instituti, Axborot texnologiyalari sikli o'qituvchisi
e-mail:boynazarovotabek0712@mail.ru*

Kriptovalyutalarning global miqyosda keng tarqalishi bilan bir qatorda, ularni ishlab chiqarish jarayoni — ya'ni mayning (mining) ham juda tez sur'atlar bilan ommalashmoqda. Mayning – bu blokcheyn tizimida tranzaksiyalarni tasdiqlash va yangi bloklar yaratish uchun maxsus hisoblash quvvatiga ega qurilmalar yordamida amalga oshiriladigan texnik jarayondir. Ayniqsa Bitcoin va boshqa yuqori darajadagi kriptovalyutalarni qazib olish ko'p sonli hisoblash amallarini talab qiladi, bu esa juda katta miqdorda elektr energiyasini sarflashga olib keladi.

Mazkur jarayonning asosiy muammolaridan biri – uning ko'pincha yashirin ravishda, ruxsatsiz yoki nazoratsiz tarzda amalga oshirilishidir. Ko'plab hollarda maynerlar elektr energiyasini noqonuniy ravishda, masalan, davlat yoki korxonalariga tegishli elektr tarmoqlaridan yashirincha foydalanadilar. Bu holat esa nafaqat iqtisodiy zarar keltiradi, balki elektr tarmoqlarida ortiqcha yuklama yuzaga kelishiga sabab bo'ladi. Natijada tarmoqlarda kuchlanish pasayishi, avariya va uzilishlar, hatto yong'in kabi texnik nosozliklar sodir bo'lishi mumkin. Zamonaviy mayning qurilmalari kichik o'lchamli, shovqinsiz va ko'chma bo'lgani sababli, ularni aniqlash tobora qiyinlashmoqda.

Bu holatlar mayning faoliyatini aniqlash va uni tartibga solish bo'yicha texnik va huquqiy choralarni kuchaytirish zaruratini yuzaga keltirmoqda. Ayniqsa, elektr energiyasi taqchilligi yoki energiya ta'minotida uzilishlar yuzaga keladigan hududlarda bu masala jiddiy ahamiyat kasb etadi. Shu sababli, energiya resurslaridan oqilona foydalanish, elektr tarmoqlarini himoya qilish, noqonuniy faoliyatni bartaraf etish va davlat manfaatlarini himoya qilish maqsadida mayning qurilmalarini aniqlash bo'yicha tizimli va zamonaviy yondashuvlar ishlab chiqilmoqda.

Kripto-maynerlar odatda quyidagi qurilmalar yordamida ishlaydi:

- ✓ ASIC (Application-Specific Integrated Circuit) – faqat bitta algoritim (masalan, SHA-256) uchun optimallashtirilgan.
- ✓ GPU (Graphics Processing Unit) – ko'p tarmoqli ishlov berish imkoniyati bilan.
- ✓ FPGA (Field-Programmable Gate Array) – dasturlanadigan va moslashtiriladigan qurilmalar.

Bu qurilmalar kuchli hisoblash imkoniyatiga ega bo‘lib, yuqori harorat, elektr yuklamasi va signal shovqinini yuzaga keltiradi – bu esa ularni aniqlash imkonini beradi.

Eng ko‘p qo‘llaniladigan va ishonchli usul — elektr iste‘moli tahlili:

- ✓ Maynerlar odatda uzluksiz ishlaydi, 24/7 elektr tortadi.
- ✓ Uy yoki bino darajasidagi normadan ortiq energiya iste‘moli aniqlanadi.
- ✓ Smart-meter texnologiyalari (aqlli hisoblagichlar) yordamida vaqt bo‘yicha grafiklar va anomaliyalar tahlil qilinadi.

Issiqlik va ovoz monitoringi

- ✓ ASIC qurilmalar yuqori issiqlik chiqaradi. Termal kameralar yoki infraqizil detektorlar yordamida aniqlash mumkin.
- ✓ Ventilyatorlar kuchli shovqin chiqaradi (50–70 dB). Uydagi nooddiy ovoz signalini aniqlovchi detektorlar yordam beradi.
- ✓ Issiqlik pastki qavatdagi shift yoki devor orqali tarqalishi mumkin – bu issiqlik tarqalish sxemasi orqali ko‘rinadi.

Internet trafik monitoringi

- ✓ Mayning qurilmalari blockchain tarmoqlari bilan uzluksiz bog‘langan bo‘ladi (masalan, Bitcoin tarmog‘i).
- ✓ DNS tahlili orqali mining pool serverlariga ulanayotgan IP-manzillar aniqlanadi.
- ✓ Mahalliy routerlar orqali quyidagi xizmatlarga trafik kuzatiladi: slushpool, f2pool, antpool, nicehash.

Radioto‘lqinlar va elektromagnit tahlil

- ✓ Maynerlar elektromagnit to‘lqinlar chiqaradi.
- ✓ Maxsus qurilmalar bilan RF (radio frequency) spektri tahlil qilinadi.
- ✓ Har xil qurilmalar o‘ziga xos to‘lqin uzatadi, bu orqali identifikatsiya qilish mumkin.

2024–2025 yillar davomida bir qator davlatlarda noqonuniy mayning faoliyatiga qarshi kurash kuchaytirilgan. masalan:

- ✓ O‘zbekistonda 2025 yil boshida Sirdaryo viloyatida aniqlangan noqonuniy kripto-ferma 34,3 milliard so‘mlik elektr energiyasini noqonuniy iste‘mol qilgani ma‘lum bo‘ldi.
- ✓ Malayziyada 2018–2023 yillarda mayning tufayli 723 million AQSh dollariga teng elektr energiyasi o‘g‘irlangan.
- ✓ Kuvaytda 2024 yilda birgina shaharda mayning qurilmalari olib tashlanganidan keyin elektr iste‘moli 55% ga kamaygan.

Qarshi choralar va monitoring tizimlari

<i>Usul</i>	<i>Amaliy yechim</i>
Smart elektr monitoring	IoT asosida ishlovchi aqlli hisoblagichlar o'rnatish
ISP darajasida tahlil	Internet provayderlarining DNS trafik tahlili
Issiqlik skanerlari	Termal kameralardan foydalanish (ko'p qavatli uylarda)
Jamiyatdan xabar olish	Mahalla inspektori va elektr nazoratchilari orqali monitoring

Kriptoalyuta mayningi global raqamli iqtisodiyotning ajralmas qismiga aylangan bo'lsa-da, uning energiya infratuzilmasiga ko'rsatgan salbiy ta'siri tobora kuchaymoqda. Ushbu tadqiqot davomida aniqlanishicha, mayning qurilmalari, ayniqsa ASIC va GPU asosida ishlovchi qurilmalar, katta miqdorda elektr energiyasi sarflaydi va bu holat ko'plab hollarda yashirin yoki noqonuniy shaklda amalga oshirilmoqda. Bunday faoliyat natijasida nafaqat davlat budjetiga zarar yetkaziladi, balki elektr tarmoqlari haddan tashqari yuklanadi, xavfsizlik xavflari yuzaga keladi va ekologik muvozanat buziladi.

Tahlil etilgan aniq holatlar, xususan O'zbekiston, Malayziya va Kuvayt kabi davlatlar misolida ko'rsatadiki, mayning qurilmalarini aniqlash va nazoratga olish masalasi dolzarb ahamiyat kasb etmoqda. Aqlli hisoblagichlar, issiqlik va elektromagnit monitoring, internet trafik tahlili hamda jamoatchilik xabardorligi kabi texnik va ijtimoiy vositalar bu borada samarali natija berayotganini isbotlamoqda.

Foydalanilgan adabiyotlar ro'yhati:

1. J. Kim, S. Lee. Anomaly Detection in Cryptocurrency Mining Activities Using Deep Learning. IEEE Transactions on Information Forensics and Security, vol. 19, pp. 1234-1245. 2024y.
2. R. Patel, Y. Zhang. Smart Grid-Based Detection of Unauthorized Crypto-Mining Devices via Power Consumption Profiling Energy Informatics, vol. 7, art. 12. 2024y.
3. V. Veselý, M. Žádník, How to detect cryptocurrency miners? By traffic forensics! Digital Investigation, 31, 1–14. 2019y. DOI: 10.1016/j.diin.2019.08.002
4. A. Gangwal, S. Piazzetta, G. Lain, M. Conti. Detecting Covert Cryptomining using HPC. 2019y. arXiv preprint arXiv:1909.00268. arXiv:1909.00268

SHAXSIY MA'LUMOTLARNING O'G'IRLANISHI VA ULARNING NOQONUNIY FOYDALANILISHI

Boynazarov Otabek Murot o'g'li

*IIV Malaka oshirish instituti, Axborot texnologiyalari sikli o'qituvchisi
e-mail:boynazarovotabek0712@mail.ru*

Raqamli texnologiyalar rivojlanishi bilan birga shaxsiy ma'lumotlarning xavfsizligi dolzarb muammolardan biriga aylandi. Zamonaviy davrda jinoyatchilar shaxsiy ma'lumotlarni o'g'irlash va ularni noqonuniy ishlatish uchun turli usullardan foydalanmoqdalar. Ushbu tezisda shaxsiy ma'lumotlarni o'g'irlash usullari, ulardan noqonuniy foydalanish yo'llari va bu holatlarning huquqiy oqibatlarini tahlil qilinadi.

Shaxsiy ma'lumotlarni qo'lga kiritishda phishing keng tarqalgan usul hisoblanadi. Uning email phishing, spear phishing va vishing kabi shakllari mavjud bo'lib, ularning har biri ma'lum maqsadli foydalanuvchilarga qaratilgan. Jinoyatchilar ishonchli ko'rinishga ega xabarlar orqali foydalanuvchilarning login, parol, karta ma'lumotlarini qo'lga kiritadilar.

Bundan tashqari, ijtimoiy muhandislik (social engineering) usuli ham keng qo'llaniladi. Bu usulda jinoyatchi odamlarning psixologik zaifliklaridan foydalanadi: telefon orqali yolg'on ma'lumotlar berish, tanishlar nomidan so'rov yuborish yoki ijtimoiy tarmoqlar orqali ishonch qozonish orqali shaxsiy ma'lumotlarni yig'adi.

Zararli dasturlar – malware va ransomware – orqali ham ma'lumotlar o'g'irlanadi. Malware foydalanuvchi kompyuteriga yashirin tarzda o'rnatib, shaxsiy fayllarni, login va parollarni yig'adi. Ransomware esa kompyuter fayllarini shifrlab, ularni ochish evaziga foydalanuvchidan pul talab qiladi. Yirik korporatsiyalar tizimlaridagi zaifliklar orqali amalga oshiriladigan ma'lumot buzilishlari (data breach) natijasida millionlab foydalanuvchilarning ma'lumotlari o'g'irlanadi. Bunday ma'lumotlar ko'pincha qora bozorlarda (dark web) sotuvga qo'yiladi.

O'g'irlangan shaxsiy ma'lumotlar quyidagi maqsadlarda noqonuniy ishlatiladi:

- ✓ Bank firibgarligi – hisob raqamlaridan pul o'g'irlash, soxta kreditlar olish;
- ✓ Identifikatsiya o'g'irligi – boshqa shaxs nomidan hujjatlar tayyorlash, moliyaviy xizmatlardan foydalanish;
- ✓ Shantaj – nozik yoki shaxsiy ma'lumotlarni oshkor qilish tahdidi orqali foyda ko'rish;
- ✓ Kiberhujumlar – DDoS hujumlar yoki tizimlarga zarar yetkazish maqsadida.

Shuningdek, shaxsiy ma'lumotlarning noqonuniy savdosi orqali jinoyatchilar katta miqdorda daromad olishmoqda. Ular kredit kartasi raqamlari, ijtimoiy xavfsizlik raqamlari, login va parollarni dark web orqali sotishadi.

Bu kabi jinoyatlarning huquqiy oqibatlari jiddiydir. Shaxsiy ma'lumotlarni noqonuniy egallash va tarqatish ko'plab davlatlarda jinoiy javobgarlikka sabab bo'ladi. Masalan, Yevropa Ittifoqida GDPR qonuni orqali bunday holatlar qat'iy nazorat qilinadi.

Shaxsiy ma'lumotlarni o'g'irlash va undan foydalanish bo'yicha statistik jadval

№	Yo'nalish	Statistika / Fakt	Manba (yil)
1	Global kiberjinoyatlar zarari	2025-yilda yillik zarar 10,5 trillion dollar	DeepStrike (2025)
2	O'rtacha ma'lumot buzilishi zarari	Dunyo bo'yicha: 4,88 mln \$, AQShda: 9,36 mln \$	DeepStrike (2025)
3	Phishing email soni (kunlik)	3,4 milliard email yuboriladi	TechMagic (2024)
4	Credential theft o'sishi	2025-yilda 160% ga oshdi	ITPro (2025)
5	Malware hujumlari manbai	Malware hujumlarining 94% phishing orqali boshlanadi	TechMagic (2024)
6	AI yordamida phishing	AI-phishing hujumlari 4000% ga oshdi	DeepStrike (2025)
7	Identifikatsiya o'g'irligi zarari (AQSh)	2022-yilda 56 mlrd \$, har bir jabrdiyda o'rtacha 1107 \$ zarar	Market.us (2023)
8	Ma'lumotlar buzilishi holatlari	AQShda 2024-yilda 859 532 ta shikoyat , 16 mlrd \$ zarar	IC3 / FBI (2024)

Shaxsiy ma'lumotlarning o'g'irlanishi zamonaviy kiberxavfsizlik muammosining markazida turgan holatdir. Uning oldini olish uchun texnik vositalar bilan birga foydalanuvchilarning bilim va ogohliligi ham muhim ahamiyatga ega. Har bir foydalanuvchi o'zining shaxsiy ma'lumotlarini himoya qilish uchun zarur choralarni ko'rishi lozim.

Foydalanilgan adabiyotlar ro'yhati:

1. A. Karimov, Z. Islomov. Shaxsiy ma'lumotlarni himoya qilish va kiberxavfsizlik. Toshkent Axborot Texnologiyalari Jurnal, vol. 12, pp. 45-58. 2023y.
2. Markuson, N. AI and Cybercrime: How Artificial Intelligence is Changing Digital Threats, 2025.

INSAYDER TAHDIDLARNI ANIQLASHDA TANLANMANI SHAKLLANTIRISH VA AVTOMATIK SINFLASHTIRISH

Muhammadiyev Firdavs Rudaki o'g'li

Mirzo Ulug'bek nomidagi O'zbekiston Milliy universiteti Axborot xavfsizligi kafedrasida o'qituvchisi

Kiberxavfsizlikda ichki tahdidlar, ayniqsa insayder tahdidlar tashkilotlar axborotlarini jiddiy xavf ostiga qo'yadi. IBM Security Intelligence ma'lumotlariga ko'ra, kiberjinoyatlarning deyarli 60% insayderlar bilan bog'liq. Ushbu tezisda aynan insayder tahdidlarini aniqlashda sun'iy intellekt modellarini o'qitish uchun tanlanmani shakllantirish bosqichlari chuqur tahlil qilinadi.

Tadqiqotda tanlanmani shakllantirish uchun manbalarini (Windows Event Logs, NTFS loglari va boshqalar) aniqlash, zarur atributlarni tanlash, ma'lumotlarni to'plash, tozalash va normallashtirish bosqichlari bajarildi. Xususan, foydalanuvchilarning fayllar ustidagi harakatlari (yaratish, o'chirish, nusxalash, ochish va h.k.) raqamli shaklda ifodalaniib, ma'lumotlar tanlanmasi tuzildi. Shundan so'ng, tanlanma Z-Score, Isolation Forest, One-Class SVM va LOF kabi intellektual algoritmlari asosida anomaliyalarni aniqlash amalga oshirildi. Tadqiqotda 2632 ta holatdan to'rt algoritm bo'yicha quyidagi miqdorda anomaliyalar aniqlandi (1-jadval):

1-jadval.

Metod	Anomaliya soni	Ulushi (%)
Isolation Forest	182	7.94%
LOF	242	10.56%
One-Class SVM	387	16.88%
Z-Score	374	16.32%

Har bir algoritm bo'yicha aniqlangan anomaliyalar o'zaro taqqoslandi. Tahlil natijalariga ko'ra, turli algoritmlarning birgalikdagi ishlatilishi yuqori aniqlikda ishonchli anomal holatlarni aniqlash imkonini beradi.

Ayniqsa, LOF va Z-Score usullari orasida kuchli moslik kuzatildi. 149 ta holat kamida uchta metod tomonidan birgalikda anomaliya deb baholangan bo‘lib, ular ishonchli anomaliya sifatida tasniflandi (2-jadval).

2-jadval.

Metodlar kombinatsiyasi	Mos kelgan holatlar soni
Isolation Forest & LOF	85
Isolation Forest & SVM	79
Isolation Forest & Z-Score	152
LOF & SVM	102
LOF & Z-Score	159
SVM & Z-Score	155

Bunday yondashuv ansambl yondashuvi orqali aniqlikni oshirish imkonini yaratadi. Aniqlikni oshirish uchun tanlanmadagi holatlarni ekspert tomonidan tekshirish orqali sinflarga ajratish mumkin. Bu orqali tanlanmani ikkita anomal yoki normal sinfga ajratsa bo‘ladi. Natijada intellektual modellarni o‘qitish imkoni paydo bo‘ladi. Jadvaldan ko‘rish mumkinki, turli usullar orasida moslik farqlari mavjud bo‘lsa-da, ba’zi holatlar 3 yoki 4 algoritm tomonidan bir ovozdan anomaliya sifatida baholangan (3-jadval). Bu esa tanlangan yondashuvning ishonchliligini oshiradi.

3-jadval.

Metodlar soni bilan moslik	Holatlar soni	Ulushi (%)
0 ta metod tomonidan	1618	70.59%
1 ta metod tomonidan	348	15.18%
2 ta metod tomonidan	177	7.72%
3 ta metod tomonidan	113	4.93%
4 ta metod tomonidan	36	1.57%

Ushbu tadqiqot sun‘iy intellekt asosidagi insayder tahdidlarni aniqlovchi tizimlar uchun tanlanma shakllantirishning muhimligini ko‘rsatadi. To‘g‘ri tanlanma modelning aniqligini belgilaydi va DLP hamda UEBA tizimlarida intellektual algoritmlarni muvaffaqiyatli joriy etishga asos bo‘ladi.

Foydalanilgan adabiyotlar ro‘yhati:

1. <https://securityintelligence.com/articles/83-percent-organizations-reported-insider-threats-2024>.

2. G‘.U.Jurayev, R.X. Alaev, O.N. Bozorov, F.R. Muhammadiyev “Konfidensial ma’lumotlarning sizib chiqishini bartaraf etishga mo‘ljallangan dasturiy mahsulotlarning tahlili”, Scientific-technical journal (STJ FerPI, ФapIII ИТЖ, ИТЖ ФерПИ, 2023, Т.27, №2).

3. F.R. Muhammadiyev “DLP tizimlarida insayderlarni anomal holatlar orqali aniqlashning algoritmi tahlili” International scientific and technical conference “digital technologies: problems and solutions of practical implementation in the spheres” 2023 yil.

4. F.R. Muhammadiyev “Kompyuter tizimlarida konfidentsial ma'lumotlarning sizib chiqish kanallarini nazorat qilish modeli va algoritmi”. МУҲАММАД АЛ-ХОРАЗМИЙ АВЛОДЛАРИ Илмий-амалий ва ахборот-таҳлилий журнал 4/2023.

АНАЛИЗ ЦИФРОВЫХ СЛЕДОВ В СОЦИАЛЬНЫХ СЕТЯХ (МЕТОДЫ, ИНСТРУМЕНТЫ И ПЕРСПЕКТИВЫ)

Ш.А. Холиков

Главный научный сотрудник УОБ РУ

Аннотация. Цифровые следы, оставляемые пользователями в социальных сетях, представляют собой важный источник информации для анализа поведения, выявления угроз и проведения расследований. В статье рассматриваются виды цифровых следов, методы их извлечения и интерпретации, а также области применения анализа, включая профайлинг, цифровую криминалистику и информационную безопасность. Особое внимание уделено этическим и правовым аспектам, связанным с анализом пользовательских данных.

Ключевые слова: цифровые следы, социальные сети, профайлинг, криминалистика, искусственный интеллект, OSINT, анализ поведения.

Социальные сети стали неотъемлемой частью современной цифровой коммуникации. Миллиарды пользователей ежедневно публикуют информацию, вступают во взаимодействия, проявляют активность, оставляя после себя множество цифровых следов. Эти следы представляют огромную ценность не только для маркетинга и аналитики, но и для криминалистических и правовых целей — от расследования киберпреступлений до оценки угроз информационной безопасности.

Современные социальные сети стали неотъемлемой частью жизни миллиардов людей. Каждое действие пользователя — публикация, лайк, комментарий, переход по ссылке — оставляет цифровой след. Эти данные представляют огромную ценность для бизнеса, государственных структур, исследователей и киберпреступников. Анализ цифровых следов позволяет выявлять интересы аудитории, прогнозировать поведение, предотвращать мошенничество и даже раскрывать преступления.

Цифровые следы можно разделить на несколько категорий. Текстовый контент включает посты, сообщения и комментарии, которые раскрывают мысли и предпочтения пользователей. Мультимедийные данные — фотографии, видео и аудио — несут информацию о визуальных предпочтениях и местах посещения. Метаданные, такие как время активности, геолокация и технические параметры устройства, помогают установить поведенческие паттерны. Социальные взаимодействия — друзья, подписки, репосты — формируют карту связей между людьми.

Для анализа этих данных применяются различные методы. Текстовый анализ включает sentiment-анализ для определения эмоциональной окраски сообщений и тематическое моделирование для выявления ключевых тем обсуждений. Сетевой анализ изучает связи между пользователями, выявляя влиятельных участников и скрытые сообщества. Компьютерное зрение и аудиоанализ помогают распознавать объекты на изображениях и идентифицировать голос. Поведенческий анализ отслеживает активность пользователей, предсказывая их дальнейшие действия.

Понятие и классификация цифровых следов

Цифровые следы — это отражение нашей онлайн-жизни, и их анализ открывает новые горизонты в маркетинге, безопасности и социологии. Но вместе с мощными инструментами приходит ответственность за их использование. Баланс между технологическим прогрессом и защитой приватности станет главным вызовом в этой области. В социальных сетях их можно классифицировать на следующие категории:

Явные (активные) следы: публикации, лайки, комментарии, репосты, фото и видео.

Неявные (пассивные) следы: логи активности, метаданные (время входа, геолокация, тип устройства), история просмотра и переходов.

Поведенческие следы: частота активности, лексика, стиль общения, структура социальных связей.

Методы анализа цифровых следов

Анализ цифровых следов включает в себя следующие методы:

1. Сбор и извлечение данных

- Web scraping: автоматизированный сбор открытых данных (с соблюдением закона).
- OSINT-инструменты: Maltego, Spiderfoot, SocialLinks, Sherlock.
- API-платформы: Twitter API, Facebook Graph API, Telegram Bot API.

2. Обработка и структурирование

- ✓ Предобработка текста (очистка, нормализация, лемматизация).

- ✓ Выделение сущностей (NER), временных меток и геоданных.
- ✓ Построение графов социальных связей.

3. Анализ и интерпретация

- Контент-анализ: темы, тональность, эмоциональный окрас публикаций.
- Сетевой анализ: выявление центров влияния, бот-сетей, подозрительных кластеров.
- Профайлинг: построение цифрового портрета личности по поведенческим данным.
- ML/AI: классификация (бот/человек), прогнозирование поведения, выявление аномалий.

Области применения анализа цифровых следов

а. Криминалистика и расследования

Установление личности и социальных связей подозреваемых.

Анализ активности до, во время и после преступления.

Идентификация фейковых аккаунтов и координированной дезинформации.

б. Информационная безопасность

Мониторинг угроз (кибербуллинг, радикализация, утечки данных).

Выявление фишинговых и мошеннических кампаний в соцсетях.

с. Профайлинг и HR-аналитика

Оценка цифрового имиджа соискателей при приёме на работу.

Идентификация рисков токсичного поведения в команде.

д. Маркетинг и социология

Сегментация аудитории и персонализация рекламы.

Изучение общественного мнения и социальных трендов.

Существует множество инструментов для работы с цифровыми следами.

Программные библиотеки на Python, такие как NLTK и spaCy, используются для обработки текста, а Scikit-learn и TensorFlow — для машинного обучения.

Социальные графы анализируют с помощью NetworkX и Gephi. Для мониторинга упоминаний брендов применяются платформы вроде Brandwatch, а расследование связей между аккаунтами проводят в Maltego. API социальных сетей, таких как Twitter и VK, предоставляют легальный доступ к данным, но с ограничениями.

Технологии и инструменты

1. Аналитические платформы

- Maltego – визуальный анализ связей.
- SocialNet – выявление бот-сетей и подозрительных аккаунтов.
- Creepy, Lampyre – геолокационный и метаданный анализ.

2. ИИ и машинное обучение

- NLP-модели (BERT, RoBERTa, ChatGPT) — анализ текстов и тональности.
- Graph ML — анализ социальных графов.
- Deep learning — обнаружение фейков и deepfake-контента.

Перспективы анализа цифровых следов связаны с развитием искусственного интеллекта и больших данных. Глубокое обучение улучшает точность распознавания текста и изображений, а алгоритмы прогнозирования становятся более надежными. Однако рост возможностей анализа вызывает вопросы о приватности и этике. Регулирование сбора данных, методы анонимизации и прозрачность алгоритмов будут играть ключевую роль в будущем.

Заключение: Анализ цифровых следов в социальных сетях представляет собой важный и быстро развивающийся инструмент как для правоохранительных органов, так и для исследователей в области ИБ и социологии. Однако его использование требует соблюдения правовых и этических норм, а также критического подхода к получаемым данным. Будущее анализа цифровых следов связано с развитием ИИ, автоматизации и повышением уровня защищённости цифровых идентичностей.

Важно различать анализ открытых и закрытых данных и строго соблюдать правовые рамки, особенно в уголовно-процессуальных контекстах.

Использованные лигатуры:

1. Бойд Д., Кроуфорд К. «Критические вопросы для Big Data» // Information, Communication & Society. – Анализирует этические и методологические аспекты работы с цифровыми следами. 2012
2. Майер-Шёнбергер В., Кукьер К. Большие данные: Революция, которая изменит то, как мы живем, работаем и мыслим. – Обзор возможностей анализа цифровых данных, включая социальные сети. 2013
3. Зубов А.В., Коротенко Ю.А. «Методы анализа социальных медиа для выявления цифровых следов» // Информационные технологии и безопасность. – Описывает современные подходы к сбору и анализу данных из соцсетей. 2020
4. Grimmer J., Stewart B.M. «Text as Data: The Promise and Pitfalls of Automatic Content Analysis Methods» // Political Analysis. – Методология автоматического анализа текстовых цифровых следов. 2013
5. Russell M.A. Mining the Social Web (3rd ed.). O'Reilly. – Практическое руководство по извлечению и анализу данных из социальных платформ с использованием Python. 2019

6. Rogers R. Doing Digital Methods. SAGE Publications. – Методология исследования цифровых следов с критическим подходом. 2019

7. Воронцов К.В. Машинное обучение и анализ данных. – Учебное пособие по методам машинного обучения для обработки цифровых следов. 2018

ANALYSIS OF THE USE OF MODERN GAME BASED TECHNOLOGY IN THE STUDYING PROCESS

Tursunova Maftuna Bekhmurod qizi

*Assistant teacher of the Department of "Information Technologies" of the
Renaissance Educational university maftuna-27-97@mail.ru*

Abstract. A modern school deals with a generation of students who were born and grown up in a digital environment and require other teaching methods. Developing mass media is of social importance in our society. This article discusses the issues of using modern game based technologies in the educational process.

Key words: modern technologies, educational process, interactive games, mobile application, web-sites, Kahoot, Quizziz, Quizlet Live

The human mind is developing so much that the process of technization and computerization boldly penetrates not only into various spheres of production, but also into the spheres of culture and education. The rapid development of computer technology has brought the educational process to a new level. This, in turn, emphasizes the need for further enrichment of the content, methods and forms of training with new knowledge and skills.

Currently, educational institutions are working on such topical issues as the creation of scientific foundations for new pedagogical technologies, their classification, and the determination of methodological significance. New pedagogical technologies imply the computerization of education, as well as traditional and non-traditional methods. In this sense, the growing computer culture of information creates new relationships in the transmission and reception of information, creates a new type of thinking.

Most commonly used in schools are Kahoot, Quizziz, and Quizlet Live, which provide students with a fun and interactive way to explore their material. All three platforms have their own distinct capabilities that provide a useful path for students to take a lesson. The teacher can create and edit their own games for their students. All three have their advantages and disadvantages when it comes to learning environments.

Kahoot was one of the original online games where teachers and students could study school materials. The teacher directs and creates each question, and the students answer them as shown on the screen. It's more animated than Quizziz and Quizlet Live, with vibrant colors on the screen and fun music that encourages students to respond quickly to all questions. Players have a lead table based on speed and accuracy, but its fast-paced music may not help with accuracy either, as they want to respond quickly. Main achievements in this game:

- Possibility to answer at the same time;
- There are free templates, with these templates you can choose the type of question you want;
- The program is very easy to learn and does not require much time to learn;

Now let's look at the shortcomings of this game:

- The game depends on the speed of the Internet, in which some students may be left behind;
- It is easy for students to see and copy each other's answers;

Here are some features of this game:

- Ghost mode. Each student remembers how he wrote each question. When you play the game again in ghost mode, previous attempts are shown as "ghosts". Students can compare their current efforts with previous ones and see how they have evolved.
- Mobile app. This versatile app lets you create Kahoot.
- Friendly nickname generator. The generator allows students to choose one of three suitable nickname options.

Quizziz has also become a staple for teachers in their classrooms. It's almost the same as Kahoot, except that students can read selected items on their devices. Like Kahoot, Quizziz puts students at the forefront. The game isn't as lively or musical as Kahoot, but it does give students a good starting point to see their improvements. Main achievements in the game:

- It's student speed. No one will be disappointed because their device doesn't load the game fast enough to compete.
- Teachers can display the Student Achievements Dashboard on the projector to see each student's progress and see at a glance how many questions were answered correctly/incorrectly by the class.

And now let's look at the shortcomings of the game:

- If everyone answers different questions at different times, you will lose some excitement.
- Unlike Kahoot, students are asked a different order of questions, which, in turn, may seem boring.

Peculiarities:

Mememes. These funny message pictures are a real treat. They are displayed after answering a question to show if they are right or wrong. Quizizz even lets you create your own. You can use their preloaded images or upload your own. Homework mode. Students do not have to play live. You can use the homework mode to set the set time.

Add audio, images, and math equations. When creating a new question, use the icons next to the question you are writing. Math button loads a math symbolic keyboard. The Media button allows you to upload an audio or image.

Quizlet Live is more focused on dictionaries than other gaming platforms. Students are invited from their places to randomly organized teams that have the opportunity to interact with other students to win the game. Each team player is given a set of words that matches the description, and all teams try to answer all the words listed first. However, Quizlet Live isn't very useful for grammar or other types of non-vocabulary questions. Achievements for this game:

- Teamwork and communication.
- Every time a new game.

And now let's look at the shortcomings of the game:

- To play you will need at least six students (two teams of at least three students) and at least six cards in a set of cards.

Peculiarities:

- Real team game. This is the best way to collaborate in a game demonstration class. One student can dominate the Kahoot team game or a quiz. If each student has more than one correct answer, everyone will have more opportunities to participate.

- Built-in mechanism. Students are divided into small groups and encouraged to work with their partners. It stimulates physical movement by mixing the environment, which improves cognitive function.

In a recent FVHS student poll, Kahoot came out on top with 50% of the votes for his passion and speed, which seems to improve the learning experience. About 42% of students chose to use Quizizz. Many people like the lightness, ease and the ability to take the test at their own pace. The rest (8%) preferred Quizlet Live.

Quizizz, Kahoot, and Quizlet Live are useful, interactive, and fun ways to explore or analyze any concept, each with its own advantages and disadvantages. All three search functions allow you to find and edit games already created by others.

RAQAMLI DUNYONING ASOSI KIBERXAVFSIZLIK MUHOFAZASINING (HACKZONE) AHAMIYATI

Saatova Lolakhon Ergashevna, i.f.f.d.(PhD), dotsent.

O'zbekiston Respublikasi Harbiy aviatsiya institute Axborot texnologiyalari kafedrası professori, Qarshi shahar, e-mail: lola.saatova@mail.ru

Annotatsiya. Ushbu maqolada raqamli dunyoning asosi kiberxavfsizlik muhofazasining (hackzone) ahamiyati haqida so‘z yuritilgan. Kiberxavfsizlikning asosiy turlari va asosiy tahdidlari keng yoritilgan. Shu hihdek, bugungi kunda hackzone ishga tushirilishining asosiy sabablari to‘g‘risida fikr yuritilgan.

Kalit so‘zlar: raqamli dunyo, kiberxavfsizlik, kiberxavfsizlik muhofazasi, AKT, kiberxavfsizlik tahdidlari, internet, kompyuter tizimlari, xavf-xatarlari, raqamli texnologiyalar sektor.

ОСНОВА ЦИФРОВОГО МИРА ВАЖНОСТЬ ЗАЩИТЫ КИБЕРБЕЗОПАСНОСТИ (HACKZONE)

Аннотация. В этой статье говорится о важности защиты кибербезопасности (хакерской зоны), основе цифрового мира, широко освещены основные виды кибербезопасности и основные угрозы.

Ключевые слова: цифровой мир, кибербезопасность, защита кибербезопасности, ИКТ, угрозы кибербезопасности, Интернет, компьютерные системы, риски, сектор цифровых технологий.

Bugungi kunda zamonaviy dunyoda yangi texnologiyalar, elektron xizmatlar bizning kundalik hayotimizning ajralmas qismiga aylandi. Jamiyat kundan-kun axborot-kommunikatsiya texnologiyalariga tobora ko‘proq qaram bo‘lib borayotganligini hisobga olib, ushbu texnologiyalarni himoya qilish va ulardan foydalanish milliy manfaatlar uchun hal qiluvchi ahamiyatga ega va juda muhim mavzuga aylanmoqda.

Davlatimiz rahbari tomonidan qabul qilingan me‘yoriy hujjatlarda ham o‘z aksini ko‘rsatmoqda. Xususan, 2018 yil 21 noyabrda PQ- 4024- sonli O‘zbekiston Respublikasi Prezidentining “Axborot texnologiyalari va kommunikatsiyalarining joriy etilishini nazorat qilish, ularni himoya qilish tizimini takomillashtirish chora-tadbirlari to‘g‘risida”gi qarori buning yaqqol dalilidir.[1]

Bugungi kunda axborot jamiyatini rivojlantirishning zaruriy sharti bu kiberxavfsizlikdir, uni xavfsizlikning texnik va qonunchilikgacha bo‘lgan deyarli cheksiz ro‘yxati va ularni hal qilish yo‘li bilan ta‘minlash mumkin. kiberxavfsizlik masalalari alohida kompyuter vositasida axborot xavfsizligi darajasidan har bir davlatning axborot va milliy xavfsizligining ajralmas qismi sifatida yagona kiberxavfsizlik tizimini yaratish darajasigacha boradi. Shu

sababli, har bir tashkilot uchun kiberxavfsizlikni ta'minlash maqsadida mazkur soha bilan shug'ullanuvchi xodimlar jalb qilinmoqda va xodimlarni kiberxavfsizlikka oid bilimlar bilan doimiy tanishtirib boorish uchunqator seminar treyning mashg'ulotlari tashkil etilmoqda. Oliy ta'lim muassasalarida ham kiberxavfsizlikni fan sifatida o'tilishi buning yaqqol misolidir.

Shu o'rinda, kiberxavfsizlik — bu kompyuter tizimlari, tarmoqlar, dasturlar va ma'lumotlarni turli xavf-xatarlardan, shu jumladan, zararli hujumlar, noqonuniy kirish, axborot yo'qolishi, va tizimlarning buzilishidan himoya qilishga qaratilgan muhim sohani anglatadi. Internetning tarqalishi va raqamli texnologiyalarning kengayishi bilan, kiberxavfsizlik jahon miqyosida yirik muammo va talabga aylangan. Har bir tashkilot va shaxs, ma'lumotlarini va tizimlarini himoya qilish uchun samarali kiberxavfsizlik choralarini ko'rishlari zarur[2].

Asosiy qism. Kiberxavfsizlikning bir necha turlari mavjud bo'lib, quyida kiberxavfsizlikning asosiy turlari keltirilgan[4]:

Tarmoq xavfsizligi: Tarmoq xavfsizligi, kompyuter tarmoqlarini zararli hujumlardan, kirishdan yoki kiberxavfsizlik tahdidlaridan himoya qilishga qaratilgan. Bunga firewalllar, tarmoq monitoringi, tarmoqni shifrlash, va boshqa himoya mexanizmlari kiradi.

Axborot xavfsizligi: Axborot xavfsizligi ma'lumotlarning maxfiyligini, yaxlitligini va mavjudligini ta'minlashga yo'naltirilgan. Shifrlash, autentifikatsiya, ruxsatlar va ma'lumotlar zaxirasini yaratish kabi amaliyotlar bu sohada muhim rol o'ynaydi.

Ilova xavfsizligi: Dasturlarni ishlab chiqish jarayonida xavfsizligini ta'minlash va ularda aniqlangan xatoliklar (vulnerability) orqali kiberhujumlardan himoya qilish. Bu, xususan, veb-ilovalar va mobil ilovalar uchun muhimdir.

Operatsion tizimlar xavfsizligi: Operatsion tizimlarning, xususan, Windows, Linux, va macOS tizimlarining himoyasini ta'minlash. Bu, tizimni zararli dasturlardan, troyanlardan, va rootkitlardan himoya qilishni o'z ichiga oladi.

Mobil xavfsizlik: Mobil qurilmalarda, masalan, smartfonlar va planshetlarda ma'lumotlarni himoya qilish va zararli dasturlardan himoya qilish. Mobil xavfsizlik, shuningdek, mobil ilovalar xavfsizligini o'z ichiga oladi.

Cloud xavfsizligi: Bulutli tizimlarda (cloud computing) saqlanayotgan ma'lumotlar va resurslarni himoya qilish. Bulutdagi xizmatlar va infratuzilmalarga kirishni va ma'lumotlarni shifrlashni ta'minlash muhimdir.

Yuqorida kiberxavfsizlikning turlari haqida so'z yuritar ekanmiz, kiberxavfsizlikning asosiy tahdidlar haqida to'xtalib o'tish joizdir. Kiberxavfsizlikni buzish uchun bir nechta xatarlar mavjud. Bular quyidagi shakllarda bo'lishi mumkin[3]:

Zararli dasturlar (Malware): Zararli dasturlar, kompyuter tizimlariga zarar yetkazish yoki ma'lumotlarni o'g'irlash uchun ishlatiladi. Bunga viruslar, troyanlar, ransomware (yoki "qirolik dasturi") va boshqalar kiradi.

Ransomware: Ransomware tizimni shifrlab, foydalanuvchidan ma'lumotni qaytarib olish uchun pul talab qiladi. Bu hujumlar odatda tizimlarga zarar yetkazadi va moliyaviy zarar keltiradi.

Phishing (uydirma hujumlar): Phishing xujumlari foydalanuvchilarga o'zlarini ishonchli manba sifatida ko'rsatib, shaxsiy ma'lumotlarini yoki login ma'lumotlarini o'g'irlashga harakat qiladi. Bunday hujumlar, odatda, elektron pochta orqali amalga oshiriladi.

Denial of Service (DoS) hujumlari: DoS va DDoS (Distributed Denial of Service) hujumlari tizimga yoki veb-saytga ortiqcha yuk tashlash orqali, uning ishlashini blokirovka qiladi, shunday qilib u foydalanuvchilarga xizmat ko'rsatish imkoniyatidan mahrum bo'ladi.

SQL Injection: SQL injection hujumlari, veb-saytning ma'lumotlar bazasiga o'zgartirishlar kiritish yoki ma'lumotlarni o'g'irlash uchun ishlatiladi. Bu turdagi hujumlar veb-illovalar xavfsizligini buzadi.

Man-in-the-Middle (MITM) hujumlari: MITM hujumlarida hujumchi ikki tomonlama aloqa orasiga kirib, ma'lumotlarni o'g'iraydi yoki o'zgartiradi. Bu hujum odatda internetda ma'lumotlarni yuborish va qabul qilishda yuzaga keladi.

Zero-Day xatoliklari: Zero-day xatoliklari — bu dastur yoki tizimdagi yetishmovchiliklar bo'lib, ular hali ishlab chiquvchilar tomonidan tuzatilmagan bo'ladi. Zero-day hujumlari tezda tizimni buzishi mumkin.

Quyida kiberxavfsizlikni ta'minlashning asosiy usullari keltirib o'tilgan:

Xavfsizlikni monitoring qilish: Tizimni doimiy ravishda monitoring qilish orqali, kiberhujumlar va tizimdagi zaif joylarni tezda aniqlash mumkin. Bu uchun tarmoqni kuzatish, log fayllarini tahlil qilish va xavfsizlik protokollarini joriy etish zarur.

Shifrlash: Ma'lumotlarni shifrlash — bu kiberhujumlardan himoya qilishning eng samarali usullaridan biridir. Shifrlash ma'lumotlarni faqatgina ishonchli manbalar bilan o'qish imkonini beradi, shu bilan ularning o'g'irlanishini oldini oladi.

Autentifikatsiya va avtorizatsiya: Foydalanuvchi tizimga kirishdan oldin autentifikatsiyadan o'tishi va faqat kerakli huquqlarga ega bo'lishi lozim. Ikki bosqichli autentifikatsiya (2FA) ham xavfsizlikni oshirishda muhim ahamiyatga ega.

Xavfsizlikni yangilab turish: Tizimlar va dasturlarni muntazam yangilab turish, ular orasidagi zaif joylarni yopish va kiberhujumlardan himoya qilish

imkonini beradi. Bu antivirus dasturlari va xavfsizlik yamoqlarini o'z vaqtida o'rnatish kerakligini anglatadi.

Xodimlarni xavfsizlikka o'rgatish: Kiberhujumlarga qarshi kurashishda foydalanuvchilarning xabardorligini oshirish juda muhim. Bunga xodimlarga phishing hujumlarini aniqlash va kuchli parollar yaratish bo'yicha treninglar o'tkazish kiradi.

Resurslarni ajratish va himoya qilish: Tizimdagi barcha resurslarni himoya qilish uchun ularni ajratib, o'zaro izolyatsiya qilish muhim. Bu orqali tizimga kirishni faqat zarur hollarda ruxsat berish mumkin[5].

Shuni ta'kidlash mumkinki, kiberxavfsizlik nafaqat texnologiya sohasida, balki butun jamiyatda jiddiy e'tibor talab etadigan soha bo'lib qolmoqda. Shu sababli, kiberxavfsizlikni o'rganish va unga doir yangi usullarni ishlab chiqish zarur. Kiberxavfsizlik mutaxassislari, yoki etikal xakerlar, Internetda xavfsizlikni ta'minlash, tizimlarni sinash va hujumlar oldini olishga yordam berish uchun o'z bilim va ko'nikmalarini doimiy ravishda yangilab turishlari kerak.

Shu sababli HackZone - Kiberxavfsizlik va Etikal xakerlikni o'rganish platformasining ishga tushirilish lozim.

HackZone — bu kiberxavfsizlik va etik xakerlikni o'rganish uchun mo'ljallangan innovatsion platforma bo'lib, u onlayn ta'lim, amaliy mashg'ulotlar va kiberhujumlarni oldini olish bo'yicha o'quv materiallarini taqdim etadi. HackZone, xususan, yangi boshlovchilar va tajribali xavfsizlik mutaxassislari uchun yuqori sifatli va amaliy ma'lumotlarni taqdim etadi. U 2023-yilning oxirida o'z faoliyatini boshlagan va kiberxavfsizlik sohasida o'rganishni istagan har bir inson uchun imkoniyatlar yaratadi[3].

HackZone ishga tushirilishining asosiy sabablari mavjud bo'lib, HackZone platformasining ishga tushirilishi bir nechta omillar bilan bog'liq:

Kiber xavfsizlikning muhimligi: Internetda va raqamli dunyoda texnologiyalar va tizimlar tobora rivojlanib, yangi xavflar yuzaga kelmoqda. Kiberhujumlar, axborot o'g'irlash, tarmoq buzilishlari kabi tahdidlar bilan kurashish uchun maxsus bilim va ko'nikmalar kerak. HackZone ushbu muammolarga yechim topish va xavfsizlikni ta'minlash uchun ta'lim imkoniyatlarini yaratishga intiladi.

Etikal xakerlikni rivojlantirish: Etikal xakerlik, ya'ni tizimlar va tarmoqlarni o'rganish va buzish usullarini ishlatish orqali ularni yaxshilash, kiberxavfsizlik sohasida muhim rol o'ynaydi. HackZone platformasi etik xakerlikni o'rganish, ularning faoliyatini to'g'ri yo'naltirish va xavfsizlikni oshirish uchun imkoniyat yaratadi.

Interaktiv ta'lim: HackZone interaktiv va amaliy mashg'ulotlar, tarmoq sinovlari, va real dunyo kiberhujumlariga qarshi kurashish uchun laboratoriyalarni

taklif etadi. Bu, o'quvchilarga o'z bilimlarini real sharoitlarda sinab ko'rishga imkon beradi.

HackZone platformasi o'quvchilarga bir qator ta'lim bo'limlarini taqdim etadi, ularning har biri kiberxavfsizlikning muhim jihatlarini o'z ichiga oladi:

Tarmoq xavfsizligi: Tarmoqni himoya qilish, tarmoq monitoringi va DDoS hujumlariga qarshi kurashish bo'yicha o'quv materiallari.

Penetratsion testlash: Tizimlarga kirish va ularni sinash usullarini o'rganish. HackZone foydalanuvchilari veb-saytlar, tizimlar va dasturlarni zaifliklar bo'yicha tekshirishda ishtirok etishadi.

Phishing va Social Engineering: Phishing hujumlari va ijtimoiy muhandislik (social engineering) usullarini aniqlash va ularni oldini olish bo'yicha amaliy qo'llanmalar.

Linux xavfsizligi: Linux tizimlarida ishlash, tizimni sozlash va xavfsizlikni ta'minlash bo'yicha o'quv materiallari.

Etikal xakerlikning asoslari: Etikal xakerlikning asosiy printsiplari, huquqiy jihatlar va axloqiy masalalari.

Xulosa

HackZone platformasi, o'zining ta'lim va amaliyotni birlashtirgan yondashuvi bilan, kiberxavfsizlikka qiziquvchi mutaxassislar va yangi boshlovchilar uchun o'zgarishlar kiritish maqsadida faoliyat ko'rsatmoqda. U nafaqat o'quvchilarga zarur bilimlarni berish, balki ularda kiberxavfsizlikka bo'lgan xabardorlikni oshirish va etikal xakerlik sohasida yetuk mutaxassislar tayyorlashga yordam beradi.

Foydalanilgan adabiyotlar ro'yxati:

1. O'zbekiston Respublikasi Prezidentining "Axborot texnologiyalari va kommunikatsiyal
2. arining joriy etilishini nazorat qilish, ularni himoya qilish tizimini takomillashtirish chora-tadbirlari to'g'risida"gi qarori. 2018 yil 21 noyabr, PQ-4024- son.
3. www.itu.int - Xalqaro elektroaloqa uyushmasining rasmiy sayti
4. <https://tace.uz> - Kiberxavfsizlik markazi davlat unitar korxonasi rasmiy sayti
5. Ganiyev S.K. "Kiberxavfsizlik asoslari". O'quv qo'llanma.
6. Saatova L.E. "Approaches to the Formation of the Digital Economy" (inglizcha). American Journal of Economics and Business Management, 2024, 7(11), 1118-1124
7. Saatova L.E. "Formation of the Digital Economy in Uzbekistan and its Indicators" International Journal on Economics, Finance and Sustainable Development (IJEFS), Indoneziya, Volume:6, Issue:1, 24-January-2024 e-ISSN 2620-6269, p-ISSN: 2615 - 4021 2024 P-64-68

KIBERJINOYATCHILIKNI RIVOJLANISHIDA DARKNETNING O‘RNI

Risqaliyev Jaxongir Dadajon-o‘g‘li

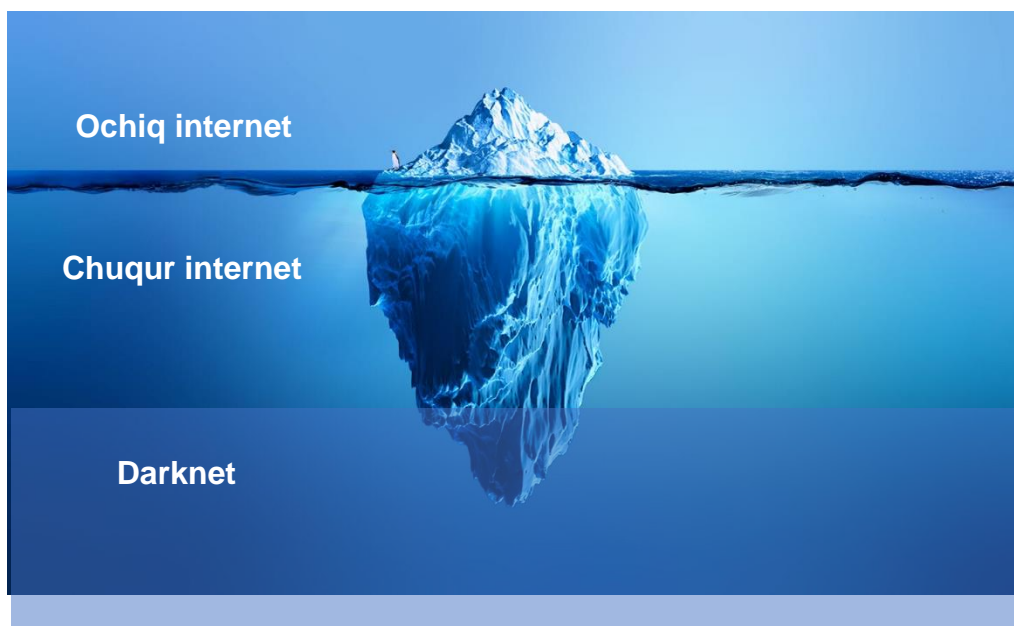
Ichki ishlar vazirligi Malaka oshirish instituti katta o‘qituvchisi

Annotatsiya: Internetning bir qismi, maxsus dasturlar orqaligina kirish mumkin bo‘lgan darknetdan kiberjinoatchilar qurol-yarog‘, giyohvand moddalar va odam savdosi kabi noqonuniy faoliyat uchun foydalanib kelishmoqda. Tor tarmog‘i hamda kriptovalyutalarning yaratilishi jinoyatchilarga noqonuniy faoliyatlarni anonim tarzda amalga oshirishlariga imkon berdi. Buning natijasida esa darknetdan foydalanish ko‘payib bormoqda.

Kalit so‘zlar: internet, darknet, kiberjinoatchilik, Tor brauzer.

Foydalanuvchi so‘rov orqali Google, Yandex yoki Bing internet qidiruv tizimlaridan oladigan ma‘lumotlar ochiq internetdagi ma‘lumotlardir. Internetning shunday tarkibiy qismlari borki, u yerdagi ma‘lumotlar yuqoridagi qidiruv tizimlariga ko‘rinmaydi.

Mutaxassislar odatda internetni quyidagi 3 ta qatlamga, ya‘ni ochiq internet (surface web), chuqur internet (deep web), yopiq internet yoki darknet (dark web)



1-rasm. Internet qatlamlari

bo‘lishadi (1-rasm).

Ochiq internet – bu barcha uchun ochiq bo‘lgan internetdir. Agar butun internetni aysberk deb tassavur qilinsa, ochiq internetni aysberkni uchi deb qarash mumkin. Google Chrome, Microsoft Edge yoki Mozilla Firefox kabi an‘anaviy brauzerlar orqali kirish mumkin bo‘lgan barcha ommaviy veb-saytlar ochiq internetda joylashadi. Bunday saytlarni mashhur qidiruv tizimlarida osongina

topish mumkin, chunki qidiruv tizimlari internetni ko‘rinadigan havolalar orqali indekslanadi. Statistik ma‘lumotlarga qaraganda ochiq internet jami internetning 5 %idan kamrog‘ini tashkil qiladi⁵.

Chuqur internet (deep web) – ochiq internet ostidagi, kuchli himoyalangan sayt yoki ma‘lumotlar bazalaridan tashkil topgan internet hisoblanadi. Bunday saytlarga kirish uchun oddiy brauzerlarni ishlatsa bo‘ladi, ammo bunday saytlar internet qidiruv tizimlari tomonidan aniqlanmaydi. Bu saytlarni chuqur internetga joylashtirilishining sababi xakerlarning hujumidan himoya qilishdir⁶. Odatda chuqur internetdagi axborot tizimlari xavfsizlik devori (firewall) ortiga yashiriladi. Chuqur internetda bank, soliq, moliya, elektron pochta, tibbiyot xujjatlari yoki ijtimoiy tarmoq xabarlarini bo‘ladi.

Darknet (dark web) – bu oddiy brauzerlar orqali kirib bo‘lmaydigan, internetning yashirin, shifrlangan qismidir. Darknet dastlab AQShda harbiy aloqa uchun ishlab chiqilgan bo‘lsa-da, hozirda odamlar noqonuniy yoki anonim faoliyatlarni amalga oshirishda foydalanib kelishmoqda. Darknet foydalanuvchining haqiqiy IP-manzilini anonimlashtiradigan murakkab tizimlardan foydalanadi, bu esa qurilma qaysi veb-saytlarga tashrif buyurganligini aniqlashni juda qiyinlashtiradi⁷.

Satoshi Nakamoto ismli odam tomonidan 2009-yilda birinchi kriptovalyuta, ya‘ni Bitcoinni taqdim etilishi internetda noqonuniy operatsiyalarni amalga oshirishda inqilob yasadi⁸. Chunki, bitkoinlardagi anonimlik, transchegaraviy operatsiyalarning qulayligi va hisob-kitoblarning yakuniyligi jinoyatchilar uchun saytda o‘zlarining noqonuniy faoliyatini amalga oshirishda mukammal vositaga aylandi.

Darknetga Tor (The Onion Router) brauzer yoki I2P (Invisible Internet Project) kabi anonimlashtiruvchi dasturlar orqali kiriladi. Darknet saytlarini yuqori darajadagi “.onion” domeni bilan ajratib olish mumkin.

Masalan,

- <https://duckduckgogg42xjoc72x3sjasowoarfbgcmvfimaftt6twagswzczad.onion/>
- <http://dreadytofatroptsdj6io7l3xptbet6onoyno2yv7jicoxknyazubrad.onion/>

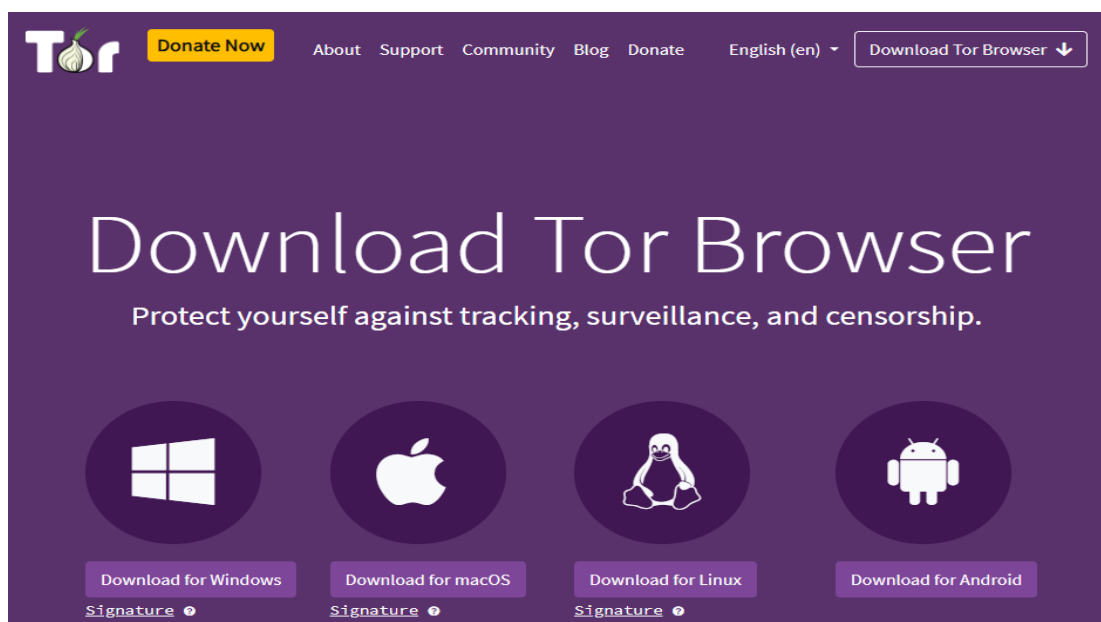
Tor brauzerini <https://www.torproject.org/download/> saytiga kirib, bepul yuklab olish mumkin (2-rasm).

⁵ <https://www.kaspersky.com/resource-center/threats/deep-web>

⁶ <https://texnokun.uz/?p=3842>

⁷ <https://www.ceopeducation.co.uk/parents/articles/what-is-the-dark-web/>

⁸ <https://www.soscanhelp.com/blog/history-of-the-dark-web>



2-rasm. Tor brauzerini yuklab olish sayti interfeysi

Tor tarmog‘i orqali veb-trafikni shifrlash va qayta yo‘naltirish uchun “onion” marshrutlashdan foydalanadi. Ma‘lumotlar bir nechta shifrlash qatlamlarida himoyalanganidan so‘ng, veb-trafik onion routerlari deb ataladigan bir qator tarmoq tugunlari orqali uzatiladi. Har bir marshrutizator (yoki tugun) ma‘lumotlar to‘liq shifrlangan yakuniy manzilga yetguncha shifrlash qatlamini yo‘q qiladi⁹.

So‘rov yuborilganda, so‘rovdagi paketlar (ma‘lumotlar bloklari) alohida shifrlanadi. Keyin Tor ko‘p qatlamli shifrlangan ma‘lumotlarni Tor sxemasini tashkil etuvchi xalqaro proksi-serverlarning 3 ta qatlami bo‘ylab uzatadi, ular har biri bitta qatlam shifrini ochadi. Tarmoq tugunlarining 3 ta qatlamini quyidagicha:

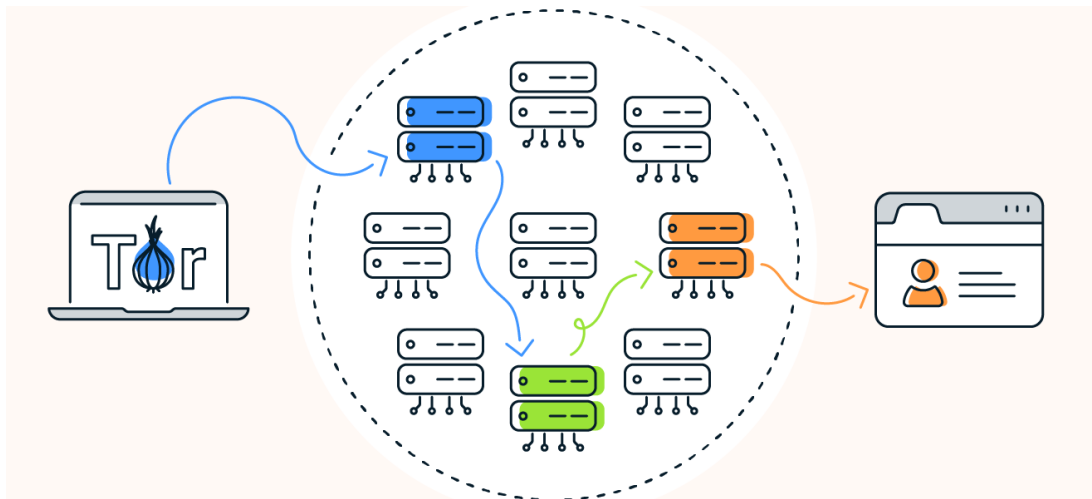
1. *Kirish/qo‘riqlash tugunlari:* Birinchidan, Tor brauzeri hammaga ma‘lum bo‘lgan kirish tuguniga tasodifiy ulanadi. Kirish tugunlari ma‘lumotlarni Tor sxemasiga kiritadi, bu ma‘lumotlarni uzatadigan o‘rta tugun manzilini ochish uchun shifrlashning birinchi qatlamini parolini hal qiladi.

2. *O‘rta tugun:* Ushbu tugun kirish tugunidan so‘rovni oladi. U so‘rov kelgan kirish tugunining IP-manzilini biladi, lekin asl so‘rov egasining shifrlangan IP-manzilini bilmaydi. O‘rta tugun keyingi paketning shifrini ochib, sxemadagi keyingi tugunni ko‘rsatadi, ammo so‘rovning mazmuni va yakuniy manzili shifrlaydi.

3. *Chiqish tugunlari:* Chiqish tugunlari so‘rovni qabul qiladi va oxirgi manzilni ko‘rsatib, oxirgi paketning shifrini ochadi. Shifrlashning oxirgi qatlami o‘chirilgach, shifrlangan ma‘lumotlar Tor tarmog‘idan chiqib va oxirgi server manziliga yetib boradi (3-rasm).

⁹ <https://www.avast.com/c-tor-dark-web-browser>

Tor brauzer IP-ni yashiradi va foydalanuvchining internetdagi faoliyatini kuzatishni qiyinlashtiradi. Joylashuv va identifikatorni yashirish uchun tarmoq tugunlari orqali ma'lumotlarni uzatishdan tashqari, Torning onion marshruti maxfiylikni yanada mustahkam himoya qilish uchun ko'p qatlamli shifrlashdan foydalanadi.



3-rasm. Tor brauzeri trafikni shifrlash va shifrini ochish uchun kirish tugunlari (ko'k), o'rta tugun (yashil) va chiqish tugunlari (to'q sariq) orqali veb-trafikni yuboradi

Qisqacha qilib aytganda, darknet internetning yashirin qismi bo'lib, anonimlik va ba'zi hollarda noqonuniy faoliyatlar uchun foydalaniladi. Shu bilan birga, u huquqiy maqsadlarda ham ishlatilishi mumkin, lekin foydalanishda ehtiyotkor bo'lish talab etiladi.

REFERENCES:

1. Bash, L. (2003). *Adult Learners in the Academy*. Bolton: Anker Publishing Company.
2. Jarvis. P. (2004). *Adult Education and Lifelong Learning: Theory and Practice*. 3rd. London: Falmer Press. Malcolm.
3. S.Knowles (2014) - *The Adult Learner: A Neglected Species*. American society for training and development.
4. Madison Tight, M. (2003). *Key Concepts in Adult Education and Training*. Florence, Ky.: Routledge.

AXBOROT TEXNOLOGIYALARIDAN FOYDALANGAN HOLDA SODIR ETILADIGAN HUQUQBUZARLIKLARGA QARSHI KURASHISHNING DOLZARB MUAMMOLARI VA YECHIMLARI

Odilov Nordirbek Odil o'g'li

IIV Malaka oshirish instituti Maxsus-kasbiy fanlar kafedrası katta o'qituvchisi,

Email: odilovbek056@gmail.com

Anotatsiya: Hozirgi kunda axborot texnologiyalarining jadal rivojlanishi bilan birga, ulardan foydalangan holda sodir etilgan huquqbuzarliklar ham ortib bormoqda. Axborot texnologiyalari orqali sodir etiladigan huquqbuzarliklar jamiyatning barcha jabhalariga salbiy ta'sir ko'rsatib, xavfsizlik va huquqiy tartibga jiddiy tahdid soladi. Maqolada axborot texnologiyalari asosida sodir etiladigan huquqbuzarliklar turlari, ularning kelib chiqish sabablari, hamda ularga qarshi samarali kurashishning huquqiy, texnologiyaviy va ijtimoiy yo'nalishlari tahlil qilingan. Shuningdek, zamonaviy axborot xavfsizligi tizimlari, huquqiy normalar va davlat siyosati asosidagi integratsiyalangan yondashuvlar ko'rib chiqilgan.

Kalit so'zlar: Axborot texnologiyalari, kiberhuquqbuzarliklar, kiberxavfsizlik, kiberhujumlar, raqamli huquqbuzarliklar, huquqiy tartib, elektron jinoyatchilik, davlat siyosati.

Axborot texnologiyalari har bir jamiyatning iqtisodiy, ijtimoiy va siyosiy sohalariga chuqur kirib bormoqda. Ularning yordamida axborotni saqlash, qayta ishlash va tarqatish juda osonlashdi. Biroq, axborot texnologiyalari tizimlarining kengayishi va ularning turli sohalarida joriy etilishi bilan birga, ushbu sohada sodir etiladigan huquqbuzarliklar soni ham sezilarli darajada o'sdi. Internet va raqamli texnologiyalar jadal rivojlanishi natijasida paydo bo'lgan kiberhuquqbuzarliklar, shu jumladan moliyaviy firibgarlik, ma'lumotlarni o'g'irlash, elektron hujumlar va axborot xavfsizligi buzilishlari jamiyat hayoti uchun katta xavf tug'diradi. Shuning uchun axborot texnologiyalaridan foydalangan holda sodir etiladigan huquqbuzarliklarga qarshi samarali kurashish chora-tadbirlarini ishlab chiqish va amalga oshirish dolzarb vazifaga aylandi.

Axborot texnologiyalari orqali sodir etiladigan huquqbuzarliklar turlari va xususiyatlari. Axborot texnologiyalari yordamida sodir etiladigan huquqbuzarliklar turlari:

- Kiberhujumlar va xakerlik faoliyati: Kompyuter tizimlariga noqonuniy kirish, ma'lumotlarni buzish yoki o'g'irlash maqsadida turli xil texnik vositalar

orqali amalga oshiriladi. Bunda viruslar, troyanlar, DDoS hujumlari va boshqa zararli dasturlar qo'llaniladi.

- Ma'lumotlarni o'g'irlash va o'zgartirish: Shaxsiy ma'lumotlar, moliyaviy ma'lumotlar va boshqa maxfiy axborotlarni noqonuniy tarzda olish yoki ularni o'zgartirish.

- Moliyaviy firibgarlik: Elektron to'lov tizimlari, onlayn bank xizmatlari va kriptovalyuta bilan bog'liq jinoyatlar. Misol uchun, fishing, frod, mablag'larni o'g'irlash.

- Intellektual mulkni buzish: Litsenziyasiz dasturlar, kontent o'g'irlash va noqonuniy tarqatish, avtorlik huquqlarining buzilishi.

- Kiberqo'rqitish va jinoyatchilik: Internetda shaxsga bosim o'tkazish, kiberbulling, yoshlarga zararli ma'lumot tarqatish, terrorchilik va ekstremizmga aloqador materiallarni tarqatish.

Axborot texnologiyalarida huquqbuzarliklarning rivojlanish sabablari:

- Qonunchilik va me'yoriy bazaning yetishmasligi: Yangi texnologiyalar tez rivojlanayotgani bilan qonunchilik ularga mos ravishda yangilanmaydi, bu huquqbuzarliklarga qarshi kurashishda qiynchilik tug'diradi.

- Texnik va tashkiliy jihatdan zaifliklar: Maqsadli hujumlarni oldini olish uchun zarur bo'lgan infratuzilmalar yetarlicha rivojlanmagan.

- Malakali mutaxassislarining yetishmasligi: Axborot xavfsizligi sohasida kadrlarni tayyorlashda, ularning malakasini oshirishda muammolar bor.

- Jamoatchilikning axborot xavfsizligi bo'yicha bilim darajasining pastligi: Internet foydalanuvchilari kiberhujumlarga qarshi qanday choralar ko'rishni bilishmaydi.

- Xalqaro hamkorlikdagi muammolar: Kiberhujumlar ko'pincha davlatlar hududidan tashqari amalga oshirilganligi sababli, ularni aniqlash va jazolashda xalqaro hamkorlik muhim ahamiyat kasb etadi, ammo bu sohada muammolar mavjud.

Axborot texnologiyalari asosida sodir etiladigan huquqbuzarliklarga qarshi kurashish usullari:

- Qonunchilikni takomillashtirish: Axborot texnologiyalari va kiberhuquq sohasidagi qonunlarni doimiy ravishda yangilash, yangi tahdidlarga moslashtirish. Shuningdek, jinoyatlarni aniqlash va jazolashni mustahkamlaydigan normalarni joriy etish.

- Kiberxavfsizlik infratuzilmasini mustahkamlash: Davlat darajasida kiberxavfsizlik markazlari tashkil etish, ularni zarur jihozlar va innovatsion texnologiyalar bilan ta'minlash.

- Mutaxassislarni tayyorlash va malakasini oshirish: Axborot xavfsizligi sohasida ilmiy-tadqiqot faoliyatini kengaytirish, yuqori malakali kadrlar tayyorlash va ularning malakasini muntazam oshirish uchun dasturlar yaratish.

- Jamoatchilikni axborot xavfsizligiga oid bilimlar bilan ta'minlash: Internetda xavfsizlik choralari, shaxsiy ma'lumotlarni muhofaza qilish, elektron xatarlar haqida keng jamoatchilikni o'qitish va ogohlantirish.

- Xalqaro hamkorlikni mustahkamlash: Kiberhuquqbuzarliklarga qarshi kurashishda xalqaro kelishuvlar, ma'lumot almashish, qonuniy yordam va boshqa chora-tadbirlarni kuchaytirish.

O'zbekistonda kiberxavfsizlik va huquqbuzarliklarga qarshi kurashishning hozirgi holati:

- O'zbekiston Respublikasi axborot texnologiyalarini rivojlantirish va kiberxavfsizlik sohasida qator qonunlar va qarorlarni qabul qilgan. Jumladan, "Axborot texnologiyalari to'g'risida", "Kiberxavfsizlik to'g'risida"gi qonunlar mavjud. Shu bilan birga, davlat darajasida kiberxavfsizlik markazlari faoliyati yo'lga qo'yilgan va ushbu sohada ilmiy tadqiqotlar amalga oshirilmoqda. Ammo, xalqaro tajribalardan samarali foydalanish, kadrlar tayyorlash va jamoatchilikni ma'lumotlantirish sohalarida yanada sezilarli ishlar qilish zarur.

Xulosa qilib, Axborot texnologiyalaridan foydalangan holda sodir etiladigan huquqbuzarliklar — bu zamonaviy jamiyatning eng dolzarb muammolaridan biridir. Ularning oqibatlari nafaqat iqtisodiy zararlar, balki ijtimoiy barqarorlikka ham ta'sir ko'rsatadi. Maqolada ko'rsatilganidek, ushbu muammolarga qarshi kurashish uchun huquqiy bazani takomillashtirish, kiberxavfsizlikni mustahkamlash, malakali mutaxassislarni tayyorlash va jamoatchilikni axborot xavfsizligi sohasida bilim bilan ta'minlash muhimdir. Shuningdek, xalqaro hamkorlikni kuchaytirish va innovatsion texnologiyalarni joriy etish ham muhim ahamiyatga ega. Davlat, xususiy sektor va jamoatchilikning hamkorligi ushbu muammoning yechimini topishda asosiy rol o'ynaydi.

Foydalanilgan adabiyotlar:

1. Abdurahmonov M. Axborot texnologiyalari va huquqbuzarliklar: nazariya va amaliy jihatlar. — Toshkent, 2021.

2. Saidov J. Kiberxavfsizlik va kiberhuquq. — Samarqand, 2020.

Xalq deputatlari mahalliy kengashlari materiallari. Kiberxavfsizliklarga qarshi kurash. — Toshkent, 2022.

3. International Telecommunication Union (ITU). Global Cybersecurity Index. — 2023.

4. Ro'ziev A. Axborot texnologiyalari orqali sodir etiladigan huquqbuzarliklar va ularga qarshi kurashish choralari. — Toshkent, 2019.

5. O‘zbekiston Respublikasi Kiberxavfsizlik va Axborot texnologiyalari to‘g‘risidagi qonunlar.

6. Kiberxavfsizlik va raqamli xavfsizlik sohasida xalqaro standartlar (ISO/IEC 27001).

AXBOROT TEXNOLOGIYALARIDAN FOYDALANGAN HOLDA DRONLARDAN HUQUQBUZARLIKNI ANIQLASH YECHIMLARI

Abdiraximov Amriddin Abdiraximovich

IIV Malaka oshirish instituti, Axborot texnologiyalari sikli o‘qituvchisi

Annotatsiya. Ushbu tezisda zamonaviy jamiyatda huquqbuzarliklarni aniqlash va oldini olish maqsadida axborot texnologiyalari va dronlardan foydalanish keng tarqalmoqda. Dronlar yordamida huquqbuzarliklarni aniqlashning samarali usullari, sun‘iy intellekt, kompyuter ko‘rish va ma‘lumotlar tahlili texnologiyalarining qo‘llanishi hamda ularning huquqiy jihatlari haqida batafsil tushunchalar berilgan.

Kalit so‘zlar: Dronlar, huquqbuzarlik, sun‘iy intellekt, kompyuter ko‘rish, monitoring, ma‘lumotlar tahlili, real vaqtda kuzatuv, huquqiy jihatlar, xavfsizlik.

Dronlarning real vaqtda monitoring qilish qobiliyati, yashirin kameralar orqali jinoyatchilarni aniqlash, transport hodisalarini tekshirish kabi imkoniyatlari o‘rganilgan. Tadqiqot natijalari shuni ko‘rsatadiki, dronlar huquqni muhofaza qilish organlariga tez va aniq ma‘lumot olish imkonini beradi, biroq shaxsiy hayot himoyasi va ma‘lumotlar xavfsizligi masalalari hal etilish choralari ko‘rilmoqda. Zamonaviy texnologiyalarning rivojlanishi bilan birga huquqni muhofaza qilish sohasida yangi usullar joriy etilmoqda. [1]

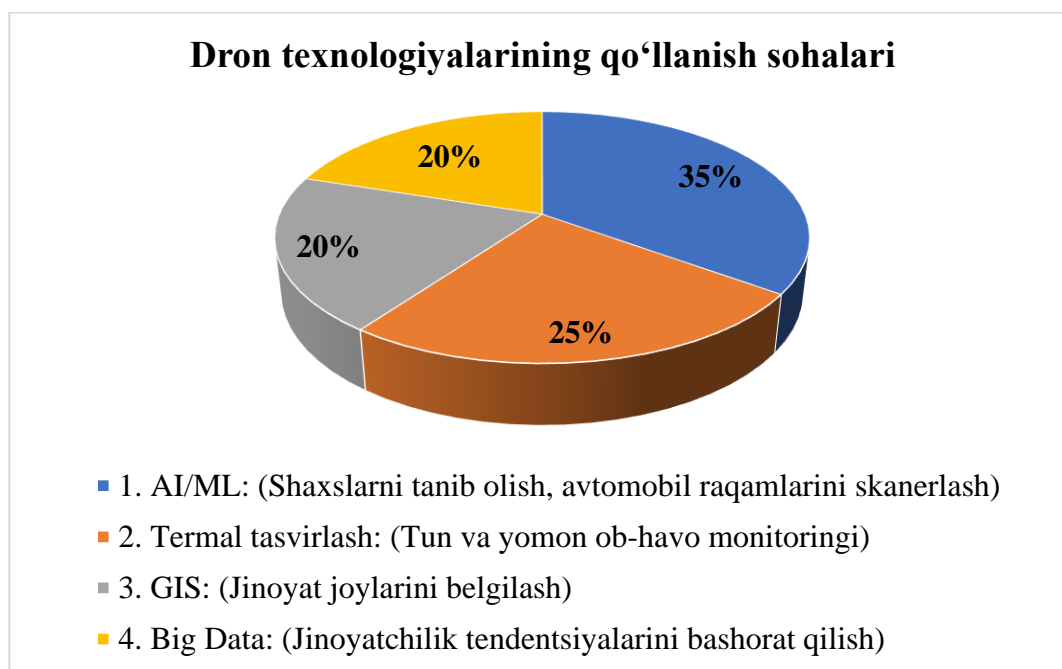
Dronlar – bu havo monitoringi, yirik hududlarni nazorat qilish va huquqbuzarliklarni aniqlashda samarali vosita hisoblanadi.

Uchuvchisiz uchadigan apparatlar (dronlar) so‘nggi yillarda harbiy, tijorat va hatto kundalik hayotda keng qo‘llanilmoqda. Bu texnologiya juda foydali bo‘lsa-da, xavfsizlik sohasida katta tahdidlarga ham olib kelmoqda. Xavfsiz hududlarda, masalan, harbiy obyektlar, aeroportlar yoki maxfiy muassasalar atrofida dronlar orqali amalga oshirilgan noqonuniy kuzatuvlar, xujumlar va maxfiy ma‘lumotlarning o‘g‘irlanishi xavf tug‘diradi. Shu sababli, uchuvchisiz uchadigan apparatlarga qarshi kurashish vositalarini yaratish, shu jumladan, matematik modellarni ishlab chiqish, sohada katta ahamiyatga ega.

Dronlarning huquqbuzarliklarni aniqlashdagi roli.

Dronlar quyidagi jihatlarda huquqni muhofaza qilish organlariga yordam beradi:

- ✓ Real vaqtda monitoring – yirik hududlarni tez va samarali nazorat qilish imkoniyati.
- ✓ Sun'iy intellekt (AI) va kompyuter ko'rish – shubhali harakatlarni avtomatik aniqlash.
- ✓ Tergov va dalil to'plash – jinoyat joyini fotosurat va videolar orqali hujjatlashtirish.
- ✓ Trafik nazorati – qoidabuzarliklar va avariyalarni tezda aniqlash.



1-rasm. Dron huquqbuzarliklarni aniqlash grafigi

Uchuvchisiz uchadigan apparatlar (dronlar) xavfsizlikni tahdid qilayotgan bir paytda, ularning qarshi kurashish vositalarini ishlab chiqish juda muhimdir. Matematik modellar, fizik hodisalarni, elektromagnit to'liqlarni va dinamikani hisobga olgan holda, tizimlarning samaradorligini aniqlashda yordam beradi. Dronlarga qarshi kurashish texnologiyalarining kelajakda yanada takomillashuvi va samaradorligi ushbu modellarga asoslanadi, va ularning to'g'ri ishlashi uchun yangi ilmiy yondashuvlar zarur bo'ladi.

Dronlar orqali sodir etiladigan huquqbuzarliklarga qarshi kurashishda axborot texnologiyalari asosida ishlab chiqilgan yechimlar muhim rol o'ynaydi. Sun'iy intellekt, elektromagnit to'liqlar va dinamik modellar yordamida dronlarning tahdidlarini bartaraf etish samaradorligini oshirish mumkin. Kelajakda bu sohada ilmiy tadqiqotlarni kuchaytirish va qonuniy bazani takomillashtirish zarur.

Foydalanilgan adabiyotlar ro'yhati:

1. A.A.Abdiraximov "Harbiy pedagogika ta'limining innovatsion yondashuvlari muammo va yechimlari" To'plam. _Sirdaryo., 2025. _55 b.
2. A.A.Abdiraximov "Obyektlarning majmuaviy xavfsizlik tizimlari, natija va istiqbollari:" Xalqaro tajriba" Xalqaro ilmiy – amaliy konferensiya materiallari To'plam. _Toshkent., 2025. _117 b.
3. Simon J. Julier and Jeffrey K. Uhlmann A New Extension of the Kalman Filter to Nonlinear Systems
4. Арипджанов М.К. Авиация метеорологияси, Тошкент, ТДАИ, 2008.
5. Учебное пособие «Основы аэродинамики и динамики полета летательных аппаратов» посвящено одному из разделов дисциплины «Основы авиации»
6. <https://www.dronedefence.co.uk/about/>
7. <https://www.defence-industries.com/>

KIBERXAVFSIZLIKNI OLDINI OLISHGA DOIR AYRIM TUSHUNCHALAR

Butayev Isroil Nazirovich

IIV MOI, KTF Jangovar va jismoniy tayyorgarlik sikli katta o'qituvchisi

Annotatsiya. *Ushbu tezis zamonaviy axborot jamiyatida kiberxavfsizlik muammolari tobora murakkablashib borayotgan bo'lsa, unga qarshi choralar ham doimiy ravishda takomillashtirilmoqda. Kiberxavfsizlikning asosiy tushunchalari, tahdidlar turlari va ularga qarshi himoya usullari ilmiy nuqtai nazardan yoritilgan.*

Kalit so'zlar: *kiberxavfsizlik, kriptografiya, tarmoq himoyasi, ma'lumotlar xavfsizligi, sun'iy intellekt, kiberjinoyat, foydalanuvchi xabardorligi, huquqiy tartibga solish.*

Bugungi kunda jamiyatimizda global muammolari qatoriga yangidan-yangi turlari bilan tilga olinayotgan kiberjinoyatchilik kirib kelganiga ham ancha bo'ldi. Uning bizga ma'lum bo'lgan virusli dasturlarni tarqatish, parollarni buzib kirish, kredit karta va boshqa bank rekvizitlaridagi mablag'larni o'zlashtirish talon-toroj qilish, shuningdek, internet orqali qonunga zid axborotlar, xususan, bo'hton, ma'naviy buzuq ma'lumotlarni tarqatish bilan bashariyat hayotiga katta xavf solayotganidan ko'z yuma olmaymiz.

Axborot xavfsizligi – ma'lumotlarni yo'qotish va o'zgartirishga yo'naltirilgan tabiiy yoki sun'iy xossalari tasodifiy va qasddan ta'sirlardan xar qanday tashuvchilarda axborotning himoyalanganligiga aytiladi.[1]

Axborotning himoyasi – boshqarish va ishlab chiqarish faoliyatining axborot xavfsizligini ta'minlovchi va tashkilot axborot zaxiralarining yaxlitligi, ishonchliligi, foydalanish osonligi va maxfiylikni ta'minlovchi qat'iy reglamentlangan dinamik texnologik jarayonga aytiladi. [2]

Kiberxavfsizlik tushunchasiga ta'riflar quyidagicha ta'rif bergan:

Kiberxavfsizlik – hisoblashga asoslangan bilim sohasi bo'lib, buzg'unchilar mavjud bo'lgan sharoitda amallarni kafolatlash uchun o'zida texnologiya, inson, axborot va jarayonni mujassamlashtirgan. U xavfsiz kompyuter tizimlarini yaratish, amalga oshirish, tahlil qilish va testlashni o'z ichiga oladi.[3]

Kiberxavfsizlik ta'limning mujassamlashtirilgan bilim sohasi bo'lib, qonuniy jixatlarni, siyosatni, inson omilini, etika va risklarni boshqarishni o'z ichiga oladi.

Tarmoq bo'yicha faoliyat yuritayotgan Cisco tashkiloti esa kiberxavfsizlikka quyidagicha ta'rif bergan:

Kiberxavfsizlik – tizimlarni, tarmoqlarni va dasturlarni raqamli hujumlardan himoyalash amaliyoti. Ushbu kiberhujumlar odatda maxfiy axborotni boshqarish, almashtirish yoki yo'q qilishni; foydalanuvchilardan pul undirishni; yoki normal ish faoliyatini uzub qo'yishni maqsad qiladi. Hozirgi kunda samarali kiberxavfsizlik choralarini amalga oshirish insonlarga qaraganda qurilmalar sonining ko'pligi va buzg'unchilar salohiyatini ortishi natijasida amaliy tomondan murakkablashib bormoqda.

Kiberxavfsizlik konsepsiyasi – axborot xavfsizligi muammosiga rasmiy qabul qilingan qarashlar tizimi va uni zamonaviy tendensiyalarni hisobga olgan holda yechish yo'llari.

Kiberxavfsizlik siyosati bu – tashkilotning maqsadi va vazifasi hamda xavfsizlikni ta'minlash sohasidagi chora-tadbirlar tavsiflanadigan yuqori sathli reja hisoblanadi. U xavfsizlikni ta'minlashning barcha dasturlarini rejalashtiradi. Apparat vositalar va dasturiy ta'minot ish jarayonini ta'minlovchi vositalar hisoblanadi va ular xavfsizlik siyosati tomonidan qamrab olinishi shart.[4]

Tashkilotning amaliy xavfsizlik siyosati qo'yidagi bo'limlarni o'z ichiga olishi mumkin: umumiy nizom; parollarni boshqarish siyosati; foydalanuvchilarni identifikatsiyalash; foydalanuvchilarning vakolatlari; tashkilot axborot kommunikatsion tizimini kompyuter viruslardan himoyalash; tarmoq ulanishlarini o'rnatish va nazoratlash qoidalari; elektron pochta tizimi bilan ishlash bo'yicha xavfsizlik siyosati qoidalari; axborot kommunikatsion tizimlar xavfsizligini ta'minlash qoidalari; foydalanuvchilarning xavfsizlik siyosatini qoidalari bajarish bo'yicha majburiyatlari va h.k.lar.

Axborot xavfsizligi siyosati tashkilot masalalarini yechish himoyasini yoki ish jarayoni himoyasini ta'minlashi shart.

Bugungi kunda O'zbekiston Respublikasida "Kiberxavfsizlik to'g'risida"gi qonun qabul qilindi. Qonunning maqsadi mamlakatda kiberxavfsizlik sohasidagi munosabatlarni tartibga solishdan iborat bo'lib, uning asosiy vazifalari kibermakonda shaxs, jamiyat va davlat manfaatlarini tashqi va ichki tahdidlardan himoya qilish hisoblanadi. Qonunda kiberjinoyatchilik, kibertahdid, kiberxavfsizlik, kiberhimoya va kiberhujum kabi tushunchalar qo'llanib, kiberxavfsizlikni ta'minlashning asosiy prinsiplari va bu sohadagi davlat siyosati asosiy yo'nalishlari belgilab berilgan.[5]

Davlat xavfsizlik xizmati kiberxavfsizlik sohasidagi vakolatli davlat organi etib belgilanib, uning huquqlari va majburiyatlari mustahkamlab qo'yilmoqda.

Qonun bilan kiberxavfsizlik sub'ektlarining huquq va majburiyatlari, ularning kiberxavfsizlik talablariga muvofiqligi yuzasidan ekspertizadan majburiy tartibda yoki kiberxavfsizlik sub'ektlari tashabbusiga ko'ra amalga oshirilishi belgilab qo'yildi.

Kiberxavfsizlik faqat texnologik yechimlar bilan cheklanib qolmaydi, balki u foydalanuvchilarning xabardorligi, korxonalarining investitsiyalari va davlatlararo hamkorlikni talab qiladi. Har bir foydalanuvchi o'z ma'lumotlarini himoya qilish bo'yicha asosiy choralarni bilishi va ularni qo'llashi zarur.

Foydalanilgan adabiyotlar:

1. Ganiev S.K., Karimov M.M., Xudoyqulov Z.T., Kadirov M.M. Axborot xavfsizligi bo'yicha atama va tushunchalarning rus, o'zbek va ingliz tillaridagi izohli lug'ati // Toshkent 2017, -B. - 480.

2. Stallings, W. (2017). Cryptography and Network Security: Principles and Practice. Pearson.

3. Schneier, B. (2015). Data and Goliath: The Hidden Battles to Collect Your Data and Control Your World. W. W. Norton & Company.

4. Kaspersky Lab. (2021). Cyberthreats: Trends and Predictions. Kaspersky Security Bulletin.

5. European Union Agency for Cybersecurity (ENISA). (2022). Threat Landscape Report.

6. ISO/IEC 27001:2022. Information security management systems – Requirements.

7. Dileep Kumar G, Manoj Kumar Singh and M.K. Jayanthi. Network Security Attacks and Countermeasures. Indexed In: SCOPUS |Copyright: © 2016 Pages: 357

AXBOROT TEXNOLOGIYALARI YORDAMIDA JINOYATLARNI OLDINI OLISH

Muslimov Xusan Nishonboyevich

O'zbekiston Respublikasi Ichki ishlar vazirligi Malaka oshirish instituti Jangovar tayyorgarlik sikli o'qituvchisi

Annotatsiya. Mazkur maqolada axborot texnologiyalarining jinoyatlarning oldini olishdagi roli tahlil qilinadi. Unda zamonaviy videokuzatuv tizimlari, sun'iy intellekt, yuzni aniqlash, geolokatsiya va ma'lumotlar tahlili kabi texnologiyalar yordamida jinoyatchilikka qarshi samarali kurashish imkoniyatlari yoritilgan. Shuningdek, texnologiyalardan foydalanishda uchraydigan asosiy muammolar — shaxsiy daxlsizlik, texnik va moliyaviy cheklovlar, kadrlar yetishmovchiligi haqida so'z yuritiladi. Maqolada jinoyatlarning oldini olishni kuchaytirish uchun texnologik, huquqiy va ijtimoiy yo'nalishlarda berilgan takliflar asosida kompleks yondashuv zarurligi asoslab berilgan.

Kalit so'zlar: Axborot texnologiyalari, jinoyatlarning oldini olish, videokuzatuv tizimi, sun'iy intellekt, yuzni aniqlash, geolokatsiya, raqamli xavfsizlik, jinoyatchilik, profilaktika, huquqni muhofaza qilish.

Zamonaviy axborot texnologiyalarining jadal rivojlanishi jamiyat hayotining barcha sohalariga chuqur ta'sir ko'rsatmoqda. Bu texnologiyalar nafaqat kundalik hayotni yengillashtirishda, balki huquqni muhofaza qilish, xavfsizlikni ta'minlash va jinoyatchilikka qarshi kurashish tizimida ham katta imkoniyatlar yaratmoqda. Bugungi kunda jinoyatlarni oldindan aniqlash, ularning oldini olish va profilaktika choralarini ko'rishda axborot texnologiyalaridan foydalanish samarador yechim sifatida qaralmoqda.

Axborot texnologiyalari jinoyatlarni aniqlashdan ko'ra, ularning oldini olishda ancha samarali vosita bo'lib xizmat qilmoqda. Bu boradagi eng muhim texnologiyalar quyidagilardan iborat:

Videokuzatuv tizimlari: Jamoat joylari, muassasalar va turar joylar atrofidagi videokameralar jinoyatni sodir etish ehtimolini kamaytiradi va jinoyatchilarni fosh qilishda muhim rol o'ynaydi. Ushbu videokuzatuv moslamalari yordamida jinoyatchilarni shaxsini aniqlash, qilgan jinoyatini fosh qilishda juda katta yordam beradi.

Sun'iy intellekt: asosidagi tahlil: Katta hajmdagi ma'lumotlarni tahlil qilish orqali jinoyat sodir bo'lishi mumkin bo'lgan joylar va shaxslarni aniqlash imkonini beradi.

Yuzni aniqlash (identifikatsiya) tizimlari: Jinoyatga moyil yoki o'ta xafli jinoyatchilarni hamda qidiruvdagi shaxslarni ommaviy joylarda tezda aniqlash imkonini beradi. Mazkur qurilmalarni avto turargohlarga, shaharlar aro qatnovchi

avtobuslarning shox bekatlariga, metroga kirish va chiqish joylariga, serqatov yo'llarning chetlariga o'rnatish ancha samara beradi.

Geolokatsiya va GPS kuzatuv: Shubhali harakatlarni aniqlash, transport vositalari harakatini nazorat qilish orqali jinoyatlarning oldini olishda muhim aҳaмият касб этади. Mazkur tizim orqali jinoyatchilar tomonidan olib qochilgan avtotransportlarni joylashuvini yoki harakat yo'nalishini aniqlash mkmkin.

Ma'lumotlar bazasini tahlil qilish: Jinoyatchilik statistikasiga asoslanib, qaysi hududda qanday jinoyatlar ko'proq sodir bo'layotganini aniqlab, ushbu jinoyatlarga qarshi profilaktik tadbirlarni kuchaytirish orqali jinoyatchilikni kamaytirish va oldini olish mumkin.

Garchi globallashuv jarayonida axborot texnologiyalari keng joriy qilinayotgan bo'lsa-da, bir qator muammo va kamchiliklar hali ham mavjudligi dilni xira qiladigan holat. Quyida mazkur muammo va kamchiliklar xaqida qisqacha to'xtalib o'tamiz.

Shaxsiy hayot daxlsizligining buzilishi — videokuzatuv va ma'lumot yig'ish tizimlari noto'g'ri ishlatilsa, fuqaroning konstitutsiyaviy huquqlari buzilishi mumkin;

Texnik imkoniyatlarning cheklanganligi — ayrim hududlarda internet yoki elektr ta'minoti sustligi bu texnologiyalarni to'liq qo'llashga to'sqinlik qiladi;

Kadrlar yetishmasligi — zamonaviy texnologiyalarni boshqarish uchun malakali mutaxassislar kerak;

Moliyaviy mablag'larning yetishmasligi — ilg'or xavfsizlik tizimlari qimmatga tushadi.

Jinoyatlarning oldini olishda axborot texnologiyalaridan samarali foydalanish uchun quyidagi yo'nalishlarga e'tibor qaratish zarur:

Texnologik infratuzilmani rivojlantirish: sun'iy intellekt, va boshqa tizimlarni mahalliy hududlar darajasigacha kengaytirish;

Huquqiy asoslarni takomillashtirish: Axborot texnologiyalarining qonuniy va tartibli ishlatilishini nazorat qilish;

Mutaxassislar tayyorlash: Huquqni muhofaza qiluvchi organlar va xavfsizlik xizmatlari uchun IT sohasida bilimli kadrlar yetishtirish;

Xalqaro tajribalardan foydalanish: Rivojlangan mamlakatlar tajribasini o'rganish va mahalliy sharoitga moslashtirish;

Jamoatchilik bilan hamkorlik: Fuqarolarni jinoyatchilikka qarshi kurashda texnologiyalar yordamida faol ishtirok etishga jalb qilish.

Xulosa qilib aytganda, axborot texnologiyalari jinoyatlarning oldini olishda samarali vosita bo'lib xizmat qilmoqda. Ular nafaqat jinoyat sodir bo'lganidan so'ng iz qoldirish, balki jinoyatning umuman ro'y bermasligi uchun profilaktika choralarini kuchaytirishga xizmat qiladi. Kelgusida bu texnologiyalarni huquqiy va

axloqiy jihatdan to‘g‘ri qo‘llash orqali jamiyatda xavfsizlik darajasini yanada oshirish mumkin.

Adabiyotlar ro‘yxati:

1. O‘zbekiston Respublikasi Jinoyat kodeksi. — Toshkent: Adolat, 2023.
2. O‘zbekiston Respublikasi Prezidentining “Raqamli O‘zbekiston — 2030” strategiyasi to‘g‘risidagi qarori, PQ–6079-son, 5-oktabr 2020-yil.
3. Axmedov A.M. *“Axborot xavfsizligi va uning huquqiy asoslari”*. — Toshkent: Iqtisodiyot, 2022.
4. Xolmurodov B.B. *“Kiberxavfsizlik asoslari”*. — Toshkent: Innovatsiya, 2021.
5. Karimov A.K. *“Huquqbuzarliklarning oldini olishda raqamli texnologiyalarning o‘rni”*. — “Yuridik fanlar axborotnomasi”, 2023, №2, 45–50-betlar.
6. “Dunyoda jinoyatchilikka qarshi kurashda zamonaviy texnologiyalar”. *Jahon amaliyoti sharhi*, 2022, №1.
7. Interpol. *“Cybercrime and Digital Policing Trends”* — <https://www.interpol.int>, 2024.
8. Europol. *“Internet Organised Crime Threat Assessment (IOCTA)”*, 2023.
9. Yar M., Steinmetz K. *“Cybercrime and Society”*. — London: Sage Publications, 2020.
10. Wall D.S. *“Policing the Digital Age: Crime, Technology and the Future of Law Enforcement”*. — Routledge, 2019.

KIBERXAVFSIZLIK SOHASIDAGI DOLZARB MUAMMOLAR VA ULARNI HAL ETISH YO‘LLARI

Raximov Sherbek Kamolovich

O‘zbekiston Respublikasi IIV Malaka oshirish instituti

Maxsus fanlar sikli o‘qituvchisi

Bugungi o‘zaro bog‘liq dunyoda kiber xavfsizlik zamonaviy jamiyatlar va iqtisodiyotlarni qo‘llab-quvvatlovchi raqamli ekotizimlarni himoya qilish uchun asos bo‘lib xizmat qildi. Raqamli texnologiyalarga tayanish misli ko‘rilmagan darajaga yetdi, innovatsiyalar, iqtisodiy o‘sish va ijtimoiy taraqqiyotga turtki bo‘ldi. Biroq, bu ishonch, shuningdek, hayotimizni yaxshilash uchun mo‘ljallangan tizimlarni buzishi mumkin bo‘lgan muhim zaifliklarni keltirib chiqardi. Shuning uchun kiberxavfsizlik ruxsatsiz kirish, zararli hujumlar va ma’lumotlarning buzilishidan himoya qilishga qaratilgan keng ko‘lamli amaliyot, siyosat va texnologiyalarni o‘z ichiga oladi. Shaxsiy shaxsiy ma’lumotlarni himoya qilishdan

tortib, muhim infratuzilmaning yaxlitligini ta'minlashgacha, kiberxavfsizlikning roli raqamli o'zaro aloqalarga ishonchni saqlash va zamonaviy institutlarning barqarorligini saqlashda muhim ahamiyatga ega. Xizmatlarni tezkor raqamlashtirish va internetga ulangan qurilmalarning ko'payishi hujum yuzasini eksponent ravishda kengaytirdi. Narsalar Interneti (IoT) orqali o'zaro bog'langan milliardlab qurilmalar bilan zaifliklar endi an'anaviy IT tizimlari bilan chegaralanib qolmaydi, balki kundalik jihozlar, transport vositalari va hatto tibbiy asboblarga ham tarqaladi. Ushbu keng va o'zaro bog'liq raqamli landshaft kiber mudofaaga ko'p qirrali va proaktiv yondashuvni talab qiladigan hukumat, korporativ va individual domenlardagi zaifliklarni ochib beradi. Ushbu zaifliklarni bartaraf etishning oqibatlarini halokatli bo'lishi mumkin, moliyaviy yo'qotishlar va obro'ga etkazilgan zarardan tortib, muhim xizmatlardagi uzilishlar va milliy xavfsizlikka tahdidlargacha¹⁰.

Kiberxavfsizlik – bu nafaqat texnologik muammo, balki ijtimoiy, iqtisodiy va huquqiy sohalarni ham qamrab olgan murakkab tizimdir. Bugungi kunda kiberjinoyatlar sonining oshishi, axborot tizimlariga hujumlarning murakkablashuvi va yangi tahdidlarning paydo bo'lishi ushbu sohadagi muammolarni yanada keskinlashtirmoqda.

Shu bois, kiberxavfsizlik sohasidagi dolzarb muammolarni aniqlash va ularni samarali hal etish yo'llarini izlash – davlat, korxonalar va jamiyat oldidagi muhim vazifalardan biridir. Ushbu maqolada kiberxavfsizlikka taalluqli asosiy muammolar tahlil qilinib, ularni bartaraf etishda zamonaviy texnologiyalar va qonunchilikning roli ko'rib chiqiladi. Shuningdek, samarali strategiyalar va innovatsion yechimlar taklif etiladi, ular orqali raqamli makondagi xavfsizlikni mustahkamlash mumkinligi ko'rsatib o'tiladi.

Kiberxavfsizlik — bu kompyuter tizimlari, tarmoqlar, dasturlar va ma'lumotlarni ruxsatsiz kirish, buzilish, o'g'rilash yoki zarar yetkazilishidan himoya qilish jarayonlari va choralaridir¹¹.

Oddiy qilib aytganda, kiberxavfsizlik internet va boshqa raqamli texnologiyalar orqali yuzaga keladigan tahdidlar va hujumlardan shaxsiy hamda korporativ ma'lumotlarni, tizimlarni va infratuzilmani himoya qilishga qaratilgan.

Misollar:

- Antivirus dasturlari,
- Parol va shifrlash usullari,
- Tarmoq xavfsizligini ta'minlash vositalari,

¹⁰ Biryukov, A., & Khovratovich, D. (2017). Cybersecurity in blockchain technology: Challenges and solutions. *International Journal of Network Security*, 19(3), 451-461.

¹¹ Anderson, R. (2020). *Security engineering: A guide to building dependable distributed systems* (3rd ed.). Wiley.

- Kiberxurujlarni aniqlash va oldini olish tizimlari.

Kiberxavfsizlik bugungi kunda har qanday tashkilot va shaxs uchun juda muhim, chunki raqamli dunyo tobora kengayib, undagi tahdidlar ham ko‘paymoqda.

Kiberxavfsizlik sohasidagi muammolar zamonaviy axborot texnologiyalari rivojlanishi bilan chambarchas bog‘liq bo‘lib, ularning murakkabligi va ko‘lami tobora ortib bormoqda. Asosiy muammolardan biri sifatida tarmoq xavfsizligining yetarlicha ta‘minlanmasligi, ayniqsa kichik va o‘rta biznes subyektlarida kuzatiladi. Ko‘plab tashkilotlar moliyaviy va kadr resurslari yetishmasligi sababli zamonaviy xavfsizlik vositalarini joriy eta olmaydi, bu esa kiberhujumlarga nisbatan zaiflikni oshiradi.

Shuningdek, yangi turdagi tahdidlar — masalan, ransomware (shifrovchi viruslar), phishing (firibgarlik maqsadida ma‘lumotlarni o‘g‘irlash) va DDoS-hujumlar — doimiy ravishda rivojlanib, yanada murakkab shakl olmoqda. Bu holat esa xavfsizlik tizimlarini doimiy yangilab borishni va xodimlarning kiberxavfsizlik bo‘yicha muntazam o‘qitilishini talab qiladi. Ammo ko‘plab tashkilotlarda kiberxavfsizlik bo‘yicha malakali mutaxassislarning yetishmasligi dolzarb muammo hisoblanadi.

Sun‘iy intellekt (AI) va mashinani o‘rganish (ML) texnologiyalarini kiber xavfsizlik tadqiqotlariga kiritish raqamli tahdidlarni aniqlash va oldini olishda inqilob qildi. Ma‘lum kiber tahdidlarning keng ma‘lumotlar to‘plamida o‘qitilgan ML algoritmlari an‘anaviy usullar orqali aniqlash qiyin bo‘lgan naqsh va anomalialarni aniqlashga qodir. Masalan, sun‘iy intellekt bilan ishlaydigan tizimlar nol kunlik zaifliklarni aniqlash yoki zararli dasturlarning variantlarini xulq-atvor xususiyatlariga qarab tasniflash uchun tarmoq trafigini tahlil qilishi mumkin. Bashoratli modellar tadqiqotchilarga potentsial tahdidlarni taxmin qilish va oldini olish choralarini ko‘rish imkonini beradi va shu bilan muvaffaqiyatli hujumlar ehtimolini kamaytiradi. AI va ML texnologiyalarining integratsiyasi kiber tahdidlarning dinamik xususiyatiga javob berish qobiliyatining sezilarli o‘sishini anglatadi¹².

Ma‘lumotlarni yig‘ish jarayoni topilmalarning ishonchligi va haqiqiylikini ta‘minlash uchun puxta ishlab chiqilgan. Birlamchi ma‘lumotlar tarmoq jurnallari, tizim auditi yo‘llari va zararli dastur namunalaridan to‘planib, kiber hodisalar haqida bevosita ma‘lumot berdi. Ikkilamchi ma‘lumotlar kontekstli ma‘lumot va qiyosiy istiqbollarni taklif qiluvchi amaliy tadqiqotlar, sanoat hisobotlari va ekspertlar tomonidan ko‘rib chiqilgan nashrlarni o‘z ichiga olgan. Ma‘lumotlar

¹² Chen, T. M., & Zhao, H. (2018). Cybersecurity challenges in the era of AI and machine learning. *IEEE Security & Privacy*, 16(2), 50–55.

yig'ish atrofidagi axloqiy mulohazalar qat'iy rioya qilindi, maxfiy ma'lumotlarning maxfiyligi va yaxlitligini ta'minlash¹³.

Yana bir muhim masala – shaxsiy ma'lumotlar xavfsizligi. Raqamli xizmatlar ko'payishi bilan birga, shaxsiy ma'lumotlarning noqonuniy yig'ilishi va tarqalishi holatlari ham ko'paymoqda. Bu nafaqat foydalanuvchilarning ishonchini so'ndiradi, balki qonunchilik darajasida ham javobgarlik masalalarini keltirib chiqaradi. Shu sababli, shaxsiy ma'lumotlarni himoya qilishga oid qonunlarni takomillashtirish va ularni amaliyotda qat'iy qo'llash zarurati kuchaymoqda.

Muammolarni hal etishda davlat organlari, xususiy sektor va fuqarolik jamiyati o'rtasida samarali hamkorlik muhim ahamiyatga ega. Davlat tomonidan kiberxavfsizlik siyosatini shakllantirish, normativ-huquqiy bazani mustahkamlash va xodimlarni o'qitish dasturlarini amalga oshirish asosiy yo'nalish hisoblanadi. Shu bilan birga, zamonaviy texnologiyalar, xususan sun'iy intellekt va avtomatlashtirilgan tizimlar yordamida tahdidlarni tezda aniqlash va ularga qarshi tezkor choralar ko'rish imkoniyatlari kengaymoqda.

O'rganilgan ma'lumotlar va muhokamalar natijasida kiberxavfsizlik sohasida quyidagi asosiy natijalarga erishildi:

Kiberxavfsizlik muammolari ko'lami keng va murakkab ekanligi aniqlanmoqda. Raqamli infratuzilmaning jadal rivojlanishi bilan birga yangi turdagi tahdidlar paydo bo'lmoqda, bu esa xavfsizlik tizimlarini muntazam takomillashtirishni taqozo etadi. Ayniqsa, kichik va o'rta biznes subyektlari uchun xavfsizlik resurslarining yetishmasligi muhim zaiflik omili hisoblanadi¹⁴.

Shaxsiy ma'lumotlarni himoya qilish bo'yicha qonunchilik va amaliyotdagi bo'shliqlar mavjudligi ko'rsatildi. Bu holat foydalanuvchilar ma'lumotlarining noqonuniy tarqalishi va ularning huquqlarining buzilishiga olib kelmoqda. Qonunlarni takomillashtirish va ularni samarali amalga oshirish muhim ahamiyatga ega.

Texnologik yechimlar va innovatsiyalar kiberxavfsizlikni mustahkamlashda katta rol o'ynaydi. Sun'iy intellekt, avtomatlashtirilgan monitoring va blokcheyn kabi texnologiyalar yordamida kiberxavfsizlik tizimlarining samaradorligini oshirish mumkinligi aniqlanmoqda.

Kiberxavfsizlik sohasida malakali kadrlar yetishmovchiligi dolzarb muammo bo'lib qolmoqda. Bu esa tashkilotlarning samarali himoya choralari ko'rishiga to'sqinlik qilmoqda. Shu sababli, xodimlarni doimiy ravishda o'qitish va malaka oshirishga alohida e'tibor qaratish zarur.

¹³ Kshetri, N. (2017). 1 The Emerging Role of Big Data in Key Development Issues: Opportunities, Challenges, and Concerns. *Big Data for Development*, 1-21.

¹⁴ National Institute of Standards and Technology. (2018). *Framework for Improving Critical Infrastructure Cybersecurity* (Version 1.1).

Davlat va xususiy sektor o'rtasidagi hamkorlik kiberxavfsizlikni ta'minlashda muhim omil sifatida ajralib turadi. Normativ-huquqiy bazani takomillashtirish, davlat siyosatini shakllantirish va birgalikdagi loyihalarni amalga oshirish orqali kiberxavfsizlik sohasida sezilarli yutuqlarga erishish mumkin.

Kiberxavfsizlik sohasidagi dolzarb muammolarni hal etish uchun texnologik, huquqiy va ijtimoiy yondashuvlarni uyg'unlashtirish zarur. Zamonaviy texnologiyalarni joriy etish, qonunchilikni takomillashtirish, shuningdek, kadrlar malakasini oshirish bo'yicha chora-tadbirlarni amalga oshirish raqamli makonda ishonchli va xavfsiz muhit yaratishda muhim ahamiyatga ega. Shu bilan birga, davlat, xususiy sektor va jamiyat o'rtasidagi hamkorlikni mustahkamlash orqali kiberxavfsizlik sohasida yanada samarali natijalarga erishish mumkin.

Xulosa qilib aytganda, kiberxavfsizlik sohasidagi muammolarni kompleks tarzda hal etish uchun texnologik, huquqiy va ijtimoiy yondashuvlarning uyg'unligi talab etiladi. Innovatsion yechimlar va xalqaro tajriba asosida ishlab chiqilgan strategiyalar ushbu sohada samarali natijalarga erishishga yordam beradi.

1. Anderson, R. (2020). *Security engineering: A guide to building dependable distributed systems* (3rd ed.). Wiley.
2. Chen, T. M., & Zhao, H. (2018). Cybersecurity challenges in the era of AI and machine learning. *IEEE Security & Privacy*, 16(2), 50–55.
3. Kshetri, N. (2017). 1 The Emerging Role of Big Data in Key Development Issues: Opportunities, Challenges, and Concerns. *Big Data for Development*, 1-21.
4. National Institute of Standards and Technology. (2018). *Framework for Improving Critical Infrastructure Cybersecurity* (Version 1.1).
5. Biryukov, A., & Khovratovich, D. (2017). Cybersecurity in blockchain technology: Challenges and solutions. *International Journal of Network Security*, 19(3), 451-461. [https://doi.org/10.6633/IJNS.201703.19\(3\).11](https://doi.org/10.6633/IJNS.201703.19(3).11)

АХБОРОТ ТЕХНОЛОГИЯЛАРИДАН ФОЙДАЛАНГАН ҲОЛДА СОДИР ЭТИЛАДИГАН ҲУҚУҚБУЗАРЛИКЛАРНИНГ ОЛДИНИ ОЛИШ МАСАЛАЛАРИ

Бейсенов Кенжабай Сарсанбаевич

*ИИВ Малака ошириш институти Касбий тайёргарлик факултети
Махсус фанлар цикли ўқитувчиси э-mail: bisenovkenjaboy@gmail.com*

Аннотация. Ушбу мақолада ахборот технологиялари орқали амалга ошириладиган ҳуқуқбузарликлар турлари, уларнинг жамият ва шахс хавфсизлигига таъдиди, шунингдек, бундай жиноятларнинг олдини олиш

бўйича миллий ва халқаро тажрибалар таҳлил қилинади. Ахборот хавфсизлиги, киберҳимоя ва ҳуқуқий механизмларни такомиллаштириш зарурлигига алоҳида эътибор қаратилган.

Аннотация. в данной статье анализируются виды правонарушений, осуществляемых с помощью информационных технологий, их угроза безопасности общества и личности, а также национальные и международные эксперименты по предотвращению подобных преступлений. Особое внимание уделяется необходимости совершенствования информационной безопасности, киберпреступности и юридической механики.

Annotation. this article analyzes the types of violations carried out through Information Technology, their threat to the security of society and the individual, as well as national and international experiments on the Prevention of such crimes. Particular attention is paid to the need to improve information security, cybercrime and legal mechanics.

Tayanch so'zlar: ахборот технологиялари, фишинг, rahamli texnologiyalar, кибержиноятлар, kompyuter dasturlari, компьютер, интернет.

Ключевые слова: информационные технологии, фишинг, рахамические технологии, киберпреступность, компьютерное программное обеспечение, компьютер, интернет.

Base words: Information Technology, phishing, compassionate technologies, cybercrime, computer programs, computer, internet.

Жадал ривожланаётган ахборот технологиялари инсон ҳаётининг барча соҳаларига ўз таъсирини ўтказмоқда. Бироқ, бу жараён билан бир қаторда ахборот муҳитида ҳуқуқбузарликлар сони ҳам ортиб бормоқда. Хусусан, кибержиноятлар, шахсий маълумотларни ўғрилаш, электрон қаллоблик каби ҳолатлар ахборот технологияларидан нотўғри фойдаланиш натижасида юзага келмоқда¹⁵.

Ахборот технологиялари орқали содир этиладиган ҳуқуқбузарликлар

Ахборот технологиялари орқали содир этиладиган ҳуқуқбузарликлар куйидагиларни ўз ичига олади:

- Кибержиноятлар: Компьютер ва интернет орқали содир этиладиган жиноятлар, жумладан, дастурий таъминотга ноқонуний кириш, вирус тарқатиш, DDoS ҳужумлар¹⁶.

¹⁵ Сиддиқов А. "Ахборот технологиялари ва ҳуқуқбузарликлар". — Тошкент: "Юрист нашриёти", 2021.

¹⁶ Casey, Eoghan. *Digital Evidence and Computer Crime: Forensic Science, Computers and the Internet*. Academic Press, 2011.

• Кибержиноятлар бугунги ахборот асрида энг долзарб муаммолардан бирига айланган. Интернет ва рақамли технологияларнинг кенг тарқалиши орқали жиноятчилар янги имкониятларга эга бўлмоқдалар. Кибержиноятлар нафақат шахсий манфаатларга зарар етказди, балки миллий хавфсизлик, иқтисодий барқарорлик ва жамиятнинг умумий ахборот муҳитига ҳам таҳдид солади¹⁷.

Кибержиноятларнинг хавфли оқибатлари

Кибержиноят — бу ахборот технологияларидан, айниқса интернет, компьютер ёки бошқа рақамли қурилмалардан фойдаланган ҳолда содир этиладиган ноқонуний ҳаракатлар мажмуасидир¹⁸. Улар одатда қуйидаги мақсадларда амалга оширилади:

- Молиявий манфаат олиш;
- Маълумотларни ўғирлаш ёки йўқ қилиш;
- Ахборот тизимларини ишдан чиқариш;
- Давлат ёки хусусий ташкилотларга саботажю

Кибержиноятлар кўп қиррали бўлиб, улар қуйидагича таснифланади¹⁹:
Компьютерга ноқонуний кириш (hacking) — компьютер ёки тармоқ тизимига рухсатсиз кириш ва маълумотларга зиён етказиш.

Фишинг (phishing) — сохта веб-сайтлар ёки электрон хатлар орқали фойдаланувчилардан шахсий маълумотларни олиш.

Малваре тарқатиш — вирус, троян, ransomware ва бошқа зарарли дастурларни тарқатиш орқали зарар етказиш.

DDoS ҳужумлар — веб-сайтларни ёки серверларни кўп миқдордаги сунъий сўровлар орқали ишдан чиқариш.

Онлайн қаллоблик — сохта онлайн дўконлар, инвестиция схемалари ва бошқа алдамчилик усуллари.

Кибертерактлар — сиёсий ёки идеологик мақсадларда давлат ёки йирик ташкилотлар ахборот инфратузилмасига ҳужум қилиш²⁰.

Кибержиноятлар нафақат иқтисодий, балки ижтимоий ва сиёсий оқибатларга ҳам эга:

Шахсий маълумотларнинг ошкор бўлиши — фуқароларнинг шахсий ҳаётига аралашиш, уларга шантаж ва босим ўтказиш ҳолатлари.

Молиявий йўқотишлар — банк ҳисобларидан пул ўғирлаш, криптовалюта қаллобликлари.

¹⁷ Даниярова З.М. “Ахборот хавфсизлиги ва кибержиноятлар”, Тошкент, 2022.

¹⁸ Интерпол расмий сайти: “Cybercrime Overview” – <https://www.interpol.int>

¹⁹ Casey, E. *Digital Evidence and Computer Crime*, Academic Press, 2011.

²⁰ Stallings, W. *Network Security Essentials: Applications and Standards*, Pearson, 2016.

Корхоналар фаолиятига таҳдид — маълумотлар базасининг йўқолиши, мижозлар ишончининг пасайиши.

Миллий хавфсизликка таҳдид — давлат органларининг ахборот тизимларига ҳужумлар орқали маълумот ўғирлаш²¹.

Фишинг ва қаллоблик: Фойдаланувчиларни алдаш орқали уларнинг шахсий маълумотларини қўлга киритиш ва молиявий йўқотишларга олиб келади²².

Фишинг — бу кибержиноятнинг бир тури бўлиб, у сохта веб-сайтлар, электрон почталар, СМС ёки ижтимоий тармоқлар орқали фойдаланувчини алдаш ва ундан шахсий ёки молиявий маълумотларни (логин, парол, карта рақами ва бошқалар) олишга қаратилган амалиётдир²³.

Фишингнинг кенг тарқалган турлари:

- Spear phishing — муайян шахс ёки ташкилотга қаратилган, шахсийлаштирилган алдаш хати.
- Clone phishing — олдинги ҳақиқий хабарнинг клонин тайёрлаш орқали алдаш.
- SMS phishing (smishing) — мобил телефон орқали СМС ёки мессенжерлар орқали амалга ошириладиган алдаш.
- Voice phishing (vishing) — телефон орқали “банк ходими” ёки “ҳуқуқни муҳофаза қилувчи орган” номидан қўнғироқ қилиб, фойдаланувчини шубҳали операцияларга ишонтириш²⁴.

Онлайн қаллоблик шакллари

Фишингдан ташқари, ахборот муҳитидаги бошқа қаллоблик шакллари ҳам мавжуд. Уларга қуйидагилар киради:

- Сохта интернет дўконлар — арзон нархда товар таклиф қилиб, тўловдан сўнг алоқа узилиши.
- Понзи схемалари ва “инвестиция” лойиҳалари — фойдаланувчиларни тез фойда билан ўзига жалб қилиш ва маблағни ўғирлаш.
- Онлайн танишув қаллобликлари (romance scams) — ишонч қозониб, кейинчалик пул талаб қилиш.
- Нотўғри тўлов платформаларига йўналтириш — фойдаланувчини сохта тўлов саҳифаларига олиб бориш ва маълумотларни олиш²⁵.

Қаллоблик ва фишингнинг оқибатлари

Бундай жиноятлар натижасида:

²¹ Ўзбекистон Республикаси “Ахборот хавфсизлиги тўғрисида”ги Қонуни, 2020 йил 15 сентябрь.

²² Federal Trade Commission. “How to Recognize and Avoid Phishing Scams.” <https://consumer.ftc.gov>.

²³ Federal Trade Commission (FTC). “How to Recognize and Avoid Phishing Scams.” <https://consumer.ftc.gov/articles/how-recognize-and-avoid-phishing-scams>

²⁴ Europol. “Internet Organised Crime Threat Assessment (IOCTA) 2022.” <https://www.europol.europa.eu>

²⁵ Самадов Ш. “Замонавий интернет қаллобликлари ва кураш чоралари”, Тошкент, 2022.

- Фуқаролар шахсий маълумотларини йўқотади;
- Молиявий йўқотишларга учрайди;
- Корхоналарга зарар етказилади (ишонч пасайиши, тизимларга вирус тушиши);
- Ижтимоий ишончсизлик, давлат ва фуқаро ўртасидаги муносабатларга салбий таъсир кўрсатилади²⁶.

Олдини олиш чоралари

Аҳоли ва ходимларни хабардор қилиш — фишинг белгилари, эҳтиёт чоралари ҳақида мунтазам ўқув машғулоти ўтказиш.

Техник чоралар — антифишинг филтрлари, икки босқичли аутентификацияни жорий этиш.

Қонунчиликни кучайтириш — фишинг ва онлайн қаллобликка қарши махсус жиноят таркибларини жорий қилиш.

Фойдаланувчи хабардорлигини ошириш — расмий ташкилотлар ҳеч қачон парол ёки карта маълумотларини сўрамаслиги ҳақида тушунтиришлар бериш²⁷.

Шахсий маълумотларни бузиш: Ижтимоий тармоқларда ёки маълумот базаларида сақланадиган шахсий маълумотларнинг тарқалиши ёки ўғирланиши²⁸.

Оммавий хавф ва ҳуқуқий оқибатлар

Бундай ҳуқуқбузарликлар нафақат шахсий хавфсизлик, балки миллий хавфсизлик учун ҳам жиддий таҳдид солади. Шу боис, қатор мамлакатлар киберҳимоя соҳасида мустаҳкам ҳуқуқий база шакллантирмоқда. Ўзбекистонда ҳам 2020 йилда қабул қилинган “Ахборот хавфсизлиги тўғрисида”ги қонун ушбу соҳадаги ҳуқуқий муносабатларни тартибга солишда муҳим ўрин тутди²⁹.

Ҳуқуқбузарликларнинг олдини олишдаги чоралар

Қонунчиликни такомиллаштириш: Ахборот жиноятларига қарши курашишни таъминловчи аниқ ва қатъий ҳуқуқий асосларни яратиш.

Техник чоралар: Киберхавфсизлик тизимларини жорий этиш, firewall, antivirus, шифрлаш технологияларидан фойдаланиш³⁰.

Аҳолини хабардор қилиш: Интернет маданиятини ошириш, оммавий ахборот воситалари орқали профилактик тадбирлар ўтказиш.

²⁶ Stallings, William. *Network Security Essentials: Applications and Standards*, 6th ed., Pearson, 2016.

²⁷ Ўзбекистон Республикаси Жиноят кодекси, янги таҳрир, 2024 йил, 273-модда (ахборот технологиялари соҳасидаги қаллоблик).

²⁸ Самадов А. "Киберҳимоя ва маълумотлар хавфсизлиги", Тошкент, 2020.

²⁹ Ўзбекистон Республикаси Қонуни “Ахборот хавфсизлиги тўғрисида”, 2020 йил 15 сентябрь.

³⁰ Stallings, W. *Network Security Essentials: Applications and Standards*. Pearson Education, 2016.

Халқаро ҳамкорлик: Интерпол, ИТУ каби халқаро ташкилотлар билан ҳамкорликда ахборот жиноятларига қарши курашиш³¹.

Хулоса ўрнида, ахборот технологиялари инсон фаолиятини энгиллаштириш билан бирга, муайян хавф-хатарларни ҳам келтириб чиқаради. Шу боис, бу соҳадаги ҳуқуқбузарликларнинг олдини олишда комплекс ёндашув, яъни ҳуқуқий, техник ва тарғиботи усулларини биргаликда қўллаш муҳим аҳамиятга эга.

Фойдаланилган адабиётлар:

1. Сиддиқов А. "Ахборот технологиялари ва ҳуқуқбузарликлар". — Тошкент: "Юрист нашриёти", 2021.
2. Casey, Eoghan. *Digital Evidence and Computer Crime: Forensic Science, Computers and the Internet*. Academic Press, 2011.
3. Federal Trade Commission. "How to Recognize and Avoid Phishing Scams." <https://consumer.ftc.gov>.
4. Самадов А. "Киберҳимоя ва маълумотлар хавфсизлиги", Тошкент, 2020.
5. Ўзбекистон Республикаси Қонуни "Ахборот хавфсизлиги тўғрисида", 2020 йил 15 сентябрь.
6. Stallings, W. *Network Security Essentials: Applications and Standards*. Pearson Education, 2016.
7. Interpol. "Cybercrime Directorate." <https://www.interpol.int>
8. Даниярова З.М. "Ахборот хавфсизлиги ва кибержиноятлар", Тошкент, 2022.
9. Интерпол расмий сайти: "Cybercrime Overview" – <https://www.interpol.int>
10. Casey, E. *Digital Evidence and Computer Crime*, Academic Press, 2011.
11. Stallings, W. *Network Security Essentials: Applications and Standards*, Pearson, 2016.
12. Ўзбекистон Республикаси "Ахборот хавфсизлиги тўғрисида"ги Қонуни, 2020 йил 15 сентябрь.
13. Иброҳимов Қ. "Ахборот хавфсизлиги ва киберҳимоя", Тошкент, 2021.
14. Federal Trade Commission (FTC). "How to Recognize and Avoid Phishing Scams." <https://consumer.ftc.gov/articles/how-recognize-and-avoid-phishing-scams>
15. Europol. "Internet Organised Crime Threat Assessment (IOCTA) 2022." <https://www.europol.europa.eu>

³¹ Interpol. "Cybercrime Directorate." <https://www.interpol.int>

16. Самадов Ш. “Замонавий интернет қаллобликлари ва кураш чоралари”, Тошкент, 2022.

17. Stallings, William. *Network Security Essentials: Applications and Standards*, 6th ed., Pearson, 2016.

СУНЬИЙ ИНТЕЛЛЕКТНИНГ ҲАЁТИМИЗДАГИ АҲАМИЯТИ

Тасимов Нурмахан Зоиржанович

Ўзбекистон Республикаси Ички ишлар вазирлиги Малака ошириш институти Жанговар тайёргарлик цикли ўқитувчиси

Аннотация. Мақолада сунъий интеллект технологияларининг замонавий жамиятдаги аҳамияти ва таъсири ўрганилди. Сунъий интеллектнинг ижтимоий-иқтисодий соҳалардаги қўлланилиши, айниқса меҳнат бозори, тиббиёт, таълим ва медиа соҳаларидаги имкониятлари ҳамда хавфлари таҳлил қилинди. Шунингдек, Ўзбекистонда сунъий интеллектни ривожлантиришга қаратилган давлат сиёсати ва киберхавфсизлик муаммолари ҳам кўриб чиқилди. Мақола сунъий интеллектни тўғри ва оқилона жорий этишнинг долзарблигини таъкидлайди.

Калит сўзлар: Сунъий интеллект, ахборот технологиялари, меҳнат бозори, тиббиёт ва таълимда сунъий интеллект, киберхавфсизлик ва рақамли трансформация.

Ҳозирги замон ахборот технологиялари ва сунъий интеллектнинг ривожланиши ҳаётимизнинг барча соҳаларига катта таъсир кўрсатмоқда. Сунъий интеллект нафақат янги технологиялардан бири, балки ижтимоий ва иқтисодий соҳаларда мураккаб жараёнларни автоматлаштириш ва такомиллаштириш учун муҳим воситага айланди. Шунингдек, унинг тараққиёти янги имкониятлар билан бирга, айрим муаммолар ва хавф-хатарларни ҳам олиб келмоқда. Мақолада сунъий интеллектнинг ҳаётимизга таъсири, ижобий ва салбий томонлари ҳамда уни ривожлантириш ва қонуний тартибга солиш масалалари муҳокама қилинади.

Ахборот технологиялари ривожланиши натижасида сунъий интеллект реалликка айланди ва шиддат билан ҳаётимизга кириб келди. Ҳозирда биз фойдаланаётган кўплаб дастурлар, жумладан, мобиль қурилмаларнинг барчаси сунъий тафаккур маҳсулидир. Уларни яратиш ва йиғиш жараёнида ҳам махсус роботларнинг беминнат хизматидан фойдаланилади. Аниқроғи, бир роботни яратиш учун бошқа бир робот ишлатилади.

Шу ўринда савол туғилиши табиий. Сунъий интеллект одамлардан ишини тортиб олиб қўймайдими? Сунъий интеллектнинг ўзи одамларнинг ишини олиб қўймайди, лекин ундан унумли фойдалана оладиган бошқа

одамлар тортиб олиши мумкин. Сунъий интеллектнинг айнан ўзидан кўрқиш керак эмас, балки уни яхшилаб ўрганиш зарур бўлади. Бугунги кунда у айниқса медиа соҳасига шиддат билан кириб келди. Тасвир устида ишлаш, монтаж қилиш кабиларда қўл келяпти. Чет элда шу даражага чикдики, телевиденияда бошловчиларнинг сунъий интеллект шакли яратилиб, дастурлар олиб борилмоқда. Сунъий интеллектнинг салбий жиҳатлари борми? Бундай олиб қараганда, салбий томонлар ҳамма нарсада бор. Айтайлик, оддий пичоқдан ошхона анжоми сифатида, ҳам курол сифатида ҳам фойдаланиш мумкин. Сунъий интеллект ҳам нима мақсадда, кимнинг қўлида ишлатилишига қараб фойдали ёки зарарли бўлиши мумкин.

Яна шунга эътибор қаратиш лозимки, сунъий интеллект дунёдаги ҳар тўртинчи иш ўрнига таъсир кўрсатмоқда. Сунъий интеллект технологияларининг энг катта таъсири офис ишларига тўғри келади, чунки генератив сунъий интеллект кўплаб вазифаларни автоматлаштириш қобилиятига эга. Халқаро меҳнат ташкилоти ва Полша Миллий тадқиқот институти томонидан ўтказилган янги қўшма тадқиқотга кўра, сунъий интеллектдан фойдаланишнинг энг катта эҳтимолий натижаси – инсонни компьютер билан тўлиқ алмаштириш эмас, балки меҳнат жараёнининг трансформацияланиши бўлади.

Қайд этилишича, сунъий интеллект меҳнат бозорида эркаклар ва аёлларга турлича таъсир кўрсатади. Дунёдаги иш ўринларининг қарийб 25 % потенциал равишда сунъий интеллект таъсирига учрайди. Ривожланган давлатларда ушбу кўрсаткич 34 % га тенг. Шу билан бирга, унинг аёллар фаолиятига таъсир кўрсатиш эҳтимоли юқори. Сунъий интеллект турли соҳаларда, масалан, тиббиётда ҳам фойдали бўлиши мумкин. Тасаввур қилинг, махсус дастурга соғлиғингизга оид шикоятларни ёзиб берсангиз, у сизга ташхис қўяди. Яъни, қандай даволаниш йўллари кўрсатиб беради ва керакли шифокорга йўналтиради. Албатта, сунъий интеллект ҳақиқий шифокорларнинг ўрнини эгалламайди ва бу ҳақда ўзи ҳам айтади.

У касалингизни аниқлаб, даволаниш учун қайси шифокорга мурожаат қилишни тавсия қилади. Шунингдек, у мақолалар ёзишда, жуда йирик базадаги маълумотларни таҳлил қилишда қўл келади. Сунъий интеллект матнлар, суратлар, аудио ва видеолар генерациясида ёрдамчи вазифасини бажаради. Таълим соҳасида ҳам унинг ўрни жуда аҳамиятли. Масалан, ChatGPTга ойига муайян миқдорда пул тўлаб, обуна бўлиш катта фойда берди. У фарзандларингизга турли фанларда маълумотларни жуда ҳам яхши биладиган ўқитувчи бўлиши мумкин. Сунъий интеллект аввал боланинг фанни билиш даражасини аниқлайди ва ҳар бир болага мос дастурни тузиб беради, фанни ўргатади.

Юқорида таъкидлаганимиздек, сунъий интеллектнинг салбий томонлари ҳам бор. Масалан, таниқли шахсларнинг, тадбиркорларнинг юзлари ва овозларини ишлатиб, уларнинг қиёфасида одамлардан алдов йўли билан пул ундириш ҳолатлари бўлиши мумкин. Яъни, «Биз сизга кўп даромад қилиш йўллариини ўргатамиз, бунинг учун шу ҳаволага ўтинг ва мен сизга қандай бойиганимни ўргатаман», деган видеолар ижтимоий тармоқларда пайдо бўлмоқда. Бундай видеолар Фасебоок ва Инстаграмда кўп тарқалди. Афсуски, кўпчилик билмагани ва маълумотларни текшириш имкони бўлмагани учун алданиб, катта пулга чув тушиб қолаётгани ҳам ҳеч биримизга сир эмас. Ҳозир биз шунақа замонда яшайпмизки, ҳар бир кўрган нарсамизни албатта текширишимиз керак. Сунъий интеллект ёрдамида қонуний даромад олиш ҳам мумкин. Оддий мисол, дизайн соҳасида ишласангиз ёки бу соҳада таълимингиз бўлмаса ҳам, сунъий интеллектдан фойдаланиб сўзлар орқали логотиплар чизишингиз мумкин. Кейин уларни сотсангиз бўлади. Ёки контент яратиш даврида яшайпмиз. У контент яратишда ҳам жуда катта ёрдам беради.

Мамлакатимизда сунъий интеллектни янада ривожлантириш, деярли барча соҳага уни тадбив этиш мақсадида бир қанча меъёрий ҳужжатлар қабул қилинмоқда. Хусусан, Ўзбекистон Республикаси Президентининг 2024 йил 10 октябрь кундаги “Сунъий интеллект технологияларини 2030 йилга қадар ривожлантириш стратегиясини тасдиқлаш тўғрисида”ги ПҚ-358-сон Қарори қабул қилинган. Унда ижтимоий соҳа ва иқтисодиёт тармоқларида сунъий интеллект технологияларини жорий қилиш учун қулай шарт-шароитлар яратиш, мамлакатимизнинг сунъий интеллект технологияларидан фойдаланувчи дунёнинг етакчи давлатлари қаторига киришига эришиш, шунингдек, «Рақамли Ўзбекистон — 2030» Стратегиясида белгиланган мақсадлар ижросини таъминлаш мақсадида бир қатор вазифалар белгилаб берилган.

Бундан ташқари, Давлатимиз раҳбарининг 2025 йил 30 апрель кундаги “Ички ишлар органлари тизимини рақамли трансформация қилиш бўйича комплекс чора-тадбирлар тўғрисида”ги ПҚ-155-сон Қарори ҳам бугунги кунда долзарб аҳамиятга эга. Чунки ахборот технологияларининг ривожланиши, инсон ҳаётининг барча жабҳаларига кириб келиши қулайликлар билан бирга, янги таҳдидларни ҳам олиб келмоқда. Миллий сегментимизда киберхавфсизлик таҳдидлари ҳам параллель равишда ўсмоқда. Фирибгарлик йўли билан персонал, яъни шахсга доир маълумотларнинг ўғирланиши асосий таҳдидлардан бўлиб бормоқда. Бундай шароитда ички ишлар ходимларининг ахборот технологияларидан кенг

фойдаланишлари билан бир қаторда, улар ёрдамида амалга оширилган жиноятларга ҳам қарши курашиш вазифаси турибди.

Давлатимиз раҳбарининг юқорида тилга олинган қароридан ички ишлар органларини рақамли трансформация қилиш асосий устувор вазифа сифатида белгиланган. Соҳада киберхавфсизликни таъминлаш, жиноятларга қарши курашиш йўналишида сунъий интеллект ва ахборот технологиялари имкониятларидан кенг фойдаланиш назарда тутилганлиги билан ҳам бу қарор аҳамиятлидир.

Хулоса қилиб айтганда, сунъий интеллектнинг зараридан фойдаси кўп, албатта. Фақат ундан тўғри, оқилона жойдаланиш лозим. Ҳозирда кўп такрорланаётганидек, у кўрқинчли ва чеклаб қўйиладиган хавф эмас. Уни инсон бошқарувидан чиқариб юбормаслик керак. Бироқ нима бўлганда ҳам, унга онгли мавжудот сифатида қараш нотўғри. Чунки у улкан имкониятларга эга бўлсада, инсон томонидан ихтиро қилинганлигини унутмаслигимиз керак.

Фойдаланилган адабиётлар рўйхати:

1. Ўзбекистон Республикаси Президентининг 2024 йил 10 октябрь кундаги “Сунъий интеллект технологияларини 2030 йилга қадар ривожлантириш стратегиясини тасдиқлаш тўғрисида”ги ПҚ-358-сон Қарори.
2. Ўзбекистон Республикаси Президентининг 2025 йил 30 апрель кундаги “Ички ишлар органлари тизимини рақамли трансформация қилиш бўйича комплекс чора-тадбирлар тўғрисида”ги ПҚ-155-сон Қарори.
3. Халқаро меҳнат ташкилоти ва Полша Миллий тадқиқот институтининг “Сунъий интеллектнинг меҳнат бозорига таъсири” бўйича қўшма тадқиқоти.
4. Жаҳон ахборот технологиялари ва сунъий интеллект соҳасидаги замонавий илмий мақолалар ва таҳлиллар.

KIBERJINOYATLARGA QARSHI KURASHISHDA ZAMONAVIY TEKNOLOGIYALARNING ROLI: SUN'IY INTELLEKT VA BLOKCHeyN TEKNOLOGIYALARI

Muslimov Xusan Nishonboyevich

O'zbekiston Respublikasi Ichki ishlar vazirligi Malaka oshirish instituti Jangovar tayyorgarlik sikli o'qituvchisi

Bugungi kunda axborot texnologiyalari tez sur'atlarda rivojlanib borayotgani bilan birga, kiberjinoyatlar ham global xavf sifatida tobora ko'payib bormoqda. Internet tarmoqlari va raqamli xizmatlarning kengayishi kiberxavfsizlik muammolarini yanada murakkablashtiradi, natijada zararli dasturlar, firibgarlik, ma'lumotlarni o'g'irlash kabi jinoyatlar ko'paymoqda. Shu sababli

kiberjinoyatlarga qarshi samarali kurashish uchun yangi va ilg'or texnologiyalarni qo'llash zarurati yuzaga kelmoqda.

Sun'iy intellekt (SI) va blokcheyn texnologiyalari zamonaviy kiberxavfsizlik sohasida innovatsion vositalar sifatida katta ahamiyat kasb etmoqda. Sun'iy intellekt yordamida kiberxurujlarni aniqlash va oldini olish, avtomatlashtirilgan xavfsizlik tizimlarini yaratish imkoniyati kengaymoqda. Shu bilan birga, blokcheyn texnologiyasi ma'lumotlar xavfsizligi, ularning o'zgartirilmasligi va shaffofligini ta'minlashda yangi imkoniyatlar yaratmoqda.

Ushbu maqolada kiberjinoyatlarga qarshi kurashishda sun'iy intellekt va blokcheyn texnologiyalarining roli tahlil qilinib, ularning samaradorligi hamda amaliy qo'llanilish yo'llari ko'rib chiqiladi.

Sun'iy intellekt kiberxavfsizlik sohasida xavf-xatarlarni aniqlash, ularga javob berish va oldini olishda samarali vosita sifatida keng qo'llanilmoqda. Bugungi kunda kiberhujumlar murakkab va tezkor tarzda amalga oshirilayotgani sababli, sun'iy intellekt kiberxavfsizlikni ta'minlashda juda muhim rol o'ynaydi. Quyida sun'iy intellekt texnologiyasining kiberxavfsizlikdagi asosiy qo'llanilish yo'nalishlari ko'rib chiqiladi:

1. Xavfni aniqlash va tahlil qilish. Sun'iy intellekt tizimlari kiberxavfsizlikda eng samarali xavf-xatarlarni aniqlash va tahlil qilish vositalaridan biridir. Sun'iy intellekt algoritmlari, foydalanuvchi faoliyatini va tarmoqdagi trafikni doimiy ravishda kuzatib boradi va odatiy holatlardan og'ishlarni tezda aniqlaydi. Bu tizimlar yirik ma'lumotlar bazalaridan foydalanib, zararli harakatlarni yoki tahdidlarni erta bosqichda sezadi, bu esa kiberhujumlarga qarshi tezkor choralar ko'rish imkonini beradi. Masalan, AQShdagi moliyaviy kompaniyada sun'iy intellekt real vaqt rejimida kiberhujumni aniqlab, uni dastlabki bosqichdayoq to'xtatishga yordam bergan. Bugungi kunda Darktrace kabi tizimlar 110 dan ortiq mamlakatda minglab tashkilotlarni xuddi shunday real vaqt rejimida himoya qilmoqda.

2. Zararli dasturlarni aniqlash. Sun'iy intellekt zararli dasturlarni aniqlashda keng qo'llaniladi. Traditsion antivirus dasturlari faqat ma'lum bir zararli dasturlarni aniqlay oladi, lekin sun'iy intellekt tizimlari yangi va ilgari noma'lum zararli dasturlarni o'z-o'zini o'rgatish asosida aniqlash imkoniyatiga ega. Sun'iy intellekt yordamida, zararli dasturlar tizimga kirish usulini va uning qanday faoliyat yuritishini o'rganadi, bu esa unga mutatsiyalangan yoki yangi turdagi zararli dasturlarni oldindan aniqlash imkonini beradi. Sun'iy intellektning o'rganish qobiliyati tizimni doimiy ravishda yangilab boradi va tahdidlarni yangi shakllariga moslashishga yordam beradi. Sun'iy intellekt asosidagi Cylance kabi tizimlar WannaCry kabi global tahdidlarni tahlil qilib, yangi mutatsiyalangan versiyalarini oldindan aniqlash imkonini bergan. Tadqiqotlarga ko'ra, sun'iy

intellekt asosidagi antiviruslar an'anaviy antiviruslarga qaraganda 60% ko'proq yangi tahdidlarni erta aniqlaydi³².

3. Phishing hujumlarini oldini olish. Phishing hujumlari kiberjinoyatchilar tomonidan foydalanuvchilarni aldanishga undash uchun ishlatiladi. Sun'iy intellekt tizimlari foydalanuvchi xatti-harakatlarini tahlil qilish va shubhali xabarlar yoki havolalarni avtomatik tarzda aniqlash imkoniyatiga ega. Shuningdek, phishing hujumlariga oid ilg'or usullarni (masalan, soxta veb-saytlar yoki manipulyatsiya qilingan email xabarlar) avtomatik tarzda identifikatsiya qilishda sun'iy intellekt tizimlarining o'z-o'zini o'rgatish funksiyasi yordam beradi. Bunda sun'iy intellekt foydalanuvchini ogohlantirishi yoki xabarni avtomatik tarzda bloklashi mumkin. Shu bilan birga, Google sun'iy intellekti 2021-yilda Gmail orqali yuborilgan 100 milliondan ortiq phishing xabarlarini avtomatik ravishda bloklagan. Bugungi kunda Gmail AI tizimi phishing hujumlarini 99,9% aniqlik bilan aniqlay oladi.

4. Avtomatik javob va reaksiya. Kiberxavfsizlikni ta'minlashda sun'iy intellektning asosiy afzalliklaridan biri uning avtomatik javob berish imkoniyatidir. Kiberhujumlar aniqlangach, Sun'iy intellekt tizimlari avtomatik tarzda zarur choralarni ko'rishga o'rgatilgan. Masalan, tizimga kirish urinishlarini bloklash, zararli dasturlarni o'chirish yoki zarar ko'rgan tizimni izolyatsiya qilish kabi chora-tadbirlar Sun'iy intellekt tomonidan tezkor amalga oshiriladi. Inson aralashuvisiz amalga oshiriladigan bu jarayonlar, kiberhujumlarni oldini olishda samarali bo'lib, tizimning uzluksiz ishlashini ta'minlaydi. Bunday avtomatik javoblar nafaqat vaqtni tejaydi, balki kiberxavfsizlikning yanada samarali boshqarilishini ta'minlaydi³³.

Shuningdek, Microsoftning Azure Sentinel tizimi sun'iy intellekt yordamida hujumlarni aniqlagandan so'ng, zararli trafikni bloklash, shubhali qurilmalarni ajratish va xavf darajasini baholash kabi chora-tadbirlarni avtomatik ravishda amalga oshiradi. Shunday tizimlar kiberhujumlarga javob berish samaradorligini 70% ga oshirgan. So'nggi yillarda sun'iy intellekt texnologiyalari kiberxavfsizlik sohasida samarali vosita sifatida faol qo'llanilmoqda. Xususan, turli mamlakatlarda sun'iy intellekt asosida kiberjinoyatchilikka qarshi kurashish bo'yicha aniq natijalarga erishilmoqda. 2024-yilga oid quyidagi tahliliy ma'lumotlar sun'iy intellekt texnologiyalarining kiberxavfsizlikda tutgan o'rnini yaqqol namoyon etadi³⁴.

³² Mirzayev Sh. R. (2024). Kiberxavfsizlik sohasida sun'iy intellekt va blokcheyn texnologiyalarini qo'llash imkoniyatlari. *Science and innovation*, 3(Special Issue 42), 179-185.

³³ Giyazova, N.B. (2024). Zamonaviy raqamli iqtisodiyotdagi muammolar va chora-tadbirlar. *Science and innovation*, 3(Special Issue 42), 482-489

³⁴ Shukhratovna, U. M., & Bayazovna, G. N. (2025). Foreign experience in the development of mobile internet. *innovation in the modern education system*, 6(49), 250-256.

2024-yil uchun mamlakatlar kesimida sun'iy intellektning kiberxavfsizlik sohasidagi qo'llanilishi va oldini olish natijalari jadval shaklida tayyorlandi:

Mamlakat	Sun'iy intellekt qo'llanilish sohasi	Oldini olish natijalari (asosiy ko'rsatkichlar)
AQSh	Kiberhujumlarni aniqlash, tahdidlarni bashorat qilish, avtomatlashtirilgan xavfsizlik tizimlari	Kiberhujumlar soni 25% ga kamaydi; xakerlik hujumlarini 40% aniqlash darajasi oshdi
Xitoy	Ma'lumotlarni tahlil qilish, tarmoq monitoringi, kiberjinoyatlarni tez aniqlash	Kiberjinoyatlar 30% kamaydi; sun'iy intellekt yordamida zararli dasturlarni aniqlash 35% ga oshdi
Germaniya	Korxonada xavfsizligi, foydalanuvchi autentifikatsiyasi, tahdidlarni prognoz qilish	Ma'lumotlar buzilish holatlari 20% ga kamaydi; kiberxavfsizlik insidentlari 25% ga pasaydi
Janubiy Koreya	IoT qurilmalarining himoyasi, tarmoq xavfsizligi, real vaqt monitoring	IoT qurilmalariga hujumlar 28% ga kamaydi; xavfsizlik signalining aniqligi 38% ga oshdi
Buyuk Britaniya	Moliyaviy sektorni himoya qilish, sun'iy intellekt asosida firibgarlikni aniqlash	Moliyaviy firibgarlik holatlari 22% ga kamaydi; real vaqt tahdidlarni aniqlash 33% ga oshdi ³⁵

Blokcheyn texnologiyasi kiberxavfsizlikni ta'minlashda samarali vosita sifatida qabul qilinmoqda. Uning asosiy afzalliklari, ya'ni ma'lumotlarni o'zgartirishning imkonsizligi, shaffoflik va ishonchlilik, kiberxavfsizlikni mustahkamlashda katta rol o'ynaydi. Blokcheyn texnologiyasi ma'lumotlarning xavfsizligini ta'minlashda bir qator imkoniyatlar yaratadi. Quyida blokcheynning kiberxavfsizlikda qo'llanilishining asosiy yo'nalishlari ko'rib chiqiladi:

1. Ma'lumotlar integritetini ta'minlash. Blokcheyn texnologiyasining asosiy afzalligi uning o'zgartirilmasligi hisoblanadi. Har bir blok o'zaro kriptografik bog'lanishlar bilan ulanib, tizimdagi ma'lumotlar ishonchliligini ta'minlaydi. Blokcheyn orqali ma'lumotlarni soxtalashtirish yoki o'zgartirish deyarli imkonsiz bo'ladi, bu esa kiberxavfsizlikni kuchaytiradi. Misol uchun, Walmart o'zining ta'minot zanjirini boshqarishda blokcheyn texnologiyasidan foydalanadi. Har bir

³⁵ International Telecommunication Union. (2024). *Global cybersecurity index 2024*. ITU Publications. <https://www.itu.int/en/ITU-D/Cybersecurity/Pages/GCI.aspx>.

mahsulotning kelib chiqishi va yetkazib berish jarayonidagi har bir qadam blokcheynga yoziladi. Agar mahsulot sifati bo'yicha muammo chiqsa, Walmart bir necha soniya ichida uning manbasini aniqlay oladi³⁶.

2. Decentralizatsiya va xavfsizlik. Blokcheynning markazlashtirilmagan tuzilishi tizimni yanada xavfsiz qiladi. Ma'lumotlar bir nechta joyda saqlanadi, bu esa tizimga kirish va ma'lumotlarni o'g'irlashni qiyinlashtiradi. Markazlashtirilgan tizimlarga nisbatan blokcheynning decentralizatsiya qilingan strukturasi biror qismning buzilishi butun tizimga zarar yetkazmaydi. Blokcheyn tarmoqlariga hujum qilish uchun kiberjinoyatchilar tarmoq quvvatining kamida 51% ini egallashi kerak. Bu esa katta energiya va resurs talab qiladi, shuning uchun blokcheyn tizimlariga bo'lgan muvaffaqiyatli hujumlar darajasi an'anaviy markazlashgan tizimlarga nisbatan 90% kam.

3. Xavfsiz autentifikatsiya va identifikatsiya. Blokcheyn foydalanuvchi identifikatsiyasini xavfsiz va ishonchli tarzda amalga oshirish imkonini beradi. Kriptografik kalitlar yordamida foydalanuvchilarni tasdiqlash jarayoni an'anaviy tizimlarga nisbatan yanada xavfsizdir, bu esa "account takeover" kabi hujumlarga qarshi samarali himoya yaratadi. Bunga qo'shimcha, Microsoft o'zining Azure Active Directory (Azure AD) tizimiga blokcheyn asosida Decentralized Identity funksiyasini qo'shgan. Bu funksiyada foydalanuvchilar o'z shaxsiy ma'lumotlarini blokcheynga joylashtirib, nazoratni o'z qo'lida saqlaydi³⁷.

4. Smart kontraktlar va avtomatik shartnomalar. Blokcheyn asosidagi smart kontraktlar taraflar o'rtasidagi shartnomalarni avtomatik tarzda bajarilishini kafolatlaydi. Shartnomalar blokcheynda xavfsiz tarzda saqlanadi va barcha harakatlar tasdiqlanishi kerak, bu esa shaffoflikni ta'minlab, soxtalashtirish va manipulyatsiya qilish imkoniyatlarini kamaytiradi. Shuningdek, Siemens smart kontraktlar orqali logistika va yuk tashish jarayonlarini avtomatlashtirishda blokcheyn texnologiyasidan foydalanilmoqda. Yuk jo'natish va qabul qilish shartlari to'liq bajarilgandagina to'lov amalga oshiriladi, bu ishonchli va xavfsiz hamkorlik uchun zamin yaratadi. Smart kontraktlar asosidagi tizimlar 2023-yilda xalqaro savdoda hujjatlarni soxtalashtirish holatlarini 70% ga kamaytirgan. Blokcheyn hamyon foydalanuvchilari sonining keskin o'sishi (2016 yilda 10 mln.dan 2021 yilda 80 mln.ga) kiberxavfsizlik tahdidlarini oshirdi. Bu phishing hujumlari, kalitlarni o'g'irlash va firibgarlik kabi xatarlarning ko'payishiga olib keldi. Foydalanuvchilarni himoya qilish uchun ikki bosqichli autentifikatsiya,

³⁶ Rustam o'g'li, R. J., & Bayazovna, G. N. (2025). Mobil to'lovlar va ularning iqtisodiyotdagi ahamiyati. *The theory of recent scientific research in the field of pedagogy*, 3(30), 193-197.

³⁷ Sayfullayeva, M. (2023). Establishment Of Agritourism Clusters In Uzbekistan Based On The Principles Of Sustainable Tourism. *Центр научных публикаций (Buxdu. Uz)*, 35(35).

apparat hamyonlari va xavfsizlik bo'yicha xabardorlikni talab qiladi. Blockcheyn tizimining kengayishi bilan xavfsizlikni ta'minlash ustuvor vazifa bo'lib qolyapti.

Xulosa qilib aytganda, bugungi globallashgan dunyoda raqamli texnologiyalarning keng qo'llanilishi yangi imkoniyatlar yaratish bilan birga, turli xavf-xatarlarni ham yuzaga keltirmoqda. Kiberxavfsizlik nafaqat texnologik, balki strategik ahamiyatga ega bo'lib, uning to'g'ri boshqarilishi iqtisodiyot barqarorligi va rivojlanishi uchun muhimdir. Sun'iy intellekt va blokcheyn texnologiyalari kabi ilg'or texnologiyalar kiberxavfsizlik sohasida yangi ufqlarni ochmoqda. Sun'iy intellekt xavf-xatarlarni aniqlash va ularga tezkor javob berishda samarali vosita bo'lib, zararli dasturlarni aniqlash va phishing hujumlarini oldini olish kabi yo'nalishlarda muvaffaqiyatli qo'llanilmoqda. Blokcheyn texnologiyasi esa ma'lumotlarning yaxlitligi va ishonchliligini ta'minlash, decentralizatsiya orqali tizimlarni mustahkamlash hamda xavfsiz autentifikatsiya kabi muhim imkoniyatlarni taqdim etadi.

1. Mirzayev Sh. R. (2024). Kiberxavfsizlik sohasida sun'iy intellekt va blokcheyn texnologiyalarini qo'llash imkoniyatlari. *Science and innovation*, 3(Special Issue 42), 179-185.

2. Giyazova, N.B. (2024). Zamonaviy raqamli iqtisodiyotdagi muammolar va chora-tadbirlar. *Science and innovation*, 3(Special Issue 42), 482-489.

3. Shukhratovna, U. M., & Bayazovna, G. N. (2025). Foreign experience in the development of mobile internet. *innovation in the modern education system*, 6(49), 250-256.

4. Rustam o'g'li, R. J., & Bayazovna, G. N. (2025). Mobil to'lovlar va ularning iqtisodiyotdagi ahamiyati. *The theory of recent scientific research in the field of pedagogy*, 3(30), 193-197.

5. Sayfullayeva, M. (2023). Establishment Of Agritourism Clusters In Uzbekistan Based On The Principles Of Sustainable Tourism. *Центр научных публикаций (Buxdu. Uz)*, 35(35).

6. International Telecommunication Union. (2024). *Global cybersecurity index 2024*. ITU Publications. <https://www.itu.int/en/ITU-D/Cybersecurity/Pages/GCI.aspx>.

JINOYATCHILARNING YASHIRINGAN JOYLARINI AXBOROT TEXNOLOGIYALARI YORDAMIDA ANIQLASH USULI

O‘rinxojayev Hondamir Nematjonovich

*IIV Malaka oshirish instituti, KTF Jangovar va jismoniy tayyorgarlik sikli
o‘qituvchisi*

Annotatsiya. Mazkur tezisda jinoyatchilarning yashiringan joylarini aniqlashda axborot texnologiyalari (AT)dan foydalanishning samarali usullari va zamonaviy metodlari tahlil qilingan. Axborot texnologiyalarining jinoyatchilarni qidirishdagi roli, ularning monitoring, geolokatsiya va ma'lumotlarni qayta ishlash vositalari orqali aniqlash jarayonlari tavsiflangan. Shuningdek, aniqlash samaradorligini oshirishga qaratilgan yangi texnologiyalar va algoritmlar tahlili taqdim etildi.

Kalit so‘zlar: Jinoyatchilar, yashiringan joy, axborot texnologiyalari, geolokatsiya, monitoring, ma'lumotlarni qayta ishlash, aniqlash usullari.

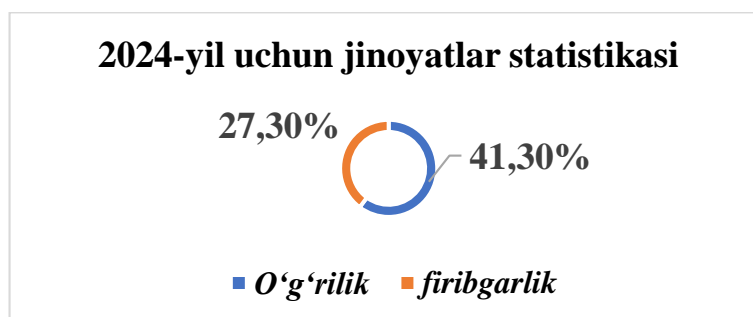
Bugungi kunda jamiyatimizda dolzarb muammolari qatoriga jinoyatchilikning zamonaviy turlari kirib kelmoqda. Jinoyatchilarni aniqlash va ularni yashiringan joylarini topish – Ichki ishlar sohasidagi muhim vazifadir. Zamonaviy dunyoda axborot texnologiyalari turli sohalarda katta o‘rin egallamoqda. Jinoyatchilarni qidirishda ham axborot texnologiyalaridan samarali foydalanish imkoniyatlari ko‘paymoqda. Ushbu tezisda jinoyatchilarning yashiringan joylarini aniqlashda axborot texnologiyalarining qo‘llanilishi va bu sohadagi ilg‘or usullar muhokama qilinadi

Jinoyatchi – mazkur shaxs huquq-tartibot tizimida jazolanadigan jinoyat qilgan yoki jinoyatga aloqador bo‘lgan shaxs sifatida ta’riflanadi. O‘zbekiston Respublikasining Jinoyat kodeksi 15-moddasida jinoyatchi tushunchasi aniq belgilangan bo‘lib, unda jinoyat qilgan shaxsga nisbatan qonuniy choralar qo‘llanilishi nazarda tutiladi.[1] Madaniyat va jamiyat tartib-qoidalari asosida jinoyatchi faoliyati jamiyat xavfsizligiga, shaxslar huquq va erkinliklariga zarar yetkazadi.

Axborot texnologiyalari jinoyatchilarni aniqlash va ularning faoliyatini kuzatishda muhim rol o‘ynaydi. Ichki ishlar tizimida jinoyatchilarning internet va boshqa elektron tarmoqlardagi faoliyatini monitoring qilish, ularning yashiringan joylari va harakatlarini aniqlashda qo‘llaniladi.

Shu tariqa, axborot texnologiyalari va MJTKA jinoyatchilarni aniqlashda zamonaviy huquqiy asos bo‘lib xizmat qiladi, JKda belgilangan normalarga muvofiq jinoyatchilikka qarshi kurashishni samarali yo‘lga qo‘yish imkonini beradi.

- ✓ Axborot tizimlari va ma'lumotlar bazasini tahlil qilish;
- ✓ Geolokatsiya va GPS texnologiyalarini qo'llash;
- ✓ Kameralar va monitoring tizimlari orqali videojavoblar tahlili;
- ✓ Mobil qurilmalardan va internet tarmog'idan olingan ma'lumotlarni tahlil qilish;
- ✓ Mashina o'rganish (machine learning) algoritmlari yordamida ma'lumotlarni klassifikatsiya qilish va aniqlash.[2]



1-rasm. Jinoyatchilik statistikasi

Tadqiqot ko'rsatdiki, axborot texnologiyalari jinoyatchilarni yashiringan joylarini aniqlashda yuqori samaradorlikka ega. Geolokatsiya tizimlari va video monitoring integratsiyasi aniqlik darajasini sezilarli oshiradi. Mashina o'rganish algoritmlari ma'lumotlarni tez va aniq tahlil qilishga yordam beradi. Shu bilan birga, axborot xavfsizligi va shaxsiy ma'lumotlarni himoya qilish masalalariga katta e'tibor qaratilsa, texnologiyalarni qo'llash samaradorligi yanada oshadi.[3-4]

Jinoyatchilarni yashiringan joyini aniqlash jarayonida axborot texnologiyalarining qo'llanilishi turli jihatdan afzalliklar beradi. Masalan, geolokatsiya ma'lumotlari orqali tezkor aniqlash imkoniyati paydo bo'ladi. Shu bilan birga, ma'lumotlarni avtomatik qayta ishlash va tahlil qilish orqali katta hajmdagi ma'lumotlardan samarali foydalanish mumkin. Lekin, bu texnologiyalarni qo'llashda xususiylik va axloqiy masalalar ham e'tibordan chetda qolmasligi kerak.

Axborot texnologiyalari jinoyatchilarni yashiringan joylarni aniqlashda muhim ahamiyatga ega. Hozirgi kunda bu sohada yangi texnologiyalar va algoritmlar ishlab chiqilmoqda, ular huquq-tartibot tizimlarini zamonaviylashtirishga xizmat qiladi. Tadqiqot natijalari shuni ko'rsatadiki, axborot texnologiyalari va geolokatsiya usullarini kompleks qo'llash jinoyatchilarni tez va aniq aniqlash imkoniyatini beradi. Kelgusida ushbu texnologiyalarning yanada takomillashtirilishi va etik jihatdan to'g'ri qo'llanilishi ustuvor vazifa hisoblanadi.[5]

Foydalanilgan adabiyotlar:

1. Axborot texnologiyalari va huquq-tartibot sohasidagi zamonaviy trendlar. Toshkent, 2023.
2. Geolocation technologies and criminal tracking: a review. Journal of Security Studies, 2022.
3. Mashina o'rganishning huquqiy sohada qo'llanilishi. Moskva, 2021.
4. Videomonitoring va axborot xavfsizligi. Samara, 2020.
5. Ethical considerations in data privacy for law enforcement. International Journal of Ethics, 2024.

OLIV TA'LIM MUASSASALARIDA LOYIHAVIY BOSHQARUVNI JORIY ETISH ZARURATI

Matyaqubova Firuza Baxodirovna

*Ichki ishlar vazirligi Malaka oshirish instituti Kasbiy tayyorgarlik sikli
o'qituvchisi*

Abstract. This article analyzes the necessity of implementing project management in higher education institutions. Project management is considered an innovative management model that enhances the quality of education, promotes scientific research, improves infrastructure, and ensures the efficient use of resources. The article comprehensively explores the advantages of this system, its implementation principles, and its impact on the development of higher education institutions. The study results indicate that adopting project management contributes to increasing the effectiveness of the educational process and strengthening universities' positions in international rankings.

Key words: higher education, project management, education quality, innovative management, scientific research, infrastructure, resource management, international ranking, university development, strategic planning.

Аннотация. В данной статье анализируется необходимость внедрения проектного управления в высших учебных заведениях. Проектное управление рассматривается как инновационная модель управления, которая способствует повышению качества образования, развитию научных исследований, совершенствованию инфраструктуры и эффективному использованию ресурсов. В статье подробно рассматриваются преимущества данной системы, принципы её внедрения и влияние на развитие высших учебных заведений. Результаты исследования показывают, что применение проектного управления способствует повышению эффективности

образовательного процесса и укреплению позиций университетов в международных рейтингах.

Ключевые слова: высшее образование, проектное управление, качество образования, инновационное управление, научные исследования, инфраструктура, управление ресурсами, международный рейтинг, развитие университета, стратегическое планирование.

Аннотация. Ushbu maqolada oliy ta'lim muassasalarida loyihaviy boshqaruv tizimini joriy etishning dolzarbligi tahlil qilinadi. Loyihaviy boshqaruv ta'lim sifatini oshirish, ilmiy-tadqiqot ishlarini rivojlantirish, infratuzilmani takomillashtirish va resurslardan samarali foydalanish imkonini beruvchi innovatsion boshqaruv modeli sifatida qaraladi. Maqolada ushbu tizimning afzalliklari, joriy etish tamoyillari va oliy ta'lim muassasalarining rivojlanishiga ta'siri keng yoritilgan. Tadqiqot natijalari loyihaviy boshqaruvni amalga oshirish ta'lim jarayonining samaradorligini oshirish va universitetlarning xalqaro reytinglardagi mavqeini mustahkamlashga xizmat qilishini ko'rsatadi.

Калит so'zlar: oliy ta'lim, loyihaviy boshqaruv, ta'lim sifati, innovatsion boshqaruv, ilmiy-tadqiqot, infratuzilma, resurslarni boshqarish, xalqaro reyting, universitet rivojlanishi, strategik rejalashtirish.

Zamonaviy dunyoda ta'lim tizimi doimiy rivojlanish va yangilanish jarayonida bo'lib, oliy ta'lim muassasalari oldida samaradorlikni oshirish, resurslardan oqilona foydalanish va xalqaro maydonda raqobatbardoshlikni ta'minlash kabi muhim vazifalar turibdi. Shu sababli, loyihaviy boshqaruv tizimini joriy etish bugungi kun talabi bo'lib, ta'lim jarayonini takomillashtirish va innovatsion rivojlanishga erishishda samarali vosita hisoblanadi.

Loyihaviy boshqaruv deganda, aniq maqsadga yo'naltirilgan, vaqt va resurslar doirasida amalga oshiriladigan boshqaruv tizimi tushuniladi. Bu tizim ta'lim muassasalarining strategik maqsadlariga erishish, innovatsion loyihalarni yo'lga qo'yish va ularni sifatli amalga oshirish imkonini beradi. Oliy ta'lim muassasalarida loyihaviy boshqaruvni joriy etish bir qancha yo'nalishlarda muhim ahamiyat kasb etadi. Birinchidan, ta'lim sifatini oshirishga xizmat qiladi. Chunki loyihaviy boshqaruv yangi o'quv dasturlarini ishlab chiqish, innovatsion pedagogik texnologiyalarni joriy etish va professor-o'qituvchilar malakasini oshirish kabi jarayonlarni tizimli tashkil etishga imkon yaratadi. Ikkinchidan, ilmiy-tadqiqot faoliyatini rivojlantirishga yordam beradi. Universitetlarda grantlar, innovatsion tadqiqotlar va xalqaro hamkorlik asosida olib boriladigan loyihalarni samarali boshqarish orqali ilmiy ishlarning natijadorligini oshirish mumkin bo'ladi.

Bundan tashqari, loyihaviy boshqaruv universitet infratuzilmasini rivojlantirishda ham muhim rol o'ynaydi. Masalan, zamonaviy laboratoriyalar,

raqamli kutubxonalar, tadqiqot markazlari va boshqa ta'lim resurslarini yaratish loyihalari oliy ta'lim muassasalarining jahon standartlariga moslashishiga xizmat qiladi. Shu bilan birga, loyihaviy boshqaruv ta'lim muassasalarining moliyaviy barqarorligini ta'minlash, resurslardan samarali foydalanish va mablag'larni maqsadli yo'naltirish imkonini beradi.

Loyihaviy boshqaruvni joriy etishda bir nechta muhim tamoyillarga amal qilish zarur. Bularga aniq maqsadni belgilash, samarali rejalashtirish, resurslarni to'g'ri taqsimlash, monitoring va baholash, xavflarni boshqarish hamda jamoaviy ishlash kiradi. Agar ushbu tamoyillar asosida oliy ta'lim muassasalari boshqaruv tizimini takomillashtirsa, bu nafaqat ta'lim jarayonining sifatini oshirishga, balki universitetlarning xalqaro reytinglarda mavqeini mustahkamlashga ham yordam beradi.

Oliy ta'lim tizimi jamiyatning barqaror rivojlanishida muhim o'rin tutadi. Bugungi kunda ta'lim sohasida globallashtirish, raqamli transformatsiya va innovatsiyalar jarayoni jadallashtirib borayotgani sababli universitetlar va institutlar o'z faoliyatini samarali boshqarish usullarini izlashga majbur. Shunday yondashuvlardan biri loyihaviy boshqaruv bo'lib, u oliy ta'lim muassasalarida samaradorlikni oshirish, resurslarni to'g'ri taqsimlash va innovatsion g'oyalarni amalga oshirishda muhim vosita hisoblanadi.

Loyihaviy boshqaruv aniq maqsadlarga yo'naltirilgan, belgilangan muddat va resurslar doirasida amalga oshiriladigan boshqaruv tizimi bo'lib, u universitetlarda ta'lim, ilmiy-tadqiqot, moliyaviy va infratuzilmaviy loyihalarni samarali amalga oshirish imkonini beradi. An'anaviy boshqaruv tizimidan farqli ravishda, loyihaviy boshqaruv har bir jarayonni bosqichma-bosqich rejalashtirish, amalga oshirish va natijalarini baholashga asoslangan.

Loyihaviy boshqaruvning oliy ta'lim muassasalaridagi roli

1. Ta'lim sifatini oshirish – Innovatsion pedagogik texnologiyalarni joriy etish, zamonaviy o'quv dasturlarini ishlab chiqish va professor-o'qituvchilarning malakasini oshirish bo'yicha loyihalar tashkil etish imkonini beradi.
2. Ilmiy-tadqiqot faoliyatini rivojlantirish – Grantlar va tadqiqot loyihalarini samarali boshqarish orqali ilmiy izlanishlar natijadorligini oshirishga xizmat qiladi.
3. Infratuzilmani takomillashtirish – Universitetlar uchun laboratoriyalar, kutubxonalar, innovatsion markazlar va elektron resurslarni yaratish jarayonlarini tizimli tashkil etish imkonini beradi.
4. Xalqaro hamkorlikni kengaytirish – Chet el universitetlari bilan hamkorlikda loyihalar ishlab chiqish va xalqaro ta'lim dasturlarida ishtirok etish imkoniyatlarini kengaytiradi.

5. Moliyaviy barqarorlikni ta'minlash – Resurslardan oqilona foydalanish, grant va investitsiyalarni jalb qilish orqali universitetlarning barqaror rivojlanishiga hissa qo'shadi.

Loyihaviy boshqaruvni joriy etishda asosiy tamoyillar

1. Maqsadga yo'naltirilganlik – Har bir loyiha universitet strategik rejalari bilan bog'liq bo'lishi kerak.
2. Rejalashtirish va prognozlash – Loyiha natijalari oldindan aniq belgilanishi va amalga oshirish bosqichlari rejalashtirilishi zarur.
3. Resurslarni samarali boshqarish – Moddiy, moliyaviy va insoniy resurslarni optimal taqsimlash talab etiladi.
4. Monitoring va baholash – Loyihaning har bir bosqichi tahlil qilinib, uning natijalari baholanib borilishi lozim.
5. Xavflarni boshqarish – Mavjud muammolar va kutilmagan vaziyatlarga moslashish uchun ehtiyot choralarini ko'rish.
6. Jamoaviy ishlash – Universitet rahbariyati, professor-o'qituvchilar, talabalar va tashqi hamkorlarning samarali hamkorligini ta'minlash.

Xulosa

Oliy ta'lim muassasalarida loyihaviy boshqaruvni joriy etish zamonaviy ta'lim tizimini rivojlantirish va uning samaradorligini oshirishning muhim shartidir. Bu boshqaruv modeli ta'lim sifatini oshirish, ilmiy va innovatsion loyihalarni rivojlantirish, universitetlarning xalqaro miqyosdagi mavqeini mustahkamlash va resurslarni samarali boshqarishda katta ahamiyatga ega. Shuning uchun, oliy ta'lim muassasalari loyihaviy boshqaruv tamoyillarini faol joriy etishi va rivojlantirishi lozim. Xulosa qilib aytganda, oliy ta'lim muassasalarida loyihaviy boshqaruvni joriy etish ta'lim jarayonini yanada samarali tashkil qilish, ilmiy va innovatsion faoliyatni rivojlantirish, moddiy-texnik bazani mustahkamlash va xalqaro hamkorlikni kengaytirishda muhim ahamiyatga ega. Shuning uchun loyihaviy boshqaruv tizimini yo'lga qo'yish va uni takomillashtirish oliy ta'limning kelajakdagi barqaror rivojlanishi uchun zaruriyat hisoblanadi.

Foydalanilgan adabiyotlar ro'yxati:

1. Xodjayev N. Raqamli ta'lim va uning istiqbollari. – Toshkent: Fan va texnologiya, 2021.
2. UNESCO. Digital Learning and Education Policies. – Paris: UNESCO Publishing, 2022.
3. Oliy ta'lim muassasalarida loyihaviy boshqaruv tamoyillari. Ilmiy-amaliy konferensiya materiallari. Toshkent, 2022.

4. Turner, J. R. Gower Handbook of Project Management. Gower Publishing, 2016.

5. Malik, S. & Waseem, M. Implementation of Project-Based Learning in Higher Education Institutions. Journal of Education and Research, 2020.

AXBOROT TEXNOLOGIYALARIDAN FOYDALANGAN HOLDA SODIR ETILADIGAN GIYOHVANDLIK VOSITALARI YOKI PSIXOTROP MODDALAR BILAN QONUNGA XILOF RAVISHDA MUOMILA QILISHGA OID JINOYATLARNI TERGOV QILISHNING AYRIM JIXATLARI

Subanov Olimjon Suyarkul o'g'li

*O'zbekiston Respublikasi Ichki ishlar vazirligi Malaka oshirish instituti
Yuridik fanlar kafedrasida katta o'qituvchisi*

Annotatsiya. Mazkur maqolada Axborot texnologiyalaridan foydalangan holda sodir etiladigan giyohvandlik vositalari yoki psixotrop moddalar bilan qonunga xilof ravishda muomila qilishga oid jinoyatlarni tergov qilishning ayrim jixatlari yoritilgan.

Kalit so'zlar: Axborot texnologiyalari, giyohvandlik vositalari, psixotrop moddalar, jinoyatlarni tergov qilish, uyushgan jinoyatchilik, ichki ishlar vazirligi.

So'ngi yillarda butun dunyoda jinoyatchilikning yangicha turlari, shakllari va ko'rinishlarining paydo bo'lishi, jinoyatlarni sodir etish usullari o'zgarib borayotganligi, xususan ijtimoiy tarmoqlar, internet bilan bog'liq holda sodir etilayotgan jinoyatlar, kiberjinoyatchilik tezkor-qidiruv faoliyatini tashkil etishda faoliyatni amalga oshiruvchi tuzilmalarga qo'shimcha vazifalar yuklaydi. Buni, O'zbekiston Respublikasi Prezidentining 2021-yil 26-mart kunidagi "Jamoat xavfsizligini ta'minlash va jinoyatchilikka qarshi kurashish sohasida ichki ishlar organlari faoliyatini sifat jihatidan yangi bosqichga ko'tarish chora-tadbirlari to'g'risida"gi PF-6196-son Farmonida ham ko'rishimiz mumkin.

Xususan, farmonda Ichki ishlar organlarining tezkor-qidiruv faoliyatini quyidagi yo'nalishlar bo'yicha takomillashtirish vazifasi qo'yilgan. Jumladan, uyushgan jinoyatchilik, terrorizm va ekstremizm, giyohvand vositalar, psixotrop moddalar va ularning analoglari noqonuniy aylanmasiga qarshi kurashish chora-tadbirlari samaradorligini oshirish;

– axborot texnologiyalari va Internet tarmog'idan foydalanish sohasidagi jinoyatlarga qarshi kurashish borasida tubdan yangi mexanizmlarni joriy etish;

– tezkor bo'linmalar faoliyatini apparat-dasturiy ta'minlash, zamonaviy axborot texnologiyalarini keng tatbiq etish.

Shuni alohida ta'kidlash joizki, O'zbekistonda giyohvandlik vositalari bilan bog'liq vaziyat doimo davlat va jamiyatning alohida e'tiborida bo'lib keladi. Hozirgi vaqtda davlat va jamoat tuzilmalari tomonidan giyohvandlik tahdidiga qarshi kurashishning yagona tizimini yaratish bo'yicha bir qator tashkiliy-huquqiy, profilaktik va iqtisodiy chora-tadbirlar amalga oshirilmoqda. Ushbu tizimda giyohvandlik vositalarining qonunga xilof ravishda muomala qilinishiga qarshi kurashishning asosiy yo'nalishlaridan biri huquqni muhofaza qiluvchi organlar tomonidan mazkur jinoyatlarni oldini olish va aniqlashdan iborat. O'tkazilayotgan chora-tadbirlarga qaramay mazkur turdagi qonunbuzarlik yildan yilga oshib, turlari ko'payib bormoqda, masalan:

2020-yilda O'zbekiston Respublikasida tezkor-qidiruv va tezkor profilaktik chora-tadbirlar natijasida giyohvandlik vositalarining noqonuniy aylanmasi bilan bog'liq 6032 ta jinoyat aniqlangan (2019-yilda – 5026, 20,01%) qayd etilgan. Ushbu ko'rsatgich mamlakatimizga chegaradosh davlatlarda quyidagicha ko'rinishga ega: Qozog'iston Respublikasida 7808 ta jinoyat aniqlangan (2019-yilda – 7016; 11,2% ga oshgan); Tojikiston Respublikasida 700 (2019-yilda – 574; 21,95% ga oshgan) oshganligini; Qirg'iziston Respublikasida esa 795 (2019-yilda – 999; 20,42% ga kamaygan) pasayishni kuzatish mumkin. Shu bilan birga, O'zbekiston Respublikasida besh yillik statistik ma'lumotlarni (2016-2020-yillar) hisobga olgan holda giyohvandlik vositalari bilan bog'liq jinoyatlar: kontrabanda 29,9 %ga, giyohvandlik vositalaridan iborat o'simliklarini yetishtirish 1,1 % ga, ularni qonunga xilof ravishda tayyorlash va boshqa harakatlar 26 % ga oshgan. Ushbu sohada yoshlarning 33,2 % ga, tibbiyot xodimlari va chet el fuqarolarining jinoyatchiligi 2 barobarga oshgan.

Ushbu jinoyatning hozirgi kunda asosan internet tarmoqlarida sodir etib kelinmoqda. Axborot texnologiyalari rivojlangan bugungi kunda giyohvandlik vositalarining noqonuniy aylanmasi, xalqaro terrorizm, qurol-yaroq savdosi va boshqa shu kabi jinoyatlarni sodir etishda internet tarmoqlaridan foydalanish holatlari ko'payib bormoqda. Ma'lumotlarga ko'ra, AQSH, Yevropa Ittifoqi davlatlari, Ukraina, Rossiya va Belarus Respublikasida giyohvandlik vositalari savdosining salmoqli qismi aynan internet tarmoqlari orqali amalga oshirilmoqda. Ushbu holatlarning asosiy sabablari sifatida quyidagilarni ko'rsatish mumkin:

1) giyohvandlik vositalarining mayda chakana savdosini bevosita kontaktsiz va tomonlarning shaxsini sir saqlagan holda tashkil etish imkoniyati;

2) tashkilotchilar xavfsizligini ta'minlovchi murakkab ierarxiya sxemalarining tashkil etilishi;

3) pul mablag'larini bank sektoridan tashqari qalbaki elektron hisoblar orqali tranzaksiya qilish va daromadni anonim tarzda naqd pulga aylantirish;

4) internet tarmoqlarida narkojinoyatchilikni aniqlash va fosh etishda huquqtartibot idoralarining tajribasi yetarlicha emasligi;

5) keng auditoriya va xaridorlar bazasi;

6) dunyoning deyarli barcha davlatlarida narkobiznesni tashkil etish imkoniyati;

7) qo‘shimcha ish kuchini internet-reklama orqali jalb etish.

Axborot texnologiyalaridan foydalanib sodir etilgan giyoxvandlik va psixotrop moddalar sotish jinoyatini fosh etishda tezkor hodim, surishtiruvchi va tergovchining dastlabki surishtiruv jarayonida bo‘ladigan hamkorlikning samaradorligi ko‘p jihatdan quyidagilarda o‘z ifodasini topgan:

1) hamkorlik qiluvchi sub’ektlar faoliyatida kriminalistik taktika qoidalariga amal qilishning ahamiyatga egaligi;

2) hamkorlik taktikasini qo‘llayotgan sub’ektlar faoliyatining vositalari, usullari va huquqiy bazasi o‘zaro farq qilishi;

3) ichki ishlar organlari tezkor xodimlarining surishtiruv va tergov yo‘nalishidagi xodimlar bilan dastlabki tezkor surishtiruv choratadbirlarini amalga oshirishida hamkorlikning aniq maqsad va yo‘nalishlarini belgilab olish zarurligi.

Axborot texnologiyalaridan foydalanib sodir etilgan giyoxvandlik va psixotrop moddalar sotish jinoyatini o‘z vaqtida aniqlash va fosh etishda shuningdek bunday turdagi jinoyatlarning oldini olish bo‘yicha zarur qarorlar qabul qilishda faoliyatning huquqiy asosini ta‘minlab beruvchi kiberjinoyatchilikka qarshi kurashish bo‘yicha normativ-huquqiy hujjatlar loyihalarini ishlab chiqish zarur.

Bugungi kunda giyohvandlik vositalarining noqonuniy aylanmasida internet tarmoqlaridan foydalanilayotganligi mazkur jinoyatlarni aniqlash va ularga chek qo‘yishda muayyan qiyinchiliklarni yuzaga keltirmoqda. Bu esa o‘z navbatida mazkur sohada yetuk mutaxassislarni tayyorlash hamda bu turdagi jinoyatlarni fosh etish uchun zarur bo‘lgan texnik imkoniyatlarni yaratish va doimiy ravishda takomillashtirib borishni taqozo etadi³. Yuqorida keltirilgan tahlildan kelib chiqib, xulosa sifatida quyidagi takliflar bildiriladi. Bular:

- doimiy ravishda, ushbu jinoyat holatlari yuzasidan kelib tushgan har bir murojaatlarni tekshiruv natijasi bo‘yicha uning qonuniyligi va jazo muqarrarligini ta‘minlash maqsadida, O‘zbekiston Respublikasi IIV tizimida respublika miqyosida, axborot texnologiyalaridan foydalanib sodir etilgan giyoxvandlik va psixotrop moddalar sotish oldi-berdisi orqali sodir etilayotgan firibgarlik jinoyatlarini sodir etishga moyil shaxslar ro‘yxatining yagona bazasini shakllantirish, ushbu shaxslar to‘g‘risida ma‘lumotlarning viloyatlararo almashinuvini va tezkor ishlar olib borilishini yo‘lga qo‘yish;

- hozirgi kundagi axborot texnologiyalari sohasi bo'yicha mutaxassislar tayyorlab berayotgan oliy va o'rta-maxsus ta'lim o'quv yurtlari talabalari va ularning bitiruvchilari tomonidan mazkur turdagi jinoyatlarni sodir etilishini oldini olish maqsadida, ularni huquqiy ongini shakllantirish, talabalar ongida internet tarmoqlari orqali jinoyat sodir etilishi qonunchilik bilan taqiqlanganligi va tegishli javobgarlikni keltirib chiqarishi yuzasidan ilmiy asoslangan yagona mafkuraviy yo'nalish ishlab chiqish;

- barcha ta'lim muassasalarida internet tarmog'iga ulangan axborot resurslaridan samarali foydalanish ko'nikmasini tashkil etish uchun "Xavfsiz Internet", "Internet madaniyati" mavzularida o'quv mashg'ulotlari tashkil etish kabilardi.

Jinoyat ishinini qo'zg'atish to'g'risidagi masalani hal etishda surishtiruvchi yoki tergovchi birinchi navbatda quyidagi holatlarni aniqlash zarur:

1) olingan moddalarni narkotik vositalar va o'zida narkotik moddalarni tashkil qiluvchi dorilar ro'yxatiga kiritilganligi yoki kiritilganmaganligini;

2) olinayotgan narkotik vositalar va psixotrop moddalarning sonini va sifati;

3) JKning 276-moddasida ko'rsatilgan qonunga xilof harakatlarning sodir etilganligini;

4) jinoyat guruh tarkibida sodir etilganligi va guruh tarkibini;

5) qachon, qaerda, kim tomonidan va qanday usullarda qonunga xilof ravishdagi harakatlar sodir etilganligini, qanday niqoblash usullari qo'llanilganligini;

6) narkotik moddalar va uning tarqalishiga ko'maklashgan yo'llar(kanallar)ni (kim, qanday usullarda va qancha narhda ularni o'tkazib yurganligini);

7) narkotik vositalar va psixotrop moddalarni tayyorlashda xizmat qilgan xomashyolarni qaerdan olinganligini kim ularni yetkazib turganligini;

8) jinoyatni sodir etish maqsadi va motivlarini;

9) narkotiklarning olingan manbaalarini;

10) javobgarlikning darajasi va xususiyatiga ta'sir etuvchi hamdajinoyatchi shaxsini tavsiflovchi holatlarni;

11) narkotik va psixotrop moddalarni realizatsiya qilish natijasida olingan foyda va daromad miqdorlarini;

12) bunday turdagi jinoyatning sodir etish sabab va shart-sharoitlarini.

Narkotik vositalar yoki psixotrop moddalar bilan bog'liq jinoyatlarning sodir etilish holatlarining xususiyatidan kelib chiqqan holda aniqlanishi lozim bo'lgan holatlar yuzasidan qo'yiladigan savollar ro'yxati yanada kengaytirilishi mumkin bo'ladi.

Narkotik vositalar yoki psixotrop moddalar bilan bog'liq jinoyatlar haqidagi jinoyat ishi bo'yicha tergov qilishning dastlabki bosqichida quyidagi ikkita vaziyatlar xususiyatlidir:

1) huquq tartibot organlari xodimlari tomonidan gumonlanuvchi jinoyat sodir etish vaqtida yoki sodir etib bo'lgan vatqning o'zida yetarli dalillar bilan qo'lga olingan vaziyat;

2) narkotik moddalarni qonunga xilof ravishda muomamala qilish jinoyati bo'yicha gumon qilingan holda qo'lga olinga, ammo bu vaqtda uning yonidan narkotik moddalar topilmagan vaziyat.

Birinchi vaziyat bo'yicha quyidagi tipik tergov harakatlar, tashkiliy va tezkorqidiruv choralarni o'tkazish talab etiladi: gumonlanuvchini ushlab va shaxsiy tintuvni amalga oshirish, ushlab o'tkazilgan joy (bino, xizmat xonasi, tayyorlov laboratoriyasi, narkotik moddalar tarkibida bo'lgan o'siliklar yetishtirilgan maydon)ni ko'zdan kechirish, narkotik moddalarni, hujjatlarni, predmetlarni, narkomanning kiyim kechagini ko'zdan kechirish, narkotik moddalarga bo'lgan tobeligi va mastligini aniqlash predmetida ushlangan shaxsni tibbiy guvohlantirish, sud-tibbiyot, kimyoviy, fizik va boshqa ekspertizalarni tayinlash; narkomanning yashash va ish joyida tintuv o'tkazish, gumonlanuvchini so'roq qilish, guvohlarni so'roq qilish, narkotiklar yashirilgan joyini, aloqador shaxslarni, narkotik moddalarni qaysi shaxslar tomonidan yoki qaysi kanalar orqali olinayotganligini, barcha jinoyat ishtirokchilarini aniqlash bo'yicha tezkor-qidiruv chora-tadbirlarini o'tkazish va boshq.

Ikkinchi vaziyat bo'yicha quyidagi harakatlarni amalga oshirish talab etiladi: narkotik moddalarga bo'lgan tobeligi va mastligini aniqlash predmetida ushlangan shaxsni tibbiy guvohlantirish, narkomanning yashash va ish joyida tintuv o'tkazish, gumonlanuvchini so'roq qilish, guvohlarni so'roq qilish, narkotiklar yashirilgan joyini, aloqador shaxslarni, narkotik moddalarni qaysi shaxslar tomonidan yoki qaysi kanalar orqali olinayotganligini, barcha jinoyat ishtirokchilarini aniqlash bo'yicha tezkor-qidiruv chora-tadbirlarini o'tkazish va boshq.

Tergovga qadar ish yurituv bosqichida tadqiq qilinayotgan masalaning yana bir muhim jihati bu narkotik moddalar va psixotrop moddalarni o'tkazishni ko'zlamasdan tayyorlash, saqlash, olish, jo'natish va boshqa harakatlar bilan bog'liq jinoyatlarni sodir etayotgan shaxslarni ushlab vaqtida qo'llanilayotgan o'ziga xos taktik xususiyatlarni aniqlashdir. Gumonlanuvchi shaxsni ushlab mustaqil tergov harakatlardan biri hisoblanadi va ushbu harakatlar surishtiruvchi va dastlabki tergov organlari xoimlari tmonidan amalga oshirilishi lozim. Biroq, narkotik vositalar va psixotrop moddalarning qonunga xilof ravishda muomalasi bilan shug'ullanyotgan shaxsning ushlab tadbiri asosan surishtiruv organining rahabriyati tomonidan tezkor vakillar, profilaktika inspektorlari, ularning

yordamchilari, Milliy gvardiya jamoat xavfsizligi xodimlarining axborotlariga tayangan holda tashkillashtiriladi.

O‘zbekiston Respublikasi Ma‘muriy javobgarlik to‘g‘risidagi kodeksining talablariga binoan shaxsni va narsa-buyumlarni tekshirish, daliliy ashyo sifatida qo‘llanilishi mumkin bo‘lgan buyum va hujjatlarni olib qo‘yish. Agarda olib qo‘yilgan narkotik vositalar va psixotrop moddalar, ushlangan shaxsni fosh etadigan, o‘zida jinoyat alomatlari bor bo‘lgan predmetlar jinoyat tarkibi mavjudligidan dalolat bergan vaqtda vaqtni o‘tkazmasdan jinoyat ishini qo‘zg‘atish lozim bo‘ladi. Shundan so‘ng, shaxsni protsessual tartibda ushlanganligi to‘g‘risidagi masala hal etiladi, hamda tegishli tezkor-qidiruv chora-tadbirlar va tergov harkatlari amalga oshiriladi.

Narkotik vositalar va psixotrop moddalarni iste‘mol qiluvchilar va shular bilan shug‘ullanuvchi shaxslarni ushlab to‘g‘ri tashkil etilgan holatlarda ushbu moddalarni sotgan shaxslar, tashuvchilarni, tayyorlash va saqlanish joylarini, shuningdek jinoyatni sodir etishda qo‘llanilgan vositalarni aniqlash yetarli imkoniyatlarni beradi. Masalan, o‘zida narkotik moddalarni olib yurgan shaxsni ushlangan vaqtda, ushbu moddani kimdan olganligini, kim bunday ishlar bilan shug‘ullanayotganligini, qaysi manzilda yashayotganligini, ushbu manzilda yana qancha miqdorda narkotik vositalar va psixotrop moddalar borligini aniqlash mumkin bo‘ladi.

Ushlab amalga oshirilgan vaqtning o‘zidayoq shaxsiy tekshiruvni amalga oshirib, unda bor bo‘lgan barcha narkotiklarni, hujjatlarni, jinoyat izlarini o‘zida namoyon etadigan predmetlarni va ushlangan shaxsni jinoyat ishi bo‘yicha aloqador bo‘lgan boshqa buyumalarni ham olib qo‘yish talab etiladi. Ushlab va tekshiruvni amalga oshirgandan keyin ushlab amalga oshirilgan joyni ko‘zdan kechirish talab etiladi, chunki jinoyatchi o‘zida bo‘lgan narkotiklar yoki uni jinoyatda gumonlash imkonini beradigan boshqa narsalarni yerga tashlab yuborishi mumkin. Ushlab ikki tartibda amalga oshirilishi mumkin.

Agarda jinoyat ishi ko‘zg‘atilgunga qadar bo‘lsa, unda ma‘muriy tartibda yoxud agarda jinoyat ishi qo‘zg‘atilgan bo‘lsa, jinoyat-protsessual tartibda amalga oshirilishi mumkin. Narkotik vositalar va psixotrop moddalar bilan bog‘liq huquqbuzarliklarda ushlabni o‘tkazish chog‘ida quyidagi tipik xatolarga yo‘l qo‘yilishiga e‘tibor qaratish zarur:

– tezkor-qidiruv xodimlari tomonidan narkotik moddalarni qonunga xilof ravishda muomala qilayotgan shaxsni ushlab harakatini tergovchining ishtirokisiz, shuningdek, jinoyatchini fosh etishi mumkin bo‘lgan barcha holatlar haqida oldindan u bilan kelishmagan holda amalga oshirish;

– ushlab vaqtida faqat jinoyatchining o‘zini qo‘lga olishga qaratilgan maqsad bilan harakatlanish, bunday holat esa protsessual va tezkor-qidiruv

tadbirlar orqali isbotlash talab etadigan holatlarni ko‘zdan chetda qoldirishga, narkotiklar kelib tushishi mumkin bo‘lgan kanalar va ularning manbaalarini, shuningdek ushbu jinoyatga aloqador bo‘lgan barcha ishtirokchilarni aniqlashga imkon bermasdan qoladi;

– ushlar vaqtida yoki ushlaridan keyin o‘tkazilgan protsessual harakatlar natijalarida olingan ma’lumotlarni sifatsiz rasmiylashtirish.

Xulosa o‘rnida shuni aytish joizki, giyohvandlikka qarshi kurashning asosiy muammolaridan biri bolalar va o‘smirlar tomonidan toksik dorilarni q o‘llashdir. Katta falokatning ta'sirchan miqdori, shuningdek ularning oqibatlari qonunlarni buzish va taxminan 75% qizlar fohishalikka aylanishiga hamda ko‘pincha OITS bilan kasallanishlariga va giyohvandlik saratoni kasalligini keltirib chiqaradi. Giyohvandlik vositalari va psixotrop moddalar bilan qonunga xilof muomala qilish bilan bog‘liq jinoyatlarni oldini olish va aniqlash bu o‘z o‘rnida nafaqat xalqni jinoyatchilarda tozalash, balki jamiyatni parokanda qiladigan ilatdan halos qilish ham demakdir.

Foydalanilgan adabiyotlar ro‘yxati:

1. O‘zbekiston Respublikasining Konstitutsiyasi T. “O‘zbekiston” 2023-yil.
2. O‘zbekiston Respublikasining Jinoyat kodeksi. O‘zbekiston Respublikasi Qonun hujjatlari milliy bazasining rasmiy veb-sayti www.lex.uz.
3. O‘zbekiston Respublikasining Jinoyat–protsessual kodeksi. O‘zbekiston Respublikasi Qonun hujjatlari milliy bazasining rasmiy veb-sayti www.lex.uz.
4. “Giyohvandlik vositalari to‘g‘risida”gi Yagona Konvensiya (1961-yil 30-mart).
5. O‘zbekiston Respublikasining 1999-yil 19-avgustdagi “Giyohvandlik vositalari va psixotrop moddalar to‘g‘risida”gi 813-I-sonli Qonuni. O‘zbekiston Respublikasi Qonun hujjatlari milliy bazasining rasmiy veb-sayti www.lex.uz.
6. Abdullaev X., Payziev A. Giyohvandlik vositalari yoki psixotrop moddalar va kuchli ta’sir qiluvchi dorilarning noqonuniy aylanishiniga qarshi kurashishning muammolari va yechimlari //Science and innovation. – 2022. – T. 1. – №. C8. – S. 29-32.

AXBOROT-KOMMUNIKATSIYA TEXNOLOGIYALARIDAN FOYDALANGAN HOLDA ICHKI ISHLAR ORGANLARINING INSON HUQUQLARINI HIMOYA QILISH SOHASIDA NODAVLAT NOTIJORAT TASHKILOTLARI BILAN SAMARALI HAMKORLIGINI YO'LGA QO'YISH MEXANIZMLARI

s.f.b.f.d Kenjayev Jasur Omon o'g'li

IIV Malaka oshirish instituti Maxsus-kasbiy fanlar kafedrasida dotsenti

Annotatsiya. Mazkur maqolada axborot texnologiyalari sohasida ichki ishlar organlarining inson huquqlarini himoya qilishda nodavlat tashkilotlari bilan hamkorlik o'rnatishdagi muammo va uning yechimlari yoritilgan.

Kalit so'zlar: Ichki ishlar organlari, nodavlat notijorat tashkilotlar, hamkorlik, axborot texnologiyalari sohasi, inson huquqlarini himoya qilish

Hozirgi kunda ichki ishlar organlari aholining tinch va farovon hayot kechirishini ta'minlash, jinoyatchilik va boshqa huquqbuzarliklarga qarshi kurashish, jamoat tartibini saqlash, shuningdek, boshqa hayotiy muhim vazifalarni amalga oshirishda alohida o'rin egallaydi.

“Ichki ishlar organlaridagi xizmat davlat xizmatining turi bo'lib, fuqarolarning huquqlari, erkinliklari va qonuniy manfaatlarini, jismoniy va yuridik shaxslarning mulkini, konstitutsiyaviy tuzumni himoya qilish, qonun ustuvorligini, shaxs, jamiyat va davlat xavfsizligini ta'minlash, shuningdek, huquqbuzarliklarning oldini olish va profilaktikasini bo'yicha vazifalarni amalga oshirishdan iborat”.³⁸

Zamon shiddat bilan rivojlanmoqda. Mamlakatimizda zamonaviy axborot texnologiyalar kirib bormagan soha qolmagan. Tabiiyki har bir mamlakatning keskinlik bilan rivojlanishi va uning boshqa davlatlar bilan teng raqobatbardoshligini ta'minlash orqali zamonaviy axborot-kommunikatsiya hamda “raqamli” texnologiyalar jamiyat va davlat hayotining barcha jabhalariga qanchalik joriy etilgani bilan baholanmoqda.

Global taraqqiyot sharoitida axborot texnologiyalari mohiyatini oshirishning yanada zamonaviy, innovatsion usullarini izlab topish, axborotlashtirish jarayoniga har tomonlama ko'maklashish, ularni hayotga keng joriy etish davlat faoliyatining muhim yo'nalishlaridan biriga aylanmoqda. Zero, axborotlashtirish tizimida davlat siyosatini olib borish masalasi strategik ahamiyatga ega vazifadir. Hozirgi kunda axborot texnologiyalarining jadal rivojlanishi va kishilik jamiyatining barcha

³⁸ O'zbekiston Respublikasi Prezidentining 29.11.2017 yildagi “Ichki ishlar organlari kadrlari bilan ishlash va ularning xizmatini tashkil etish tartibini tubdan takomillashtirish chora-tadbirlari to'g'risida”gi PQ-3413-son Qarori bilan tasdiqlangan “Ichki ishlar organlarida xizmatni o'tash tartibi to'g'risida”gi Nizom.

sohalarida Internetdan keng foydalanish kundalik faoliyatning bir qismini tashkil etib, xizmat ko'rsatish, ilm-fan, ta'lim, elektron tijorat, shuningdek zamonaviy insonning fikrlash tarziga o'zining ijobiy ta'siri bilan kirib keldi.

Mamlakatimizda ham bugungi davrning eng zaruriy talablaridan kelib chiqib, birinchi o'rinda mavjud barcha sohalarga zamonaviy texnologiyalarni joriy etishga alohida e'tibor qaratilmoqda. Bu esa borgan sari o'zining ijobiy samarasini bermoqda.

Buning yorqin misoli sifatida, "2020-yil 1-noyabrdan boshlab respublikamizdagi barcha vazirlik va idoralar, mahalliy ijro etuvchi hokimiyat organlarida amaldagi rahbar o'rinbosarlaridan biriga raqamlashtirish bo'yicha o'rinbosar (Chief Digital Officer) vakolatlari yuklatildi".³⁹

Shundan so'ng, O'zbekiston Respublikasi Ichki ishlar vazirining axborot texnologiyalari bo'yicha o'rinbosari lavozimi joriy etilib, bevosita bo'ysunuvchi xizmatlar Axborot texnologiyalari, aloqa va axborotni himoyalash boshqarmasi, Migratsiya va fuqarolikni rasmiylashtirish bosh boshqarmasi hamda Huquqiy statistika va tezkor-hisob ma'lumotlar markazi etib belgilangan.

Ichki ishlar organlarining axborot texnologiyalari sohasida inson huquqlarini himoya qilish maqsadida, o'tgan davr mobaynida profilaktika inspektoriga masofadan turib murojaat yuborish va uni ko'rib chiqish jarayonini kuzatib borish, aholi bilan o'zaro tezkor muloqotni yo'lga qo'yish, profilaktika inspektorlari va sektor rahbarlari faoliyatiga baho berish imkonini beruvchi «Smart mahalla» axborot dasturi faoliyati yo'lga qo'yilganligi ahamiyatlidir.

Bundan tashqari, "viloyat, tuman va shahar ichki ishlar organlari rahbarlari tomonidan har oy yakuni bo'yicha aholiga Internet tizimidagi axborot resurslari orqali hududdagi kriminogen vaziyat yuzasidan «profilaktik-ogohlantiruvchi murojaat» qilib borish amaliyotini joriy etilgan".⁴⁰

Ichki ishlar organlari faoliyatiga raqamli va zamonaviy axborot texnologiyalarini keng joriy etish orqali, jinoyatlar va ma'muriy huquqbuzarliklar statistikasini yuritish, jinoyatchilik holatini, shu jumladan hududlar va huquqbuzarliklar turlari kesimida statistik tahlilni amalga oshirish, huquqbuzarliklarning oldini olish, ularni aniqlash va fosh etishda foydalanish uchun tezkor-ma'lumotlar hisoblari, ichki ishlar organlarining arxiv-ma'lumotlari va maxsus fondlarini yuritish, shuningdek, shaxslarning qidiruvini e'lon qilish jarayonini ta'minlash, avtotransport vositalari, fuqaroviy va xizmat o'qotar

³⁹ O'zbekiston Respublikasi Prezidentining 05.10.2020 yildagi "Raqamli O'zbekiston - 2030" strategiyasini tasdiqlash va uni amalga oshirish chora-tadbirlari to'g'risida"gi PF-6079-son Farmoni.

⁴⁰ O'zbekiston Respublikasi Prezidentining 26.03.2021 yildagi "Jamoat xavfsizligini ta'minlash va jinoyatchilikka qarshi kurashish sohasida ichki ishlar organlari faoliyatini sifat jihatidan yangi bosqichga ko'tarish chora-tadbirlari to'g'risida"gi PF-6196-sonli Farmoni.

qurollari, qidiruvdagi shaxslar va ashyolar, shuningdek, “huquqbuzarliklarning oldini olish va jinoyatchilikka qarshi kurashish samaradorligiga ko‘maklashuvchi boshqa ma’lumotlar bo‘yicha avtomatlashtirilgan axborot bankini yuritilishiga xamda ichki ishlar organlari xodimlari va ular oila a’zolarining ijtimoiy-huquqiy himoyasini hamda maishiy sharoitlarini yaxshilashga erishilmoqda”.⁴¹

Ichki ishlar organlari faoliyatiga to‘liq raqamli va axborot texnologiyalarini faol joriy etilishi natijasida, aholiga elektron davlat xizmatlarini ko‘rsatish sifatini oshirish, byurokratik to‘siq va g‘ovlarga yo‘l qo‘ymaslik hamda idoralararo elektron hamkorlik kengaytirilayotganligi ayni muddao bo‘lmoqda.

Respublikamizda inson huquqlarini himoya qilish, turli xil ko‘rinishdagi sarsongarchilik, ovvoragarchilik, sansolarlik, ortiqcha vaqt va harajatlarning oldini olish maqsadida haydovchining yo‘l-patrul xizmati inspektoriga taqdim etilishi lozim bo‘lgan hujjatlari yonida bo‘lmagan taqdirda mazkur hujjatlar maxsus planshet qurilmasi yordamida identifikatsiya ID-kartasi orqali tekshiriladi.

Bunda, “identifikatsiya ID-kartaga ega fuqarolarga tegishli transport vositasi haydovchisidan yangi namunadagi haydovchilik guvohnomasi, transport vositasini ro‘yxatdan o‘tkazganlik to‘g‘risidagi, transport vositasiga egalik qilish, egasi yo‘qligida undan foydalanish yoki uni tasarruf etish huquqini tasdiqlovchi hujjatlar, transport vositalari egalarining fuqarolik javobgarligini majburiy sug‘urta qilish bo‘yicha sug‘urta polisini talab qilish amaliyoti bekor qilinadi”.⁴²

Axborot texnologiyalari sohasida ichki ishlar organlarining inson huquqlarini himoya qilishda nodavlat tashkilotlari bilan hamkorligi asosiy muhim o‘ziga xos jihatlarni belgilaydi. Misol uchun, ichki ishlar organlari faoliyatidagi korrupsiya holatlari bo‘yicha internet va ijtimoiy tarmoqlarda e‘lon qilingan xabarlarni nodavlat tashkilotlari batafsil o‘rganishi hamda ularning natijalarini keng jamoatchilikka yetkazish orqali turli xil tushunmovchiliklarga barham beriladi.

Shuningdek, nodavlat-notijorat tashkilotlar bilan hamorlikda ichki ishlar organlari faoliyati samaradorligini oshirish maqsadida, tarkibiy va hududiy bo‘linmalarda sog‘lom ma‘naviy-ruhiy muhitni, qonuniylik, yuqori huquqiy madaniyat va ma‘naviy-axloqiy sifatlarni ta‘minlashga oid taklif hamda tavsiyalar ishlab chiqiladi.

Shuningdek, Ichki ishlar organlari faoliyati haqida ommaviy axborot vositalari va ijtimoiy tarmoqlarda axborot berib borish xamda ichki ishlar organlarining nodavlat notijorat tashkilotlari, ommaviy axborot vositalari va

⁴¹ O‘zbekiston Respublikasi Prezidentining 26.03.2021 yildagi “Jamoat xavfsizligini ta‘minlash va jinoyatchilikka qarshi kurashish sohasida ichki ishlar organlari faoliyatini sifat jihatidan yangi bosqichga ko‘tarish chora-tadbirlari to‘g‘risida”gi PF-6196-sonli Farmoni.

⁴² O‘zbekiston Respublikasi Vazirlar Mahkamasining 15.10.2021 yildagi “Ichki ishlar organlari faoliyatiga zamonaviy axborot texnologiyalarini keng joriy etish chora-tadbirlari to‘g‘risida”gi 645-sonli Qarori

fuqarolik jamiyatining boshqa institutlari, shuningdek fuqarolar bilan samarali hamkorligini ta'minlash, ichki ishlar organlariga nodavlat notijorat tashkilotlari va fuqarolik jamiyatining boshqa institutlaridan kelib tushgan ijtimoiy, siyosiy va boshqa jihatlardan ahamiyatga molik loyihalarni amalga oshirilishiga va natijalarini jamoatchilik nuqtai nazaridan tahlil qilishga ko'maklashish yo'lga qo'yilmoqda.

Axborot texnologiyalari sohasida ichki ishlar organlarining inson huquqlarini himoya qilishda nodavlat tashkilotlari bilan hamkorlikda fuqarolar, nodavlat notijorat tashkilotlari va boshqa fuqarolik jamiyati institutlarining ichki ishlar organlari faoliyatiga oid davlat siyosati bo'yicha tashabbus va murojaatlarini ko'rib chiqishda ishtirok etadi, ularni amalga oshirish uchun tegishli taklif va tavsiyalar tayyorlaydi, ichki ishlar organlari bilan fuqarolar, nodavlat notijorat tashkilotlari va boshqa fuqarolik jamiyati institutlarining samarali shakl hamda usullarda o'zaro hamkorligi tahlilini amalga oshiradi, shuningdek, ularni takomillashtirish bo'yicha takliflar ishlab chiqadi. O'z maqsad va vazifalarini amalga oshirishda nodavlat notijorat tashkilotlari, ommaviy axborot vositalari, shuningdek, fuqarolik jamiyatining boshqa institutlari hamda fuqarolar bilan hamkorlik qiladi.

Prezidentimiz ta'biri bilan aytganda, "Erkin fuqarolik jamiyatini barpo etish, inson huquq va erkinliklarini himoya qilish borasida amalga oshirayotgan islohotlarimizda nodavlat notijorat tashkilotlarining o'rni va roli beqiyos ekanini alohida ta'kidlash joiz".⁴³

Axborot texnologiyalari sohasida inson huquq va erkinliklari ta'minlanishining muhim sharti, bu huquqiy kafolatlarning yaratilganligi hisoblanadi. Ya'ni, bu – fuqarolar huquq va erkinliklarining Konstitutsiya va qonunlarda mustahkamlanishi hamda ularni ta'minlashga, amalga oshirishga qaratilgan boshqa huquqiy hujjatlarning mavjudligi hisoblanadi.

Axborot texnologiyalari sohasida ichki ishlar organlarining inson huquqlarini himoya qilishda nodavlat tashkilotlari bilan hamkorligi borasida quyidagi muammo va kamchiliklarga duch kelinmoqda:

1. Ichki ishlar organlari hamda nodavlat tashkilotlar tomonidan hamkorlikda axborot texnologiyalari sohasida inson huquqlarini himoya qilishni mustahkamlash va ta'minlashga qaratilgan huquqiy hujjatlarni hozirgi zamon talablari darajasida emasligi;

2. Axborot texnologiyalari sohasida inson huquqlarini himoya qilish faoliyatida ichki ishlar organlari bilan nodavlat tashkilotlar va boshqa jamoatchilik tuzilmalari o'rtasida hamkorlikni kuchaytirish zarurligi;

⁴³ Ўзбекистон Республикаси Президенти Шавкат Мирзиёевнинг 23.12.2017 йилдаги "Олий Мажлисга murojaatномаси"

3. Ichki ishlar organlari va nodavlat tashkilotlar bilan hamkorlikda axborot texnologiyalari sohasida inson huquqlarini himoya qilish faoliyatini sifat jihatidan yangi bosqichga olib chiqish zarurligi;

4. So‘nggi vaqtlarda aynan axborot texnologiyalari sohasida sodir etilayotgan jinoyatlar va huquqbuzarliklarni sodir etish holatlarining afsuski xanuzgacha uchrayotganligi;

5. Axborot texnologiyalari sohasida rahbar xodimlarining shaxsiy tarkib ustidan nazorati talab darajasida emasligi;

Yuqoridagi keltirib o‘tilgan muammolarni hal etish borasida quyidagi taklif-tavsiyalarni keltirish mumkin:

✓ xodimlarni vatanparvarlik, qasamyodiga sadoqat ruhida, shuningdek, Konstitutsiya va normativ-huquqiy hujjatlar hamda kasbiy madaniyat talablariga so‘zsiz rioya qilish ruhida tarbiyalash va muhim kasbiy sifatlarni shakllantirish;

✓ xizmat intizomi, qonuniylik va inson huquqlariga qat’iy amal qilgan holda xizmat vazifalari samarali ijro etilishini ta’minlash;

✓ xodimlarning ma’naviy-ma’rifiy saviyasini oshirish va o‘z ustida muntazam ishlashni tashkillashtirish, bu borada jamoat tashkilotlari va keng jamoatchilik imkoniyatlaridan unumli foydalanish;

✓ xodimlar bilan o‘tkaziladigan ma’naviy-ma’rifiy ishlarni amalga oshirishda ichki ishlar organlarining faxriylari, soha olimlari, jurnalistlar, nodavlat tashkilotlari vakillari, xotin-qizlar kengashlari va yoshlar ittifoqi boshlang‘ich tashkilotlari kabi jamoatchilik tuzilmalarini jalb etish, ularning imkoniyatidan keng foydalanish;

✓ Ichki ishlar organlari hamda nodavlat tashkilotlar tomonidan hamkorlikda axborot texnologiyalari sohasida inson huquqlarini himoya qilishni mustahkamlash va ta’minlashga qaratilgan huquqiy hujjatlarning soddalashtirilgan holda qabul qilish;

✓ Axborot texnologiyalari sohasida inson huquqlarini himoya qilish faoliyatida ichki ishlar organlari bilan nodavlat tashkilotlar va boshqa jamoatchilik tuzilmalari bilan hamkorligini kuchaytirish borasidagi ishlarni ko‘rib chiqish;

✓ Ichki ishlar organlari hamda nodavlat tashkilotlar bilan hamkorlikda axborot texnologiyalari sohasida inson huquqlarini himoya qilish faoliyati bo‘yicha bilim va ko‘nikmalari hozirgi zamon talablari darajasiga yetkazish maqsadida qisqa muddatli o‘quv-seminar treninglarni tashkil etish;

✓ So‘nggi vaqtlarda aynan axborot texnologiyalari sohasida sodir etilayotgan jinoyatlar va huquqbuzarliklarni sodir etish holatlarining oldini olish va sodir etilganlarini fosh etish maqsadida nodavlat tashkilotlarining imkoniyatlaridan foydalanish;

✓ Axborot texnologiyalari sohasida inson huquqlarini himoya qilish faoliyatida rahbar xodimlarining shaxsiy tarkib ustidan nazorat mexanizmlarini belgilovchi “nazorat harakatlari protokoli” amaliyotga keng miqyosda jalb qilish maqsadga muvofiq bo‘ladi.

Yuqorida ko‘rsatilgan taklif va tavsiyalarni amalda keng joriy etish natijasida kelgusida ichki ishlar organlari hamda nodavlat tashkilotlar bilan hamkorlikda “Inson qadri uchun” tamoyili asosida davlatning yuksak ma’naviy-axloqiy fazilatlariga ega, o‘z burchiga sodiq, vatanparvar va xalqparvar vakili etib tarbiyalash orqali aholining chinakam roziligiga erishish to‘liq ta’minlanadi.

Foydalanilgan adabiyotlar:

1. O‘zbekiston Respublikasining Kostitutsiyasi. 2023 yil.
2. O‘zbekiston Respublikasining 2016 yil 16 sentabr kunidagi “Ichki ishlar organlari to‘g‘risidagi” O‘RQ-407-sonli qonuni.
3. O‘zbekiston Respublikasi Prezidentining 2017 yil 29 noyabrdagi “Ichki ishlar organlari kadrlari bilan ishlash va ularning xizmatini tashkil etish tartibini tubdan takomillashtirish chora-tadbirlari to‘g‘risida” PQ-3413-sonli qarori.
4. O‘zbekiston Respublikasi Prezidentining 05.10.2020 yildagi “Raqamli O‘zbekiston - 2030” strategiyasini tasdiqlash va uni amalgi oshirish chora-tadbirlari to‘g‘risida”gi PF-6079-son Farmoni.
5. O‘zbekiston Respublikasi Prezidentining 26.03.2021 yildagi “Jamoat xavfsizligini ta’minlash va jinoyatchilikka qarshi kurashish sohasida ichki ishlar organlari faoliyatini sifat jihatidan yangi bosqichga ko‘tarish chora-tadbirlari to‘g‘risida”gi PF-6196-sonli Farmoni.
6. O‘zbekiston Respublikasi Vazirlar Mahkamasining 15.10.2021 yildagi “Ichki ishlar organlari faoliyatiga zamonaviy axborot texnologiyalarini keng joriy etish chora-tadbirlari to‘g‘risida”gi 645-sonli Qarori
7. O‘zbekiston Respublikasi Prezidenti Shavkat Mirziyoevning 23.12.2017 yildagi “Oliy Majlisga murojaatnomasi”

ТОШКЕНТ МЕТРОПОЛИТЕНИДА ЖАМОАТ ХАВФСИЗЛИГИ ВА ХУҚУҚБУЗАРЛИКЛАР ПРОФИЛАКТИКАСИНИ ТАЪМИНЛАШДА ЗАМОНАВИЙ ТЕХНОЛОГИЯЛАРНИНГ ЎРНИ

Ислombeков Бeҳзoдбeк Ислombeкович

Жамоат хавфсизлиги университети мустақил изланувчиси

Islambekov1802@gmail.com

Бугун жаҳонда юз бераётган мураккаб ва таҳликали шарт-шароитлар, технологик тараққиётнинг жадал суръатларда ўсиб бориши ва шунинг баробарида ҳуқуқбузарлик ҳолатларининг ҳам замонга мослашиб бораётганлиги ҳуқуқни муҳофаза қилиш, айниқса ички ишлар органлари ходимларидан уларга қарши курашнинг энг замонавий методларини ишлаб чиқиш ва қўллашни талаб қилмоқда. Айниқса, ҳар куни минглаб йўловчиларга хизмат кўрсатадиган, уларнинг хавфсиз ҳаракатланиши ва кундалик фаолиятини таъминлайдиган метрополитен тизимида бу ўта муҳим ва асосий вазифа ҳисобланади.

Ўзбекистон Республикаси Президентининг “Транспорт ва туризм объектларида жамоат хавфсизлигини таъминлашнинг самарали тизимини жорий этишга оид қўшимча чора-тадбирлар тўғрисида”ги 2019 йил 6 март ПҚ-4229-сон қарорида [1] белгилаган масалалар бевосита Тошкент метрополитенида хизмат олиб бораётган ички ишлар органлари ходимларига ҳам тегишли бўлиб, бу уларнинг замонавий ахборот технологиялардан фойдаланишга оид фаолиятини янада такомиллаштиришга туртки беради.

Шу муносабат билан, метрополитендаги ички ишлар органлари ходимларининг жамоат хавфсизлигини таъминлаш йўналишида метрополитен инфратузилмаси объектларида содир этиладиган ҳуқуқбузарликларга қарши курашида замонавий техника воситаларини қўллаш кўникмасини шакллантириш, бу борада хорижий тажрибаларни ўрганиш, видеокузатув воситаларни такомиллаштириш ва ҳуқуқбузар шахс кийёфасини идентификация қилишда сунъий интеллект асосида бошқариладиган рақамли технологиялардан фойдаланиш шу куннинг энг муҳим талабларидан бири саналади. Аммо метрополитенда ҳуқуқбузарликларнинг олдини олишда ушбу объектнинг ўзига хос тизимга, ёпиқ худудга ва шу сабабли, юқори хавф манбаига ҳам эга эканлиги ҳамда бошқа хусусиятини ҳисобга олиш лозим.

Россиялик олим Д.М.Плугар [2] темир йўл транспорти объектларининг террорчиликдан ҳимояланганлиги тўғрисидаги қонунлар ижроси устидан

прокурор назорати мавзуида тадқиқот олиб борган. Унинг тадқиқотида 2007 йил 13 августда Россия Федерациясининг йирик шаҳарлари Москва – Санкт Петербург йўналишида, 2009 йил 27 ноябрда “Невский экспресс” тезюарар поездида, 2013 йил 3 апрелда Волгоград темир йўл вокзалида, 2017 йил 3 апрелда Петербург метрополитенининг “Сенная площадь” ва “Технологический институт” бекатларида содир этилган террорчилик актларини мисол келтириб, темир йўл, метрополитен объектларининг терроризмдан ҳимояланганлик ҳолати устидан назоратнинг таъминланиши масаласини таҳлил қилади.

У РФнинг темир йўл транспорти тармоқлари объектларида терроризмга қарши курашишга тааллуқли турли қонунлар ва қонунчилик ҳужжатларининг бажарилиши, давлат бюджетидан бу соҳага ажратиладиган маблағларнинг тўғри ва ўз ўрнида сарфланишини назорат қилиш хусусида сўз юритади. Унинг бу тадқиқоти кўпроқ ижтимоий-иқтисодий, норматив-ҳуқуқий, профилактик аҳамият касб этса-да, метрополитен объектларида жамоат хавфсизлигини таъминлаш масалалари ҳақида ўта умумий, билвосита маълумотга эга бўламиз.

Шунингдек Москва юридик институти жиноят ҳуқуқи кафедраси тадқиқотчиси Г.Г.Пайлеванян [3] эса ўз тадқиқотида метрополитен объектларида метронинг ишлаш хавфсизлигига тажовуз қилувчи жиноятлар ҳақида фикр юритади. У жамоат хавфсизлигига таҳдид, метрополитенда белгиланган ҳаракатланиш қоидаларига риоя қилмасликнинг жиноий-ҳуқуқий оқибатларини тадқиқ қилади. Олим метрополитенни бир қатор жиддий хусусиятларига кўра темир йўл транспортининг мустақил, автоном тури эканлиги билан фарқ қилишини таъкидлайди. Унинг фикрича, бу фарқлар қуйидагилар:

- 1) йўл тизимининг шаҳар ҳудуди доираси билан ёпиқлиги;
- 2) шаҳар ичида йўловчи ташишга мақсадли равишда мўлжалланганлиги;
- 3) йўлларнинг асосан ер остида жойлашганлиги;
- 4) йўлнинг бир даражадаги бошқа транспорт тури билан туташмаганлиги ва кесишмаганлиги;
- 5) поездлар ҳаракати бошқаруви, йўл блокировкаси ва ҳаракат устидан назоратнинг юқори даражада автоматлашганлиги;
- 6) эскалатор махсус транспорт воситаси каби техник тизим бўлиб, муайян қоидаларга биноан хизмат кўрсатувчи персоналларнинг мавжудлиги.

Маълумки, Тошкент метрополитенида содир этиладиган ва энг кўп учрайдиган жиноят тури бу – ўғрилиқ ҳисобланади. Ушбу турдаги жиноятни очишда, албатта биринчи навбатда, бекат ва поезд вагонларидаги видеокузатув воситаларидан фойдаланилади. Жиноят қайси бекатда, қачон,

каерда ва қандай ҳолатда, ким томонидан содир этилганлигини аниқлаш бир қарашда осондек туюлса-да, ҳуқуқбузар шахс ҳам унга тайёргарлик кўрганлиги, жиноятни платформалар ёки вагонларда тикилинч пайтларда содир этишини эсдан чиқармаслик керак. Жиноятни очишга масъул тезкор ходимлар айнан шунга эътибор қаратадилар. Пул ва қимматбаҳо нарсаларни ўғирлаш ҳам айнан шундай вазиятларда содир этилади. Аслида, ғаразли ниятда содир этиладиган ҳуқуқбузарликлар (хусусан жиноятлар) метрополитенда ҳам етарлича учраб туради.

Аммо шуни афсус билан таъкидлаш жоизки, бугунги кунда ахборот оқимларининг жадал ва кўплиги, одамларнинг аксарияти электрон тизимларга ишониб, боғланиб қолганлиги содда ва ишонувчан фуқароларнинг жиноят қурбонига айланиб қолишига сабаб бўлмоқда. Бу ҳолат устамон фирибгар шахсларнинг компьютер тизимлари орқали турли фейкларни ўйлаб чиқариши, қандай бўлмасин одамларни алдаб, ишончига кириб, телефон орқали шахсий карточкалари рақамини аниқлаш ва меҳнат билан топган пулларини ечиб олишдан иборат. Бу бир қарашда оддий ҳолдек туюлса-да, айрим ақл ва фаросатли катта ёшдаги кишиларнинг ҳам бундай алдовларга учиши ҳолларининг учраб туриши ажабланарлидир.

Бундай жиноятларга қарши курашувчи Ички ишлар вазирлиги қошида ташкил этилган медиа марказ ҳам баъзида бундай ҳуқуқбузарликларни аниқлашда қийинчиликларга дуч келади. Чунки бундай жиноятларни содир этадиган фуқаролар чет эл мамлакатларида бўлиб, ҳар хил йўллар билан фуқароларнинг пул маблағларига тузоқ қўйиш “тактикасини” ишлаб чиқадилар ва усталик билан қўллайдилар. Бунда фуқароларимизнинг менталитети, руҳий ҳолати, кўнгилчанг ва ишонувчанлиги панд беради. Шуларни ҳисобга олган ҳолда, метрополитен ҳудудида бўлган йўловчиларнинг хавфсизлиги, соғлиғи, мол-мулкининг бутлигини таъминлашда фақат ҳуқуқбузарликларга қарши интенсив курашнинг ўзигина кифоя қилмайди, назаримизда.

Шу муносабат билан, ҳозирги шароитда метрополитен объектларида содир этиладиган жиноятлар ичида кўпроқ учрайдиган ўғрилик, безорилик, фирибгарлик, гиёҳвандлик ва бошқа жиноятлар қаторида компьютер тизимлари орқали одамлар ишончига кириб, уларнинг мол-мулкига тажовуз қилиш жиноятларини ҳам жамоат хавфсизлигига таҳдид қилувчи асосий омиллардан бири деса бўлади. Сабаби, бундай жиноятлар ахборот технологияларини фақат пухта эгаллаган, уни бутун тафсилотларигача яхши тушунадиган хакерлар томонидан ғаразли ниятда содир этилади. Аммо бунга аниқлаш ҳар қанча қийин ва муракаб бўлмасин, унинг чорасини ишлаб чиқишга кўмаклашадиган технологиялар мавжуд ва амал қилмоқда.

Шу муносабат билан, юқоридаги ҳолатларни ҳисобга олган ҳолда ахборот технологияларидан фойдаланиб содир этиладиган ҳуқуқбузарликларнинг олдини олишда куйидагиларга эътибор бериш мақсадга мувофиқдир:

биринчидан, метрополитен объектларида рақамли технологиялардан фойдаланишнинг оптимал вариантларини ишлаб чиқиш ва амалга киритиш;

иккинчидан, метро бекатларида фуқароларнинг телефонлардаги ҳар хил алдовларга учмасликларини тарғиб қилувчи банерлар ўрнатиш;

учинчидан, йўловчиларнинг ҳаёти, соғлиғи, мол-мулкини асраш ва ўз манзилигача етказиб қўйиш билан боғлиқ барча функцияларни амалга оширишни тўла-тўқис визуал бошқарилишини таъминлаш;

тўртинчидан, метрополитен медиа ахборот технологиялари тизимини ҳар томонлама такомиллаштириш ва “хавфсиз шаҳар” тизими билан интеграция қилиш;

бешинчидан, ахборот технологияларини қўллаган ҳолда метрополитенда жамоат тартиби, фуқаролар хавфсизлиги ва ҳуқуқбузарликлар профилактикасини таъминлашнинг энг мақбул самарали ечимларини ишлаб чиқиш.

Фойдаланилган адабиётлар:

1. Транспорт ва туризм объектларида жамоат хавфсизлигини таъминлашнинг самарали тизимини жорий этишга оид қўшимча чоратадбирлар тўғрисида: Ўзбекистон Республикаси Президентининг 2019 йил 6 март ПҚ-4229-сон қарори //Қонун ҳужжатлари маълумотлари миллий базаси, 07.03.2019 й., 07/19/4229/2710-сон; 10.02.2021 й., 06/21/6165/0104-сон, Қонунчилик маълумотлари миллий базаси, 01.12.2021 й., 06/21/27/1116-сон; 15.01.2022 й., 06/22/52/0029-сон; 02.08.2022 й., 07/22/339/0703-сон.

2. Плугарь Д.М. Прокурорский надзор за исполнением законов об антитеррористической защищенности объектов железнодорожного транспорта: автореф.дисс.на соис.уч.степени канд.юрид.наук. – Москва: Академия Генеральной прокуратуры Российской Федерации, 2018. – 29 с.

3. Пайлеваян Г.Г. Ответственность за нарушение правил безопасности движения и эксплуатации транспорта на метрополитене: автореф.дисс.на соис.уч.степени канд.юрид.наук. – Москва: Московский юридический институт, 1991. – 23 с

МЕТРОПОЛИТЕНДА ЖАМОАТ ТАРТИБИ ВА ФУҚАРОЛАР ХАВФСИЗЛИГИНИ ТАЪМИНЛАШ ҲАМДА

ХУҚУҚБУЗАРЛИКЛАРНИНГ ОЛДИНИ ОЛИШДА СУНЪИЙ ИНТЕЛЛЕКТДАН ФОЙДАЛАНИШНИНГ АФЗАЛЛИКЛАРИ

Исломбеков Бехзодбек Исломбекович

Жамоат хавфсизлиги университети мустақил изланувчиси

Islambekov1802@gmail.com

Аннотация. Ушбу мақолада Тошкент метрополитенида жамоат хавфсизлигини таъминлашни такомиллаштиришда сунъий интеллектдан фойдаланишнинг афзал жиҳатлари таҳлил этилган.

Таянч сўзлар: метрополитен, жамоат хавфсизлиги такомиллаштириш, сунъий интеллект, фуқаролар хавфсизлиги.

Ҳозирги кунга келиб жаҳондаги ривожланган мамлакатларнинг метрополитенларида жамоат хавфсизлигини таъминлашнинг энг оптимал воситаларидан бири бўлган сунъий интеллектдан фойдаланишнинг жамоат тартиби ва фуқаролар хавфсизлигини таъминлаш ҳамда ҳуқуқбузарликларнинг олдини олишда энг самарали ечимлардан бири ҳисобланади. Чунки йўловчи ташишда энг оммавий ва ўрнини ҳеч нарса билан алиштириб бўлмайдиган метрополитенда хавфсизлик масаласи аҳоли учун ҳар томонлама мақбул, қулай ҳамда мутлақо хавфсиз бўлиши талаб қилинади.

Айнан шунинг учун ҳам бугунги кунда метрополитенга кираётган йўловчиларнинг юз қиёфасини идентификация қилиш, ҳуқуқбузарликда гумон қилинган шахсларни хавфсизлик тизими тармоқларига уланган Ички ишлар вазирлиги Ахборот маркази маълумотлар базасидан аниқлаш, умуман, метрополитен ҳудудида тартиб-интизомни сақлашда хизмат олиб бораётган полиция ёки ички ишлар органлари ходимларига яқиндан кўмаклашувчи сунъий интеллектдан фойдаланишнинг ғоят самарали эканлиги ўз исботини топмоқда.

Сунъий интеллектдан фойдаланишнинг кўп қиррали йўналишлари, унинг ҳуқуқий асослари ва субъектчилиги (ёки субъект бўла олмаслиги), инсон онги ва шуурини лол қолдирадиган алгоритмик хусусиятлари, келажакда инсон ақл-заковатини эгаллаб олиб ундан ўзиб кетиши борасида хавотирга сабаб бўладиган жиҳатлари ҳақида олим ва тадқиқотчилар ўртасида қизгин баҳслар бўлаётган бир шароитда унинг жамоат хавфсизлигини таъминлаш йўналишидаги хизматига баҳо бериш муҳим масала ҳисобланади. Ўзбекистон Республикаси Президентининг “Сунъий интеллект технологияларини 2030 йилга қадар ривожлантириш стратегиясини тасдиқлаш тўғрисида”ги 2024 йил 14 октябр ПҚ-358-сонли

Қарорида [1] сунъий интелект технологияси – сунъий интелектдан фойдаланишга асосланган технологиялар, шу жумладан, интеллектуал видеотаҳлил, нутқни таниб олиш ва синтезлаш, қабул қилинган қарорларни интеллектуал қўллаб-қувватлашнинг истиқболли усуллари сифатида таъкидланади.

“Сунъий интелект технологияларини 2030 йилга қадар ривожлантириш стратегияси”да унга қуйидагича таъриф берилган “Сунъий интелект – инсоннинг билим ва кўникмаларига тақлид қилиш имконини берувчи (шу жумладан, мустақил равишда ўрганиш ва ечимларни излаш) ҳамда аниқ вазифаларни бажаришда инсон ақлий фаолияти натижалари билан таққосланадиган натижаларни олиш имконини берадиган технологик ечимлар мажмуи” [2].

Мисолларга мурожаат қиладиган бўлсак, масалан, аҳолиси бир ярим миллиарддан ортиқ бўлган Хитой давлатида бутун мамлакат ҳудудида сунъий интелектдан фойдаланиш ўзини оқламоқда. Мамлакат кўча ва хиёбонлари, йирик корпорация ва концернлар, корхона, ташкилот, муассаса ва бошқа барча манзиллар, масканлар юз минглаб энг замонавий видеокузатув воситалари билан қамраб олинган. Рақамли технологиялар асосида ишлайдиган “ақлли” оптик “кўз”лар орқали визуал бошқариладиган бундай камералар мамлакат барча фуқароларининг хатти-ҳаракатларини уларнинг ҳуқуқ ва манфаатларига дахл қилмаган ҳолда кузатиш ҳуқуқи ва имкониятига эга.

Булар жамоат хавфсизлигини таъминлаш мақсадида ишлайди ва ҳар қандай ҳуқуқбузарлик ҳолатларининг олдини олади, уларни бартараф этади ва ҳуқуқбузарларни ушлаб жавобгарликка тортишда полиция органларига яқиндан кўмаклашади. Эндиликда дунёнинг йирик ва ривожланган кўпчилик давлатларида бу амалиёт қўлланилмоқда. Чунки дунёда инсоният кушандаси терроризм хавфи ҳануз сақланиб қолмоқда ва бўй кўрсатмоқда.

Россиялик олим А.В.Швецовнинг маълумотига кўра, дунёнинг 13 та мамлакатида 1977–2017 йиллар оралиғида жами 33 та террористик акт содир этилган, бунда 465 нафар одам ҳалок бўлган, 8535 нафар киши турли даражада шикастланган [3].

Кейинги салкам 50 йил (1977–2025) ичида жаҳондаги етакчи давлатлар Англия (2005 йил), Франция (Париж 1996 йил), Испания (Мадрид 2004 йил), Япония (Токио – 1995 йил), Россия (Москва – 2010 йил), Белоруссия (Минск 2023 йил) ва бошқа давлатлар метрополитенларида содир этилган террорчилик ҳужумлари кескин ва кечиктириб бўлмас хавфсизлик чораларини кўришни тақозо этади.

Айнан шу сабабли, XXI бошларидан минтақада давлатларнинг зудлик билан глобал даражада кенг миқёсли хавфсизлик чораларини ишлаб чиқиш харакати бошланди. Барча мамлакатлар чегара назорати остонасидан бошлаб, бутун худудлари бўйлаб визуал кузатув воситалари ўрнатиш, сунъий интелект имкониятларидан кенг фойдаланишга қарор қилинди, аҳоли энг кўп фойдаланадиган метрополитенлар тизими барча хавфсизлик техника воситалари билан тўлиқ қамраб олинди.

Масалан, 2024 йил 13 февралда Москва шаҳрида бўлиб ўтган “Транспортда терроризм ва хавфсизлик” мавзуидаги XXVIII Бутунроссия конференцияси материаллари маълумотларида таъкидланишича Санкт-Петербург метрополитенида 2006 йилдан 2023 йилгача бўлган давр оралиғида амалга оширилган ишлар кўламини оладиган бўлсак, унга кўра: 63 та станция ва 1 та депо майдончаси интеллектуал видеокузатув воситалари билан жиҳозланган; барча бекатларнинг чиқиш йўлакларига радиацион назоратни амалга оширувчи жами 83 та турникетлар ўрнатилган; метрополитен объектларининг чиқиш зоналари ва кўздан кечириш пунктларида жами 532 рамкадан иборат стационар металл детекторлар ўрнатилган; жами 83 та вестюбеллар турли типдаги (“SmartSkan XR 6045”, “Di-Skan 6040”, “Инспектор-6040Z”, Инспектор “55/65ZX”, “Сириус-II”) рентгенли кўздан кечириш қурилмалари билан жиҳозланган.

Барча бекатлар ва депо майдончаларида “МО-2М”, М-ИОН” туридаги портловчи моддалар бўғини аниқлашда 116 та детекторлардан фойдаланилади. Киришни назорат қилиш тизими билан метрополитеннинг барча объектлари (жами 72 бекат ва 6 та майдонча) жиҳозланган. Москва метрополитенида эса 2024 йилнинг июнь ойидан бошлаб инсон қиёфасини идентификация қиладиган сунъий интелектдан кенг фойдаланилмоқда.

Бугунги кунда пойтахтимиз метрополитени объектларида ҳам сунъий интелект имкониятларидан фойдаланиш йўналишида бир қатор лойиҳалар ишлаб чиқилди ва тест синовлари ўтказилмоқда. Мавжуд 50 дан ортиқ бекатларда ўрнатилган видеокамераларнинг ситуатив марказдан бошқарилиши ва ИИБ Ахборот маркази маълумотлар базасига уланиши ҳеч шубҳасиз, келгусида метрополитендаги ички ишлар органлари ходимлари ишини анча енгиллаштиради ҳамда жамоат тартибини сақлаш, фуқаролар хавфсизлигини таъминлаш ва ҳуқуқбузарликларнинг олдини олишда юқори натижалар беради.

Хулоса қилиб айтганда, инсон тафаккури, ақл-идроки маҳсули бўлган сунъий интелектнинг метрополитен объектларида қўлланилиши, “хавфсиз шаҳар” тизимига интеграция қилиниши, ҳеч шубҳасиз, нафақат метрополитен, балки бутун мамлакат доирасида жамоат хавфсизлигини

таъминлашда ғоят самарали ҳисобланади ҳамда инсоннинг яқин кўмакчисига айланади.

Фойдаланилган адабиётлар:

1. Сунъий интеллект технологияларини 2030 йилга қадар ривожлантириш стратегиясини тасдиқлаш тўғрисида: Ўзбекистон Республикаси Президентининг 2024 йил 14 октябр ПҚ-358-сон Қарори. Lex.uz

2. Sun'iy intellekt texnologiyalarini 2030-yilga qadar rivojlantirish strategiyasi. URL: <https://www.lex.uz/docs/-7158604>

3. Щвецов А.В. Обеспечение безопасности и защиты метрополитенов от несанкционированного вмешательства и воздействий: Автореф. дисс. канд. тех. наук. – Москва: Российский университет транспорта (МИИТ), 2018. – С.7.

КИБЕРЖИНОЯТНИ ОЛДИНИ ОЛИШ ЙЎЛЛАРИ

Вахидов Аъзамжон Саиджонович

*ИИВ Малака ошириш институти КТФ Махсус фанлар цикли бошлиғи
доцент*

Аннотация. Ушбу мақолада замонавий жамиятда кенг тарқалаётган кибержиноятчилик муаммоси, унинг турлари ва жамият, фуқаро ҳамда давлатга етказадиган салбий оқибатлари муҳокама қилинган. Шунингдек, кибержиноятларнинг олдини олиш бўйича самарали чора-тадбирлар – ахборот хавфсизлигини таъминлаш, киберсаводхонликни ошириш, ҳуқуқий базани такомиллаштириш ва халқаро ҳамкорлик масалаларига эътибор қаратилган. Мақола ахборот технологияларидан хавфсиз фойдаланиш ва рақамли муҳитда шахсий ҳамда умумий хавфсизликни таъминлашда амалий тавсияларни ўз ичига олади.

Калит сўзлар: кибержиноят, киберхавфсизлик, ахборот хавфсизлиги, интернет жиноятлари, фишинг, рақамли хавфсизлик, компьютер жиноятлари, кибержиноятчилар, электрон жиноят, ахборот технологиялари, зарарли дастурлар, шахсий маълумотлар, киберфирибгарлик, онлайн хавфсизлик, киберҳимоя, киберсаводхонлик, кибержиноятчиликка қарши кураш, ахборотни муҳофаза қилиш, давлат хавфсизлиги, кибертерроризм

Ҳозирги рақамли асрда ахборот технологиялари ҳаётимизнинг ажралмас қисмига айланди. Интернет ва рақамли дастурлардан фойдаланиш орқали одамлар ўзаро алоқа қилади, маълумот алмашади, савдо-сотик амалга оширади ҳамда давлат хизматларидан фойдаланади. Бироқ, ахборот технологиялари имкониятлари ошгани сари улардан ноқонуний мақсадларда фойдаланувчи шахслар кибержиноятчилар ҳам кўпаймоқда. Шу сабабли,

кибержиноятчиликка қарши курашиш ва уни олдини олиш муаммоси жаҳон ҳамжамияти олдида турган долзарб масалалардан биридир.

Кибержиноят – бу интернет, компьютер тармоқлари ёки рақамли қурилмалар орқали амалга ошириладиган жиноят туридир. Улар қуйидагиларни ўз ичига олади жумладан, шахсий маълумотларни ўғирлаш (фишинг), интернетда фирибгарлик, компьютер вируслари ва зарарли дастурларни тарқатиш, давлат ва тижорат сирларини ўзлаштириш, банккомат ва банк тизимларига ноқонуний кириш, кибертерроризм ва кибершантаж.

Кибержиноятлар фақат шахсий эмас, балки жамият ва давлат миқёсида ҳам жиддий оқибатларга олиб келиши мумкин хусусан, шахсларнинг молиявий зарар кўриши, шахсий маълумотларнинг тарқалиши, ишончли маълумотларнинг бузилиши, корхона ва ташкилотлар фаолиятининг издан чиқиши, давлат хавфсизлигига таҳдид солиши мумкин.

Кибержиноятни содир этилиш сабаблари ва уларга имкон берувчи шарт-шароитларни ўрганиб чиқиб чиқмасдан уларни олдини олиш ва қарши курашиш мумкин эмас. Шу муносабат билан кибер жиноятларни содир этиш сабаблари ва уларга имкон берувчи шарт-шароитларни қуйидаги омилларга ажратиб таҳлил қилинди. Жумладан:

1. Технологик ривожланиш ва интернетнинг оммавийлашуви - ҳозирги кунда ахборот-коммуникация технологиялари тез суръатларда ривожланмоқда. Интернет ва мобил қурилмаларнинг кенг тарқалиши одамлар ҳаётини осонлаштирган бўлса-да, кибержиноятчилар учун ҳам янги имкониятлар яратди. Масалан, кўплаб қурилмалар ва тизимларда хавфсизлик чоралари етарлича мустаҳкам эмас, янги дастурлар ва технологиялар тез яратилмоқда, аммо уларни ҳимоя қилиш тизимлари ушбу ривожланишга қараб етарлича тез мослашмайди, интернетда шахсий маълумотлар очик қолиши ва уларни осонликча ёзиш мумкинлиги кибержиноятчилар учун қулайлик яратади.

2. Шахсий маълумотларга бўлган талабнинг ошиши - ҳозирги замонда шахсий маълумотлар — пул, паспорт маълумотлари, банк карталари, электрон почта ва ижтимоий тармоқ аккаунтлари — катта иқтисодий ва шахсий қийматга эга. Кибержиноятчилар бу маълумотларни ўғирлаш ёки сохталаштириш орқали молиявий фойда олишга ҳаракат қилади. Шу сабабли кибержиноятчиларнинг асосий мақсади шахсий маълумотларни тўплаш ва уларни ноқонуний йўл билан сотиш ёки фирибгарлик қилиш, инсонларнинг ўз маълумотларини интернетда бепарво тарзда тарқатиши ҳам имкон беради.

3. Хавфсизлик маданияти ва киберсаводхонликнинг пастлиги - кўп ҳолатларда кибержиноятлар инсонларнинг билими ва эҳтиёткорлиги камлиги сабаб содир этилади. Бунинг асосий сабаблари фойдаланувчиларнинг мустаҳкам пароллар танламаслиги, бир паролдан кўп жойда фойдаланиши,

электрон почта ёки мессенжерда фишинг ҳаволаларини очиш, антивирус дастурлари ва тизим янгиланишларини ўрнатмаслик, ахборот хавфсизлигига оид замонавий таҳдидлар ҳақида етарлича маълумотга эга бўлмаслик.

4. Қонунчилик ва ҳуқуқни муҳофаза қилиш тизимининг камчиликлари - кибержиноятчиликка қарши курашиш учун самарали қонунчилик зарур. Аммо кўп мамлакатларда бу соҳадаги қонунлар етарлича мустаҳкам эмас ёки тез-тез ўзгариб туради. Шунингдек, кибержиноятчиларни аниқлаш ва жиноятларни тергов қилиш мураккаб, кибержиноятчилик кўпинча халқаро даражада амалга оширилиши сабабли, давлатлар ўртасида ҳамкорлик йўқлиги ёки камлиги, жазо чоралари етарлича қатъий ва оддий эмаслиги жиноятчилик учун қулай шароит яратади.

5. Иқтисодий ва ижтимоий омиллар - кибержиноятчилик кўпинча иқтисодий қийинчиликлар, ишсизлик ва камбағаллик билан боғлиқ. Ижтимоий нотенглик, таълимсизлик ва ёшлар орасида ижтимоий қўллаб-қувватлашнинг йўқлиги қуйидаги ҳолатларга олиб келиши мумкин. Жумладан, ёшлар ва иқтисодий қийинчиликдаги шахслар осон йўл билан даромад топиш мақсадида қонунга зид ҳаракатларга қўл урмоқда, кибержиноятчиликни содир этиш учун талаб қилинадиган билимларни осон ва тез ўзлаштириш мумкинлиги.

6. Психологик ва шахсий омиллар - кибержиноятчилар кўпинча психологик жиҳатдан белгиланган хусусиятларга эга бўлади, яъни ақл-заковати ва компьютер билимлари юқори бўлган шахслар ноқонуний фойда олиш учун ўз билимларини қўллайди, жиноятчилик орқали маъмурий ва иқтисодий назоратни айлантиришга интилиш, киберхужумлар орқали ўз қудратини ва таъсирини намойиш қилиш истаги.

Кибержиноятчиликнинг содир этилиши турли сабаблар ва шарт-шароитлар билан боғлиқ бўлиб, улар бир-бири билан ўзаро боғлиқ ҳолда ишлайди. Технологик имкониятлар, инсон омили, ижтимоий-иқтисодий шароитлар ҳамда ҳуқуқий базадаги камчиликлар кибержиноятчилар учун қулай майдон яратади. Шу боис, кибержиноятларни олдини олишда нафақат техник воситалар, балки ижтимоий, иқтисодий ва ҳуқуқий чоралар комплекс ҳолда амалга оширилиши зарур.

Кибержиноятчиликни олдини олиш муаммоси ҳозирги кунда дунёдаги энг жиддий хавфлардан бири ҳисобланади. Бу борада турли соҳалардаги олимлар ва мутахассислар ўз фикрларини илмий изланишлар орқали билдирганлар.

- Джоэл Скарф (2019) ўзининг “Cybersecurity and Crime Prevention” номли асарида кибержиноятларнинг олдини олиш учун технологик воситалар, ҳуқуқий базалар ва фойдаланувчиларни хабардор қилишнинг биргаликда амалга оширилиши зарурлигини таъкидлайди. Унинг фикрига

кўра, фақатгина техник ечимларга таяниб қолиш етарли эмас, одамларнинг киберхавфсизлик борасидаги билимлари ва одатларини шакллантириш муҳимдир.

- Мария Гонсалес (2021) “International Journal of Cybersecurity” журналида интернетнинг чегара билмас табиати сабабли давлатлар ўртасида халқаро ҳамкорликнинг жуда муҳим эканини таъкидлайди. У киберқонунчиликни мувофиқлаштириш ва жинойтчиларни қидиришда ахборот алмашинуви тизимларини мустаҳкамлаш зарурлигини таъкидлайди.

- Питер Чанг (2018) “Information Security Management” асарида киберхужумларнинг кўпчилиги инсон омиллари билан боғлиқ эканини таъкидлаб, фойдаланувчиларни киберхавфсизлик бўйича доимий равишда ўқитишни энг самарали йўл деб ҳисоблайди. Унинг сўзларига кўра, фишинг ва ижтимоий муҳандислик усуллари орқали амалга ошириладиган хужумлардан ҳимоя қилишда одамларнинг хабардорлиги ҳал қилувчи аҳамиятга эга.

- Оксана Иванова (2020) “Cyber Law and Policy Review” журналида қонунчиликни доимий равишда такомиллаштириш ва жинойтчиларга нисбатан қатъий жазо чораларини қўллаш кибержинойтларни олдини олишда муҳим омиллардан эканини таъкидлайди. У, шунингдек, қонунларнинг технологиялар ривожига мослаштирилиши зарурлигини ёзади.

Бундан ташқари, Дилшод Ҳасанхўжаев, *“Киберхавфсизлик — бу фақат технология эмас, балки жамият маданияти ҳамдир. Миллий қонунчиликни такомиллаштириш билан бирга, фуқароларнинг ахборот хавфсизлиги маданиятини оширишга эътибор қаратиш керак”*⁴⁴.

Ғиёсиддин Ғафуров, *“Кибержинойтларга қарши самарали курашни учун қонунчилик тизимини доимий янгилаб бориш ва амалга ошириш жараёнларини такомиллаштириш муҳим аҳамиятга эга”*⁴⁵.

Нодиржон Ғафуров, *“Технологиялар ривожланмоқда, демак, кибержинойтларга қарши курашни усуллари ҳам доимий равишда инновацион бўлиши лозим. Бу соҳадаги илм-фанни ва амалиётни бирлаштириш зарур.”* Деб фикр билдиришигана⁴⁶.

Юқорида келтирилган олимларнинг фикридан келиб чиқиб қуйидаги фикрни билдириш мумкин. Хусусан, бугунги кунда ахборот технологиялари

⁴⁴ Дилшод Ҳасанхўжаев. “Ахборот хавфсизлиги соҳасидаги миллий қонунчиликни такомиллаштириш йўллари” Ахборот технологиялари ва коммуникацияларини ривожлантириш вазирлиги илмий журналлари.- 2021.

⁴⁵ Ғиёсиддин Ғафуров. “Кибержинойтчиликка қарши миллий қонунчиликни такомиллаштириш муаммолари”: Ўзбекистон Республикаси қонуншунослик журнали (Ўзбекистон Миллий университети нашри).- 2019.

⁴⁶ Нодиржон Ғафуров. “Инновацион технологиялар ва киберхавфсизлик муаммолари”. Тошкент ахборот технологиялари университети илмий нашрлари. 2020.

хаётимизга жуда тез ва чуқур кириб келган бир пайтда, кибержиноятлар нафақат фуқароларнинг шахсий маълумотларига, балки давлат хавфсизлиги, иқтисодиёт, таълим, тиббиёт ва бошқа муҳим соҳаларга ҳам таҳдид солмоқда. Шунинг учун кибержиноятларга қарши курашиш нафақат ҳуқуқни муҳофаза қилиш органларининг вазифаси, балки давлат сиёсатининг стратегик йўналишига айланиши керак. Кибержиноятлар — бу янги авлод жинояти. Уларга қарши курашиш учун эскича ёндашувлар етарли эмас. Миллий қонунчиликни мустаҳкамлаш, жамоатчилик онгини ошириш, илм-фанга таяниш ва халқаро тажрибани интеграция қилиш орқалигина самарали курашни ташкил этиш мумкин. Бу йўлда давлат, жамият, хусусий сектор ва албатта, олимларнинг ҳамкорлиги ҳал қилувчи аҳамиятга эга.

Кибержиноятчиликка қарши курашишда жамоавий ва шахсий даражада комплекс ёндашув зарур. Қуйида кибержиноятларнинг олдини олишда муҳим ҳисобланган чора-тадбирларни амалга ошириш мақсадга мувофиқдир:

1. Ахборот хавфсизлигини таъминлаш - ахборот хавфсизлигини таъминлаш – кибержиноятларнинг олдини олишда асосий омиллардан биридир. Бу учун, антивирус дастурларидан фойдаланиш, компьютер ва мобил қурилмаларни мунтазам янгилаб туриш, қурилмаларга парол қўйиш ва унинг мустаҳкамлигини таъминлаш, Wi-Fi тармоқларини муҳофаза қилиш (шифрлаш ва MAC-фильтрлаш усуллари).

2. Ходимлар ва фойдаланувчиларни хабардор қилиш - кибержиноятлар кўп ҳолатда одамларнинг ўзига хос билимсизлиги орқали амалга оширилади. Шунинг учун ахборот хавфсизлиги бўйича мунтазам тренинглар ташкил этиш, электрон почта орқали фишингга қарши огоҳликни ошириш, ёшлар ўртасида рақамли саводхонликни ривожлантириш.

3. Қонунчилик базасини такомиллаштириш - кибержиноятларга қарши самарали курашиш учун ахборот хавфсизлиги ва кибержиноятларга оид аниқ ва қатъий қонунлар қабул қилиниши, жиноятчиларга нисбатан мустаҳкам жазо чоралари белгиланиши, суд-тергов тизимида электрон далилларни қабул қилиш амалиётини кенгайтириш.

4. Миллий ва халқаро ҳамкорликни йўлга қўйиш - кибержиноятлар кўпинча чегара билмайди, шу боис давлатлар ўртасида киберқонунчилик бўйича келишувлар имзоланиши, интерпол ва бошқа халқаро ташкилотлар билан ҳамкорлик қилиш, ахборот алмашинувини таъминлаш ва жиноятчиларни қидиришда ҳамкорлик қилиш.

5. Рақамли технологиялардан оқилона фойдаланиш - электрон почта, мессенжер ва веб-сайтларда ҳаволаларни очишда эҳтиёт бўлиш яъни тасдиқланмаган дастурларни ўрнатмаслик, сайфрланган (HTTPS) веб-сайтлардан фойдаланиш, шахсий маълумотларни очиқ платформада тарқатмаслик.

Хулоса ўрнида шуни айтиш мумкинки, кибержиноятчилик замонавий жамият учун катта таҳдид солаётган муаммодир. Уни олдини олиш ҳар бир фуқаро, ташкилот ва давлатнинг масъулиятига боғлиқ. Ахборот хавфсизлигини таъминлаш, киберсаводхонликни ошириш, самарали қонунчилик ва халқаро ҳамкорлик – кибержиноятларга қарши курашишнинг энг муҳим йўллари дир. Фақат шундагина биз рақамли муҳитда хавфсиз ва ишончли фаолият юритиш имконига эга бўламиз.

Фойдаланилган адабиётлар рўйхати:

1. Ўзбекистон Республикаси 2022 йил 15 апрелдаги “Киберхавфсизлик тўғрисида”ги ЎРҚ-764-сон қонуни;
2. Ўзбекистон Республикаси Президентнинг 2022 йил 28 январдаги “Янги Ўзбекистоннинг 2022–2026 йилларга мўлжалланган тараққиёт стратегияси тўғрисида”ги ПФ-60-сон Фармони;
3. Роско П. Грин (Ross J. Anderson) Security Engineering: A Guide to Building Dependable Distributed Systems: 1997 (биринчи нашр);
4. Ғиёсиддин Ғафуров. “Кибержиноятчиликка қарши миллий қонунчиликни такомиллаштириш муаммолари”: Ўзбекистон Республикаси қонуншунослик журнали (Ўзбекистон Миллий университети нашри).- 2019;
5. Дилшод Ҳасанхўжаев. “Ахборот хавфсизлиги соҳасидаги миллий қонунчиликни такомиллаштириш йўллари” Ахборот технологиялари ва коммуникацияларини ривожлантириш вазирлиги илмий журналлари.- 2021;
6. Нодиржон Ғафуров. “Инновацион технологиялар ва киберхавфсизлик муаммолари”. Тошкент ахборот технологиялари университети илмий нашрлари. 2020.

AXBOROT TEXNOLOGIYALARIDAN FOYDALANGAN HOLDA SODIR ETILADIGAN HUQUQBUZARLIKLAR UCHUN MA’MURIY JAVOBGARLIK

Хожиакбар Хусанович Бахромов

ИИВ Малака оширish instituti Yuridik fanlar kafedراسи dotsenti

Annotatsiya. Maqolada axborot texnologiyalaridan foydalanish sohasidagi huquqbuzarliklar, ularning turlari, eng ko‘p sodir etiladigan ko‘rinishlari hamda ularni oldini olish va qarshi kurashish masalalari yoritilgan.

Kalit so‘zlar: axborot texnologiyalari, axborot va kompyuter tizimidan foydalanish sohasidagi huquqbuzarliklar, axborot va kompyuter tizimidan foydalanish sohasidagi huquqbuzarliklar uchun belgilangan ma‘muriy javobgarlik.

Аннотация. В статье рассматриваются правонарушения в сфере использования информационных технологий, их виды, наиболее распространенные проявления, а также вопросы предупреждения и борьбы с ними.

Ключевые слова: информационные технологии, правонарушения в сфере использования информационных и компьютерных систем, административная ответственность за правонарушения в сфере использования информационных и компьютерных систем.

Annotation. The article discusses offenses in the use of information and computer systems, their types, the most common manifestations, as well as issues of prevention and control.

Keywords: information technologies, offenses in the use of information and computer systems, administrative liability for offenses in the use of information and computer systems.

Butun dunyoda bo‘lgani kabi mamlakatimizda ham axborot-kommunikatsiya texnologiyalarining o‘rni kuchayib borayotgani, zarur axborotlardan tezkor xabardor bo‘lish, muayyan amallarni tezkor bajarish, turli interaktiv xizmatlardan tez va qulay foydalanish imkoniyatlarini beradi. Bu esa, yurtimizdagi turli korxonalar, tashkilot va muassasalarda faoliyat olib boradigan xodim va xizmatchilarning shu jumladan, fuqarolarimizning zamonaviy axborot-kommunikatsiya texnologiyalaridan samarali foydalanishlariga keng imkoniyat. Zero, global taraqqiyot sharoitida har bir odam ham axborot-kommunikatsiya texnologiyalaridan unumli foydalanish huquqiga ega.

Shu bois, yurtimizda axborot texnologiyalari, telekommunikatsiya va axborot tizimi, tarmoqlari, internet xizmatlarini rivojlantirish hamda zamonaviylashtirish muhim va asosiy yo‘nalishlardan biridir. Ushbu yo‘nalishda ularni jahon standartlariga yetkazish maqsadida keng ko‘lamli ishlar amalga oshirilmoqda.

Mazkur maqsad va natijalarga erishish hamda bu boradagi ijtimoiy munosabatlarni tartibga solish uchun respublikamizda zarur me‘yoriy-huquqiy asoslar yaratilgan jumladan, O‘zbekiston Respublikasining

“Telekommunikatsiyalar to‘g‘risida”gi, “Axborotlashtirish to‘g‘risida”gi, “Elektron raqamli imzo to‘g‘risida”gi, “Elektron hujjat aylanishi to‘g‘risida”gi, “Elektron tijorat to‘g‘risida”gi, “Elektron hukumat to‘g‘risida”gi, “Kiberxavfsizlik to‘g‘risida”gi qonunlar hamda O‘zbekiston Respublikasi Prezidentining bir qancha farmonlari, hukumat qarorlari qabul qilingan. Shuningdek, faol rivojlanib borayotgan raqamlashtirish islohotlari sharoitida ushbu me‘yoriy-huquqiy asoslar yanada takomillashtirilib borilmoqda.

Bugungi kunda, internet va raqamlashtirish davrida iqtisodiyot tarmoqlarida zamonaviy axborot-kommunikatsiya texnologiyalarini keng joriy etish, “Elektron hukumat” tizimi faoliyatini yanada rivojlantirish ustuvor ahamiyatga egadir. Jahon tajribasi shundan dalolat beradiki, ayni paytda global iqtisodiyotda kompyuter va telekommunikatsiya texnologiyalari, dasturiy ta‘minot mahsulotlarini ishlab chiqarish va ular asosida keng turdagi interfaol xizmatlar ko‘rsatishni o‘z ichiga olgan axborot-kommunikatsiya texnologiyalari sohasining roli va ahamiyati tobora ortib bormoqda.

Axborot-kommunikatsiya texnologiyalarining rivojlanishi mamlakatning raqobatdoshlik darajasiga ta‘sir ko‘rsatishi, katta hajmda axborot to‘plash va uni umumlashtirish imkonini berishi, boshqarishni strategik darajada tashkil etish uchun keng imkoniyatlar ochib berishini unutmashimiz zarur, axborot-kommunikatsiya texnologiyalarining mamlakatimizni ijtimoiy-iqtisodiy rivojlanishida tutgan o‘rni muhim ahamiyat kasb etadi.

Mazkur fikrlardan kelib chiqib shuni ta‘kidlash kerakki, bu sohada yaratilgan imkoniyatlar huquq va erkinliklar hamda ijtimoiy munosabatlarga tajovuz qilinishi ya‘ni yuqorida qayd etilgan qonunlar talablarining buzilishi – huquqshunoslikda huquqbuzarlik deb hisoblanadi hamda o‘z xususiyati ijtimoiy zarari yoki ijtimoiy xavfiga ko‘ra ikki turga tasniflanadi.

Birinchisi, ma‘muriy javobgarlik to‘g‘risidagi kodeksida nazarda tutilgan (ijtimoiy zararli) qilmishlar ma‘muriy huquqbuzarlik deb topilib ma‘muriy javobgarlikka tortilishiga sabab bo‘ladi.

Ikkinchisi, o‘z xususiyati va ijtimoiy xavfliligiga ko‘ra jinoyat kodeksida nazarda tutilgan (ijtimoiy xavfli) qilmishlar jinoyat deb topilib jinoiy javobgarlikka tortilishiga asos bo‘ladi.

O‘zbekiston Respublikasining “Axborotlashtirish to‘g‘risida”gi 2003-yil 11- dekabrda qabul qilingan 560-II-son qonunining “Hamma erkin foydalanishi mumkin bo‘lgan axborotni Internet jahon axborot tarmog‘ida tarqatish” deb nomlangan **12¹-moddasi** birinchi va ikkinchi qismlarida nazarda tutilgan talablar, majburiyatlarni buzganlik amaldagi qonunchilikka muvofiq ya‘ni, ma‘muriy yoki jinoiy javobgarlikka sabab bo‘ladi. Bular quyidagilardir:

Veb-saytning va (yoki) veb-sayt sahifasining yoxud boshqa axborot resursining egasi, shu jumladan bloger hamma erkin foydalanishi mumkin bo'lgan axborot joylashtiriladigan Internet jahon axborot tarmog'idagi o'z veb-saytidan va (yoki) veb-sayt sahifasidan yoxud boshqa axborot resursidan:

1) O'zbekiston Respublikasining mavjud konstitutsiyaviy tuzumini, hududiy yaxlitligini zo'rlik bilan o'zgartirishga da'vat etish;

2) ommaviy tartibsizliklarga, fuqarolarga nisbatan zo'ravonlik qilishga, shuningdek belgilangan tartibni buzgan holda o'tkaziladigan yig'ilishlar, mitinglarda, ko'cha yurishlarida va namoyishlarda ishtirok etishga da'vat qilish, shuningdek mazkur noqonuniy harakatlarni muvofiqlashtirish;

3) jamoat tartibiga yoki xavfsizligiga tahdid soluvchi yolg'on axborot tarqatish;

4) urush, zo'ravonlik va terrorizmni, shuningdek diniy ekstremizm, separatizm va fundamentalizm g'oyalarini targ'ib qilish;

5) davlat sirlarini yoki qonun bilan qo'riqlanadigan boshqa sirni tashkil etuvchi ma'lumotlarni oshkor etish;

6) milliy, irqiy, etnik yoki diniy adovat qo'zg'atuvchi, shuningdek fuqarolarning sha'ni va qadr-qimmatiga yoki ishchanlik obro'siga putur yetkazuvchi, ularning shaxsiy hayotiga aralashishga yo'l qo'yuvchi axborotni tarqatish;

7) jamiyatga, davlatga, davlat ramzlariga hurmatsizlikni namoyon etuvchi, shu jumladan beodoblik bilan ifodalangan axborotni tarqatish;

8) giyohvandlik vositalarini, psixotrop moddalarni va prekursorlarni targ'ib qilish;

9) pornografiyani, zo'ravonlikni va shafqatsizlikni targ'ib qilish, shuningdek o'z joniga qasd qilishga da'vat etish;

10) o'zga shaxslarga tegishli bo'lgan intellektual mulk ob'ektlaridan qonunga xilof ravishda foydalanish;

11) fuqarolarni, shu jumladan voyaga yetmagan shaxslarni ularning hayotiga va (yoki) sog'lig'iga yoxud o'zga shaxslarning hayotiga va (yoki) sog'lig'iga tahdid soluvchi g'ayrihuquqiy harakatlarni sodir etishga undashga yoki boshqa tarzda jalb qilishga qaratilgan axborotni tarqatish;

12) qonunga muvofiq jinoiy va boshqa javobgarlikka sabab bo'ladigan o'zga harakatlarni sodir etish maqsadlarida foydalanilishiga yo'l qo'ymasligi shart.

Veb-saytning va (yoki) veb-sayt sahifasining yoxud boshqa axborot resursining egasi, shu jumladan bloger:

13) hamma erkin foydalanishi mumkin bo'lgan axborot joylashtiriladigan Internet jahon axborot tarmog'idagi o'z veb-saytiga va (yoki) veb-sayt sahifasiga yoxud boshqa axborot resursiga hamma erkin foydalanishi mumkin bo'lgan

axborot joylashtirilguniga qadar uning to'g'riligini tekshirishi, shuningdek joylashtirilgan axborotning noto'g'riligi aniqlangan taqdirda, uni darhol o'chirib tashlashi;

14) hamma erkin foydalanishi mumkin bo'lgan axborot joylashtiriladigan Internet jahon axborot tarmog'idagi o'z veb-sayti va (yoki) veb-sayt sahifalari yoxud boshqa axborot resursining, shu jumladan tezkor xabarlar almashish tizimlarining monitoringini ushbu moddaning birinchi qismida ko'rsatilgan axborot va materiallarni aniqlash maqsadida amalga oshirishi;

15) ushbu moddaning birinchi qismida ko'rsatilgan axborot aniqlangan taqdirda, darhol mazkur axborotni o'chirib tashlash choralarini ko'rishi shart.

Ushbu moddaning birinchi va ikkinchi qismlarida belgilangan majburiyatlarni veb-saytning va (yoki) veb-sayt sahifasining yoxud boshqa axborot resursining egasi, shu jumladan bloger tomonidan bajarilmagan taqdirda, mazkur veb-saytdan va (yoki) veb-sayt sahifasidan yoxud boshqa axborot resursidan foydalanish O'zbekiston Respublikasi Vazirlar Mahkamasi belgilagan tartibda maxsus vakolatli organ tomonidan cheklanishi mumkin.

Mazkur moddaning birinchi va ikkinchi qismlarida nazarda tutilgan talablar veb-saytning va (yoki) veb-sayt sahifasining yoxud boshqa axborot resursining egasi, shu jumladan bloger tomonidan bajarilmaganligi natijasida huquqlari va qonuniy manfaatlari buzilgan shaxslar o'z huquqlarini, sha'ni, qadr-qimmatini va ishchanlik obro'sini himoya qilish uchun, shu jumladan zararning o'rnini qoplash, ma'naviy ziyonni kompensatsiya qilish to'g'risidagi da'volar bilan belgilangan tartibda sudga murojaat qilishga haqli.

Amaldagi Ma'muriy javobgarlik to'g'risidagi kodeksning 10-moddasiga asosan ma'muriy javobgarlik to'g'risidagi qonunchilikka binoan ma'muriy javobgarlikka tortish nazarda tutilgan, shaxsga, fuqarolarning huquqlari va erkinliklariga, mulkchilikka, davlat va jamoat tartibiga, tabiiy muhitga tajovuz qiluvchi g'ayrihuquqiy, aybli (qasddan yoki ehtiyotsizlik orqasida) sodir etilgan harakat yoki harakatsizlik ma'muriy huquqbuzarlikdir.

Mazkur huquqbuzarlik uchun ma'muriy javobgarlik, basharti bu huquqbuzarlik o'z xususiyatiga ko'ra jinoiy javobgarlikka tortishga sabab bo'lmagan taqdirda, qo'llaniladi.

Huquqbuzarlikning ikkinchi turi ya'ni jinoyat (jinoiy huquqbuzarlik) ma'muriy huquqbuzarlikdan o'z xususiyati, ijtimoiy xavfliligi hamda shaxsning sodir etgan jinoyati uchun yuzaga keladigan sudlanganlik huquqiy holati hamda jazoning og'irligi bilan farq qiladi.

Axborot texnologiyalaridan foydalangan holda sodir etiladigan ma'muriy huquqbuzarliklarni tahlil qilib ko'rib chiqishdan avval "axborot texnologiyasi" tushunchasini aniqlashtirib olish lozim.

O‘zbekiston Respublikasining “Axborotlashtirish to‘g‘risida”gi 2003 yil 11 dekabrda qabul qilingan 560-II-son qonunining “Asosiy tushunchalar” deb nomlangan 3-moddasida “axborot texnologiyasi”ga quyidagicha tushuncha berilgan:

“axborot texnologiyasi – axborotni to‘plash, saqlash, izlash, unga ishlov berish va uni tarqatish uchun foydalaniladigan jami uslublar, qurilmalar, usullar va jarayonlar”.

Axborot texnologiyalaridan foydalangan holda sodir etiladigan ma‘muriy huquqbuzarliklarni tahlil qiladigan bo‘lsak amaldagi ma‘muriy javobgarlik to‘g‘risidagi kodeksning Maxsus qismida dispozitsiyada aynan “axborot texnologiyalaridan foydalangan holda” so‘zlaridan iborat sodir etiladigan ma‘muriy huquqbuzarlik faqat 1ta (Shaxsga doir ma‘lumotlar to‘g‘risidagi qonunchilikni buzish) deb nomlangan 46²-moddada nazarda tutilgan.

Biroq, ma‘muriy huquqbuzarlikni “ommaviy axborot vositalarida, telekommunikatsiya tarmoqlarida yoki Internet jahon axborot tarmog‘ida reklama qilish, namoyish etish, tarqatish” kabi qilmishlarda namoyon bo‘lgan ma‘muriy huquqbuzarliklar soni avval ta‘kidlangan (46²-moddadagi) 1ta huquqbuzarlik bilan birga hisoblanganda 9ta moddalarda nazarda tutilgan 9ta turdagi ma‘muriy huquqbuzarliklar va ular uchun ma‘muriy javobgarlik belgilangan. Ular quyidagilar:

- 1) **46²-modda.** Shaxsga doir ma‘lumotlar to‘g‘risidagi qonunchilikni buzish;
- 2) **56²-modda.** Giyohvandlik vositalari, ularning analoglari yoki psixotrop moddalar hisoblanmaydigan kuchli ta‘sir qiluvchi moddalarni targ‘ib qiluvchi mahsulotni tayyorlash, tarqatish, reklama qilish, namoyish etish;
- 3) **56⁴-modda.** Giyohvandlik vositalarini, ularning analoglarini yoki psixotrop moddalarni targ‘ib qiluvchi mahsulotni tayyorlash, tarqatish, reklama qilish, namoyish etish
- 4) **189-modda.** Pornografik mahsulotni tayyorlash, olib kirish, tarqatish, reklama qilish, namoyish etish
- 5) **189¹-modda.** Tazyiqni, zo‘ravonlikni yoki shafqatsizlikni targ‘ib qiluvchi mahsulotni tayyorlash, olib kirish, tarqatish, reklama qilish, namoyish etish
- 6) **191-modda.** Qimor va tavakkalchilikka asoslangan boshqa o‘yinlar (3-qismida);
- 7) **195²-modda.** Huquqni muhofaza qiluvchi organlar xodimlarining foto- va (yoki) videotasvirini ularning obro‘sizlantirilishiga olib keladigan tarzda buzib tarqatish
- 8) **201¹-modda.** Qonunchilik hujjatlarini bajarmaslikka yoki buzishga omma oldida da‘vat qilish
- 9) **202²-modda.** Yolg‘on axborot tarqatish (1, va 2-qismlarida).

Yuqorida ko‘rib chiqilgan masalalardan kelib chiqib shuni ta’kidlash kerakki, mamlakatimizda axborot va kompyuter tizimidan foydalanish sohasidagi ijtimoiy munosabatlar normativ-huquqiy jihatdan to‘liq huquqiy tartibga solingan hamda ma’muriy va jinoiy-huquqiy jihatdan muhofazalangan.

Shu bois, jamiyatimizning barcha a’zolari ayniqsa, yoshlar mazkur qonunchilikning mazmuni, mohiyati va talablarini tushunishi, o‘rganishi hamda eng avvalo ularning talablariga rioya etishlari muhim hamda zaruriy ahamiyat kasb etadi.

Foydalanilgan adabiyotlar ro‘yxati:

1. O‘zbekiston Respublikasi Konstitutsiyasi. (Yangi tahrirda) 2023 yil 30 aprel.
2. O‘zbekiston Respublikasining “Kiberxavsizlik to‘g‘risida”gi O‘RQ-764-son qonuni. 2022 yil 15 aprel.
3. O‘zbekiston Respublikasining Ma’muriy javobgarlik to‘g‘risidagi kodeksi. O‘zbekiston Respublikasi Oliy Kengashining Axborotnomasi. 1995. 1-son.
4. O‘zbekiston Respublikasining Jinoyat kodeksi. O‘zbekiston Respublikasi Oliy Kengashining Axborotnomasi. 1995. 1-son.
5. O‘zbekiston Respublikasining 2024 yil 19 yanvardagi O‘RQ-899-sonli qonuni. Qonunchilik ma’lumotlari milliy bazasi, 19.01.2024 y., 03/24/899/0048-son.

AXBOROT TEXNOLOGIYALARI SOHASIDAGI HUQUQBUZARLIKLARNING HUQUQIY ASOSLARI

Xojiakbar Xusanovich Baxramov

IIV Malaka oshirish instituti Yuridik fanlar kafedrasi dotsenti

Subanov Olinjon Suyarkul o‘g‘li

IIV Malaka oshirish instituti Yuridik fanlar kafedrasi katta o‘qituvchisi

Annotasiya. Mazkur maqolada axborot texnologiyalari sohasidagi huquqbuzarliklarning huquqiy asoslari yoritilgan.

Kalit soʻzlar: Axborot texnologiyalari, huquqbuzarliklar profilaktikasi, huquqbuzarlikning obʻekti, huquqbuzarlikning obʻektiv tomoni, huquqbuzarlikning subʻekti, huquqbuzarlikning subʻektiv tomoni.

Yurtimizda jadallik bilan zamonaviy axborot-kommunikatsiya texnologiyalarining oʻrni tobora ortib borayotgani, zarur axborotlardan tezkor xabardor boʻlish, turli interaktiv xizmatlardan foydalanish imkonini yaratmoqda. Bu esa, jamiyatimiz aʼzolarining shu jumladan yoshlarning zamonaviy axborot-kommunikatsiya texnologiyalaridan samarali foydalanishlarini taqozo etadi. Zero, global taraqqiyot sharoitida har bir inson ham axborot-kommunikatsiya texnologiyalaridan unumli foydalanish huquqiga ega. Chunki, ularning kunlik faoliyatida amalga oshiradigan ishlarida kompyuter texnikasidan, tarmoq texnologiyalaridan unumli foydalanishlari ularning ish sifatini ortishi, sarflanadigan vaqtni tejash imkonini beradi.

Shuning uchun, mamlakatimizda kompyuter va axborot texnologiyalari, telekommunikatsiya va maʼlumot uzatish tarmoqlari, internet xizmatlarini rivojlantirish hamda zamonaviylashtirish muhim va asosiy yoʻnalishlardan biri. Mazkur yoʻnalishda ularni jahon standartlariga yetkazish maqsadida keng koʻlamli ishlar amalga oshirildi va bu boradagi ishlar izchillik bilan davom ettirilmoqda.

Ushbu maqsad va natijalarga erishish hamda bu boradagi ijtimoiy munosabatlarni tartibga solish uchun respublikamizda muhim meʼyoriy-huquqiy asoslar yaratilgan jumladan, Oʻzbekiston Respublikasining “Aloqa toʻgʻrisida”gi, “Pochta aloqasi toʻgʻrisida”gi, “Telekommunikatsiyalar toʻgʻrisida”gi, “Axborotlashtirish toʻgʻrisida”gi, “Elektron raqamli imzo toʻgʻrisida”gi, “Elektron hujjat aylanishi toʻgʻrisida”gi, “Elektron tijorat toʻgʻrisida”gi, “Elektron hukumat toʻgʻrisida”gi, “Kiberxavfsizlik toʻgʻrisida”gi qonunlar hamda Oʻzbekiston Respublikasi Prezidentining qator farmonlari, hukumat qarorlari qabul qilingan. Shuningdek, faol rivojlanib borayotgan bozor munosabatlari sharoitida ushbu meʼyoriy-huquqiy asoslar yanada takomillashtirilib borilmoqda.

Raqamli iqtisodiyotni faol rivojlantirish, barcha tarmoqlar va sohalarda, eng avvalo, davlat boshqaruvi, taʼlim, sogʻliqni saqlash va qishloq xoʻjaligida zamonaviy axborot-kommunikatsiya texnologiyalarini keng joriy etish boʻyicha kompleks chora-tadbirlar amalga oshirilmoqda. Jumladan, elektron hukumat tizimini takomillashtirish, dasturiy mahsulotlar va axborot texnologiyalarining mahalliy bozorini yanada rivojlantirish, respublikaning barcha hududlarida IT-parklarni tashkil etish, shuningdek, sohani malakali kadrlar bilan taʼminlashni koʻzda tutuvchi 220 dan ortiq ustuvor loyihalarni amalga oshirish boshlangan.

Shuningdek, 40 dan ortiq axborot tizimlari bilan integratsiyalashgan geoportalni ishga tushirish, jamoat transporti va kommunal infratuzilmani boshqarishning axborot tizimini yaratish, ijtimoiy sohani raqamlashtirish va

keyinchalik ushbu tajribani boshqa hududlarda joriy qilishni nazarda tutuvchi «Raqamli Toshkent» kompleks dasturi izchillik bilan amalga oshirilmoqda.

Mamlakatimizda raqamli industriyani jadal rivojlantirish, milliy iqtisodiyot tarmoqlarining raqobatbardoshligini oshirish maqsadida O‘zbekiston Respublikasi Prezidentining 2020-yil 5-oktabrda «Raqamli O‘zbekiston–2030» Strategiyasini tasdiqlash va uni samarali amalga oshirish chora-tadbirlari to‘g‘risida PF-6079-son Farmoni bilan «Raqamli O‘zbekiston –2030» Strategiyasi tasdiqlangan [1].

Mazkur Strategiya iqtisodiyot tarmoqlari, ijtimoiy soha va davlat boshqaruvi tizimining jadal raqamli rivojlanishini ta‘minlash, shu jumladan elektron davlat xizmatlarini ko‘rsatish mexanizmlarini yanada takomillashtirish maqsadida ishlab chiqilgan. Strategiya O‘zbekiston Respublikasining raqamli iqtisodiyot va elektron hukumatni rivojlantirishning strategik maqsadlari, ustuvor yo‘nalishlari hamda o‘rta va uzoq muddatli istiqbolli vazifalarini belgilaydi, shuningdek, BMTning Barqaror rivojlanish maqsadlari va Elektron hukumatni rivojlantirish reytingida belgilangan ustuvor vazifalardan kelib chiqib, raqamli texnologiyalarni yanada keng joriy etish uchun asos bo‘lib xizmat qiladi.

Mazkur sohada yaratilgan imkoniyatlar huquq va erkinliklar hamda ijtimoiy munosabatlarga tajovuz qilinishi ya‘ni, yuqorida qayd etilgan qonun va qonun osti hujjatlar talablarining buzilishi – huquqbuzarlik deb hisoblanadi hamda muayyan yuridik javobgarlikka tortilishga sabab bo‘ladi. O‘zbekiston Respublikasining “Huquqbuzarliklar profilaktikasi to‘g‘risida”gi 2014-yil 14-may qonunining 3-moddasiga binoan “huquqbuzarlik – sodir etilganligi uchun ma‘muriy yoki jinoiy javobgarlik nazarda tutilgan aybli g‘ayrihuquqiy qilmish (harakat yoki harakatsizlik) dir [2].

O‘zbekiston Respublikasining Ma‘muriy javobgarlik to‘g‘risidagi kodeksining 10-moddasiga asosan ma‘muriy javobgarlik to‘g‘risidagi qonunchilikka binoan ma‘muriy javobgarlikka tortish nazarda tutilgan, shaxsga, fuqarolarning huquqlari va erkinliklariga, mulkchilikka, davlat va jamoat tartibiga, tabiiy muhitga tajovuz qiluvchi g‘ayrihuquqiy, aybli (qasddan yoki ehtiyotsizlik orqasida) sodiretilgan harakat yoki harakatsizlik ma‘muriy huquqbuzarlikdir [3].

Mazkur huquqbuzarlik uchun ma‘muriy javobgarlik, basharti bu huquqbuzarlik o‘z xususiyatiga ko‘ra jinoiy javobgarlikka tortishga sabab bo‘lmagan taqdirda, amalga oshiriladi.

Huquqbuzarlikning ikkinchi turi ya‘ni, jinoyat (jinoiy huquqbuzarlik) ma‘muriy huquqbuzarlikdan ijtimoiy xavfliligi hamda shaxsning sodir etgan jinoyati uchun hukm etilganida yuzaga keladigan sudlanganlik huquqiy holati bilan farq qiladi.

O‘zbekiston Respublikasining Jinoyat kodeksining 14-moddasiga binoan Jinoyat kodeksi bilan taqiqlangan, aybli ijtimoiy xavfli qilmish (harakat yoki

harakatsizlik) jazo qo‘llash tahdidi bilan jinoyat deb topiladi. Jinoyat kodeksi bilan qo‘riqlanadigan ob‘ektlarga zarar yetkazadigan yoki shunday zarar yetkazish real xavfini keltirib chiqaradigan qilmish ijtimoiy xavfli qilmish deb topiladi.

O‘zbek tilining izohli lug‘atida kompyuter (*ingl. computer, lotincha computare – hisoblamoq, hisoblab chiqmoq ma’nolarini bildiradi*) murakkab qurilmaga ega bo‘lgan elektron hisoblash mashinasidir. O‘zbekiston Respublikasi Ma’muriy javobgarlik to‘g‘risidagi kodeksining “Transportdagi, yo‘l xo‘jaligi va aloqa sohalaridagi huquqbuzarliklar uchun ma’muriy javobgarlik” deb nomlangan XI-bobida Aloqa, axborot tizimi va kompyuter tizimidan foydalanish qoidalarini buzganlik uchun 151–156-moddalarida ya’ni, jami 8ta moddada nazarda tutilgan huquqbuzarliklarni sodir etganlik uchun ma’muriy javobgarlik belgilangan. Boshqacha qilib aytganda, 8 ta turdagi qonunga xilof qilmishlar uchun ma’muriy javobgarlik nazarda tutilgan. Ular quyidagilardir:

151-modda. Ruxsatsiz radiouzatkich shoxobchasi o‘rnatish va (yoki) undan foydalanish, shuningdek abonentlik qurilmasini elektr aloqa tarmoqlariga ulash;

152-modda. Radioelektron vositalar va yuqori chastotali qurilmalardan foydalanish tartibini buzish;

153-modda. Aloqa xizmatining sifatiga doir normalar va davlat standartlarini buzish;

154-modda. Aloqa yo‘llari va inshootlarini muhofaza qilish qoidalarini buzish;

155-modda. Axborotdan foydalanish qoidalarini buzish;

155¹-modda. Kompyuter tizimidan foydalanish qoidalarini buzish;

155²-modda. Telekommunikatsiya tarmog‘idan qonunga xilof ravishda (ruxsatsiz) foydalanish;

156-modda. Avtomat telefonlarni shikastlantirish.

Ulardan ayrimlarini yuridik tahlil qiladigan bo‘lsak, jumladan, kodeksning

155-moddasi Axborotdan foydalanish qoidalarini buzish deb nomlangan bo‘lib, ushbu modda to‘rt ta qismdan iborat bo‘lib, quyidagi g‘ayrihuquqiy qilmishlar uchun ma’muriy javobgarlikni nazarda tutadi.

Axborot tizimidan foydalanish maqsadida unga ruxsatsiz kirib olishda ifodalangan axborot va axborot tizimlaridan foydalanish qoidalarini buzish – fuqarolarga bazaviy hisoblash miqdorining uchdan bir qismidan bir baravarigacha, mansabdor shaxslarga esa – bir baravaridan uch baravarigacha miqdorda jarima solishga sabab bo‘ladi.

Axborot tizimlarining ishini buzishga olib kelgan huddi shunday huquqbuzarlik, huddi shuningdek kirish cheklangan axborot tizimlarini axborot-hisoblash tarmoqlariga ulash chog‘ida tegishli himoya choralarini ko‘rmaganlik – fuqarolarga bazaviy hisoblash miqdorining bir baravaridan uch baravarigacha,

mansabdor shaxslarga esa – uch baravaridan besh baravarigacha miqdorda jarima solishga sabab bo‘ladi.

Yuridik va jismoniy shaxslarning axborot tizimlarini xalqaro axborot tarmoqlariga qonunga xilof ravishda ulash, bu tarmoqlarga tegishli himoya choralarini ko‘rmasdan ulanish, huddi shuningdek ulardan ma’lumotlarni qonunga xilof ravishda olish – fuqarolarga bazaviy hisoblash miqdorining ikki baravaridan besh baravarigacha, mansabdor shaxslarga esa – besh baravaridan yetti baravarigacha miqdorda jarima solishga sabab bo‘ladi.

O‘zganing elektron hisoblash mashinalari uchun yaratilgan dasturi yoki ma’lumotlar bazasini o‘z nomidan chiqarish yoxud qonunga xilof ravishda undan nusxa olish yoki bunday asarlarni tarqatish – fuqarolarga bazaviy hisoblash miqdorining bir baravaridan uch baravarigacha, mansabdor shaxslarga esa –uch baravaridan besh baravarigacha miqdorda jarima solishga sabab bo‘ladi.

Mazkur huquqbuzarlikning yuridik tarkibini quyidagicha ifodalash mumkin.

Huquqbuzarlikning ob‘ekti –aloqa, axborot va axborot tizimidan foydalanish sohasidagi qonunchilik bilan qo‘riqlanadigan ijtimoiy munosabatlardir.

Huquqbuzarlikning ob‘ektiv tomoni – g‘ayrihuquqiy harakat, shuningdek harakatsizlikda ifodalanadigan qilmishlardir. Jumladan, ushbu moddaning birinchi va to‘rtinchi qismlarida nazarda tutilgan qilmishlar g‘ayrihuquqiyharakat orqali sodir etiladi. 155-moddaning ikkinchi va uchinchi qismlarida nazarda tutilgan qilmishlar g‘ayrihuquqiy harakat bilan ham harakatsizlik bilan ham sodir etilishi mumkin.

Huquqbuzarlikning sub‘ektiv tomoni – qasddan ham ehtiyotsizlik orqasida ham sodir etilishi mumkin bo‘lgan qilmishlardir.

Huquqbuzarlikning sub‘ekti –16 yoshga to‘lgan aqli raso jismoniy shaxslar ya’ni, fuqarolar shuningdek, mansabdor shaxslar ham javobgarlikka tortilishi mumkin. Mazkur huquqbuzarlikni jinoyat ishlari bo‘yicha tuman (shahar) sudlari ko‘rib chiqib jazo qo‘llash to‘g‘risida qaror qabul qiladilar.

Ma‘muriy javobgarlik to‘g‘risidagi kodeksning 155¹-moddasi Kompyuter tizimidan foydalanish qoidalarini buzish deb nomlangan hamda ushbu modda ikki qismdan iborat bo‘lib, quyidagi g‘ayrihuquqiy qilmishlar uchun ma‘muriy javobgarlikni nazarda tutadi.

Kompyuter tizimidan foydalanishga ruxsati bo‘lgan shaxsning ushbu tizimdan foydalanishning belgilangan qoidalarini buzishi kompyuter axborotining yo‘q qilib yuborilishiga, to‘sib qo‘yilishiga, modifikatsiyalashtirilishiga, kompyuter uskunasi ishlashining buzilishiga sabab bo‘lsa, – fuqarolarga bazaviy hisoblash miqdorining besh baravaridan yetti baravarigacha, mansabdor shaxslarga esa – yetti baravaridan o‘n baravarigacha miqdorda jarima solishga sabab bo‘ladi.

Xuddi shunday huquqbuzarlik konfidensial axborot mavjud bo'lgan kompyuter tizimidan foydalanish vaqtida sodir etilsa, – fuqarolarga bazaviy hisoblash miqdorining yetti baravaridan o'n baravarigacha, mansabdor shaxslarga esa – o'n baravaridan o'n besh baravarigacha miqdorda jarima solishga sabab bo'ladi.

Mazkur huquqbuzarlikning yuridik tarkibini quyidagicha ifodalash mumkin.

Huquqbuzarlikning ob'ekti – axborot va kompyuter tizimidan foydalanish sohasidagi qonunchilik bilan qo'riqlanadigan ijtimoiy munosabatlardir.

Huquqbuzarlikning ob'ektiv tomoni – moddaning birinchi, ikkinchi qismida ham g'ayrihuquqiy harakat bilan sodir etiladigan qilmishlardir.

Huquqbuzarlikning sub'ektiv tomoni – qasddan sodir etilishi mumkin bo'lgan qilmishlardir.

Huquqbuzarlikning sub'ekti sifatida – kompyuter tizimidan foydalanishga ruxsati bo'lgan shaxs shuningdek mansabdor shaxs ham javobgarlikka tortilishi mumkin.

Ma'muriy javobgarlik to'g'risidagi kodeksning 245-moddasiga binoan mazkur huquqbuzarlikni ham jinoyat ishlari bo'yicha tuman (shahar) sudlari ko'rib chiqib jazo qo'llash to'g'risida qaror qabul qiladilar.

Shuningdek, ma'muriy javobgarlik to'g'risidagi qonunchilikda ommaviy axborot vositalarida, telekommunikatsiya tarmoqlarida yoki Internet jahon axborot tarmog'idan foydalangan holda birinchi marotaba sodir etilgan yana quyidagi qilmishlar uchun ham ma'muriy javobgarlik belgilangan jumladan, ular quyidagi huquqbuzarliklardir:

1. **189-modda.** Pornografik mahsulotni tayyorlash, olib kirish, tarqatish, reklama qilish, namoyish etish – ommaviy axborot vositalarida, telekommunikatsiya tarmoqlarida yoki Internet jahon axborot tarmog'ida reklama qilish, namoyish etish, tarqatish uchun;

2. **189¹-modda.** Tazyiqni, zo'ravonlikni yoki shafqatsizlikni targ'ib qiluvchi mahsulotni tayyorlash, olib kirish, tarqatish, reklama qilish, namoyish etish – ommaviy axborot vositalarida, telekommunikatsiya tarmoqlarida yoki Internet jahon axborot tarmog'ida reklama qilish, namoyish etish, tarqatish uchun;

3. **191-modda.** Qimor va tavakkalchilikka asoslangan boshqa o'yinlar – Qimor va tavakkalchilikka asoslangan boshqa o'yinlarni tashkil etish yoki o'tkazish uchun telekommunikatsiya tarmoqlarida, shu jumladan Internet jahon axborot tarmog'i provayderlari tomonidan xizmatlar ko'rsatish yoki xizmatlar ko'rsatishga ko'maklashish, tegishli dasturiy ta'minotdan nusxa ko'paytirish, uni ko'paytirish, tarqatish uchun;

4. **201¹-modda.** Qonunchilik hujjatlarini bajarmaslikka yoki buzishga omma oldida da'vat qilish – O'zbekiston Respublikasining qonunchilik hujjatlari talablarini jamoat tartibiga va jamoat xavfsizligiga tahdid soladigan tarzda bajarmaslikka yoki buzishga, shu jumladan ommaviy axborot vositalaridan, telekommunikatsiya tarmoqlaridan, Internet jahon axborot tarmog'idan, shuningdek matni ko'paytirishning bosma yoki boshqa usullaridan foydalangan holda omma oldida da'vat qilish uchun;

5. **202²-modda.** Yolg'on axborot tarqatish – Shaxsning qadr-qimmati kamsitilishiga yoki uning obro'sizlantirilishiga olib keladigan yolg'on axborotni tarqatish, shu jumladan ommaviy axborot vositalarida, telekommunikatsiya tarmoqlarida yoki Internet jahon axborot tarmog'ida tarqatish uchun ma'muriy javobgarlik belgilangan.

Yuqorida ko'rib chiqilgan masalalardan kelib chiqib shuni ta'kidlash kerakki, mamlakatimizda zamonaviy axborot-kommunikatsiya texnologiyalari tizimidan foydalanish sohasidagi ijtimoiy munosabatlar normativ-huquqiy jihatdan to'liq huquqiy tartibga solingan hamda ma'muriy va jinoiy-huquqiy jihatdan muhofazalangan. Zero, mazkur qonunchilikni buzganlikda aybdor bo'lgan shaxslar belgilangan tartibda javobgarlikka tortiladi. Demak, jamiyatimizning barcha a'zolari shu jumladan, yoshlar mazkur qonun hujjatlarining mohiyati vatalablarini tushunishi, o'rganishi hamda ularning talablariga rioya etishlari muhim ahamiyat kasb etadi.

Foydalanilgan adabiyotlar:

1. O'zbekiston Respublikasi Prezidentining 2020-yil 5-oktyabrda «Raqamli O'zbekiston–2030» Strategiyasini tasdiqlash va uni samarali amalga oshirish chora-tadbirlari to'g'risida PF-6079-son Farmoni. <https://lex.uz/uz/docs/5030957>

2. O'zbekiston Respublikasining 2014-yil 14-may kunidagi “Huquqbuzarliklar profilaktikasi to'g'risida”gi O'RQ-371-son qonuni. <https://lex.uz/docs/2387357?ONDATE2=26.01.2022&action=compare>.

3. O'zbekiston Respublikasining Ma'muriy javobgarlik to'g'risidagi kodeksi. 2025 <https://lex.uz/docs/97664>

4. O'zbekiston Respublikasining Jinoyat kodeksi. 2025 <https://www.lex.uz/acts/111453>

AXBOROT TEXNOLOGIYALARIDAN FOYDALANGAN HOLDA SODIR ETILADIGAN HUQUQBUZARLIKLARNING OLDINI OLISHDA SUN'IY INTELLEKTNING O'RNI

Beysenov Kenjabay Sarsanbayevich

IIV Malaka oshirish instituti KTF Maxsus fanlar sikli o'qituvchisi

bisenovkenjaboy@gmail.com

Annotatsiya. Mazkur maqolada axborot texnologiyalaridan foydalangan holda sodir etiladigan huquqbuzarliklarning oldini olishda sun'iy intellektning o'rni bo'yicha ilmiy asoslangan taklif va tavsiyalar berilgan.

Kalit so'zlar: Internet, axborot texnologiyalari. huquqbuzarliklarning oldini olish, raqamli texnologiyalar, axborotni saqlash va yig'ish; axborotni tizimlashtirish, sun'iy intellekt, komp'yuter tarmoqlari, monitoring.

Аннотация. В данной статье даны научно обоснованные предложения и рекомендации по роли искусственного интеллекта в предупреждении правонарушений, совершаемых с использованием информационных технологий.

Ключевые слова: Интернет, информационные технологии. профилактика правонарушений, цифровые технологии, хранение и сбор информации; систематизация информации, искусственный интеллект, компьютерные сети, мониторинг

Annotation. this article provides scientifically based proposals and recommendations on the role of artificial intelligence in the Prevention of violations committed using information technology.

Keywords: Internet, Information Technology. prevention of violations, digital technologies, storage and collection of information; systematization of information, artificial intelligence, computer networks, monitoring.

Jadal rivojlanayotgan axborot texnologiyalari jamiyat hayotining deyarli barcha sohalariga chuqur kirib borgan. Biroq ushbu imkoniyatlar bilan birga, kiberxuquqbuzarliklar, ma'lumotlar o'g'irlanishi, soxta kontent tarqatilishi kabi xavfli illatlar ham paydo bo'lmoqda. Sun'iy intellekt (SI) ushbu tahdidlarni bartaraf etishda muhim vositaga aylanmoqda.

1. Axborot texnologiyalari orqali sodir etiladigan huquqbuzarliklar

Axborot texnologiyalari yordamida amalga oshiriladigan huquqbuzarliklar turlicha ko'rinishda bo'lishi mumkin:

- Fishing va kiberhujumlar – shaxsiy ma'lumotlarni qonuniysiz olishga qaratilgan harakatlar;
- Soxta xabarlar tarqatilishi (feyklar) – jamoat fikriga ta'sir qilish yoki panika keltirib chiqarish maqsadida tarqatiladi;
- Dipfeyk texnologiyalari – soxta video va audiolar orqali shaxs sha'niga dog' tushirish;
- Onlayn firibgarlik – elektron to'lovlar va shubhali savdo platformalari orqali.

Kiberxavfsizlik bo'yicha xalqaro tashkilotlar ma'lumotlariga ko'ra, 2023 yilda faqatgina feyk kontent tarqatilishi bilan bog'liq jinoyatlar 37% ga oshgan. [1]

2. Sun'iy intellektning huquqbuzarliklarni aniqlash va oldini olishdagi ahamiyati

Sun'iy intellekt axborot sohasidagi jinoyatlarga qarshi quyidagi yo'llar bilan samarali kurash olib boradi:

2.1. Avtomatik tahlil va monitoring

Sun'iy intellekt algoritmlari turli platforma va veb-saytlardagi ma'lumotlarni real vaqtda tahlil qilib, shubhali kontentni aniqlaydi. Masalan, "natural language processing (NLP)" texnologiyalari orqali yozma materiallarda yolg'on va buzg'unchi mazmundagi ifoda va konstruksiyalar tan olinadi.

Google va Meta kabi korporatsiyalar NLP asosida feyk xabarlarini 95% holatda aniqlash imkoniyatiga ega ekanini ma'lum qilgan. [2]

2.2. Kiberxujumlarni bashorat qilish

SI vositalari kiberhujum belgilari (IP harakatlar, noodatiy faollik, ma'lumotlarning shifrlanishi)ni oldindan tahlil qilib, hujumlarni oldindan bashorat qilishi mumkin.

IBM Security 2024 hisobotiga ko'ra, sun'iy intellekt asosidagi kiberxavfsizlik tizimlari 43% kamroq zarar bilan ishlaydi. [3]

2.3. Foydalanuvchi xulqini tahlil qilish

Sun'iy intellekt orqali foydalanuvchining internetdagi xatti-harakatlari tahlil qilinib, ularni shubhali yoki standartdan chetga chiqqan holatlarda avtomat ravishda xabar berish yoki bloklash amaliyoti yo'lga qo'yiladi.

PayPal va Mastercard kabi moliyaviy platformalarda AI yordamida transaksiyalarning 99% xavfsizligi ta'minlanadi. [4]

3. Sun'iy intellekt asosidagi huquqiy chora-tadbirlar va algoritmlar

Sun'iy intellekt huquqbuzarliklarga qarshi faqat texnik emas, balki huquqiy va institutsional usullar orqali ham faoliyat ko'rsatishi mumkin:

- Fuqarolarni himoya qilish: shaxsiy ma'lumotlardan foydalanish qoidalarini nazorat qilish;

- Kontentni belgilash (markirovka): shubhali ma'lumotlarni avtomat belgilash va foydalanuvchini ogohlantirish;

- Jinoiy tahdidlarni prognoz qilish: ma'lumotlar bazasi va tarixiy ma'lumotlarga tayangan holda potensial tahdidlarni bashorat qilish.

Yevropa Ittifoqining 2023 yilda qabul qilingan "AI Act" hujjatida yuqori xavfli sun'iy intellekt tizimlarini huquqiy nazoratga olish belgilab qo'yilgan. [5]

4. O'zbekistonda sun'iy intellekt va axborot xavfsizligi sohasidagi islohotlar

O‘zbekistonda ham axborot xavfsizligini ta‘minlash va sun‘iy intellekt texnologiyalarini huquqbuzarliklarga qarshi qo‘llash borasida qator ishlar amalga oshirilmoqda:

O‘zbekiston Respublikasi Prezidentining 2020 yil 5 oktyabrdagi "Raqamli O‘zbekiston - 2030" [Strategiyasini](#) tasdiqlash va uni samarali amalga oshirish chora-tadbirlari to‘g‘risidagi PF-6079-son Farmonining 1-ilovasi bilan “Raqamli O‘zbekiston — 2030» [strategiyasi](#)” qabul qilindi;

- 2021–2024 yillarda Kiberxavfsizlik strategiyasi doirasida axborot xatarlarini bartaraf etish tizimlari joriy etildi;

- Axborot texnologiyalari va sun‘iy intellekt vositalarini qonuniy maqsadlarda qo‘llashni rag‘batlantiruvchi farmon va qarorlar qabul qilingan.

O‘zbekiston Respublikasi Prezidentining 2024 yil 14 oktyabrdagi “Sun‘iy intellekt texnologiyalarini 2030 yilga qadar rivojlantirish strategiyasini tasdiqlash to‘g‘risida”gi PQ-358-son qarorining 1-ilovasi bilan “Sun‘iy intellekt texnologiyalarini 2030 yilga qadar rivojlantirish strategiyasi”tasdiqlangan. [6]

5. Muammolar va yechimlar

5.1. Eticheskiy va huquqiy muammolar

Sun‘iy intellekt mustaqil qaror qabul qilganda, uning oqibati uchun kim javob beradi? Bu javobgarlik masalasi ayniqsa muhimdir.

5.2. Yechimlar:

- Sun‘iy intellekt algoritmlarini shaffoflashtirish;
- Davlat va xususiy sektor hamkorligini kuchaytirish;
- Axborot savodxonligini oshirish;
- Xalqaro tajriba asosida huquqiy bazani takomillashtirish.

Harvard AI Ethics Lab tavsiyasiga ko‘ra, har bir SI tizimi uchun alohida hisobotlilik mexanizmi joriy qilinishi kerak. [7]

Xulosa o‘rnida, axborot texnologiyalaridan foydalanilgan holda sodir etiladigan huquqbuzarliklar zamonaviy jamiyat xavfsizligiga jiddiy tahdid solmoqda. Sun‘iy intellekt bu tahdidlarga qarshi samarali kurash olib borish uchun muhim vosita hisoblanadi. O‘zbekistonda mazkur yo‘nalishda tashlangan qadamlar ijobiy natija bermoqda. Biroq bu sohadagi qonunchilikni muntazam ravishda yangilab borish, axborot savodxonligini oshirish va xalqaro hamkorlikni kengaytirish juda muhim.

Foydalanilgan adabiyotlar ro‘yxati:

1. Cybercrime Trends Report – Interpol, 2024
2. Meta AI Content Moderation Whitepaper, 2023
3. IBM Security AI in Cyber Defense Report, 2024
4. Mastercard AI Transaction Security Report, 2023
5. European Union AI Act, 2023

6. O‘zbekiston Respublikasi Prezidentining 2024 yil 14 oktyabrdagi “Sun’iy intellekt texnologiyalarini 2030 yilga qadar rivojlantirish strategiyasini tasdiqlash to‘g‘risida”gi PQ-358-son qarori – www.lex.uz
7. Harvard University AI Ethics Lab Guidelines, 2023

AXBOROT MAKONIDA EKSTREMIZM VA RADIKALIZM: JISMONIY TAYYORGARLIK VA SPORT ORQALI IMMUNITETNI SHAKLLANTIRISH

Burxonov Bahodir Hayotovich

O‘zbekiston Respublikasi Ichki ishlar vazirligi

Malaka oshirish instituti Jismoniy tayyorgarlik sikli o‘qituvchisi

bahodirburxonov87@gmail.com

Annotatsiya. Ushbu maqolada zamonaviy axborot makonida ekstremistik va radikal g‘oyalar tarqalishining xavflari hamda ularga qarshi kurashishda yoshlar orasida jismoniy tayyorgarlik va sportning ijtimoiy-psixologik ahamiyati yoritilgan. Sport faoliyatining nafaqat jismoniy sog‘lomlashtirish, balki ijtimoiy ong va qaror qabul qilish madaniyatini shakllantirishdagi o‘rni tahlil qilinadi.

Kalit so‘zlar: ekstremizm, radikalizm, axborot makoni, sport, jismoniy tayyorgarlik, raqamli tahdid, yoshlar, ijtimoiy immunitet.

Аннотация. В статье рассматриваются современные угрозы, связанные с распространением экстремистских и радикальных идей в информационном пространстве, особенно среди молодежи. Подчеркивается значимость физической подготовки и спорта как эффективных средств формирования психологической устойчивости, гражданского самосознания и социальной ответственности. Анализируются возможности спорта в профилактике вовлечения молодежи в деструктивные идеологии, а также представлены практические рекомендации по укреплению информационного иммунитета через физическую активность.

Ключевые слова: экстремизм, радикализм, информационное пространство, молодежь, спорт, физическая подготовка, информационная безопасность, цифровые угрозы, социальная устойчивость.

Abstract. This article explores the growing threats posed by the spread of extremist and radical ideologies in the digital environment, particularly among youth. It highlights the role of physical training and sports as effective tools for developing psychological resilience, civic awareness, and social responsibility. The paper analyzes how sports can serve as a preventive mechanism against youth

involvement in destructive ideologies and offers practical recommendations for enhancing digital immunity through physical activity.

Keywords: extremism, radicalism, information space, youth, sports, physical training, information security, digital threats, social resilience.

Kirish. Raqamli transformatsiya va internet texnologiyalarining keskin rivojlanishi bilan bir qatorda, axborot makonida ijtimoiy barqarorlikka tahdid soluvchi radikal va ekstremistik g'oyalarning tarqalish xavfi ham ortib bormoqda. Ayniqsa, yoshlar ushbu axborot oqimlariga eng ko'p ta'sirchan qatlam hisoblanadi. Shu bois, nafaqat texnik va huquqiy choralar, balki ijtimoiy-psixologik himoya vositalari, jumladan sport va jismoniy tarbiya orqali ham bunday tahdidlarga qarshi immunitet shakllantirish dolzarb vazifa sifatida namoyon bo'lmoqda.

1. Raqamli makonda ekstremizm va radikalizmning kuchayishi: muammo mohiyati.

So'nggi yillarda dunyo miqyosida ekstremizm va radikalizmning shakllanishi va tarqalishi uchun asosiy platformalardan biri bu – internet va ijtimoiy tarmoqlar bo'lib qolmoqda. O'zbekiston ham ushbu global axborot makonining ajralmas qismi sifatida ushbu xavf bilan yuzma-yuz turibdi. Ekstremistik guruhlar ijtimoiy tarmoqlarda yoshlarni radikal g'oyalarga jalb etish, ularni yolg'on ma'lumotlar orqali manipulyatsiya qilish, soxta ideal g'oyalar ortidan ergashtirish kabi maqsadlarda faoliyat olib borishmoqda.

Yoshlarning bu kabi kontentlarga nisbatan ta'sirchanligi quyidagi omillar bilan izohlanadi:

- Psixologik barqarorlikning pastligi, o'z-o'zini anglash va qadrlash hissining rivojlanmaganligi;

- Axborot tanqidiy tahlil qilish ko'nikmalarining sustligi, ya'ni ma'lumotni tahlil qilish o'rniga uni shunchaki qabul qilishga moyillik;

- Ijtimoiy hayotdagi o'z o'rnini topa olmaslik, ya'ni bo'shliqni to'ldirish uchun virtual makonga berilib ketish;

- Ijtimoiy tarmoq orqali o'zini namoyon etish ehtiyoji, ya'ni e'tiborga, tan olinishga bo'lgan ichki ehtiyojdan foydalanish orqali ularga ta'sir o'tkazish.

Shu boisdan, nafaqat texnik xavfsizlik tizimlari, balki shaxsiy immunitet, psixologik barqarorlik va ijtimoiy faol muhitga ega yoshlarni tarbiyalash masalasi bugungi kunning eng muhim yo'nalishlaridan biridir.

2. Jismoniy tayyorgarlik va sportning tarbiyaviy va psixologik salohiyati

Jismoniy tarbiya va sport faoliyati yosh avlodning har tomonlama rivojlanishida muhim o'rin tutadi. Bu jarayon faqat jismoniy salomatlikni tiklash va mustahkamlash bilan cheklanmaydi. Sport yoshlar ongida ijobiy qarashlarni

shakllantirish, ijtimoiy rol va javobgarlikni his qilish, sog‘lom raqobat, mehnatsevarlik va intizom kabi fazilatlarni tarbiyalaydi.

Psixologik barqarorlik va sport o‘rtasidagi bog‘liqlik ilmiy jihatdan isbotlangan: sport bilan shug‘ullanuvchi yoshlar depressiya, yolg‘izlanish, tajovuzkorlik yoki g‘azabga berilish kabi holatlarga kamroq duch kelishadi. Aynan mana shu hissiyotlar ekstremistik guruhlar tomonidan mohirlik bilan ekspluatatsiya qilinadi. Demak, sport – bu nafaqat tanani, balki ongni ham chiniqtiradigan kuchli vositadir.

Shuningdek, jismoniy mashg‘ulotlar va sport musobaqalari:

- Jamoaviylik va ijtimoiy hamkorlikni kuchaytiradi, bu esa ijtimoiy ajralib qolish hissini kamaytiradi;

- O‘ziga bo‘lgan ishonchni oshiradi, shaxsiy g‘urur va o‘z qadrini anglashni kuchaytiradi;

- Qonuniy yo‘ldan muvaffaqiyatga erishish mumkinligini isbotlaydi, bu esa radikal yondashuvlarga muqobil ijobiy hayotiy yo‘l sifatida xizmat qiladi.

3. Ekstremistik g‘oyalarga qarshi immunitetni shakllantirishda sportning amaliy funksiyasi

Yoshlar orasida radikal g‘oyalarga qarshi immunitetni shakllantirishda sport quyidagi yo‘nalishlarda foydali vosita bo‘la oladi:

a) Bo‘sh vaqtni mazmunli tashkil etish. Ayniqsa o‘smirlar va talabalar orasida bo‘sh vaqtning noto‘g‘ri tashkil etilishi – ular orasida ijtimoiy tarmoqlarga haddan ziyod berilib ketish, radikal kontentlarni ko‘rish va unga qiziqish uyg‘otish ehtimolini oshiradi. Sport to‘garaklari, musobaqalar, sportga asoslangan loyihalar bu xavfni kamaytiradi.

b) Ijtimoiy bog‘liqlikni mustahkamlash. Sport orqali yoshlar do‘st orttiradi, jamoadagi o‘z o‘rnini anglaydi, sog‘lom ijtimoiy aloqalarga ega bo‘ladi. Bu esa radikal guruhlarining “sen jamiyatda keraksan” degan yolg‘on va’dalariga ishonch hosil qilishiga to‘sqinlik qiladi.

c) Vatanparvarlik va fuqarolik ongini oshirish. Sport orqali milliy qadriyatlar, tarixiy faxr, vatanga muhabbat, qonunlarga hurmat targ‘ib qilinadi. Bu yoshlarning o‘z yurti manfaatlariga zid bo‘lgan har qanday radikal qarashlarni inkor etishlariga xizmat qiladi.

d) Psixologik mustahkamlikni kuchaytirish. Sport mashg‘ulotlari orqali stressga bardoshlilik, o‘zini boshqarish, sabr-toqat kabi sifatlar shakllanadi. Bu esa yoshlarni manipulyatsiya qilishga nisbatan kamroq moyil bo‘lishlariga yordam beradi.

Taklif va tavsiyalar

Ushbu maqsadlarni amalga oshirish uchun quyidagi amaliy choralar dolzarb hisoblanadi:

- Maktab va oliy ta'lim muassasalarida jismoniy tarbiya darslariga axborot madaniyati va internet xavfsizligi bo'yicha maxsus bloklar kiritish;

- Sport tadbirlarini nafaqat jismoniy, balki ma'naviy tarbiya vositasiga aylantirish – musobaqalardan avval yoki keyin yoshlar bilan radikalizmning zararli oqibatlari haqida ochiq muloqotlar o'tkazish;

- Sport federatsiyalari va jismoniy tarbiya muassasalari tomonidan antiekstremistik tashabbuslarni ilgari surish – sportchilarni bu borada rol model sifatida shakllantirish;

- Mahalla, maktab va yoshlar ittifoqi orqali sport klublarida “axborot xavfsizligi elchilari” kabi faol yoshlar guruhlarini tashkil etish.

Xulosa qilib, axborot makonidagi tahdidlar bilan faqat texnik yoki huquqiy choralar yordamida kurashish yetarli emas. Yoshlar ongini, psixologik qarshilik kuchini mustahkamlovchi omillar, xususan sport va jismoniy tayyorgarlik — bu sohadagi muhim ijtimoiy vositalardan biridir. Yurtimizda sog'lom turmush tarzini targ'ib qilish orqali radikalizmga qarshi samarali ijtimoiy immunitet yaratish mumkin.

Foydalanilgan adabiyotlar.

1. Karimov I.A. “Yuksak ma'naviyat – yengilmas kuch”. – T.: Ma'naviyat, 2008.

2. O'zbekiston Respublikasi Prezidentining “Yoshlar ma'naviyatini yuksaltirish va ularning bo'sh vaqtini mazmunli tashkil etish to'g'risida”gi PQ-4968-sonli qarori.
2021-yil.

3. UNODC (2022). “Sport as a tool for preventing violent extremism”.

4. Cyber Peace Foundation (2021). “Digital safety and youth resilience strategies”.

JAMOAT XAVFSIZLIGINI TA'MINLASHDA MAFKURAVIY TAHDIDLARGA QARSHI KURASHISH MEXANIZMLARINI TAKOMILLASHTIRISH

Ro'ziyeva Gulsanam Sultonmurodovna

IIV Malaka oshirish instituti Maxsus-kasbiy fanlar kafedrasi katta o'qituvchisi

Annotatsiya. Mazkur ilmiy maqolada O'zbekistonda jamoat xavfsizligini ta'minlashda mafkuraviy tahdidlarga qarshi kurashish, jamoat xavfsizligiga ta'sir etuvchi asosiy omillar, mavjud muammolar va ularni bartaraf etish yo'llari keng tahlil etilgan. Mafkuraviy tahdidlarga qarshi kurashish sohasining rivoji, ayniqsa,

fuqarolarning huquqiy va axloqiy ongi, ijtimoiy faolligini oshirish orqali xavfsizlikni mustahkamlash imkoniyatlari ko‘rib chiqilgan.

Kalit so‘zlar: mafkuraviy tahdid, ma’naviyat, xavfsizlik, ijtimoiy barqarorlik, jinoyatchilik, profilaktika, huquqiy ong, fuqarolik jamiyati, islohotlar, davlat siyosati.

Аннотация. В данной научной статье дается комплексный анализ борьбы с идеологическими угрозами в обеспечении общественной безопасности в Узбекистане, основные факторы, влияющие на общественную безопасность, существующие проблемы и пути их устранения. Рассматривается развитие сферы борьбы с идеологическими угрозами, в частности, возможности укрепления безопасности путем повышения правового и нравственного сознания и социальной активности граждан.

Ключевые слова: идеологическая угроза, духовность, безопасность, социальная стабильность, преступность, профилактика, правосознание, гражданское общество, реформы, государственная политика.

Abstract. This scientific article provides a comprehensive analysis of the fight against ideological threats in ensuring public security in Uzbekistan, the main factors affecting public security, existing problems and ways to eliminate them. The development of the field of combating ideological threats, in particular, the possibilities of strengthening security by increasing the legal and moral awareness and social activity of citizens, are considered.

Keywords: ideological threat, spirituality, security, social stability, crime, prevention, legal awareness, civil society, reforms, public policy.

«Biz yaratayotgan yangi O‘zbekistonning mafkurasi ezgulik, odamiylik, gumanizm g‘oyasi bo‘ladi. Biz mafkura deganda, avvalo, fikr tarbiyasini, milliy va umuminsoniy qadriyatlar tarbiyasini tushunamiz. Ular xalqimizning necha ming yillik hayotiy tushuncha va qadriyatlariga asoslangan»⁴⁷

Shavkat Mirziyoyev

Jahonda globallashuv jarayonining tobora avj olishi, zamonaviy axborot texnologiyalari sohasidagi yutuqlardan yovuz maqsadlar yo‘lida foydalanish orqali inson ongi va qalbini egallash uchun mafkuraviy kurashlarning kuchayishi xavfsizlik va barqarorlikka tahdid solmoqda. Yangi asrda jamiyat xavfsizligiga tahdid soladigan omillar tobora murakkablashib, ularning ko‘lami kengayib bormoqda.

⁴⁷ Prezident Shavkat Mirziyoyevning 2021-yil 19-yanvardagi ma’naviyat masalalariga bag‘ishlab o‘tkazilgan videoselektor yig‘ilishi.

Xususan, kiberjinoyatchilik, terrorizm, ekstremizm, narkotrafik kabi transmilliy tahdidlar global muammoga aylanib ulgurdi. Bunday sharoitda xavfsizlikni ta'minlashning an'anaviy usullari yetarli samara bermaydi. Ayniqsa, bugungi kunda xalqaro maydonda mafkuraviy, g'oyaviy va informatsion kurashlar kuchayib borayotgan hozirgi murakkab va tahlikali davrda davlatni milliy xavfsizligini ta'minlashda ma'naviy-ma'rifiy ishlarni zamon talablari asosida tashkil etish, yoshlarimizni turli mafkuraviy xurujlardan himoya qilish, yon-atrofdagi yuz berayotgan voqealarga teran nigoh bilan nazar solish, fuqarolarimizda daxldorlik hissini oshirish, tinch-osoyshta hayotimizni turli xavf-xatar va tahdidlardan asrash vazifasi muhim ahamiyat kasb etadi. "Ayni vaqtda hozirgi murakkab zamon tinch-osoyshta hayotimizni asrash va mustahkamlash, xalqimizning kafolatlangan xavfsizligini ta'minlash masalasini yanada dolzarb qilib qo'yimoqda"⁴⁸.

Insoniyatning shunday mo'jizakor yutuqlaridan ham ba'zi buzg'unchilar salbiy maqsadlarda foydalanayotganlari taassufli holdir. "Ayni paytda hayot haqiqati shuni ko'rsatadiki, har qanday taraqqiyot mahsulidan ikki xil maqsadda ezgulik va yovuzlik yo'lida foydalanish mumkin. Agarki bashariyat tarixini, uning tafakkur rivojini tarkibiy ravishda ko'zdan kechiradigan bo'lsak, hayotda insonni kamolotga, yuksak marralarga chorlaydigan ezgu g'oya va ta'limotlar bilan yovuz va zararli g'oyalar o'rtasida azaldan kurash mavjud bo'lib kelganini va bu kurash bugun ham davom etayotganini ko'ramiz,— deb ta'kidlagan edi Birinchi Prezidentimiz I.A.Karimov. Bugungi kunda zamonaviy axborot maydonidagi harakatlar shu qadar tig'iz, shu qadar tezkorki, endi ilgari gidek, ha, bu voqea bizdan juda olisda yuz beribdi, uning bizga aloqasi yo'q, deb beparvo qarab bo'lmaydi. Ana shunday kayfiyatga berilgan xalq yoki millat taraqqiyotidan yuz yillar orqada qolib ketishi hech gap emas"⁴⁹.

Millat taraqqiyoti haqida so'z borganda qadimdan buyuk ajdodlarning intellektual salohiyati yuksalishida g'oya muhim o'rin tutgani ma'lum. Buni birgina bebaho ma'naviy xazinamiz "Avesto"ning tub mohiyatini belgilab beradigan "Ezgu fikr, ezgu so'z, ezgu amal" g'oyasidan ham bilsa bo'ladi. Ayni paytda globallashuv jarayonida milliy g'oya mafkuraviy ta'sir o'tkazishning asosiy quroliga aylangan. Aytish joizki, globallashuvning jadallashuvi sharoitida milliy ma'naviyat mavjudligining o'zi yetarli emas, unda tashqi tahdidlarga qarshi qaratilgan ichki ruhiy qudrat, uning amal qilishi va faoliyat ko'rsatishi ham zarur bo'ladi⁵⁰.

⁴⁸ Prezident Shavkat Mirziyoyev Qonun ustuvorligi va inson manfaatlarini ta'minlash — yurt taraqqiёti va xalq farovonligining garovi // URL - <http://uz.uz/oz/politics/onun-ustuvorligi-va-inson-manfaatlarini-taminlash-yurt-tara--07-12-2016>

⁴⁹ Karimov I.A. Yuksak maъnaviyat — engilmas kуч. —T.: Maъnaviyat, 2008. — 111 б.

⁵⁰ Отамуродов С. Глобаллашув ва миллат. —Т.: Янги аср авлоди, 2008. — 170 б.

Inson tabiatidagi qiziq bir holat azal-azaldan kuzatiladi. Ya'ni, qachon va qayerdagi biror ijobiy hodisa yuz bersa, unga qarshi kushandalar ham paydo bo'lavergan. Aytaylik, diniy qadriyatlar, ilm-fan yutuqlari, adabiyot, san'at va ma'naviyat ham insoniyatni globalashtirishga xizmat qilishini izohlashga hojat yo'q. "Jahonning turli nuqtalarida hamon davom etayotgan urushlar va qarama-qarshiliklar, saqlanib qolayotgan davlatlararo, millatlararo va dinlararo ziddiyatlar, mingyillik rivojlanish deklaratsiyasida ta'kidlanganidek, qashshoqlik, ochlik, onalar va bolalar o'limi, epidemiyalar va insoniyatning boshqa muammolariga qarshi kurash borasidagi eng jiddiy to'siqlar bo'lib qolmoqda"⁵¹.

O'zbekiston mustaqillikka erishgandan keyingi yangi taraqqiyot bosqichida davlat siyosatining eng muhim yo'nalishlaridan biri sifatida jamiyatda xavfsizlikni ta'minlash, jinoyatchilikning oldini olish, shuningdek, fuqarolarning huquqiy, siyosiy va ma'naviy dunyoqarashini oshirish vazifasi belgilangan. Ya'ni, davlat boshqaruvida nafaqat xavfsizlik choralari kuchaytirish, balki aholining ongini yuksaltirish orqali barqaror va sog'lom jamiyatni shakllantirish ustuvor maqsad hisoblanadi.

Prezidentimiz Shavkat Mirziyoyev bu borada shunday deydi: *"Biz xavfsizlik deganda faqat jismoniy xavfsizlikni emas, balki fuqarolarimizning ongini, qalbini, yuragini asrashni ham tushunamiz. Ma'naviyat eng kuchli qalqon bo'lishi kerak."*⁵²

Mafkuraviy tahdidlar – bu muayyan ijtimoiy guruh yoki jamiyatning ongini o'zgartirish, ekstremistik g'oyalarni singdirish, zo'rvonlikka undash kabi harakatlar orqali xavfsizlikni izdan chiqarishga qaratilgan harakatlardir⁵³. Mafkuraviy tahdid — bu jamiyat, davlat yoki muayyan guruhning aqliy-ruhiy, dunyoqarash va qadriyat tizimiga qarshi yo'naltirilgan ta'sirlar bo'lib, uning natijasida odamlarning ongi, e'tiqodi, g'oyasi va ijtimoiy fikri o'zgarishiga olib keladi.

Mafkuraviy tahdidlar quyidagi xususiyatlarga ega:

1. Internet va ijtimoiy tarmoqlar orqali tarqalishi – bu platforma orqali radikal g'oyalar tez va keng tarqalishi mumkin. Internet va ijtimoiy tarmoqlar orqali mafkuraviy tahdidlar tarqalishi — bu zamonaviy jamiyat uchun eng katta xavflardan biridir. Axborot texnologiyalarining jadal rivojlanishi natijasida, insonlar axborotni tez va oson qabul qilish imkoniga ega bo'ldi, lekin bu holat zararli g'oyalar, soxta ma'lumotlar va buzg'unchi mafkuraviy ta'sirlar tarqalishiga ham sharoit yaratdi.

⁵¹ Ўзбекистон Республикаси Президенти Ислам Каримовнинг БМТ саммити мингйиллик ривожланиш мақсадларига бағишланган ялпи мажлисидаги нутқи. //Халқ сўзи, 2010 йил 21 сентябрь.

⁵² Prezident Shavkat Mirziyoyevning, 2022-yil, Ma'naviyat haftaligi ochilish marosimi yig'ilishi

⁵³ Абдурахмонов, К. (2020). Мafkuraviy tahdidlar va ularning ijtimoiy ta'siri. Toshkent: "Fan" nashriyati

Internet va ijtimoiy tarmoqlar orqali tarqaladigan mafkuraviy tahdidlar turlari:
Ekstremistik va terroristik g‘oyalar:

Internet orqali yoshlarga radikal g‘oyalar singdiriladi.

Ba’zi saytlar va kanallar terrorizmni oqlash, yoshlarni jalb qilish bilan shug‘ullanadi.

Yolg‘on va soxta axborot (feyk):

Jamiyatda beqarorlik uyg‘otish uchun turli feyk xabarlar tarqatiladi.

Maqsad — insonlar ongida shubha, xavotir va ishonchsizlik paydo qilish.

Madaniy va milliy qadriyatlarga qarshi g‘oyalar:

Mahalliy til, din, an’analar mensimaslik bilan tanqid qilinadi.

G‘arb madaniyatini cheksiz ideal sifatida ko‘rsatish orqali yoshlarni o‘z milliylikdan uzoqlashtirishga harakat qilinadi.

Ma’lumot uyushtirilgan kiberhujumlar va targ‘ibotlar orqali:

Ba’zi holatlarda, boshqa davlatlar tomonidan axborot urushi olib boriladi. Bundan maqsad mamlakat ichkarisida ijtimoiy yoki siyosiy beqarorlik yuzaga keltirish hisoblanadi.

Internet va ijtimoiy tarmoqlar orqali mafkuraviy tahdidlar tarqalish usullari:

- YouTube, Telegram, TikTok, Instagram, Facebook kabi platforma va kanallar orqali.

- Bloglar va forumlarda g‘oyaviy ta’sir o‘tkazuvchi kontentlar.

- Onlayn o‘yinlar, video-kontent orqali yumor niqobi ostida radikal g‘oyalarni singdirish.

2. Yoshlar ongiga ta’sir qilish orqali tarqalishi – yosh avlod mafkuraviy ta’siriga ko‘proq moyildir, chunki ular axborotni tanlash va tahlil qilish qobiliyatini hali to‘liq shakllantirmagan bo‘ladi. Yoshlar — jamiyatning eng ta’sirchan va ta’sirlanuvchan qatlami hisoblanadi. Shu bois, mafkuraviy tahdidlar asosan yoshlar ongiga ta’sir qilish orqali tarqaladi. Bunday ta’sirlar ko‘pincha yoshlarning turli qiziqishlaridan kelib chiqib, fe’l-atvori, fikrlash tarzi, hayotiy maqsadlari va qadriyatlarini o‘zgartirishga qaratilgan bo‘ladi.

Mafkuraviy tahdidning maqsadlari sifatida quyidagilarni keltirish mumkin:

- Milliy va ma’naviy qadriyatlarni mensimaslik.

- Davlatga, jamiyatga va urf-odatlariga nisbatan salbiy munosabat uyg‘otish.

- Yoshlarni radikal, ekstremistik yo‘nalishlarga jalb qilish.

- Jamiyatda beqarorlik va bo‘linish chiqarish.

Bu turdagi mafkuraviy tahdid oqibatida jamiyatning milliy mafkuradan uzoqlashishi, o‘zaro totuvlikka putur yetishi, yoshlarning ongida “o‘zim bilganimcha yashayman” degan g‘oyaning kuchayishi, shuningdek, yoshlar orasida ma’naviy inqiroz va ijtimoiy muammolar ko‘payishi yuzaga kelishi mumkin.

Shu kabi salbiy holatlarning oldini olish maqsadida, qo‘yidagi yo‘llar orqali biz yoshlarni mafkuraviy tahdidlardan himoya qilishimiz mumkin:

- Ta‘lim orqali: ya‘ni ta‘lim jarayonida tanqidiy fikrlashni rivojlantirish, axborot savodxonligini oshirish.

- Ota-ona va ustoz nazorati: mas‘ul shaxslar hamkorlikda farzandlar bilan tez-tez suhbatlar o‘tkazish orqali farzandning qanday kontent ko‘rayotganini bilish.

- Milliy mafkura asosida tarbiya: tarix, madaniyat, din va ma‘naviyatni chuqur o‘rgatish.

- Pozitiv onlayn muhit yaratish: ijobiy kontentlar, milliy qahramonlar va zamonaviy obrazlar.

3. Milliy va diniy ehtiyojlardan foydalanish orqali tarqalishi – ekstremistik guruhlar o‘z mafkurasini milliy, diniy yoki ijtimoiy adolat tuyg‘ulari bilan niqoblab tarqatishi mumkin. Milliy va diniy ehtiyojlardan foydalanish orqali mafkuraviy tahdidlarni tarqatish — bu zamonaviy mafkuraviy kurash usullaridan biri bo‘lib, u jamiyatdagi eng nozik his-tuyg‘ular — milliylik, dindorlik, adolatparvarlik, va ma‘naviy qadriyatlar orqali insonlar ongiga ta‘sir qilishga qaratilgan.

Milliy ehtiyojlar - millat manfaatlari niqobi ostida boshqa millatlarga nisbatan nafrat uyg‘otish, separatizm va milliy dushmanlikni qo‘zg‘atish.

Diniy ehtiyojlar - dindan niqob sifatida foydalanish, dinni noto‘g‘ri talqin qilish, radikal va dahshatli aqidalarni "islomga mos" deb ko‘rsatish, yoshlarning e‘tiqodidan foydalanish.

Milliy ehtiyojlar orqali:

- "Millatimiz zulmda", "bizning haqqimiz toptalyapti" degan milliy tuyg‘ularni qo‘zg‘atish.

- Milliy muammolar orqali odamlarni ijtimoiy isyonga undash.

- Turli ijtimoiy tarmoqlarda “milliy qahramonlik” niqobida hukumatga va jamiyatga qarshi chiqishni targ‘ib qilish.

Diniy ehtiyojlar orqali:

- Haqiqiy islom va uning bag‘rikenglik g‘oyalarini qoralash

- Jannat, shihodat, yoki jihad va hijrat kabi diniy tushunchalarni noto‘g‘ri talqin qilish.

- Internetda yoshlar ongiga ta‘sir qiluvchi “islomiy ko‘rinishdagi” videolar, maqolalar, bloglar orqali radikal guruhlariga jalb qilish.

Jamiyatda mafkuraviy tahdidlarga qarshi kurash mexanizmlarini takomillashtirish yo‘nalishlari:

1. Axborot-xavfsizlik monitoring tizimlarini kuchaytirish

Zamonaviy dasturiy ta'minot va sun'iy intellekt texnologiyalari yordamida internet makonidagi shubhali kontentlarni avtomatik aniqlash va tahlil qilish mexanizmlarini yo'lga qo'yish zarur⁵⁴.

2. Ta'lim muassasalarida mafkuraviy immunitetni shakllantirish

Maktab va oliy ta'lim muassasalarida mafkuraviy tahdidlar va axborot xavfsizligiga oid maxsus fanlar joriy etish, yoshlar orasida tanqidiy fikrlashni rivojlantirish lozim⁵⁵.

3. Jamoatchilik bilan hamkorlik mexanizmlarini rivojlantirish

Mahalla, NNTlar va fuqarolik jamiyati institutlari orqali profilaktik tadbirlarni kengaytirish, aholi ongini oshirish maqsadida media-kampaniyalar o'tkazish samarali hisoblanadi⁵⁶.

4. Qonunchilik bazasini takomillashtirish

Mafkuraviy tahdidlarga qarshi kurashishda huquqiy mexanizmlarni mustahkamlash, ayniqsa onlayn muhitda radikal g'oyalar tarqatilishini cheklash bo'yicha aniq me'yorlar kiritish zarur⁵⁷.

Xulosa qilib, Jamoat xavfsizligini ta'minlash faqatgina kuch ishlatish orqali emas, balki ongli, bilimli va mas'uliyatli fuqarolarni tarbiyalash orqali amalga oshiriladi. Mafkuraviy tahdidlarga qarshi kurashda davlat, jamiyat va ta'lim muassasalari o'rtasidagi hamkorlik hal qiluvchi ahamiyatga ega.

Foydalanilgan adabiyotlar:

1. O'zbekiston Respublikasi Prezidenti Shavkat Mirziyoyevning 2021-yil 19-yanvardagi ma'naviyat masalalariga bag'ishlab o'tkazilgan videoselektor yig'ilishi.

2. O'zbekiston Respublikasi Prezidenti Shavkat Mirziyoyevning 2022-yil Ma'naviyat haftaligi ochilish marosimi yig'ilishi

3. O'zbekiston Respublikasi Prezidenti Shavkat Mirziyoyev // Qonun ustuvorligi va inson manfaatlarini ta'minlash – yurt taraqqiyoti va xalq farovonligining garovi // URL - <http://uza.uz/oz/politics/onun-ustuvorligi-va-inson-manfaatlarini-taminlash-yurt-tara--07-12-2016>

4. Birinchi Prezident Islom Karimovning BMT sammiti mingyillik rivojlanish maqsadlariga bag'ishlangan yalpi majlisidagi nutqi. //Xalq so'zi, 2010 yil 21 sentyabr.

5. Birinchi Prezident Islom Karimov // Yuksak ma'naviyat – yengilmas kuch. – T.: Ma'naviyat, 2008. – 111 b.

6. S.Otamurodov // Globallashuv va millat. –T.: Yangi asr avlodi, 2008. – 170 b.

⁵⁴ “Интернет хавфсизлиги ва кибер таҳдидларга қарши кураш”, Ўзбекистон Киберхавфсизлик агентлиги, 2023.

⁵⁵ Зуфаров, М. (2021). Ёшлар ва мафкуравий таҳдидлар. Тошкент: “Ўқитувчи”.

⁵⁶ Маҳалла ва ННТлар фаолияти ҳақида Республика ахборот маркази ҳисоботи, 2022.

⁵⁷ Ўзбекистон Республикаси “Ахборотлаштириш тўғрисида”ги Қонунига сўнгги ўзгаришлар, 2024.

7. T.Eshbekov // Mafkura maydonida axborot-psixologik xavfsizlik (o'quv qo'llanma) // Mirzo ulug'bek nomidagi O'zbekiston milliy universiteti – 2011

8. "Internet xavfsizligi va kiber tahdidlarga qarshi kurash", O'zbekiston Kiberxavfsizlik agentligi-2023.

9. O'zbekiston Respublikasi "Axborotlashtirish to'g'risida"gi Qonuniga so'nggi o'zgartishlar-2024.

10. M.Zufarov // *Yoshlar va mafkuraviy tahdidlar*. Toshkent: "O'qituvchi"-2021.

MAFKURAVIY TAHDIDLARNING JAMIYAT RIVOJIGA SALBIY JIHATLARI

Ro'ziyeva Gulsanam Sultonmurodovna

IIV Malaka oshirish instituti Maxsus-kasbiy fanlar kafedrasida katta o'qituvchisi

Annotatsiya. Mazkur ilmiy maqolada O'zbekistonda jamoat xavfsizligini ta'minlashda mafkuraviy tahdidlarga qarshi kurashish, jamoat xavfsizligiga ta'sir etuvchi asosiy omillar, mavjud muammolar va ularni bartaraf etish yo'llari keng tahlil etilgan. Mafkuraviy tahdidlarga qarshi kurashish sohasining rivoji, ayniqsa, fuqarolarning huquqiy va axloqiy ongi, ijtimoiy faolligini oshirish orqali xavfsizlikni mustahkamlash imkoniyatlari ko'rib chiqilgan.

Kalit so'zlar: mafkuraviy tahdid, ma'naviyat, xavfsizlik, ijtimoiy barqarorlik, jinoyatchilik, profilaktika, huquqiy ong, fuqarolik jamiyati, islohotlar, davlat siyosati.

Аннотация. В данной научной статье дается комплексный анализ борьбы с идеологическими угрозами в обеспечении общественной безопасности в Узбекистане, основные факторы, влияющие на общественную безопасность, существующие проблемы и пути их устранения. Рассматривается развитие сферы борьбы с идеологическими угрозами, в частности, возможности укрепления безопасности путем повышения правового и нравственного сознания и социальной активности граждан.

Ключевые слова: идеологическая угроза, духовность, безопасность, социальная стабильность, преступность, профилактика, правосознание, гражданское общество, реформы, государственная политика.

Abstract. This scientific article provides a comprehensive analysis of the fight against ideological threats in ensuring public security in Uzbekistan, the main factors affecting public security, existing problems and ways to eliminate them. The development of the field of combating ideological threats, in particular, the

possibilities of strengthening security by increasing the legal and moral awareness and social activity of citizens, are considered.

Keywords: ideological threat, spirituality, security, social stability, crime, prevention, legal awareness, civil society, reforms, public policy.

Kirish: «Biz yaratayotgan yangi O‘zbekistonning mafkurasi ezgulik, odamiylik, gumanizm g‘oyasi bo‘ladi. Biz mafkura deganda, avvalo, fikr tarbiyasini, milliy va umuminsoniy qadriyatlar tarbiyasini tushunamiz. Ular xalqimizning necha ming yillik hayotiy tushuncha va qadriyatlariga asoslangan»⁵⁸

Dunyoda globallashuv jarayonining tobora avj olishi, zamonaviy axborot texnologiyalari sohasidagi yutuqlardan yovuz maqsadlar yo‘lida foydalanish orqali inson ongi va qalbini egallash uchun mafkuraviy kurashlarning kuchayishi xavfsizlik va barqarorlikka tahdid solmoqda. Yangi asrda jamiyat xavfsizligiga tahdid soladigan omillar tobora murakkablashib, ularning ko‘lami kengayib bormoqda. Xususan, kiberjinoyatchilik, terrorizm, ekstremizm, narkotrafik kabi transmilliy tahdidlar global muammoga aylanib ulgurdi. Bunday sharoitda xavfsizlikni ta‘minlashning an‘anaviy usullari yetarli samara bermaydi. Ayniqsa, bugungi kunda xalqaro maydonda mafkuraviy, g‘oyaviy va informatsion kurashlar kuchayib borayotgan hozirgi murakkab va tahlikali davrda davlatni milliy xavfsizligini ta‘minlashda ma‘naviy-ma‘rifiy ishlarni zamon talablari asosida tashkil etish, yoshlarimizni turli mafkuraviy xurujlardan himoya qilish, yon-atrofdagi yuz berayotgan voqealarga teran nigoj bilan nazar solish, fuqarolarimizda daxldorlik hissini oshirish, tinch-osoyishta hayotimizni turli xavf-xatar va tahdidlardan asrash vazifasi muhim ahamiyat kasb etadi. “Ayni vaqtda hozirgi murakkab zamon tinch-osoyishta hayotimizni asrash va mustahkamlash, xalqimizning kafolatlangan xavfsizligini ta‘minlash masalasini yanada dolzarb qilib qo‘ymoqda”⁵⁹.

Insoniyatning shunday mo‘jizakor yutuqlaridan ham ba‘zi buzg‘unchilar salbiy maqsadlarda foydalanayotganlari taassufli holdir. “Ayni paytda hayot haqiqati shuni ko‘rsatadiki, har qanday taraqqiyot mahsulidan ikki xil maqsadda ezgulik va yovuzlik yo‘lida foydalanish mumkin. Agarki bashariyat tarixini, uning tafakkur rivojini tarkibiy ravishda ko‘zdan kechiradigan bo‘lsak, hayotda insonni kamolotga, yuksak marralarga chorlaydigan ezgu g‘oya va ta‘limotlar bilan yovuz va zararli g‘oyalar o‘rtasida azaldan kurash mavjud bo‘lib kelganini va bu kurash bugun ham davom etayotganini ko‘ramiz,— deb ta‘kidlagan edi Birinchi Prezidentimiz I.A.Karimov.

⁵⁸ Prezident Shavkat Mirziyoyevning 2021-yil 19-yanvardagi ma‘naviyat masalalariga bag‘ishlab o‘tkazilgan videoselektor yig‘ilishi.

⁵⁹ Prezident Shavkat Mirziyoyev Qonun ustuvorligi va inson manfaatlarini ta‘minlash – yurt taraqqiyoti va xalq farovonligining garovi // URL - <http://uza.uz/oz/politics/onun-ustuvorligi-va-inson-manfaatlarini-taminlash-yurt-tara--07-12-2016>

Bugungi kunda zamonaviy axborot maydonidagi harakatlar shu qadar tig'iz, shu qadar tezkorki, endi ilgorigidek, ha, bu voqea bizdan juda olisda yuz beribdi, uning bizga aloqasi yo'q, deb beparvo qarab bo'lmaydi. Ana shunday kayfiyatga berilgan xalq yoki millat taraqqiyotdan yuz yillar orqada qolib ketishi hech gap emas"⁶⁰.

Millat taraqqiyoti haqida so'z borganda qadimdan buyuk ajdodlarning intellektual salohiyati yuksalishida g'oya muhim o'rin tutgani ma'lum. Buni birgina bebaho ma'naviy xazinamiz "Avesto"ning tub mohiyatini belgilab beradigan "Ezgu fikr, ezgu so'z, ezgu amal" g'oyasidan ham bilsa bo'ladi. Ayni paytda globallashuv jarayonida milliy g'oya mafkuraviy ta'sir o'tkazishning asosiy quroliga aylangan. Aytish joizki, globallashuvning jadallashuvi sharoitida milliy ma'naviyat mavjudligining o'zi yetarli emas, unda tashqi tahdidlarga qarshi qaratilgan ichki ruhiy qudrat, uning amal qilishi va faoliyat ko'rsatishi ham zarur bo'ladi⁶¹.

Inson tabiatidagi qiziq bir holat azal-azaldan kuzatiladi. Ya'ni, qachon va qayerdagi biror ijobiy hodisa yuz bersa, unga qarshi kushandalar ham paydo bo'lavergan. Aytaylik, diniy qadriyatlar, ilm-fan yutuqlari, adabiyot, san'at va ma'naviyat ham insoniyatni globallashtirishga xizmat qilishini izohlashga hojat yo'q. "Jahonning turli nuqtalarida hamon davom etayotgan urushlar va qarama-qarshiliklar, saqlanib qolayotgan davlatlararo, millatlararo va dinlararo ziddiyatlar, mingyillik rivojlanish deklaratsiyasida ta'kidlanganidek, qashshoqlik, ochlik, onalar va bolalar o'limi, epidemiyalar va insoniyatning boshqa muammolariga qarshi kurash borasidagi eng jiddiy to'siqlar bo'lib qolmoqda"⁶².

O'zbekiston mustaqillikka erishgandan keyingi yangi taraqqiyot bosqichida davlat siyosatining eng muhim yo'nalishlaridan biri sifatida jamiyatda xavfsizlikni ta'minlash, jinoyatchilikning oldini olish, shuningdek, fuqarolarning huquqiy, siyosiy va ma'naviy dunyoqarashini oshirish vazifasi belgilangan. Ya'ni, davlat boshqaruvida nafaqat xavfsizlik choralari kuchaytirish, balki aholining ongini yuksaltirish orqali barqaror va sog'lom jamiyatni shakllantirish ustuvor maqsad hisoblanadi.

Prezidentimiz Shavkat Mirziyoyev bu borada shunday deydi: *"Biz xavfsizlik deganda faqat jismoniy xavfsizlikni emas, balki fuqarolarimizning ongini, qalbini, yuragini asrashni ham tushunamiz. Ma'naviyat eng kuchli qalqon bo'lishi kerak."*⁶³

⁶⁰ Каримов И.А. Юксак маънавият – енгилмас куч. –Т.: Маънавият, 2008. – 111 б.

⁶¹ Отамуродов С. Глобаллашув ва миллат. –Т.: Янги аср авлоди, 2008. – 170 б.

⁶² Ўзбекистон Республикаси Президенти Ислон Каримовнинг БМТ саммити мингйиллик ривожланиш мақсадларига бағишланган ялпи мажлисидаги нутқи. //Халқ сўзи, 2010 йил 21 сентябрь.

⁶³ Prezident Shavkat Mirziyoyevning, 2022-yil, Ma'naviyat haftaligi ochilish marosimi yig'ilishi

Mafkuraviy tahdidlar – bu muayyan ijtimoiy guruh yoki jamiyatning ongini o‘zgartirish, ekstremistik g‘oyalarni singdirish, zo‘ravonlikka undash kabi harakatlar orqali xavfsizlikni izdan chiqarishga qaratilgan harakatlardir⁶⁴. Mafkuraviy tahdid — bu jamiyat, davlat yoki muayyan guruhning aqliy-ruhiy, dunyoqarash va qadriyat tizimiga qarshi yo‘naltirilgan ta’sirlar bo‘lib, uning natijasida odamlarning ongi, e’tiqodi, g‘oyasi va ijtimoiy fikri o‘zgarishiga olib keladi.

Mafkuraviy tahdidlar quyidagi xususiyatlarga ega:

4. Internet va ijtimoiy tarmoqlar orqali tarqalishi – bu platforma orqali radikal g‘oyalar tez va keng tarqalishi mumkin. Internet va ijtimoiy tarmoqlar orqali mafkuraviy tahdidlar tarqalishi — bu zamonaviy jamiyat uchun eng katta xavflardan biridir. Axborot texnologiyalarining jadal rivojlanishi natijasida, insonlar axborotni tez va oson qabul qilish imkoniga ega bo‘ldi, lekin bu holat zararli g‘oyalar, soxta ma’lumotlar va buzg‘unchi mafkuraviy ta’sirlar tarqalishiga ham sharoit yaratdi.

Internet va ijtimoiy tarmoqlar orqali tarqaladigan mafkuraviy tahdidlar turlari:
Ekstremistik va terroristik g‘oyalar:

Internet orqali yoshlarga radikal g‘oyalar singdiriladi.

Ba’zi saytlar va kanallar terrorizmni oqlash, yoshlarni jalb qilish bilan shug‘ullanadi.

Yolg‘on va soxta axborot (feyk):

Jamiyatda beqarorlik uyg‘otish uchun turli feyk xabarlar tarqatiladi.

Maqsad — insonlar ongida shubha, xavotir va ishonchsizlik paydo qilish.

Madaniy va milliy qadriyatlarga qarshi g‘oyalar:

Mahalliy til, din, an’analar mensimaslik bilan tanqid qilinadi.

G‘arb madaniyatini cheksiz ideal sifatida ko‘rsatish orqali yoshlarni o‘z milliylikdan uzoqlashtirishga harakat qilinadi.

Ma’lumot uyushtirilgan kiberhujumlar va targ‘ibotlar orqali:

Ba’zi holatlarda, boshqa davlatlar tomonidan axborot urushi olib boriladi. Bundan maqsad mamlakat ichkarisida ijtimoiy yoki siyosiy beqarorlik yuzaga keltirish hisoblanadi.

5. Yoshlar ongiga ta’sir qilish orqali tarqalishi – yosh avlod mafkuraviy ta’sirga ko‘proq moyildir, chunki ular axborotni tanlash va tahlil qilish qobiliyatini hali to‘liq shakllantirmagan bo‘ladi. Yoshlar — jamiyatning eng ta’sirchan va ta’sirlanuvchan qatlami hisoblanadi. Shu bois, mafkuraviy tahdidlar asosan yoshlar ongiga ta’sir qilish orqali tarqaladi. Bunday ta’sirlar ko‘pincha yoshlarning turli

64 Абдурахмонов, К. (2020). Мafkuraviy tahdidlar va ularning ijtimoiy ta’siri. Toshkent: “Fan” nashriyoti

qiziqishlaridan kelib chiqib, fe'l-atvori, fikrlash tarzi, hayotiy maqsadlari va qadriyatlarini o'zgartirishga qaratilgan bo'ladi.

Mafkuraviy tahdidning maqsadlari sifatida quyidagilarni keltirish mumkin:

- Milliy va ma'naviy qadriyatlarni mensimaslik.
- Davlatga, jamiyatga va urf-odatlariga nisbatan salbiy munosabat uyg'otish.
- Yoshlarni radikal, ekstremistik yo'nalishlarga jalb qilish.
- Jamiyatda beqarorlik va bo'linish chiqarish.

Bu turdagi mafkuraviy tahdid oqibatida jamiyatning milliy mafkuradan uzoqlashishi, o'zaro totuvlikka putur yetishi, yoshlarning ongida "o'zim bilganimcha yashayman" degan g'oyaning kuchayishi, shuningdek, yoshlar orasida ma'naviy inqiroz va ijtimoiy muammolar ko'payishi yuzaga kelishi mumkin.

Shu kabi salbiy holatlarning oldini olish maqsadida, qo'yidagi yo'llar orqali biz yoshlarni mafkuraviy tahdidlardan himoya qilishimiz mumkin:

• Ta'lim orqali: ya'ni ta'lim jarayonida tanqidiy fikrlashni rivojlantirish, axborot savodxonligini oshirish.

• Ota-ona va ustoz nazorati: mas'ul shaxslar hamkorlikda farzandlar bilan tez-tez suhbatlar o'tkazish orqali farzandning qanday kontent ko'rayotganini bilish.

• Milliy mafkura asosida tarbiya: tarix, madaniyat, din va ma'naviyatni chuqur o'rgatish.

• Pozitiv onlayn muhit yaratish: ijobiy kontentlar, milliy qahramonlar va zamonaviy obrazlar.

6. Milliy va diniy ehtiyojlardan foydalanish orqali tarqalishi – ekstremistik guruhlar o'z mafkurasini milliy, diniy yoki ijtimoiy adolat tuyg'ulari bilan niqoblab tarqatishi mumkin. Milliy va diniy ehtiyojlardan foydalanish orqali mafkuraviy tahdidlarni tarqatish — bu zamonaviy mafkuraviy kurash usullaridan biri bo'lib, u jamiyatdagi eng nozik his-tuyg'ular — milliylik, dindorlik, adolatparvarlik, va ma'naviy qadriyatlar orqali insonlar ongiga ta'sir qilishga qaratilgan.

Milliy ehtiyojlar - millat manfaatlari niqobi ostida boshqa millatlarga nisbatan nafrat uyg'otish, separatizm va milliy dushmanlikni qo'zg'atish.

Diniy ehtiyojlar - dindan niqob sifatida foydalanish, dinni noto'g'ri talqin qilish, radikal va dahshatli aqidalarni "islomga mos" deb ko'rsatish, yoshlarning e'tiqodidan foydalanish.

Xulosa. Jamoat xavfsizligini ta'minlash faqatgina kuch ishlatish orqali emas, balki ongli, bilimli va mas'uliyatli fuqarolarni tarbiyalash orqali amalga oshiriladi. Mafkuraviy tahdidlarga qarshi kurashda davlat, jamiyat va ta'lim muassasalari o'rtasidagi hamkorlik hal qiluvchi ahamiyatga ega.

Foydalanilgan adabiyotlar:

1. O‘zbekiston Respublikasi Prezidenti Shavkat Mirziyoyevning 2021-yil 19-yanvardagi ma’naviyat masalalariga bag‘ishlab o‘tkazilgan videoselektor yig‘ilishi.
2. O‘zbekiston Respublikasi Prezidenti Shavkat Mirziyoyevning 2022-yil Ma’naviyat haftaligi ochilish marosimi yig‘ilishi
3. O‘zbekiston Respublikasi Prezidenti Shavkat Mirziyoyev // Qonun ustuvorligi va inson manfaatlarini ta’minlash – yurt taraqqiyoti va xalq farovonligining garovi // URL - [http://uza.uz/oz/politics/onun-ustuvorligi-va-inson-manfaatlarini-taminlash yurt-tara--07-12-2016](http://uza.uz/oz/politics/onun-ustuvorligi-va-inson-manfaatlarini-taminlash-yurt-tara--07-12-2016)
4. Birinchi Prezident Islom Karimovning BMT sammiti mingyillik rivojlanish maqsadlariga bag‘ishlangan yalpi majlisidagi nutqi. //Xalq so‘zi, 2010 yil 21 sentyabr.
5. Birinchi Prezident Islom Karimov // Yuksak ma’naviyat – yengilmas kuch. – T.: Ma’naviyat, 2008. – 111 b.
6. S.Otamurodov // Globallashuv va millat. –T.:Yangi asr avlodi, 2008. – 170b.
7. T.Eshbekov // Mafkura maydonida axborot-psixologik xavfsizlik (o‘quv qo‘llanma) // Mirzo ulug‘bek nomidagi O‘zbekiston milliy universiteti – 2011
8. “Internet xavfsizligi va kiber tahdidlarga qarshi kurash”, O‘zbekiston Kiberxavfsizlik agentligi-2023.
9. O‘zbekiston Respublikasi “Axborotlashtirish to‘g‘risida”gi Qonuniga so‘nggi o‘zgartishlar-2024.
10. M.Zufarov // *Yoshlar va mafkuraviy tahdidlar*. Toshkent: “O‘qituvchi”-2021.
11. Mahalla va NNTlar faoliyati haqida Respublika axborot markazi hisoboti-2022.

IJTIMOIIY TARMOQLARDAGI FIRIBGARLIK DOLZARB MUAMMOLAR VA ULARGA QARSHI KURASHISH USULLARI

Turayev Murodxon Ayubxonovich

*IIV Malaka oshirish instituti, KTF Jangovar va jismoniy tayyorgarlik sikli
boshlig‘i*

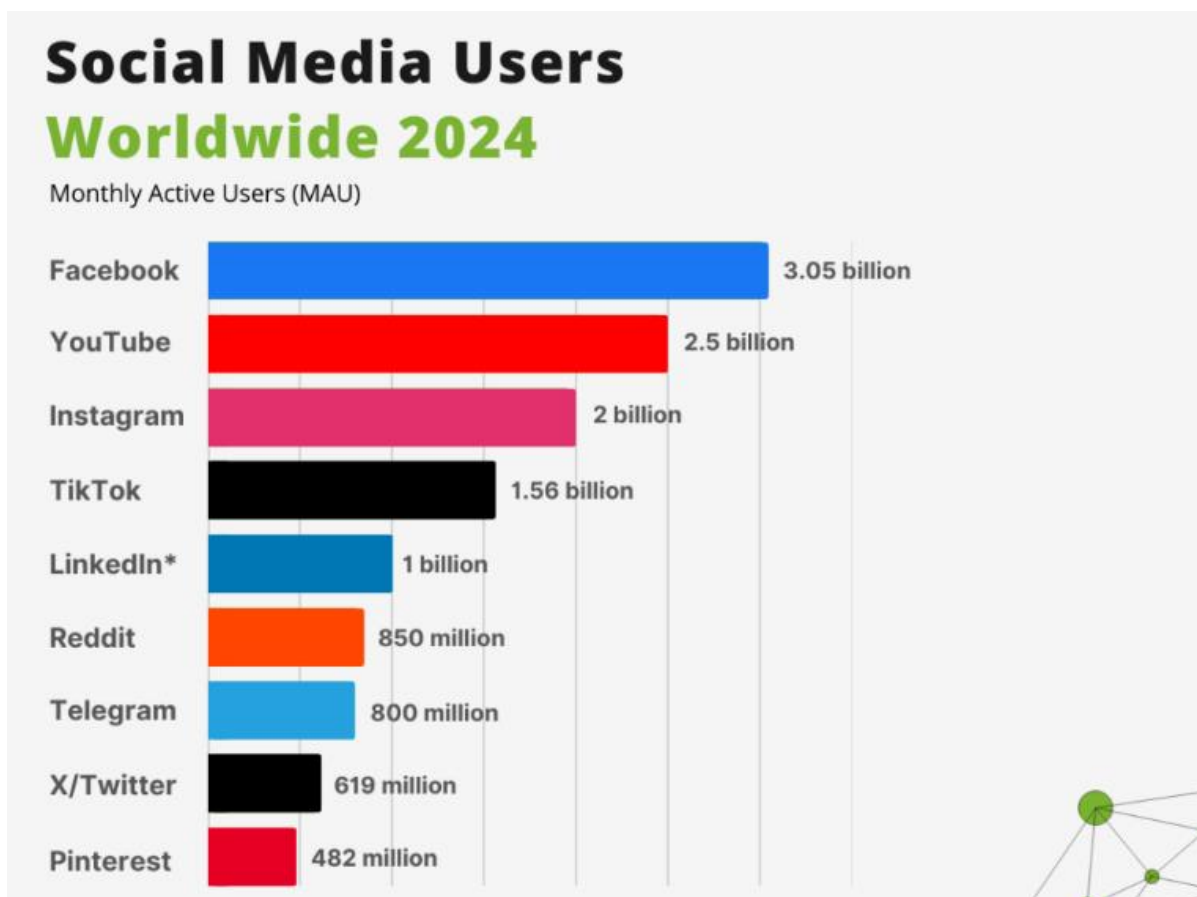
Annotatsiya. Ushbu maqolada ijtimoiy media platformalarida keng tarqalgan firibgarlik turlari (fake profillar, phishing, rom-rom skemalari, clickbait reklamalar va boshqalar), ularning oldini olish choralari va qonuniy himoya mexanizmlari tahlil qilinadi. Tadqiqotda xalqaro va milliy statistik ma’lumotlar, ekspertlar fikrlari, shuningdek, firibgarlik qurboni bo‘lgan shaxslar holatlari namoyish etilgan. Maqolaning asosiy maqsadi – foydalanuvchilarni xavf ostida

qoldirmaydigan, xavfsiz ijtimoiy muhitni shakllantirishga yordam beruvchi amaliy tavsiyalar ishlab chiqish.

Kalit soʻzlar: Ijtimoiy tarmoqlar, kiberjinoyat, firibgarlik (fraud), phishing, fake profil, maʼlumotlar xavfsizligi, siberhuquq, foydalanuvchilar himoyasi.

Ijtimoiy tarmoqlar zamonaviy kommunikatsiyaning ajralmas qismiga aylangan boʻlsa-da, ularning qulayligi bilan birga koʻplab xavflarni ham olib kelmoqda. Soʻnggi yillarda Facebook, Instagram, Telegram va TikTok kabi platformalarda firibgarlik holatlari keskin oʻsdi. Bu muammoni hal qilish uchun ham foydalanuvchilar, ham platforma egalari, ham qonun chiqaruvchi organlar samarali choralarni koʻrishlari zarur. Maqola muallifi ushbu masalaga bagʻishlangan tadqiqotlar, statistik maʼlumotlar va amaliy misollar asosida yechimlarni taklif etadi.[1]

Ijtimoiy tarmoqlar zamonaviy jamiyatda aloqa, biznes va axborot almashishning asosiy vositasiga aylangan. Biroq, ularning keng qoʻllanilishi bilan birga firibgarlik (fraud) ham jiddiy muammo sifatida namoyon boʻlmoqda. Oʻrganishlar shuni koʻrsatadiki, har yili millionlab foydalanuvchilar ijtimoiy media orqali firibgarlik qurboniga aylanmoqda. Ushbu maqolada olimlarning tadqiqotlari, statistik maʼlumotlar va amaliy yechimlar asosida ijtimoiy tarmoqlardagi firibgarlikning dolzarb muammolari va ularga qarshi kurashish usullari muhokama qilinadi. [7]



1-rasm. Statista.com manbasi.

Axborot texnologiyalari jinoyatchilarni aniqlash va ularning faoliyatini kuzatishda muhim rol o‘ynaydi. Ichki ishlar tizimida jinoyatchilarning internet va boshqa elektron tarmoqlardagi faoliyatini monitoring qilish orqali aniqlanib boriladi.

1. Fake Profillar va Identifikatsiya O‘g‘irligi

Tadqiqot: Stanford Universitetining 2023-yilgi hisoboti shuni ko‘rsatadiki, Facebook va Instagramda 10% ga yaqin profil soxta yoki o‘g‘irlangan identifikatsiyaga ega.

Olimlar fikri: Dr. Emily Roberts (Kiberpsixologiya): “Fake profillar odamlarning ishonchini qo‘lga kiritish uchun moslashtirilgan psixologik usullardan foydalanadi. Ularni aniqlash uchun AI asosidagi tizimlar zarur.”[2]

2. Phishing va Social Engineering

Statistika: Kaspersky Lab (2024) ma’lumotlariga ko‘ra, ijtimoiy tarmoqlardagi phishing hujumlari 2020-yilga nisbatan 65% ga oshgan.

Olimlar fikri: Prof. John Smith (Siberxavfsizlik): “Firibgarlar odamlarning hissiy zaifliklaridan foydalanadi. Masalan, “Sizning akkauntingiz bloklandi kabi xabarlar yuborib, foydalanuvchilarni veb-sahifalarga yo‘naltiradi.”

3. Rom-rom (Romance) Firibgarlik

Tadqiqot: FBI (2023) ma'lumotlariga ko'ra, AQShda yiliga \$1 milliarddan ortiq pul romance scam qurboni bo'lganlar tomonidan yo'qotiladi.

Olimlar fikri: Dr. Sarah Johnson (Kriminologiya): "Rom-rom firibgarlik qurboni bo'lganlar ko'pincha uzoq muddatli psixologik ta'sirga duchor bo'lishadi. Bu nafaqat moliyaviy, balki ruhiy zarar ham yetkazadi."

4. Clickbait va Soxta Reklamalar

Statistika: Statista (2024) – Har 3 ta onlayn reklamadan 1 tasi firibgarlik yoki noto'g'ri ma'lumotga asoslangan.

Olimlar fikri: Prof. David Lee (Media Tadqiqotlari): "Ijtimoiy tarmoqlar algoritmlari sensatsion kontentni ko'proq tarqatadi, bu esa firibgarlar uchun qulay muhit yaratadi." [3-4]

Xulosa va Takliflar

Ijtimoiy tarmoqlardagi firibgarlik faqat texnologik muammo emas, balki jamiyatning barcha qatlamlarini qamrab olgan global muammodir. Olimlarning fikriga ko'ra, buning oldini olish uchun quyidagi choralar samarali bo'lishi mumkin: [5-6]

- ✓ AI va kiberxavfsizlikni rivojlantirish (firibgarlikni avtomatik aniqlash);
- ✓ Foydalanuvchilarni tizimli ravishda o'qitish (media savodxonligini oshirish);
- ✓ Qonuniy jazolarni qattiqroq qo'llash (xalqaro hamkorlikni mustahkamlash).

Foydalanilgan adabiyotlar:

1. Stanford University (2023). "Social Media Fraud: Trends and Detection."
2. Kaspersky Lab (2024). "Phishing Attacks in Social Networks."
3. FBI Internet Crime Report (2023).
4. MIT Technology Review (2023). "AI vs. Fake Profiles."
5. Interpol (2023). "Global Cybercrime Strategies."
6. UNESCO (2024). "Digital Literacy for Safer Internet".

КИБЕРПРЕСТУПНОСТЬ В ЦИФРОВУЮ ЭПОХУ: ТЕНДЕНЦИИ РАЗВИТИЯ, ПРОБЛЕМЫ И МЕХАНИЗМЫ ПРОТИВОДЕЙСТВИЯ

Албеков Шокир Адилбекович

*Старший преподаватель цикла физической подготовки
Институт повышения квалификации МВД Республики Узбекистан
shokiralbekov@gmail.com*

Аннотация. Современное общество переживает стремительный процесс цифровизации, что наряду с очевидными преимуществами, сопровождается масштабным ростом киберпреступности. В данной статье проводится комплексный анализ природы киберпреступности, её эволюции, классификации, а также ключевых вызовов в борьбе с этим феноменом. Особое внимание уделяется международному опыту, правовому регулированию, технологиям противодействия, а также перспективам развития национальной системы кибербезопасности в Узбекистане. Предложены рекомендации, направленные на совершенствование механизмов предупреждения и раскрытия преступлений в цифровой среде.

Ключевые слова: киберпреступность, цифровизация, информационная безопасность, хакерство, кибермошенничество, противодействие, Узбекистан, международное сотрудничество.

РАҚАМЛИ АСРДА КИБЕРЖИНОЯТЧИЛИК: РИВОЖЛАНИШ ТЕНДЕНЦИЯЛАРИ, МУАММОЛАРИ ВА ҚАРШИ КУРАШ МЕХАНИЗМЛАРИ

Албеков Шокир Адилбекович

*Ўзбекистон Республикаси ИИВ Малака ошириш институти
Жисмоний тайёргарлик цикли катта ўқитувчиси
shokiralbekov@gmail.com*

Аннотация. Замонавий жамият жадал рақамлаштириш жараёнини бошдан кечирмоқда, бу эса аниқ афзалликлар билан бир қаторда кибержиноятчиликнинг кенг кўламли ўсиши билан бирга кечмоқда. Ушбу мақолада кибержиноятчиликнинг моҳияти, унинг эволюцияси, таснифи, шунингдек, ушбу ҳодисага қарши курашдаги асосий муаммолар комплекс таҳлил қилинади. Халқаро тажриба, ҳуқуқий тартибга солиш, қарши курашиш технологиялари, шунингдек, Ўзбекистонда миллий киберхавфсизлик тизимини ривожлантириш истиқболларига алоҳида эътибор қаратилмоқда. Рақамли муҳитда жиноятларнинг олдини олиш ва

фош этиш механизмларини такомиллаштиришга қаратилган тавсиялар таклиф этилган.

Калит сўзлар: кибержиноятчилик, рақамлаштириш, ахборот хавфсизлиги, хакерлик, киберфирибгарлик, қарши кураш, Ўзбекистон, халқаро ҳамкорлик.

CYBERCRIME IN THE DIGITAL ERA: DEVELOPMENT TRENDS, PROBLEMS, AND CONTRADICTION MECHANISMS

Albekov Shokir Adilbekovich

*Senior teacher of physical training cycle Institute for Advanced Studies of the
Ministry of Internal Affairs of the Republic of Uzbekistan
shokiralbekov@gmail.com*

Abstract. Modern society is experiencing a rapid digitalization process, which, along with obvious advantages, is accompanied by a large-scale increase in cybercrime. This article comprehensively analyzes the nature of cybercrime, its evolution, classification, and key challenges in combating this phenomenon. Special attention is paid to international experience, legal regulation, countermeasure technologies, as well as the prospects for developing the national cybersecurity system in Uzbekistan. Recommendations aimed at improving the mechanisms for preventing and solving crimes in the digital environment have been proposed.

Keywords. cybercrime, digitalization, information security, hacking, cyber fraud, counteracting, Uzbekistan, international cooperation.

ВВЕДЕНИЕ: Цифровая трансформация стремительно охватывает все сферы жизни - от коммерческого сектора до органов государственного управления. Вместе с этим растёт и зависимость от информационно-коммуникационных технологий (ИКТ), что, в свою очередь, способствует росту угроз, связанных с их преступным и несанкционированным использованием. Сегодня киберпреступность стала неотъемлемой частью мировой криминальной среды, и её масштабы продолжают расти. По оценкам экспертов, мировой экономический ущерб от киберпреступлений в 2024 году превысил 8 триллионов долларов США.

Для Узбекистана, активно внедряющего цифровые технологии в экономику, систему электронного правительства и онлайн-сервисы, обеспечение кибербезопасности становится вопросом стратегической важности. Киберпреступность охватывает широкий спектр незаконных действий, совершаемых с использованием интернета, компьютерных сетей, программных решений и цифровых устройств. Она включает как адаптацию традиционных преступлений к цифровой среде (например, мошенничество в сети), так и совершенно новые угрозы, характерные только для виртуального пространства — такие как вредоносные атаки, взломы и распределённые атаки отказа в обслуживании (DDoS).

Ключевые черты киберпреступности заключаются в её трансграничном характере, анонимности исполнителей, высокой технической сложности, постоянной эволюции используемых методов и инструментов, а также в крайне низком уровне раскрываемости - в среднем по миру лишь 15–20% подобных преступлений удаётся раскрыть. Международное сообщество условно делит киберпреступления на три группы.

Первая – это, преступления, направленные против цифровых систем и сетей, включая несанкционированный доступ к данным, вредоносные программы и атаки, нарушающие работу информационных систем.

Вторая - правонарушения, в которых компьютер используется как инструмент совершения преступлений, таких как фишинг, кража данных банковских карт, онлайн-вымогательство, распространение программ-вымогателей (ransomware) и незаконная торговля персональной информацией.

Третья категория охватывает преступления, связанные с контентом: распространение запрещённых материалов, включая детскую порнографию, призывы к экстремизму и насилию, пропаганду наркотиков и самоубийств.

Современные тенденции указывают на ежегодный рост числа киберпреступлений в среднем на 15–20 процентов. Характер атак усложняется за счёт внедрения искусственного интеллекта, машинного обучения и ботнетов. Всё чаще наблюдается коммерциализация киберпреступности - разработка и продажа готовых наборов инструментов для проведения атак. Объектами киберугроз становятся не только отдельные пользователи, но и критически важные элементы национальной инфраструктуры: банковская система, транспорт, энергетика, государственные учреждения.

Для противодействия таким угрозам важно международное сотрудничество. Будапештская конвенция 2001 года остаётся единственным универсальным международным договором по борьбе с

киберпреступностью, подписанным более чем 65 государствами. Хотя Узбекистан пока не является полноправным участником этой конвенции, уже ведётся работа по приведению национального законодательства в соответствие с её положениями. Кроме того, сотрудничество осуществляется через структуры, такие как Интерпол, Европол, ШОС, ОДКБ и Международный союз электросвязи (ITU).

В Узбекистане борьба с киберпреступностью сталкивается с рядом сложностей. Одной из основных проблем является недостаточная правовая база - в уголовном законодательстве ещё не все формы киберпреступлений имеют чёткие определения. Сказывается также нехватка квалифицированных специалистов в таких областях, как цифровая криминалистика и аналитика информационной безопасности. Хотя национальный центр кибербезопасности был создан, он пока не функционирует в полной мере. Граждане, особенно пожилые и молодые, обладают недостаточной цифровой грамотностью, что делает их уязвимыми перед киберугрозами. Кроме того, техническое оснащение правоохранительных органов остаётся на низком уровне: программное обеспечение устарело, а лицензированные решения и цифровые лаборатории имеются в ограниченном количестве.

Для эффективного противодействия киберпреступности необходимо предпринимать шаги на нескольких уровнях. В законодательной сфере требуется обновление Уголовного кодекса с учётом современных форм киберпреступлений, принятие специализированного закона «О кибербезопасности», а также нормативное регулирование обработки и хранения персональных данных. Институциональные меры включают создание координационного центра по вопросам кибербезопасности, развитие национального центра реагирования на инциденты в киберпространстве (CERT.uz), а также формирование специализированных подразделений в структурах МВД, СНБ и прокуратуры.

С технологической точки зрения важным направлением является внедрение систем мониторинга и анализа безопасности (SIEM), использование решений на базе ИИ для обнаружения угроз, развитие национальной облачной инфраструктуры с защищённым доступом, а также применение технологии блокчейн для подтверждения подлинности транзакций и данных.

Необходимо также уделить внимание образовательной и культурной составляющей. Это включает введение в школах и вузах дисциплин по цифровой гигиене и кибербезопасности, открытие магистратур по подготовке специалистов в этой области, а также проведение широкомасштабных медиакампаний, направленных на повышение осведомлённости населения.

Перспективы развития кибербезопасности в Узбекистане предусматривают принятие долгосрочной Национальной стратегии до 2030 года, подключение к международным системам раннего оповещения, создание платформ для реагирования на инциденты в частном секторе, а также формирование «киберрезерва» — инициативной группы IT-специалистов, способной участвовать в защите инфраструктурной безопасности страны.

В целом, киберпреступность является не временной угрозой, а долгосрочным вызовом, с которым необходимо бороться комплексно и системно. Только постоянное развитие, модернизация нормативной базы, повышение цифровой культуры и активное участие в международных инициативах позволят Узбекистану эффективно защищать свои интересы в цифровом пространстве.

Литература:

1. Конвенция о киберпреступности (Будапешт, 2001)
2. Закон Республики Узбекистан от 15.04.2022 г. О кибербезопасности № ЗРУ-764.
3. Алимова Р.Р. Борьба с киберпреступностью в республике узбекистан. киберпреступность как вид мошенничества. // [Central Asian Research Journal for Interdisciplinary Studies \(CARJIS\)](#). 2022.
4. Абдуллаев Р.Р. Киберугрозы и безопасность: Узбекистан в цифровую эпоху – Ташкент, 2023
5. Хайдаров Д. Правовые аспекты борьбы с киберпреступлениями в Узбекистане // Юридическая наука, №2, 2024

АХБОРОТ ТЕХНОЛОГИЯЛАРИ ВА ХАВФСИЗЛИГИ СОҶАСИДАГИ ЖИНОЯТЛАРНИНГ ОЛДИНИ ОЛИШНИНГ ЎЗИГА ХОС ХУСУСИЯТЛАРИ

Убайдуллаев Шерзод Музаффарович

*ИИВ Малака ошириш институти Махсус-касбий фанлар кафедраси
катта ўқитувчиси*

Глобал тараққиёт шароитида ахборот технологиялари моҳиятини оширишнинг янада замонавий, инновацион усуллари излаб топиш, ахборотлаштириш жараёнига ҳар томонлама кўмаклашиш, уларни ҳаётга кенг жорий этиш давлат фаолиятининг муҳим йўналишларидан бирига

айланмоқда. Зеро, ахборотлаштириш тизимида давлат сиёсатини олиб бориш масаласи стратегик аҳамиятга эга вазифадир⁶⁵.

Дунёда ахборот технологиялари ва хавфсизлиги соҳасидаги жинойтчиликка қарши курашиш муаммолари тобора глобал аҳамият касб этмоқда. Хусусан БМТ Бош Ассамблеяси, Европа кенгаши, ШХТ, МДХ, Араб давлатлари лигаси ва бошқа ташкилотлар томонидан ахборот-коммуникатсия технологияларидан жинойий мақсадларда фойдаланишга қарши курашиш бўйича ҳалқаро ҳуқуқий ҳужжатлар қабул қилинган. Статистик маълумотларга кўра, ҳозирги вақтда **7 миллиардга** яқин инсон (дунё аҳолисининг 95%) электр алоқасининг кўчма тармоқлари билан қамраб олинган⁶⁶, йилига кибержинойтчилик оқибатида етказилган моддий зарарнинг миқдори дунё ЯИМнинг **1 %ни** ташкил этади⁶⁷.

Янгидан-янги турлари билан тилга олинмаган кибержинойтчиликнинг ижтимоий ҳаётимизга кириб келганига ҳам анча бўлди ва уни асримизнинг глобал муаммолари қаторига қўшимиз мумкин. Унинг бизга маълум бўлган вирусли дастурларни тарқатиш, паролларни бузиб кириш, кредит карта ва бошқа банк реквизитларидаги маблағларни ўзлаштириш талон-тарож қилиш, шунингдек Интернет орқали қонунга зид ахборотлар, хусусан бўҳтон, маънавий бузуқ маълумотларни тарқатиш билан башарият ҳаётига катта хавф солаётганидан кўз юмиб бўлмайди.

Интернет (ингл. Интернет) – ахборотни сақлаш ва узатиш учун мўлжалланган бутунжаҳон умумлаштирилган компьютер тўридир. Кўпинча “Умумжаҳон тўри” ёки “Глобал тўр” деб номланади. Унинг асосида “Бутунжаҳон ўргимчак тўри” (World Wide Web, WWW) ва бошқа алоқа системалари фаолият юритади.

Ҳозир бутун дунёдаги инсониятнинг 63 фоизи интернетдан фойдаланади. Қарийб бир йилда интернет фойдаланувчилари сони 200 миллионга ортган. Фойдаланувчиларнинг асосий қисми (**92,4 фоиз**) мобил қурилмалар орқали интернетдан фойдаланади. Ўзбекистонда интернет фойдаланувчилари сони **27 миллиондан** ошган, шундан **25 миллиондан** кўпроғи мобил интернет фойдаланувчилари ҳисобланишади⁶⁸.

Ахборот технологияларининг кенг миқёсда ривожланиши бир вақтнинг ўзида кўп турдаги жинойтларнинг содир этилишига имкон яратди, ўз навбатида ушбу турдаги жинойтларни аниқлаш ва уларни олдини олишда

⁶⁵ Х.Б. Абдреймов Ахборот технологиялари соҳасидаги жинойтлар ва улардан ҳимояланиш усуллари ИИВ Академия Магистратура ингловчиси.

⁶⁶ Расулев А. К. Ахбороттехнологияларивахавфсизлигисоҳасидаги жинойтларга қарши курашишнинг жинойт-ҳуқуқий ва криминологик чораларини такомиллаштириш. Юрид. фанлар доктори диссертациясининг автореферати. Т., ИИВ Академияси, 2018. - Б-5.

⁶⁷ <http://www.statista.com/The-StatisticsPortal>).

⁶⁸ <https://review.uz/oz/post/ozbekistonda-internet-xizmatidan-foydalanuvchilar-soni-272-milliondan-oshdi>

юқори билим ва касбий тайёргарликни талаб қилмоқда. Шундай қилиб, “ахборот технологиялари соҳасидаги жинойт” компьютерлар ва маълумотларни қайта ишлаш тизимларидан фойдаланган ҳолда содир этиладиган жиноий қилмиш бўлиб, бунинг учун қонунчиликда жиноий жавобгарлик назарда тутилган. Шу боис, фуқаролар ўртасида ахборот технологиялари соҳасидаги жинойтлар тўғрисида маълумотларни тарқатиш ва тарғибот-ташвиқот ишларини олиб бориш зарур.

Ахборотлашган жамият тезлик билан шаклланиб, ахборот дунёсида давлат чегаралари деган тушунча йўқолиб бормоқда. Жаҳон компьютер тармоғи давлат бошқарувини тубдан ўзгартирмоқда.

Ҳудудий жойлашишидан қатъий назар, кундалик ҳаётимизга турли хилдаги ахборотлар интернет халқаро компьютер тармоғи орқали кириб келади. Шунинг учун ҳам мавжуд ахборотлардан ноқонуний фойдаланиш, ўзгартириш, йўқотиш ва уларга кириш каби муаммолардан ҳимоя қилиш долзарб масала бўлиб қолди.

Маълумотларга кўра, дунё бўйлаб ҳар йили **500 миллиондан** ортиқ киберхужумлар уюштирилади. Ҳар сонияда дунёдаги ҳар **12 нафар** инсондан бири кибермаконда содир этилган хужумлар қурбонига айланмоқда. Хусусан, АҚШ, Франция, Англия, Белгия, Германия, Луксембург каби давлатларда кибержинойтчилик кўрсаткичи умумий жиноятчиликнинг **60–65 фоизини** ташкил этади.

Экспертларнинг ҳисоб-китобича, киберхужумларнинг асосий қисми махфий маълумотларни қўлга киритиш, уларни ўзгартириш ёки йўқотиш, фойдаланувчилардан пул талаб қилиш ёки бизнес жараёнларини издан чиқаришга қаратилмоқда. Бунинг натижасида бир йилда дунё иқтисодиёти ўртача **20 миллиард** АҚШ долларидан зиёд миқдорда зарар кўрмоқда.

Ўзбекистонда ҳам сўнгги уч йилда кибержинойтлар **8,3 бараварга** кўпайиб, умумий жиноятчиликнинг **5 фоизини** ташкил этмоқда. Масалан, кибермаконда фирибгарлик билан боғлиқ ҳолатлар **13 бараварга**, ўғрилиқ **20 бараварга**, товламачилик, туҳмат ва ҳақорат қилиш билан боғлиқ жиноятлар эса **4,9 бараварга** ортган.

Жиноий-ҳуқуқий тушунчада компьютер ахбороти ахборот технологиялари соҳасидаги жиноятларнинг предмети ҳисобланади. Масалан бундай ҳолатлар Жиноят кодекси 2781, 2782, 2784, 2786 ва 2787-моддаларининг диспозитсияларида тўғридан-тўғри кўрсатилган. Бошқа ҳолларда эса предметнинг аниқланиши жиноят таркиби бошқа элементларининг аниқланиши билан боғлиқ (ЖКнинг 2783 ва 2785-моддалари).

Ўзбекистон Республикаси Жиноят кодекси Махсус қисмининг ахборот технологиялари соҳасидаги жиноятларга оид бобининг хусусияти шундаки, унда ахборотнинг алоҳида тури – компьютер ахбороти ҳақида сўз боради.

Юқоридагилардан келиб чиққан ҳолда таъкидлаш мумкинки, ушбу турдаги жиноятлар ахборот технологияларидан қонуний, хавфсиз фойдаланишни таъминловчи муносабатларга бевосита тажовуз қилади ҳамда фойдаланувчиларнинг ахборот технологиялари соҳасидаги қонуний манфаатларига зарар етказди.

Ахборот технологиялари соҳасидаги жиноятларнинг олдини олишда куйидагиларга алоҳида эътибор қаратиш таклиф этилади:

биринчидан, Ўзбекистон Республикаси Жиноят кодексининг 168-моддаси 2-қисми “в” бандини “телекоммуникатсия тармоқларидан, шунингдек, Интернет жаҳон ахборот тармоғидан ёки электрон тўлов воситаларидан фойдаланиб” тарзида баён этиш, 273-моддаси 2-қисмини “телекоммуникатсия тармоқларидан, шунингдек Интернет жаҳон ахборот тармоғидан фойдаланиб содир этилган бўлса” таҳриридаги янги “д” банди билан тўлдириш.

Содир этилаётган фирибгарлик жиноятлари таҳлил қилинганида, аксарият бу турдаги жиноятлар ахборот технологияларидан фойдаланган ҳолда, айниқса, мобил иловалар орқали банк пластик карталаридан пулларни фирибгарлик ва ўғрилиқ қилиш орқали ўзлаштириш ҳолатлари кўпаймоқда.

Амалдаги Жиноят кодексининг 168-моддаси 2-қисми “в” бандида ёки 169-моддаси 3-қисми “б” бандида компьютер техникасидан фойдаланиб содир этилган фирибгарлик ва ўғрилиқ жиноятлари учун жавобгарлик белгиланган. Бироқ “Компютер техникасидан фойдаланиб содир этиш” тушунчаси тор маънода бўлиб, ҳозирда бу турдаги жиноятларнинг содир этиш усулини тўлиқ қамраб олмаяпти.

Қолаверса, мазкур моддани шу йўналишда 2022 йил 15 апрелда қабул қилинган “Киберхавфсизлик тўғрисида”ги Қонун талабларига мослаштириш лозим.

Таклиф этилаётган *“Телекоммуникатсия тармоқларидан, шунингдек Интернет жаҳон ахборот тармоғидан ёки электрон тўлов тизимларидан фойдаланиб”* жумласи Россия Федератсияси Жиноят кодексининг 159.6-моддасида ўз аксини топган бўлиб, ушбу қилмиш учун алоҳида жиноий жавобгарлик белгиланган. Бундан ташқари, Россия Федератсияси Жиноят кодексининг 159.3.-моддасида электрон тўлов воситаларидан фойдаланиб содир этилган фирибгарлик учун алоҳида жиноий жавобгарлик белгиланган.

Шунингдек, Украина Жиноят кодексининг 190-моддасида, Латвия Жиноят кодексининг 177.1-моддасида қонунга хилоф равишда электрон

ҳисоблаш машинаси техникасидан фойдаланганлик ва автомат тизимида маълумотларга ишлов беришда фирибгарлик содир этганлик учун махсус жинойий жавобгарлик белгиланган;

иккинчидан, мобил илова аккаунтини фаоллаштиришда (телефон аппаратининг ИМЕИ коди, ИП-манзиллар рўйхатидан ташқари) фойдаланувчининг юз кўриниши (Фасе ИД), географик жойлашув (геопозитсия - Лосатион) маълумотларини тўлиқ киритишга доир техник шартни жорий этиш.

Маълумот учун: 2017 йилда Россиядаги “Сбербанк” ҳамда “Точка” номли мобил иловаларида “Фасе ИД”, “Лосатион” функциясининг жорий этилиши улар билан боғлиқ жинойятларнинг **85 %**га камайишига олиб келган. Мазкур амалиётнинг йўлга қўйилиши мобил иловалар орқали содир қилинаётган жинойятларнинг камайишига, жинойятни содир қилган шахс ҳамда жойлашган манзили ҳақидаги маълумотларни ўз вақтида аниқлашга, молия хизматларини кўрсатиш субъектлари ҳамда дастурий таъминотдаги хавфсизлик даражаси яхшиланишига, фуқароларнинг пластик карталаридаги маблағлари ишончли муҳофаза қилиниши таъминланишига хизмат қилади;

учинчидан, “Ропулатион оф Узбекистан” ахборот-қидирув-маълумотнома тизимини жорий қилиш ва бунда сунъий интеллект технологиялари имкониятларидан кенг фойдаланиш.

Дунёнинг етакчи давлатлари (Италия, АҚШ ва ҳ.к.) тажрибасига кўра, мамлакат аҳолисининг ҳар бирининг туғилганидан бошлаб вафот этгунига қадар барча жараён, жумладан боғчада, мактабда (литсей, коллеж, техникум ва ҳ.к.), олий таълим муассасасида таълим олиш ва иш жойидаги меҳнат қилиш жараёнларида унинг феъл-атвори, қизиқиши, атрофидаги инсонлари, оилавий аҳволи ва ҳ.к. маълумотлари доимий ва мунтазам тўлдирилиб бориладиган, марказлаштирилган, рухсат даражалари белгиланган “Ропулатион оф Узбекистан” ахборот-қидирув-маълумотнома тизимини жорий қилиш ва бунда сунъий интеллект технологиялари имкониятларидан кенг фойдаланиш таклиф этилади.

Бу тизим мамлакатимиз аҳолиси тўғрисида барча маълумотларни жамлаганлиги сабаб жинойятларни “иссиқ изи”дан очиш ҳар бир криминал вазиятда аниқ ва тўғри қарорлар қабул қилиш учун хизмат қилади. Мазкур тизимнинг ички ишлар тизимларига жорий қилинаётган рақамли технологиялар билан интеграциялашуви бугунги кунда жинойятларни жиловлаш учун энг катта самара берадиган тадбирлардан бири бўлади;

тўртинчидан, ижтимоий тармоқларда таниқли бўлган блогер, вайнер ҳамда тиктокерлардан кенг фойдаланган ҳолда ахборот технологиялари

соҳасидаги жиноятларнинг олдини олиш бўйича тарғибот-ташвиқот тадбирларини янада кучайтириш.

Сўнги вақтларда аҳолининг ҳуқуқий маданиятини оширишда, жиноятчиликка қарши курашда ижтимоий тармоқларнинг роли ошиб бормоқда.

Хусусан, айрим блогер, вайнер, тиктокерлар томонидан жамиятнинг барча ижтимоий соҳаларида бўлаётган жараёнларни турли кўринишларда намойиш этишлари миллионлаб фуқаролар томонидан томоша қилиниб, ижтимоий тармоқларда аҳоли орасида муҳокамалар қилинмоқда.

Ҳозирда аҳолининг ҳуқуқий маданиятини оширишда, кибержиноятчиликка қарши курашда блогер, вайнер, тиктокерларнинг хизматларидан фойдаланишни кучайтириш орқали фуқароларни ўзига жалб қиладиган, кўплаб муҳокамаларга сабаб бўладиган ижтимоий роликлар, карикатуралар, видеороликлар, буклетлар, суръатлар ишлаб чиқиш ва уларни аҳоли орасида, айниқса, блогер, вайнер, тиктокерларнинг шахсий профилларида намойиш қилиш мақсадга мувофиқдир.

ЯНГИ ЎЗБЕКИСТОНДА РАҚАМЛИ ИҚТИСОДИЁТ

Убайдуллаев Шерзод Музаффарович

*ИИВ Малака ошириш институти Махсус-касбий фанлар кафедраси
катта ўқитувчиси*

Ҳозирги кунда рақамли иқтисодиётнинг дунё миқёсида тутган ўрни ва унинг ривожланиш тенденциялари тобора ортиб бормоқда. Мисол учун, маълумотлар оқими кўламининг ўзгариши интернет протоколи (IP) га асосланган глобал трафик ҳажмининг 1992 йилда кунига 100 гигабайтни ташкил этган бўлса, 2019 йилда бу кўрсаткич секундига 89000 Гб дан ошди. Бу маълумотлар рақамли иқтисодиёт ривожланишининг дастлабки босқичига тегишли эканини ҳисобга олсак, унинг ривожланиши суръати тўғрисида тасаввур ҳосил қилиш қийин эмас. Прогнозларга кўра, 2022 йилга келиб глобал IP-трафик ҳажми секундига 150700 Гб га етади, бу Интернет тармоғида янги фойдаланувчиларнинг кўпайиши ва Интернетнинг янада кенгайиши натижасида амалга ошади⁶⁹. Жаҳон миқёсида олиб қарайдиган бўлсак, рақамли иқтисодиётнинг ривожланиш географиясида икки мамлакат етакчи ўринни эгаллаб турибди. Булар АҚШ ва Хитой.

⁶⁹ 1 БМТ савдо ва ривожланиш конференцияси. Рақамли иқтисодиёт бўйича ҳисобот (2019). https://unctad.org/en/PublicationsLibrary/der2019_overview_ru.pdf

Бу мамлакатларга блокчейн технологияси билан боғлиқ бўлган барча патентларнинг 75 фоизи, “Internet of Things (Нарсаларинтернети)”га⁷⁰ сарфланадиган харажатларнинг 50 фоизи ва булутли ҳисоблаш очик технологиялари глобал бозорининг 75 фоизидан ортиғи тўғри келади. Энг диққатга сазовор томони шундаки, улар дунёдаги 70 та энг йирик рақамли платформаларнинг бозор капиталлашувининг 90фоизини назорат қилишади. Технологияларда глобал устунликка интилишнинг оқибатида юзага келади.

АҚШ ва Хитойнинг ЯИМ ҳажми бўйича жаҳонда биринчи ва иккинчи ўринларни эгаллаб турганлигини эътиборга олсак, рақамли технологияларнинг мамлакат иқтисодиётини ривожлантиришда стратегик аҳамиятга эга эканлигига яна бир бор ишонч ҳосил қилишмумкин. Ҳозирги пайтда компьютерлаштириш ва юқори технологиялар асрида рақамли иқтисодиёт ҳаётимизнинг ҳар бир жабҳасига: соғлиқни сақлаш, таълим, интернет-банкнинг, ҳукуматга дахлдор бўлмоқда.

Ўзбекистон Республикаси Президентининг “Рақамли иқтисодиёт ва электрон ҳукуматни кенг жорий этиш чора-тадбирлари тўғрисида”ги 2020 йил 28 апрелдаги, ПҚ-4699-сонли Қарори асосида 2023 йилга келиб рақамли иқтисодиётнинг мамлакат ялпи ички маҳсулотига улушини 2 бараварга кўпайтиришни назарда тутилган.

Иқтисодиётни ривожлантириш стратегияси саноат, хизмат кўрсатиш соҳаси ва қишлоқ хўжалигини раванқ топтириш, тадбиркорда ташаббускорликни кучайтириш, молиявий ресурслар билан таъминлаш каби омилларга асосланади. Иқтисодиётда чуқур таркибий ўзгаришларни амалга ошириш ҳисобига 2035 йилга бориб, мамлакат ялпи ички маҳсулоти 122 миллиард долларга етказилади. Ўсиш суръатининг бундай кўламини белгилашда ЯИМнинг номинал ўсиши, иқтисодиёт самарадорлиги, аҳоли жон бошига даромадлар ошиши ҳисобга олинган.

Ижтимоий соҳани ривожлантириш бўлимида таълим тизими, меҳнат бозори ҳисобига инсон капиталини ривожлантириш, аҳолининг барча қатламларини сифатли тиббий хизмат билан қамраб олиш, илм-фан ва инновацияларни ривожлантириш орқали аҳолининг соғлиғини яхшилаш кўрсаткичларини ошириш, ижтимоий ҳимоя, атроф-муҳитни асраш, илғор фикрлайдиган янги авлодни шакллантириш, мамлакатнинг миллий брендини халқаро миқёсда оммалаштириш каби мақсадлар баён этилган. Ўзбекистонни 2035 йилгача ривожлантириш стратегияси Ҳаракатлар стратегиясининг

⁷⁰ Internet of Things, IoT – қурилмаларни компьютер тармоғига бирлаштирадиган ва уларга дастурий таъминот, амалий дастурлар ёки техник воситалардан фойдаланган ҳолда маълумотларни тўплаш, таҳлил қилиш, қайта ишлаш ва бошқа объектларга узатиш имконини берадиган технология.

мантикий давоми бўлиб, юртимиз тараққиётида янги саҳифа очиши билан аҳамиятлидир. Стратегия лойиҳасида белгиланган марраларга эришиш учун ҳар бир соҳада ислоҳотларни босқичма-босқич, аниқ муддатларда руёбга чиқариш прогнозлари кўрсатилган.

Мамлакатни бугунги кунда демократик, эволюцион йўлдан ривожланиши энг самарали йўл бўлиб, ўзининг самарали натижаларини бермоқда. Бозор иқтисодиёти шароитида ҳамма нарсани талаб ва таклиф белгилайди. Аҳолининг талаб ва таклифини қондириш мақсадида Ўзбекистон Республикаси Президентининг 2022 йил 28 январдаги ПФ-60-сонли фармонининг *учунчи устувор йўналишида Миллий иқтисодиётни жадал ривожлантириш ва юқори ўсиш суръатларини таъминлаш* доирасида корхоналарнинг модернизация қилиш ва жадал ривожлантириш орқали рақамли иқтисодиёт технологияларни жорий этиш бўйича илмий-тадқиқот ишларини кенгайтириш катта аҳамият касб этади. стратегиясини 2035 йилларда амалга оширишда рақамли иқтисодиёт муҳим роль ўйнайди. Ўзбекистон Республикаси Президенти Ш.М.Мирзиёевнинг Олий Мажлисга Мурожаатномасида таъкидлаганидек: “...рақамли иқтисодиётни шакллантириш керакли инфратузилма, кўп маблағ ва меҳнат ресурсларини талаб этишини жуда яхши биламиз. Бироқ, қанчалик қийин бўлма-син, бу ишга бугун киришмасак, қачон киришамиз?! Эртага жуда кеч бўлади.

Шу боис, рақамли иқтисодиётга фаол ўтиш – келгуси 5 йилдаги энг устувор вазифаларимиздан бири бўлади. Рақамли технологиялар нафақат маҳсулот ва хизматлар сифатини оширади, ортиқча харажатларни камайтиради”⁷¹. Умумжаҳон тенденциялари ва ташқи сиёсатда рўй бераётган ҳодисалардан келиб чиқиб, Ўзбекистон олдида глобал рақобатбардошлик ва миллий хавфсизлик масаласи турибди ва ушбу масалани ҳал қилишда мамлакатда рақамли иқтисодиётни ривожлантириш муҳим роль ўйнайди. Рақамли иқтисодиётнинг айрим элементлари аллақачон муваффақият билан ишламоқда.

Ҳозирги кунда, ҳужжатлар ва коммуникацияларнинг оммавий равишда рақамли воситаларга ўтказилишини ҳисобга олиб, электрон имзога рухсат бериш, давлат билан мулоқот қилиш ҳам электрон платформага ўтказилмоқда. Ўзбекистон Республикасининг “Илм-фан ва илмий фаолият тўғрисида”ги 2019 йил 29 октябрдаги 576-сонли қонунига асосан илм-фан ва технологияларни ривожлантиришнинг устувор йўналишлари миллий иқтисодиёт рақобатбардошлиги ҳамда самарадорлигига эришиш, меҳнат унумдорлигини ошириш, янги тармоқларни яратиш, аҳоли турмуш даражаси,

⁷¹ 3Мирзиёев Ш.М. Ўзбекистон Республикаси Президенти Ш.М.Мирзиёевнинг Олий Мажлисга Мурожаатномаси. // Халқ сўзи, 2022 йил.

илм-фан ва таълим тизимларини сифат жиҳатидан юксалтириб бориш билан боғлиқ муаммоларнинг илмий ечимини таъминлаш мақсадида ишлаб чиқилади⁷².

Иқтисодиёт тармоқларида инновация, замонавий техника ва технологиялар қўллашни амалга ошириш учун рақамли иқтисодиётдан кенг фойдаланиш зарур. Ушбу талабларга жавоб бериш учун “Рақамли иқтисодиёт” фани бўйича чуқур билимга эга бўлиш муҳим аҳамиятга эга. Иқтисодий жараёнларни рақамлаштириш нафақат бевосита ахбороткоммуникация тармоғини, балки мамлакат хўжалик фаолиятининг барча соҳаларини ҳам қамраб оладиган кенг қамровли тенденцияга айланиб бормоқда.

Интернет-савдо, рақамли қишлоқ хўжалиги, «ақлли» электр-тармоқ тизимлари, учувчисиз транспорт, шахсийлаштирилган соғлиқни сақлашда рақамли иқтисодиёт инқилоби кучли ҳис қилинмоқда. Шу сабабли Ўзбекистон Республикаси Президентининг 2018 йил 22 ноябрда қабул қилинган қарорида таъкидланишича: «Рақамли иқтисодиётни жадал ривожлантириш учун шарт-шароитлар яратиш, давлат бошқаруви тизимини янада такомиллаштириш, ундан фойдаланиш имкониятларини кенгайтириш, замонавий инфратузилмани қўллаш муҳим аҳамиятга эга»⁷³ деб кўрсатилиши рақамли иқтисодиётни ривожлантириш инфратузилмасини амалга ошириш кўзда тутилган.

Ўқув қўлланмани ўзлаштириш натижасида талаба: — рақамли иқтисодиётнинг технологик, ҳолатий, ташкилий-ҳуқуқий ҳамда институционал хусусиятларини инобатга олган вазиятларни тўғри моделлаштириш, рақамли иқтисодиёт инфратузилмасини ташкил этиш; “блокчейн” технологияларнинг моҳиятини англаб етиш; глобал ахборот ресурс базаларидан самарали фойдаланиш усул ва йўллари билди ва улардан фойдалана олади;

- рақамли иқтисодиётни ривожлантириш, “блокчейн” технологияларини жорий этиш; давлат хусусий шериклик шартларида рақамли иқтисодиётни ривожлантириш, крипто-биржалар фаолиятини ташкил этиш, энг истиқболли ва стратегик муҳим лойиҳаларни амалга ошириш кўникмаларига эга бўлади;

- рақамли трансформациясининг ижобий ҳамда салбий оқибатлари, уларга таъсир этувчи омилларни аниқлаш; рақамли иқтисодиётнинг макро

⁷² Ўзбекистон Республикасининг “Илм-фан ва илмий фаолият тўғрисида”ги Қонуни, 29 октябр 2019 йил.

⁷³ Ўзбекистон Республикаси Президентининг «Рақамли иқтисодиётни ривожлантириш мақсадида рақамли инфратузилмани янада модернизация қилиш чора-тадбирлари тўғрисида»ги Қарори// «Халқ сўзи» газетаси, 22 ноябрь 2018 йил

хамда микро даражадаги кўрсаткичларга таъсирини баҳолаш; рақамли трансформация самарадорлигини баҳолаш;

- ахборот хавфсизлиги муаммоларини аниқлаш; давлат хусусий шерикчилик асосида рақамли иқтисодиётни ривожлантириш учун платформалар ташкил этиш кўникмаларига эга бўлади.

Юқоридагиларга асосланиб, Ўзбекистон Республикаси иқтисодиёт тармоқларида олиб борилаётган иқтисодий ислохотлар йўналишларининг мазмун ва моҳиятини ҳамда корхоналарда рақамли иқтисодиётни қўллашда Ўзбекистон Республикаси Олий Мажлиси томонидан қабул қилинган қонунларга, Ўзбекистон Республикаси Президенти Ш.М.Мирзиёев асарларига, Президент фармон ва қарорларига, Вазирлар Маҳкамасининг қарорларига асосланади. Бундан ташқари, корхоналарда рақамли иқтисодиёт муаммолари билан шуғулланувчи профессорўқитувчилар, талабалар, тадқиқотчилар, илмий изланувчилар, тадбиркорлар ҳамда бошқа иқтисодиёт тармоқлари ходимлари ҳам фойдаланишлари мумкин.

AXBOROT TEXNOLOGIYALARI SOHASIDAGI JINOYATLAR: XAVF, SABAB VA YECHIMLAR

Aliyeva Zuxra Mamatkulovna

IV Malaka oshirish instituti Maxsus kasbiy fanlar kafedراسи katta o'qituvchisi

Annotasiya. Mazkur maqolada axborot texnologiyalari sohasidagi jinoyatlar tushunchasi, ularning turlari, kelib chiqish sabablari, jamiyat va davlatga yetkazayotgan salbiy oqibatlarini tahlil qilingan. Shuningdek, O'zbekistonda kiberxavfsizlik sohasida amalga oshirilayotgan islohotlar, qonunchilik asoslari va muammoni hal qilishga qaratilgan tavsiyalar ilmiy tahlil qilingan.

Tayanch so'zlar: Elektron hukumat, raqamli banklar, axborot texnologiyalari sohasidagi jinoyatlar, kiber jinoyatlar, asosiy omillari, onlayn tovlamachilik, kiberxujum, kibermadaniyat.

Axborot texnologiyalari XXI-asrning eng muhim kashfiyotlaridan biri bo'lib, barcha sohalarda tub o'zgarishlarga sabab bo'ldi. Elektron hukumat, raqamli banklar, masofaviy ta'lim, onlayn savdo va boshqa ko'plab elektron tizimlar inson hayotini yengillashtirdi. Biroq, axborot texnologiyalarining rivojlanishi bilan birga, jamiyat uchun jinoyatchilikning yangi bir turini, ya'ni **kiberjinoyatchilikni** yuzaga keltirdi. Bu esa o'z navbatida jamiyatimiz xavfsizligiga jiddiy tahdid sola boshladi.

O‘zbekiston ham bu jarayondan chetda qolmadi. Internet foydalanuvchilar sonining keskin ko‘payishi, raqamli xizmatlarning ommalashuvi bu jinoyatchilar uchun keng imkoniyatlarni yaratdi.

Bu maqolada aynan shu kabi axborot texnologiyalari bilan bog‘liq jinoyatlar tahlil qilinadi.

Axborot texnologiyalari sohasidagi jinoyatlar — bu axborot texnologiyalari, axborot tizimlari, axborot va telekommunikasiya tarmoqlaridan foydalangan holda sodir etilgan va jamoatchilik bilan munosabatlarga zarar yetkazishga qaratilgan ijtimoiy xavfli qilmishlardir. Ular kiber jinoyatlar sifatida tanilgan va an‘anaviy jinoyatlardan quyidagicha farqlanadi:

1. **Anonim shaklda** amalga oshiriladi;
2. **Geografik nuqtai nazaridan chegaraga ega emas** (xoriydan turib ham boshqariladi);
3. **Isbotlashning murakkabligi**, bunda ko‘p holatda texnik tahlillar talab qiladi;
4. **Yetkazilgan zarar darajasi va qamrovining kattaligi** (minglab odamlarni qamrab oladi).

Kiberjinoyatlarning bir turi, yuqori texnologiyali jinoyatlar kompyuterlar yoki uning tarmoqlariga hujum qilish uchun elektron va raqamli texnologiyalardan foydalanadigan jinoyatlar tushuniladi. Bunday jinoyatlarga kompyuterni buzish yoki ma‘lumotlardan ruxsatsiz foydalanish, tarqatish, xizmat ko‘rsatishdan bosh tortish hujumlari va kompyuter viruslarini tarqatish kiradi.

Bugungi kunda internet foydalanuvchilarining soni kundan-kunga oshishi, o‘z navbatida jinoyatchilar uchun yangi jinoyat turlarini kashf etishiga qulay imkoniyatlar eshigini ochib bermoqda.

Afsuski, hozirda axborot va telekommunikasiya resurslaridan jinoiy maqsadlarda foydalanish jamiyat uchun eng katta xavflardan biriga aylandi.

Axborot va telekommunikasiya resurslariga internet tarmog‘i, messengerlar (Telegram, WhatsApp, Signal), ijtimoiy tarmoqlar (Facebook, Instagram, X, TikTok va h.k), elektron pochta va SMS xizmatlari, onlayn platformalarni (savdo, bank, o‘yinlar, ta‘lim, forumlar) kiritish mumkin.

Aynan shu resurslar bugungi jinoyatchilar uchun eng qulay va samarali hamda anonim vositaga aylanmoqda.

O‘zbekistonda eng ko‘p keng tarqalgan axborot jinoyatlari firibgarlik, mualliflik huquqini buzish, telefon va internet orqali tovlamachilik, kibershantaj va shaxsiy ma‘lumotlar bilan tahdid qilish, onlayn bulling va yoshlar orasida kiberqizg‘inlik kabi turlari tarqalgan.

Mazkur jinoyatlar sodir etilishining asosiy omillari sifatida **moliyaviy manfaat** bunda bank hisoblarini buzish, onlayn to‘lovlarni o‘g‘irlash, **xavfsizlik**

tizimlarining zaifligi — ko‘plab korxonalar, muassasa, tashkilotlarda kiberximoya talab darajasida emasligi, **aholining huquqiy savodxonligining yetishmasligi** bunda yoshlar orasida internetdagi harakatlarining huquqiy oqibatini tushunmasligi, mavjud qonunchilikdagi huquqiy bo‘shliqlar va jinoiy jazo muqarrarligining pastligidir.

Eng avvalom bor kiberjinoyatlarning sodir etilish sabablaridan birinchi navbatda, jamiyatning iqtisodiy holati, shuningdek, har bir jinoyatchining moddiy ahvolidir. Odamlarni bu jinoyatga qo‘l urishiga masalan, ishsizlik, kam oyliq haqi, qambag‘allik, ochlik, uy-joysizlik, narxlarning ko‘tarilishi kabi ijtimoiy hodisalar sabab bo‘lmoqda.

Yoshlarimizni bo‘sh vaqtlaridan unumli foydalanmay, internet tarmoqlari orqali rasmiy bo‘lmagan kanallarga kirib a‘zo bo‘lishi, bunda ular bu harakati bilan biron bir qilmish sodir etishi, biroq bu harakatning huquqiy oqibati borligini anglab yetmasligi yoki o‘ta ishonuvchan va o‘ta qiziquvchanliklari oqibatida shaxsiy foto suratlarini, shaxsiga doir ma‘lumotlarni ochiq holda joylashi, telegramm kanallardagi har xil lavhalarga o‘z fikriy munosabatlarini yozma bayon qilishlari bois, o‘zlari biron bir jinoyatning sub‘ekti bo‘lib qolishiga sababchi bo‘lmoqdalar. Biroq ayrim fuqarolar o‘z moliyaviy ehtiyojini yaxshilash, yengil daromad topish maqsadida bila turib qasdan jinoyat sodir etayotganlar soni oshib bormoqda.

Bunga misol qilib, onlayn tovlamachilik, ekstremizm vva radikalizm g‘oyalarini tarqatish, shaxsiy ma‘lumotlar bazasiga kiberxujum qilish, psixologik ta’sir qilish, bulling, qalbaki (feyk) xujjatlar va ma‘lumotlar yaratish kabi tahdidlar ko‘payib bormoqda.

Bugungi kunda yurtimizda axborot texnologiyalari yordamida sodir etiladigan bu kabi jinoyatlarga qarshi kurashish faoliyatini yanada kuchaytirish maqsadida O‘zbekiston Respublikasi Prezidentining 2025-yil 30-apreldagi “Axborot texnologiyalari yordamida sodir etiladigan jinoyatlarga qarshi kurashish faoliyatini yanada kuchaytirishga qaratilgan chora-tadbirlar to‘g‘risida”gi PQ-153-son qarori qabul qilindi.

Qarorga ko‘ra, O‘zbekiston Respublikasida kiberjinoyatlarga qarshi kurashish yo‘nalishida yagona ishlash amaliyotini yo‘lga qo‘yish, bu borada barcha mas’ul davlat organlari va muassasalari faoliyatini muvofiqlashtirish hamda manzilli hamkorligini tashkil etish bo‘yicha vakolatli organ Ichki ishlar vazirligi etib belgilandi.

O‘zbekistonda Axborot texnologiyalari yo‘nalishida kiberjinoyatlarga qarshi kurashish vakolati O‘zbekiston Respublikasi Ichki ishlar vazirligiga berilgan. Qarorda ustivor vaziflar, normativ-huquqiy mexanizmlarni takomillashtirish,

kiberjinoyatlarning oldini olish va uni fosh etish mexanizmlari, shuningdek, unga qarshi kurashishda ilmiy yondashuvlar bo'yicha aniq chora-tadbirlar belgilangan.

Shuningdek, qarorda Kiberjinoyatlarning oldini olish yo'nalishidagi targ'ibot-tashviqot tadbirlarida respublika miqyosida har yilning noyabr oyini «Kibermadaniyatni yuksaltirish oyligi» deb e'lon qilish belgilandi.

Xulosa qilib, bu jinoyat va tahdidlarni bartaraf etish uchun qonunlar bilan emas, balki profilaktika, ta'lim, madaniyat va fuqarolarning raqamli savodxonligini oshirish, xavfsizlik standartlarini yaratish, xalqaro hamkorlikni kuchaytirish talab etiladi.

Adabiyotlar ro'yxati:

1. O'zbekiston Respublikasi konstitutsiyasi;
2. O'zbekiston Respublikasi Jinoyat kodeksi;
3. O'zbekiston Respublikasi Prezidentining 2025-yil 30-apreldagi "Axborot texnologiyalari yordamida sodir etiladigan jinoyatlarga qarshi kurashish faoliyatini yanada kuchaytirishga qaratilgan chora-tadbirlar to'g'risida"gi PQ-153-son qarori;

КИБЕР МАКОНДА СОДИР БЎЛАЁТГАН ЖИНОЯТЛАРГА ҚАРШИ ҚУРАШИШНИНГ АЙРИМ ХУСУСИЯТЛАРИ

З. Р. Умаров

*ИИБ Малака ошириш институти Махсус касбий фанлар кафедраси
профессори*

Бугунги кунга келиб глобал ахборот майдонида кибер жиноятлар билан боғлиқ янгидан-янги тахдидлар кузатилмоқда. Шу сабабдан виртуал оламдаги ҳужумлардан ҳимояланиш масаласи дунё ҳамжамиятини жиддий ташвишга солмоқда. Барчамизга маълумки кибержиноятчиларнинг ҳаракатлари нафақат шахсларнинг шахсий маълумотлари, балки давлатларнинг хавфсизлиги, иқтисодий барқарорлиги ва фуқароларнинг ҳуқуқларини ҳам хавф остига қўймоқда. Кибержиноятчиликка қарши курашиш учун ҳуқуқий, ташкилий, молиявий-иқтисодий ва муҳандислик-техник жиҳатлардан комплекс чоралар кўриш лозимлигини тақозо қилмоқда.

Мухтарам Президентимиз Шавкат Мирзиёев 2024 йил 10 январь куни ўтказилган видеоселектор йиғилишида "Кибер-хавфсизликни таъминлаш ва кибер жиноятларга қарши курашиш фуқароларнинг хавфсизлиги ва давлат барқарорлиги учун муҳим омилдир. Бироқ, бу борадаги ишлар талаб даражасида эмас, соҳани такомиллаштириш бўйича қилинадиган ишлар

кўп”⁷⁴ дея таъкидланганди. Президентимиз томонидан билдирилган ушбу танқидий сўзлар кибер жиноятларга қарши курашиш бўлинмалари фаолиятининг самарадорлигини ошириш зарурлигини кўрсатмоқда.

Кибер жиноятлар – бу интернет ва ахборот-коммуникация технологияларидан (АКТ) фойдаланиб содир этиладиган ноқонуний хатти-ҳаракатлар бўлиб, улар шахсий маълумотларни ўғирлаш, молиявий зарар келтириш, жамоат тартибини бузиш ёки давлат хавфсизлигига таҳдид солишга қаратилган бўлади. Кибер жиноятларнинг асосий турларига фишинг, ransomware, DDoS ҳужумлари, маълумотларни ноқонуний олиш, киберфирибгарлик ва хакерлик киради⁷⁵.

Кибер жиноятларнинг ўзига хос хусусиятлари уларни анъанавий жиноятлардан фарқ қилувчи омилларга эга:

- Жадал ривожланиш хусусиятига эга: Кибер жиноятларнинг усул ва воситалари технологиялар ривожланиши билан мунтазам ўзгариб боради. Масалан, сунъий интеллект (AI) асосидаги фишинг ҳужумлари 2024 йилда 25% га ошган⁷⁶

– Трансмиллий хусусиятга эгаллиги: Кибер жиноятлар кўпинча бир неча давлат чегараларидан ўтиб содир қилинади, бу эса уларни аниқлаш ва тергов қилишни қийинлаштиради. Масалан, Интерпол маълумотларига кўра, 2023 йилда кибер жиноятларнинг 60% трансмиллий характерга эга бўлган⁷⁷.

– Анонимлик хусусиятига эгаллиги: Кибер жиноятчилар VPN, Тор тармоқлари ва бошқа анонимлаштириш воситаларидан фойдаланиб, ўз шахсини яширишади⁷⁸.

Интернет билан боғлиқ хавфсизликни таъминлаш бўйича халқаро Symantec Security ташкилотининг маълумотларига кўра, ҳозирда ҳар сонияда дунёдаги 12 нафар инсондан биттаси интернет ҳужуми қурбони бўлмоқда ва ҳар йили 556 млн. дан кўпроқ киберҳужум уюштирилади ва бунда жабрланувчилар кўрадиган зарар миқдори 100 млрд. АҚШ долларидан кўпроқдир⁷⁹.

Дунёда «Глобал ахборотлаштириш ва компьютерлаштириш асри»да инсоният ҳаётида жахоншумул ихтироларни яратилиши билан бир қаторда,

⁷⁴ Мирзиёев Ш.М. “Киберхавфсизлик ва жамоат хавфсизлигини таъминлаш бўйича вазифалар” Халқ сўзи, 2024, 10 январь.

⁷⁵ UNODC. “Cybercrime and Its Impact on Global Economy” 2023

⁷⁶ Lee, K. “AI in National Cybersecurity” Cybersecurity Journal, 2024.

⁷⁷ Interpol. “Global Cybercrime Programme” <https://www.interpol.int/>, 2024.

⁷⁸ Smith, J. “Global Cybercrime Trends” Journal of Cybersecurity, 2023.

⁷⁹ А.Анорбоев, Р.Хурсанов. Кибержиноятлар хавфини баргараф этиш йўллари. Илмий мақола. ОДИЛ СУДЛОВ. Ҳуқуқий, илмий-амалий нашр. 5/2020. 25-27 бетлар. https://sud.uz/wp-content/uploads/2021/odilsudlov/5_uz.pdf.

ахборот хавфсизлигига тобора таҳдиди ошиб бораётган интернет тармоқларидан фойдаланиб содир этилган жиноятларнинг тезкор тактик ва криминалистик жиҳатларини чуқур ўрганиш ҳамда таҳлил қилиш орқали, уларнинг содир этилиш усули ва воситаларига эътибор қаратган ҳолда тегишли куч ва воситалардан самарали фойдаланиш бўйича аниқ чора тадбирларни белгилаб олиш ва шу орқали содир этилган жиноятларни қисқа фурсатларда фош этиш юзасидан зарур таклиф ва тавсияларни ишлаб чиқиш бугунги ҳаётимизнинг долзарб масалаларига айланиб бормоқда.

Ўзбекистон Республикаси Президенти Шавкат Мирзиёев Шанхай ҳамкорлик ташкилотига аъзо давлатлар раҳбарлари кенгашининг мажлисида таъкидлаганидек, “кўп жиҳатдан аллақачон замонавий ҳаётни белгилаётган хавфсиз ахборот-коммуникация технологияларини ривожлантириш масалаларига ҳам эътибор қаратишни истар эдим.

Фақат кучларни бирлаштириш орқали, бир пайтнинг ўзида, ахборот маконидаги таҳдидларни камайтира борган тақдирдагина биз рақамлаштириш афзалликларидан тўла фойдалана олишимиз мумкин.

Кибержиноятчиликка қарши курашиш учун кўшма платформани яратиш вазифаси тобора долзарб бўлиб бормоқда⁸⁰.

Бугунги кунда мамлакатимизда интернетдан фойдаланувчилар сони 31 миллиондан ошиб бормоқда ва интернет тармоғига кирувчиларнинг аксарият қисми асосан мобил телефонлар орқали киришмоқда. Интернет тармоғидан фойдаланувчилар сонининг ортиши ва хизмат турлари кўпайиб бориши билан бирга кундалик ҳаётимизда кибержиноятчилик билан боғлиқ жиноятларни сони ҳам ортиб бормоқда. Ҳозирда республикамизда кибержиноятчиликнинг қуйидаги турлари нисбатан кўп содир этилаётганлиги маълум Жумладан:

- интернет фойдаланувчиларнинг шахсий (махфий) маълумотларини эгаллаш ва уларни ошкор қилиш билан қўрқитиб товламачилик қилиши (кибертовламачилик);

- фирибгарлар фойдаланувчилар телефониغا хар-хил танлов ғолиби бўлганлиги ҳақидаги хабарни юбориб, уларнинг банк карталари билан боғлиқ бир марталик юборилган SMS-кодни, тижорат банклари, тўлов тизими операторлари ва тўлов ташкилотларининг мобил иловаларига кириш ҳуқуқини берувчи логин ва паролларни эгаллаб, пластик картасидага маблағларни ўзлаштириши;

⁸⁰ Ўзбекистон Республикаси Президенти Шавкат Мирзиёевнинг Шанхай ҳамкорлик ташкилотига аъзо давлатлар раҳбарлари кенгашининг мажлисидаги нутқи. // <https://president.uz/uz/lists/view/5542> (16.09.2022 й.)

- Охирги вақтларда авж олаётган фирибгарлик турларидан яна бири – Telegram гуруҳларга одам қўшиш орқали қанчадир маблағ билан тақдирланишдир. Ушбу ҳолатда ҳам фирибгарлар телефон рақам ва пластик карта маълумотларини билиб олиб, ҳисобдан пул ечиб олиши;

- ижтимоий тармоқда зўрлик ишлатиш билан қўрқитиши, ҳақорат, суицид ҳолатлари (кибербуллинг) ва бошқалар .

Юқорида келтирилган фирибгарликларни олдини олиш ва уларга қарши курашиш мақсадида мамлакатимизда олиб борилаётган рақамли иқтисодиётга оид ислоҳотларнинг самарадорлигини ошириш ҳамда фуқароларимизнинг ахборот технологиялари соҳасидаги билимлари даражасини оширилиши муҳимдир. Бу борада ишларимизни янада жадаллаштиришимиз халқимизнинг ахборот технологияларига нисбатан ишончи ҳамда онгининг ортиб боришига хизмат қилади. Мамлакатимизда амалга оширилаётган суд-ҳуқуқ тизимидаги ислоҳотлардан кўзланган асосий мақсад ҳам жамиятда тинчлик ва осойишталикни сақлаш, жамоат тартиби ҳамда хавфсизлигини таъминлаш, фуқароларнинг ҳуқуқ, эркинликларини ҳар қандай кўринишдаги тажовузлардан ҳимоя қилишдир.

Ахборот технологияларидан фойдаланиб содир этилаётган фирибгарлик жиноятларига қарши курашиш самарадорлигини оширишга мақсадида, банк пластик карталари ва интернет хизматлари орқали содир этилган ҳар бир пул ўғирлаш ва фирибгарлик ҳолатлари бўйича олиб борилаётган дастлабки суриштирув ҳаракатлари юзасидан тез фурсатда қонуний қарор қабул қилинишини таъминлаш мақсадида, Ички ишлар вазирлиги билан Марказий Банк, процессинг марказлари (uzcard, humo), интернет тўлов тизими иловалари (payme, paynet, klik, apelsin, ва ҳ.к) марказлари билан самарали ҳамкорлик механизмларини йўлга қўйиш мақсадга мувофиқ бўлади.

Бундан ташқари банк пластик карталаридан фирибгарлик орқали пул маблағларини талон-тарож қилинишининг олдини олиш мақсадида мижозлар томонидан ўзларига тегишли бўлган банк пластик карталарини турли иловаларга улаш ва фаоллаштиришда “Face-ID” тизимидан фойдаланишни киритиш билан ахборот технологияларидан фойдаланиб содир этилаётган турли фирибгарликлардан фуқароларимизни ҳимоялаган бўламиз.

Бугунги кунда ахборот технологиялари орқали содир этилган ҳуқуқбузарлик ҳолатлари юзасидан келиб тушган ҳар бир мурожаатларни текширув натижаси бўйича унинг қонунийлиги ва жазо муқаррарлигини таъминлаш мақсадида, Ўзбекистон Республикаси ИИВ тизимида Республика миқёсида ушбу турдаги жиноятларни содир этиб келаётган ҳамда жиноятларни содир этишга мойил шахсларни рўйхатининг ягона базасини

шакллантириш ва бу борада маълумотлар алмашинуви билан боғлиқ тезкор ишларни амалга оширилиши муҳим вазифалардан бир бўлиб қолмоқда.

Ахборот технологиялари орқали содир этиладиган ҳуқуқбузарликларга қарши курашиш ваколатига эга давлат органлари, жумладан, Ички ишлар органлари ходимларининг кибержиноятчиликка қарши кураш ва ахборот технологияларидан фойдаланиб содир этилган фирибгарликлар бўйича билим ва кўникмаларини мунтазам равишда такомиллаштириб бориш юзасидан чора тадбирларни белгилаб олиниши зарур.

Хулоса қилиб айтганда, ахборот технологияларидан фойдаланиб содир этилган фирибгарлик жиноятларини аниқлаш, олдини олиш, қарши курашиш ва уни бартараф этиш бўйича зарур қарорлар қабул қилиш, кибержиноятчиликка қарши курашиш бўйича норматив-ҳуқуқий ҳужжатлар лойиҳаларини ишлаб чиқишда иштирок этиш, давлат органлари ва халқ манфаатларига таҳдид солувчи киберхатарларни аниқлаш ва уларга қарши курашиш, фуқароларнинг ҳуқуқ ва эркинликларига таҳдид солувчи кибержиноятларнинг содир этилишига имкон яратувчи сабабларни бартараф этиш каби муҳим вазифаларни бажариш ҳам бугунги куннинг долзарб масалаларидан бири эканлигини унутмаслик лозим. Бинобарин, мамлакатимиздаги ҳар бир фуқаронинг хавфсизлигини таъминлаш энг муҳим масалалардан бири ҳисобланади.

AXBOROT TEXNOLOGIYALARI SOHASIDAGI JINOYATLARNI OLDINI OLIH MUAMMOLARI VA YECHIM YO'LLARI

Otayev O'tkirbek Matyoqubovich

*IIV Malaka oshirish institute Kasbiy tayyorgarlik fakulteti Maxsus fanlar
sikli katta o'qituvchisi*

Annotatsiya. Zamonaviy dunyoda inson faoliyatining barcha sohalarida raqamlashtirish jarayonlari tez rivojlanib bormoqda. Axborot texnologiyalari inson turmushida muhim o'rin tutadi, shu bilan birga, yangi xavf-xatarlarni ham keltirib chikaradi. Ushbu maqolada axborot texnologiyalari sohasidagi jinoyatlarni oldini olish choralari, ularning turi va tuzilishi, shuningdek, davlat va jamiyat tomonidan ko'rilayotgan vazifalar tahlil etiladi.

Tayanch so'zlar: Jinoyat kodeksi, Axborot texnologiyalari, Xakerlik, Fishing, Elektron shantaj, Dennoma hujumlari DDoS.

Axborot xavfsizligining muhimligi bugungi kunda faqat korxonalar va tashkilotlar uchun emas, balki davlatlar va butun jamiyat uchun ham dolzarb

masala hisoblanadi. Xakerlik, shug'ullantirish, shaxsiy ma'lumotlarni yagonalashtirish va boshqa nomaqbul harakatlar keng tarqalganligi sababli, ularga qarshi chora-tadbirlarni ijobiy ravishda amaliyotga kiritish lozim.

Axborot texnologiyalari sohasida jinoyatlarning turlari va oqibatlari

Jinoyatlarning axborot texnologiyalari sohasida namoyon bo'lishi yangi va uzoq muddatli muammolarni keltirib chiqaradi. Bu jinoyatlardan asosiylari:

Xakerlik — tizimlarga ruxsatsiz kirish. Bu dastlabki etapda texnik huquq buzilishi sifatida ko'rilsa, keyinchida uni jinoyat hisoblashga asos tug'diradi. Masalan, bank tizimlariga xakerlar tomonidan hujum o'tkizilishi orqali millionlab pullar o'g'irlangan hodisalari bor.

Fishing — foydalanuvchilarning parollari, pasport ma'lumotlari yoki bank kartasi raqamlarini olish uchun elektron pochta yoki saytlarda qiymatli ma'lumotlarni so'rash orqali o'tkaziladi.

Dennoma hujumlari DDoS — serverlarga hujum qilib, ularni ishlash qobiliyatini yo'q qilish. Bu hujumlar orqali saytlar mustahkam bloklanadi va biznesga jiddiy zarar yetkaziladi.

Elektron shantaj — ma'lumotlarni shifrlash yoki o'g'irlash orqali foydalanuvchining kompyuteri yoki tizimida ishtirok ettirish. Shu bilan birga, terroristik tashkilotlar internetni o'z maqsadlari uchun ishlatishi keng tarqalgan.

Oqibatlar:

Shaxsiy ma'lumotlarning o'g'irlanishi;

Korxonalariga milliardlab zaar yetkazilishi;

Davlat tizimlarining xarajati;

Ijtimoiy ishonchning kamayishi.

Jinoyatlarni oldini olish chora-tabirlari

Jinoyatlarni oldini olish uchun tegishli texnik, huquqiy va tashkiliy chora-tadbirlarni ko'rish lozim.

Texnik chora-tadbirlar

Antivirus dasturlarini o'rnatish;

Faylvollardan foydalanish;

Shaxsiy ma'lumotlarni shifrlash;

Huquqiy chora-tadbirlar

Axborot xavfsizligi sohasidagi qonunlarni takomillash;

Elektron jinoyatlar uchun jiddiy jarimalar belgilash;

Xalqaro huquqiy hamkorlikni mustahkamlash (masalan, Budapesht konvensiyasi).

Tashkiliy chora-tadbirlar

Axborot xavfsizligi bo'yicha xodimlarni o'qitish;

Yeyekshiruvlar o'tkazish;

Davlatning roli va vazifalari

Uzbekiston Respublikasida axborot xavfsizligini ta'minlash bo'yicha hozirda samarador chora-tadbirlar amalga oshirilmoqda. Masalan, «Axborot xavfsizligi to'g'risida»gi Qonun hamda boshqa normativ-huquqiy aktlar yaratildi.

Xoziirda vazifasi fakat huquqiy bankani yartishga emas, balki nabora texnologiy sohasida ta'lim berish, kadrgy i tayyorlash xamjir

Axborot texnologiyalari (AT) sohasida kiber jinoyatlarga qarshi chora-tadbirlarning amaliyotga tushurilishi muhim ijobiy natijalar beradi. Bu natijalar davlat, korxonona va shaxsiy foydalanuvchilar uchun ahamiyat keltiradi. Kuyida xorijiy tajriba va umumiy ko'zga ko'rinadigan natijalar keltirilgan.

Jinoyat sonining kamayishi

Kuchaytirilgan kiber xavfsizlik chora-tadbirlari,

faol monitoring tizimlari,

shifrlash vositalari,

regulyar testlashlar (pentest) kiber jinoyatlar sonining kamayishiga olib keldi. Masalan, Yaponiyada kiber xavfsizlik strategiyasining amaliyotga kiritilishidan so'ng, 2015–2020 yillar davomida ma'lumot o'g'irlanishi 38% kamaygan.

Ma'lumotlarning ishonchli saqlash, yomon dasturlar (viruslar) tomonidan buzilishi, minimal darajaga etkazilmoqda. Bank muassasalari, kapital bozorlari, tashabbuslikorxonalar va shaxsiy foydalanuvchilar uchun ahamiyatli imkoniyatdir.

Iqtisodiy zararining kamayishi, Kiber jinoyatlar tufayli iqtisodiy yuqori zararlar etishi mumkin. Korxonalarining dasturlar tizimi ishtirok etadi. Foydalanuvchi ma'lumotlari saqlanib qoladi. Xalq orasida elektron xizmatlarga ishonch oship bormoqda. Foydalanuvilarning ongida o'zgarish, oldini olish chora-tadbirlari texnika yaxshilanishni emas, balki foydalanuvi ongidagi o'zgarishni keltiradi.

Parol xavfsizligini saqlash, Soksta veb-saytov aniklash, kabi ko'nikmalar keng tarqalmoqda.

Xalqaro hamkorlikning kuchaishi, kiber jinoyatlarning xalqaro tabiati taqiqlanmagan bo'lsa, xalqaro tashkilotlar bilan hamkorlik muhimi. Bu jarayon natijasida, xalqaro hamkorlikning kuchaishi, kiber jinoyatlarning xalqaro tabiati taqiqlanmagan bo'lsa, xalqaro tashkilotlar bilan hamkorlik muhimi. Bu jarayon natijasida:, Interpol, Yevropol, BMT. jinoyatchini aniklash va uni sudga tortish mumkin bo'ldi. Masalan, Avstraliya va Yaponiya, kiber-xavfsizlika javobgarlikka tartish mustahkamlangan.

Kadrlarni tayyorlashda o'zgarish, kiber xavfsizlik sohasida mutaxassislar sonining oshishi — yana bir muhim natija. Uni ta'minlash uchun: Yuqori ta'lim

muassasalarida kiber-xavfsizlik buyicha davlat tashkilotlarida maxsus kurslar yaratish.

Axborot texnologii sohasidagi jinoyatlar bugungi kunda ijtimoiy, iqtisodiy va politike sohalarida jiddiy xavf-xatar hisoblanadi. Ularga qarshi kurashish uchit kompleks yondashuv, zamonaviy texniki, mustahkam huquqiy baza va jamiyatning faol ishtiroki kerak.

Adabiyotlar ro'yxati:

1. O'zbekiston Respublikasi Prezidentining «Axborot xavfsizligi to'g'risida»gi Farmoni, 2020 y.
2. Bektemirov M.A. Axborot xavfsizligi asoslari . Toshkent, 2021y.
3. ISO/IEC 27001:2013 – Axborot xavfsizligi upravleniya sistemami.
4. Xudaybergenov A.S. Kompyuter rabotayet kak kurashish vositalari . Toshkent, 2019y.
5. Yevropa kelishuv-bitimlari. Budapeshtskaya konvensiyasi (Konvensiya o kiberprestupnosti), 2001 y.

AXBOROT TEXNOLOGIYALARIDAN FOYDALANGAN HOLDA SODIR ETILADIGAN JINOYATLAR UCHUN JAVOBGARLIK MASALALARI

Ganiev Shaxobitdin Xolmatovich

IIV Malaka oshirish instituti Yuridik fanlar kafedrasi katta o'qituvchisi

Annotatsiya. Ushbu maqolada axborot texnologiyalaridan foydalangan holda sodir etiladigan jinoyatlar tushunchasi, turlari va javobgarlik masalalari bilan bir qatorda ushbu turdagi jinoyatlar uchun javobgarlikda mavjud muammolar va ularning echimlari hamda samarali jihatlariga e'tibor qaratilgan.

Kalit so'zlar: Axborot texnologiyalari, jinoyat, kiberjinoyatchilik, kiberxavfsizlik, tovlamachilik, firibgarlik, o'g'irlik, jinoyatchilik statistikasi.

Bugungi kunda dunyoda axborot tizimi va axborot texnologiyalari rivojlanib borayotgani sari axborot texnologiyalari sohasidagi jinoyatlar, shuningdek, axborot tizimidan, shu jumladan axborot texnologiyalaridan foydalanib sodir etilayotgan jinoyatlar sodir etilishi ham sezilarli darajada oshib bormoqda. Buning oqibatida respublika miqyosida sodir etilayotgan jinoyatlar salmog'ini oshishiga ham o'zining jiddiy ta'sirini ko'rsatmoqda. Bu holat esa, jamiyat hayotining bir nechta sohalariga bir vaqtning o'zida kirib boradigan jiddiy tahdidlar mavjudligi haqida xulosa qilish imkonini beradi. Sababi, oxirgi yillar ichida ushbu turdagi jinoyatlar natijasida juda ko'plab insonlar moddiy va ma'naviy zarar ko'rdilar.

Shuning uchun ham bu borada Prezidentimiz Sh.M.Mirziyoyev tomonidan 2025-yil 30-aprel kuni "Axborot texnologiyalari yordamida sodir etiladigan

jinoyatlarga qarshi kurashish faoliyatini yanada kuchaytirishga qaratilgan chora-tadbirlar to'g'risida"gi PQ-153-son qarori qabul qilindi.

Ushbu qarorni qabul qilishdan maqsad kiberjinoyatlarning barvaqt oldini olish hamda ularni fosh etish samaradorligini oshirish bo'yicha amaldagi qonunchilik hujjatlarini takomillashtirish va qator tashkiliy-texnik choralarni ko'rish belgilandi.

Jumladan, kiberjinoyatlarga qarshi kurashish yo'nalishida yagona ishlash amaliyotini yo'lga qo'yishni nazarda tutuvchi alohida qonun loyihasini ishlab chiqish hamda yuridik shaxslar tomonidan kiberxavfsizlik talablariga rioya etmaganlik uchun, shuningdek, axborot texnologiyalari sohasidagi barcha jinoyatlar yuzasidan javobgarlikni kuchaytirish bo'yicha qonunchilikka o'zgartirishlar kiritish topshirildi.

Shuningdek, qaror bilan shaxslarning bank kartalaridagi pullari talon-toroj qilinishini to'xtatish maqsadida banklar, to'lov tizimi operatorlari va to'lov tashkilotlariga zamonaviy antifrod va antivirus himoya tizimlarini joriy etish hamda firibgarlar tomonidan soxta raqamlar orqali fuqarolarga qo'ng'iroq qilishlarini texnik (imkonsiz qilish) cheklash kabi choralar belgilandi.

2025-yildan boshlab, har yili bir oy davomida "Kibermadaniyatni yuksaltirish oyligi" kompleks targ'ibot oyligini o'tkazish hamda tashviqot ishlari sohaga oid barcha davlat va nodavlat tashkilotlari tomonidan faol tarzda olib borish orqali aholining raqamli immuniteti va ogohligini oshirishning doimiy tizimi yo'lga qo'yiladi.

Mazkur qarorda ko'rsatilgan vazifalarning amalga oshirilishi mas'ul davlat organlari, tashkilotlar, banklar, to'lov tizimi operatorlari va to'lov tashkilotlarining fuqarolarning kiberjinoyatlardan jabrlanib qolishining oldini olish hamda ularning moliyaviy xavfsizligini mustahkamlash bo'yicha mas'uliyatini oshishiga xizmat qiladi.

Amaldagi O'zbekiston Respublikasi Jinoyat kodeksining XX¹-bobi "Axborot texnologiyalari sohasidagi jinoyatlar" deb nomlangan bo'lib, 278¹-modda. Axborotlashtirish qoidalarini buzish, 278²-modda. Kompyuter axborotidan qonunga xilof ravishda (ruxsatsiz) foydalanish, 278³-modda. Kompyuter tizimidan, shuningdek telekommunikatsiya tarmoqlaridan qonunga xilof ravishda (ruxsatsiz) foydalanish uchun maxsus vositalarni o'tkazish maqsadini ko'zlab tayyorlash yoxud o'tkazish va tarqatish, 278⁴-modda. Kompyuter axborotini modifikatsiyalashtirish, 278⁵-modda Kompyuter sabotaji, 278⁶-modda Zarar keltiruvchi dasturlarni yaratish, ishlatish yoki tarqatish, 278⁷-modda Telekommunikatsiya tarmog'idan qonunga xilof ravishda (ruxsatsiz) foydalanish, 278⁸-modda. Kripto-aktivlar aylanmasi sohasidagi qonunchilikni buzish, 278⁹-modda. Mayning faoliyatini qonunga xilof ravishda amalga oshirish

kabi jinoyatlarini o'z ichiga qamrab oladi. Mazkur jinoyatlar aynan axborot texnologiyalari sohasida sodir etiladigan jinoyat turlari hisoblanadi.

Bundan tashqari, Jinoyat kodeksida axborot texnologiyalaridan foydalangan holda sodir etiladigan jinoyat turlari ham mavjud bo'lib, unga ko'ra qaysi turdagi jinoyat axborot texnologiyalaridan foydalangan holda sodir etilsa, o'sha jinoyatning moddasida og'irlashtiruvchi holat sifatida belgilab qo'yilgan. Bunga misol qilib, Jinoyat kodeksining X-bobi "O'zgalar mulkini talon-toroj qilish" jinoyatlarining bir turi sifatida 168-modda. Firibgarlik hisoblanib, agarda ushbu jinoyat axborot texnologiyalaridan foydalangan holda sodir etiladigan bo'lsa, u holda 168-modda 3-qismi "g" bandi axborot tizimidan, shu jumladan axborot texnologiyalaridan foydalanib sodir etilgan bo'lsa, bilan malakalanib, bazaviy hisoblash miqdorining uch yuz baravaridan to'rt yuz baravarigacha miqdorda jarima yoki ikki yildan uch yilgacha axloq tuzatish ishlari yoxud muayyan huquqdan mahrum etilgan holda besh yildan sakkiz yilgacha ozodlikdan mahrum qilish bilan jazolanishi belgilangan.

Shuningdek, bunday qoida 169-modda. O'g'irlik jinoyatida ham belgilab qo'yilgan bo'lib, qonunga xilof ravishda (ruxsatsiz) axborot tizimiga kirib yoki undan foydalanib sodir etiladigan bo'lsa, og'irlashtiruvchi holat sifatida 169-modda 3-qismi "b" bandi bilan malakalanib, besh yildan sakkiz yilgacha ozodlikdan mahrum qilish bilan jazolanishi belgilangan.

O'zgalar mulkini talon-toroj qilish jinoyatining yana bir turi 165-modda. Tovlamachilik, ya'ni jabrlanuvchiga yoki uning yaqin kishilariga zo'rlik ishlatish, mulkiga shikast yetkazish yoki uni nobud qilish yoxud jabrlanuvchining axborot resursini yo'q qilish, o'zgartirish, egallab olish yoki to'sib qo'yish yoki jabrlanuvchi uchun sir saqlanishi lozim bo'lgan ma'lumotlarni oshkor qilish, uni sharmanda qiladigan uydirmalar tarqatish bilan qo'rqitib o'zgan mulkni yoki mulkiy huquqni topshirishni, mulkiy manfaatlar berishni yoxud mulkiy yo'sindagi harakatlar sodir etishni talab qilish yoxud jabrlanuvchini o'zining mulkini yoki mulkka bo'lgan huquqini berishga majbur qiladigan sharoitga solib qo'yish jinoyati hisoblanadi.

Bugungi kunda ushbu jinoyatni sodir etilishi hanuzga qadar davom etib kelmoqda, eng achinarlisi ushbu jinoyat ham axborot tizimidan, shu jumladan axborot texnologiyalaridan foydalanib sodir etilib kelinayotganligi holatlari ko'p uchrab turibdi. Biroq, 165-moddada 168 va 169-moddalarning 3-qismidagi og'irlashtiruvchi holat sifatida alohida band bilan kiritilmagan. Bu bilan an'anaviy tarzda sodir etilgan tovlamachilik uchun va axborot tizimidan, shu jumladan axborot texnologiyalaridan foydalanib sodir etilgan tovlamachilik uchun ham 165-modda 1-qismi bilan javobgarlikka tortilishi belgilab qo'yilgan.

Fikrimizcha, aynan shuning uchun ham tovlamachilik jinoyatini axborot tizimidan, shu jumladan axborot texnologiyalaridan foydalanib sodir etilishi holatlari tez-tez uchrab turibdi. Chunki, hozirgi kunda ushbu jinoyatni sodir etmoqchi bo‘layotgan shaxslar ham oldindan biladiki, agar tovlamachilik jinoyatini axborot texnologiyalaridan foydalanib sodir etadigan bo‘lsa, birinchidan jinoyat qonunchiligida bu borada huquqiy ta'sir chorasi og‘irlashtirilmagan, ikkinchidan uning xavfsizligi ta'minlanadi, uchinchidan huquqni muhofaza qiluvchi organ xodimlariga uning shaxsini aniqlash uchun qiyinchiliklar mavjud bo‘ladi, sababi mazkur jinoyatni “Telegram”, “Instagram” yoki “Facebook” intimoiy tarmoqlari orqali yopiq turdagi profilidan foydalanib sodir etadigan bo‘lsa, ushbu saytlar O‘zbekiston Respublikasining yurisdiksiyasidan ro‘yxatdan o‘tmaganligi uchun yopiq profil egasi haqida ma'lumot olishning imkoni bo‘lmaydi.

Hozirgi kunda jinoyat qonunchiligida ushbu kamchilikning mavjudligi bois, tovlamachilik jinoyatini axborot tizimidan, shu jumladan axborot texnologiyalaridan foydalanib sodir etish holatlari ko‘payib borayotgani ushbu jinoyatning salmog‘ini oshishiga sabab bo‘lmoqda.

Shu sababli, tovlamachilik jinoyatiga o‘zgartirish va qo‘shimcha kiritib, axborot tizimidan, shu jumladan axborot texnologiyalaridan foydalanib sodir etiladigan bo‘lsa, uni 2-qismiga alohida band tariqasida og‘irlashtiruvchi holat sifatida belgilanishi maqsadga muvofiqdir.

Xulosa sifatida qayd etish lozimki, axborot texnologiyalaridan foydalangan holda sodir etiladigan jinoyatlarni barvaqt oldini olish maqsadida, yuqorida keltirilgan muammolarni bartaraf etish uchun bu bo‘yicha jinoyat qonunchiligiga o‘zgartirish va qo‘shimchalar kiritish hamda samarali amaliyotni tatbiq etish orqali, yoki javobgarlikni kuchaytirish yo‘li bilan erishish mumkin.

Foydalanilgan adabiyotlar:

1. O‘zbekiston Respublikasi Jinoyat kodeksi – T.: 2025.
2. O‘zbekiston Respublikasi Jinoyat-protsessual kodeksi – T.: 2025.
3. O‘zbekiston Respublikasining 2022-yil 15-apreldagi “Kiberxavfsilik to‘g‘risida”gi O‘RQ-764-son qonuni.
4. O‘zbekiston Respublikasi Prezidentining 2022-yil 22-yanvardagi “2022-2026 yillarga mo‘ljallangan Yangi O‘zbekistonning taraqqiyot strategiyasi to‘g‘risida”gi PF-60-son farmoni.
5. O‘zbekiston Respublikasi Prezidentining 2025-yil 30-apreldagi “Axborot texnologiyalari yordamida sodir etiladigan jinoyatlarga qarshi kurashish faoliyatini yanada kuchaytirishga qaratilgan chora-tadbirlar to‘g‘risida”gi PQ-153-son qarori.

INTERNET XURUJLARIDAN VOYAGA YETMAGANLARNI ASRASH DOLZARB VAZIFA

Xushvaqtov Erkin Temirovich

IIV MOI Maxsus-kasbiy fanlar kafedrası katta o'qituvchisi

Hozirgi dunyoda fan va texnika taraqqiyoti yutuqlari ijtimoiy hayotning barcha hodisalariga o'z ta'sirini ko'rsatmoqda. Jinoyatchilik ham bundan mustasno emas. Axborot-texnologiyalari shu jumladan, Internet tarmog'iga kriminal tahdidlarning kirishi davrimizning eng xavfli jarayonlaridan biridir. Hozirda Internet tarmog'idagi jinoyatchilikni tushunish, unga baho berish va unga qarshi kurashish muammolarining dolzarbligini barcha olimlar tomonidan alohida e'tirof etilmoqda. Mamlakatimizda zamonaviy axborot-kommunikatsiya texnologiyalarini jamiyatning turli jabhalariga joriy etish borasida keng ko'lamli ishlar amalga oshirilmoqda.

Ko'rsatilayotgan xizmatlar turi kengayib, sifat jihatidan yangi bosqichga ko'tarilishi natijasida yurtimizda internet tarmog'idan foydalanuvchilar soni tobora oshib bormoqda. Bugungi kunda O'zbekistonda Internet xizmatidan foydalanuvchilar soni 31 mlndan oshganligi, shundan mobil Internet foydalanuvchilari soni 29,5 mlanni tashkil etayotganligini ta'kidlash lozim. Buning natijasida mamlakatimizda aholi, ayniqsa, voyaga yetmaganlar axborot resurslardan, jumladan, internet tarmog'idan foydalanish imkoniyati kengaymoqda.

Axborot xavfsizligini ta'minlashga qaratilgan eng muhim vazifalar haqida so'z borar ekan, bunda voyaga yetmaganlarni axborot olish madaniyatini shakllantirish, ularni g'oyaviy-mafkuraviy tajovuzlardan himoyalash mexanizmlarini takomillashtirish davr talabi ekanligini bilish lozim. Xususan, voyaga yetmaganlar internet tarmog'idan foydalanganda madaniyat va axloq me'yorlariga rioya qilishni, mafkuraviy immunitetni kuchaytirish, xususan, internet tarmog'iga axborotni joylashtirish, tarqatish, izlash, foydalanish kabi xususiyatlarni o'z ichiga olgan axborot xavfsizligi va internet madaniyatini mukammal o'zlashtirishlarini hamda bu boradagi tegishli huquqiy va tashkiliy tavsiyalarni yanada takomillashtirish zarur.

Bir so'z bilan aytganda, dunyoda kechayotgan murakkab jarayonlar barchamizdan voyaga yetmaganlar tarbiyasiga yanada e'tiborliroq bo'lishni taqozo etmoqda. Bu jarayonda esa nafaqat davlat tashkilotlari yoki ta'lim muassasalari, balki fuqarolik jamiyati institutlari ishtirok etishlari bugungi kun talabidir. INTERNET [lot. inter – aro va net (work) – tarmoq] – katta (global) va kichik (lokal) kompyuter tarmoqlarini o'zaro bog'lovchi butunjahon kompyuter tizimi.

Unda geografik o‘rni, zamon va makondan qat’i nazar, ayrim kompyuter va mayda tarmoqlar o‘zaro hamkorlikda global informatsiya infratuzilmasini tashkil etadi. Qaydnomalar tizimi bilan boshqariladigan barcha hosila tarmoqlar hamkorlikda iste’molchilarga informatsiyani saqlash, e’lon qilish, jo‘natish, qabul qilish, izlash va ma’lum bo‘lgan barcha variantlar (matn, tovush, videotasvir, fotosurat, grafika, musiqa tarzida va boshqa ko‘rinishlar) da informatsiya almashinishga imkon yaratadi.

Internet barcha an’anaviy informatsiya tizimlari – telekommunikatsiya, teleradioeshittirish, informatsiyalarni xalqaro miqyosda faol almashtirish va boshqaning texnologik imkoniyatlarni uyg‘unlashtirib qo‘llanganligi uchun u bir necha vazifani – informatsiya va bilimlar manbai; ommaviy axborot vositasi, insoniyat faoliyatining barcha sohalari (shu jumladan, ta’lim-tarbiya, siyosiy, ijtimoiy, iqtisodiy, madaniy, sayyohlik va boshqalar)ga taalluqli informatsiya xizmatlari tizimi; istiqbolli bozor va milliy kompaniyalarning xalqaro informatsiya maydoni va jahon bozoriga eng tejamli va tezkor usulda qo‘shilish imkonini beradigan vosita vazifasini o‘taydi.

Hech hisoblab ko‘rganmisiz, kun davomida necha bor internet tarmog‘iga kirasiz? Ko‘pchilik uyqudan uyg‘oniboq, telefonini qo‘lga olib, ijtimoiy tarmoqlarga ko‘z tashlaydi, tunda uyquga ketish oldidan global tarmoqda yana “sayr” qilmasdan ko‘zini yummaydi. Shunday emasmi? Yangiliklardan, voqea-hodisalardan boxabar bo‘lar ekanmiz, darhol uni tanishlarga jo‘natamiz.

Yangi O‘zbekistonimizning buyuk kelajagi bugungi yosh avlodaziz farzandlarimizning ma’naviy qiyofasiga, ularning jismoniy kamoloti va axloqiy pokligining darajasiga ham bevosita, ham bilvosita bog‘liqdir. Shu bois voyaga yetmaganlar tarbiyasi masalasi respublikamiz istiqlolining dastlabki kunlaridanoq davlat siyosatining eng ustuvor yo‘nalishi sifatida belgilanadi. Voyaga yetmaganlarni internet xurujlaridan asrash uchun nafaqat davlat organlari, balki nodavlat tashkilotlar, uyushmalar, jamiyat va birlashmalar va boshqalarning o‘zaro zich hamkorligi, ularga ijtimoiy ko‘mak berishning turli usullarini qo‘llash, profilaktik ishlarni va boshqalarni amalga oshirish kerak. Shuningdek, yosh avlod tarbiyasiga ham g‘oyat katta e’tiborimizni qaratishimiz lozim.

Umuman jinoyatchilik, shu jumladan, voyaga yetmaganlar tomonidan sodir etiladigan jinoyatchilik o‘zgaruvchan hodisa va ko‘pgina omillarga bog‘liq. Shuning uchun hozirgi kunda davlatimizning barcha sohalarida bo‘layotgan o‘zgarishlar voyaga yetmaganlar o‘rtasidagi jinoyatchilikning holati, strukturasi va xarakteriga jiddiy ta’sir ko‘rsatadi. Qayd etilganlar hamda boshqa omillar voyaga yetmaganlar xulq-atvorining buzilishi va ko‘pincha ular tomonidan turli jinoyatlar sodir etilishiga olib keladi. Statistik ma’lumotlar va kriminologik tadqiqotlarning ko‘rsatishicha, voyaga yetmaganlar va ular ishtirokida ichki ishlar organlarida

barcha xizmat yo‘nalishlarida ro‘yxatga olinadigan umumiy jinoyatlarning 10 foiziga yaqini, jinoyat-qidiruv yo‘nalishi bo‘yicha esa – 13 foizi sodir etiladi.

Ayol jinsidagi voyaga yetmaganlar o‘rtasidagi jinoyatlar soni erkak jinsidagi voyaga yetmaganlar jinoyatiga qaraganda, shahar joylarida yashaydiganlar o‘rtasida 18 foiz kam va bu qishloq joylarida yashaydiganlarga qaraganda ikki baravardan ortiqni tashkil etadi. Ayrim olimlar voyaga yetmaganlar jinoyatchiligining sabablari jumlasiga quyidagilarni kiritadi: yashash, o‘qish yoki ish joyidagi muhitning salbiy ta‘siri; o‘qishni tashlab ketgan o‘smirlar uzoq vaqt muayyan ish bilan shug‘ullanmasligi; o‘smirning noto‘g‘ri tarbiyalanishini belgilovchi shart-sharoit omillari; yoshi katta jinoyatchilarning dalolatchiligi; zo‘ravonlik va qonunsizlikni ifodalovchi kitoblar va filmlar ta‘siri.

Voyaga yetmaganlar tomonidan internetda sodir etiladigan quyidagi sabablarni keltirish mumkin: nazoratsizlik; umumiy ta‘lim maktablari va litseylarda ta‘lim-tarbiya ishlarida mavjud kamchiliklar; madaniy hordiq chiqarishni tashkil etishdagi kamchiliklar; voyaga yetmaganlar jinoyatchiligining oldini olish hamda unga qarshi bevosita kurash olib borish vazifalari zimmasiga yuklangan organlar faoliyatidagi kamchiliklar. Ayrimlar voyaga yetmaganlar jinoyatchiligining sabablari qatoriga quyidagilarni kiritadi: o‘smirning kayfiyati va ruhiyatiga ta‘sir ko‘rsatuvchi hayotdagi muvaffaqiyatsizliklar; ma‘naviy va axloqiy mo‘ljallarning beqarorligi; shaxslar jinoiy guruhi bilan yaqin aloqada bo‘lish yoki muayyan sharoitda ular o‘smirga salbiy ta‘sir ko‘rsatishi; ruhiyatining ayrim xususiyatlari; oila yoki jamoadagi noqulay shartsharoitlar.

Bundan tashqari, voyaga yetmaganlar tomonidan sodir etilayotgan turli xil jinoyatchilik, birinchi navbatda, o‘sha shaxsda huquqiy tarbiya va huquqiy madaniyatning yetishmasligi ham sababdir. Huquqiy ongi, tarbiyasi va huquqiy madaniyati yetuk bo‘lmagan voyaga yetmagan shaxs jamiyatda amalga oshirayotgan ayrim salbiy harakatlarni jinoyat ekanligini tushunmaydi. Masalan, voyaga yetmagan o‘smir mayda o‘g‘irlik huquqbuzarlik ekanligini, buning oqibatida javobgarlik masalasi borligini huquqiy ongi huquqiy madaniyati yetishmasligi va huquqiy tarbiyaga ega emasligi uchun bilmaydi.

Natijada ana shunday huquqbuzarliklar o‘rnini katta jinoyatlar egallaydi. Shuning uchun jamiyatimizda ro‘y berayotgan huquqiy o‘zgarishlar va huquqiy tarbiya bilan bog‘liq bo‘lgan masalalar yoshlarga o‘z vaqtida yetib borishi kerak. Ya‘ni, voyaga yetmaganlarni jinoyat sodir etgandan keyin emas, balki shaxsning jinoyat sodir etishining oldini olish maqsadida bu borada ko‘plab ma‘lumotga ega bo‘lishi lozim. Sir emaski, o‘smirlar bu boradagi jinoiy javobgarlik, jazo choralari to‘g‘risidagi ma‘lumotlarni faqat jinoyat sodir etganlaridan keyingina huquqni muhofaza qiluvchi organ xodimlaridan eshitib, tushunib olishadi.

Kriminologik olimlar voyaga yetmaganlar jinoyatchiligining sabablari sifatida quyidagi holatlarni ko'rsatib o'tadilar:

- * oiladagi va turmushdagi salbiy ta'sirlar;
- * nosog'lom turmush tarzi; * yomon xulqli shaxslar bilan aloqada bo'lish;
- * o'qimaydigan voyaga yetmaydiganlarning ozoq vaqt mobaynida muayyan foydali mashg'ulot bilan shug'ullanmaganligi;
- * o'smirning noto'g'ri qabul qilishga sabab bo'ladigan holatlarning voyaga yetmagan shaxsida juda qiyin kechishi;
- * katta yoshdagi jinoyatchilar tomonidan huquqbuzarliklarga va turli g'ayriijtimoiy xatti-harakatlarga jalb qilinishi.

Voyaga yetmaganlar tomonidan internetda sodir etiladigan jinoyatlarning sabablariga bolaning kayfiyati va ruhiy holatiga ta'sir qiladigan va muayyan iz qoldiradigan hayotdagi omadsizlik; axloqiy va etik e'tiqodlarining turg'un emasligi, jinoiy guruhlar bilan bevosita aloqada bo'lish yoki muayyan sharoitlarda bunday guruh a'zolarining bolaga ta'siri, ruhiy holatdagi ayrim sifatlar, ayrim harakatlarga nisbatan romantik qarashlar va shunday harakatlarning sodir etishga moyillikning kuchayishi kabilarni aytish mumkin. O'smirlar tomonidan sodir etiladigan internet xurujlaridan asrash huquqbuzishlarning sabablari oiladagi, turmushdagi, jamoadagi nosog'lom muhit kabilar bo'lishi mumkin. Lekin bunday holatlar bolaga huquqbuzishlarning sababi sifatida faqat muayyan sharoitlardagina ta'sir qilishi mumkin, ya'ni voyaga yetmaganlarning irodasi bo'sh yoxud o'z ijtimoiy-etik harakatlarini nazorat qilolmasligi mumkin.

Foydalangan adabiyotlar ro'yxati:

1. O'zbekiston Respublikasining Konstitutsiyasi // URL:<http://www.lex.uz>.
2. O'zbekiston Respublikasining "Huquqbuzarliklar profilaktikasi to'g'risida"gi qonuni // URL:<http://www.lex.uz>.
3. O'zbekiston Respublikasining Jinoyat kodeksi // URL:<http://www.lex.uz>.
4. Rossiya Federatsiyasi Jinoyat kodeksi https://www.consultant.ru/document/cons_doc_LAW_10699/.
5. X.B. *Abdreymov* Axborot texnologiyalari sohasidagi jinoyatlar va ulardan himoyalash usullari *IIV Akademiya Magistratura inglovchisi*.
6. A.K.Rasulev Axborot texnologiyalari va xavfsizligi sohasidagi jinoyatlarga qarshi kurashishning jinoyat-huquqiy va kriminologik choralarini takomillashtirish. Yurid. fanlar doktori dissertatsiyasining avtoreferati. T., IIV Akademiyasi, 2018. - B-5.

СОВУҚ ҚУРОЛЛАР ВА СОВУҚ ҚУРОЛ СИФАТИДА ФОЙДАЛАНИШ МУМКИН БЎЛГАН АШЁЛАРНИНГ ТАКТИК-ТЕХНИК ХУСУСИЯТЛАРИГА КЎРА ҲУҚУҚИЙ МАЛАКАЛАШНИНГ АЙРИМ МАСАЛАЛАРИ

Юлдашев Шухрат Нуралиевич

*ЎР ИИБ Эксперт-криминалистика бош маркази бошлигининг 1-ўринбосари
shuxrat0379gmail.com*

Жамоат хавфсизлигини таъминлаш ва жамоат тартибини сақлаш, жиноятларни олдини олиш ва унга қарши курашиш самарадорлигини ошириш, айниқса, вояга етмаган ва ёшлар ўртасида совуқ қурол ёки совуқ қурол сифатида фойдаланилиши мумкин бўлган ашёларни қўллаш натижасида содир этилиши мумкин бўлган ҳуқуқбузарликларга чек қўйиш мақсадида совуқ қурол ва совуқ қурол сифатида фойдаланилиши мумкин бўлган ашёларнинг муомаласи Ўзбекистон Республикасининг 2019 йил 29 июлдаги “Қурол тўғрисида”ги ЎРҚ-550-сон, 2020 йил 5 ноябрдаги “Жамоат хавфсизлигини таъминлашга доир қонун ҳужжатлари янада такомиллаштирилиши муносабати билан Ўзбекистон Республикасининг айрим қонун ҳужжатларига ўзгартириш ва қўшимчалар киритиш тўғрисида”ги ЎРҚ-645-сон ва 2022 йил 31 майдаги “Қурол тўғрисидаги қонунчилик такомиллаштирилиши муносабати билан Ўзбекистон Республикасининг айрим қонун ҳужжатларига ўзгартириш ва қўшимчалар киритиш ҳақида”ги ЎРҚ-772-сон Қонунларига мувофиқ тартибга солинган.

Хусусан, Ўзбекистон Республикасининг 2020 йил 5 ноябрдаги “Жамоат хавфсизлигини таъминлашга доир қонун ҳужжатлари янада такомиллаштирилиши муносабати билан Ўзбекистон Республикасининг айрим қонун ҳужжатларига ўзгартириш ва қўшимчалар киритиш тўғрисида”ги ЎРҚ-645-сон ва 2022 йил 31 майдаги “Қурол тўғрисидаги қонунчилик такомиллаштирилиши муносабати билан Ўзбекистон Республикасининг айрим қонун ҳужжатларига ўзгартириш ва қўшимчалар киритиш ҳақида”ги ЎРҚ-772-сон Қонунлари билан:

Ўзбекистон Республикасининг Маъмурий жавобгарлик тўғрисидаги Кодексига совуқ қурол ёки совуқ қурол сифатида фойдаланилиши мумкин бўлган ашёлар билан муомалада бўлиш қоидаларининг бузилиши учун алоҳида маъмурий жавобгарлик чоралари белгиланган.

Шу билан бирга, Ўзбекистон Республикаси Жиноят кодексининг 104 ва 105-моддаларида назарда тутилган жиноятларни қурол ёки совуқ қурол сифатида фойдаланилиши мумкин бўлган ашёларни ишлатиб содир этилганлик учун жавобгарлик кучайтирилганлиги, шунингдек тигли совуқ

қуролни, улоқтириш қуролини сақлаш, олиб юриш, ташиш қоидаларини бузганлик учун ушбу Кодекснинг 249-моддаси билан жиноий жавобгарлик ҳам белгиланган.

Таъкидлаш лозимки, фуқаролар қуйидаги ҳолларда жамоат жойларида совуқ қурол ва совуқ қурол сифатида фойдаланилиши мумкин бўлган ашёларни олиб юриш ва ташиш ҳуқуқига эга:

бевосита касбий фаолиятда, спорт фаолиятида ёки хўжалик-маиший мақсадларда фойдаланиш билан боғлиқ бўлган ҳолларда – ёпиқ ҳолда (ғилофда);

ов пичоқлари – овчи сифатида овчилик жамиятидан рўйхатдан ўтганлик тўғрисидаги ҳужжат мавжуд бўлганда (ов қилишда);

шахсий автотранспорт воситасида (шунингдек, мопед (скутер)да) – ёпиқ ҳолда (ғилофда) ва хавфсизлик чоралари таъминланган ҳолда (хайдовчидан бошқа шахсларнинг назари тушмайдиган ҳолда).

Шунингдек, спорт учун мўлжалланган тигли совуқ қурол ва улоқтириш қуролларини сақлаш, ташиш ва фойдаланиш фақат Ўзбекистон Республикаси Ёшлар сиёсати ва спорт вазирлиги томонидан белгиланган тартибда спорт иншоотлари ҳудудида ўтказилиши мумкин.

Жамоат тартибини ва жамоат хавфсизлигини таъминлаш, жиноятчиликка қарши курашиш, объектларни кўриқлаш бўйича хизмат вазибаларини бажарувчи махсус органлар ва ҳарбий тузилмалар ходимлари, шунингдек қуролларни ишлаб чиқариш, сотиш, йиғиш ва кўрсатиш билан шуғулланувчи юридик шахслар томонидан совуқ қуролларни сақлаш, ташиш, олиб юриш ва улардан фойдаланиш қонун ҳужжатларида белгиланган тартибда амалга оширилади.

Жисмоний шахслардан олинган ашёлар совуқ қурол ёки совуқ қурол сифатида фойдаланилиши мумкин бўлган ашёлар тоифасига кириш-кирмаслиги ички ишлар органлари эксперт-криминалистика бўлинмаларининг совуқ қурол суд экспертизаси ҳулосасига (маълумотномасига) асосан белгиланади.

ИИВнинг 2025 йил 6 февралдаги “Ички ишлар органларининг эксперт-криминалистика бўлинмаларида қуролни коллекциялаш ҳамда кўргазмага қўйиш тартиби тўғрисидаги низомни тасдиқлаш ҳақида”ги 64-сон буйруғи талабларига мувофиқ ички ишлар органлари эксперт-криминалистика бўлинмаларининг мурожаатига асосан совуқ қурол ва совуқ қурол сифатида фойдаланилиши мумкин бўлган ашёлар давлат суд-экспертиза муассасасининг коллекциясига қўшилади.

Шунингдек, совуқ қурол ҳамда совуқ қурол сифатида фойдаланилиши мумкин бўлган ашёларни ажратиш ҳамда ишлаб чиқариш соҳасида

Ўзбекистон стандартлаштириш, метрология ва сертификатлаштириш агентлигининг “Хорижий мамлакатларнинг миллий стандартини Ўзбекистон Республикасида қўллаш тўғрисида” 2020 йил 24 июлдаги 500-сон қарори қабул қилинган бўлиб, рўйхати қуйидаги келтирилган Россия Федерациясининг миллий стандартлари Ўзбекистон Республикаси ҳудудида 2020 йил 24 октябрдан бошлаб қўлланилиши белгиланган:

1. ГОСТ Р 51548-2000 “Ножи для выживания (Общие технические условия)”;
2. ГОСТ Р 51215-98 “Оружие холодное (Термины и определения)”;
3. ГОСТ Р 52737-2007 “Тесаки охотничьи, мачете туристические, разделочные, инструменты для восстановительных и спасательных работ (Общие технические требования и методы испытаний на безопасность)”;
4. ГОСТ Р 51715-2001 “Изделия декоративные и сувенирные, сходные по внешнему строению с холодным или метательным оружием (Общие технические требования)”;
5. ГОСТ Р 51644-2000 “Ножи разделочные и шкурорезные (Общие технические условия)”;
6. ГОСТ Р 51501-99 “Ножи туристические и специальные спортивные (Общие технические условия)”;
7. ГОСТ Р 51015-97 “Ножи хозяйственные и специальные (Общие технические условия)”;
8. ГОСТ Р 51500-99 “Ножи и кинжалы охотничьи (Общие технические условия”.

Шуни алоҳида таъкидлаш лозимки, Ўзбекистон Республикаси Маъмурий жавобгарлик тўғрисидаги Кодекснинг 185²-моддаси 1-қисмида шахс томонидан ушбу моддада кўрсатилган мақсадларда фойдаланиш билан боғлиқ ҳолда (мақсадли) совуқ қурол сифатида фойдаланилиши мумкин бўлган ашёларни жамоат жойида очик ҳолда (ғилофсиз) олиб юрганлик учун жавобгарлик белгиланмоқда.

Мазкур модданинг иккинчи қисмида совуқ қурол сифатида фойдаланилиши мумкин бўлган ашёларни касбий фаолиятда, спорт фаолиятида ёки хўжалик-маиший мақсадларда фойдаланиш билан боғлиқ бўлмаган ҳолларда (мақсадсиз) жамоат жойларида олиб юрганлик учун, шунингдек фуқаровий қуролни (бундан ўзини ўзи ҳимоя қилиш қуроли мустасно), совуқ қуролни ва совуқ қурол сифатида фойдаланилиши мумкин бўлган ашёларни ўзини ўзи ҳимоя қилиш учун олиб юрганлик учун жавобгарлик белгиланган.

Мазкур чекловлар “Қурол тўғрисида”ги Қонуннинг 9-моддаси 6, 8 ва 9-бандларида белгилаб ўтилган бўлиб, ушбу нормалар Маъмурий

жавобгарлик тўғрисидаги Кодексининг 185³-моддасида назарда тутилган, яъни совуқ қуролнинг қонунга хилоф муомаласи учун жавобгарлик белгиланган.

Янги таҳрирдаги Конституциямизнинг 25-моддасига мувофиқ, яшаш ҳуқуқи ҳар бир инсоннинг ажралмас ҳуқуқидир ва у қонун билан муҳофаза қилинади. Инсон ҳаётига суиқасд қилиш энг оғир жиноят ҳисобланади.

Маълумки, “баданга шикаст етказиш” деганда, инсон органлари ёки организми тўқималари анатомик тўқислиги ёки улар физиологик вазифасининг ташқи таъсир оқибатида бузилиши тушунилади.

Амалдаги Жиноят кодексининг 104-моддасида содир этилаётган пайтда ҳаёт учун хавfli бўлган қасддан баданга оғир шикаст етказиш натижасида кўриш, сўзлаш, эшитиш қобилиятини йўқотиш ёхуд бирон аъзонинг ишдан чиқиши ёки унинг фаолияти тамоман йўқолиши, руҳий ҳолатининг бузилиши ёки соғлиғининг бошқача тарзда бузилишига, умумий меҳнат қобилиятининг ўттиз уч фоизидан кам бўлмаган қисмининг доимий йўқолиши ёки ҳомиланинг тушиши ёхуд баданнинг тузалмайдиган даражада хунуклашишига сабаб бўлса ва ушбу кодекснинг 126¹-моддасида назарда тутилган жиноят аломатлари мавжуд бўлмаса, ушбу қилмишга жиноий жавобгарлик белгиланган.

Бундан ташқари ушбу модданинг 2-қисми “л” бандида қуролни ёки совуқ қурол сифатида фойдаланилиши мумкин бўлган ашёларни ишлатиб содир этганлик учун ҳам жавобгарлик назарда тутилган.

“Қурол тўғрисида”ги Қонунда совуқ қурол сифатида фойдаланилиши мумкин бўлган ашёга таъриф берилган. Унга кўра, касбий, ишлаб чиқариш ёки спорт фаолиятида ёхуд хўжалик-маиший мақсадларда фойдаланиш учун мўлжалланган, саноат усулида ёки қўлбола тарзда ясалган тиғли, кесувчи ашёлар (пичоқлар, бигизлар ва бошқа учи ўткирланган санчиладиган, кесувчи ашёлар), жисмоний куч ишлатганда шикаст етказиши мумкин бўлган ашёлар (бейсбол биталари, софтбол ўйини учун биталар) совуқ қурол сифатида фойдаланилиши мумкин бўлган ашё деб топилади.

Амалиётда шахс баданига оғир шикаст етказиш жиноятини турли ашёларни (темир ва тош бўлағи, кетмон дастаси ва шу каби тиғли, кесувчи бўлмаган) қўллаб содир этиш ҳолатлари ҳам учраб туради. Бироқ қонунчилик мазмунидан келиб чиққан ҳолда ушбу ашёларни совуқ қурол сифатида фойдаланилиши мумкин бўлган ашё деб топиш мумкин эмас. Шу боис совуқ қурол суд экспертизаси томонидан ушбу ашёларни совуқ қурол сифатида фойдаланилиши мумкин бўлган ашё деб топиб бўлмаслик ҳақида хулосалар берилмоқда. Ҳолбуки, ушбу ашёлар кишининг соғлиғига амалда шикаст етказиши мумкин бўлган ашё ҳисобланади.

Ички ишлар органларига ушбу турдаги ҳуқуқбузарликларни аниқлаш ва ҳуқуқбузар томонидан маъмурий ҳуқуқбузарлик содир этган фактини исботловчи процессуал ҳужжатлар ҳамда маъмурий ҳуқуқбузарлик тўғрисидаги баённома расмийлаштириш ва мазкур ҳолатни қонуний кўриб чиқишлик учун тўпланган ҳужжатларни Маъмурий судга юбориш ваколати берилган.

Шунга эътибор қаратиш лозимки, ички ишлар органлари ходимларини маъмурий ҳуқуқбузарлик содир этган шахсга жазо чораларини кўриш ваколати берилмаган, яъни жазо тайинлаш ёки жазодан озод қилиш масаласини ҳал қилиш тегишли суд ваколатига ўтказилган.

Ички ишлар органлари томонидан маъмурий ҳуқуқбузарлик ҳолати аниқланган тақдирда у бўйича расмийлаштирилиши лозим бўлган ҳужжатлар ва маъмурий ҳуқуқбузарлик тўғрисидаги баённома тузиш шартлари Ўзбекистон Республикасининг Маъмурий жавобгарлик тўғрисидаги Кодексида белгилаб берилган.

Бундан ташқари, фуқаро маъмурий ҳуқуқбузарлик содир этганлигини инкор қилиш, ўз ҳуқуқларини судга қадар бўлган вақтда ҳамда судда шахсан ўзи ёки адвокат ёрдамида ҳимоя қилиш ҳуқуқи мавжуд.

Ҳолат ҳолисона ва объектив кўриб чиқилиши учун ички ишлар органлари маъмурий ҳуқуқбузарлик фактини тўлиқ исботлаши ва ҳуқуқбузарни важларини текшириши лозим.

Судда тарафларнинг тенглиги ва тортишувчанлигини амалга ошириш механизмлари мавжудлиги, ҳуқуқбузар ўзининг ҳуқуқларини бевосита ўзи ёки адвокат ёрдамида ҳимоя қилиш ҳуқуқи таъминланиши, шунингдек Ўзбекистон Республикаси фуқаролари, чет эл фуқаролари ва фуқаролиги бўлмаган шахслар давлат органлари ва бошқа органларнинг, мансабдор шахсларнинг ҳар қандай ғайриқонуний хатти-ҳаракатларидан (қарорларидан), шунингдек ҳаёти ва соғлиғи, шаъни ва кадр-қиммати, шахсий эркинлиги ва мол-мулки, бошқа ҳуқуқ ва эркинликларига тажовузлардан суд ҳимоясида бўлиш ҳуқуқига эгаллиги Ўзбекистон Республикасининг “Судлар тўғрисида”ги Қонунида белгилаб ўтилган.

Совуқ қурол ва совуқ қурол сифатида фойдаланилиши мумкин бўлган ашёларнинг тактик-техник хусусиятларига кўра ҳуқуқий малакада куйидагиларга эътибор қилиниши лозим:

жисмоний шахслардан олинган ашёлар совуқ қурол ёки совуқ қурол сифатида фойдаланилиши мумкин бўлган ашёлар тоифасига кириш-кирмаслигини фақат илмий-асосланган совуқ қурол суд экспертизаси ҳулосасига асосан белгиланиши амалиётини жорий этиш;

Ўзбекистон Республикаси ҳудудида фуқаровий ва хизмат қуроли сифатида муомалада бўлиши тақиқланган совуқ қурол ва ашёларнинг тури, хили, номланиши ва совуқ қурол туркумига тааллуқлигини ёки кирмаслигини белгилаш;

фуқаровий совуқ қурол ва совуқ қурол сифатида фойдаланилиши мумкин бўлган ашёларнинг ашёларнинг тури, хили, номланиши ва совуқ қурол сифатида фойдаланилиши мумкин бўлган ашё туркумига тааллуқлигини ёки кирмаслигини белгилаш;

фуқаролар томонидан фуқаровий, совуқ қурол ёки совуқ қурол сифатида фойдаланилиши мумкин бўлган ашёларни жамоат жойларида олиб юриш ва ташиш ҳолатини инобатга олиш.

Ҳодиса жойидан ёки тергов ҳаракатлари давомида олинган совуқ қурол ёки совуқ қурол сифатида фойдаланилиши мумкин бўлган ашёларда мавжуд бўлган бармоқ ёки биологик изларни (қон, биологик материаллар ва ҳ.к.) йўқ қилмаслиги ёки яроқсиз ҳолатга келтирмаслиги мақсадида совуқ қурол ёки совуқ қурол сифатида фойдаланилиши мумкин бўлган ашёларни мутахассис томонидан тиббий қўлқоплар билан олиниши ва картон қутисига қадоқлаш. Қутига қадоқлашда совуқ қуролнинг ташқи қисмларида мавжуд бўлган изларни яроқсиз ҳолатга келтирмаслик усулида албатта мутахассис томонидан қадоқланиши керак.

Бармоқ излари ва биологик излари мавжуд бўлган совуқ қурол ёки совуқ қурол сифатида фойдаланилиши мумкин бўлган ашёларни полиэтилен пакетлар, конверт ва қопларга ўраш ва қадоқлаш таъқиқланади. Бу ҳолатда совуқ қурол ёки совуқ қурол сифатида фойдаланилиши мумкин бўлган ашёлардаги излар яроқсиз ҳолатга келиши мумкин. Шунингдек, биологик излар чириб кетиши мумкин.

Бундан ташқари, жиноят жойидан олинган пичоқ бўйича бир қатор экспертизалар тайинланиши мумкин ва унинг кетма-кетлигига эътибор қилиш керак. Хусусан, битта пичоқ бўйича аввал биологик ёки ДНК экспертизаси тайинлаш керак, кейин ёки комплекс ДНК ва дактилоскопик экспертизаси, бундан кейин совуқ қурол ва трасологик суд экспертизаси тайинланиши мақсадга мувофиқ.

Умуман олганда, терговга қадар текширув, суриштирув ва дастлабки тергов фаолиятида жавобгарлик белгиланган совуқ қурол ва совуқ қурол сифатида фойдаланилиши мумкин бўлган ашёларнинг тактик-техник хусусиятларига кўра ҳуқуқий малакалашда совуқ қурол суд экспертизаси ҳулосасига асосланиш мақсадга мувофиқ.

Хулоса ўрнида шунини айтиш мумкинки, совуқ қуроллар экспертизаси муаммоларини комплекс ёндошув асосида ҳал этиш жамоат жойларида

аҳолининг хавфсизлигини таъминлаш ҳамда фуқароларнинг ҳаёти ва соғлигини муҳофаза қилишда муҳим аҳамият касб этади деб ҳисоблаймиз.

БИБЛИОГРАФИК МАНБААЛАР:

1. Ўзбекистон Республикасининг 2019 йил 29 июлдаги “Қурол тўғрисида”ги ЎРҚ-550-сон Қонуни;
2. Ўзбекистон Республикасининг 2020 йил 5 ноябрдаги “Жамоат хавфсизлигини таъминлашга доир қонун ҳужжатлари янада такомиллаштирилиши муносабати билан Ўзбекистон Республикасининг айрим қонун ҳужжатларига ўзгартириш ва қўшимчалар киритиш тўғрисида”ги ЎРҚ-645-сон Қонуни;
3. Ўзбекистон Республикасининг 2022 йил 31 майдаги “Қурол тўғрисидаги қонунчилик такомиллаштирилиши муносабати билан Ўзбекистон Республикасининг айрим қонун ҳужжатларига ўзгартириш ва қўшимчалар киритиш ҳақида”ги ЎРҚ-772-сон Қонуни;
4. ГОСТ Р 51548-2000 “Ножи для выживания (Общие технические условия)”;
5. ГОСТ Р 51215-98 “Оружие холодное (Термины и определения)”;
6. ГОСТ Р 52737-2007 “Тесаки охотничьи, мачете туристические, разделочные, инструменты для восстановительных и спасательных работ (Общие технические требования и методы испытаний на безопасность)”;
7. ГОСТ Р 51715-2001 “Изделия декоративные и сувенирные, сходные по внешнему строению с холодным или метательным оружием (Общие технические требования)”;
8. ГОСТ Р 51644-2000 “Ножи разделочные и шкуросъемные (Общие технические условия)”;
9. ГОСТ Р 51501-99 “Ножи туристические и специальные спортивные (Общие технические условия)”;
10. ГОСТ Р 51015-97 “Ножи хозяйственные и специальные (Общие технические условия)”;
11. ГОСТ Р 51500-99 “Ножи и кинжалы охотничьи (Общие технические условия)”;
12. А.И.Устинов “Холодное оружие и бытовые ножи” М.78.

ZARARLI AXBOROTLARNING YOSHLAR O‘RTASIDA TARQALISHINI OLDINI OLISH

Yuldashev Qudrat Abduvaxatovich

atta o‘qituvchisi, falsafa doktori, (PhD)

“Global axborotlashtirish va kompyuterlashtirish asri”da insoniyat hayotiga olamshumul ixtirolar bilan bir qatorda, axborot xavfsizligiga taxdid solayotgan kompyuter jinoyatchiligi kabi ulkan muammolar ham kirib kelmoqda. Axborot texnologiyalari sohasidagi yangiliklar ushbu sohalardan xabardorlikni dolzarb masalaga aylantirdi. Dunyo bo‘yicha son-sanoqsiz odamlar internet xizmatlaridan foydalanmoqdalar, axborot almashmoqda, o‘z bilimlarini oshirishmoqda hamda turli masalalarni zudlik bilan hal qilmoqdalar.

Bugun yoshidan, qaysi ijtimoiy guruh yoki qatlama mansubligidan qat’iy nazar – internetdan foydalanuvchilar hamon ortib borayotgan bo‘lsa-da, bunda o‘quvchi yoshlarning soni kengayib borayotganligi bu sohada tushintirish va targ‘ibot ishlari olib borishni taqozo qiladi. Internet paydo bo‘lgandan beri ba’zilar uni ijobiy baholashsa, ba’zilar salbiy tomonlarini gapiradi. Bu mavzudagi maqbul qarash shuki, internet ham televizor, radio kabi bir vosita. Uni yaxshilikka ishlatsak yaxshi, yomonlikka ishlatsak yomon narsaga aylanadi.

Bu yerdagi eng muhim omil – inson omilidir. Chunki inson bir paytning o‘zida to‘g‘ri ma’lumot ham, yomon ma’lumot ham tarqatishi mumkin. Uning muqobilida o‘quvchi-yoshlar tushunib tushunmay har qanday yaxshi yoki yomon ma’lumotni qabul qilib olishi mumkin. Demak o‘qituvchi-murabbiylarning muhim vazifasi - internetdan foydalanayotgan yosh avlodga to‘g‘ri yo‘lni ko‘rsatish, zararli oqibatlardan ogohlantirishdir. Boshqa tomondan esa ijtimoiy tarmoqlarda milliy qadriyatlarimizga zid g‘oyalarni targ‘ib qilayotgan shaxslar ta’siriga tushmaslik yo‘llarini o‘rgatishdir.

Statistik ma’lumotlarga ko‘ra mamlakatimizda ayni vaqtda “Facebook”da 4,7 million, “Instagram” da 3,7 million, “LinkedIn”da 288 ming, “Telegram”da 18 million, “Odnoklassniki”da 16,7 million, “Twitter”da 51,6 ming va “V-kontakte”da 2,6 million foydalanuvchi mavjud bo‘lib, ularning ko‘pchiligini tashkil etadi. Keyingi vaqtlarda “ommaviy madaniyat” niqobi ostida yoshlarimiz ongiga salbiy ta’sir etuvchi axloqiy buzuvchi va zo‘ravonlik g‘oyalarni tarqatish, turfa yo‘llar bilan boylik orttirishni, milliy ma’naviy madaniyatga amal qilmaslikni, ularni o‘zgartirish va ayrim hollarda yo‘qotishni targ‘ib qiluvchi harakatlarqilinyapti. Internet tarmog‘i orqali tarqatilayotgan g‘arazli ma’lumotlar,

turli buzg‘unchi g‘oyalar, odob-axloqni yemiruvchi illatlar aholini tashvishga solyapti.

Prezidentimiz Shavkat Mirziyoyev Oliy Majlis va O‘zbekiston xalqiga Murojaatnomasida “Biz jamiyatimizda har qanday radikallashuvga, yoshlarimiz ongini buzg‘unchi yot g‘oyalar bilan zaharlashga, dindan siyosiy maqsadlarda foydalanishga, ma’rifat o‘rnini jaholat egallashiga yo‘l qo‘ymaymiz. Buning uchun nafaqat mas’ul tashkilotlar, balki barchamiz birgalikda muqaddas dinimizning insonparvarlik mohiyatini ochib berish, farzandlarimizni milliy va umumbashariy qadriyatlar ruhida tarbiyalash bo‘yicha oila, mahalla va ta’lim maskanlarida ish olib borishimiz zarur” deb ta’kidladilar⁸¹.

Bugungi kunda O‘zbekistonda Internet xizmatidan foydalanuvchilar soni 31 mlndan oshganligi, shundan mobil Internet foydalanuvchilari soni 29,5 mlzni tashkil etayotganligini ta’kidlash lozim⁸². Internet. Xalqaro tarmoq. Hozirgi kunda jahondagi eng yirik tarmoq. Eng o‘ziga tortuvchi va eng xavfli tarmoq. Eng rivojlangan va eng vaqtni oluvchi tarmoq. Haqiqiy “o‘rgimchak to‘ri” bo‘lgan tarmoq. Ko‘zga ko‘rinmas tuzoqqa ilintiruvchi tarmoq. Ha biz shunday zamonda yashayapmizki, biror kunimizni internetsiz o‘tkaza olmaymiz. Bir kun kirmasak, xuddi biror narsamizni yo‘qotib qo‘ygandekmiz.

Kimdir yangilik olish maqsadida, kimdir axborot ulashish maqsadida, kimdir ilm olish maqsadida, kimdir o‘yin o‘ynash maqsadida, kimdir behayoliklardan nafsini qondirish maqsadida, kimdir shunchaki, bekorchilikdan vaqtini o‘tkazish maqsadida, kimdir kino ko‘rish maqsadida, kimdir kerakli dasturlarni yuklash maqsadida, kimdir boylik orttirish maqsadida, kimdir kimnidir aldash maqsadida, kimdir biznesini rivojlantirish maqsadida, kimdir nimadir sotib olish maqsadida. Albatta, internet uzog‘imizni yaqin, og‘irimizni yengil, birimizni ikki, ishimizni oson qilishga xizmat qiladi.

Internet xurujlari haqida gapirganda, eng avvalo g‘oyaviy, mafkuraviy, axboriy, psixologik, siyosiy, harbiy, iqtisodiy xurujlarni eslash lozim. Chunki XXI asr axborot asri bo‘lgani sababli, ushbu asrda eng qimmat manba bu axborotdir. Birgina axborot (yolg‘on, buzg‘unchi yoki tuzoqli) bilan butun bir davlat ichida yoki xalqlar, millatlar orasida, kishilar orasida yoxud davlatlararo, qit‘alararo turli nizolar, kelishmovchiliklar, hatto qonli urushlar keltirib chiqarish mumkin. Undan tashqari yoshlar tarbiyasini buzishga qaratilgan behayollik, zo‘ravonlik, beparvolik, dangasalik va shu kabi boshqa salbiy jihatlarga undovchi xurujlar haqida gapiriladi.

⁸¹ <https://www.xabar.uz/jamiyat/shavkat-mirziyoyevning-oliy-majlis-va-ozbekiston-xalqi>

⁸² <https://aniq.uz/yangiliklar/uzbekistonda-internet-xizmatidan-foydalanuvchilar>.

Bu xurujlar ham o'sib kelayotgan yosh avlodning buzilishiga, uning oqibatida esa butun bir xalq, millat, jamiyatning buzilishiga, turli fisq-fasod, fitnalar yoyilishiga, o'g'riliklar, giyovandlik, boqimandaliklar, fahsh ishlari ko'payishiga olib keladi. Axborot iste'moli madaniyatini shakllantirish, g'oyaviy immunitetni mustahkamlashda asosan, pedagoglar, jurnalistlar, yozuvchilar, rejissorlar, psixologlar, axborot texnologiyasi sohasi mutaxassislari, siyosatshunoslar, davlat arboblari, rahbarlar, ota-onalar, mahallalar, ekspertlar, imomlar, hukumat organlari xodimlari, qo'yingki, har bir ong-tafakkuri sog'lom shaxs o'z hissasini qo'shishi kerak. Yoshlarni internetdagi zararli xurujlardan asrash, ularni axborot texnologiyalaridan unumli foydalanishga o'rgatish masalalari bo'yicha ilg'or xalqaro tajribalar asosida barcha hududlarda Raqamli texnologiyalar o'quv markazlari tashkil etildi.

Bu maskanlarda elektron tijorat va dasturlash bepul o'rgatilmoqda, axborot texnologiyalari sohasida biznes bo'yicha innovatsion ko'nikmalar shakllantiriladi, "startap" loyihalarga yordam ko'rsatiladi. Shuningdek, hozirgi kunda barcha maktablardagi kompyuter sinflarini zamonaviy texnologiyalar va yuqori tezlikdagi internet tarmog'i bilan ta'minlash bo'yicha choratadbirlar rejasi ishlab chiqilib, bosqichma-bosqich amalga oshirilmoqda. Yangi tashkil etiladigan kompyuter o'yinlari markazlari yosh avlodning bilim va dunyoqarashini kengaytirishga qaratilmoqda.

Yosh avlod tarbiyasi barcha zamonlarda ham muayyan xalq, millat yoki elat emas, balki butun dunyo hamjamiyatini o'ylantirib kelayotgan muhim va dolzarb masala bo'lgan. Insonga aynan yoshligida berilgan ijobiy yoki salbiy ta'lim-tarbiya oradan yillar o'tib o'z ta'sirini ko'rsatishi bizga ma'lum. Yoshlar bizning kelajagimiz. Kechagi va bugungi kun bilan emas, balki ertangi kun uchun kelajak avlod borasida qayg'urish kerak. Bundan ko'rinib turibdiki, yoshlarni ma'rifatli qilib tarbiyalash uning dunyoga kelishidan boshlanishi va davomiylilik kasb etishi lozimligi natijada bolalarimiz jamiyatimizda o'rnatilgan qonun-qoidalarga muntazam rioya etish va qonunlarga ixtiyoriy itoatkorlik ruhini singdirib borishni bildiradi.

Bola dunyoga kelganidan boshlab unga g'amxo'rlik qilish, sog'lom va to'g'ri tarbiya hamda zamonaviy ta'lim olishini ta'minlash – jamiyatimiz kelajagi, ertangi kunimiz poydevoridir. Nega deganda, bolalar zilol suvga o'xshaydi. Suv qaysiki idishga solinsa, shu idish shaklini olganidek, bolalar muhit, ota-ona va tarbiyachilar odob-axloqi va xatti-harakatlarini aynan ko'rganidek qabul qilishi hech kimga sir emas. Zotan, "Qush uyasida ko'rganini qiladi", degan naql bejiz aytilmagan. O'ylaymizki, yuqoridagi vazifalardan kelib chiqib, quyidagi yo'nalishlar yoshlar o'rtasida internet tarmog'i orqali tarqatilayotgan zararli axborotlarning profilaktikasini yanada kuchaytirishga xizmat qiladi:

– ta’lim jarayonida yoshlarni turli yot g‘oyalar ta’siridan, axborot xurujlaridan, “ommaviy madaniyat”ning salbiy ta’siridan himoya qilish maqsadida ularda vatanparvarlik, yurtga sadoqat va uning taqdiriga daxldorlik tuyg‘ularini singdirish kabi masalalarga alohida e’tiborni qaratish;

– yoshlarning bo’sh vaqtlarini mazmunli o‘tkazishda ularni yomon yo‘llarga kirib ketishidan saqlashda maktabdan tashqari ta’limning shakllarini tubdan yangilash;

– ta’lim muassasalarining pedagog o‘qituvchilarning ota-onalari bilan aloqalarni kuchaytirish, hozirgi globallashuv sharoitlarining salbiy oqibatlari yuzasidan ota-onalar o‘rtasida tushuntirish ishlarini yo‘lga qo‘yish; – yoshlarni axloqiy negizlarni buzishga olib keladigan xatti-harakatlardan, terrorizm va diniy ekstremizm, separatizm, fundamentalizm, zo‘ravonlik va shafqatsizlik g‘oyalaridan himoya qilish;

– mahalla va oilada yoshlar o‘rtasida kitobxonlikni keng targ‘ib qilish; – yoshlarning huquqiy ongi va huquqiy madaniyati darajasini yuksaltirish kabilardan iboratdir.

Xulosa o‘rnida internet bu johil uchun jaholat, jinoyatchi uchun jinoyat, tijoratchi uchun tijorat, zoniy uchun zino, sudxo‘r uchun ribo, o‘g‘ri uchun o‘g‘rilik, to‘g‘ri uchun to‘g‘rilik, tolibi ilm uchun ilm, olim uchun ziyo, zolim uchun zulm, da’vatchi uchun da’vat, adashgan uchun razolat, munajjim uchun bashorat manbaidir.

Foydalangan adabiyotlar ro‘yxati:

1. O‘zbekiston Respublikasining Konstitutsiyasi // URL:<http://www.lex.uz>.
2. O‘zbekiston Respublikasining “Huquqbuzarliklar profilaktikasi to‘g‘risida”gi qonuni // URL:<http://www.lex.uz>.
3. O‘zbekiston Respublikasining Jinoyat kodeksi // URL:<http://www.lex.uz>.
4. Rossiya Federatsiyasi Jinoyat kodeksi [https://www.consultant.ru/ document/ cons doc LAW 10699/](https://www.consultant.ru/document/cons_doc_LAW_10699/).
5. X.B. *Abdreymov* Axborot texnologiyalari sohasidagi jinoyatlar va ulardan himoyalaniş usullari *IIV Akademiya Magistratura inglovchisi*.
6. A.K.Rasulev Axborot texnologiyalari va xavfsizligi sohasidagi jinoyatlarga qarshi kurashishning jinoyat-huquqiy va kriminologik choralarini takomillashtirish. Yurid. fanlar doktori dissertatsiyasining avtoreferati. T., IIV Akademiyasi, 2018. - B-5.

KIBERJINOYATLARDAN HIMOYA QILISHDA AI ALGORITMLARINING ROLI

Y.B. Tashmanov

IIV Malaka oshirish instituti katta o'qituvchisi, PhD.

E.E. Kanaev

IIV Malaka oshirish instituti Axborot texnologiyalar bo'limi katta mutaxasisi

Zamonaviy dunyoda axborot texnologiyalari (AT) rivojlanishi jamiyatning barcha sohalariga chuqur ta'sir ko'rsatmoqda, ammo bu jarayon bilan bir qatorda kiberjinoyatlar soni ham keskin oshib bormoqda. Masalan, ma'lumot o'g'irlash, phishing hujumlari, deepfake videolar va onlayn firibgarliklar kabi huquqbuzarliklar iqtisodiy zararlarga va shaxsiy hayotga jiddiy tahdid solmoqda. Global miqyosda kiberjinoyatlar natijasidagi zarar 2025-yilga kelib 10,5 trillion dollarga yetishi kutilmoqda. O'zbekistonda esa vaziyat yanada dolzarb: oxirgi besh yilda kiberjinoyatlar soni 6700% ga oshgan bo'lib, 2025-yil boshida ular barcha qayd etilgan jinoyatlarning 42% ini tashkil etmoqda. 2023-yilda kiberjinoyatlar umumiy jinoyatlarning 6,2% ini tashkil etgan bo'lsa, 2024-yilda bu ko'rsatkich 44,4% ga yetgan. Raqamli iqtisodiyotning jadal o'sishi, jumladan, onlayn savdo va raqamli xizmatlarning kengayishi, kiberxavfsizlikka bo'lgan ehtiyojni yanada kuchaytirmoqda, chunki O'zbekistonning kiberxavfsizlik bozori 2025-yilda 87,85 million dollarga yetishi prognoz qilinmoqda.

Ushbu muammolarga qarshi kurashda sun'iy intellekt (SI) va chuqur o'qitishga asoslangan algoritmlar muhim rol o'ynamoqda. Xususan, video tasvirlarda obyektlarni avtomatik aniqlash modellari, masalan, YOLO (You Only Look Once), Faster R-CNN (Region-based Convolutional Neural Network) va SSD (Single Shot MultiBox Detector), real vaqt rejimidagi kuzatuv tizimlarida noqonuniy harakatlarni aniqlash va oldini olish imkonini beradi. Bu algoritmlar dronlar orqali noqonuniy kuzatuv, deepfake videolar bilan firibgarlik yoki xavfsizlik tizimlariga hujumlar kabi kiberjinoyatlarga qarshi samarali vosita sifatida qo'llanilishi mumkin. Ushbu maqola mazkur modellarning afzalliklari, muammolari va O'zbekiston sharoitida kiberxavfsizlikni kuchaytirishdagi rolini tahlil qiladi.

Kiberjinoyatchilikning dolzarb muammolari quyidagilardan iborat:

1. Real vaqt rejimidagi tahdidlar: Video oqimlar orqali sodir etiladigan huquqbuzarliklar, masalan, dronlar yordamida noqonuniy kuzatuv yoki deepfake videolar bilan firibgarlik, tezlik va aniqlik talab etadi. Ilgari qo'lda belgilangan usullar samarasiz bo'lgan, ammo chuqur o'qitishga asoslangan modellarning rivojlanishi bu muammoni hal qilishga yordam bermoqda.

2. Kichik obyektlarni aniqlashdagi qiyinchiliklar: Kiberjinoyatchilikda kichik elementlar (masalan, virus kodlari yoki video tasvirlardagi yashirin obyektlar) ni aniqlash qiyin. YOLO modeli yuqori tezlikda ishlaydi (155 kadr/s gacha), lekin kichik obyektlarni lokalizatsiyada kamchiliklarga ega. Faster R-CNN va SSD esa ko‘proq aniqlik beradi, ammo hisoblash murakkabligi yuqori.

3. Ma’lumotlar xavfsizligi va shaxsiy hayot: AT orqali sodir etiladigan huquqbuzarliklar ma’lumotlarni o‘g‘irlashga olib keladi. Video kuzatuv tizimlarida obyektlarni avtomatik aniqlash (masalan, noqonuniy harakatlarni) huquqbuzarliklarni oldini olishga yordam bersa-da, bu texnologiyalar o‘zi ham huquqbuzarlikka sabab bo‘lishi mumkin (masalan, shaxsiy ma’lumotlarni suiiste’mol qilish).

4. Tez rivojlanayotgan tahdidlar: Deepfake va AI-generatsiya qilingan kontentlar bilan bog‘liq huquqbuzarliklar ko‘paymoqda. Ushbu muammolarni hal qilish uchun bir bosqichli detektorlar (YOLO, SSD) va ikki bosqichli modellarni (Faster R-CNN) birlashtirish kerak.

Adabiyotlarda ko‘rsatilishicha, YOLOv7 modeli tezlik va aniqlik bo‘yicha ustunlik qiladi (5-160 kadr/s), SSD esa multi-scale feature maps orqali turli o‘lchamdagi obyektlarni aniqlaydi. Faster R-CNN esa Region Proposal Network (RPN) yordamida aniq lokalizatsiya ta’minlaydi.

Yechimlar va metodologiyada huquqbuzarliklarga qarshi kurashishda quyidagi yechimlar taklif etiladi:

1. Avtomatik aniqlash tizimlarini joriy etish: YOLO modeli real vaqt rejimidagi kuzatuv tizimlarida qo‘llanilishi mumkin. Masalan, tasvirni gridlarga bo‘lib, bounding boxlar va sinf ehtimollarini hisoblash orqali noqonuniy obyektlarni (masalan, dronlar yoki noqonuniy transport) aniqlash. Xatolik funksiyasi:

$$L = \lambda_{coord} L_{loc} + L_{class} \quad L = \lambda_{coord} L_{loc} + L_{class}$$

Bu model kiberhuquqbuzarliklarni tez aniqlashga yordam beradi.

2. Ikki bosqichli modellardan foydalanish: Faster R-CNN RPN orqali obyekt bo‘lishi mumkin bo‘lgan hududlarni taklif qiladi va ROI Pooling yordamida aniqlashtiradi. Ushbu model deepfake videolarda yolg‘on obyektlarni aniqlashda samarali. Umumiy xatolik funksiyasi:

$$L = L_{RPN} + L_{FastRCNN} \quad L = L_{RPN} + L_{FastRCNN}$$

Regressiya loss: $L_{reg} = \sum_i p_i * \sum_{j \in \{x,y,w,h\}} smoothL1(t_{ji} - \hat{t}_{ji})$

$$L_{reg} = \sum_i p_i * \sum_{j \in \{x,y,w,h\}} smoothL1(t_{ji} - \hat{t}_{ji})$$

3. SSD modeli orqali balansli yechim: SSD bir bosqichli detektor bo‘lib, VGG-16 asosida ishlaydi va multi-scale feature maps yordamida kichik va katta

obyektlarni aniqlaydi. Kiberxavfsizlikda, masalan, video tahlilida noqonuniy harakatlarni aniqlash uchun ideal. Umumiy xatolik funksiyasi:

$$L=L_{conf}+\alpha L_{loc} \quad L=L_{\{conf\}}+\alpha L_{\{loc\}} \quad L=L_{conf}+\alpha L_{loc}$$

Bu model 46 fps tezlikda 74% aniqlik beradi, bu real vaqt rejimidagi kiberhuquqbuzarliklarga qarshi kurashish uchun mos.

4. Integratsiya va optimallashtirish: Ushbu modellarni birlashtirib, gibrid tizim yaratish mumkin. Masalan, YOLO tez aniqlash uchun, Faster R-CNN aniqlik uchun. O‘zbekiston kontekstida ushbu algoritmlarni milliy xavfsizlik tizimlariga integratsiya qilish, qonun hujjatlarini takomillashtirish va ta’lim dasturlarini rivojlantirish kerak.

Natijalarda ko‘rsatilishicha, SSD300 modeli tezlik va aniqlik bo‘yicha ustun (74% mAP, 46 fps), YOLO esa 21 fps tezlikda ishlaydi.

Xulosa o‘rnida axborot texnologiyalari orqali sodir etiladigan huquqbuzarliklarga qarshi kurashishda YOLO, Faster R-CNN va SSD kabi algoritmlar muhim rol o‘ynaydi. Ushbu modellarning afzalliklari (tezlik, aniqlik) muammolarni hal qilishga yordam bersa-da, kamchiliklari (kichik obyektlarni aniqlashdagi qiyinchiliklar) ni bartaraf etish uchun doimiy optimallashtirish talab etiladi. O‘zbekistonda kiberxavfsizlikni kuchaytirish uchun ushbu texnologiyalarni qo‘llash, qonuniy bazani takomillashtirish va mutaxassislar tayyorlash zarur. Kelajakda AI-ni etik va xavfsiz qo‘llash orqali huquqbuzarliklarni minimallashtirish mumkin.

Foydalanilgan adabiyotlar:

1. Peiyuan Jiang, Daji Ergu, Fangyao Liu, Ying Cai, Bo Ma: A Review of Yolo Algorithm Developments. *Procedia Computer Science* Volume 199, 2022, Pp:1066-1073.
2. Rishabh Singh: Understanding and Implementing Faster R-CNN. *Medium*, October 15, 2024.
3. Nosirov K., Norinov M., Abdukadirov B. Image filtering algorithm based on the analysis of the main components // *International Conference on Information Science and Communications Technologies (ICISCT)*. – 2019. Pp. 1-3.
4. Norinov M., Abdukadirov B., Gofurov M. Application of Fourier Methods and Discrete-Cosinus Transformation in the Process of Processing of TV Images // *International Journal of Innovative Technology and Exploring Engineering*. – 2019. – Vol. 8, Issue 9S3. – Pp. 1565-1568.
5. Niyozmatova N., Mamatov N., Samijonov A., Abdukadirov B., Abdullayeva B. Algorithm for determining the coefficients of the interpolation polynomial of Newton with separated differences // *IOP Conference Series: Materials Science and Engineering*. – 2020. – Vol. 862, Issue 042019. – Pp. 1-4.

АХБОРОТ ТЕХНОЛОГИЯЛАРИДАН ФОЙДАЛАНГАН ҲОЛДА СОДИР ЭТИЛАДИГАН АХЛОҚҚА ҚАРШИ ҚАРАТИЛГАН ЖИНОЯТЛАР УЧУН ЖАВОБГАРЛИК

Баҳромжон Бахтиёрович Турғунбаев

*Ўзбекистон Республикаси, ИИВ Малака ошириш институти, Юридик
фанлар ўқитувчиси*

Кибертехнологиялар орқали вояга етмаган шахсни ғайриижтимоий хатти-ҳаракатларга жалб қилиш. Кибертехнологиялар орқали вояга етмаган шахсни ғайриижтимоий хатти-ҳаракатларга жалб қилиш жинояти энг оғир жиноятлардан бири ҳисобланади, сабаби вояга етмаганларни ғайриижтимоий хатти-ҳаракатларга жалб қилиш орқали, уларга ҳам руҳий, ҳам жисман зарар келтириш мумкин, қолаверса, уларнинг келажагини барбод қилиш орқали бутун бир жамиятнинг кейинги ривожига салбий таъсир кўрсатиш мумкин.

Мазкур жиноят объектив томондан вояга етмаган шахсни кибертехнологиялар орқали спиртли ичимликлар истеъмол қилишга, гиёвандлик воситалари ва уларнинг аналоглари ёки психотроп ҳисобланмаган ёки ҳисобланмаганидан қатъий назар кишининг ақл-идрокига таъсир қиладиган восита ва моддаларни истеъмол қилишга ёки порнографик маҳсулотлар тайёрлаш билан боғлиқ ўзга юмушларга жалб қилиш орқали содир этилади ва ушбу жиноятнинг объектини вояга етмаган шахснинг нормал ҳаётига, ахлоқий ва жисмоний ривожланиши, унинг соғлиғи, жамоат хавфсизлиги ва тартибини таъминловчи ижтимоий муносабатлар ташкил этади. Ушбу жиноят тўғри қасддан 18 ёшга тўлган ақли расо шахс томонидан кибертехнологиялардан фойдаланган ҳолда содир этилади ва юқорида саналган ҳаракатларга вояга етмаган шахс томонидан содир этилган вақтдан бошлаб тугалланган ҳисобланади.

Интернет ёки телекоммуникация тармоқлари орқали вояга етмаган шахсни ғайриижтимоий қилмишларга жалб қилганлик учун Қоғоғистон жиноят кодексининг 132-моддасининг 2-қисмида учун жиноий жавобгарлик белгиланган. Бироқ, Ўзбекистон жиноят кодексининг 127-моддасида, Литва жиноят кодексининг 159-моддасида, Тожикистон жиноят кодексининг 166-моддасида, Қирғизистон жиноят кодексининг 180-моддасида бу ҳолат назарда тутилмаган.

Шунга кўра, бу тоифадаги жиноятлар содир этилишининг олдини олиш, жамиятда соғлом муҳитни яратиш, вояга етмаган шахсларнинг жиноятчилигига қарши тизимли курашиш, виртуал оламда содир этилаётган ва содир этилиши учун шарт-шароит яратиб берилаётган бу каби жиноятларнинг олдини олиш, уларни фош қилиш, одатий ҳолатга нисбатан кибермуҳит орқали жиноят содир этиш ҳам вақт, ҳам иқтисодий жиҳатдан

кулайлигини, эскирган техник сўзлардан фойдаланмаслик, қонунчиликда ягона тушунчалар бўлишини таъминлаш мақсадида ва кибертехнологик ҳуқуқий асослар талабларидан келиб чиқиб, Ўзбекистон Республикаси Жиноят кодексининг 127-моддаси учинчи қисмини монография 1-иловасининг 6-бандида назарда тутилган тартибда “г” банд билан тўлдириш таклиф қилинади.

Киберпорнография. Киберпорнография жинояти ҳам киберсексуализм каби кенг тарқалган жиноятлардан бири ҳисобланади ва ушбу жиноят объектив томондан кибертехнологиялар орқали вояга етмаган шахс тасвирланган ёки тасвирланмаганидан қатъий назар порнографик маҳсулотни тарқатиш, реклама қилиш, намойиш этиш ёки шундай мақсадда тайёрлаш ёхуд давлат ҳудудига олиб кириш ёки шундай мақсадларда вояга етмаган шахсни жалб қилиш орқали содир этилади.

Статистик маълумотларга қараганда ҳафтасига америкаликлар 10 соатга қадар порнографик маҳсулотлардан баҳрамад бўлишар экан ва уларнинг кўпчилиги киберсекс тузоқларга тушиб қолган шахслардир. Э.Л.Кочкинанинг фикрича, киберпорнография вояга етмаган фуқароларнинг порнографик филмлари, видеолари ва фотосуратларини жойлаштиришга имкон берадиган порнографик сайтлардир.

Аммо, наздимизча, киберпорнографияда вояга етмаган шахсларни жалб қилиш билан боғлиқ ҳолатлар жиноятни оғирлаштирувчи ҳолат деб эътироф этилиши ва порнографик характердаги барча маҳсулотлар жамланган ва кўриш, баҳрамад бўлиш имконини берадиган истаган сайтлар, видео, аудиороликлар, ёзувлар ва бошқа порнографик хусусиятга эга воситаларнинг барчасини юқорида таъкидланган ҳолатлар аниқланганлиги жиноятни квалификация қилиш имконини беради. Ушбу жиноятларнинг объектини жамиятнинг ахлоқи ва ёшларнинг нормал ҳаёт кечириши ва соғлиғини муҳофаза қилувчи ижтимоий муносабатлар ташкил этади.

Мазкур жиноят предмети кибертехнологиялар орқали узатилаётган истаган бир порнографик маҳсулотлар ҳисобланади ва бунда кибертехнологиялар мазкур жиноятни амалга ошириш учун восита бўлиб хизмат қилади. Қозоғистон жиноят кодексининг 311-моддасида телекоммуникация тармоқлари ёки Интернет орқали порнографик материаллар ёки объектларни тарқатганлик, реклама қилганлик, кино-, видео материаллар, расмлар кўринишида тайёрлаганлик, ноқонуний давлат чегарасидан олиб ўтганлик, сотганлик, қонунга хилоф равишда ишлаб чиқарганлик, Тожикистон жиноят кодексининг 241-моддасининг 3-қисми “б”-бандида ахборот ва телекоммуникация тармоқларидан (шу жумладан Интернет) фойдаланган ҳолда Тожикистон Республикасининг давлат чегараси орқали ноқонуний ўтказганлик, ҳар қандай шаклда тарқатганлик, оммавий намойиш қилганлик, реклама қилганлик, вояга етмаган шахслар

орасида шундай маҳсулотлар ва буюмларни тарқатганлик, намоёиш этганлик, реклама қилганлик, Тожикистон Республикасининг 241-2-моддасининг “г” ва “д”-бандларида ахборот ва телекоммуникация тармоқларидан (шу жумладан Интернет) фойдаланган ҳолда вояга етмаган шахсни порнографик материаллар ёки буюмларни ишлаб чиқаришга жалб қилганлик, Руминия жиноят кодексининг 374-моддасида, Франция жиноят кодексининг 227-23-моддасида вояга етмаган, яъни 18 ёшга тўлмаган шахснинг фотосурати ёки бундай суратни порнографик ҳолатга келтириб, уни тарқатиш мақсадида фиксация қилганлик, ёзиб олганлик ёки суратни юборганлик, бундай шаклдаги маҳсулотларни ҳар қандай усулда тарқатганлик, шу жумладан, телекоммуникация тармоқларидан фойдаланиб порнографик маҳсулотларни тарқатганлик, Қирғизистон жиноят кодексининг 168-моддасида, Турманистон жиноят кодексининг 155-моддасида, Литва жиноят кодексининг 162-моддасида, Литва жиноят кодексининг 308- моддасида, 312-моддасида вояга етмаганларнинг порнографик тасвирлари бўлган материаллар ёки буюмларни тарқатганлик, омма олдида намоёиш қилганлик ёки реклама қилганлик, тарқатганлик чегара орқали олиб ўтганлик, ушбу маҳсулотларни тайёрлаш учун вояга етмаган шахсни актёр сифатида иштирок этишга жалб қилганлик, вояга етмаганни порнографик маҳсулотлар билан муомала қилишга жалб қилганлик, Украина жиноят кодексининг 301-моддасида порнографик тусдаги кинофилмлар, видеофилмлар, компьютер дастурларини вояга етмаганларга сотиш ёки уларни бундай маҳсулотларга жалб қилганлик, Белоруссия жиноят кодексининг 343- ва 343-1-моддаларида компьютер, телекоммуникация, Интернет тармоғи орқали порнография материалларини ёки вояга етмаган шахсларни жалб қилган ҳолда порнографик мазмундаги тасвирлар, филмлар, видеофилмлар ёки бошқа порнографик объектларни тарқатганлик, реклама қилганлик, эфирга узатганлик учун жиноий жавобгарлик белгиланган.

Ўзбекистон Республикаси Президентининг “Ташқи бозорларда маҳаллий маҳсулотлар рақобатдошлигини таъминлаш ва экспортини рағбатлантиришга доир қўшимча чора-тадбирлари тўғрисида” 2017 йил 15 декабрдаги ПФ–5286-сон Фармони билан тасдиқланган рўйхатга асосан порнографик маҳсулотлар Ўзбекистон Республикасига олиб кириши тақиқланган нарсалар рўйхатига киритилган . Шу сабабдан ҳам мазкур жиноят порнографик маҳсулотни тарқатиш, реклама қилиш, намоёиш этиш ёки шундай мақсадда тайёрлаш ёхуд давлат ҳудудига олиб кириш бошланган ёки шундай мақсадларда вояга етмаган шахсни жалб қилиш орқали содир этилган вақтдан бошлаб тугалланган ҳисобланади. Жиноят 16 ёшга тўлган ақли расо жисмоний шахс томонидан тўғри қасддан содир этилади.

Порнография муомаласининг олдини олиш мақсадида ҳозирги кунда Ўзбекистонда изчил ишлар амалга оширилмоқда, хусусан, Вазирлар

Маҳкамасининг 2007 йил 28 июндаги 132-сон қарори билан тасдиқланган “Ўзбекистон Республикасида босма ва китоб, телерадио-, аудиовизуал маҳсулотлар ва Интернет тармоғи ахборот ресурсларини ишлаб чиқариш ва тарқатиш соҳасида қонун ҳужжатларига риоя қилиниши устидан мониторинг олиб бориш тартиби тўғрисида”ги низом қабул қилинган бўлиб, ушуб низом асосида порнографик хусусиятдаги босма ва китоб, телерадио-, аудиовизуал маҳсулотлар ва Интернет тармоғи ахборот ресурсларини ишлаб чиқариш ва тарқатиш соҳасида қонун ҳужжатларига риоя қилиниши устидан Ахборот ва оммавий коммуникациялар агентлигининг Оммавий коммуникациялар масалалари бўйича маркази томонидан тизимли мониторинг олиб борилмоқда.

Таъкидлаш жоизки, киберпорнография жинояти содир этилиши вақтида нафақат жабрланувчи зарар кўриши, балки унга унинг хизмат ёки бошқа компютери орқали зарар келтириши оқибатида, у бошқа шахсларнинг олдида айбдор бўлиб қолиши, мазкур жиноят содир этилиши натижасида ўзга жиноятлар амалга оширилиши учун шарт-шароит яратиб берилиши, шунингдек, ахборот-коммуникация технологияларига кирмаган воситалар орқали порнографик маҳсулотлар тарқатилиши мумкин.

Шу сабабдан ҳам, ахборот-коммуникация технологиялари (кибертехнологиялар) орқали содир этиладиган киберпорнографиянинг олдини олиш, бу турдаги жиноятлар одатий порнографияга оид жиноятларга қараганда кўпроқ зарар келтириши мумкинлигини, қонунчиликда ягона, аммо эскирмаган тушунчалардан фойдаланиш зарурлигини, бугунги кунда ахборот технологиялари ўзининг техник имкониятлари жиҳатидан ахборот коммуникация технологиялари ёки рақамли технологиялар ёхуд кибертехнологияларни ўзида қамраб ололмастлигини инобатга олиб, кибертехнологик ҳуқуқий асослар талабларидан келиб чиқиб, Ўзбекистон Республикаси Жиноят кодексининг 130-моддаси учинчи қисмини монография 1-иловасининг 7-бандига мувофиқ ўзгартиш киритиш таклиф қилинади.

Киберзўравонлик. Киберзўравонлик жинояти объектив томондан кибертехнологиялар орқали зўравонликни ёки шафқатсизликни тарғиб қилувчи маҳсулотни тарқатиш, реклама қилиш, намойиш этиш ёки шундай мақсадда тайёрлаш ёхуд давлат ҳудудига олиб кириш йўли билан содир этилади ва жамоат одоб-ахлоқи, ёшларнинг нормал ахлоқий ривожланиши, маънавий ва ахлоқ тамойилларни муҳофазаловчи иижтимоий муносабатлар жиноят объектини, 16 ёшга тўлган ақли расо жимоний шахс жиноят субъектини ва тўғри қасд жиноят субъектив томонини ҳамда зўравонлик ва шафқатсизликни тарғиб қилувчи истаган нарса ва буюмлар жиноят предметини ва ахборот-коммуникация технологиялари жиноят воситасини ташкил қилади.

Киберзўравонлик интернет орқали мутассил давом этувчи, такрорий ва узоқ вақт давомида бировнинг шаъни ва кадр-қимматини камситувчи ҳаракатларни амалга оширишда ифодаланади. Бунда, рухий зўравонлик орқали зулм ўтказётган шахс анонимлиги, Интернет орқали ёқимсиз хабарлар тун-у кун кенг оммага тарқалиши билан фарқланиб, жабрланувчига ғоят катта азоб-уқубат келтириши билан бошқа зўравонликлардан кескин фарқланади. Мазкур жиноят Интернет тармоғидан фойдаланиб, иш ёки ўқиш жойи, оилада турли хил ҳақоратлар, тухмат, таъна, миш-мишлар, уйдирма хабарлар тарқатишда ифодаланади. Шунингдек, Интернет ва ижтимоий тармоқлар орқали инсонинг руҳиятига қаттиқ таъсир этувчи, уни изтиробга солувчи бешафқат муносабат ва зўравонлик саҳналарини намойиш этишни ҳам шахсга бўлган зўравонлик, деб эътироф этиш мумкин. Ўзбекистон жиноят кодексининг 130-1-моддасида зўравонликни ёки шафқатсизликни тарғиб қилувчи маҳсулотни тайёрлаш, олиб кириш, тарқатиш, реклама қилиш, намойиш этиш учун жиноий жавобгарлик назарда тутилган бўлиб, бунда жиноятнинг қай йўл орқали содир этилганлиги аҳамиятга олинмаган, бироқ ҳозирги кун талаби ва ахборот соҳасининг ривожини мазкур жиноят моддасини қайта кўриб чиқишни тақозо этади.

Франция жиноят кодексининг 227-24-моддасида инсон кадр-қимматига жиддий зарар етказиши мумкин бўлган ҳар қандай маълумотлардан, зўравон ёки порнографик тусдаги маълумотлардан фойдаланган ҳолда ишлаб чиқариш, ташиш, тарқатиш ёки бундай хабарни сотиш учун жавобгарлик белгиланган ва бунда босма ёки аудиовизуал воситалар ёрдамида содир этилган бўлса, жавобгарликни аниқлаш учун оммавий ахборот воситалари фаолиятини тартибга солувчи қонунларнинг махсус қоидалари қўлланилишлиги кўрсатиб ўтилган, Қозоғистон жиноят кодексининг 134-моддасининг 3-қисми 1-1-бандига асосан, телекоммуникация тармоғи ёки Интернетдан фойдаланган ҳолда вояга етмаган шахсни зўрлик ишлатиб ёки ундан фойдаланиш билан кўрқитиш, ўзига қарам бўлган мавқеидан фойдаланиш, шантаж қилиш, мулкни йўқ қилиш ёки бузиш ёхуд алдаш йўли билан фоҳишалик билан шуғулланиш ҳамда вояга етмаган шахсни фоҳишалikka жалб қилиш учун, 313-моддасида шафқатсизлик ва зўравонлик маданиятини тарғиб қилувчи қонуний равишда тарқатиш ёки реклама қилиш, тарқатиш, реклама қилиш, филм ва видео материаллар ва бошқа асарларни намойиш этиш, шунингдек шафқатсизлик ва зўравонлик маданиятини тарғиб қилувчи босма оммавий ахборот воситаларини, кино ёки видео материалларни ноқонуний сотиш учун жиноий жавобгарлик белгиланган.

Таъкидлаш жоизки, киберзўравонлик жинояти содир этилиши вақтида нафақат жабрланувчи зарар кўриши, балки унга унинг хизмат ёки бошқа компютери орқали зарар келтириши оқибатида, у бошқа шахсларнинг

олдида айбдор бўлиб қолиши, мазкур жиноят содир этилиши натижасида ўзга жиноятлар амалга оширилиши учун шарт-шароит яратиб берилиши, шунингдек, ахборот-коммуникация технологияларига кирмаган воситалар орқали зўравонлик маҳсулотлар тарқатилиши мумкин. Шу сабабдан ҳам, кибертехнологиялар орқали содир этиладиган киберзўравонликнинг олдини олиш, бу турдаги жиноятлар одатий зўравонликка оид жиноятларга қараганда кўпроқ зарар келтириши мумкинлигини, қонунчиликда ягона, аммо эскирмаган тушунчалардан фойдаланиш зарурлигини, бугунги кунда ахборот технологиялари ўзининг техник имкониятлари жиҳатидан кибертехнологияларни ўзида тўлиқ қамраб ололмастлигини инобатга олиб, кибертехнологик ҳуқуқий асослар талабларидан келиб чиқиб, Ўзбекистон Республикаси Жиноят кодексининг 130-1-моддаси иккинчи қисмини монография 1-иловасининг 8-бандига мувофиқ ўзгартиш таклиф қилинади. Мазкур кодексларнинг тўлиқ рўйхати диссертациянинг фойдаланилган адабиётлар рўйхатида берилган.

Киберқўшмачилик. Киберқўшмачилик бутун дунё томонидан ахлоққа қарши қаратилган жиноятларнинг энг юқори чўққисига етишини таъминлайдиган жиноят сифатида таърифланади. Кибермаконда ғаразли ва бошқа паст ниятларда киберқўшмачи ўзининг маҳсулотларини, яъни шахслар доирасини реклама қилади, уларнинг олди-сотдисини амалга оширади, бу орқали пул ишлайди ёхуд ўзга паст ишларни бажариши орқали жамиятга иснод келтиради ва зиён етказди. Ҳозирги кунда киберқўшмачилик кўпайиб кетишига Интернет оламининг тезкорлиги ва маълумот алмашинувининг кундан-кунга ўсаётганлиги, энг муҳими иқтисодий ва ташкилий томондан ушбу жиноятни амалга ошириш хавфсиз бўлганлиги сабаб бўлмоқда.

Ушбу жиноят объектини жамиятда ўрнатилган нормал ахлоқий муҳофаза қилинадиган ижтимоий муносабатлар ташкил этади. Мазкур жиноят фақатгина тўғри қасддан амалга оширилган тақдирда жиноят таркибли сифатида эътироф этилади. Жиноят ғаразли ва бошқа паст ният хусусида манфаатдор шахсга ахборот берилган вақтдан бошлаб, ўртада ўзаро келишув бўлган ёки бўлмаганидан қатъий назар тугалланган ҳисобланади. Жиноят кибертехнологиялар орқали амалга оширилганлиги сабабли жиноятчини топиш жуда мушкулдир. Ҳозирги кунда жиноятчилар уларнинг IP-манзилини (IP-адрес) қидириш ёки сохта манфаатдор шахсларни киберқўшмачилар билан юзма-юз учрашувини ўтказиб, олди-сотдини амалга ошириш вақтида тезкор-қидирув органлари томонидан рейд (тезкор-қидирув) ҳаракатлари амалга оширилган вақтда ушланмоқдалар. Ҳозирги кунда Интернет оламида турли хил веб-сайт сифатида рўйхатдан ўтган ёки ўтмаганлигидан қатъий назар ўзга телекоммуникация воситалари орқали кибержиноятчилар пул ишлаш мақсадида ўзларининг ёки ўзга шахсларнинг шахвоний ҳаракатларини акс эттирувчи ахборотларни тўғридан-тўғри

узатиши орқали жабрланувчиларга зарар келтираётганлигини ҳар қадамда кузатиш мумкин. Мазкур жиноят жиноятчи учун ҳам иқтисодий, ҳам вақт нуқтаи назаридан самарали бўлганлиги, жиноят ўзининг жуда кенг аудитория вакиллари ўзида жалб қилиш имкониятига эга бўлганлиги ва жиноят натижасида келиб чиққан зарар жуда катта бўлиши мумкинлиги, жиноят қонунчилигида ягона тушунча қўлланилиши ҳам қонунийлик, ҳам адолат нуқтаи назаридан зарурлиги, техник жиҳатдан кибертехнологиялар ва ахборот-коммуникация технологиялари жиноят қонунчилигида назарда тутилган технологияларни ўзида тўлиқ қамраб олишлигини инобатга олиб, кибертехнологик ҳуқуқий асослар талабларидан келиб чиқиб, Ўзбекистон Республикаси Жиноят кодекси 131-моддасининг тўртинчи қисмини монография 1-иловасининг 9-бандида назарда тутилган таҳрирда “т” банд билан тўлдириш таклиф қилинади.

Фойдаланилган адабиётлар:

1. Муҳаммад ал-Хоразмий номидаги ТАТУ Фарғона филиали "Ал-Фарғоний авлодлари" электрон илмий журнали ИССН 2181-4252 Том: 1 | Сон: 1 | 2024-йил.
2. Электронный научный журнал "Потомки Аль-Фаргани" Ферганского филиала ТАТУ имени Мухаммада аль-Хоразми ИССН 2181-4252 Том: 1 2024 йил.
3. Турдиматов М.М., Мирзаев Ж.Б. Ахборотни ҳимоялашда ёпиқ виртуал қобиғини лойихалашни математик модели. JOURNAL OF SCIENCE AND INNOVATION.

MUNDARIJA:

KIRISH SO‘ZI.....	2
1. TARMOQ VA DASTURIY TA‘MINOT XAVFSIZLIGINI OSHIRISHDA ILG‘OR HIMOYA VOSITALARINING TAHLILI	5
U.E. RASULEV	
2. КИБЕРЖИНОЯТ НИМА ВА УНДАН ҚАНДАЙ ҲИМОЯЛАНИШ КЕРАК	7
Б.Б. ҚУДРАТОВ	
3. АХБОРОТ-ТЕЛЕКОММУНИКАТСИЯ ТЕХНОЛОГИЯЛАРИДАН FOYDALANIB SODIR ETILAYOTGAN JINOYATLARGA QARSHI KURASHNI TASHKIL ETISH	11
E.E. MARUPOV	
4. ELLIPTIC VOSITALARIDAN КРИПТОВАЛЮТА ТРАНЗАКЦИЯЛАРИНИ ТАҲЛИЛ ҚИЛИШДА ФОЙДАЛАНИШ МАСАЛАСИ	16
X.P. ТУХТАМАТОВ	
5. SUN‘IY INTELLEKTDAN FOYDALANGAN HOLDA АХБОРОТ ТЕХНОЛОГИЯЛАРИ SOHASIDA HUQUQBUZARLIKLARGA QARSHI KURASHNING DOLZARBLIGI VA ISTIQBOLLARI.....	19
Y.B. TASHMANOV	
6. МАЙНИНГ ҚУРИЛМАЛАРИНИНГ ХАВФЛАРИ ВА УЛАРНИ АНИQLASH STRATEGIYALARI.....	23
O.M. BOYNAZAROV	
7. SHAXSIY MA‘LUMOTLARNING O‘G‘IRLANISHI VA ULARNING NOQONUNIY FOYDALANILISHI.....	26
O.M. BOYNAZAROV	
8. INSAYDER TAHDIDLARNI АНИQLASHDA TANLANMANI SHAKLLANTIRISH VA AVTOMATIK SINFLASHTIRISH	28
F.R. MUHAMMADIYEV	
9. АНАЛИЗ ЦИФРОВЫХ СЛЕДОВ В СОЦИАЛЬНЫХ СЕТЯХ	30
Ш.А. ХОЛИКОВ	
10. ANALYSIS OF THE USE OF MODERN GAME BASED TECHNOLOGY IN THE STUDYING PROCESS.....	34
M.B. TURSUNOVA	
11. RAQAMLI DUNYONING ASOSI KIBERXAVFSIZLIK MUHOFAZASINING (HACKZONE) АНАМИЯТИ	37
L.E. SAATOVA	
12. КИБЕРЖИНОЯТЧИЛИКНИ RIVOJLANISHIDA DARKNETNING O‘RNI	42
J.D. RISQALIYEV	

13. AXBOROT TEXNOLOGIYALARIDAN FOYDALANGAN HOLDA SODIR ETILADIGAN HUQUQBUZARLIKLARGA QARSHI KURASHISHNING DOLZARB MUAMMOLARI VA YECHIMLARI.....	46
<i>N.O. ODILOV</i>	
14. AXBOROT TEXNOLOGIYALARIDAN FOYDALANGAN HOLDA DRONLARDAN HUQUQBUZARLIKNI ANIQLASH YECHIMLARI.....	49
<i>A.A. ABDIRAXIMOV</i>	
15. KIBERXAVFSIZLIKNI OLDINI OLISHGA DOIR AYRIM TUSHUNCHALAR	51
<i>I.N. BUTAYEV</i>	
16. AXBOROT TEXNOLOGIYALARI YORDAMIDA JINOYATLARNI OLDINI OLISH ...	54
<i>X.N. MUSLIMOV</i>	
17. KIBERXAVFSIZLIK SOHASIDAGI DOLZARB MUAMMOLAR VA ULARNI HAL ETISH YO‘LLARI	56
<i>SH.K. RAXIMOV</i>	
18. AXBOROT TEXNOLOGIYALARIDAN FOYDALANGAN HOLDA SODIR ETILADIGAN HUQUQBUZARLIKLARNING OLIDINI OLISH MASALALARI	60
<i>K.S. BEYSENOV</i>	
19. СУНЬИЙ ИНТЕЛЛЕКТНИНГ ҲАЁТИМИЗДАГИ АҲАМИЯТИ.....	66
<i>H.3. TACIMOV</i>	
20. KIBERJINOYATLARGA QARSHI KURASHISHDA ZAMONAVIY TEXNOLOGIYALARNING ROLI: SUN'YIY INTELLEKT VA BLOKCHEYN TEXNOLOGIYALARI	69
<i>X.N. MUSLIMOV</i>	
21. JINOYATCHILARNING YASHIRINGAN JOYLARINI AXBOROT TEXNOLOGIYALARI YORDAMIDA ANIQLASH USULI.....	75
<i>H.N. O'RINXOJAYEV</i>	
22. OLIY TA'LIM MUASSASALARIDA LOYIHAVIY BOSHQARUVNI JORIY ETISH ZARURATI.....	77
<i>F.B. MATYAQUBOVNA</i>	
23. AXBOROT TEXNOLOGIYALARIDAN FOYDALANGAN HOLDA SODIR ETILADIGAN GIYOHVANDLIK VOSITALARI YOKI PSIXOTROP MODDALAR BILAN QONUNGA XILOF RAVISHDA MUOMILA QILISHGA OID JINOYATLARNI TERGOV QILISHNING AYRIM JIXATLARI	81
<i>O.S. SUBANOV</i>	
24. AXBOROT-KOMMUNIKATSIYA TEXNOLOGIYALARIDAN FOYDALANGAN HOLDA ICHKI ISHLAR ORGANLARINING INSON HUQUQLARINI HIMOYA QILISH SOHASIDA NODAVLAT NOTIJORAT TASHKILOTLARI BILAN SAMARALI HAMKORLIGINI YO'LGA QO'YISH MEXANIZMLARI	88

J.O. KENJAYEV

25. ТОШКЕНТ МЕТРОПОЛИТЕНИДА ЖАМОАТ ХАВФСИЗЛИГИ ВА
ҲУҚУҚБУЗАРЛИКЛАР ПРОФИЛАКТИКАСИНИ ТАЪМИНЛАШДА ЗАМОНАВИЙ
ТЕХНОЛОГИЯЛАРНИНГ ЎРНИ94

Б.И. ИСЛОМБЕКОВ

26. МЕТРОПОЛИТЕНДА ЖАМОАТ ТАРТИБИ ВА ФУҚАРОЛАР ХАВФСИЗЛИГИНИ
ТАЪМИНЛАШ ҲАМДА ҲУҚУҚБУЗАРЛИКЛАРНИНГ ОЛДИНИ ОЛИШДА СУНЪИЙ
ИНТЕЛЛЕКТДАН ФОЙДАЛАНИШНИНГ АФЗАЛЛИКЛАРИ97

Б.И. ИСЛОМБЕКОВ

27. КИБЕРЖИНОЯТНИ ОЛДИНИ ОЛИШ ЙЎЛЛАРИ.....101

А.С. ВАХИДОВ

28. АХБОРОТ ТЕХНОЛОГИЯЛАРИДАН ФОЙДАЛАНГАН HOLDA SODIR
ETILADIGAN HUQUQBUZARLIKLAR UCHUN MA’MURIY JAVOBGARLIK.....106

Х.Х. ВАХРАМОВ

29. АХБОРОТ ТЕХНОЛОГИЯЛАРИ SOHASIDAGI HUQUQBUZARLIKLARNING
HUQUQIY ASOSLARI112

Х.Х. ВАХРАМОВ, О.С. SUBANOV

30. АХБОРОТ ТЕХНОЛОГИЯЛАРИДАН ФОЙДАЛАНГАН HOLDA SODIR
ETILADIGAN HUQUQBUZARLIKLARNING OLDINI OLISHDA SUN’IY
INTELLEKTNING O‘RNI118

К.С. БЕЙСЕНОВ

31. АХБОРОТ МАКОНИДА ЕКСТРЕМИЗМ ВА РАДИКАЛИЗМ: JISMONIY
TAYYORGARLIK VA SPORT ORQALI IMMUNITETNI SHAKLLANTIRISH122

В.Н. BURXONOV

32. JAMOAT XAVFSIZLIGINI TA’MINLASHDA MAFKURAVIY TAHDIDLARGA
QARSHI KURASHISH MEKANIZMLARINI TAKOMILLASHTIRISH125

G.S. RO‘ZIYEVA

33. MAFKURAVIY TAHDIDLARNING JAMIYAT RIVOJIGA SALBIY JIHATLARI.....132

G.S. RO‘ZIYEVA

34. IJTIMOIY TARMOQLARDAGI FIRIBGARLIK DOLZARB MUAMMOLAR VA
ULARGA QARSHI KURASHISH USULLARI137

М.А. TURAYEV

35. КИБЕРПРЕСТУПНОСТЬ В ЦИФРОВУЮ ЭПОХУ: ТЕНДЕНЦИИ РАЗВИТИЯ,
ПРОБЛЕМЫ И МЕХАНИЗМЫ ПРОТИВОДЕЙСТВИЯ141

Ш.А. АЛБЕКОВ

36. АХБОРОТ ТЕХНОЛОГИЯЛАРИ ВА ХАВФСИЗЛИГИ СОҲАСИДАГИ
ЖИНОЯТЛАРНИНГ ОЛДИНИ ОЛИШНИНГ ЎЗИГА ХОС ХУСУСИЯТЛАРИ.....145

Ш.М. УБАЙДУЛЛАЕВ

37. ЯНГИ ЎЗБЕКИСТОНДА РАҚАМЛИ ИҚТИСОДИЁТ	150
<i>Ш.М. УБАЙДУЛЛАЕВ</i>	
38. АХБОРОТ ТЕХНОЛОГИЯЛАРИ SOHASIDAGI JINOYATLAR: XAVF, SABAB VA YECHIMLAR	154
<i>Z.M. ALIYEVA</i>	
39. КИБЕР МАКОНДА СОДИР БЎЛАЁТГАН ЖИНОЯТЛАРГА ҚАРШИ КУРАШИШНИНГ АЙРИМ ХУСУСИЯТЛАРИ.....	157
<i>З.Р. УМАРОВ</i>	
40. АХБОРОТ ТЕХНОЛОГИЯЛАРИ SOHASIDAGI JINOYATLARNI OLDINI OLIISH MUAMMOLARI VA YECHIM YO'LLARI	161
<i>О'М. ОТАҲЕВ</i>	
41. АХБОРОТ ТЕХНОЛОГИЯЛАРИДАН FOYDALANGAN HOLDA SODIR ETILADIGAN JINOYATLAR UCHUN JAVOBGARLIK MASALALARI	163
<i>SH.X. G'ANIYEV</i>	
42. INTERNET XURUJLARIDAN VOYAGA YETMAGANLARNI ASRASH DOLZARB VAZIFA	168
<i>E.T. XUSHVAQTOV</i>	
43. СОВУҚ ҚУРОЛЛАР ВА СОВУҚ ҚУРОЛ СИФАТИДА ФОЙДАЛАНИШ МУМКИН БЎЛГАН АШЁЛАРНИНГ ТАКТИК-ТЕХНИК ХУСУСИЯТЛАРИГА КЎРА ҲУҚУҚИЙ МАЛАКАЛАШНИНГ АЙРИМ MASALALARI	172
<i>Ш.Н. ЮЛДАШЕВ</i>	
44. ZARARLI АХБОРОТЛАРНИНГ YOSHLAR O'RTASIDA TARQALISHINI OLDINI OLIISH	179
<i>Q.A. YULDASHEV</i>	
45. KIBERJINOYATLARDAN NIHOYA QILISHDA AI ALGORITMLARINING ROLI ...	183
<i>Y.B. TASHMANOV, E.E. KANAYEV</i>	
46. АХБОРОТ ТЕХНОЛОГИЯЛАРИДАН ФОЙДАЛАНГАН ҲОЛДА СОДИР ЭТИЛГАН АХЛОҚҚА ҚАРШИ ҚАРАТИЛГАН ЖИНОЯТЛАР УЧУН ЖАВОБГАРЛИК.....	184
<i>Б.Б. ТУРҒУНБАЕВ</i>	

O‘zbekiston Respublikasi Ichki ishlar vazirligi Malaka oshirish instituti

**AXBOROT TEXNOLOGIYALARIDAN FOYDALANGAN
HOLDA SODIR ETILADIGAN HUQUQBUZARLIKLARGA
QARSHI KURASHISHNING DOLZARB MUAMMOLARI VA
YECHIMLARI**

Respublika ilmiy-amaliy konferensiya materiallari to‘plami

Toshkent 2025-yil 26-iyun

TAHRIRIYAT A‘ZOLARI:

E.E. Marupov, Y.B. Tashmanov, J.D. Risqaliyev, O.M. Boynazarov,
A.A. Abdiraximov

Bosishga ruxsat etildi 30.06.2025-y. Nashriyot-hisob tabog‘i 12.
Adadi 10-nusxa. Buyurtma № ____. Bahosi shartnoma asosida

O‘zbekiston Respublikasi IIV Malaka oshirish instituti,
100213. Toshkent shahar. Husayn Boyqaro ko‘chasi, 27a-uy.