

**KIBERJINOYATCHILIKKA QARSHI KURASHISHDA ICHKI ISHLAR ORGANLARINING O'RNI**

mayor O.Mustafayev
Jizzax mintaqaviy o'quv markazi
Jismoniy va jangovar tayyorgarlik
sikli katta o'qtuvchisi.

Annotatsiya: Maqolada zamonaviy raqamli muhitda kiberjinoyat-chilikka qarshi kurashishda ichki ishlar organlarining o'rni, vazifalari va faoliyat yo'nalishlari tahlil qilingan. Kiberjinoyatlarning o'ziga xos xususiyatlari, ularni aniqlash va fosh etishda raqamli texnologiyalarning ahamiyati, elektron dalillar bilan ishlash, fuqarolar o'rtasida kiberxavfsizlik madaniyatini shakllantirish, huquqbuzarliklarning barvaqt oldini olish hamda bank-moliya tashkilotlari va boshqa vakolatli idoralar bilan hamkorlik masalalari yoritilgan.

Kalit so'zlar: kiberjinoyatchilik, kiberxavfsizlik, raqamli texnologiyalar, elektron dalillar, internet firibgarligi, profilaktika, raqamli muhit, axborot xavfsizligi, idoralararo hamkorlik.

Аннотация: В статье проанализированы роль, задачи и основные направления деятельности органов внутренних дел в борьбе с киберпреступностью в современной цифровой среде. Освещены особенности киберпреступлений, значение цифровых технологий в их выявлении и раскрытии, вопросы работы с электронными доказательствами, формирования культуры кибербезопасности среди граждан, раннего предупреждения правонарушений, а также взаимодействия с банковско-финансовыми организациями и другими уполномоченными органами.

Ключевые слова: киберпреступность, кибербезопасность, цифровые технологии, электронные доказательства, интернет-мошенничество, профилактика, цифровая среда, информационная безопасность, межведомственное взаимодействие.

Abstract: The article analyzes the role, tasks, and main areas of activity of internal affairs bodies in combating cybercrime in the modern digital environment. It examines the specific characteristics of cybercrimes, the importance of digital technologies in their detection and investigation, the handling of electronic evidence, the development of a culture of cybersecurity among citizens, the early prevention of offenses, as well as cooperation with banking and financial organizations and other authorized agencies.

Keywords: cybercrime, cybersecurity, digital technologies, electronic evidence, Internet fraud, prevention, digital environment, information security, interagency cooperation.

XXI asrda raqamli texnologiyalarning jadal rivojlanishi ijtimoiy munosabatlarning deyarli barcha sohalariga ta'sir ko'rsatmoqda. Davlat boshqaruvi,



bank-moliya tizimi, ta'lim, tibbiyot, savdo, transport va boshqa sohalarda raqamli texnologiyalardan keng foydalanilayotgani jamiyat hayotini ancha yengillashtirmoqda.

Biroq raqamlashtirish jarayoni bilan bir vaqtda yangi turdagi xavf va tahdidlar ham paydo bo'lmoqda. Jumladan, axborot texnologiyalaridan foydalanib sodir etiladigan jinoyatlar soni va shakllari kengayib, kiberjinoyatchilik huquqni muhofaza qiluvchi organlar oldiga yangi vazifalarni qo'ymoqda.

Kiberjinoyatchilikning o'ziga xos jihati shundaki, jinoyat sodir etuvchi shaxs va jabrlanuvchi turli hududlarda bo'lishi, jinoyat izlari esa raqamli muhitda qolishi mumkin. Shu sababli bunday jinoyatlarni aniqlash, hujjatlashtirish va fosh etish an'anaviy jinoyatlarga nisbatan o'ziga xos yondashuvni talab qiladi.

O'zbekistonda ham kiberjinoyatchilikka qarshi kurashish masalasi davlat siyosatining muhim yo'nalishlaridan biriga aylanmoqda. Xususan, 2025 yil 30 iyuldagi Prezident qarori bilan Ichki ishlar vazirligi mamlakatda kiberjinoyatlarga qarshi kurashish yo'nalishida yagona ishlash amaliyotini tashkil etish, mas'ul davlat organlari faoliyatini muvofiqlashtirish va manzilli hamkorlikni ta'minlash bo'yicha vakolatli organ etib belgilangan.

2026-yilda Ichki ishlar vazirligi tizimida kiberjinoyatchilikka qarshi kurashish va aholining kiberxavfsizlik madaniyatini oshirish masalalariga alohida e'tibor qaratilmoqda. IIVning rasmiy ma'lumotlarida ichki ishlar organlari xodimlarining kiberxavfsizlik sohasidagi bilim va ko'nikmalarini muntazam oshirish, zamonaviy texnologiyalar hamda kiberjinoyatlarni aniqlash va ularga qarshi kurashishning yangi usullarini o'zlashtirish vazifalari belgilangan.

Shu sababli kiberjinoyatchilikka qarshi kurashishda ichki ishlar organlarining vazifalarini ilmiy-nazariy va amaliy nuqtai nazardan o'rganish dolzarb ahamiyat kasb etadi.

1. Kiberjinoyatchilik tushunchasi va uning o'ziga xos xususiyatlari

Kiberjinoyatchilik - axborot-kommunikatsiya texnologiyalari, kompyuter tizimlari, telekommunikatsiya tarmoqlari yoki raqamli platformalardan foydalanish bilan bog'liq holda sodir etiladigan jinoiy qilmishlar majmuidir.

Kiberjinoyatlar turli shakllarda namoyon bo'lishi mumkin. Ularga internetdagi firibgarlik, kompyuter ma'lumotlariga qonunga xilof ravishda kirish, elektron to'lovlar bilan bog'liq jinoiy harakatlar, zararli dasturlardan foydalanish, shaxsiy ma'lumotlardan noqonuniy foydalanish kabi qilmishlar kiradi.

Kiberjinoyatchilikning asosiy xususiyatlarini quyidagicha ifodalash mumkin:

Birinchidan, jinoyat sodir etiladigan muhit virtual xususiyatga ega.

Ikkinchidan, jinoyatchi shaxs o'z shaxsini yashirish yoki turli raqamli vositalar orqali izlarni murakkablashtirishga harakat qilishi mumkin.

Uchinchidan, jinoyat natijasida yetkazilgan zarar bir shaxs bilan cheklanmasdan, ko'plab fuqarolar yoki tashkilotlarga ta'sir qilishi mumkin.

To'rtinchidan, jinoyat izlarining muhim qismi elektron shaklda mavjud bo'ladi.



Beshinchidan, jinoyatni sodir etish va uning oqibatlari turli hududlarda yuzaga kelishi mumkin.

Mazkur xususiyatlar ichki ishlar organlarining kiberjinoyatchilikka qarshi kurashishda zamonaviy texnik vositalar, maxsus bilim va xalqaro hamkorlik mexanizmlaridan foydalanishini taqozo etadi.

2. Ichki ishlar organlarining kiberjinoyatchilikka qarshi kurashishdagi huquqiy asoslari

Kiberjinoyatchilikka qarshi kurashish O'zbekiston Respublikasining Konstitutsiyasi, Jinoyat kodeksi, Jinoyat-protsessual kodeksi, "Ichki ishlar organlari to'g'risida"gi Qonun, "Kiberxavfsizlik to'g'risida"gi Qonun va boshqa normativ-huquqiy hujjatlar asosida amalga oshiriladi.

Kiberxavfsizlikni ta'minlashda davlat organlari, tashkilotlar va boshqa sub'ektlarning huquq va majburiyatlarini belgilashga qaratilgan huquqiy mexanizmlar ham shakllantirilmoqda.

2025-yilda qabul qilingan Prezident qarorlaridan birida Ichki ishlar vazirligi kiberjinoyatlarga qarshi kurashish sohasida yagona ishlash amaliyotini yo'lga qo'yish va davlat organlari hamda boshqa mas'ul tashkilotlar o'rtasida hamkorlikni muvofiqlashtirish bo'yicha vakolatli organ sifatida belgilandi. Shu qarorda kiberjinoyatlarning oldini olish, aholining kibermadaniyatini oshirish va bank-moliya sektorining xavfsizligini ta'minlashga qaratilgan choralar ham nazarda tutilgan.

2026-yilda parlament darajasida ham kiberjinoyatchilikka qarshi kurashish mexanizmlarini kuchaytirish masalasi muhokama qilinmoqda. Qonunchilik palatasi materiallarida Ichki ishlar vazirligiga ushbu sohada davlat siyosatini muvofiqlashtirish, profilaktika ishlarini tashkil etish, huquqbuzarliklarni fosh etish va vakolatli idoralar o'rtasida hamkorlikni ta'minlashga qaratilgan aniq vakolatlar berish nazarda tutilgani qayd etilgan.

Bu holat kiberjinoyatchilikka qarshi kurashishda ichki ishlar organlarining vazifalari faqat jinoyatni fosh etish bilan cheklanmasdan, profilaktika, tahlil, muvofiqlashtirish va aholi bilan ishlashni ham qamrab olishini ko'rsatadi.

3. Kiberjinoyatlarning oldini olish - ichki ishlar organlarining muhim vazifasi

Kiberjinoyatchilikka qarshi samarali kurashishda profilaktika alohida o'rin tutadi.

Aksariyat kiberjinoyatlar fuqarolarning raqamli xavfsizlik qoidalariga yetarli darajada rioya qilmasligi, firibgarlik usullarini yaxshi bilmasligi yoki shaxsiy ma'lumotlarini himoya qilishda ehtiyotsizligi natijasida osonlashishi mumkin.

Shu sababli ichki ishlar organlari aholi o'rtasida kiberxavfsizlik madaniyatini oshirishga qaratilgan profilaktik tadbirlarni tizimli tashkil etishi zarur.

Bunday tadbirlar quyidagi yo'nalishlarda amalga oshirilishi mumkin:

- aholiga internetdagi xavflar haqida tushuntirish;



- keng tarqalgan firibgarlik usullari haqida ogohlantirish;
- shaxsiy ma'lumotlarni himoya qilish bo'yicha tavsiyalar berish;
- yoshlar o'rtasida raqamli xavfsizlik bo'yicha targ'ibot olib borish;
- ta'lim muassasalari bilan hamkorlik qilish;
- bank va to'lov tashkilotlari bilan profilaktik tadbirlarni tashkil etish;
- ijtimoiy tarmoqlarda ogohlantiruvchi materiallarni tarqatish.

2026-yilda IIVning rasmiy materiallarida kiberjinoyatlarning oldini olish, aholi o'rtasida kiberxavfsizlik madaniyatini yuksaltirish va fuqarolarni internetdagi xavflardan ogohlantirishga qaratilgan profilaktik tadbirlar kuchaytirilayotgani qayd etilgan.

Demak, profilaktika ichki ishlar organlarining kiberjinoyatchilikka qarshi kurashishdagi eng muhim strategik vazifalaridan biri hisoblanadi.

4. Kiberjinoyatlarni aniqlash va fosh etish

Ichki ishlar organlarining asosiy vazifalaridan biri sodir etilgan kiberjinoyatlarni o'z vaqtida aniqlash va fosh etishdan iborat.

Kiberjinoyatlarni aniqlashda raqamli izlar, elektron ma'lumotlar, internetdagi faollik, moliyaviy operatsiyalar va boshqa raqamli ma'lumotlar muhim ahamiyat kasb etadi.

Bunday jinoyatlarni fosh etish jarayonida quyidagi vazifalar muhim hisoblanadi:

- jinoyat haqidagi xabar va murojaatlarni qabul qilish;
- dastlabki ma'lumotlarni tekshirish;
- raqamli izlarni aniqlash;
- elektron dalillarni protsessual talablar asosida mustahkamlash;
- jinoyat sodir etish usulini aniqlash;
- jinoyatga aloqador shaxslarni aniqlash;
- moliyaviy operatsiyalarni tahlil qilish;
- tegishli tashkilotlardan qonuniy tartibda axborot olish;
- tergov va tezkor-qidiruv tadbirlarini amalga oshirish;
- jinoyat ishi bo'yicha dalillarni umumlashtirish.

Kiberjinoyatlarni fosh etishda texnik bilimga ega mutaxassislar bilan tergovchilarning hamkorligi muhim ahamiyatga ega.

5. Elektron dalillar bilan ishlash

Kiberjinoyatchilikka qarshi kurashishda elektron dalillar markaziy o'rinlardan birini egallaydi.

Elektron dalil sifatida kompyuter, telefon, elektron pochta, internet akkauntlari, elektron to'lovlar, raqamli fayllar va boshqa axborot manbalarida saqlanadigan ma'lumotlar ahamiyat kasb etishi mumkin.



IQTIDOR & INTELLEKT

Biroq elektron dalillar bilan ishlashda ularning haqiqiyligi, yaxlitligi va protsessual tartibda olinganligi muhim.

Shu sababli ichki ishlar organlari xodimlari:

- raqamli ma'lumotlarni aniqlash;
- ularni saqlash;
- nusxalash;
- tahlil qilish;
- o'zgarishlardan himoyalash;
- protsessual hujjatlarda to'g'ri qayd etish bo'yicha maxsus bilim va ko'nikmalarga ega bo'lishi lozim.

Kiberjinoyatchilikning rivojlanishi tergov amaliyotida raqamli kriminalistika usullaridan kengroq foydalanish zaruratini keltirib chiqarmoqda.

6. Internet firibgarligiga qarshi kurashish

So'nggi yillarda internet va elektron to'lov xizmatlaridan foydalanishning kengayishi moliyaviy firibgarlikning raqamli shakllariga ham yangi imkoniyatlar yaratmoqda.

Internet firibgarligida fuqarolarning ishonchiga kirish, soxta xabarlar yuborish, qalbaki internet sahifalaridan foydalanish yoki boshqa aldash usullari qo'llanishi mumkin.

Bunday jinoyatlarga qarshi kurashishda ichki ishlar organlarining banklar, to'lov tashkilotlari va telekommunikatsiya sohasi sub'ektlari bilan hamkorligi muhim.

2025-yilgi Prezident qarorida banklar, to'lov tizimi operatorlari va to'lov tashkilotlarining kiberjinoyatlarning oldini olish va mijozlarning moliyaviy xavfsizligini ta'minlashdagi mas'uliyatiga alohida e'tibor qaratilgan.

2026-yilda IIVning rasmiy hisobotida Markaziy bank bilan hamkorlikda tashkil etilgan maxsus tizim natijasida jinoiy faoliyat bilan bog'liq bank kartalarini bloklash va katta miqdordagi mablag'larning noqonuniy chiqib ketishining oldini olish bo'yicha natijalar qayd etilgan.

Bu amaliyot kiberjinoyatchilikka qarshi kurashishda ichki ishlar organlari va moliyaviy institutlar o'rtasidagi tezkor axborot almashinuvi qanchalik muhimligini ko'rsatadi.

7. Idoralararo hamkorlikni ta'minlash

Kiberjinoyatchilik transchegaraviy va ko'p tarmoqli xususiyatga ega bo'lgani sababli uning oldini olish va fosh etishda bitta davlat organining harakati yetarli bo'lmasligi mumkin.

Shu sababli ichki ishlar organlari:

- prokuratura;
- sud organlari;
- Markaziy bank;



- Raqamli texnologiyalar sohasidagi vakolatli organlar;
- banklar;
- to'lov tashkilotlari;
- telekommunikatsiya operatorlari;
- ta'lim muassasalari;
- xalqaro tashkilotlar bilan hamkorlik qilishi muhim.

2026-yil mart oyida Oliy Majlis Qonunchilik palatasida kiberjinoyatchilikka qarshi kurashish masalalari muhokama qilinganda ichki ishlar organlari bilan bir qatorda Markaziy bank, ta'lim sohasidagi vazirliklar, Raqamli texnologiyalar vazirligi va boshqa sub'ektlar ishtirok etgani ham sohada kompleks hamkorlik zarurligini ko'rsatadi.

8. Aholining kiberxavfsizlik madaniyatini oshirish

Kiberjinoyatchilikka qarshi kurashishning yana bir muhim yo'nalishi aholining raqamli savodxonligini oshirishdir.

Ichki ishlar organlarining profilaktik faoliyati faqat huquqbuzarlik sodir etgan shaxslarga nisbatan chora ko'rishdan iborat bo'lmasligi kerak.

Aholiga:

- shaxsiy ma'lumotlarni himoya qilish;
- shubhali xabarlariga ishonmaslik;
- elektron to'lovlarda xavfsizlik qoidalariga rioya qilish;
- notanish manbalarga maxfiy ma'lumotlarni bermaslik;
- internetdagi firibgarlik alomatlarini tanish;
- shubhali holatlarda vakolatli organlarga murojaat qilishkabi masalalar bo'yicha tushuntirish ishlari olib borilishi zarur.

IIV Kiberjinoyatlarga qarshi kurashish departamentining rasmiy ijtimoiy tarmoq sahifalarida kiberxavfsizlik bo'yicha tavsiyalar, ogohlantirishlar va profilaktik materiallar muntazam e'lon qilinishi ham mazkur vazifaning amaliy ko'rinishlaridan biridir.

9. Kiberjinoyatlarga qarshi kurashishda kadrlar masalasi

Kiberjinoyatchilikka qarshi samarali kurashish professional kadrlarni talab qiladi.

An'anaviy yuridik bilimlar bilan bir qatorda ichki ishlar organlari xodimi:

- axborot texnologiyalari;
- kompyuter tarmoqlari;
- raqamli kriminalistika;
- elektron dalillar;
- kiberxavfsizlik;
- ma'lumotlarni tahlil qilish;



zamonaviy raqamli platformalar bo'yicha yetarli bilimga ega bo'lishi lozim. 2026-yil avgust oyida IIV tizimida kiberxavfsizlik sohasida xodimlarning bilim va ko'nikmalarini muntazam oshirish, zamonaviy axborot texnologiyalari hamda

kiberjinoyatlarni aniqlash va ularga qarshi kurashishning yangi usullarini o'rganish zarurligi alohida ta'kidlangan.

Shu nuqtai nazardan ichki ishlar organlarida kiberjinoyatchilikka qarshi kurashish bo'yicha ixtisoslashgan mutaxassislarni tayyorlash va qayta tayyorlash tizimini rivojlantirish maqsadga muvofiq.

10. Kiberjinoyatchilikka qarshi kurashishda raqamli tahlilning ahamiyati

Zamonaviy kiberjinoyatchilikka qarshi kurashishda ma'lumotlarni tahlil qilish texnologiyalaridan samarali foydalanish muhim.

Jinoyatlar haqidagi ma'lumotlarni tahlil qilish orqali:

- jinoyat sodir etishdagi umumiy tendensiyalar;
- foydalanilayotgan usullar;
- jinoyatlarning hududiy xususiyatlari;
- takroriy jinoyatlar;
- shubhali moliyaviy operatsiyalar;
- xavf guruhlari aniqlanishi mumkin.

Bu esa ichki ishlar organlariga profilaktik choralarni oldindan belgilash imkonini beradi.

Shuning uchun kiberjinoyatchilikka qarshi kurashishda "jinoyat sodir bo'lgandan keyin harakat qilish" modeli bilan bir qatorda "xavfni oldindan aniqlash va uning oldini olish" modeliga bosqichma-bosqich o'tish maqsadga muvofiq.

11. Xalqaro hamkorlikni rivojlantirish

Kiberjinoyatchilikning muhim xususiyatlaridan biri uning davlat chegaralarini tan olmasligidir.

Jinoyatchi bir mamlakatda, jabrlanuvchi boshqa mamlakatda, raqamli infratuzilma esa uchinchi mamlakatda joylashgan bo'lishi mumkin.

Bunday sharoitda kiberjinoyatlarni fosh etish uchun xalqaro hamkorlik muhim ahamiyatga ega.

Ichki ishlar organlarining xalqaro hamkorligi:

- axborot almashinuvi;
- jinoyatchilarni aniqlash;
- elektron dalillarni olish;
- transchegaraviy jinoyatlarni tergov qilish;
- xalqaro qidiruv;
- mutaxassislar tajribasini almashishkabi yo'nalishlarda amalga oshirilishi mumkin.



Bu borada xalqaro standartlarni milliy amaliyotga moslashtirish ham muhim vazifalardan biri hisoblanadi.

12. Kiberjinoyatchilikka qarshi kurashishdagi asosiy muammolar

Mavjud amaliyotni tahlil qilish asosida kiberjinoyatchilikka qarshi kurashishda quyidagi muammolarni ajratish mumkin.

Birinch muammo - kiberjinoyat usullarining tez o'zgarishi.

Jinoyatchilar yangi texnologiya va raqamli xizmatlardan foydalangan holda yangi usullarni qo'llashi mumkin.

Ikkinchi muammo - malakali kadrlarga ehtiyoj.

Kiberjinoyatlarni tergov qilish yuridik bilim bilan bir qatorda maxsus texnik bilimni talab qiladi.

Uchinchi muammo - elektron dalillarning o'ziga xosligi.

Raqamli ma'lumotlarni to'g'ri olish, saqlash va protsessual jihatdan mustahkamlash muhim.

To'rtinchi muammo - jinoyatlarning transchegaraviy xususiyati.

Kiberjinoyatlarning bir qismi xorijiy raqamli infratuzilmalardan foydalangan holda sodir etilishi mumkin.

Beshinchi muammo - aholining raqamli xavfsizlik bo'yicha bilimlari yetarli emasligi.

Fuqarolarning kiberxavfsizlik madaniyatini oshirish profilaktikaning muhim shartidir.

13. Ichki ishlar organlari faoliyatini takomillashtirish bo'yicha takliflar

Yuqoridagi tahlillar asosida quyidagi ilmiy-amaliy takliflarni ilgari surish mumkin.

1. Ixtisoslashgan kadrlar tayyorlashni kuchaytirish. Kiberjinoyatchilikka qarshi kurashish bo'yicha maxsus o'quv dasturlarini kengaytirish, xodimlarni muntazam qayta tayyorlash va ularning raqamli kompetensiyalarini oshirish zarur.

2. Raqamli kriminalistika imkoniyatlarini kengaytirish. Elektron dalillarni aniqlash, yig'ish, saqlash va tahlil qilish bo'yicha zamonaviy laboratoriyalar va mutaxassislar salohiyatini rivojlantirish maqsadga muvofiq.

3. Idoralararo tezkor axborot almashinuvini takomillashtirish. Ichki ishlar organlari, banklar, to'lov tashkilotlari va boshqa vakolatli sub'ektlar o'rtasida qonuniy va himoyalangan axborot almashinuvi mexanizmlarini rivojlantirish zarur.

4. Kiberjinoyatlarni prognoz qilish tizimini joriy etish. Jinoyatlar statistikasi va boshqa qonuniy manbalardagi ma'lumotlarni tahlil qilish asosida xavflarni oldindan aniqlash mexanizmlarini rivojlantirish lozim.

5. Aholining kiberxavfsizlik madaniyatini oshirish. Profilaktik materiallarni faqat rasmiy tadbirlar doirasida emas, balki ommaviy axborot vositalari, ta'lim muassasalari va raqamli platformalar orqali muntazam yetkazish kerak.

6. Jabrlangan fuqarolar bilan ishlash mexanizmlarini takomillashtirish. Kiberjinoyat qurbonlariga huquqiy axborot berish, murojaatlarni tezkor ko'rib



IQTIDOR & INTELLEKT

chiqish **JURNALI** buzilgan huquqlarni tiklashga ko'maklashish tizimini yanada takomillashtirish maqsadga muvofiq.

7. Kiberjinoyatchilik bo'yicha yagona tahliliy bazani rivojlantirish. Hududlar va jinoyat turlari kesimida ma'lumotlarni tahlil qilish ichki ishlar organlarining profilaktik faoliyatini yanada manzilli tashkil etish imkonini beradi.

Xulosa. Kiberjinoyatchilik raqamli iqtisodiyot va axborot texnologiyalari rivojlanishi sharoitida jamiyat xavfsizligiga ta'sir ko'rsatuvchi muhim tahdidlardan biri sifatida namoyon bo'lmoqda.

Uning o'ziga xosligi jinoyatlarning raqamli muhitda sodir etilishi, elektron izlarning mavjudligi, jinoyatchilarning masofadan harakat qilishi va ayrim hollarda transchegaraviy xususiyat kasb etishi bilan izohlanadi.

Shu sababli ichki ishlar organlarining kiberjinoyatchilikka qarshi kurashishdagi vazifalari ham kengayib bormoqda.

Bugungi kunda mazkur vazifalarni shartli ravishda kiberjinoyatlarning oldini olish, aniqlash, fosh etish, elektron dalillar bilan ishlash, aholining kiberxavfsizlik madaniyatini oshirish, idoralararo hamkorlikni ta'minlash va zamonaviy raqamli texnologiyalardan foydalanish kabi asosiy yo'nalishlarga ajratish mumkin.

O'zbekistonda 2025-yildan boshlab kiberjinoyatchilikka qarshi kurashish bo'yicha yagona ishlash amaliyotini yo'lga qo'yish va ichki ishlar organlarining mazkur sohadagi muvofiqlashtiruvchi rolini kuchaytirishga qaratilgan choralar belgilangan. 2026-yilda esa ichki ishlar organlari xodimlarining kiberxavfsizlik sohasidagi bilim va ko'nikmalarini oshirish, aholi o'rtasida kiberxavfsizlik madaniyatini yuksaltirish hamda profilaktik tadbirlarni kuchaytirish vazifalariga alohida e'tibor berilmoqda.

Fikrimizcha, kelgusida kiberjinoyatchilikka qarshi kurashish samaradorligini oshirishning eng muhim shartlari - malakali kadrlar tayyorlash, raqamli kriminalistikani rivojlantirish, elektron dalillar bilan ishlash amaliyotini takomillashtirish, idoralararo axborot almashinuvini kuchaytirish va profilaktik ishlarni manzilli tashkil etishdan iborat.

Eng muhimi, kiberjinoyatchilikka qarshi kurashishni faqat jinoyat sodir etilgandan keyingi huquqiy ta'sir choralari bilan cheklamasdan, xavflarni barvaqt aniqlash va ularning oldini olishga yo'naltirish zarur.

Shunday yondashuv ichki ishlar organlarining jamoat xavfsizligini ta'minlashdagi rolini kuchaytirish, fuqarolarning raqamli huquqlarini himoya qilish va O'zbekistonning raqamli makonida xavfsiz muhitni shakllantirishga xizmat qiladi.



Foydalanilgan adabiyotlar

- 1.O‘zbekiston Respublikasining Konstitutsiyasi. — Toshkent, 2023.
- 2.O‘zbekiston Respublikasining Jinoyat kodeksi.
- 3.O‘zbekiston Respublikasining Jinoyat-protsessual kodeksi.
- 4.O‘zbekiston Respublikasining “Ichki ishlar organlari to‘g‘risida”gi Qonuni.
- 5.O‘zbekiston Respublikasining “Kiberxavfsizlik to‘g‘risida”gi Qonuni.
- 6.O‘zbekiston Respublikasi Prezidentining 2021-yil 26 martdagi PF-6196-son “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 Farmoni.
- 7.O‘zbekiston Respublikasi Prezidentining 2021-yil 29 noyabrdagi PF-27-son “O‘zbekiston Respublikasi jamoat xavfsizligi konsepsiyasini tasdiqlash va uni amalga oshirish chora-tadbirlari to‘g‘risida”gi Farmoni.
- 8.O‘zbekiston Respublikasi Prezidentining 2025-yilda axborot texnologiyalari yordamida sodir etiladigan jinoyatlarga qarshi kurashish faoliyatini kuchaytirishga qaratilgan qarori.
- 9.O‘zbekiston Respublikasi Oliy Majlisi Qonunchilik palatasining kiberxavfsizlik va kiberjinoyatchilikka qarshi kurashish masalalariga oid materiallari, 2026-yil.
- 10.O‘zbekiston Respublikasi Ichki ishlar vazirligining kiberjinoyatchilikka qarshi kurashish bo‘yicha rasmiy materiallari, 2026-yil.
- 11.O‘zbekiston Respublikasi IIV Kiberjinoyatlarga qarshi kurashish departamentining rasmiy axborot materiallari.