INNOVATIVE WORLD
Ilmiy tadqiqotlar markazi

YANGI RENESSANS

ILMIY JURNALI

2026/4

+998335668868
www.innoworld.net

Google Scholar doi zenodo OpenAIRE

YANGI RENESSANS

ILMIY JURNALI
TO'PLAMI

3 - JILD, 4 - SON
2026

www.innoworld.net

O'ZBEKISTON-2026

Raqamli dunyoda xavfsizlik: ichki ishlar organlarining kiberjinoyatchilikni oldini olishdagi asosiy vazifalari.

Podpolkovnik: **Axmedov Farxod Saydalieyvich**
Malaka oshirish instituti Kasbiy tayyorgarlik fakulteti Maxsus fanlar sikli o‘qituvchisi
Farhodahmedov486@gmail.com
+99899 8226327

Aholining tinch va osoyishta hayotini ta’minlash, jinoyatchilik va huquqbuzarliklarga qarshi kurashish, jamoat tartibini saqlash – bugungi kunda eng muhim vazifadir.

Shavkat Mirziyoev

Annotasiya: Mazkur maqolada zamonaviy axborot-kommunikatsiya texnologiyalarining rivojlanishi sharoitida Ichki ishlar organlari (IIO) tomonidan kiberxavfsizlikni ta’minlash va kiberjinoyatchilikka qarshi kurashishning dolzarb masalalari yoritilgan. Aholining kibersavodxonligini oshirish, onlayn tahdidlarni monitoring qilish va barvaqt aniqlash, texnik va kadrlar salohiyatini mustahkamlash hamda xalqaro hamkorlikni rivojlantirish masalalariga alohida e’tibor qaratilgan bo’lib, kiberjinoyatlarning oldini olishda kompleks yondashuv zarurligi asoslab, bir qator vazifalar berilgan.

Kalit so‘zlar: kiberxavfsizlik, Ichki ishlar organlari, kiberjinoyatchilik, profilaktika, axborot texnologiyalari, raqamli savodxonlik, kompyuter, internet va xalqaro hamkorlik.

Jamiyat hayotining barcha sohalariga axborot-kommunikatsiya texnologiyalarining jadal kirib borishi nafaqat qulayliklar yaratdi, balki yangi turdagi tahdidlarni ham yuzaga keltirdi. Bugungi kunda internet orqali sodir etilayotgan jinoyatlar, ya’ni kiberjinoyatchilik global muammoga aylanib ulgurdi. Firibgarlik, bank kartalaridan mablag‘larni o‘g‘irlash, shaxsiy ma’lumotlarni oshkor qilish va davlat ahamiyatiga molik tizimlarga hujumlar fuqarolarning ham, davlatning ham xavfsizligiga jiddiy putur yetkazmoqda.

Bunday sharoitda jamiyatda huquq-tartibotni ta’minlovchi asosiy kuch bo‘lgan Ichki ishlar organlarining roli mutlaqo yangi bosqichga ko‘tarildi. Jinoyatlarning virtual olamga ko‘chishi huquq-tartibot organlaridan nafaqat jismoniy, balki raqamli makonda ham faol va samarali harakat qilishni talab etmoqda.

Muhtaram Prezidentimiz Shavkat Mirziyoev: **“Xalqimiz yaratgandan avvalo tinchlik-xotirjamlikni so‘raydi. Shundan so‘ng o‘z uyim, boshpanam**

bo‘lsa, oilam, bola-chaqam bilan sog‘-salomat yashasam, deydi. Biz xalqimizning ana shunday orzu-niyatlarini ro‘yobga chiqarish uchun ikkita masalaga, ya’ni ichki ishlar va sog‘liqni saqlash tizimini isloh qilishga alohida e’tibor qaratayapmiz”, deganlarida tinchlik-xotirjamlikning inson, jamiyat, davlatning eng muhim hayotiy manfaatlarini ro‘yobga chiqarishdagi o‘rni hamda bu buyuk ne’matni ta’minlash umummilliy vazifa ekanligini nazarda tutadi.

Kiberxavfsizlik bu - u kompyuterlar, serverlar, mobil qurilmalar, tarmoqlar va elektron tizimlar orqali yaratilgan va qayta ishlanadigan ma’lumotlarni himoya qilish uchun amalga oshiriladigan protseduralar va vositalar to‘plami sifatida belgilanishi mumkin. Oddiy qilib aytganda, kiberxavfsizlik – bu muhim tizimlar va nozik ma’lumotlarni raqamli hujumlardan himoya qilish amaliyotidir.

Kiberxavfsizlik XX-asrning ikkinchi yarmi va XXI-asrda jahon mamlakatlari, xalqlari hayotiga tahdid soluvchi, jamiyatda beqarorlik va qo‘rquv uyg‘otish, axborotni egallash, uni o‘zgartirish, yo‘q qilish yoki axborot tizimlari va resurslarini ishdan chiqarish maqsadida kibermakonda dasturiy ta’minot va texnik vositalardan unumli foydalanishlar avj olib ketdi.

Kiberxavfsizlikning oldini olishda ichki ishlar organlarining roli juda muhimdir. Ular kiberhavfsizlikni ta’minlashda ham davlat, ham jamoat xavfsizligini nazarda tutadi. Ichki ishlar organlari kiberhavfsizlik bilan bog‘liq bir qator vazifalarni amalga oshiradi, shu jumladan:

Kiberxavflarning aniqlanishi va tahlil qilinishi: Ichki ishlar organlari kiberxavfsizlik holatlarini kuzatib, kompyuter va internet asosida sodir bo‘ladigan jinoyatlarni aniqlash, tahlil qilish va xulosa chiqarish uchun maxsus bo‘limlarga ega. Ular ushbu tahlillar natijasida jinoyatchilarning ishlatgan metodlarini aniqlab, ularga qarshi kurashni samarali tashkil qiladilar.

Kiberjinoyatlarga qarshi kurashish: Ichki ishlar organlari, xususan, kiberjinoyatlarga oid huquqni muhofaza qiluvchi organlar, kiberxavfsizlikni buzgan shaxslarni aniqlab, javobgarlikka tortishadi. Bu bo‘yicha qonunchilikni yaxshi bilish va tartibga solish mexanizmini qo‘llash muhimdir.

Farqlangan jinoyatlarning oldini olish: Internet orqali tarqatilgan yolg‘on axborot, jamoat tartibini buzishga qaratilgan xabardorlik va boshqa zararli kontentlardan himoya qilish uchun ichki ishlar organlari kiberxavfsizlikka oid to‘g‘ri siyosat va choralar ishlab chiqadilar.

Fuqarolarga ma’lumot berish va yordam ko‘rsatish: Ichki ishlar organlari kiberxavfsizlikning eng samarali usullaridan biri fuqarolarni tahdidlardan habar qilish va ularga kiberhavfsizlik bo‘yicha bilim berish hisoblanadi. Har xil treninglar, seminarlar va xabardorlik dasturlari orqali aholini ogohlantirish muhim.

Ta’lim va mutaxassislarni tayyorlash: Kiberxavfsizlik sohasida malakali mutaxassislarni tayyorlash, kiberjinoyatlarga qarshi kurashish uchun qonunga xos bilimlarini rivojlantirish, mamlakat bo‘yicha katta ahamiyatga ega. Ichki ishlar

organlari shuningdek, boshqa davlatlar bilan hamkorlikda treninglar va seminarlar o‘tkazishga mas’ul.

Texnik kuzatuv va monitoring: Ichki ishlar organlari milliy xavfsizlik va kiberhavfsizlikning yaxshi ishlashini ta’minlash uchun kiberhujumlarning har qanday shakllarini monitoring qilish, tahlil qilish va oldini olish choralarini ko‘rish vazifasini ham bajaradi.

Jumladan, ichki ishlar organlarining kiberxavfsizlikni ta’minlash sohasidagi faoliyati kompleks yondashuvni talab etadi. Bu faqat sodir etilgan jinoyatni tergov qilish emas, balki birinchi navbatda uning barvaqt oldini olishga qaratilgan chora-tadbirlar tizimidir. Ushbu yo‘nalishdagi asosiy vazifalarni quyidagicha tasniflash mumkin:

birinchidan, kiberprofilaktika va aholining kibersavodxonligini oshirishda - bu yo‘nalish kiberjinoyatchilikka qarshi kurashning eng samarali usuli hisoblanadi. Chunki ko‘p hollarda jinoyatchilar fuqarolarning raqamli texnologiyalardan foydalanishdagi beparvoligi yoki bilimsizligidan foydalanadilar.

Ichki ishlar organlari xodimlari OAV, ijtimoiy tarmoqlar va mahallalarda fuqarolarga kiberfiribgarlarning tuzog‘iga tushmaslik yo‘llarini tushuntiradilar. “Foydalanuvchi gigienasi”, kuchli parollar yaratish, ikki bosqichli autentifikatsiyani yoqish va shubhali havolalarga kirmaslik bo‘yicha doimiy tavsiyalar berib borish orqali aholini bank kartalari bilan bog‘liq firibgarliklardan ogohlantirish uchun tijorat banklari bilan birgalikda SMS-xabarnomalar va ijtimoiy roliklar tayyorlab borish.

ikkinchidan, monitoring va barvaqt aniqlash (Kiberrazvedka) - kibermakondagi tahdidlarni o‘z vaqtida aniqlash uchun doimiy kuzatuv olib borish zarur, bunda diniy ekstremizm, terrorizmni targ‘ib qiluvchi, giyohvand moddalar savdosi bilan shug‘ullanuvchi yoki firibgarlik maqsadlarida yaratilgan veb-saytlar va ijtimoiy tarmoqlardagi guruhlarni aniqlash va ularni bloklash choralarini ko‘rish hamda muhim infratuzilma ob’ektlariga nisbatan bo‘lishi mumkin bo‘lgan kiberhujumlar belgilarini oldindan aniqlash va tizim administratorlarini ogohlantirish.

uchinchidan, texnik va kadrlar salohiyatini oshirish orqali kvalifikatsiyali mutaxassislar va zamonaviy texnologiyalarsiz kiberjinoyatchilarga qarshi kurashishda maxsus bo‘linmalarni tashkil etish orqali ichki ishlar vazirligi tizimida faqat kiberxavfsizlik masalalari bilan shug‘ullanuvchi yuqori texnologiyali markazlar va bo‘limlar faoliyatini kuchaytirish.

Xodimlarni o‘qitish orqali ichki ishlar organlarini belgilangan muddatlarda raqamli forenzika (raqamli dalillarni yig‘ish), kriptoanaliz va dasturlash asoslari bo‘yicha muntazam ravishda malakasini oshirib borish.

to‘rtinchidan, xalqaro hamkorlikni yo‘lga qo‘yishda kiberjinoyatlar ko‘pincha transchegaraviy xarakterga ega bo‘lib, jinoyatchi bir davlatda turib, boshqa davlat fuqarosiga zarar yetkazishlar ko‘payganini inobatga olib, interpol va boshqa xalqaro tashkilotlar orqali xorijiy hamkasblar bilan kiberjinoyatchilar, ularning usullari va ishlatilgan serverlar haqida tezkor ma’lumot almashish hamda virtual olamdagi uyushgan jinoiy guruhlarni fosh etish va qo‘lga olish bo‘yicha xalqaro qo‘shma tadbirlarda ishtirok etish choralarini jadallashtirish.

Bugungi dolzarb zamonda raqamli texnologiyalar barcha sohalarga va odamlar hayotiga jadal kirib bormoqda. Ushbu soha rivojlanib borgani sari, bundan g‘araz maqsadda foydalanuvchilar ham ortmoqda. Hozirgi kunda, viloyat hududida sodir etilayotgan jami jinoyatlar orasida internet va kompyuter texnologiyalari bilan bog‘liq jinoyatlar keskin oshmoqda.

Ushbu holatlarning oldini olish va aholining ogohligini oshirish maqsadida, Respublika hududida bu turdagi huquqbuzarliklarning oldini olish bo‘yicha kompleks targ‘ibot-tashviqot tadbirlari Ichki ishlar organlarining tashabbusi bilan o‘tkazilishi belgilangan.

Agar O‘zbekiston Respublikasining xalqaro shartnomasida O‘zbekiston Respublikasining kiberxavfsizlik to‘g‘risidagi qonunchiligida nazarda tutilganidan boshqacha qoidalar belgilangan bo‘lsa, xalqaro shartnoma qoidalarida qo‘llanilishi ko‘rsatib o‘tilgan.

Qabul qilingan qonunda kiberxafvsizlik sohasidagi muhim tushunchalarning to‘liq ma’nolari ochib berildi. Qonunda kiberxafvsizlik sohasidagi munosalatlarni o‘z prinslari orqali tartibga solish belgilandi. Bu prinsiplarni qonuniylik, kibermakonda shaxs, jamiyat va davlat manfaatlarini himoya qilishning ustuvorligi, kiberxavfsizlik sohasini tartibga solishga nisbatan yagona yondashuv, kiberxavfsizlik tizimini yaratishda mahalliy ishlab chiqaruvchilar ishtirokining ustuvorligi, O‘zbekiston Respublikasining kiberxavfsizlikni ta’minlashda xalqaro hamkorlik uchun ochiqligi kabi prinsiplar tashkil qiladi[9].

[9] *Manba. Prezidentimiz Shavkat Mirziyoevning 2022-yil 3-fevraldagi “Internet tarmog‘ida sodir etilayotgan huquqbuzarliklarning barvaqt oldini olishga doir qo‘shimcha chora-tadbirlar to‘g‘risida”gi Qarori.*

O‘zbekiston Respublikasida kiberxavfsizlik sohasidagi yagona davlat siyosatini O‘zbekiston Respublikasi Prezidenti belgilaydi. O‘zbekiston Respublikasi Davlat xavfsizlik xizmati kiberxavfsizlik sohasidagi vakolatli davlat organidir. O‘zbekiston Respublikasi Davlat xavfsizlik xizmatiga kiberxavfsizlik sohasidagi normativ-huquqiy hujjatlarni va davlat dasturlarini ishlab chiqishi, kiberxavfsizlik to‘g‘risidagi qonunchilik hujjatlarining ijro etilishi ustidan nazoratni amalga oshirishi, kiberxavfsizlik hodisalari yuzasidan tezkor-qidiruv tadbirlarini, tergovga qadar tekshiruvlarni va tergov harakatlarini amalga oshirish, kiberxavfsizlik hodisalarining oldini olish, ularni aniqlash va bartaraf etish hamda ularga nisbatan tegishli chora-tadbirlarni, shu jumladan ularning oqibatlarini tugatish bo‘yicha tashkiliy-texnik chora-tadbirlarni ko‘rishi, favqulodda vaziyatlarda axborot tizimlari va resurslarini kiberhimoya qilish hamda kiberxavfsizlik sohasidagi boshqa masalalar bo‘yicha chora-tadbirlarni o‘z ichiga olgan rejalarni ishlab chiqishi, kiberxavfsizlikni ta’minlashga doir ishlarni, shuningdek muhim axborot infratuzilmasi obektlarida kiberhujumlarning oldini olishga, ularni aniqlashga va ularning oqibatlarini tugatishga doir ishlarni tashkil etishi, muhim axborot infratuzilmasi obektlarining kiberxavfsizligini ta’minlashga doir talablarni belgilashi kabi bir qancha yangi vazifalar yuklatildi.

Kiberxavfsizlik to‘g‘risidagi qonunda quyidagi asosiy tushunchalar qo‘llaniladi:

axborotlashtirish ob’ekti — turli darajadagi va maqsaddagi axborot tizimlari, telekommunikatsiya tarmoqlari, axborotga ishlov berishning texnik vositalari, ushbu vositalar o‘rnatilgan va foydalaniladigan xonalar;

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

kibermakon — axborot texnologiyalari yordamida yaratilgan virtual muhit;

kibertahdid — kibermakonda shaxs, jamiyat va davlat manfaatlariga tahdid soluvchi shart-sharoitlar va omillar majmui;

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

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

kiberxavfsizlik ob'ekti — axborotning kiberhimoya qilinishini hamda milliy axborot tizimlari va resurslarining kiberxavfsizligini ta'minlashga doir faoliyatda foydalaniladigan axborot tizimlari majmui, shu jumladan muhim axborot infratuzilmasi ob'ektlari;

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

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

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

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

muhim axborot infratuzilmasi ob'ektlari — davlat boshqaruvi va davlat xizmatlari ko'rsatish, mudofaa, davlat xavfsizligini, huquq-tartibotni ta'minlash, yoqilg'i-energetika majmui (atom energetikasi), kimyo, neft-kimyo tarmoqlari, metallurgiya, suvdan foydalanish va suv ta'minoti, qishloq xo'jaligi, sog'liqni saqlash, uy-joy kommunal xizmatlar ko'rsatish, bank-moliya tizimi, transport, axborot-kommunikatsiya texnologiyalari, ekologiya va atrof-muhitni muhofaza qilish, strategik ahamiyatiga ega bo'lgan foydali qazilmalarni qazib olish va qayta

ishlash sohasida, ishlab chiqarish sohasida, shuningdek iqtisodiyotning boshqa tarmoqlarida va ijtimoiy sohada qo‘llaniladigan axborotlashtirish tizimlari;

muhim axborot infratuzilmasi sub’ektlari — davlat organlari va tashkilotlari, shuningdek mulk, ijara huquqlari asosida yoki boshqa qonuniy asoslarda muhim axborot infratuzilmasi ob’ektlariga egalik qiluvchi yuridik shaxslar, shu jumladan muhim axborot infratuzilmasi ob’ektlarining ishlashini hamda hamkorligini ta’minlovchi yuridik shaxslar va (yoki) yakka tartibdagi tadbirkorlar[10].

Yaqin yillarda kiber jinoyatchilikning eng yirik turi - yuqori malakali kiber jinoiy guruhlar ko‘payishi va ifratuzilmaga hujum uyushtirilishidan iborat bo‘ladi, deydi “Laboratorii Kasperskogo” rahbari Yevgeniy Kasperskiy “RIA Novosti” muxbiri bilan suhbatda.

Birinchi trend – kiber jinoyatchilik ommaviy tus oladi. Taassufki, iqtisodiy inqiroz davrida ushbu illat ayniqsa ko‘p urchiydi. Jinoyatchilar safi endi-endi to‘lib kelmoqda, - deydi u.

Olimning ta’kidlashicha, “Kaspersky Security Network” ma’lumotiga ko‘ra, iyul oyida dunyo bo‘yicha har kuni 400 mingdan ortiq zarar keltiruvchi dasturiy ta’minot paydo bo‘lgan. “Har kuni shuncha zararli virus tarqatish uchun qancha xaker zarur bo‘ladi, bu savolga javob berish mushkul”, deydi u. “Albatta, ularda avtomatlashtirish, kodlarni avtomatik generatsiyalash imkoni mavjud. Umuman, xakerlar soni 100 mingdan ortiq, deyishsa, hayron qolmagan bo‘lardi, - qo‘shimcha qildi Kasperskiy.

Ikkinchi trend – yuqori malakali kiber jinoyatchi guruhlar paydo bo‘lishi. Darvoqe, ilk shunday tuzilma – “Sarbanak” guruhi 2014-yilda paydo bo‘lgan edi. Bungacha davlatlar homiylik qilgan xakerlar va oddiy jinoyatchilar faoliyat olib borishgan. “Sarbanak” ortidan yana ko‘plab professional guruhlar paydo bo‘ldi, – deydi mashhur dasturchi.

Uchinchi trend – infratuzilmaga hujum uyushtiruvchilar safi keyingi yillarda borgan sari kengaymoqda. “Sur’atiga baho bera olmayman, chunki ular qaysi yo‘ldan

[10] *Manba. O‘zbekiston Respublikasining 2022-yil 15-aprel kunidagi “Kiberxavfsizlik to‘g‘risida”gi O‘RQ-764-son Qonuni.*

yuradi, bunday guruhlar uchun qaysi mavzu dolzarb ekanini oldindan aytish qiyin. Jinoyatchilar faoliyati ko‘p omillarga bog‘liq. Hujumlar murakkablashadi, borgan sari ko‘p texnologiyalar hujum ostida qoladi, lekin hujum qaysilariga uyushtirilishi va qanday tartibda kechishi siz bilan bizga bog‘liq emas, - qo‘shimcha qildi u.

Kasperskiy dunyoning turli hududlaridagi xakerlarning ixtisoslashuvi haqida ham so‘z yuritib, xitoylik kiber jinoyatchilar ko‘proq botnetlar (zararli dasturiy ta’minot bilan zararlantirilgan kompyuterlar tarmog‘i), rossiyaliklar dasturlash – raqamli belgilarni aniqlash, Lotin Amerikasi xakerlari esa moliyaviy qallobliklar bo‘yicha ish olib boradi.

Eng qizig‘i, jinoyatchilarda ixtisoslashuv mavjud. Xitoyliklar ko‘proq botnetlar bilan ishlaydi, raqamli kodlardan foydalanuvchi xakerlar tez-tez ruscha so‘zlashadi, moliyaviy tovlamachilik bilan shug‘ullanuvchi xakerlar asosan Lotin Amerikasi mintaqasidan, - deydi u[11].

Mamlakatimizning har bir fuqarosi ichki ishlar organlari xodimi timsolida o‘zining xayoti, sog‘ligi, sha’ni va qadr-qimmatini har qanday tajovuzlardan muhofaza qilishga va og‘ir damda yordam berishga tayyor bo‘lgan himoyachisini ko‘rishi hamda o‘zining havfsizligi ta’minlanganligini his qilishi zarur.

Prezidentimiz ichki ishlar organlarining kasb bayrami munosabati bilan yo‘llagan tabrigida **«Agar davlat tayanadigan asosiy ustun qonun bo‘lsa, uning kuchini amalda namoyon etadigan eng samarali tizim bu – ichki ishlar sohasi, desak, ayni haqiqat bo‘ladi»,** deya e’tirof etgan edi. Bu yuksak baho osoyishtalik posbonlarini qonun ustuvorligini ta’minlash yo‘lida yanada fidoyilik bilan xizmat qilishga undaydi.

Xulosa qilib aytganda, bugungi shiddat bilan rivojlanayotgan raqamli davrda kiberxavfsizlikni ta’minlash nafaqat texnik masala, balki milliy xavfsizlik va ijtimoiy barqarorlikning garovidir. Kiberjinoyatchilikning transchegaraviy tabiati va uning doimiy ravishda takomillashib borayotgani ichki ishlar organlari zimmasiga mutlaqo yangi va murakkab vazifalarni yuklamoqda.

[11] *Manba. O‘zbekiston Milliy axborot agenligi.*

Tadqiqotlar shuni ko‘rsatadiki, an’anaviy tezkor-qidiruv usullari raqamli makonda sodir etilayotgan jinoyatlarga qarshi kurashishda yetarli samara bermayapti. Shu sababli, ichki ishlar organlarining faoliyatini kiberjinoyatlarning oqibatlari bilan kurashishdan ko‘ra, ularning barvaqt oldini olishga (profilaktikaga) yo‘naltirish strategik ahamiyatga ega. Bu borada aholining kiber-savodxonligini oshirish, kiber-gigiyena qoidalarini keng targ‘ib qilish asosiy drayver bo‘lib xizmat qiladi.

FOYDALANILGAN ASOSIY ADABIYOTLAR

O‘zbekiston Respublikasining Konstitutsiyasi. –T., 2023-yil
O‘zbekiston Respublikasining 2016-yil 16-sentyabrdagi “Ichki ishlar organlari to‘g‘risida”gi O‘RQ-407-son Qonuni;
O‘zbekiston Respublikasining 2022-yil 15-aprel kunidagi “Kiberxavfsizlik to‘g‘risida”gi O‘RQ-764-son Qonuni.
O‘zbekiston Respublikasi Prezidentining 2022-yil 3-fevraldagi “Internet tarmog‘ida sodir etilayotgan huquqbuzarliklarning barvaqt oldini olishga doir qo‘shimcha chora-tadbirlar to‘g‘risida”gi Qarori.

Internet saytlari

http://gov.uz /iiv/ (O‘zbekiston Respublikasi IIV);
http://ipkmvd.uz (O‘zbekiston Respublikasi IIV Malaka oshirish instituti);
http://akadmvd.uz (O‘zbekiston Respublikasi IIV Akademiyasi);
http://lex.uz (O‘zbekiston Respublikasi Qonun hujjatlari ma’lumotlari milliy bazasi);