

O'ZBEKISTONDA KIBERJINOYATCHILIKNING OLDINI OLISH: AXBOROT MAKONI VA INTERNET TARMOG'IDA NAZORATNI KUCHAYTIRISH MASALALARI

Jo'rayev O'zbekxon Dilshodbek o'g'li

Farg'ona davlat universiteti, Huquqshunoslik fakulteti,

Yurisprudensiya yo'nalishi talabasi.

Telefon: +998908451200 E-mail: jurayevxofiz@gmail.com

<https://doi.org/10.5281/zenodo.23036011>

Annotatsiya. Maqolada O'zbekistonda kiberjinoiyatchilikka qarshi kurashish, axborot makonida internet nazoratini kuchaytirish hamda milliy qonunchilik asosi tahlil qilingan.

Shuningdek, bank-moliya tizimini himoya qilishda sun'iy intellekt texnologiyalarini va ilg'or monitoring tizimlarini joriy etishning strategik ahamiyati xolis baholangan.

Kalit so'zlar: Kiberxavfsizlik, kibermakon, kiberjinoiyatchilik, internet nazorati, sun'iy intellekt, moliya, qonunchilik, monitoring, profilaktika, kadrlar.

ПРЕДУПРЕЖДЕНИЕ КИБЕРПРЕСТУПНОСТИ В УЗБЕКИСТАНЕ: ВОПРОСЫ УСИЛЕНИЯ КОНТРОЛЯ В ИНФОРМАЦИОННОМ ПРОСТРАНСТВЕ И СЕТИ ИНТЕРНЕТ

Аннотация. В статье анализируются проблемы борьбы с киберпреступностью в Узбекистане, усиление интернет-контроля в информационном пространстве и национальное законодательство. Также оценивается стратегическое значение внедрения технологий искусственного интеллекта и передовых систем мониторинга для защиты банковско-финансовой системы.

Ключевые слова: Кибербезопасность, киберпространство, киберпреступность, интернет-контроль, искусственный интеллект, финансы, законодательство, мониторинг, профилактика, кадры.

PREVENTING CYBERCRIME IN UZBEKISTAN: ISSUES OF STRENGTHENING CONTROL IN THE INFORMATION SPACE AND THE INTERNET

Abstract. The article analyzes cybercrime challenges in Uzbekistan, strengthening internet control within the information space, and national legislation. It also evaluates the strategic importance of implementing artificial intelligence technologies and advanced monitoring systems to protect the banking and financial infrastructure.

Keywords: Cybersecurity, cyberspace, cybercrime, internet control, artificial intelligence, finance, legislation, monitoring, prevention, cadres.

KIRISH:

Internet va zamonaviy texnologiyalar hayotimizga qanchalik chuqur kirib borgan bo'lsa, virtual olamdagi tahdidlar va jinoyatlar ham shunchalik ko'payib bormoqda. O'zbekiston Jinoyat kodeksida aynan kompyuter va internet orqali sodir etiladigan huquqbuzarliklar uchun alohida bob ajratilgan bo'lib, unda kiber-makondagi har bir noqonuniy harakatning chegaralari aniq belgilangan. Bu borada eng birinchi navbatda saytlar, ma'lumotlar bazasi va davlat yoki xususiy tashkilotlarning tizimlariga mas'ul bo'lgan shaxslarning beparvoligiga e'tibor qaratiladi. Agar biror tashkilot o'z tizimining xavfsizligini ta'minlamasa, kiber-himoya choralarini ko'rmasa va buni orqasidan tizim buzilib, odamlarga yoki davlatga katta zarar yetsa, o'sha mas'ul xodim qonun oldida javob beradi. Bu qoida tizim egalari ulkan texnik mas'uliyat yuklaydi.

Shu bilan birga, bugungi kunda hayotda eng ko'p uchrayotgan holatlardan biri — birovning kompyuteriga, ijtimoiy tarmoqdagi sahifasiga yoki shaxsiy ma'lumotlariga ruxsatsiz, yashirincha kirishdir. Qonunga ko'ra, birovning ma'lumotlarini o'g'irlash, nusxa ko'chirish, o'chirib yuborish yoki tizim ishini bloklab qo'yish jiddiy jinoyat hisoblanadi va buni bir guruh shaxslar kelishib qilsa yoki o'z mansabidan foydalanib sodir etsa, jazo choralari yanada og'irlashadi. Kiberjinoyatchilar o'z maqsadlariga erishish uchun ko'pincha maxsus vositalardan foydalanishadi. Shuning uchun ham birovning kompyuter tizimini buzib kirishga mo'ljallangan maxsus qurilmalar yoki xakerlik dasturlarini tayyorlash, ularni boshqalarga sotish yoki internetda tarqatish qat'iy man etiladi. Bu harakat shunchaki oddiy qilmish emas, balki raqamli makonda kiber-qurol tarqatish bilan tenglashtiriladi. Bunga parallel ravishda, tizimdagi real ma'lumotlarni o'zgartirish, ularga zarar yetkazish yoki ataylab yolg'on ma'lumotlarni kiritish ham kiber-makondagi barqarorlikni buzadi. Masalan, biror tizimdagi moliyaviy raqamlarni o'zgartirib qo'yish yoki bazadagi ma'lumotlarni soxtalashtirish fuqarolarga va davlatga to'g'ridan-to'g'ri ziyon yetkazadi. Kiber-tahdidlarning eng xavfli ko'rinishi esa kompyuter sabotaji va zararli viruslar tarqatish bilan bog'liqdir. Birovning kompyuter uskunasi yoki butun boshli korxona infratuzilmasini qasddan urib tushirish, ishdan chiqarish hamda internetda odamlarning telefon yoki kompyuterlariga virus yuqtiruvchi dasturlarni tarqatish jamiyat xavfsizligiga katta zarba beradi. Amaldagi qonunlarimizda bunday qilmishlarning har biri uchun katta miqdordagi jarimalar, axloq tuzatish ishlari va bir necha yilga ozodlikdan mahrum qilish jazolari belgilangan bo'lsa-da, texnologiyalar shiddat bilan o'zgarayotgani bois, ushbu jinoiy-huquqiy normalarni ham doimiy ravishda davr talabiga moslab kuchaytirib borish zarurati yaqqol sezilmoqda.

Biroq mukammal huquqiy bazaning mavjudligi amaliyotda kiberjinoyatchilik xavfini o'z-o'zidan to'liq bartaraf eta olmaydi. Amaldagi qonunlar qanchalik qat'iy bo'lmasin, virtual makonning chegarasiz tabiati va kiberjinoyatchilarning doimiy ravishda yangi texnik usullarni o'ylab topayotgani huquq-tartibot idoralari oldiga yangi murakkab vazifalarni qo'ymoqda.

Bugungi kunda O'zbekiston axborot makonida eng katta muammolardan biri — kiber-hujumlarning transchegaraviy xarakterga egaligidir, ya'ni jinoyatchilar ko'pincha mamlakat hududidan tashqarida turib, xorijiy serverlar va anonim tarmoqlar orqali milliy infratuzilmaga yoki fuqarolarning moliyaviy aktivlariga zarar yetkazishmoqda. Bunday sharoitda faqatgina sodir etilgan jinoyat oqibatlari bilan kurashish yetarli emas, balki asosiy diqqat-e'tibor axborot vositalari va internet trafigi ustidan preventiv monitoring tizimini kuchaytirishga qaratilishi shart.

Internet provayderlar va yirik raqamli platformalar bilan hamkorlikda shubhali faollikni barvaqt aniqlovchi intellektual filtrlarni joriy etish orqali kiber-tahdidlarning katta qismini tarmoq darajasidayoq bloklash imkoniyati paydo bo'ladi. Shu bilan birga, zamonaviy kiber-himoya tizimini shakllantirishda inson omilini ham unutmaslik lozim, chunki ko'plab tizimli buzilishlar va firgarliklar aynan foydalanuvchilarning raqamli gigiyena qoidalariga rioya qilmasligi hamda oddiy beparvoligi oqibatida yuzaga kelmoqda. Shu sababli, axborot xavfsizligini ta'minlashning eng samarali strategiyasi — davlat tomonidan raqamli makon nazoratini kuchaytirish bilan bir qatorda, aholining kiber-savodxonlik darajasini tizimli ravishda oshirib borishdir. Faqatgina yuqori texnologik nazorat mexanizmlari, qat'iy huquqiy javobgarlik va jamiyatning kiber-tahdidlarga nisbatan hushyorligi o'zaro uyg'unlashgan taqdirdagina O'zbekistonning raqamli kelajagi va milliy xavfsizligi ishonchli qalqon bilan ta'minlanadi.

Jinoyat kodeksidagi jazo choralarining samaradorligini ta'minlash va mamlakat virtual makonini tizimli himoya qilish maqsadida O'zbekistonda kiberxavfsizlik sohasidagi munosabatlarni huquqiy jihatdan tartibga soluvchi maxsus qonunchilik asosi yaratilgan bo'lib,

uning fundamental poydevorini mamlakat parlamenti tomonidan qabul qilingan va ma'qullangan "Kiberxavfsizlik to'g'risida"gi fundamental Qonun tashkil etadi. Mazkur qonun hujjati raqamli dunyodagi murakkab virtual jarayonlarni aniq huquqiy qoliplarga solishda davlat siyosatining ustuvor yo'nalishlarini belgilab beradi. Qonunchilikda kibermakonda shaxs, jamiyat va davlat manfaatlarining tashqi hamda ichki tahdidlardan himoyalanganlik holatiga kiberxavfsizlik deb aniq ta'rif berilgan bo'lib, ushbu tizim doirasida kiberjinoyatchilik tushunchasining mazmun-mohiyati ham to'liq ochib berilgan. Unga ko'ra, virtual muhitda ma'lumotlarni ruxsatsiz egallash, o'zgartirish, yo'q qilish yoki butun boshli axborot resurslarini ishdan chiqarish maqsadida dasturiy ta'minot hamda maxsus texnik vositalardan foydalanib sodir etiladigan har qanday qasddan qilingan harakatlar kiberhujum va jiddiy xavfsizlik hodisasi sifatida baholanadi.

Bunday tahdidlarning oldini olish, ularga qarshi qalqon yaratish va tizimlarning barqaror faoliyatini qayta tiklash maqsadida davlat tomonidan huquqiy, tashkiliy, moliyaviy-iqtisodiy hamda muhandislik-texnik chora-tadbirlar majmuini o'z ichiga olgan kiberhimoya mexanizmi joriy etilgan. Ushbu himoya tizimining eng strategik nuqtasi — bu davlat boshqaruvi, mudofaa, huquq-tartibot, bank-moliya, transport, sog'liqni saqlash va eng muhimi, yoqilg'i-energetika kabi hayotiy muhim tarmoqlarda qo'llaniladigan axborotlashtirish tizimlarini, ya'ni muhim axborot infratuzilmasi obyektlarini kiber-zarbalardan asrash hisoblanadi. Davlat bunday muhim obyektlar va milliy raqamli platformalar xavfsizligini ta'minlashda bir nechta o'zgaras prinsiplarga tayanadi. Bular orasida qonuniylik, yagona davlat siyosati va tizimli monitoring yondashuvlaridan tashqari, kiberxavfsizlik tizimini yaratishda mahalliy ishlab chiqaruvchilar ishtirokining ustuvorligi prinsipi alohida ahamiyatga ega. Ya'ni, davlat organlari o'z kiberxavfsizligini ta'minlash uchun zarur bo'lgan texnik va dasturiy vositalarni xarid qilishda mamlakat hududida ishlab chiqarilgan tovar va xizmatlarga ustunlik beradi, bu esa milliy dasturiy mahsulotlar bozorini rivojlantirishga xizmat qiladi. Shu bilan birga, O'zbekiston kiber-tahdidlarning global xarakterini hisobga olgan holda xalqaro hamkorlik uchun hamisha ochiq bo'lib, agar mamlakat imzolagan xalqaro shartnomalarda milliy qonunlardan ko'ra mukammalroq qoidalar belgilangan bo'lsa, xalqaro huquq normalarining ustuvorligini tan oladi.

Ushbu yaxlit va tizimli strategiyaning yagona davlat siyosatini belgilash esa bevosita O'zbekiston Respublikasi Prezidentining vakolatiga kirib, raqamli dunyodagi milliy xavfsizlikni eng oliy darajada kafolatlaydi.

Ushbu qonuniy asoslarning amaliy ijrosini ta'minlash va kiber-makondagi davlat nazoratini to'g'ridan-to'g'ri muvofiqlashtirish masalasi nihoyatda jiddiy va markazlashgan institut poydevoriga tayanadi. "Kiberxavfsizlik to'g'risida"gi Qonun hujjatiga muvofiq, O'zbekiston Respublikasi Davlat xavfsizlik xizmati ushbu sohadagi yagona va mutlaq vakolatli davlat organi etib belgilangan. Bu qoida mamlakat raqamli makonining xavfsizligini tahlil qilish va nazorat qilish shunchaki tarqoq idoralarning ishi emas, balki milliy xavfsizlikning eng yuqori bo'g'ini darajasidagi strategik vazifa ekanini anglatadi. Vakolatli organning zimmasiga kiberxavfsizlik sohasidagi normativ-huquqiy hujjatlar va davlat dasturlarini ishlab chiqishdan tortib, qonunchilik talablarining ijrosi ustidan qat'iy monitoring olib borishgacha bo'lgan ulkan mas'uliyat yuklangan. Bu borada eng muhim yo'nalishlardan biri — kiber-makondan terrorchilik, ekstremistik va boshqa qonunga xilof harakatlar yo'lida foydalanilishiga qarshi kurashish, kiberjinoyatlar yuzasidan tezkor-qidiruv hamda tergov harakatlarini o'tkazish, shuningdek, davlat va xo'jalik boshqaruvi organlarini aniqlangan zaifliklar va tizimli kiber-hujumlar to'g'risida barvaqt xabardor qilib borishdir. Shu bilan birga, muhim axborot infratuzilmasi obyektlarining yagona reyestrini shakllantirish, apparat va dasturiy vositalarni

sertifikatlashtirish hamda sohada malakali professional kadrlar tayyorlash tizimini yo'lga qo'yish ham mazkur organning asosiy funksiyalaridan hisoblanadi. Davlat ushbu vakolatlarning to'laqonli va tezkor ijrosini ta'minlash uchun maxsus huquqiy filtrlar va mislsiz vakolatlar tizimini ham taqdim etgan. Xususan, kiber-hujumlarga barham berish va favqulodda vaziyatlarda kechiktirib bo'lmaydigan choralarni ko'rish maqsadida vakolatli organ texnik qurilmalar va aloqa xizmatlaridan bepul foydalanish, davlat organlari hamda muhim infratuzilma obyektlarining axborot tizimlariga to'sqinliksiz ulanish huquqiga ega. Jinoyatchilarni ta'qib qilish yoki fuqarolar hayotiga real tahdid mavjud bo'lgan alohida kechiktirib bo'lmaydigan holatlarda, yigirma to'rt soat ichida prokurorni xabardor qilish sharti bilan, hattoki jismoniy va yuridik shaxslarning turar joylari ile boshqa obyektlariga qulflash moslamalarini buzgan holda kirish va ko'zdan kechirish huquqi qonuniy ravishda mustahkamlab qo'yilgan. Ko'rinib turibdiki, vakolatli organning qonuniy talablari va ko'rsatmalari barcha subyektlar uchun bajarilishi majburiy bo'lib, bu qat'iy vertikal tizim O'zbekistonning raqamli chegaralarini har qanday tashqi va ichki buzg'unchilik harakatlaridan ishonchli himoya qilish imkonini beradi.

Tizim xavfsizligini ta'minlash mexanizmi faqatgina vakolatli organning nazorati bilan cheklanib qolmay, jarayonning barcha ishtirokchilari, ya'ni kiberxavfsizlik subyektlarining zimmasiga ham aniq huquq va majburiyatlarni yuklaydi. Qonunchilikka ko'ra, tizim egalari o'z raqamli makonini himoya qilish uchun vakolatli davlat organidan dasturiy ta'minot va texnik uskunalar qayerida zaifliklar borligi haqida ma'lumot va maslahatlar olish huquqiga ega. Shu bilan birga, subyektlar o'z tizimlarida ma'lumotlarning o'g'irlanishi, bloklanishi yoki qalbakilashtirilishining oldini olishlari, agar ruxsatsiz kirish holatlari aniqlansa, salbiy oqibatlarni kamaytirish uchun tizimni tezkorlik bilan tiklash choralari ko'rishlari shart. Bu borada eng muhim majburiyatlardan biri — sodir bo'lgan kiber-hodisalar haqida vakolatli organga zudlik bilan xabar berish va jinoyatni to'liq fosh etish uchun raqamli izlarning saqlanishini ta'minlash hisoblanadi. Raqamli infratuzilmaning xavfsizlik darajasini xolis baholash maqsadida kiberxavfsizlik ob'ektlarini tashkiliy-texnik murakkabligiga qarab tasniflash hamda majburiy ekspertiza va attestatsiya tizimi joriy etilgan. Ayniqsa, davlat organlarining axborot tizimlari va resurslari, shuningdek, muhim axborot infratuzilmasi obyektlari kiberxavfsizlik talablariga muvofiqlik yuzasidan majburiy tartibda ekspertizadan o'tkazilishi lozim. Ushbu ob'ektlarda qo'llaniladigan har qanday apparat va dasturiy vositalar majburiy sertifikatlashtirishdan o'tishi shart bo'lib, bu choralar tizimning haqiqiy himoyalanganlik holatini aniqlashga xizmat qiladi. Kiberxavfsizlik hodisalari yuz bergan taqdirda, tekshiruvlar vakolatli organ yoki tizim egasining o'zi tomonidan amalga oshirilishi mumkin, biroq har qanday holatda ham zararli dasturlarni yo'q qilish, kiberhujum manbasini jilovlash va tizimlarni kibertahdidlardan ajratib qo'yish bo'yicha tezkor choralar ko'rilishi talab etiladi. Tizimlardagi zaifliklar va kiber-hujumlar to'g'risidagi ma'lumotlar maxfiy hisoblanib, ulardan faqat xavfni bartaraf etish uchun foydalaniladi va faqat barcha zarur xavfsizlik choralari ko'rib bo'linganidan keyingina egasining ruxsati bilan ommaga oshkor qilinishi mumkin. Aynan mana shunday qat'iy talablar va aniq yo'nalishlar yagona chora-tadbirlar majmuini shakllantirib, mamlakatning muhim strategik va ijtimoiy-iqtisodiy ahamiyatga ega bo'lgan raqamli infratuzilmasini har qanday kiber-zarbalardan ishonchli asrashga imkon beradi.

Davlatimiz raqamli makonini shunchaki an'anaviy tahdidlardan himoya qilish bilan cheklanib qolmay, kiber-makonda eng zamonaviy texnologik qurollardan, xususan, sun'iy intellekt imkoniyatlaridan tizimli foydalanish strategiyasini belgilab olmoqda. Shu maqsadda qabul qilingan Sun'iy intellekt texnologiyalarini 2030-yilga qadar rivojlantirish strategiyasi

mamlakatimizni raqamli innovatsiyalar sohasida dunyoning yetakchi davlatlari qatoriga olib chiqish bilan bir qatorda, kiber-makonni nazorat qilish va milliy xavfsizlikni ta'minlashning konseptual yo'nalishlarini qamrab oladi. Ushbu strategiya doirasida sun'iy intellekt texnologiyalarini joriy etish orqali ijtimoiy-iqtisodiy sohalarni raqamlashtirish bilan bir qatorda, axborot xavfsizligi tizimlarini tubdan modernizatsiya qilish nazarda tutilgan. Xususan, bank-moliya, soliq va bojxona tizimlarida sun'iy intellekt algoritmalaridan foydalanish birinchi navbatda virtual firgarliklarning, yashirin iqtisodiyotning va shubhali operatsiyalarning barvaqt oldini olishga hamda xavflarni intellektual boshqarishga xizmat qiladi. Davlat bunday ulkan texnologik sakrashni amalga oshirish va kiber-makonda ilg'or monitoring tizimlarini ishga tushirish uchun yirik moliyaviy va infratuzilmaviy poydevor yaratmoqda, buni doirasida yuqori quvvatli hisoblash serverlari va axborot xavfsizligi choralari ko'rilgan yaxlit "katta ma'lumotlar" bazasi shakllantirilmoqda. Shu bilan birga, sohadagi loyihalar va dasturiy mahsulotlarning xavfsizligi hamda ularda sun'iy intellekt texnologiyalarining to'g'ri qo'llanilganligini nazorat qilish maqsadida maxsus vakolatli tuzilma — Sun'iy intellekt va raqamli iqtisodiyotni rivojlantirish markazi tashkil etilgan bo'lib, u davlat organlarining axborot tizimlaridan to'siqsiz foydalanish va yaratilayotgan raqamli mahsulotlarni ekspertizadan o'tkazish huquqiga ega.

Ko'rinib turibdiki, O'zbekiston kiber-makon nazoratini kuchaytirishda faqat taqiqlar bilan cheklanmay, kiberjinoyatchilikka qarshi kurashda eng ilg'or intellektual filtrlarni va sun'iy intellekt asosidagi preventiv tizimlarni ishga solmoqda, bu esa milliy axborot makonini har tomonlama ishonchli va barqaror himoya qilishga imkon beradi.

Zamonaviy kiber-himoya strategiyasining amaliy ijrosini ta'minlashda yangi tashkil etilgan Sun'iy intellekt va raqamli iqtisodiyotni rivojlantirish markazi markaziy platforma vazifasini o'taydi. Ushbu ixtisoslashtirilgan muassasa zimmasiga raqamli makon xavfsizligi uchun zarur bo'lgan ilg'or normativ-huquqiy bazani shakllantirish, sohaga xalqaro standartlarni chuqur joriy etish hamda intellektual loyihalarni muvaffaqiyatli ishga tushirish uchun baquvvat texnik infratuzilmani yaratish kabi strategik yuklamalar yuklangan. Markaz ekspertlar hamjamiyati bilan yaqin hamkorlikda raqamli iqtisodiyot va elektron hukumat tizimini global kiber-tahdidlardan asrashning konseptual hamda uslubiy asoslarini ishlab chiqadi. Shu bilan birga, zamonaviy kiber-hujumlar va firgarliklarning asosiy nishoniga aylanib borayotgan bank-moliya tizimini tubdan isloh qilish va uni sun'iy intellekt yordamida himoyalangan ilg'or sohaga aylantirish qarorda alohida o'rin egallaydi. Xususan, Markaziy bankning Kiberxavfsizlik markazi hamda davlat ulushiga ega tijorat banklari o'z faoliyatiga yirik ma'lumotlarni qayta ishlovchi algoritmalarini tatbiq etgan holda, real vaqt rejimida moliyaviy xavflarni boshqarish va mijozlarning to'lov qobiliyatini intellektual baholash tizimini yo'lga qo'ymoqda. Bank xizmatlarining avtomatlashtirilishi bilan parallel ravishda, tarmoqda axborot xavfsizligini ta'minlash va kiber-firgarlikka qarshi kurashishning eng zamonaviy, avtomatik chiquvchi filtrlari va to'siqlari o'rnatilmoqda, bu esa plastik kartalardan pul o'g'irlash va soxta tranzaksiyalar o'tkazish kabi jinoyatlarni ildizi bilan cheklash imkonini beradi. Davlat ushbu innovatsion islohotlarning ijrosi shunchaki qog'ozda qolib ketmasligi uchun qat'iy va shaffof monitoring tizimini joriy etgan bo'lib, unda har bir davlat organining raqamli transformatsiya holatini baholashda sun'iy intellekt va kiberxavfsizlik loyihalarining natijalari bevosita inobatga olinadi. Raqamli texnologiyalar vazirligi va Hukumat darajasida olib boriladigan tizimli, tanqidiy nazorat mexanizmlari mamlakatimiz axborot makonining daxlsizligini oliy darajada kafolatlaydi hamda O'zbekistonni kiber-makonda xavfsiz va intellektual rivojlangan qudratli davlatga aylantiradi.

Mamlakatimizda kiberjinoyatchilikning barvaqt oldini olish va raqamli makon daxlsizligini ta'minlash qonuniy bazani shakllantirish bilan birga, bevosita huquqni muhofaza qilish organlarining taktik va texnik imkoniyatlarini tubdan isloh qilishni taqozo etadi. Mazkur murakkab texnologik kurashda kiber-tahdidlarga samarali qarshi turish uchun quyidagi to'rtta strategik yo'nalishni amaliyotga zudlik bilan joriy etish lozim:

Birinchidan Ichki ishlar vazirligi tizimida internet nazoratini kuchaytirish: Virtual makondagi huquqbuzarliklarni barvaqt aniqlash va jilovlash maqsadida Ichki ishlar vazirligining kiber-nazorat va preventiv monitoring mexanizmlari konseptual darajada kuchaytirilishi shart.

Jinoyatchilikning transchegaraviy va dinamik tabiatini inobatga olgan holda, vazirlik tarkibidagi maxsus tuzilmalarning nafaqat zamonaviy texnik jihozlanishini, balki ularning raqamli makondagi tezkor-qidiruv va tahliliy salohiyatini ham bir necha barobar oshirish zarur.

Ikkinchidan Internet tarmoqlarida jinoyatchilar profillarini tezkor bloklash:

Huquq-tartibot idoralari internet provayderlar hamda yirik xalqaro ijtimoiy platformalar, messenjerlar va raqamli forumlar ma'muriyati bilan to'g'ridan-to'g'ri tezkor aloqa tizimini yo'lga qo'yishi lozim. Sun'iy intellekt algoritmlariga asoslangan avtomatik tahlil tizimlari yordamida shubhali kontent va kiber-firgarlarning faolligi soniyalar ichida aniqlanishi hamda jinoyatchilarning profillari va raqamli resurslari tarmoq darajasidayoq zudlik bilan bloklanishi shart.

Uchinchidan Kiber-moliyaviy jinoyatchilarni aniqlash tizimini kuchaytirish: Plastik kartalardan pul o'g'irlash, soxta to'lov tizimlari yoki feyk havola (click) mexanizmlari orqali fuqarolarni chuv tushirish holatlariga qarshi kurashish uchun bank tizimi, to'lov tashkilotlari hamda huquq-tartibot organlarining ma'lumotlar bazalarini o'zaro tezkor almashish platformasini mukammallashtirish kerak. Jinoyatchilar tomonidan ishlatiladigan anonim hamyonlar, proksi-serverlar va VPN zanjirlarini yorib o'tish, ularning real IP-manzillarini hamda moliyaviy oqimlarining yakuniy nuqtalarini aniqlashda raqamli kriminalistika (cyber-forensics) imkoniyatlaridan maksimal darajada foydalanish davr talabidir.

To'rtinchidan Yuqori malakali professional kadrlarni tizimli tayyorlash: Kiber-makon daxlsizligini ta'minlashning eng asosiy kaliti — bu yuqori texnologik bilimlarga ega bo'lgan mutaxassislarni o'qitish tizimini yo'lga qo'yishdir. Axborot xavfsizligi, ma'lumotlar tahlili, xakerlik hujumlarini simulyatsiya qilish (ethical hacking) va kiber-huquq sohalari bo'yicha mahalliy mutaxassislarning bilim va ko'nikmalarini yetakchi xalqaro akademiyalar andozalari asosida doimiy ravishda oshirib borish lozim. Shu maqsadda Ichki ishlar vazirligi akademiyasi, Raqamli texnologiyalar vazirligi hamda yangi tashkil etilgan Sun'iy intellekt markazi hamkorligida doimiy ishlovchi kiber-poligonlar va intensiv o'quv kurslarini tashkil etish, sohaga eng iqtidorli yoshlarni jalb etish strategik ahamiyatga ega.

Faqatgina ushbu qat'iy texnik nazorat vertikal, tezkor bloklash tizimlari, kiber-moliyaviy jinoyatlarni fosh etishning intellektual mexanizmlari hamda yuqori salohiyatli professional kadrlar zanjiri uyg'unlashgandagina O'zbekiston Respublikasining raqamli suvereniteti va fuqarolarimizning virtual makondagi xavfsizligi har qanday ichki va tashqi tahdidlardan ishonchli asraladi.

O'zbekiston iqtisodiyoti va ijtimoiy hayotining shiddat bilan raqamli platformalarga ko'chishi kiberxavfsizlik masalasini milliy xavfsizlikning eng dolzarb bo'g'iniga aylantirdi.

Mamlakatimizda jinoyatchilikning transchegaraviy va dinamik tabiati kuchayib borayotgan bir sharoitda, shunchaki an'anaviy choralar bilan cheklanish yetarli emasligi yaqqol ko'rinmoqda.

Jinoyat kodeksining maxsus normalari hamda "Kiberxavfsizlik to'g'risida"gi Qonun tomonidan Davlat xavfsizlik xizmatiga berilgan mutlaq vakolatlar davlat raqamli makonining daxlsizligini ta'minlashda fundamental huquqiy va institutsional poydevor bo'lib xizmat qilmoqda.

Shu bilan birga, davlatimiz rahbari tomonidan qabul qilingan Sun'iy intellekt texnologiyalarini rivojlantirish bo'yicha 2030-yilgacha mo'ljallangan eng yangi strategiya kiber-makonni nazorat qilishni mutlaqo yangi intellektual bosqichga olib chiqdi. Endilikda virtual firgarliklarga, bank-moliya va energetika sohasidagi sabotajlarga qarshi kurashishda "katta ma'lumotlar" bazasi hamda prognozlashtiruvchi algoritmlar asosiy qurol vazifasini o'tamoqda.

Yangi tashkil etilgan Sun'iy intellekt va raqamli iqtisodiyotni rivojlantirish markazi tomonidan amalga oshirilayotgan ekspertizalar hamda kiberxavfsizlik subyektlarining raqamli izlarni saqlash borasidagi qat'iy majburiyatlari tizimning yaxlitligini ta'minlamoqda.

Xulosa o'rinda ta'kidlash lozimki, O'zbekistonning raqamli suvereniteti va fuqarolarimizning virtual xavfsizligi faqatgina qat'iy huquqiy filtrlar, zamonaviy intellektual monitoring mexanizmlari hamda yuqori salohiyatli kiber-madaniyat o'zaro uyg'unlashgandagina to'liq va ishonchli kafolatlanadi. Zero, kiber-makon milliy chegaralardan tashqarida shakllanadigan o'zgaruvchan tizim bo'lgani bois, undagi barqarorlik nafaqat bugungi tahdidlarga to'g'ri huquqiy va texnik javob bera olish, balki ertangi ehtimoliy xavflarni sun'iy intellekt va innovatsion monitoring vositalari orqali barvaqt prognoz qilish qobiliyatiga ham bevosita bog'liqdir. Shu nuqtai nazardan, davlat nazorati mexanizmlarining takomillashuvi, strategik infratuzilmalarning kiber-himoyasi hamda milliy kadrlarning intellektual salohiyati o'zaro yagona tizim sifatida harakat qilishi O'zbekistonni global raqamli makonda nafaqat xavfsiz, balki raqobatbardosh va suveren qudratga ega davlatga aylantiradi.

Binobarin, raqamli tahdidlar shiddat bilan transformatsiya bo'layotgan hozirgi davrda kiber-mudofaa tizimini doimiy ravishda yangilab borish va milliy ekotizim daxlsizligini ta'minlash shunchaki texnik zaruriyat emas, balki barqaror taraqqiyot va davlat mustaqilligining bosh mezonidir. Kelajakda global miqyosdagi har qanday kiber-hujumlarga munosib tahrir bera olish va jamiyatda yuksak darajadagi raqamli immunitetni shakllantirish orqaligina mamlakatimiz raqamli iqtisodiyot va yangi texnologiyalar asrida o'zining strategik manfaatlari hamda xavfsizlik arxitekturasini mutlaq va muqaddas saqlab qolishga erishadi.

Bu jarayonda axborot makonining huquqiy boshqaruvini yanada liberallashtirish va shu bilan birga kiber-tahdidlarga nisbatan jazo muqarrarligini ta'minlash o'rtasidagi oltin muvozanatni topish davlatimizning uzoq muddatli barqarorlik formulasiga aylanadi. Zero, raqamli dunyodagi suverenitet shunchaki texnologik ustunlik emas, balki har bir fuqaroning virtual makondagi daxlsizligi, davlatning raqamli sirlari va milliy moliya tizimining xalqaro maydondagi mutlaq mustaqilligidir. O'zbekiston o'zining strategik qadamlari bilan global kiber-makonda xavfsiz va qudratli brend sifatida shakllanishda davom etadi.

FOYDALANILGAN ADABIYOTLAR RO'YXATI :

1. Rustamboyev M.X. O'zbekiston Respublikasi Jinoyat kodeksiga sharhlar. Maxsus qism. – Toshkent: "Yuridik adabiyotlar publish", 2024.
2. O'zbekiston Respublikasining Jinoyat kodeksi (XX¹-bob. Axborot texnologiyalari sohasidagi jinoyatlar). O'zbekiston Respublikasi Qonun hujjatlari ma'lumotlari milliy bazasi.

3. O'zbekiston Respublikasining "Kiberxavfsizlik to'g'risida"gi Qonuni. 2022-yil 15-aprel, O'RQ-764-son. O'zbekiston Respublikasi Qonun hujjatlari ma'lumotlari milliy bazasi.
4. O'zbekiston Respublikasi Prezidentining "Sun'iy intellekt texnologiyalarini 2030-yilga qadar rivojlantirish strategiyasini tasdiqlash to'g'risida"gi Qarori. 2024-yil 14-oktabr, PQ-358-son. O'zbekiston Respublikasi Qonun hujjatlari ma'lumotlari milliy bazasi.
5. O'zbekiston Respublikasi Qonun hujjatlari ma'lumotlari milliy bazasi — Lexuz rasmiy sayti.