AXBOROT TEXNOLOGIYALARI YORDAMIDA SODIR ETILAYOTGAN JINOYATLARGA QARSHI KURASHISHNING ZAMONAVIY ISTIQBOLLARI

IIV Akademiyasi Oliy ta'limdan keying ta'lim fakulteti Doktorantura doktoranti
Hoshimov Ulug'bek Muhiddin o'g'li

Annotatsiya: Maqolada raqamli transformatsiya jarayonida yuzaga kelayotgan xavf-xatarlar, sun'iy intellekt, "katta ma'lumotlar" (Big Data), blokcheyn va biometrik identifikatsiya texnologiyalaridan foydalanish orqali jinoyatlarning oldini olish hamda ularni fosh etish imkoniyatlari yoritiladi. Shuningdek, xalqaro hamkorlikni kuchaytirish, milliy qonunchilikni takomillashtirish, kiberxavfsizlik madaniyatini oshirish va profilaktik chora-tadbirlarni samarali tashkil etishning ahamiyati asoslab beriladi.

Kalit so'zlar: raqamli transformatsiya, kiberxavf-xatarlar, sun'iy intellekt, katta ma'lumotlar (Big Data), blokcheyn texnologiyasi, biometrik identifikatsiya, jinoyatlarning oldini olish, jinoyatlarni fosh etish, xalqaro hamkorlik, milliy qonunchilikni takomillashtirish, kiberxavfsizlik madaniyati, profilaktik chora-tadbirlar.

Keyingi paytlarda internetdan foydalangan holda bir qator shaxslarning mobil qurilmalarini hamda ijtimoiy tarmoq va messenjerlardagi akkaunt yoki kanallarini zararli dastur yuborish yo'li bilan bloklab (to'sib) qo'yish, ma'lumotlarini o'chirib yuborish, o'zgartirish yoki olib qo'yish bilan qo'rqitib, pul yoki boshqa moddiy manfaatdorlik talab qilish holatlari ro'y bermoqda. Kibermakonda shaxslarning fotosurati, ovozi va boshqa biometrik ma'lumotlarini maxsus dasturlar yordamida soxtalashtirish holatlari ham uchrab turibdi[1].

Bu kabi xavfli nholatlar nafaqat bir mamlakat balki butun dunyo davlatlarini tashvishga solib kelayotganligi hech kimga sir emas. Tan olib aytish lozimki bugungi kunni kecha bilan solishtirib bo'lmaydi. Chunki kibernetika sohasi soniyasayin usib yangi bosqichlarga ko'tarilmoqda. Bu esa nafaqat bizni balki butun jamiyatni mazkur o'zgarishlarga tayyor turishimiz lozimligini anglatadi.

Ayni damda kiber jinoyatlar sohasini aynan bir sohaga ta'luqli deyish mushkul hisoblanadi. Chunki har bir soha borki raqamli transformatsiya bilan bog'lanmagan bulsin. Utmishdqa mazkur jinoyatlarni kamdan kam hollarda bank hisoblarini buzishga urinish kabi kurinishlarini kuzatish mumkin edi, chunki hayotimizdagi ma'lumotlarni

[1] Kun.uz "Kibermakondagi jinoyatlar uchun javobgarlik kuchaytiriladi". https://m.kun.uz/news/2023/10/26/kibermakondagi-jinoyatlar-uchun-javobgarlik-kuchaytiriladi

saaqlovchi asosiy tizimlar qog'oz hujjatlarda saqlanishi bilan bog'liq edi. Ammo endilikda esa zamonaviy tizimlar va elektron tarmoqlarsiz hayotimizni tasavvur qilish bo'lib qo'lgan.

Birlashgan Millatlar Tashkilotining Jinoyatchilikning oldini olish va huquqbuzarlarni profilaktika qilish bo'yicha 10-Kongressida tegishli seminar doirasida raqamli texnologiyalar orqali sodir etiladigan jinoyatlar uchun ikkita asosiy ta'rif ishlab chiqilgan edi. Tor ma'noda, kiberjinoyatchilik (kompyuter jinoyati) bu kompyuter tizimlari xavfsizligining buzib kirilishi va aynan kompyuterlar tomonidan ma'lumotlarning g'arazli maqsadlarda qayta ishlanib foydalanilishi tushuniladi. Kiberjinoyatchilik, keng ma'noda esa, (kompyuter bilan bog'liq jinoyatlar) kompyuter tizimi yoki tarmog'i orqali yoki aynan kompyuterga va raqamli tizimlarga nisbatan sodir etilgan har qanday noqonuniy xatti-harakatlarni, shu jumladan, kompyuter tizimi yoki tarmog'i orqali noqonuniy egalik qilish va ma'lumotlarni taqdim etish yoki tarqatish kabi jinoyatlarni qamrab oladi[2].

Kiberjinoyatchilar internet va kompyuter texnologiyalaridan foydalanuvchilarning shaxsiy kompyuterlarini, smartfon ma'lumotlarini, ijtimoiy tarmoqlardagi shaxsiy ma'lumotlarini, biznes sirlarini, milliy sirlarni va hokazolarni buzish uchun foydalanadilar[3].

Bugungi kunda kiberjinoyatlar shaxsga doir ma'lumotlarni noqonuniy egallash, bank hisoblaridagi pul mablag'larini o'zlashtirish, raqamli platformalar va axborot tizimlari faoliyatini izdan chiqarish, ijtimoiy tarmoqlar orqali firibgarlik harakatlarini amalga oshirish, jinoiy yo'l bilan topilgan mablag'larni legallashtirish (yuvish), shuningdek, terroristik va ekstremistik faoliyatni virtual makonda amalga oshirish kabi keng tarqalgan ijtimoiy xavfli ko'rinishlarda namoyon bo'lmoqda.

Internet tarmoqlari va suniy intelekt texnologiyalaring salbiy ta'siri borasida M.N. Madaminova va L.A.Valiyevlar o'z maqolalarida "Deepfake texnologiyalari psixologik ta'sir, manipulyatsiya va feyk yangiliklar tarqalishiga sabab bo'ladi. Bu esa saylov natijalariga, jamoatchilik fikriga va hatto shaxsiy obro'ga jiddiy zarar yetkazishi mumkin[4]" deb hisoblaydi.

Axborot texnologiyalarining terroristik va ekstremistik xatti-harakatlarida foydalanishi mazkur jinoyatchilikni yangi bosqichga olib chiqdi va kiberterrorizm kabi tushuncha va yanginoyatchilikning kurinishlari vujudga keldi.

[2] Javlon Zoilboyev "Kiberxavfsizlik, raqamli huquq va raqamli gigiyena – kiberjinoyatchilikka qarshi muqobil yechim" https://www.researchgate.net/publication/362407860_Kiberxavfsizlik_raqamli_huquq_va_raqamli_gigiyena_-_kiberjinoyatchilikka_qarshi_muqobil_yechim

[3] Sh.Sh.Suyunov "Kiberjinoyatlarning sabablari va oldini olish choralari". https://econferences.ru/index.php/arims/article/view/7300

[4] M.N. Madaminova va L.A.Valiyev "Globallashuv davrida internet xavfi". https://cyberleninka.ru/article/n/globallashuv-davrida-internet-xavfi-1

Bu borada A.U. Anorboyev kiberterrorizm maxsus xaker dasturlari orqali kompyuter boshqaruvi tarmoqlarini egallab olish va kompyuter viruslari yordamida internet tarmog'ida terakt sodir etish, internet tarmog'ini ishdan chiqarishni ko'zda tutadi, shuningdek kiberterrorizmni - terroristik maqsadlar yo'lida kompyuter va telekommunikatsiya texnologiyalari (asosan internet)dan foydalanish ekanligini ta'diklashgan[5].

Axborot texnologiyalari sohasidagi jinoyatchilikning usishiga sabab bulayotgan va unga qarshi kurashishni qiyilashuviga olib keluvchi sabablarni Internet ijtimoiy tarmoqlari, messenjerlar va videoxosting platformalarida tarqatilayotgan noqonuniy kontent muomalasini cheklash hamda ushbu huquqbuzarliklarni sodir etayotgan shaxslarni aniqlash jarayonida mazkur platformalarning bosh ofislari bilan samarali hamkorlikni yo‘lga qo‘yish masalasida qator tashkiliy-huquqiy muammolar mavjud. Xususan, yurisdiksiya masalalari, axborot almashinuvi mexanizmlarining aniq tartibga solinmaganligi hamda platformalar tomonidan so‘rovlarga o‘z vaqtida javob berilmasligi amaliy samaradorlikka salbiy ta'sir ko‘rsatmoqda.

Bundan tashqari Axborot-kommunikatsiya texnologiyalari yordamida sodir etilayotgan huquqbuzarlik va jinoyatlarni o‘z vaqtida aniqlash, fosh etish hamda oldini olish jarayonida bir qator tizimli muammolar mavjud. Avvalo, raqamli izlarni (digital footprints) aniqlash va tahlil qilish faoliyati yetarli darajada institutsionallashtirilmagan hamda zamonaviy texnologik vositalar bilan to‘liq ta'minlanmagan. Bu esa nafaqat umumiy kiberjinoyatlarni, balki internet tarmoqlari orqali amalga oshirilayotgan terrorizm va ekstremizm bilan bog‘liq jinoyatlarni ham erta bosqichda aniqlash imkoniyatlarini sezilarli darajada cheklaydi. Chunki bunday jinoyatlar ko‘pincha yashirin kommunikatsiya kanallari va anonim platformalar orqali sodir etiladi.

Internet ijtimoiy tarmoqlarini monitoring qilish jarayonida jinoyat alomatlari mavjud bo‘lgan manbalar (akkaunt, profil va veb-saytlar) foydalanuvchilari to‘g‘risidagi ma'lumotlarni tizimli ravishda to‘plash va qayta ishlash mexanizmlarining yetarli darajada yo‘lga qo‘yilmaganligi ham amaliy samaradorlikka salbiy ta'sir ko‘rsatmoqda. Ayniqsa, terroristik va ekstremistik mazmundagi kontentni tarqatayotgan shaxslarni aniqlash, ularning o‘zaro aloqadorligini fosh etish hamda transmilliy tarmoqlarini aniqlash jarayonida bu kamchiliklar yaqqol namoyon bo‘ladi.

Shuningdek, sun'iy intellekt texnologiyalari vositasida sodir etilayotgan jinoyatlarga qarshi kurashish sohasida normativ-huquqiy asoslar to‘liq shakllanmagan. Mazkur yo‘nalishda huquqiy tartibga solish mexanizmlarining aniq belgilanmaganligi yangi turdagi kiberxavflarga, jumladan, terroristik va ekstremistik g‘oyalarni avtomatlashtirilgan tarzda tarqatish, radikallashuv jarayonlarini onlayn muhitda

[5] А.У.Анорбоев “Кибержиноятчилик, унга карши курашиш муаммолари ва киберхавфсизликни таъминлаш истикболлари”. - Тошкент.: 2020. - 197 б.

tezlashtirish kabi holatlarga nisbatan tezkor va samarali choralar ko‘rishni qiyinlashtiradi.

Anonim kripto-aktivlar orqali jinoiy faoliyatni moliyalashtirish, shuningdek, internetning yopiq tarmoqlarida (darknet segmentida) moddiy manfaat evaziga taklif etilayotgan noqonuniy xizmatlardan foydalanish holatlarini aniqlash bo‘yicha monitoring, tahlil va ma’lumotlar to‘plash tizimi yetarlicha rivojlanmagan. Bu holat ayniqsa terroristik va ekstremistik tuzilmalarni moliyalashtirish, ularning faoliyatini yashirin qo‘llab-quvvatlash mexanizmlarini aniqlashda jiddiy muammolarni keltirib chiqarmoqda. Natijada bunday faoliyatni barvaqt aniqlash va moliyaviy oqimlarni to‘sib qo‘yish mexanizmlari to‘liq samaradorlikka ega emas.

Bundan tashqari, internet ijtimoiy tarmoqlarida tarqatilayotgan taqiqlangan mazmundagi, xususan terrorizm va ekstremizmni targ‘ib qiluvchi kontentlarni aniqlash va ularni tezkor bartaraf etish tizimi takomillashtirishni talab etadi. Axborot texnologiyalari orqali sodir etilayotgan jinoyatlarni fosh etishda tezkor-qidiruv tadbirlarining, xususan “ma’lumotlar to‘plash” va “shaxsning aynanligini aniqlash” kabi protsessual harakatlarning kibermakon imkoniyatlaridan keng foydalangan holda amalga oshirilishi yetarli darajada yo‘lga qo‘yilmaganligi ham terroristik va ekstremistik jinoyatlarning oldini olishda to‘siq bo‘lib xizmat qilmoqda.

Shu bilan birga, kripto-aktivlar bilan bog‘liq operatsiyalar ustidan samarali nazorat mexanizmlarining yetarlicha rivojlanmaganligi, shubhali va noqonuniy moliyaviy faoliyatlarni aniqlashda zamonaviy texnologik vositalardan foydalanish darajasining pastligi terrorizm va ekstremizm bilan bog‘liq moliyaviy jinoyatlarni aniqlash imkoniyatini cheklaydi. Mazkur omillar kiberjinoyatchilik, ayniqsa uning terroristik va ekstremistik ko‘rinishlariga qarshi kurashishda kompleks, innovatsion va huquqiy jihatdan puxta asoslangan yondashuvni talab etadi.

Rivojlangan davlatlar tajribasi shuni ko‘rsatadiki, axborot texnologiyalari yordamida sodir etilayotgan jinoyatlarga qarshi kurashish sohasida maxsus qonunchilik normalari qabul qilingan bo‘lib, ularda vakolatli organlarning huquq va majburiyatlari, o‘zaro hamkorlik mexanizmlari hamda javobgarlik choralarining aniq chegaralari belgilab qo‘yilgan. Bunday yondashuv kiberjinoyatlarga qarshi kurashish faoliyatining huquqiy asoslarini mustahkamlash va amaliy samaradorligini ta’minlashga xizmat qiladi.

Kiberjinoyatchilikka qarshi kurashishda, eng avvalo, amaldagi qonunchilik normalarini zamonaviy tahdid va xavf-xatarlarga moslashtirish, huquqiy ta’sir choralarini takomillashtirish hamda soha mutaxassislarining kasbiy salohiyatini muntazam ravishda oshirib borish zarur. Zero, kiberjinoyatchilikning yangi shakl va usullari tezkor rivojlanib borayotgan bir sharoitda huquqni qo‘llash amaliyoti ham innovatsion yondashuvlarni talab etadi.

Mazkur sohada davlat tomonidan tizimli e’tibor qaratilayotganining muhim dalillaridan biri — “Kiberxavfsizlik to‘g‘risida”gi qonunning qabul qilinganidir. Ushbu normativ-huquqiy hujjat 2022- yilda qabul qilinib, kiberxavfsizlikni ta’minlashning tashkiliy-huquqiy asoslarini belgilab berdi. Uning ahamiyati, avvalo, unda nazarda tutilgan talab va mexanizmlarning amaldagi raqamli muhit holatiga mosligi bilan belgilanadi.

Shu bilan birga, mazkur qonun talablari asosida ichki ishlar organlari tizimida hamda boshqa sohalarda kiberjinoyatchilikka qarshi kurashuvchi maxsus tuzilmalar tashkil etilgan bo‘lsa-da, statistik ko‘rsatkichlar kiberjinoyatchilikning yildan-yilga o‘sib borayotganini ko‘rsatmoqda. Bu esa mavjud huquqiy bazani yanada takomillashtirish, xususan, kiberjinoyatchilikning barcha zamonaviy tarmoqlarini qamrab oladigan, vakolatli davlat organlarining huquqiy maqomi va vakolat doirasini aniq belgilab beradigan alohida normativ-huquqiy hujjat loyihasini ishlab chiqish zaruratini yuzaga keltiradi.

Bizningcha mazkur qonun loyhasida axborot-kommunikatsiya texnologiyalari yordamida sodir etilayotgan jinoyatlarni, jumladan terrorizm va ekstremizm bilan bog‘liq harakatlarni aniqlash, oldini olish va fosh etish bo‘yicha kompleks choralar tizimli ravishda quyidagicha amalga oshirilishi belgilanishi lozim:

1. **Internet va ijtimoiy tarmoqlarni monitoring qilish va hamkorlik mexanizmlarini shakllantirish unda**

– Vakolatli organlar internet tarmoqlari va ijtimoiy platformalarda tarqatilayotgan qonun bilan taqiqlangan mazmundagi materiallar (terrorizm va ekstremizm g‘oyalari, giyohvandlik vositalari, pornografik kontent va boshqa) manbalarini (akkauntlar, profillar, veb-saytlar) aniqlaydi va ularni bloklash choralarini ko‘radishi;

– Shu maqsadda internet-provayderlar (masalan, Uzmobile, Ucell, Beeline va boshqa operatorlar) foydalanuvchilarning IP manzili, internetga ulanish vaqti kabi texnik ma’lumotlarni qonun hujjatlarida belgilangan doirada 1–6 oy davomida saqlash va huquqni muhofaza qiluvchi organlarning so‘rovlari asosida taqdim etish tizimi joriy etilishi;

– Platformalar bosh ofislari bilan tuziladigan kelishuvlarda axborot almashinuvi tartibi, javob berish muddatlari, maxfiylik, ma’lumotlarni qayta ishlash qoidalari va ziddiyatlarni hal etish mexanizmlari belgilanishi, shartlarni bajarmagan platformalarga nisbatan O‘zbekiston hududida faoliyatni cheklash choralarini qo‘llash nazarda tutilishi lozim.

1. Sun’iy intellekt va mashinani o‘rganish texnologiyalaridan foydalanishga oid

– GAN (Generative Adversarial Network)[6] asosidagi sun’iy intellekt tizimlari yordamida deepfake va boshqa soxtalashtirilgan kontentlarni aniqlash va ekspertiza o‘tkazish mexanizmi joriy qilinishi.

– AI va Machine Learning asosida shubhali kontentni aniqlash, cheklash va oldini olish bo‘yicha tashkiliy va texnik choralar kuchaytirilishi;

– Real vaqt rejimida ishlovchi monitoring tizimlari ishlab chiqilib, shubhali holatlar vakolatli organlarning ixtiyoriga topshirilishi.

2. **Anonim kripto-aktivlar va yopiq tarmoqlarda jinoyatlarni aniqlash borasida**

– Ichki ishlar vazirligi va tegishli idoralar anonim kripto-aktivlar orqali jinoyatlarni moliyalashtirish, darknet tarmoqlarida jinoyat xizmatlaridan foydalanish holatlarini monitoring qilish, tahlil va ma’lumotlar to‘plashni tashkil etish;

– Kripto-aktivlar va xorijiy internet-provayderlar bilan to‘g‘ridan-to‘g‘ri axborot almashinuvi mexanizmi joriy etiladi, so‘rov yuborish va ma’lumot olish tartibi ishlab chiqilishi;

3. **Tezkor-qidiruv tadbirlari va raqamli dalillarni yig‘ishda oid**

– Tezkor-qidiruv tadbirlari axborot-kommunikatsiya texnologiyalari yordamida raqamli muhitda amalga oshirilishi lozimligi, jumladan:

✓ internet tarmoqlari, ijtimoiy platformalar va messenjerlarda axborotni qidirish, monitoring va tahlil;

✓ tarmoq trafigi tahlili va kiberxavfsizlik vositalari yordamida zararli faoliyatni aniqlash;

✓ sun’iy intellekt va Machine Learning[7] tizimlari yordamida shubhali xatti-harakatlarni tahlil qilish;

✓ raqamli aloqa, moliyaviy va texnik ma’lumotlar o‘rtasidagi bog‘liqliklarni grafik asosida tahlil qilish;

✓ raqamli dalillarni aniqlash, yig‘ish, saqlash va tahlil qilish bo‘yicha kompyuter-texnik va raqamli kriminalistika vositalari;

✓ himoyalangan tarmoqlar va soxtalashtirilgan profilingizlar orqali virtual muhitda tezkor-qidiruv tadbirlarini o‘tkazish.

4. **Blokcheyn[8] va moliyaviy monitoring borasida**

– Vakolatli organlar blokcheyn tarmoqlarida amalga oshirilayotgan tranzaksiyalarni real vaqt rejimida kuzatish, tahlil qilish va xavf darajasini baholash imkonini beruvchi professional dasturiy vositalardan foydalanishi;

[6] https://medium.com/@fraidoonomarzai99/generative-adversarial-network-gan-in-depth-7a9c110dce79
[7] https://www.w3schools.com/ai/default.asp
[8] https://www.linkedin.com/pulse/blockchain-technology-10-things-you-should-know-benjamin

– Shu orqali kiberjinoyatchilik, terrorizm va ekstremizm faoliyatini moliyalashtirish yo‘llari va xavfli tranzaksiyalar aniqlanishi kabi jihatlarni alohida qayt etish loizm.

Ushbu yechimlar to‘plami kiberjinoyatchilik, shuningdek, axborot-kommunikatsiya texnologiyalari yordamida sodir etilayotgan terrorizm va ekstremizm jinoyatlarini aniqlash, oldini olish va fosh etish bo‘yicha kompleks, zamonaviy va texnologik jihatdan samarali tizimni shakllantirish imkonini beradi.

Xulosa urnida shuni aytish mumkinki, Bugungi kunda axborot-kommunikatsiya texnologiyalari yordamida sodir etilayotgan jinoyatlar, jumladan kiberjinoyatchilik, terrorizm va ekstremizm bilan bog‘liq harakatlar jiddiy xavf tug‘dirmoqda. Ularning xususiyati shundaki, ular virtual muhitda yashirin, anonim va transmilliy xarakterga ega bo‘lib, an’anaviy tezkor-qidiruv va huquqni muhofaza qilish mexanizmlari bilan to‘liq fosh etish qiyin. Shu sababli muammolarni aniqlash, raqamli izlarni tahlil qilish, monitoring tizimlarini takomillashtirish, sun’iy intellekt va mashinani o‘rganish texnologiyalaridan keng foydalanish, anonim kripto-aktivlar va yopiq tarmoqlarda moliyaviy oqimlarni nazorat qilish kabi kompleks chora-tadbirlarni joriy etish zarurati dolzarbdir.

Tahlil va yechimlar shuni ko‘rsatadiki, samarali kurash faqat huquqiy, tashkiliy va texnologik mexanizmlarni uyg‘unlashtirish orqali amalga oshirilishi mumkin. Maxsus monitoring tizimlari, tezkor-qidiruv tadbirlari, sun’iy intellektga asoslangan tahliliy vositalar, blokcheyn va moliyaviy monitoring platformalari jinoyatlarni barvaqt aniqlash va oldini olish imkoniyatini sezilarli darajada oshiradi. Shuningdek, internet-provayderlar, ijtimoiy platformalar va xorijiy xizmat ko‘rsatuvchi subyektlar bilan samarali axborot almashinuvi mexanizmlarini yo‘lga qo‘yish, normativ-huquqiy bazani zamon talablariga moslashtirish hamda soha mutaxassislarining kasbiy salohiyatini oshirish muhim ahamiyat kasb etadi.