KIBERJINOYATCHILIKNING YANGI AVLODI VA UNGA QARSHI HUQUQIY KURASH

Ulmasov Muhriddin Bobir o‘g‘li
Qoraqalpog‘iston qishloq xo‘jaligi va agrotexnologiyalar instituti
Yurisprudensiya yo‘nalishi 2-kurs talabasi
ulmasovmuhriddin426@gmail.com
+998940000313

Annotatsiya.

Mazkur maqolada raqamli texnologiyalar taraqqiyoti bilan bog‘liq holda vujudga kelayotgan kiberjinoyatchilikning yangi avlodi — sun’iy intellektga asoslangan hujumlar, xizmat sifatida taqdim etiladigan to‘lov dasturlari (Ransomware-as-a-Service), deepfake texnologiyalaridan foydalangan holda amalga oshiriladigan firibgarliklar, kriptovalyuta sohasidagi jinoyatlar hamda “buyumlar interneti” (IoT) tarmoqlariga qaratilgan hujumlar tahlil qilinadi. Ushbu yangi turdagi tahdidlarning huquqiy tabiati, ularning an’anaviy kiberjinoyatlardan farqi, xalqaro va milliy qonunchilikda ularga qarshi kurashning hozirgi holati o‘rganiladi. O‘zbekiston Respublikasining ushbu sohadagi qonunchilik bazasi tahlil qilinib, mavjud bo‘shliqlar aniqlanadi va ularni bartaraf etish yuzasidan ilmiy asoslangan takliflar ishlab chiqiladi.

Kalit so‘zlar:

kiberjinoyatchilik, raqamli xavfsizlik, sun’iy intellekt, deepfake, ransomware, kriptovalyuta jinoyatlari, buyumlar interneti, kiberxavfsizlik huquqi, Budapesht konventsiyasi, O‘zbekiston qonunchiligi.

Kirish

Axborot-kommunikatsiya texnologiyalarining jadal rivojlanishi nafaqat jamiyat hayotining barcha jabhalarini raqamlashtirdi, balki jinoiy faoliyatning yangi, sifat jihatidan murakkabroq shakllarini ham vujudga keltirdi. Agar XX asr oxiri — XXI asr boshlarida kiberjinoyatchilik asosan kompyuter viruslari, xakerlik hujumlari va oddiy firibgarlik sxemalari bilan cheklangan bo‘lsa, bugungi kunga kelib bu hodisa sun’iy intellekt, katta ma’lumotlar (Big Data), kriptovalyutalar va buyumlar interneti kabi ilg‘or texnologiyalar bilan uyg‘unlashgan holda mutlaqo yangi bosqichga o‘tdi.

Ushbu yangi avlod kiberjinoyatlari o‘zining transchegaraviyligi, yuqori texnologik murakkabligi, avtomatlashtirilganligi va an’anaviy huquq-tartibot organlari uchun aniqlash hamda isbotlash jihatidan noan’anaviyligi bilan ajralib turadi. Natijada mavjud huquqiy tizimlar — jumladan jinoyat-huquqiy normalar, protsessual tartib-qoidalar va xalqaro hamkorlik mexanizmlari — ushbu tahdidlarga adekvat javob berishda muayyan qiyinchiliklarga duch kelmoqda. Shu sababli kiberjinoyatchilikning yangi avlodini ilmiy jihatdan tahlil qilish va unga qarshi samarali huquqiy kurash mexanizmlarini ishlab chiqish dolzarb ilmiy-amaliy ahamiyat kasb etadi.

Maqolaning maqsadi — kiberjinoyatchilikning zamonaviy shakllarini tasniflash, ularning huquqiy xususiyatlarini ochib berish hamda xalqaro va milliy (O‘zbekiston Respublikasi) qonunchilik tajribasi asosida ularga qarshi kurashning mavjud holati va istiqbollarini baholashdan iborat.

1. Kiberjinoyatchilikning yangi avlodi: tushunchasi va o‘ziga xos xususiyatlari

“Kiberjinoyatchilikning yangi avlodi” tushunchasi ostida sun’iy intellekt, mashinaviy o‘rganish, katta ma’lumotlar tahlili, blokcheyn va buyumlar interneti kabi ilg‘or raqamli texnologiyalardan foydalangan holda amalga oshiriladigan,

yuqori darajada avtomatlashtirilgan va o‘zini-o‘zi takomillashtirish qobiliyatiga ega bo‘lgan jinoyiy faoliyat shakllari tushuniladi. Ushbu hodisaning bir qator o‘ziga xos xususiyatlarini ajratib ko‘rsatish mumkin.

Birinchidan, texnologik murakkablik va avtomatlashtirish darajasining yuqoriligi. Zamonaviy kiberjinoyatchilar hujumlarni amalga oshirishda inson ishtirokini minimallashtiruvchi avtonom dasturiy vositalardan foydalanadilar, bu esa jinoyatning miqyosini keskin kengaytiradi.

Ikkinchidan, “xizmat sifatida jinoyat” (Crime-as-a-Service) modelining keng tarqalishi. Endilikda murakkab kiberhujumlarni amalga oshirish uchun chuqur texnik bilimga ega bo‘lish shart emas — tayyor zararli dasturlar, hujum infratuzilmasi va hatto texnik qo‘llab-quvvatlash xizmati sifatida “qora bozor”da sotib olinishi mumkin.

Uchinchidan, transchegaraviylik va anonimlik darajasining ortishi. Kriptovalyutalar, VPN tarmoqlari va anonim brauzerlardan foydalanish jinoyatchilarning geografik joylashuvini va shaxsini aniqlashni sezilarli darajada murakkablashtiradi.

To‘rtinchidan, ijtimoiy muhandislik usullarining sifat jihatidan takomillashuvi. Deepfake texnologiyasi orqali ovoz va videotasvirni soxtalashtirish imkoniyati an’anaviy firibgarlik sxemalarini yangi, ancha ishonchli shaklga keltirmoqda.

2. Zamonaviy kiberjinoyatlarning asosiy turlari

Kiberjinoyatchilikning yangi avlodini quyidagi asosiy yo‘nalishlar bo‘yicha tasniflash mumkin.

Sun’iy intellektga asoslangan hujumlar. Mashinaviy o‘rganish algoritmlari yordamida fishing xatlarini yanada ishonchli shaklda tuzish, parollarni tezkor buzish, tarmoq zaifliklarini avtomatik qidirish kabi hujumlar tobora

ommalashmoqda. Bunday hujumlarning o‘ziga xosligi shundaki, ular vaqt o‘tishi bilan “o‘rganib”, samaradorligini oshirib boradi.

Xizmat sifatidagi to‘lov dasturlari (Ransomware-as-a-Service). Ushbu model doirasida zararli dasturlar ishlab chiquvchilari o‘z mahsulotlarini boshqa jinoyatchilarga ijaraga beradi, tushgan foyda esa ulushlar asosida taqsimlanadi. Bu holat hujumlarning sonini keskin oshirib, huquq-tartibot organlari uchun “bosh ijrochi”ni aniqlashni murakkablashtiradi.

Deepfake texnologiyasidan foydalangan firibgarlik. Yuqori martabali shaxslarning ovozi yoki videotasvirini soxtalashtirish orqali moliyaviy tashkilotlar va jismoniy shaxslarni aldash holatlari dunyo miqyosida tez sur’atlar bilan ko‘paymoqda. Bunday jinoyatlarni isbotlash uchun maxsus raqamli ekspertiza zarur bo‘ladi.

Kriptovalyuta sohasidagi jinoyatlar. Markazlashmagan moliyaviy tizimlar orqali pul yuvish, soxta investitsiya loyihalari (“rug pull”), kripto-birjalarga qaratilgan hujumlar ushbu yo‘nalishning asosiy ko‘rinishlaridir. Kriptoaktivlarning huquqiy maqomi turli davlatlarda har xil belgilanganligi ularni tergov qilishni yanada murakkablashtiradi.

Buyumlar interneti (IoT) tarmoqlariga qaratilgan hujumlar. “Aqlli uy”, sanoat boshqaruv tizimlari va tibbiy qurilmalarga ulangan IoT qurilmalarining xavfsizlik darajasi past bo‘lgani sababli, ular botnet tarmoqlarini yaratish yoki kritik infratuzilmaga hujum qilish uchun foydalaniladi.

3. Xalqaro va milliy huquqiy tartibga solish tajribasi

Kiberjinoyatchilikka qarshi kurashning xalqaro huquqiy asosi sifatida 2001-yilda qabul qilingan Kiberjinoyatchilik to‘g‘risidagi Budapesht konventsiyasini ko‘rsatish mumkin. Ushbu hujjat kompyuter tizimlariga noqonuniy kirish, ma’lumotlarga tajovuz qilish va kompyuter firibgarligi kabi jinoyatlarning umumiy ta’riflarini belgilab, davlatlararo huquqiy yordam mexanizmini shakllantirdi. Biroq

konventsiya asosan an’anaviy kiberjinoyatlarga mo‘ljallangan bo‘lib, sun’iy intellekt va kriptoaktivlar bilan bog‘liq huquqiy munosabatlarni to‘liq qamrab olmaydi, bu esa uni zamonaviylashtirish zaruratini keltirib chiqarmoqda.

O‘zbekiston Respublikasida kiberxavfsizlik sohasini tartibga soluvchi asosiy huquqiy hujjat sifatida “Kiberxavfsizlik to‘g‘risida”gi qonun, shuningdek Jinoyat kodeksining kompyuter axborotlari sohasidagi jinoyatlarga bag‘ishlangan moddalari (jumladan kompyuter tizimiga noqonuniy kirish, zararli dasturlar yaratish va tarqatish, kompyuter axborotini o‘g‘irlash bilan bog‘liq normalar) amal qiladi. Shuningdek, “Elektron tijorat to‘g‘risida”gi va “Shaxsiy ma’lumotlar to‘g‘risida”gi qonunlar raqamli munosabatlarni tartibga solishda muhim o‘rin tutadi.

Shunga qaramay, milliy qonunchilikda sun’iy intellekt yordamida sodir etiladigan jinoyatlarning yuridik tarkibi, deepfake orqali sodir etilgan firibgarlikning maxsus kvalifikatsiyasi va kriptovalyuta operatsiyalarining jinoiy-huquqiy maqomi kabi masalalar yetarlicha aniq tartibga solinmagan. Bu esa amaliyotda huquqni qo‘llash organlari oldida ushbu jinoyatlarni mavjud moddalar bo‘yicha kvalifikatsiya qilishda qiyinchiliklar tug‘dirmoqda.

4. Huquqiy kurashning muammolari va istiqbol yo‘nalishlari

O‘tkazilgan tahlil natijasida kiberjinoyatchilikning yangi avlodiga qarshi kurashishda bir qator muammoli jihatlar aniqlandi. Birinchi navbatda, huquqiy normalarning texnologik taraqqiyotdan orqada qolishi muammosi mavjud — qonunchilik odatda yangi tahdid keng tarqalganidan keyingina unga javob beradi. Ikkinchidan, transchegaraviy jinoyatlarni tergov qilishda davlatlararo huquqiy yordam jarayonining sur’ati zamonaviy raqamli hujumlarning tezligiga mos kelmaydi. Uchinchidan, raqamli dalillarni to‘plash, saqlash va sud jarayonida taqdim etishning yagona standartlashtirilgan tartibi hali to‘liq shakllanmagan.

Ushbu muammolarni bartaraf etish maqsadida quyidagi yo‘nalishlar istiqbolli hisoblanadi: milliy qonunchilikka sun’iy intellekt va kriptoaktivlar bilan bog‘liq

jinoyatlarning maxsus tarkiblarini kiritish; huquq-tartibot organlari xodimlarining raqamli sud ekspertizasi sohasidagi malakasini oshirish; xalqaro hamkorlikni, xususan operativ ma'lumot almashish mexanizmlarini kuchaytirish; shuningdek, davlat va xususiy sektor (bank-moliya tashkilotlari, IT-kompaniyalar) o'rtasida kiberxavfsizlik bo'yicha davlat-xususiy sheriklik tizimini rivojlantirish.

Xulosa

Xulosa qilib aytganda, kiberjinoyatchilikning yangi avlodi zamonaviy huquqiy tizimlar oldiga jiddiy sinovlarni qo'ymoqda. Sun'iy intellekt, deepfake, kriptovalyuta va buyumlar interneti texnologiyalari bilan uyg'unlashgan jinoiy faoliyat shakllari an'anaviy huquqiy vositalar bilan samarali kurashishni murakkablashtirmoqda. Xalqaro tajriba, xususan Budapesht konventsiyasi, muhim asos bo'lib xizmat qilsa-da, uni zamon talablariga moslashtirish zarur. O'zbekiston Respublikasi qonunchiligini ushbu yo'nalishda takomillashtirish, xalqaro hamkorlikni kengaytirish va huquqni qo'llash amaliyotini raqamli ekspertiza imkoniyatlari bilan kuchaytirish kiberjinoyatchilikning yangi avlodiga qarshi samarali huquqiy kurashning zaruriy sharti hisoblanadi.

Foydalanilgan adabiyotlar ro'yxati

1. O'zbekiston Respublikasining "Kiberxavfsizlik to'g'risida"gi Qonuni.

2. O'zbekiston Respublikasi Jinoyat kodeksi (kompyuter axborotlari sohasidagi jinoyatlarga oid moddalar).

3. Council of Europe. Convention on Cybercrime (Budapest Convention), 2001.

4. O'zbekiston Respublikasining "Shaxsiy ma'lumotlar to'g'risida"gi Qonuni.

5. O'zbekiston Respublikasining "Elektron tijorat to'g'risida"gi Qonuni.

6. UNODC. Comprehensive Study on Cybercrime. United Nations Office on Drugs and Crime.

7. Europol. Internet Organised Crime Threat Assessment (IOCTA), so'nggi nashr.