KIBERJINOYATCHILIKKA QARSHI KURASHISH AMALIYOTI: MUAMMO VA YECHIMLAR

Ganiyev Shaxobitdin Xolmatovich
O‘zbekiston Respublikasi IIV Malaka oshirish instituti Yuridik fanlar kafedrasi katta o‘qituvchisi, mayor
tel: +998903171027.

Annotatsiya. *Ushbu maqolada kiberjinoyatchilikning mazmun-mohiyati, o‘ziga xos xususiyatlari, kiberjinoyatchilikka qarshi kurashish va oldini olish, bu borada professional kadrlarni tayyorlash lozimligi, shuningdek uning samarali jihatlariga alohida e’tibor qaratilgan.*

Kalit so‘zlar: *kiberjinoyatchilik, kiberxavfsizlik, kibermakon, axborot xavfsizligi, innovatsion, fishing, huquqbuzarlik, antivirus.*

PRACTICE OF COMBATING CYBERCRIME: PROBLEMS AND SOLUTIONS

Annotation. *This article examines the essence and specific features of cybercrime, measures to combat and prevent cybercrime, and the necessity of training professional personnel in this field. Special attention is also paid to effective aspects of countering cybercrime.*

Keywords: *cybercrime, cybersecurity, cyberspace, information security, innovative, phishing, offense, antivirus.*

So‘nggi paytlarda ijtimoiy tarmoqlarda saytlarni buzib kirish, virusli dasturlar tarqatish kabi holatlar ko‘p uchrayotgani butun dunyoni tashvishga solib kelmoqda. Ayniqsa, dunyoda axborot tizimidan, shu jumladan axborot texnologiyalaridan foydalanib sodir etilib kelinayotgan jinoyatlarning salmog‘ini oshishi tendensiyasi kuzatilmoqda. Albatta, ushbu turdagi jinoyatlarni sodir etgan shaxs O‘zbekiston Respublikasi Jinoyat kodeksiga muvofiq javobgarlikka tortiladi. Statistik ma’lumotlarning tahliliga ko‘ra, oxirgi yillar ichida sodir etilgan ushbu turdagi jinoyatlar oqibatida moddiy zarar ko‘rgan jabrlanuvchilar ko‘p. Bu holat esa, jamiyat hayotining bir nechta sohalariga bir vaqtning o‘zida kirib boradigan jiddiy tahdid mavjudligi haqida xulosa qilish imkonini beradi, chunki u fuqarolarning huquq va erkinliklariga ham, butun mamlakat iqtisodiyotiga ham katta ta’sir qiladi.

Shu bois, 2021 yil 17 sentyabr kuni Tojikiston poytaxti Dushanbe shahrida o‘tkazilgan Shanxay hamkorlik tashkiloti Davlat rahbarlari kengashining yubiley majlisida

Prezidentimiz Sh.M.Mirziyoev “kibermakondagi zamonaviy tahdid va xatarlarga munosib javob qaytarish uchun ShHTning axborot xavfsizligi sohasidagi ekspertlar forumini ta’sis etish to‘g‘risida[76]” tashabbus bilan chiqqan edi.

Ushbu maqolani yoritishdan dastavval “kiberjinoyatchilik”, “kiberxavfsizlik”, “kibermakon” kabi so‘zlarning terminologok tushunchalariga to‘xtalib o‘tishimiz va ularning mazmunini tushunib olishimiz maqsadga muvofiqdir, negaki ijtimoiy va boshqa yuridik adabiyotlarda mazkur terminlar turlicha talqin qilinadi.

Jumladan, kiberjinoyatchilik deganda, 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 tushuniladi[77].

Kiberxavfsizlik deganda esa, kibermakonda shaxs, jamiyat va davlat manfaatlarining tashqi va ichki tahdidlardan himoyalanganlik holatini tushunish lozim. Shuningdek, kibermakon - axborot texnologiyalari yordamida yaratilgan virtual muhitni tushunish mumkin[78].

Hozirgi kunda axborot texnologiyalarining jadal rivojlanishi va kishilik jamiyatining barcha sohalarida Internetdan keng foydalanish kundalik faoliyatning bir qismini tashkil etib, xizmat ko‘rsatish, ilm-fan, ta’lim, elektron tijorat, shuningdek zamonaviy insonning fikrlash tarziga o‘zining ijobiy ta’siri bilan kirib keldi. Hayot sifatini yaxshilash bilan bog‘liq bo‘lgan ushbu o‘zgarishlar bilan bir qatorda, jinoyatchilikning yangi shakllarini rivojlantirishga qulay sharoitlar paydo bo‘lganligini ta’kidlash lozim. Mazkur jinoyatlar o‘z navbatida "Axborot texnologiyalari sohasidagi jinoyatlar" (elektron jinoyatlar) deb nomlanadi.

Axborot tarmog‘i va Internetning jadal rivojlanishi axborot tizimidan, shu jumladan axborot texnologiyalaridan foydalanib sodir etilayotgan jinoyatlarning yangi sodir etish usullari, sub’ektlari, shuningdek, ularga erishishning yangi yo‘llari va vositalarining paydo bo‘lishiga yordam berdi.

Axborot texnologiyalari sohasidagi jinoyatlarning umumiy ob’ektini jinoyat qonuni bilan qo‘riqlanadigan barcha ijtimoiy munosabatlar, maxsus ob’ektini jamoat xavfsizligi va jamoat tartibiga oid, turdosh ob’ektini axborot texnologiyalaridan qonuniy va xavfsiz

[76] https://daryo.uz/k/2021/09/17/shavkat-mirziyoyev-shht-majlisida-kibermakondagi-tahdidlarga-qarshi-axborot-xavfsizligi-sohasidagi-ekspertlar-forumini-tasis-etishni-ilgari-surdi

[77] O‘zbekiston Respublikasining 2022 yil 15 apreldagi “Kiberxavfsizlik to‘g‘risida”gi O‘RQ-764-son Qonuni. (Qonunchilik ma’lumotlari milliy bazasi, 16.04.2022 yil, 03/22/764/0313-son).

[78] O‘sha manba.

foydalanish borasidagi ijtimoiy munosabatlar majmui tashkil qiladi. Ushbu turdagi jinoyatlarning bevosita ob’ekti esa alohida jinoyat turidan kelib chiqadi.

Shuni alohida ta’kidlash kerakki, hozirgi kunda kiberjinoyatlarning asosiy turi sifatida "fishing", ya’ni firibgarlikning bir turi bo‘lib, uning maqsadi foydalanuvchining maxfiy ma’lumotlari - login va parolini qo‘lga kiritish orqali sodir etilayotgan jinoyatlar ko‘payib bormoqda.

Bizning fikrimizcha, fishing orqali ma’lumotlarni o‘g‘irlash, maxfiy maqsadga ega mobil ilovalar orqali elektron qurilmalarga kirib borish va aloqaning himoya qilinmagan kanallarini tomosha qilish orqali bugun ko‘pchilik internet foydalanuvchilari kiberjinoyatlarning qurboniga aylanmoqda.

Bugungi kunda kiberjinoyatchilikda muayyan shaxsning yoki ob’ektning geografik joylashgan nuqtasi to‘g‘risida xabar tarqatish, shaxsiy ma’lumotlar bazasini buzib kirish kabi xizmatlar ommalashgan. Xakkerlar bu kabi ma’lumotlarni internet va ijtimoiy tarmoq foydalanuvchilari tomonidan turli elektron resurslarga ularning foydalanish shartlarini o‘qimasdan turib kirishlari evaziga olishmoqda.

Respublikamizda fishing bilan bog‘liq holda sodir etilgan jinoyatlarning sabablari va ularning sodir etilishiga imkon bergan shart-sharoitlarning tahliliga ko‘ra, jabrlanuvchilar tomonidan asosan quyidagi xatoliklarga yo‘l qo‘yganliklari ma’lum bo‘lgan. Jumladan:

- antiviruslardan foydalanmaslik;
- elektron pochtaga kelgan noma’lum xabarlarni ochish;
- saytning manzil satrini tekshirmaslik;
- xavfsiz bo‘lmagan sahifalar orqali to‘lovlarni amalga oshirish;
- barcha to‘lovlar uchun bitta bank kartasidan foydalanish.

Agarda fuqarolarimiz ushbu xatolarga yo‘l qo‘ymasalar, albatta mazkur firibgarlikdan himoyalanish mumkin va oldi olingan bo‘lar edi.

Jinoyat-huquqiy yondashuvga ko‘ra, kompyuter axboroti yoki raqamli ma’lumotlar axborot texnologiyalari sohasidagi jinoyatlarning predmeti hisoblanadi. Kompyuter axboroti raqamli dasturiy apparatlar yordamida ishlov beriladigan va foydalaniladigan hamda shaxslar, narsalar, faktlar, hodisalar, voqealar va jarayonlar to‘g‘risidagi ma’lumotlarga, shuningdek undan foydalanish tartibini belgilagan mulkdorning identifikatsiyaviy atributlariga ega raqamli apparatlar dasturlari va ma’lumotlar bazalaridir. Raqamli apparatlar dasturlari va ma’lumotlar bazalari ham jinoiy-huquqiy muhofaza etilishi kerak. Raqamli apparatlar dasturlari bir tomondan axborotga ta’sir ko‘rsatish vositasi bo‘lsa, boshqa tomondan komandalar va ma’lumotlar majmuidan iborat axborotdir.

Mazkur turdagi jinoyatlarning sodir etilish soni kundan-kunga ko‘payib borayotganligiga asosiy sabablardan biri sifatida, Facebook, Instagram, Telegram va WhatsApp kabi ijtimoiy

tarmoqlar O‘zbekiston Respublikasining yurisdiksiyasidan ro‘yxatdan o‘tmaganligi sababli, ushbu tarmoqlar orqali jinoyat sodir etgan shaxs haqida batafsil ma’lumot olishning imkoni mavjud emas. Bunday kamchilikning mavjud ekanligi bugungi kunda ushbu turdagi jinoyatlar bo‘yicha holatlarni o‘z vaqtida sinchkovlik bilan, har tomonlama, to‘la va xolisona tekshirib chiqilishida katta muammolardan biri bo‘lib qolmoqda.

Bundan tashqari, bizning fikrimizcha mazkur turdagi jinoyatlarni tergov qilishning muammolaridan yana biri sifatida, surishtiruvchi va tergovchilarning yuridik ma’lumotdan tashqari, axborot texnologiyalari bilan bog‘liq ma’lumotlarga ega emasliklari hisoblanadi. Bu kamchilik esa, surishtiruvchi va tergovchilarning axborot texnologiyalari sohasidagi jinoyatlarning sub’ektlari va sodir etish usullari haqida chuqur tasavvurga ega bo‘lmasligiga olib kelmoqda.

Shu sababli, surishtiruvchi va tergovchilarning bu borda intellektual hamda professional salohiyatini yanada oshirish, kiberjinoyatchilikka qarshi kurashish bo‘yicha kasbiy bilimlarini chuqurlashtirish hamda ko‘nikma va mahoratlarini oshirishni ta’minlash choralarini ko‘rish lozim. Chunki, har qanday jinoyat sodir etilganida, uni sifatli tergov qilish uchun o‘sha jinoyatning tarkibini mukammal bilish talab etiladi.

Bundan tashqari, mazkur turdagi jinoyatlarni tergov qilishning deyarli barcha bosqichlarida axborot texnologiyalari va aloqa tizimlari sohasida kuchli bilim va ko‘nikmalarga ega bo‘lgan mutaxassisning yordami juda zarur bo‘ladi. Bunday mutaxassislar nafaqat maxsus bilimlari bilan tergov jarayoniga ko‘maklashishi, balki maxsus vositalardan samarali foydalanish, jinoyat izlari bo‘lishi mumkin bo‘lgan joylarni va ob’ektlarni aniqlash va ularni ko‘zdan kechirishni bevosita birga amalga oshirib berishlari mumkin.

Bunga misol qilib oladigan bo‘lsak, axborot texnologiyalari sohasidagi jinoyatlarni tergov qilishda raqamli axborotni ko‘zdan kechirish o‘ziga xos murakkabliklarga ega. Bunda albatta mutaxassis ishtirokiga zarurat tug‘iladi. Chunki, ko‘zdan kechirishda raqamli axborotning turi, nomi, hajmi, xususiyatlari va qanday xotira uskunasida joylashganligi, ma’lumotning yozilish shakli, formati, kodlanganligi, umumiy tushunarli ekanligi yoki maxsus raqamlar kombinatsiyasi (parol)dan ifodalanganligi, o‘zgartirilgan sanasi, axborot egasi haqidagi ma’lumotlar, axborot mazmuni va boshqa ahamiyatli jihatlarga e’tibor qaratish zarur.

Axborot texnologiyalari sohasidagi jinoyatlar sodir etilganligini avvalo kompyuter vositasi, tarmog‘i tizimidagi nosozlik, ishlash jarayonidagi uzilishlar, ayrim dasturiy komandalar noto‘g‘ri bajarilishi yoki bajarilmasligi, axborotga ishlov berishdagi nuqsonlar, axborotning yo‘qolishi, o‘zgarishi va shunga o‘xshash holatlar yuzaga kelishi holatlarini o‘rganish orqali aniqlash mumkin. Jinoyat sodir etilganligini, shuningdek jinoyat sodir etgan

shaxslarni aniqlash va ularni fosh etish uchun avvalo kompyuter texnikasi yoki tarmog‘ini ko‘zdan kechirish yohud tegishli ekspertiza o‘tkazish kerak bo‘ladi.

Bizningcha, axborot texnologiyalari sohasidagi jinoyatlarni tergov qilishning asosiy va eng samarali usuli bu kompyuter-texnik ekspertizasini joriy etishdir. Afsuski, bugungi kunda ularning yuqori narxi va murakkabligi tufayli, ushbu turdagi jinoyatlarni tergov qilishda bu turdagi ekspertizadan foydalanilmayapti.

Ekspertiza jarayonining o‘ziga kelsak, ekspert juda mashaqqatli ishlarni bajarishi kerak, misol uchun tashuvchi infeksiyalangan taqdirda, mutaxassis barcha o‘rnatilgan dasturlar va fayllarda mavjud bo‘lgan zararli dasturni (virusni) mustaqil ravishda topishi kerak, albatta bu juda katta vaqtni talab qiladi. Masalan, oldindan o‘rnatilgan Android operatsion tizimiga ega telefon infeksiyalanganida, shubhali ilovalar va dasturlar o‘rganiladi. Zararli virusni tekshirganda, mutaxassis kodning bir qismida virus egasining xabarisiz buzg‘unchi ma’lumotlarni yuboradigan manzilni topadi. Undan keyingi tezkor-qidiruv tadbirlari yordamida gumon qilinayotgan jinoyatchining joylashgan joyini aniqlash va uni ushlash choralari ko‘riladi, so‘ng jinoyatchi shaxsning yashash joyida tergovchi tomonidan tintuv (olib qo‘yish) tergov harakatini tashkil qilishi va o‘tkazishi natijasida ayblov xulosasining asosini tashkil etuvchi dalillar bazasini topish imkonini beradi, undan keyin boshqa tergov harakatlarini ham o‘tkazish choralari ko‘rib boriladi. Bu harakatlar, kelajakda ma’lum chegaralarda tergovchining xatti-harakatlari uchun variant va strategiyani tanlash imkoniyatini beradi.

Xulosa qilib qayd etish lozimki, agar har bir internet foydalanuvchisi va xizmat ko‘rsatuvchilar kiberolamda ham hayotdagi kabi ehtiyotkorlikni unutmasalar, aksariyat kiberjinoyatlarning oldi olingan bo‘lar edi.

Foydalanilgan adabiyotlar

1. O‘zbekiston Respublikasi Konstitutsiyasi – T.: 2024.
2. O‘zbekiston Respublikasi Jinoyat-protsessual kodeksi – T.: 2024.
3. O‘zbekiston Respublikasi Jinoyat kodeksi – T.: 2024.
4. O‘zbekiston Respublikasining 2022 yil 15 apreldagi “Kiberxavfsizlik to‘g‘risida”gi O‘RQ-764-son Qonuni
5. O‘zbekiston Respublikasi Prezidentining 2022 yil 22 yanvar kunidagi “2022 - 2026 yillarga mo‘ljallangan Yangi O‘zbekistonning taraqqiyot strategiyasi to‘g‘risida”gi 60-sonli Farmoni.