KIBERJINOYATCHILIKNI OLDINI OLISH VA UNGA QARSHI KURASHISHNI TAKOMILLASHTIRISH.

Ganiyev Shaxobitdin Xolmatovich
O‘zbekiston Respublikasi IIV Malaka oshirish instituti Yuridik fanlar kafedrasi katta o‘qituvchisi, mayor

Annotatsiya. *Ushbu maqolada kiberjinoyatchilikning tushunchasi, o‘ziga xos xususiyatlari, kiberjinoyatchilikni oldini olish va unga qarshi kurashish amaliyotini takomillashtirish, bu borada professional kadrlarni tayyorlash lozimligi, shuningdek uning samarali jihatlariga alohida e’tibor qaratilgan.*

Tayanch so‘zlar: *kiberjinoyatchilik, kiberxavfsizlik, kiberjinoyat, kibermakon, axborot xavfsizligi, telekommunikatsiya tarmoqlari, Internet jahon axborot tarmoqlari, fishing, vishing, smishing, virusli dastur.*

Dunyoda oxirgi paytlarda telekommunikatsiya, shuningdek Internet jahon axborot tarmoqlarida zarar keltiruvchi dasturlarni yaratish, ishlatish yoki tarqatish kabi holatlar ko‘p uchrayotgani butun dunyoni tashvishga solib kelmoqda. Buning oqibatida axborot texnologiyalari sohasidagi jinoyatlar va axborot tizimidan, shu jumladan axborot texnologiyalaridan foydalanib sodir etilayotgan jinoyatlarning salmog‘ini oshishi tendensiyasi kuzatilmoqda.

Ushbu maqolani yoritishdan dastavval “kiberjinoyatchilik”, “kiberjinoyat”, “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[197].

Kiberjinoyat – kompyuter va tarmoqning birgalikdagi aloqasi ostida sodir etiluvchi jinoyatning bir turidir. Kompyuter jinoyat paytida maqsadli yo‘naltirilgan qurol vazifasini bajarib beradi. Kiberjinoyat kimningdir xavfsizligi va moliyaviy saviyasiga zarar yetkazish maqsadida sodir etiladi[198].

[197] 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).

[198] https://uz.wikipedia.org/wiki/Kiberjinoyat.

Kiberxavfsizlik deganda esa, kibermakonda shaxs, jamiyat va davlat manfaatlarining tashqi va ichki tahdidlardan himoyalanganlik holatini tushunish lozim. Shuningdek, kibermakon deganda, axborot texnologiyalari yordamida yaratilgan virtual muhitni tushunish mumkin[199].

2026-yil 27-yanvar kuni Prezident Sh.M.Mirziyoev ishtirokida o‘tkazilgan “Toshkent shahrida xavfsiz muhitni shakllantirish hamda jamoat xavfsizligini samarali ta’minlash bo‘yicha namunaviy amaliyotni yaratish chora-tadbirlari yuzasidan videoselektor yig‘ilishi”da kiberjinoyatchilik masalasiga ham to‘htalib o‘tildi. Davlatimiz rahbari o‘z so‘zida “Rasmiy ma’lumotlarga ko‘ra, 2025-yili Toshkentda kiberjinoyatlar soni 16 mingdan ortgan. Fuqarolar qariyb 2 trillion so‘m moddiy zarar ko‘rgan bo‘lsa-da, ularni fosh etish 8 foizga ham yetmagan. Jinoyatchilar bank tizimidagi bo‘shliqdan, aholining ishonuvchanligidan va texnologik bilim yetishmasligidan foydalanmoqda. Ichki ishlar va prokuraturaga bu yo‘nalishda barcha masalalarni hal qilib berganman. Qani natija? Bank va to‘lov tashkilotlarida himoya tizimlarini joriy etish qachon yakunlanadi? Avvalroq, IIV O‘zbekistonda 2024-yilda umumiy jinoyatlarning 44,4 foizi kiberjinoyatlar hissasiga to‘g‘ri kelganini ma’lum qilgandi. Kiberjinoyatlarning 98 foizi bank kartalari bilan bog‘liq bo‘lib, fuqarolar 4 yilda 1,9 trln so‘m zarar ko‘rgan. Shuningdek, mashhurlar qiyofasidan foydalangan holda jinoyat sodir etish (dipfeyk) ham ommalashmoqda[200]” deb ta’kidlab o‘tdi.

Statistik ma’lumotlarning tahliliga ko‘ra, oxirgi yillar ichida sodir etilgan ushbu turdagi jinoyatlar oqibatida moddiy zarar ko‘rgan jabrlanuvchilar soni juda 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 qilmoqda.

Shuning uchun ham bejizga, 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[201]” tashabbus bilan chiqmagan edi.

Bugungi 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

[199] 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).

[200] https://www.gazeta.uz/uz/2026/01/27/cyber-crimes/.

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

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 ham ta’kidlash lozim. Mazkur jinoyatlar o‘z navbatida «Axborot texnologiyalari sohasidagi jinoyatlar» (elektron jinoyatlar) deb nomlanadi.

Shu bilan birga, axborot tarmog‘i va Internetning jadal rivojlanishi axborot tizimidan, shu jumladan axborot texnologiyalaridan, telekommunikatsiya va Internet jahon axborot tarmoqlaridan foydalanib sodir etilayotgan jinoyatlarning yangi turlari, sodir etish usullari, sub’ektlari, shuningdek, ularga erishishning yangi yo‘llari 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 foydalanish borasidagi ijtimoiy munosabatlar majmui tashkil qiladi. Ushbu turdagi jinoyatlarning bevosita ob’ekti esa alohida jinoyat turidan kelib chiqadi.

Jinoyat-huquqiy yondashuvga ko‘ra, kompyuter axboroti yoki raqamli ma’lumotlar (elektron ma’lumot) axborot texnologiyalari sohasidagi jinoyatlarning predmeti hisoblanadi.

Shuni alohida ta’kidlash kerakki, hozirgi kunda kiberjinoyatlarning asosiy turi sifatida “fishing”, ya’ni firibgarlikning bir turi bo‘lib, uning maqsadi foydalanuvchining maxfiy ma’lumotlarini qo‘lga kiritish orqali sodir etilayotgan jinoyatlar soni ko‘payib bormoqda. Unga ko‘ra, kiberhujumni amalga oshirayotgan shaxs Internet foydalanuvchilarining shaxsiy va moliyaviy ma’lumotlarini (login, parol, bank kartasi raqami, PIN-kod, CCV-kod) qo‘lga kiritish uchun soxta veb-saytlar, elektron xatlar, SMS yoki ijtimoiy tarmoqlardan foydalanadilar.

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.

Bundan tashqari, “vishing” (ovozli fishing) – bu telefon orqali amalga oshiriladigan firibgarlik usuli bo‘lib, kiberhujumni amalga oshirayotgan shaxs o‘zini go‘yoki bank, davlat idorasi, huquqni muhofaza qiluvchi organlar yoki boshqa nufuzli tashkilot vakili sifatida tanishtirib, shu yo‘l bilan jabrlanuvchilarni shaxsiy ma’lumotlarini qo‘lga kiritadi.

Shuningdek, firibgarlikning yana bir usuli “smishing” (SMS fishing) bo‘lib, unda kiberhujumni amalga oshirayotgan shaxs jabrlanuvchilarga SMS xabar orqali soxta ma’lumot yuborib, ularni shaxsiy ma’lumotlarini oshkor qilishga yoki zararli havolani bosishga majbur qiladilar.

Respublikamizda “fishing”, “vishing”, “smishing” yo‘llari bilan bog‘liq holda sodir etilayotgan jinoyatlarning sabablari va ularning sodir etilishiga imkon bergan shart-sharoitlar

borasida o‘tkazilgan tahlilga ko‘ra, jabrlanuvchilar tomonidan asosan quyidagi xato va kamchiliklarga yo‘l qo‘yayotganliklari va bu turdagi jinoyatlarni qurboniga aylanib qolayotganliklari ma’lum bo‘ldi. Jumladan:

- antiviruslardan foydalanmaslik;
- elektron pochtaga kelgan noma’lum (anonim) 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 xato va kamchiliklarga yo‘l qo‘ymasalar, albatta mazkur jinoyatlardan himoyalangan bo‘ladilar va natijada bu jinoyatlarni oldi olingan bo‘lar edi.

Kiberjinoyatlarning sodir etilish soni kundan-kunga ko‘payib borayotganligiga asosiy sabablardan biri sifatida, Facebook, Instagram, Telegram va WhatsApp kabi ijtimoiy tarmoqlar O‘zbekiston Respublikasining yurisdiktsiyasidan ro‘yhatdan o‘tmaganligini keltirib o‘tishimiz mumkin. Chunki, respublikamizda sodir etilayotgan kiberjinoyatlar asosan ushbu tarmoqlar orqali sodir etilmoqda. Bu tarmoqlar orqali kiberjinoyatni sodir etayotgan shaxs albatta yashirin profili orqali o‘zining ijtimoiy xavfli harakatlarini amalga oshiradi, lekin bu tarmoqlar bizning yurtimizda yurisdiktsiyadan ro‘yhatdan o‘tmaganligi uchun jinoyatni issiq izida fosh etish hamda jinoyat sodir etgan shaxs haqida batafsil ma’lumot olishning imkoni bo‘lmay qolmoqda. Bunday kamchilikning mavjud ekanligi bugungi kunda kiberjinoyatlar bo‘yicha holatlarni o‘z vaqtida sinchkovlik bilan, har tomonlama, to‘la va xolisona tekshirib chiqilishida katta muammo va kamchiliklardan biri bo‘lib qolmoqda.

Shu sababli, tez orada Facebook, Instagram, Telegram va WhatsApp ijtimoiy tarmoqlari bilan xalqaro shartnoma tuzib, ular bilan keng aloqani o‘rnatish lozim. Natijada, ushbu tarmoqlar orqali yashirin profil yordamida jinoyat sodir etayotgan shaxslarni aniqlash va ular haqida batafsil ma’lumotga ega bo‘lish imkoni paydo bo‘ladi hamda bu jinoyatlarni issiq izida fosh etilishiga zamin yaratiladi.

Bundan tashqari, 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‘lmasliklariga 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 tarkibiy elementlarini 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, Jinoyat-protsessual kodeksining 95^1-moddasi 4-qismida “Olib qo‘yish yoki ko‘zdan kechirish bo‘yicha tergov harakatlari olib borilayotganda mutaxassis ishtirokisiz olingan elektron ma’lumotlar nomaqbul dalillar deb topiladi[202]” deb belgilab qo‘yilgan. Sababi bu protsessual harakatlarni amalga oshirish chog‘ida 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.

Shu bois, O‘zbekiston Respublikasi Ichki ishlar vazirligi Malaka oshirish institutida Axborot texnologiyalari sohasidagi jinoyatlarni oldini olish (huquqbuzarliklar profilaktikasi bo‘linmasi), unga qarshi kurashish (jinoyat qidiruv bo‘linmasi) va tergov qilish (tergov bo‘linmalari) xodimlarini malakasini oshirish va kasbiy qayta tayyorlash o‘quv kurslari tashkil etildi. Bundan ko‘zlangan asosiy maqsad xodimlarda axborot texnologiyalari sohasidagi jinoyatlarni oldini olish, ularga qarshi kurashish va tergov qilish bo‘yicha intellektual va professional salohiyatini, kasbiy bilim, amaliy ko‘nikma va mahoratlarini shakllantirishdan iborat.

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

[202] O‘zbekiston Respublikasi Jinoyat-protsessual kodeksi (https://lex.uz/docs/111460).

avvalo kompyuter texnikasi yoki tarmog‘ini ko‘zdan kechirish yohud tegishli ekspertiza o‘tkazish kerak bo‘ladi.

Axborot texnologiyalari sohasidagi jinoyatlar borasida holatga to‘liq va xolisona aniqlik kiritishning asosiy va eng samarali usuli bu kompyuter-texnik ekspertizasini joriy etishdir. Afsuski, bugungi kunda ularning yuqori narxi va murakkabligi tufayli, respublikamizda kiberjinoyatlarni tergov qilishda bu turdagi ekspertizadan foydalanilmayapti.

Ushbu ekspertiza jarayonining o‘ziga kelsak, ekspertning faoliyati barcha davlatga tegishli va xususiy banklar ma’lumotlari bilan integratsiya qilinadi. Natijada ekspertiza tadqiqoti orqali kiberjinoyatlar bo‘yicha talon-toroj qilingan mol-mulklar aynan kim tomonidan tasarruf etilganligiga aniqlik kiritishga zamin yaratiladi. Misol uchun biron-bir shaxsning plastik kartasidan qonunga xilof ravishda pul yechiladigan bo‘lsa, ana shunda ekspert plastik kartadan pul mablag‘lari aynan qaysi hisob raqamga talon-toroj qilinganligi, oxiri kim tomonidan tasarruf etilganligi yoki qaysi bankka tegishli va qaerda turgan bankomat orqali pullar yechib olinganligi, shuningdek boshqa barcha pul aylanmalari haqida batafsil xulosa qilib beriladi. Shu tariqa ushbu jinoyatlarni fosh etish imkoni paydo bo‘ladi hamda bu borada bajariladigan ishlar hajmi kamayishiga ham olib keladi.

Bundan tashqari, ekspert tekshiruvi davomida, Android operatsion tizimiga ega telefon apparati zararlanganda, shubhali ilovalar va dasturlar o‘rganiladi. So‘ng kirib kelgan zararli virus tekshirilib, kodning bir qismida virus egasining xabarisiz buzg‘unchi ma’lumotlarni yuborgan manzil topilishiga erishiladi. So‘ngra bu ma’lumotdan tezkor-qidiruv tadbirlari davomida foydalanib, gumon qilinayotgan shaxsning joylashgan joyini aniqlash va uni ushlash choralari ko‘riladi, undan keyin jinoyatchi shaxsning yashash joyida tintuv (olib qo‘yish) tergov harakatini o‘tkazilishi mumkin va natijada ayblov xulosasining asosini tashkil etuvchi dalillar bazasini topish imkonini beradi, undan keyin vaziyatdan kelib chiqib boshqa protsessual harakatlarni ham o‘tkazish choralari ko‘rib boriladi. Bu harakatlar, kelajakda ma’lum chegaralarda surishtiruvchi va tergovchilarning 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.: 2026.
2. O‘zbekiston Respublikasi Jinoyat-protsessual kodeksi – T.: 2026.
3. O‘zbekiston Respublikasi Jinoyat kodeksi – T.: 2026.

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.

6. O‘zbekiston Respublikasi Prezidentining 2023-yil 31-maydagi “O‘zbekiston Respublikasining muhim axborot infratuzilmasi ob’ektlari kiberxavfsizligini ta’minlash tizimini takomillashtirish bo‘yicha qo‘shimcha chora-tadbirlar to‘g‘risida”gi PQ-167-son Qarori.

7. O‘zbekiston Respublikasi Prezidentining 2023-yil 31-maydagi “Ichki ishlar organlari tizimini raqamli transformatsiya qilish bo‘yicha kompleks chora-tadbirlar to‘g‘risida”gi PQ-167-son Qarori.