AXBOROT TIZIMI (TEXNOLOGIYALARI)DAN FOYDALANIB SODIR ETILADIGAN FIRIBGARLIK JINOYATI TUSHUNCHASI VA TASNIFI

Kudratov Bunyod Baxtiyorovich
Huquqni muhofaza qilish akademiyasi Raqamli kriminalistika ilmiy-tadqiqot institutining Raqamli tergovga ko‘maklashish bo‘limi boshlig‘i

Annotatsiya. *Maqolada axborot texnologiyalaridan foydalanib sodir etiladigan jinoyatlarning turlari, xususan, fishing, vishing, smishing, skimming va Internet orqali firibgarlik usullari batafsil ko‘rib chiqilgan. Shuningdek, ushbu jinoyatlarning O‘zbekiston Respublikasi Jinoyat kodeksidagi huquqiy asoslari tahlil qilinib, ularni tergov qilish jarayonida raqamli dalillardan foydalanish mexanizmlari ko‘rsatilgan.*
Kalit so‘zlar: *axborot tizimi (texnologiyalari)dan foydalanib sodir sodir etilgan firibgarlik jinoyati, fishing, vishing, Budapesht konvensiyasi, raqamli dalillar.*

КОНЦЕПЦИЯ И КЛАССИФИКАЦИЯ МОШЕННИЧЕСТВА, СОВЕРШАЕМОГО С ИСПОЛЬЗОВАНИЕМ ИНФОРМАЦИОННЫХ СИСТЕМ (ТЕХНОЛОГИЙ)

Аннотация. *В статье подробно рассматриваются виды преступлений, совершаемых с использованием информационных технологий, в частности, фишинг, вишинг, смишинг, скимминг, а также методы интернет-мошенничества. Проведен анализ правовой основы данных преступлений в Уголовном кодексе Республики Узбекистан и показаны механизмы использования цифровых доказательств в процессе их расследования.*
Ключевые слова: *мошенничество, совершенное с использованием информационных систем (технологий), фишинг, вишинг, Будапештская конвенция, цифровые доказательства.*

THE CONCEPT AND CLASSIFICATION OF FRAUD CRIMES COMMITTED USING INFORMATION SYSTEMS (TECHNOLOGIYES)

Abstract. *The article provides a detailed overviyew of crimes committed using information technologiyes, particularly phishing, vishing, smishing, skimming, and online fraud schemes. Additionally, it examines the legal framework for these crimes in the Criminal Code of the Republic of Uzbekistan and highlights the mechanisms for utilizing digital evidence in the investigation process.*
Keywords: *fraud crime committed using information systems (technologiyes), phishing, vishing, Budapest Convention, digital evidence.*

Axborot-kommunikatsiya texnologiyalari yordamida sodir etiladigan jinoyatlar deganda, jinoyat qonunchiligi bilan taqiqlangan va sodir etilishi davomida to‘liq yoki qisman axborot-kommunikatsiya texnologiyalaridan foydalangan holda amalga oshirilgan ijtimoiy xavfli qilmishlar tushuniladi.

Axborot texnologiyalari sohasidagi jinoyatlarning xavfli tomoni shundaki, mudofaa, ishlab chiqarish, iqtisodiy, bank va boshqa maqsadlardagi murakkab kompyuter tizimlarining boshqaruv sensorlari bilan bog‘liq harakatlar uchun muhim bo‘lgan ma’lumotlarning yo‘q qilinishi, bloklanishi, modifikatsiyasi odamlarning o‘limiga va ularning sog‘lig‘iga zarar yetkazishi, mulkni yo‘q qilishi, katta miqyosda iqtisodiy zarar yetkazishi mumkin.

Mazkur turdagi jinoyatlarga Internet orqali zararli viruslarning tarqalishi, parollarni buzish,

bank kartalari raqamlari va boshqa bank ma'lumotlarini o'g'irlash, fishing, noqonuniy ma'lumotlarni tarqatish (tuhmat, pornografik, etnik va diniy adovatni qo'zg'atadigan materiallar va boshqalar), shuningdek turli xil tizimlarning ishlashiga kompyuter tarmoqlari orqali zararli oqibatga olib keladigan darajada aralashish kiradi.

Jinoyat kodeksida axborot-kommunikatsiya texnikasi vositalaridan foydalanib mulkni o'zlashtirish yoki rastrata qilish, kompyuter texnikasi vositalaridan foydalanib sodir etilgan firibgarlik, kompyuter tizimiga ruxsatsiz kirish orqali mulkni o'g'irlash kabi kompyuter jinoyatlari uchun javobgarlik ko'zda tutilgan.

"Kiberjinoyatchilik" tushunchasi ham axborot-kommunikatsiya texnologiyalari sohasida sodir etilgan ko'plab turdagi jinoyatlarni o'zida birlashtirgan. Virtual tarmoqda dahshat solish, virus va boshqa zararli dasturlar, qonunga zid axborotlar tayyorlash va tarqatish, elektron xatlarni ommaviy tarqatish (spam), xakerlik hujumi, veb-saytlarga noqonuniy kirish, firibgarlik, mualliflik huquqini buzish, kredit kartochkalari raqami va bank rekvizitlarini o'g'irlash (fishing va farming) hamda boshqa turli huquqbuzarliklar shular jumlasidandir. Bunday holatlarda jinoyatchilar o'zlarini qiziqtirgan "obyektlar"ga moddiy va ma'naviy zarar yetkazishni oldilariga maqsad qilib qo'yadilar.

Kiberjinoyatchilikni xalqaro miqyosda ham, ayrim davlatlar darajasida ham tushunishda yagona yondashuv yo'qligini hisobga olib, kiberjinoyatchilik turlarini ikkita katta guruhga bo'lish mumkin.

1) jahon amaliyotida uchraydigan kiberjinoyatchilik turlari;

2) O'zbekiston Respublikasining milliy qonunchiligida nazarda tutilgan kiberjinoyatchilik turlari.

Xalqaro hujjatlarga nazar soladigan bo'lsak, Yevropa Ittifoqining Kompyuter jinoyatlari to'g'risidagi konvensiyasida *(23.11.2001-yil, Budapesht)* kiberjinoyatchilik 5 guruhga bo'lingan:

- kompyuter ma'lumotlari va tizimlarining maxfiyligi, yaxlitligi va ulardan foydalanishiga qarshi jinoyatlar (qonunga xilof ravishda foydalanish va qo'lga kiritish, ma'lumotlarga ta'sir qilish, tizimning ishlashiga ta'sir qilish, qurilmalardan noqonuniy foydalanish);
- sodir etilishi uchun kompyuter ishlatiladigan jinoyatlar (kompyuter texnologiyalari yordamida soxtakorlik, kompyuter texnologiyalari yordamida firibgarlik va h.k.);
- ma'lumotlar mazmuni bilan bog'liq jinoyatlar (bolalar pornografiyasi);
- mualliflik va turdosh huquqlarning buzilishi bilan bog'liq jinoyatlar;
- kompyuter tizimlari orqali sodir etilgan irqchilik va ksenofobiya bilan bog'liq jinoyatlar.

O'z navbatida, BMTning "Kiberjinoyatchilik muammosini har tomonlama o'rganish" mavzusidagi dastlabki hisobotida kiberjinoyatchilik uchta asosiy toifaga bo'linadi. Bular: kompyuter ma'lumotlari yoki tizimlarining maxfiyligi, yaxlitligi va ulardan foydalanish imkoniyatiga qarshi jinoyatlar; kompyuter vositalaridan foydalanish bilan bog'liq huquqbuzarliklar; kompyuter ma'lumotlarining mazmuni bilan bog'liq jinoyatlar.

Qonunchilikda axborot tizimi yoki texnologiyalaridan foydalangan holda firibgarlik qilish maxsus tartibda ko'zda tutilgan bo'lib, bu jinoyatlar o'ziga xos xususiyatlarga ega. Bunday huquqbuzarliklar, odatda, axborot xavfsizligi va shaxsiy ma'lumotlarni himoya qilish tartiblarini buzish, elektron tijorat hamda bank operatsiyalariga aralashish yoki yolg'on ma'lumotlar taqdim etish orqali amalga oshiriladi.

Firibgarlik jinoyatining ushbu turi oddiy fuqarolardan tortib, yirik kompaniyalargacha zarar yetkazishi mumkin. Jinoyatchilar, odatda, soxta veb-saytlar yaratish, fishing usullaridan foydalanish, shaxsiy ma'lumotlarni o'g'irlash, elektron hujjatlarni qalbakilashtirish, dasturiy viruslar va zararli kodlar ishlab chiqish kabi usullardan foydalanadilar.

O'zbekiston Respublikasi Jinoyat kodeksining 168-moddasi 3-qismi "g" bandida axborot tizimidan, shu jumladan axborot texnologiyalaridan foydalanib firibgarlik, ya'ni aldash yoki ishonchni suiiste'mol qilish yo'li bilan o'zganing mulkini yoki o'zganing mulkiga bo'lgan huquqni qo'lga kiritish jinoyati uchun

jinoiy javobgarlik belgilangan bo‘lib, unga ko‘ra ushbu jinoyatni sodir etgan shaxsga nisbatan bazaviy hisoblash miqdorining uch yuz baravaridan to‘rt yuz baravarigacha miqdorda jarima yoki ikki yildan uch yilgacha axloq tuzatish ishlari yoxud muayyan huquqdan mahrum etilgan holda **besh yildan sakkiz yilgacha ozodlikdan mahrum qilish** jazosi tayinlanishi belgilangan.

Shuningdek, O‘zbekiston Respublikasi Oliy sudi plenumining 2023-yil 23-iyundagi “Firibgarlikka oid ishlar bo‘yicha sud amaliyoti to‘g‘risida”gi 17-son qarorining 22-bandida berilgan tushuntirishga ko‘ra, axborot tizimidan, shu jumladan axborot texnologiyalaridan foydalanib firibgarlik sodir etish *(JK 168-moddasi uchinchi qismi “g” bandi)* deganda, moliya, bank muassasalari, fondlar va boshqalarda bo‘lgan mulkni aldov yo‘li bilan kompyuter texnikasi vositalari, aloqa vositasi, planshet yoki boshqa shu kabi texnik qurilmalar yordamida manipulyatsiya qilish orqali amalga oshiriladigan talon-toroj tushuniladi. Bunday firibgarlik kompyuter tizimida ishlov beriladigan, tegishli axborot tashuvchilarda saqlanadigan yoki ma’lumotlarni uzatish tarmoqlari bo‘yicha beriladigan axborotni o‘zgartirish yo‘li bilan ham, kompyuter tizimiga yolg‘on axborot kiritish yo‘li bilan ham sodir etilishi mumkin.

Axborot tizimidan, shu jumladan axborot texnologiyalaridan foydalanib sodir etilgan firibgarlik jinoyatini qonunga xilof ravishda (ruxsatsiz) axborot tizimiga kirib yoki undan foydalanib sodir etilgan o‘g‘irlik jinoyatidan farqlashda shuni nazarda tutish lozimki, firibgarlikda jabrlanuvchi aldov yoki ishonchi suiste’mol qilinishi oqibatida mulkini yoki unga bo‘lgan huquqni axborot texnologiyalaridan foydalanib aybdor egaligiga ixtiyoriy ravishda o‘tkazadi, bunda mulk o‘z egaligidan chiqib ketayotganligini jabrlanuvchi anglagan bo‘lishi kerak.

Agar shaxs kompyuter texnikasi yordamida qalbaki hujjat tayyorlab, so‘ng undan mulkni qo‘lga kiritish uchun foydalangan bo‘lsa, qilmishni Jinoyat kodeksining 168-moddasi uchinchi qismi “g” bandi bilan kvalifikatsiya qilib bo‘lmaydi.

Axborot texnologiyalari yordamida sodir etiladigan jinoyatlar soni va turlari yildan yilga ortib bormoqda. Quyida biz ushbu sohada eng ko‘p sodir etiladigan va nafaqat mamlakatimizda, balki dunyo miqyosida ham tergov metodikasida o‘ziga xosliklarga ega bo‘lgan bir qator jinoyat turlariga to‘xtalib o‘tamiz.

Vishing – telefon aloqasi orqali ijtimoiy muhandislikni qo‘llagan holda amalga oshiriladigan firibgarlik, bunda firibgar bank xodimi, xaridor rolini o‘ynab, to‘lov karta konfidensial ma’lumotlarini bilib oladi va kartadagi mablag‘ni o‘zining hisob raqamiga yo‘naltiradi.

O‘z navbatida, bu holatlar mamlakatimizda ham avj olmoqda. Xususan, Internet firibgarlari o‘zlarini bank xodimi sifatida tanishtirib, go‘yoki shubhali moliyaviy operatsiya yuz berayotganligi sababli bank plastik karta bloklanishi, mijozning nomidan katta miqdorda onlayn kredit olishga harakat bo‘layotganligini aytib, foydalanuvchi to‘g‘risida konfidensial ma’lumotlarni ko‘lga kiritib, pul mablag‘larini talon-toroj qilishmoqda.

Vishing uslubi yordamida konfidensial ma’lumotlarni qo‘lga kiritish orqali jabrlanuvchining bank plastik kartasidagi mablag‘larni egallashning keng tarqalgan ko‘rinishi sifatida quyidagi holatni ko‘rish mumkin.

Ijtimoiy tarmoqlarda yoki televideniyeda namoyish qilingan, moddiy ko‘makka muhtoj bo‘lgan fuqarolarni qidirib topib, ularga qo‘ng‘iroq qilib bog‘lanib, o‘zlarini xayriya jamoasining ehson qiluvchilari sifatida ko‘rsatadi. Muhtoj fuqarolarning ishonchiga kirib olgach, hozirda bank plastik kartasida qancha puli borligini va sog‘lig‘i tiklanishi uchun yana qancha mablag‘ kerakligini so‘raydi. Keyin bank plastik kartasiga mablag‘ o‘tkazib berishini aytib, bank plastik raqamini so‘raydi, keyin o‘tkazmani yuborishda muammo borligini bildirib, unga kod yuborilganligini, o‘sha kodni o‘qib berishini so‘raydi. Fuqaro kodni o‘qib bergandan so‘ng, firibgar muhtoj insonning bank plastik raqamiga ulanib olib, hisobida bo‘lgan jami mablag‘larini o‘zining bank plastik raqamiga o‘tkazib oladi.

“Nigeriyalik xati” yoki “Skam-419” – Ukrainadagi voqealardan ijobiy foydalanishni ko‘zlagan "nigeriyalik” xakerlar o‘zlarini Ukra-

inada milliardlab mablag‘i qolib ketgan siyosatchi, sanksiyalar ta’siriga tushgan rossiyalik tadbirkor deb tanishtirib, jabrlanuvchilarga meros yoki uning ulushini yuborish uchun boj, soliq, aviachipta, mehmonxona va boshqa xarajatlari uchun pul undirib kelganlar.

Ushbu kiberfiribgarlikning yana bir ko‘rinishida, firibgar o‘zini bank xodimi yoki millioner boyning vafot etganligini eshitgan rasmiy shaxs (bank xodimi) sifatida tanishtirib, uning merosini familiyadoshi bo‘lgan jabrlanuvchiga yetkazib berishda yordam ko‘rsatishni taklif qiladi.

Buning evaziga notarius xarajati, davlat boji, pochta to‘lovlari va berilgan porani o‘rnini qoplash uchun mablag‘ yuborilishini talab qiladi.

Pandemiya sharoitida “Nigeriya xatlari” ham o‘ziga xos yangi firibgarlik uslublari orqali ko‘plab fuqarolarning mablag‘larini noqonuniy qo‘lga kiritishgan.

Noqonuniy qimor o‘yinlari yoki onlayn o‘yinlar – bu Internetda eng tez ommalashayotgan sohalardan biri. Internetning afzalliklari, shuningdek dunyoning turli mamlakatlarida qimor o‘yinlarining qonuniyligi to‘g‘risidagi turli xil hujjatlarning mavjudligini bilgan holda jinoyatchilar ushbu imkoniyatlardan deyarli hamma joyda foydalanadi.

Skimming – maxsus qurilma (skimmer) yordamida bank plastik karta ma’lumotlarini o‘g‘irlash. Skimmer yordamida barcha ma’lumotlar (egasining ismi, karta raqami, amal qilish muddati, CVV va CVC kodlar) kartaning magnit chizig‘idan ko‘chiriladi. Pin-kodni minikamera yoki bankomatga o‘rnatilgan maxsus klaviatura orqali aniqlash mumkin.

Smishing – SMS xabar orqali amalga oshiriladigan fishing turi. Bunda firibgar jabrlanuvchiga fishing saytiga havolani o‘z ichiga olgan SMS xabar yuboradi va ushbu saytga kirishga undaydi.

Fishing – Internet firibgarligining bir turi bo‘lib, foydalanuvchining identifikatsion ma’lumotlarini (parol, kredit karta raqami, bank hisob raqami, telefon raqami va boshqalar) qo‘lga kiritish uning asosiy maqsadi hisoblanadi.

Fishing quyidagi ko‘rinishlarda uchraydi:

– firibgarlar tomonidan mashhur kompaniyalar nomidan login va parolni tasdiqlash so‘rovi bilan millionlab xatlar turli xil elektron pochtalarga yuboriladi. URL manzilga kirilganda haqiqiysiga judayam o‘xshash bo‘lgan resursga kiriladi;

– ehson uchun pul yig‘ilishi, xayriya tadbirlari o‘tkazish orqali mablag‘ to‘plash uchun tashkil etilgan soxta Internet tashkilotlari veb-resurslariga yo‘naltiriladi;

– narxlari judayam arzon bo‘lgan onlayn-do‘konlarda aslida mavjud bo‘lmagan tovarlar uchun mablag‘ to‘lanadi. Haqiqiy mahsulotning surati ostiga arzon narx yoziladi.

Jamiyat va texnologiyaning rivojlanishi bilan bir qatorda, axborot tizimlari orqali sodir etiladigan jinoyatlar soni ham ortib bormoqda. Bugungi kunda firibgarlik jinoyatlari an’anaviy shakllardan tashqari, raqamli texnologiyalar vositasida ham amalga oshirilmoqda. Bu esa huquqni muhofaza qiluvchi organlar oldida raqamli dalillarni topish, to‘plash va ularni protsessual tartibda rasmiylashtirish bo‘yicha yangi vazifalarni qo‘ymoqda. Shu munosabat bilan, mazkur maqolada axborot tizimlari vositasida sodir etiladigan firibgarlik jinoyatlarini tergov qilishda raqamli dalillarning o‘rni va ularning protsessual jihatlarini tahlil qilishga harakat qilamiz.

Raqamli dalillar – axborot texnologiyalari yordamida shakllangan va elektron tarzda mavjud bo‘lgan ma’lumotlar bo‘lib, ular jinoyatlarni tergov qilishda muhim ahamiyatga ega. Bunday dalillarga quyidagilar kiradi:

kompyuter va serverlarda saqlanayotgan fayllar;

elektron pochta, messenjer va ijtimoiy tarmoqlar orqali xabarlar;

IP-manzillar va Internet foydalanuvchilarining log-fayllari;

mobil qurilmalardagi ma’lumotlar, shu jumladan, qo‘ng‘iroqlar tarixi va GPS-lokalizatsiya ma’lumotlari.

Raqamli dalillarning yuridik ahamiyatini ta’minlash uchun ularni yig‘ish va rasmiylashtirishda quyidagi protsessual talablarga rioya qilish zarur:

dalillarning yaxlitligi va aslligi – raqamli

dalillar o‘zgarmagan holda saqlanishi va har qanday o‘zgartirishlar qayd qilinishi kerak;

dalillarni hujjatlashtirish – har bir olingan raqamli dalil protsessual tartibda rasmiylashtirilishi va ekspertizaga yuborilishi lozim;

mutaxassislar ishtirokini ta’minlash – kiberjinoyatchilikka oid ishlarda maxsus ekspertlar va IT mutaxassislarining ishtiroki muhim ahamiyat kasb etadi.

Tergov organlari jinoyatning sodir bo‘lish mexanizmini aniqlash uchun kiber tahlil ishlarini olib boradilar. Bu jarayonda elektron qurilmalardan, internet-provayderlardan va bank tizimlaridan ma’lumotlar so‘raladi.

Tergovchilar raqamli dalillarning manbasi, olingan sanasi va tekshirish usullarini rasmiy hujjatlar orqali tasdiqlashlari kerak. Bu jarayonda ekspert xulosasi olinib, dalillarning haqqoniyligi to‘g‘risidagi ma’lumotlar kiritiladi.

Sudda raqamli dalillarni qonuniy ishlatish uchun ularni yig‘ish, hujjatlashtirish va ekspertiza qilish jarayonlari hech qanday protsessual qonunbuzarliklarsiz amalga oshirilgan bo‘lishi kerak. Raqamli dalillarning ishonchliligini sud tomonidan baholash uchun mutaxassislarning tushuntirishlari talab qilinishi mumkin.

Axborot texnologiyalari vositasida sodir etiladigan firibgarlik jinoyatlari zamonaviy huquqiy tizim uchun jiddiy muammolarni keltirib chiqaradi. Shu sababli, raqamli dalillarni qonuniy ravishda yig‘ish va rasmiylashtirish jarayonlarini takomillashtirish talab etiladi. Bu borada quyidagi takliflarni ilgari surish mumkin:

raqamli dalillarni yig‘ish va ekspertiza qilish bo‘yicha milliy qonunchilikni xalqaro standartlarga moslashtirish;

tergov va sud organlari xodimlarini raqamli dalillar bilan ishlash bo‘yicha maxsus tayyorlash;

sudlarda raqamli dalillardan foydalanish qoidalarini aniq belgilash.

Yuqoridagi chora-tadbirlar raqamli dalillarning qonuniy tartibda yig‘ilishi va sud jarayonlarida samarali qo‘llanilishini ta’minlashga yordam beradi.

Xulosa qilib aytganda, axborot tizimi va texnologiyalaridan foydalanib sodir etiladigan firibgarlik jinoyatlari jamiyat uchun katta xavf tug‘diradi va ularga qarshi kurashda huquqni muhofaza qiluvchi organlar tomonidan zamonaviy texnologiyalardan samarali foydalanish talab etiladi. Jinoyatlarning bunday turlarini aniqlash, tergov qilish va sud muhokamasiga yetkazish uchun professional malaka, huquqiy bilim va texnik vositalardan foydalanish muhim ahamiyat kasb etadi.

Foydalanilgan manbalar

1. O‘zbekiston Respublikasining Konstitutsiyasi // lex.uz.
2. O‘zbekiston Respublikasi Jinoyat kodeksi // lex.uz.
3. O‘zbekiston Respublikasi Jinoyat-protsessual kodeksi // lex.uz.
4. O‘zbekiston Respublikasining 2024-yil 21 noyabrdagi O‘RQ-1003-sonli qonuni // lex.uz.
5. O‘zbekiston Respublikasi tomonidan ratifikatsiya qilingan xalqaro shartnomalar // lex.uz.
6. *Rustambayev M.X.* O‘zbekiston Respublikasi Jinoyat kodeksiga sharhlar. – Toshkent, 2024.
7. *Вехов В.Б., Вехова В.Б., Зуев С.В.* Цифравая криминалистика: Учебник. – М., 2022.
8. *Вехов В.Б., Зуев С.В., Григорьев В.Н.* Расследование преступлений в сфере компьютерной информации и электронных средств платежа: Учебник. – М.: 2023.
9. *Берова Д.М.* Расследование киберпреступлений // Пробелы в российском законодательстве. – М., 2021.
10. *Сафонов О.М.* Уголовно-правовая оценка использования компьютерных технологий при совершении преступлений: состояние законодательства и правоприменительной практики, перспективы совершенствования: Автореф. канд. юрид наук. – М., 2023. – 22 с.
11. *Тлиш А. Д.* Проблемы методики расследования преступлений в сфере экономической деятельности, совершаемых с использованием компьютерных технологий и пластиковых карт: Автореф. канд. юрид наук. – М., 2024. – 24 с.
12. Применение специальных познаний по преступлениям, связанным с использованием пластиковых карт / Д. М. Берова, В. А. Гаужаева // Пробелы в российском законодательстве. – 2015. – № 3.
13. *Шаевич А. А.* Особенности использования специальных знаний в сфере компьютерных технологий при расследовании преступлений: Автореф. канд. юрид наук. – М., 2023. – 22 с.