AXBOROT TEXNOLOGIYALARI SOHASIDA JINOYATCHILIKNING OLDINI OLISHNING ZAMONAVIY JIHATLARI

Mirzajonov Murodjon Muzaffar o‘g‘li
Namangan viloyati Ichki Ishlar Boshqarmasi Axborot-texnologiyalari sohasidagi jinoyatlarga qarshi kurashish boshqarmasi tergov guruhi, katta tergovchisi, katta leytenant

Annotatsiya: *Mazkur maqolada axborot texnologiyalari sohasidagi jinoyatlarni oldini olishning dolzarb masalalari tadqiq etilgan. Raqamli texnologiyalarning jadal rivojlanishi jinoyatchilikning yangi shakl va usullarini yuzaga keltirmoqda. O‘zbekiston Respublikasida kiberjinoyatlar soni so‘nggi besh yilda 68 barobarga oshib, 2024 yilda 58 800 ta jinoyat qayd etilgan. Tadqiqot doirasida mahalliy va xalqaro tajriba tahlil qilinib, Rossiya Federatsiyasi, Singapur, Estoniya kabi davlatlarning ilg‘or amaliyoti o‘rganilgan. Muallif tomonidan kiberjinoyatlarning asosiy turlari (zararli havolalar orqali kartalarni boshqarishni olish, SMS-kodlarni o‘g‘irlash, onlayn-kredit firibgarliklari) sistemalashtirilgan. Maqolada biometrik ikki faktorli identifikatsiya, dinamik o‘tkazma kechiktirish, qoidalar-triggerlarga asoslangan anomaliyalarni aniqlash, yagona maqsadli raqamlar bazasi, bank operatorlarini maxsus savollar bilan ta’minlash kabi amaliy choralar taklif etilgan. Tadqiqot natijalari huquqni muhofaza qiluvchi organlar faoliyatini samaradorligini oshirishga va aholining raqamli xavfsizligini ta’minlashga qaratilgan.*

Kalit so'zlar: *kiberjinoyatchilik, axborot texnologiyalari, jinoyatlarni oldini olish, kiberxavfsizlik, bank kartalari, biometrik identifikatsiya, sun'iy intellekt, fishing.*

MODERN ASPECTS OF CRIME PREVENTION IN THE FIELD OF INFORMATION TECHNOLOGIES

Abstract: *This article examines current challenges in preventing crimes in the field of information technology. The rapid development of digital technologies has led to the emergence of new forms and methods of criminal activity. In the Republic of Uzbekistan, the number of cybercrimes has increased 68-fold over the past five years, with 58,800 crimes recorded in 2024. The study analyzes local and international practices, examining best practices from countries such as the Russian Federation, Singapore, and Estonia. The author systematizes the main types of cybercrimes (obtaining card control through malicious links, SMS code theft, online credit fraud). The article proposes practical measures such as biometric two-factor authentication, dynamic transfer delays, rule-based anomaly detection triggers, unified fraud number database, and specialized questioning protocols for bank operators. The research findings are aimed at improving the effectiveness of law enforcement agencies and ensuring digital security of the population.*

Keywords: *cybercrime, information technology, crime prevention, cybersecurity, bank cards, biometric authentication, artificial intelligence, phishing.*

KIRISH

Zamonaviy jamiyatning taraqqiyoti axborot va kommunikatsiya texnologiyalari (AKT)ning jadal rivojlanishi bilan chambarchas bog'liq. Raqamli texnologiyalar iqtisodiyot, ta'lim, sog'liqni saqlash, moliyaviy xizmatlar va boshqa hayot sohalarida keng qo'llanilmoqda. Biroq, texnologik yutuqlar bilan birga jinoyatchilikning yangi shakllari ham yuzaga kelmoqda. Kiberjinoyatchilik bugungi kunda global xavfsizlik uchun eng jiddiy tahdidlardan biriga aylangan.

O'zbekiston Respublikasida kiberjinoyatlar muammosi tobora o'sib bormoqda. 2025-yil 29-maydagi ma'lumotlarga ko'ra, so'nggi besh yilda kiberjinoyatlar soni 68 barobarga oshgan [1]. Agar 2019-yilda 18 turda 863 ta jinoyat qayd etilgan bo'lsa, 2024-yilda bu ko'rsatkich 62 turda 58 800 tagacha yetdi [2]. Bu holat kiberjinoyatchilikning umumiy jinoyatchilikdagi ulushining keskin o'sishidan dalolat beradi: 2023-yilda bu ulush 6,2 foizni tashkil etgan bo'lsa, 2024-yilda 44,4 foizga yetdi [2]. Boshqacha qilib aytganda, har ikkinchi jinoyat axborot texnologiyalari yordamida sodir etilmoqda.

Jinoyatlar natijasida 2021-2024 yillarda fuqarolardan 1,9 trillion so'mdan ortiq mablag' o'g'irlangan [2]. Prezident Shavkat Mirziyoyev tomonidan 2026-yil 26-yanvar kuni o'tkazilgan yig'ilishda ta'kidlanganidek, faqat poytaxtda kiberjinoyatlar soni 16 mingdan oshib, fuqarolar qariyb 2 trillion so'm moddiy zarar ko'rgan, fosh etish 8 foizga ham yetmayapti [3]. Bu holat dolzarb masalalarning hal etilishini talab qiladi.

Jahon amaliyoti ham xavotirli tendensiyalarni ko'rsatmoqda. Rossiya Ichki ishlar vazirligi ma'lumotlariga ko'ra, 2024-yilda Rossiya Federatsiyasida axborot-telekommunikatsiya texnologiyalaridan foydalangan holda 765 400 ta jinoyat sodir etilgan, ulardan 369 300 tasi og'ir va o'ta og'ir jinoyatlar hisoblanadi [4]. Bu statistika kiberjinoyatchilik global muammo ekanligini tasdiqlaydi.

Mazkur tadqiqotning maqsadi O'zbekiston Respublikasi sharoitida kiberjinoyatlarni oldini olishning samarali choralarini ishlab chiqish, xalqaro tajribani tahlil qilish va amalda qo'llash mumkin bo'lgan tavsiyalar berish hisoblanadi.

ADABIYOTLAR TAHLILI

Kiberjinoyatchilikning oldini olish muammolari xorijiy va mahalliy olimlarning tadqiqotlarida keng yoritilgan. Rossiya Federatsiyasi olimlari tomonidan AKT sohasidagi jinoyatlarning huquqiy jihatlari chuqur o'rganilgan. Ayniqsa, kiberjinoyatlarning turlari, ularni sodir etish usullari va oldini olish choralari bo'yicha keng qamrovli tadqiqotlar amalga oshirilgan.

Rossiya jinoyat qonunchiligida kompyuter axboroti sohasidagi jinoyatlar uchun javobgarlik 28-bobda belgilangan [4]. Ushbu bob ruxsatsiz kompyuter axborotiga kirish, shaxsiy ma'lumotlardan noqonuniy foydalanish, zararli kompyuter dasturlarini

yaratish va tarqatish, kompyuter axborotini saqlash qoidalarini buzish hamda muhim axborot infratuzilmasiga noqonuniy ta'sir ko'rsatish kabi jinoyatlarni o'z ichiga oladi.

Singapur tajribasi ayniqsa diqqatga sazovor. Ushbu davlatda banklar ma'lum jinoyatlar turlari bo'yicha zarar ko'rgan fuqarolarga zararni qoplashga majbur [5]. Bu choralar banklarni himoya tizimlarini takomillashtirishga rag'batlantiradi va fuqarolarning moliyaviy himoyasini ta'minlaydi.

Estoniyaning raqamli imzo tizimi ham yuqori samaradorlikni ko'rsatmoqda. Barcha moliyaviy operatsiyalar uchun raqamli imzo talab qilinishi kiberjinoyatchilikni keskin qisqartirdi [6].

O'zbekiston Respublikasida qonun hujjatlari va olim tadqiqotchilarning ishlari kiberxavfsizlik siyosatining huquqiy asoslarini yaratmoqda. 2022-yil

15-apreldagi O'RQ-764-sonli "Kiberxavfsizlik to'g'risida"gi Qonun [7] va

2023-yil 31-maydagi PQ-167-sonli Prezident Qarori [8] kiberxavfsizlik tizimini tashkil etishning asosiy yo'nalishlarini belgiladi.

O'ZBEKISTON RESPUBLIKASIDA KIBERJINOYATCHILIKNING OLDINI OLISH TIZIMI

O'zbekiston Respublikasi Konstitutsiyasi [9] fuqarolarning shaxsiy ma'lumotlarini himoya qilish huququni kafolatlaydi. Ushbu konstitutsiyaviy huquqdan kelib chiqib, qator maxsus qonunlar qabul qilingan.

"Kiberxavfsizlik to'g'risida"gi Qonun [7] davlat organlarining vakolatlari va mas'uliyatini aniq belgilaydi. Qonunga muvofiq, Davlat xavfsizlik xizmati Kiberxavfsizlik sohasida vakolatli davlat organi hisoblanadi. Ushbu organning asosiy vazifalari qatoriga milliy kiberfazoni himoya qilish, kiberhujumlarni oldini olish va ularni bartaraf etish kiradi.

Prezidentning 2023-yil 31-maydagi PQ-167-sonli Qarori [8] muhim axborot infratuzilmasi obyektlarining kiberxavfsizligini ta'minlash bo'yicha qo'shimcha choralarni belgiladi. Qaror asosida kritik axborot infratuzilmasi obyektlarining Yagona davlat reyestrini shakllantirish va ularning xavfsizligini ta'minlashning tartib-qoidalari ishlab chiqildi.

2025-yilda kiberjinoyatchilikka qarshi kurashishni kuchaytirish maqsadida Ichki ishlar vazirligida Kiberxavfsizlik bo'yicha Markazi tashkil etildi [3]. Ushbu tashkiliy struktura alohida Departamentga aylantirilishi belgilandi.

Bu esa kiberjinoyatlarga qarshi kurashish tizimini yanada mustahkamlashga xizmat qiladi.

Shuningdek, 2025-yil 20-yanvarda Prezident "Cyber University" davlat universitetini tashkil etish to'g'risida Qaror imzoladi [10]. Yangi universitet axborotni himoya qilish, axborot va kiberxavfsizlik, raqamli texnologiyalar va raqamli iqtisod, sun'iy intellekt asosida avtomatlashtirilgan axborot-tahliliy tizimlarni yaratish, robototexnika va shu kabi yo'nalishlarda kadrlar tayyorlashni amalga oshiradi. Bu choralar kadrlar tayyorlashda tizimli yondashuvni ta'minlaydi.

KIBERJINOYATLARNING ASOSIY TURLARI VA SODIR ETISH USULLARI

O'zbekiston Respublikasida sodir etiladigan kiberjinoyatlarning tahlili quyidagi asosiy turlarni aniqlash imkonini beradi. Statistik ma'lumotlarga ko'ra, kiberjinoyatlarning asosiy qismini (98%) bank kartalari bilan bog'liq jinoyatlar – kiber-o'g'irlik va kiber-firibgarlik tashkil etadi [2].

1. Zararli havolalar va dasturlar orqali kartalarni boshqarish huquqini olish (60%)

Bu usul kiberjinoyatlarning eng keng tarqalgan turi hisoblanadi. Jinoyatchilar SMS, ijtimoiy tarmoqlar yoki elektron pochta orqali zararli havolalarni yuborishadi. Fuqaro havolani bosganida, mobil qurilmasiga yoki kompyuteriga zararli dastur o'rnatiladi. Bu dastur bank ilovasi ustidan nazorat o'rnatib, kartadagi mablag'larni o'g'irlaydi.

Rossiya tajribasida ham xuddi shunday holat kuzatilmoqda. 2024-yilda plastik kartalar orqali 115 500 ta o'g'irlik va firibgarlik holati qayd etilgan [4]. Zararli dasturlar asosan mobil qurilmalar uchun APK formatida taratiladi.

2. SMS-kodlarni o'g'irlash (16%)

Jinoyatchilar turli firibgarlik sxemalari yordamida bank kartalarini va mobil ilovalardagi akkauntlarni boshqarishni tasdiqlovchi SMS-kodni olishadi. Ular ko'pincha bank yoki davlat organlari xodimlari sifatida o'zlarini tanıshtirib, fuqarolardan "xavfsizlik maqsadida" SMS-kodni aytishni so'raydilar.

Ushbu usulning xavfli tomoni shundaki, ko'pchilik fuqarolar telefon orqali bank xodimi bilan gaplashayotganiga ishonib, bemalol kodlarni aytib berishadi. Aslida esa, telefon qo'ng'irog'ini jinoyatchi qilgan.

3. Jismoniy shaxs nomidan onlayn-kredit rasmiylashtirish (4%)

Jinoyatchilar fuqarolarning shaxsiy ma'lumotlari va pasport fotosuratlarini o'g'irlash orqali ularning nomidan onlayn-kredit rasmiylashtiradi. Ayrim hollarda sun'iy intellekt yordamida shaxsning yuz qiyofasi va ovozi taqlid qilinadi. Bu usul ayniqsa xavfli, chunki jabrlanuvchi kreditor bo'lib qoladi va qarzni to'lash majburiyatiga ega bo'ladi.

Rossiyada ham xuddi shunday holat mavjud. 2024-yilda kompyuter uskunalari yordamida 42 300 ta jinoyat sodir etilgan [4]. Bularning aksariyati aynan onlayn-kredit firibgarliklaridir.

4. Onlayn-savdo platformalarida firibgarlik (11%)

Jinoyatchilar mavjud bo'lmagan tovarlalar e'lonini joylashtirib, oldindan to'lov talab qilishadi. To'lov amalga oshirilgandan so'ng, ular yo'qolib ketishadi. Ayrim hollarda esa, sotuvchi sifatida o'zlarini ko'rsatib, xaridor kartasining ma'lumotlarini o'g'irlaydilar.

5. Turli firibgarlik sxemalari orqali fuqarolarning mablag'larini jalb qilish (9%)

Bu turkumga piramida tuzilmalari, soxta investitsiya loyihalari, "kriptovalyuta treyderligi" kurslari va boshqa aldov usullari kiradi. Jinoyatchilar yuqori daromad va'da qilib, odamlardan pul yig'ishadi, keyin esa yo'qolib ketishadi.

KIBERJINOYATLARGA QARSHI KURASHISHDA XALQARO TAJRIBA

Rossiya Federatsiyasining tajribasi

Rossiya Federatsiyasida kiberjinoyatlar masalasiga keng qamrovli yondashuv qo'llanilmoqda. Jinoyat kodeksining 28-bobi kompyuter axboroti sohasidagi jinoyatlar uchun to'liq javobgarlik choralarini belgilaydi [4].

2024-yilda Rossiyada 765 400 ta kiberjinoyat qayd etilgan bo'lsa-da, bu ko'rsatkichlarning statistik tahlili oldini olish choralarini takomillashtirishga imkon beradi. Rossiya tajribasida e'tiborga loyiq jihatlar:

– Moliyaviy jinoyatlarga qarshi kurashish tarmog'i (Rosfinmonitoring) faoliyati: Bank operatsiyalarini real vaqt rejimida monitoring qilish;

– Banklar tomonidan shubhali operatsiyalarni avtomatik bloklash tizimi;

– Fuqarolarni kiberxavfsizlik bo'yicha o'qitish dasturlari.

Biroq, Rossiya statistikasi ham muammoning jiddiyligini ko'rsatadi. Kiberjinoyatlar soni yuqori bo'lishi oldini olish choralariga bo'lgan ehtiyojni tasdiqlaydi.

Singapurning banklar javobgarligi tizimi

Singapur kiberxavfsizlik sohasida eng ilg'or davlatlardan biri hisoblanadi. Ushbu mamlakatda qo'llaniladigan yondashuvlardan biri banklarning moliyaviy javobgarligidir.

Singapur banklari ma'lum jinoyat turlarida jabrlanuvchilarga zararni qoplashga majbur. Ayniqsa, onlayn-kredit firibgarliklari holatida, agar bank tizimi firibgarni aniqlashda muvaffaqiyatsiz bo'lsa, bank jabrlanuvchining yo'qotgan mablag'ini qaytaradi. Bu choralar banklarni o'z himoya tizimlarini doimiy takomillashtirishga majbur qiladi.

Muhim jihat shundaki, banklar faqat o'zlari oldini olishi mumkin bo'lgan jinoyatlar uchun javobgar. Agar fuqaro o'zi ixtiyoriy ravishda mablag' o'tkazgan bo'lsa (masalan, SMS-kodni aytgan), bank javobgar emas. Bu tizim muvozanatli yondashuvni ta'minlaydi.

Estoniyaning raqamli imzo tizimi

Estoniya raqamli davlat sifatida tanilgan va uning raqamli imzo tizimi kiberjinoyatchilikni kamaytirishda yuqori samaradorlik ko'rsatmoqda. Barcha moliyaviy operatsiyalar uchun elektron raqamli imzo (e-Signature) talab qilinadi.

Raqamli imzo shaxsiy ID-karta yoki mobil qurilmadagi maxsus sertifikat orqali amalga oshiriladi. Bu usul SMS-kodlardan ancha xavfsizroq, chunki jinoyatchi sertifikatni o'g'irlay olmaydi. Natijada, Estoniyada bank kartalari bilan bog'liq jinoyatlar darajasi eng past ko'rsatkichlardan biridir.

KIBERJINOYATLARNI OLDINI OLISHNING AMALIY CHORALARI

Yuqorida keltirilgan tahlil asosida, quyida O'zbekiston Respublikasi sharoitida amalga oshirish mumkin bo'lgan konkret va amaliy choralar taklif chiqqan holda ishlab chiqilgan.

1-chora: Biometrik ikki faktorli identifikatsiyani joriy etish

Muammo: Hozirgi vaqtda qo'llaniladigan SMS-kod asosidagi identifikatsiya tizimi etarli xavfsiz emas. Statistika shuni ko'rsatadiki,

60% jinoyatlar zararli dasturlar orqali SMS-kodlarni tutib olish bilan bog'liq.

Taklif etiladigan yechim: Barcha bank ilovalari uchun biometrik identifikatsiya (barmoq izi yoki yuz tanish) ni majburiy q ilish. Zamonaviy smartfonlarning deyarli barchasida biometrik skanerlar mavjud.

Amalga oshirish mexanizmi:

– Markaziy Bank tomonidan barcha tijorat banklariga uch oy ichida ilovalarni yangilash bo'yicha yo'riqnoma berish;

– Foydalanuvchi parolni kiritgach, avtomatik ravishda biometrik tasdiqlash talab qilinsin;

– SMS-kod faqat rezerv variant sifatida qolsin (masalan, telefon skaneri ishlamasa).

Kutilayotgan natija: SMS-kod o'g'irlashga asoslangan 16% va zararli dasturlar orqali amalga oshiriladigan 60% jinoyatlarning keskin qisqarishi. Jami 76% jinoyatlar oldini olinishi mumkin.

2-chora: Yangi qabul qiluvchilarga o'tkazmalar uchun dinamik kechiktirish tizimi

Muammo: Jinoyatchilar fuqarolarni bosim ostida ushlab, zudlik bilan mablag' o'tkazishga majbur qilishadi. Fuqaro qo’rquv holatida bo'lganda, hatto himoya tizimlarining ogohlantirishlariga ham e'tibor bermaydi.

Taklif etiladigan yechim: Yangi qabul qiluvchilarga birinchi marta o'tkazma amalga oshirilganda, summa hajmiga qarab avtomatik kechiktirish.

Amalga oshirish mexanizmi:

– 1 million so'mgacha: kechiktirish yo'q;

– 1-10 million so'm: 2 soatlik kechiktirish, ushbu vaqt ichida 3 marta ogohlantirish xabari yuboriladi;

– 10 million so'mdan ortiq: 24 soatlik kechiktirish, bank xodimining majburiy qo'ng'irog'i.

Kechiktirish davomida fuqaro istalgan vaqtda operatsiyani bekor qilish imkoniyatiga ega. Agar u jinoyatchining bosimi ostida bo'lsa, 24 soat ichida o'ziga kelishi va operatsiyani to'xtatishi mumkin.

Huquqiy asos: Markaziy Bank tomonidan "Bank operatsiyalarini amalga oshirish tartibi to'g'risida"gi yo'riqnomaga qo'shimchalar kiritish.

3-chora: Qoidalar-triggerlar asosida anomaliyalarni aniqlash

Muammo: Ko'p hollarda jinoyatchilar bir vaqtning o'zida bir nechta o'tkazmalarni amalga oshiradi yoki g'ayritabiiy vaqtda (tunda) operatsiya bajaradi. Odatiy bank tizimi buni aniqlashda qiynaladi.

Taklif etiladigan yechim: Sun'iy intellekt emas, balki oddiy IF-THEN qoidalari asosida shubhali operatsiyalarni aniqlash. Bu yechim arzon va tezkor amalga oshirilishi mumkin.

Qoidalar ro'yxati:

– Agar 1 soat ichida 5 va undan ortiq turli shaxslarga o'tkazma amalga oshirilsa → avtomatik bloklash + fuqaroga qo'ng'iroq;

– Agar operatsiya tunda 3:00-6:00 oralig'ida amalga oshirilsa → qo'shimcha biometrik tasdiqlash;

– Agar yangi qurilmadan kirilgan bo'lsa va darhol katta summa o'tkazma → 2 soatlik kechiktirish;

– Agar qabul qiluvchi "qora ro'yxat"da bo'lsa → to'liq bloklash.

Amalga oshirish: Har bir bank o'z dasturiy ta'minotiga oddiy mantiqiy qoidalarni 1-2 hafta ichida qo'shishi mumkin. Bu juda arzon va samarali yechim.

4-chora: Firibgar raqamlar va havolalarning yagona ma'lumotlar bazasi

Muammo: Har bir bank o'z "qora ro'yxat"iga ega, lekin ular o'rtasida ma'lumot almashish yo'q. Natijada, bir bankda bloklangan jinoyatchi boshqa bankda erkin faoliyat yuritadi.

Taklif etiladigan yechim: Markaziy Bank va Ichki ishlar vazirligi birgalikda yagona ma'lumotlar bazasini yaratish.

Mexanizm:

– Fuqarolar Telegram-bot orqali shubhali raqamlar va havolalarni yuborishlari mumkin;

– IIV mutaxassislari ma'lumotlarni tekshiradi va tasdiqlangan hollarda bazaga qo'shadi;

– Barcha banklar real vaqt rejimida ushbu bazaga kirish huquqiga ega;

– Agar fuqaro bazadagi raqamga o'tkazma qilmoqchi bo'lsa, avtomatik bloklash.

Qo'shimcha: Pattern-matching texnologiyasi. Faqat aniq raqamlar emas, balki pattern (naqsh) ham qo'shilsin. Masalan: "So'nggi 7 kun ichida ro'yxatdan o'tgan +998 90 XXX-XX-XX formatidagi barcha raqamlar, agar ularga ko'p sonli mayda o'tkazmalar tushsa" – bu pattern shubhali hisoblansin.

Huquqiy asos: Markaziy Bank, IIV va Raqamli texnologiyalar vazirligi o'rtasida Memorandum imzolash.

5-chora: Bank operatorlarini maxsus savollar bilan ta'minlash

Muammo: Hozirgi vaqtda bank operatorlari shubhali operatsiya ko'rganlarida oddiy "Ishonchingiz komilmi?" deb so'rashadi. Bu savolga fuqaro "Ha" deb javob бepishi oson.

Taklif etiladigan yechim: Operatorlarni psixologik savollar bilan ta'minlash. Bu savollar firibgarlik holatini aniqlashga yordam beradi.

Savollar ro'yxati (operator uchun skript):

– "Bu shaxsni shaxsan taniysizmi? Qachon va qayerda uchrashgansiz?"

– "Sizga bu shaxs daromad yoki yutuq va'da qildimi?"

– "Sizdan bu operatsiyani hech kimga aytmaslikni so'radimi?"

– "Telefon orqali sizdan SMS-kod so'raganmidi?"

Agar fuqaro bu savollardan biriga ijobiy javob bersa, ehtimoli yuqoriki, u firibgarlik qurbonidir.

Amalga oshirish: Barcha bank operatorlari uchun 1 haftalik trening. Har bir operator ekranida maxsus skript bo'lishi kerak.

6-chora: Yirik o'tkazmalar uchun bank tomonidan majburiy qo'ng'iroq

Muammo: Avtomatik tizimlar hamma holatni aniqlay olmaydi. Ba'zi hollarda inson aralashuvi zarur.

Taklif: 10 million so'mdan ortiq yangi qabul qiluvchiga o'tkazmalarda bank xodimining majburiy qo'ng'irog'i.

Qo'ng'iroq davomida operator 5-chorada keltirilgan savollarni beradi. Agar fuqaro javoblari shubha tug'dirsa, operatsiya 24 soatga to'xtatiladi va IIVga xabar beriladi.

7-chora: Bank ilovalarida ta'limiy pop-up xabarlar

Muammo: Fuqarolar kiberxavfsizlik qoidalarini yetarlicha bilishmaydi.

Taklif: Har safar fuqaro ilovani birinchi marta ochganida yoki o'tkazma qilmoqchi bo'lganida qisqa ta'limiy video yoki matn ko'rsatish.

Masalan: "Bu shaxs sizdan havolani bosishni so'radimi? DIQQAT! Bu firibgarlik bo'lishi mumkin!"

Bu chora kuchli emas, lekin bepul va oson amalga oshiriladi. Minimal xarajat bilan qo'shimcha himoya qatlami yaratadi.

XULOSA

Kiberjinoyatchilik zamonaviy jamiyat oldida turgan eng jiddiy muammolardan biridir. O'zbekiston Respublikasida kiberjinoyatlar sonining so'nggi besh yilda 68 barobarga oshishi, 2024-yilda umumiy jinoyatchilikdagi ulushining 44,4 foizga yetishi muammoning dolzarbligini ko'rsatadi.

Tadqiqot natijasida quyidagi asosiy xulosalarga kelindi:

Birinchidan, kiberjinoyatlarning 98 foizini bank kartalari bilan bog'liq jinoyatlar tashkil etadi. Asosan zararli havolalar (60%), SMS-kodlarni o'g'irlash (16%), onlayn-kredit firibgarliklari (4%) kabi usullar qo'llanilmoqda. Bu holat himoya choralarini aynan ushbu yo'nalishlarga qaratish zarurligini ko'rsatadi.

Ikkinchidan, Rossiya, Singapur, Estoniya kabi davlatlarning tajribasi samarali choralar mavjudligini tasdiqlaydi. Singapurning banklar javobgarligi tizimi, Estoniyaning raqamli imzosi kabi yondashuvlar O'zbekiston sharoitiga moslashtirilishi mumkin.

Uchinchidan, sun'iy intellekt va murakkab texnologiyalardan foydalanish shart emas. Oddiy, lekin samarali qoidalar-triggerlar, biometrik identifikatsiya, dinamik kechiktirish kabi choralar arzon va tezkor amalga oshirilishi mumkin.

To'rtinchidan, institutsional hamkorlik muhim ahamiyatga ega. Markaziy Bank, Ichki ishlar vazirligi, Raqamli texnologiyalar vazirligi va tijorat banklari o'rtasida samarali ma'lumot almashish tizimi yaratilishi zarur.

Beshinchidan, fuqarolarni ma'lumotlantirish tizimi samaradorlikni oshiradi. Bank operatorlarini maxsus savollar bilan ta'minlash, ta'limiy pop-up xabarlar kabi oddiy choralar ham ijobiy natija beradi.

Taklif etilgan yettita amaliy chora – biometrik identifikatsiya, dinamik kechiktirish, qoidalar-triggerlar, yagona ma'lumotlar bazasi, maxsus savollar, majburiy qo'ng'iroqlar va ta'limiy xabarlar – kompleks tizim sifatida qo'llanilganda kiberjinoyatlarni sezilarli darajada qisqartirishi mumkin.

Istiqbolda ushbu sohada qonunchilikni takomillantirish, xalqaro hamkorlikni kengaytirish va yangi texnologik echimlarni joriy etish bo'yicha tadqiqotlarni davom ettirish zarur. Prezident Shavkat Mirziyoyev tomonidan 2025-yil 8-iyul kuni ta'kidlanganidek, huquqni muhofaza qiluvchi organlar, banklar va raqamli texnologiyalar sohasidagi barcha ishtirokchilar birgalikda samarali himoya tizimini yaratishlari lozim.

FOYDALANILGAN ADABIYOTLAR RO'YXATI:

1. O'zbekiston Respublikasining Konstitutsiyasi. – T.: 2023 y. https://lex.uz/docs/6445145

2. Gazeta.uz. Kiberjinoyatlar kundan-kunga ko'payib, uning turlari 18 tadan 62 taga chiqdi [Elektron resurs]. – 2025. – URL: https://www.gazeta.uz/ru/2025/07/09/cyber-crimes/ (murojaat qilingan sana: 07.02.2026).

3. Prezident.uz. Davlatimiz rahbari kiberjinoyatchilikka qarshi kurashish bo'yicha topshiriqlar berdi [Elektron resurs]. – 2025. – URL: https://president.uz/ (murojaat qilingan sana: 07.02.2026).

4. Rossiya Federatsiyasi Ichki ishlar vazirligi. Axborot texnologiyalari sohasidagi jinoyatlar statistikasi [Elektron resurs]. – 2024. – URL: https://мвд.рф (murojaat qilingan sana: 07.02.2026).

5. Monetary Authority of Singapore. Consumer Protection Measures [Electronic resource]. – 2024. – URL: https://www.mas.gov.sg (murojaat qilingan sana: 07.02.2026).

6. E-Estonia. Digital Signature and Cybersecurity [Electronic resource]. – 2024. – URL: https://e-estonia.com (murojaat qilingan sana: 07.02.2026).

7. O'zbekiston Respublikasining "Kiberxavfsizlik to'g'risida"gi Qonuni. 2022-yil 15-aprel, ЗРУ-764-son. https://lex.uz/ru/docs/5960609 (murojaat qilingan sana: 07.02.2026).

8. O'zbekiston Respublikasi Prezidentining 2023-yil 31-maydagi PQ-167-sonli Qarori "Muhim axborot infratuzilmasi ob'ektlarining kiberxavfsizligini ta'minlash tizimini takomillashtirish bo'yicha qo'shimcha choralar to'g'risida". https://lex.uz/docs/6479197 (murojaat qilingan sana: 07.02.2026).

9. O'zbekiston Respublikasining Konstitutsiyasi. – T.: 2023 y. https://lex.uz/docs/6445145 (murojaat qilingan sana: 07.02.2026).

10. Gazeta.uz. "Cyber University" davlat universiteti tashkil etiladi [Elektron resurs]. – 2025. – URL: https://www.gazeta.uz/ru/2025/01/22/cyber-university/ (murojaat qilingan sana: 07.02.2026).