INNOVATIVE PUBLICATION
Journal of Effective Learning and Sustainable Innovation
Vol.4 №5 (2026). MAY
innovativepublication.uz

SOCIAL ENGINEERING ATTACKS AND PROTECTION AGAINST THEM: SITUATION, PROBLEMS AND SOLUTIONS IN UZBEKISTAN

Shukurov Orzikul Pardayevich
Senior Lecturer, Department of Information Security, Muhammad al-Khwarizmi Tashkent State Technical University
myheartumi@gmail.com, +998996636990

Abstract. This scientific article analyzes modern manifestations of social engineering attacks, their prevalence in the cyberspace of Uzbekistan, and the harmful consequences they cause to society and organizations. During the study, methods such as phishing, smishing, vishing, deceiving users through malicious links, and fraud related to bank cards were studied. The main causes of social engineering attacks, vulnerabilities associated with the human factor, and technical, organizational, and legal solutions to reduce them are proposed.
Keywords: *social engineering, phishing, smishing, vishing, cybersecurity, cyber literacy, bank cards, fraud, cybercrime, authentication.*

IJTIMOIY MUHANDISLIK HUJUMLARI VA ULARDAN HIMOYALANISH MASALALARI: O‘ZBEKISTONDAGI HOLAT, MUAMMOLAR VA YECHIMLAR

Shukurov Orziqul Pardayevich
Muhammad al-Xorazmiy nomidagi TATU, Axborot xavfsizligi kafedrasi katta o‘qituvchisi
myheartumi@gmail.com, +998996636990

Annotatsiya. Mazkur ilmiy maqolada ijtimoiy muhandislik hujumlarining zamonaviy ko‘rinishlari, ularning O‘zbekiston kibermakonidagi tarqalish darajasi hamda jamiyat va tashkilotlarga yetkazayotgan zararli oqibatlari tahlil qilingan. Tadqiqot davomida fishing, smishing, vishing, zararli havolalar orqali foydalanuvchilarni aldash, bank kartalari bilan bog‘liq firibgarliklar kabi usullar o‘rganilgan. Ijtimoiy muhandislik hujumlarining asosiy sabablari, inson omili bilan bog‘liq zaifliklar hamda ularni kamaytirish bo‘yicha texnik, tashkiliy va huquqiy yechimlar taklif etilgan.
Kalit so‘zlar: *ijtimoiy muhandislik, fishing, smishing, vishing, kiberxavfsizlik, kibersavodxonlik, bank kartalari, firibgarlik, kiberjinoyat, autentifikatsiya.*

Kirish. Raqamli texnologiyalar rivojlanishi natijasida davlat boshqaruvi, bank-moliya

tizimi, elektron tijorat va masofaviy xizmatlar keng joriy etildi. Shu bilan bir qatorda, kibermakonda sodir etilayotgan jinoyatlar soni ham ortib bormoqda. Ayniqsa, inson psixologiyasi va ishonuvchanligidan foydalanishga asoslangan ijtimoiy muhandislik hujumlari bugungi kunda eng xavfli tahdidlardan biri hisoblanadi[1].

Ijtimoiy muhandislik (Social Engineering) — foydalanuvchilarning ishonchini qozonish, ularni manipulyatsiya qilish yoki aldash orqali maxfiy ma'lumotlarni qo'lga kiritishga qaratilgan usullar majmuasidir[7]. Bunda texnik vositalardan ko'ra inson omili asosiy nishon sifatida tanlanadi. Kiberjinoyatchilar foydalanuvchilarni soxta havolalar, SMS-xabarlar, telefon qo'ng'iroqlari yoki messenjerlar orqali aldab, bank kartasi ma'lumotlari, SMS-kodlar, login va parollarni qo'lga kiritadi.

So'nggi yillarda O'zbekistonda ham bu turdagi jinoyatlar keskin oshgani kuzatilmoqda. Statistik ma'lumotlarga ko'ra, 2024-yilda kiberjinoyatlarning umumiy jinoyatchilikdagi ulushi 44,4 foizga yetgan bo'lib, deyarli har ikki jinoyatdan bittasi axborot texnologiyalari orqali sodir etilgan [1][2]. O'zbekistonda kiberjinoyatchilik ko'rsatkichlari 2025–2026-yillarda ham o'sishda davom etmoqda va davlat darajasidagi eng dolzarb xavfsizlik masalalaridan biriga aylandi.

2025-yil yakunlariga ko'ra, kiberjinoyatlarning umumiy jinoyatchilikdagi ulushi yanada ortib, **49,6 foizni** tashkil etdi. Bu deyarli har ikki jinoyatdan biri raqamli makonda sodir etilayotganini anglatadi.

Ijtimoiy muhandislik hujumlarining asosiy turlari:

Fishing — foydalanuvchini soxta sayt yoki xabar orqali aldab, uning shaxsiy ma'lumotlarini qo'lga kiritishga qaratilgan hujum turidir. Odatda foydalanuvchiga bank, davlat tashkiloti yoki mashhur servis nomidan xabar yuboriladi [7]. Ushbu xabarda "akkauntingiz bloklandi", "mukofot yutdingiz", "to'lovni tasdiqlang" kabi mazmundagi murojaatlar bo'ladi.

O'zbekiston Respublikasi IIV tizimida chop etilgan ilmiy materiallarda fishing va social engineering hujumlarini aniqlash hamda ularning oldini olish bo'yicha amaliy yondashuvlar zarurligi qayd etilgan [7].

Bugungi kunda fishing hujumlari Telegram, Instagram va boshqa messenjerlar orqali ham keng tarqalmoqda. Firibgarlar zararli havolalarni yuborib, foydalanuvchi akkauntlarini egallab olmoqda [5].

Smishing — SMS orqali amalga oshiriladigan fishing hujumi hisoblanadi. Bunda foydalanuvchiga bank yoki davlat organi nomidan soxta SMS yuborilib, havola orqali ma'lumot kiritish talab qilinadi [9].

Xalqaro tadqiqotlarga ko'ra, foydalanuvchilarning muhim qismi smishing hujumlariga javob qaytarishi aniqlangan. Ayrim tadqiqotlarda ishtirokchilarning 16,92 foizi

smishing xabarlariga ishonib, zararli havolalarga kirgani qayd etilgan [9].

Vishing — telefon qo‘ng‘iroqlari orqali amalga oshiriladigan ijtimoiy muhandislik hujumidir. Firibgarlar o‘zlarini bank xodimi, huquqni muhofaza qiluvchi organ vakili yoki texnik yordam operatori sifatida tanishtirib, foydalanuvchini maxfiy ma’lumotlarni aytishga majbur qiladi.

O‘zbekistonda bank kartalari bilan bog‘liq firibgarliklarda aynan SMS-kodlarni qo‘lga kiritish keng tarqalgan usullardan biri bo‘lib qolmoqda[2]. Statistik ma’lumotlarga ko‘ra, kiberjinoyatlarning 16 foizi aynan SMS-kodlarni qo‘lga kiritish orqali amalga oshirilgan.

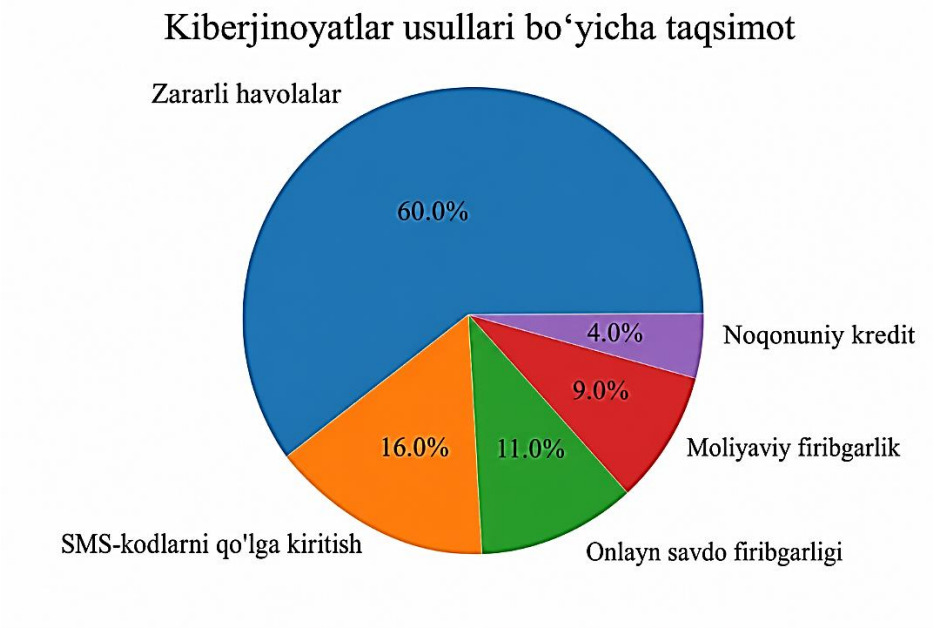
So‘nggi yillarda O‘zbekistonda kiberjinoyatlar soni keskin oshib bormoqda. Rasmiy ma’lumotlarga ko‘ra, 2021–2024-yillar davomida fuqarolardan 1 trillion 909 milliard so‘mdan ortiq mablag‘ kiberjinoyatlar orqali talon-toroj qilingan. Birgina 2024-yilning o‘zida zarar miqdori 603 milliard so‘mni tashkil etgan [3].

2025-yilning dastlabki 11 oyida fuqarolar kiberjinoyatchilar tomonidan **1,9 trillion so‘mga** yaqin (aniqrog‘i 1 trln 890 mlrd) zarar ko‘rgan.

2021–2025-yillar oralig‘ida kiberjinoyatlar soni **11 baravarga** (4 865 tadan 62 440 tagacha) ko‘paygan.

Tahlillar shuni ko‘rsatadiki, kiberjinoyatlarning **98 foizi** hali ham bank kartalari bilan bog‘liq firibgarlik va o‘g‘riliklardir. Shuningdek, kriptoaktivlar bilan bog‘liq jinoyatlar va sun’iy intellekt orqali amalga oshiriladigan **dipfeyk (deepfake)** hujumlari soni ortgan[11]. Ushbu jinoyatlar quyidagi rasmda aks etgan usullar orqali sodir etilgan(1-rasm).

Shuningdek, IIV huzuridagi Kiberjinoyatlarga qarshi kurashish markazi ma’lumotlariga ko‘ra, oxirgi besh yil ichida kiberjinoyatlar soni 68 baravarga oshgan [3].



1-rasm. Kiberjinoyatlar usullari bo‘yicha taqsimot

Bu ko‘rsatkichlar ijtimoiy muhandislik hujumlari O‘zbekistondagi kiberjinoyatlarning asosiy qismini tashkil etayotganini ko‘rsatadi.

Kiberxavfsizlik markazi tomonidan muntazam ravishda Telegram viruslari va zararli havolalar haqida ogohlantirishlar berib kelinmoqda. Markaz foydalanuvchilarga ikki bosqichli autentifikatsiyani yoqish, SMS kodlarni begonalarga bermaslik va noma’lum havolalarga kirmaslik kabi tavsiyalarni berib kelmoqda [4][5].

Bundan tashqari, darknet platformalarida O‘zbekiston fuqarolarining shaxsiy ma’lumotlari sizib chiqishi bilan bog‘liq holatlar ham qayd etilgan. Ayrim xabarlarda millionlab foydalanuvchilarga oid ma’lumotlar tarqalgan bo‘lishi mumkinligi e’tirof etilgan [3].

Ijtimoiy muhandislik hujumlarining asosiy sabablari.

Kibersavodxonlikning pastligi. Ko‘plab foydalanuvchilar zararli havolalar, fishing saytlar va firibgarlar usullarini ajrata olmaydi. Ayniqsa, katta yoshdagi fuqarolar va raqamli texnologiyalar bilan kam ishlovchi foydalanuvchilar hujumlarga tezroq uchraydi.

Inson omili. Texnik himoya vositalari mavjud bo‘lsa ham, insonning ehtiyotsizligi yoki hissiyotlarga berilishi katta xavf tug‘diradi. Firibgarlar qo‘rquv, shoshilinchlik yoki manfaatdorlik hissidan foydalanadi.

Zaif autentifikatsiya tizimlari. Ko‘plab foydalanuvchilar oddiy parollardan foydalanadi yoki bir xil parolni bir nechta platformalarda ishlatadi. Bu esa akkauntlarning oson buzilishiga olib keladi.

Ma’lumotlar sizib chiqishi. Shaxsiy ma’lumotlarning internetga sizib chiqishi

firibgarlar uchun qulay imkoniyat yaratadi. Ular foydalanuvchi haqida oldindan ma'lumot to'plab, ishonchli ko'rinishga harakat qiladi.

Ijtimoiy muhandislik hujumlari natijasida quyidagi salbiy oqibatlar yuzaga keladi:

- fuqarolarning moliyaviy mablag'lari talon-toroj qilinadi;
- bank va davlat tizimlariga bo'lgan ishonch pasayadi;
- tashkilotlarning maxfiy ma'lumotlari tarqaladi;
- shaxsiy ma'lumotlar noqonuniy bozorlarda sotiladi;
- davlat axborot tizimlariga tahdid kuchayadi.

Ayrim hollarda davlat tashkilotlari ham fishing hujumlariga duch kelmoqda. Mutaxassislarning ta'kidlashicha, tashkilot xodimlari xavfli havolalarni ochishi natijasida ichki ma'lumotlar sizib chiqishi mumkin.

Muammoning yechimlari va himoyalanish choralari.

Kibersavodxonlikni oshirish. Aholi orasida muntazam ravishda kibersavodxonlik targ'ibotini olib borish zarur. Ta'lim muassasalarida "Kiberxavfsizlik asoslari" fanlarini keng joriy etish muhim hisoblanadi[4].

Ikki bosqichli autentifikatsiya. Ikki bosqichli autentifikatsiya akkaunt xavfsizligini sezilarli oshiradi. Hatto parol qo'lga kiritilgan taqdirda ham, qo'shimcha tasdiqlash mexanizmi himoya vazifasini bajaradi[10].

Zararli havolalarni filtrlash. Bank va davlat tizimlarida fishing havolalarni avtomatik aniqlovchi texnologiyalarni keng joriy etish lozim[10].

Tashkiliy xavfsizlik siyosati. Tashkilotlarda xodimlarni muntazam o'qitish, xavfsizlik auditlarini o'tkazish va fishing simulyatsiyalaridan foydalanish tavsiya etiladi[7].

Huquqiy bazani takomillashtirish. O'zbekistonda kiberxavfsizlik sohasini rivojlantirish bo'yicha davlat siyosati kuchaytirilmoqda. 2026-yilda qabul qilingan PF-38-son Farmonda davlat organlari va xususiy sektor o'rtasida kibertahdidlarga qarshi hamkorlikni rivojlantirish vazifalari belgilangan[6].

Xulosa. Tadqiqot natijalari shuni ko'rsatdiki, ijtimoiy muhandislik hujumlari O'zbekistondagi eng dolzarb kiberxavfsizlik muammolaridan biriga aylangan[1]. Kiberjinoyatlarning katta qismi aynan inson omiliga asoslangan usullar orqali sodir etilmoqda. Ayniqsa, fishing, smishing va vishing hujumlari fuqarolar va tashkilotlarga katta moliyaviy zarar yetkazmoqda[2][3].

Mamlakatda kiberjinoyatlar sonining keskin oshishi, milliardlab mablag'larning talon-toroj qilinishi hamda shaxsiy ma'lumotlarning sizib chiqishi kibersavodxonlik va axborot xavfsizligi madaniyatini rivojlantirish zaruratini ko'rsatmoqda.

Mutaxassislar 2026-yilda O'zbekistonga qarshi qaratilgan kiberhujumlar va kibertahdidlar soni **200 milliondan** oshishi mumkinligini bashorat qilishmoqda.

Quyidagi strategik chora-tadbirlar O‘zbekistonda ijtimoiy muhandislik hujumlari xavfini sezilarli kamaytirishga xizmat qiladi:

1. Milliy kibersavodxonlik dasturini ishlab chiqish;
2. Davlat tashkilotlarida majburiy fishing treninglarini joriy etish;
3. AI asosidagi antifishing tizimlarini yaratish;
4. Zero Trust xavfsizlik modeliga o‘tish;
5. SMS autentifikatsiyadan bosqichma-bosqich voz kechish;
6. Kiberxavfsizlik bo‘yicha xalqaro hamkorlikni kengaytirish;
7. CERT va SOC markazlarini hududiy darajada rivojlantirish;
8. OTMlarda amaliy kiberxavfsizlik laboratoriyalarini yaratish;
9. Kiberjinoyatlar haqida tezkor ogohlantirish platformasini ishga tushirish;
10. Aholining barcha qatlamlari uchun ommaviy kibersavodxonlik kompaniyalarini yo‘lga qo‘yish.

Muammoni kamaytirish uchun aholining raqamli savodxonligini oshirish, kuchli autentifikatsiya mexanizmlarini joriy etish, davlat va xususiy sektor hamkorligini rivojlantirish hamda zamonaviy himoya texnologiyalaridan foydalanish muhim hisoblanadi. Shuningdek, foydalanuvchilarni muntazam ravishda ogohlantirib borish va real misollar asosida o‘qitish ijtimoiy muhandislik hujumlariga qarshi samarali vositalardan biri bo‘lib xizmat qiladi [4][6][10].

Foydalanilgan adabiyotlar

1. Gazeta.uz – Kiberjinoyatlar statistikasi
2. Spot.uz – O‘zbekistonda kiberjinoyatlar tahlili
3. Pinkod.uz – 2021–2024 yillardagi kiberjinoyatlar statistikasi
4. Kiberxavfsizlik markazi rasmiy sayti
5. Yuz.uz – Telegram viruslari haqida ogohlantirish
6. Lex.uz – PF-38-son Farmon
7. IIV ilmiy konferensiya materiallari PDF
8. Yoshlar muammolarini o‘rganish markazi – Internetdagi firibgarlik
9. Arxiv.org – Users really do respond to smishing
10. Arxiv.org – Commercial Anti-Smishing Tools
11. https://www.gazeta.uz/oz/2025/12/24/cybercrime/

Ishtirok etish uchun anketa shakli

№	Anketa shakli	
1.	Muallifning F.I.O. (to‘liq)	Shukurov Orziqul Pardayevich

2.	Tashkilot (ish joyi)	Muhammad al-Xorazmiy nomidagi TATU
3.	Material (maqola) nomi	IJTIMOIY MUHANDISLIK HUJUMLARI VA ULARDAN HIMOYALANISH MASALALARI: O‘ZBEKISTONDAGI HOLAT, MUAMMOLAR VA YECHIMLAR
4.	Sho‘ba nomi (yo‘nalishi)	
5.	Aloqa uchun telefon raqam	myheartumi@gmail.com
6.	E-mail	+998 99 663 69 90