

IJTIMOIIY MUHANDISLIK (SOCIAL ENGINEERING) HUJUMLARI VA INSON OMILI: TAHDIDLAR, PSIXOLOGIK MEXANIZMLAR VA HIMOYA STRATEGIYALARI

Mo'minov Haydar Muhiddinovich
"Realsoft Academy" MChJ direktori
E-mail: univorarsa@gmail.com
Ruzibayev Eldorjon Xoshimjon o'g'li
Toshkent Amaliy Fanlar Universiteti,
Axborot texnologiyalar fakulteti, KAX 23-01 guruh
E-mail: ruzibayeveldor@gmail.com
Maxambetov Rovshanbek Qanatboy o'g'li
Toshkent Amaliy Fanlar Universiteti,
Axborot texnologiyalar fakulteti, KAX 23-01 guruh
E-mail: oldrowka@gmail.com
Atamurodov Abbosbek Hayrullo o'g'li
Toshkent Amaliy Fanlar Universiteti,
Axborot texnologiyalar fakulteti, KAX 23-01 guruh
E-mail: a70405959@gmail.com

ANNOTATSIYA

Maqsad: Ushbu maqolada ijtimoiy muhandislik hujumlarining mohiyati, asosiy turlari, psixologik mexanizmlari va inson omilining kiberxavfsizlikdagi roli tahlil qilinadi. **Metodologiya:** Ilmiy adabiyotlarning tizimli sharhi, mavjud kiberxavfsizlik standartlari va hisobotlar tahlili asosida deskriptiv-analitik yondashuv qo'llanilgan. **Natijalar:** Phishing, vishing, smishing, baiting, pretexting va quid pro quo turidagi hujumlar tizimli tavsiflanib, ularning inson psixologiyasiga ta'sir mexanizmlari — qo'rquv, shoshilinchlik, qiziqish va avtoritetga ishonch — aniqlangan. **Xulosa:** Ijtimoiy muhandislik hujumlaridan samarali himoyalaniish texnik vositalar bilan foydalanuvchilar xabardorligini oshirish va xavfsizlik madaniyatini shakllantirish kompleks birligiga asoslanishi kerak.

Kalit so'zlar: *ijtimoiy muhandislik, kiberxavfsizlik, phishing, inson omili, axborot xavfsizligi, psixologik tahdidlar, ikki faktorli autentifikatsiya, xavfsizlik madaniyati, vishing, pretexting.*

ABSTRACT

Purpose: This article analyzes the nature of social engineering attacks, their main types, psychological mechanisms, and the role of the human factor in cybersecurity. **Methodology:** A descriptive-analytical approach was employed based on a systematic review of academic literature, existing cybersecurity standards, and incident reports. **Results:** Attacks including phishing, vishing, smishing, baiting, pretexting, and quid pro quo are systematically described, with key psychological influence mechanisms — fear, urgency, curiosity, and authority bias — identified and analyzed.

Conclusion: Effective defense against social engineering requires an integrated approach combining technical safeguards with enhanced user awareness and a robust security culture.

Keywords: *social engineering, cybersecurity, phishing, human factor, information security, psychological threats, two-factor authentication, security culture, vishing, pretexting.*

1. KIRISH

Hozirgi globallashuv va raqamli transformatsiya davrida axborot-kommunikatsiya texnologiyalari jamiyatning barcha sohalariga chuqur kirib bormoqda. Shu bilan birga, kiberxavfsizlik tahdidlari ham tobora murakkablashib, yangi shakllarga ega bo'lmoqda. Ana shunday tahdidlardan biri — ijtimoiy muhandislik (social engineering) hujumlari bo'lib, bu yo'nalish zamonaviy axborot xavfsizligining eng dolzarb muammolaridan biri sifatida tan olingan (Hadnagy, 2018; Mitnick & Simon, 2002).

Ijtimoiy muhandislik hujumlarining o'ziga xos jihati shundaki, ular texnik zaifliklardan ko'ra ko'proq inson psixologiyasi va xatti-harakatlariga ta'sir ko'rsatish orqali amalga oshiriladi. Hattoki yuqori darajada himoyalangan tizimlarda ham oddiy foydalanuvchi xatosi sababli maxfiy ma'lumotlar oshkor bo'lishi mumkin (Schneier, 2000). Cisco (2023) yillik hisobotiga ko'ra, kiberhujumlarning 74%dan ortig'ida inson omili hal qiluvchi rol o'ynagan.

Ushbu maqolaning maqsadi — ijtimoiy muhandislik hujumlarining mohiyatini yoritish, inson omilining psixologik mexanizmlarini tahlil qilish va ushbu tahdidlarga qarshi samarali himoya strategiyalarini ishlab chiqishdan iborat. Tadqiqot O'zbekiston raqamli iqtisodiyotga o'tish sharoitida axborot xavfsizligi madaniyatini shakllantirish zaruratidan kelib chiqadi.

2. ADABIYOTLAR SHARHI VA NAZARIY ASOS

Ijtimoiy muhandislik sohasidagi dastlabki fundamental asarlardan biri Mitnick va Simon (2002) tomonidan yozilgan bo'lib, ular inson ishonchini suiiste'mol qilish mexanizmlarini amaliy misollar yordamida tahlil qilgan. Hadnagy (2018) esa ijtimoiy muhandislikni "inson xakerligining fani" sifatida ta'riflab, uning psixologik asoslarini kognitiv psixologiya nuqtai nazaridan ko'rib chiqgan.

Stallings (2022) tarmoq xavfsizligi asarida ijtimoiy muhandislikni texnik hujumlarning boshlang'ich bosqichi sifatida baholagan. NIST (2023) kiberxavfsizlik doirasi (Cybersecurity Framework) esa ijtimoiy muhandislikka qarshi choralar sifatida xodimlarni o'qitish, ikki faktorli autentifikatsiya va xavfsizlik siyosatini belgilaydi.

ENISA (2023) hisobotiga ko'ra, Yevropa Ittifoqi mamlakatlarida qayd etilgan kiberintsidentlarning 57% phishing va boshqa ijtimoiy muhandislik usullaridan boshlangan. ISO/IEC 27001:2022 standarti axborot xavfsizligini boshqarish tizimlarida inson omilini boshqarishni majburiy element sifatida ko'zda tutadi. Mahalliy kontekstda O'zbekiston "Axborot xavfsizligi" bo'yicha milliy standartlari (O'zDST) ushbu yo'nalishda qonuniy-normativ baza yaratishda muhim ahamiyat kasb etadi.

3. TADQIQOT METODOLOGIYASI

Tadqiqot deskriptiv-analitik dizaynga asoslangan va quyidagi metodlardan foydalanilgan: (1) ilmiy adabiyotlarni tizimli ko'rib chiqish (2018–2024 yillar oralig'i); (2) xalqaro kiberxavfsizlik standartlari va yillik hisobotlarini tahlil qilish (NIST, ISO/IEC 27001, ENISA, Cisco, Kaspersky); (3) ijtimoiy muhandislik hujumlari turlarini qiyosiy tahlil qilish; (4) psixologik ta'sir mexanizmlarini kognitiv psixologiya nazariyalari bilan bog'lash.

Manbalar tanlanishida quyidagi mezonlarga rioya qilindi: nashr yili (asosan so'nggi 5 yil), indeksatsiyalangan jurnallarda e'lon qilinganlik, amaliy misollar bilan tasdiqlangan empirik ma'lumotlar mavjudligi. Adabiyotlar APA 7 formati asosida ro'yxatga olindi.

Eslatma: Ushbu maqola nazariy-tahliliy xarakterga ega bo'lib, birlamchi empirik ma'lumotlar to'planmagan. Kelajakdagi tadqiqotlarda O'zbekiston tashkilotlari xodimlari orasida so'rovnoma va eksperimental sinov o'tkazish rejalashtirilib, natijalar keng ko'lami randomizatsiyalashtirilgan tadqiqot asosida taqdim etiladi.

4. NATIJALAR VA MUHOKAMA

4.1. Ijtimoiy muhandislik hujumlarining asosiy turlari

Ijtimoiy muhandislik hujumlarining turlarini tizimlashtirish maqsadida mavjud adabiyotlar tahlili asosida quyidagi tasnif ishlab chiqildi (1-jadval).

Hujum turi	Kanal	Psixologik mexanizm	Misollar
Phishing	Elektron pochta, veb-sahifa	Qo'rquv, shoshilinchlik	Soxta bank xabarlar
Vishing	Telefon qo'ng'irog'i	Avtoritetga ishonch	Soxta texnik yordam
Smishing	SMS xabar	Qiziqish, urgency	"Sovrin yutdingiz" xabari
Baiting	Jismoniy/raqamli media	Qiziqish, ochko'zlik	Zararli USB disk
Pretexting	Har qanday kanal	Ishonch, obro'	Soxta auditorlik so'rovi
Quid pro quo	Telefon, email	Yordamga minnatdorlik	Texnik yordam bahonasi

1-jadval. Ijtimoiy muhandislik hujumlarining tasnifi (Hadnagy, 2018; ENISA, 2023 asosida tuzilgan)

4.2. Inson psixologiyasiga ta'sir mexanizmlari

Kognitiv psixologiya nuqtai nazaridan ijtimoiy muhandislik hujumlari inson qaror qabul qilish jarayonidagi bir qator sistematik xatoliklardan (cognitive biases) foydalanadi. Cialdini (1984/2021)ning ta'sir tamoyillari asosida quyidagi mexanizmlar aniqlandi: (1) avtoritetga bo'ysunish — rasmiy ko'rinishga ega xabarlar shubhasiz qabul qilinadi; (2) shoshilinchlik effekti — "zudlik bilan bajaring" xabarlar analitik fikrlashni to'xtatadi; (3) o'zaro manfaat — yordam so'rov konteksti ma'lumot berishga undaydi; (4) ijtimoiy tekshiruv — "boshqalar ham shunday qildi" degan xabar ishonch uyg'otadi.

Cisco (2023) hisobotiga ko'ra, hujumchilar inson omilidan foydalanish orqali kiberhujumlarning 74%ini amalga oshirmoqda. Kaspersky (2023) ma'lumotlariga ko'ra, phishing hujumlarining o'rtacha muvaffaqiyat darajasi 30–40% ni tashkil etib, moliyaviy yo'qotishlar yiliga millionlab dollarga yetmoqda.

4.3. Tashkiliy va moliyaviy oqibatlar

IBM Security (2023) yillik hisobotiga ko'ra, ijtimoiy muhandislik natijasida yuzaga kelgan ma'lumotlar buzilishining o'rtacha narxi \$4.45 millionni tashkil etgan. Tashkilotlar uchun xavflar faqat moliyaviy yo'qotishlar bilan cheklanmaydi: obro'ning pasayishi, mijozlar ishonchini yo'qotish va huquqiy javobgarlik ham muhim oqibatlar hisoblanadi. Kichik va o'rta biznes uchun bunday hujumlar faoliyatning to'xtab qolishiga olib kelishi mumkin.

5. HIMOYA CHORALARI VA XAVFSIZLIK STRATEGIYALARI

Ijtimoiy muhandislik hujumlaridan samarali himoya uchun kompleks yondashuv talab etiladi. NIST Cybersecurity Framework (2023) va ISO/IEC 27001:2022 standartlari asosida quyidagi strategiyalar tavsiya etiladi.

Birinchidan, foydalanuvchilarni muntazam ravishda o'qitish va treninglar o'tkazish eng muhim chora hisoblanadi (Hadnagy, 2018). Simulyatsiyalashgan phishing testlari xodimlarning

hushyorlik darajasini oshirishda katta ahamiyatga ega. Tadqiqotlar shuni ko'rsatadiki, muntazam o'qitish hujumlarga muvaffaqiyatli "aldanish" darajasini 60–70%ga kamaytirishi mumkin (Proofpoint, 2023).

Ikkinchidan, ikki faktorli autentifikatsiya (2FA) tizimini joriy etish parol o'g'irlangan taqdirda ham tizimga kirishni sezilarli darajada qiyinlashtiradi. Uchinchidan, tashkilotlarda rasmiy axborot xavfsizligi siyosati ishlab chiqilishi va unga qat'iy rioya qilinishi kerak. To'rtinchidan, shubhali xabarlarni aniqlash bo'yicha ko'rsatmalar va xabar berish mexanizmlari belgilanishi lozim. Beshinchidan, AI asosidagi phishing-filtr va anomaliya aniqlash tizimlari texnik himoyani kuchaytiradi.

6. CHEKLOVLAR

Ushbu tadqiqot bir qator cheklovlarga ega. Birinchidan, maqola asosan nazariy-tahliliy xarakterga ega bo'lib, O'zbekiston kontekstida to'plangan birlamchi empirik ma'lumotlarga ega emas; natijalarni mahalliy sharoitga to'liq ko'chirish ehtiyotkorlikni talab qiladi. Ikkinchidan, foydalanilgan xalqaro hisobotlar (Cisco, Kaspersky, IBM) asosan G'arb va yirik kompaniyalar kontekstini aks ettiradi; O'rta Osiyo mintaqasiga xos tendentsiyalar alohida tadqiq etilishi lozim. Uchinchidan, ijtimoiy muhandislik texnologiyalari jadal rivojlanayotgani sababli, ayrim tavsiyalar vaqt o'tishi bilan dolzarbligini yo'qotishi mumkin. To'rtinchidan, kognitiv psixologiya nazariyalarini kiberxavfsizlikka tatbiq etishda madaniy farqlar hisobga olinmagan.

7. XULOSA VA TAKLIFLAR

Ijtimoiy muhandislik hujumlari zamonaviy kiberxavfsizlikda eng xavfli tahdidlardan biri bo'lib, ularning muvaffaqiyati texnik imkoniyatlarga emas, balki inson psixologiyasiga — qo'rquv, shoshilinchlik, qiziqish va avtoritetga ishonchga — asoslanadi. Phishing, vishing, smishing, baiting, pretexting va quid pro quo usullari har biri ma'lum psixologik zaifliklardan foydalanib, tashkilot va shaxslarni katta moliyaviy va obro'li zararga uchratamoqda.

Tadqiqot natijalari asosida quyidagi takliflar ishlab chiqildi: (1) tashkilotlarda muntazam axborot xavfsizligi treninglari va simulyatsiya testlarini joriy etish; (2) barcha axborot tizimlarida ikki faktorli autentifikatsiyani majburiy qilish; (3) maktab va oliy ta'lim dasturlariga raqamli savodxonlik va kiberxavfsizlik asoslarini kiritish; (4) O'zbekiston sharoitida ijtimoiy muhandislik insidentlarini ro'yxatga olish va tahlil qilish tizimini yaratish; (5) kelajakdagi tadqiqotlarda O'zbekiston tashkilotlari xodimlari orasida empirik tadqiqot o'tkazish.

ADABIYOTLAR RO'YXATI (APA 7)

1. Cialdini, R. B. (2021). *Influence: The psychology of persuasion* (New and expanded ed.). Harper Business.
2. Cisco Systems. (2023). *Cisco annual cybersecurity report 2023*. <https://www.cisco.com/c/en/us/products/security/security-reports.html>
3. ENISA — European Union Agency for Cybersecurity. (2023). *ENISA threat landscape 2023*. <https://doi.org/10.2824/782573>
4. Hadnagy, C. (2018). *Social engineering: The science of human hacking* (2nd ed.). Wiley. <https://doi.org/10.1002/9781119433729>
5. IBM Security. (2023). *Cost of a data breach report 2023*. <https://www.ibm.com/reports/data-breach>

6. ISO/IEC 27001:2022. (2022). *Information security, cybersecurity and privacy protection — Information security management systems — Requirements*. International Organization for Standardization.
7. Kaspersky Lab. (2023). *Kaspersky security bulletin 2023*. <https://securelist.com/ksb-2023-statistics/111224/>
8. Mitnick, K. D., & Simon, W. L. (2002). *The art of deception: Controlling the human element of security*. Wiley Publishing.
9. NIST — National Institute of Standards and Technology. (2023). *Cybersecurity framework 2.0*. <https://doi.org/10.6028/NIST.CSWP.29>
10. Proofpoint. (2023). *State of the phish 2023: Annual threat report*. <https://www.proofpoint.com/us/resources/threat-reports/state-of-phish>
11. Schneier, B. (2000). *Secrets and lies: Digital security in a networked world*. Wiley.
12. Stallings, W. (2022). *Network security essentials: Applications and standards* (7th ed.). Pearson Education.