IJTIMOIY MUHANDISLIK ASOSIDAGI KIBERTAHDIDLAR: ULARNI ANIQLASH, OLDINI OLISH VA RAQAMLI DALILLAR YORDAMIDA TAHLIL QILISH

Karimboyev Jo‘shqinbek Ergashbek o‘g‘li
O‘zbekiston Respublikasi IIV Akademiyasi kursanti
Iminov Abdurasul Abdulatipovich
O‘zbekiston Respublikasi IIV Akademiyasi Raqamli texnologiyalar va axborot xavfsizligi kafedrasi boshlig‘i, matematika va fizika fanlari nomzodi, dotsent

Annotatsiya: *Ushbu maqolada ijtimoiy muhandislik asosidagi kibertahdidlar, ularning zamonaviy axborot tizimlaridagi o‘rni va ishlash mexanizmlari tahlil qilinadi. Inson omiliga asoslangan hujumlar, xususan phishing va boshqa aldash usullari orqali foydalanuvchilarga ta’sir ko‘rsatish jarayonlari yoritiladi. Shuningdek, bunday kibertahdidlarni aniqlash va oldini olishda qo‘llaniladigan asosiy yondashuvlar ko‘rib chiqiladi. Maqolada raqamli dalillar, jumladan log fayllar, tarmoq izlari va autentifikatsiya ma’lumotlarining hujumlarni tahlil qilishdagi ahamiyati ham alohida o‘rin tutadi. Tadqiqotning maqsadi ijtimoiy muhandislik hujumlarini kompleks tarzda tushunish hamda ularga qarshi samarali himoya choralarini asoslashdan iborat.*

Kalit so’zlar: *Ijtimoiy muhandislik, kibertahdidlar, kiberxavfsizlik, fishing, raqamnli kriminalistika, log fayllar, autentifikatsiya, foydalanuvchi xavfsizligi, kiberhujumlar.*

Annotation: *This article analyzes cyber threats based on social engineering, their role in modern information systems, and their operational mechanisms. It examines human-factor-based attacks, particularly phishing and other deception techniques used to manipulate users. The study also considers the main approaches used to detect and prevent such cyber threats. In addition, the article highlights the importance of digital evidence, including log files, network traces, and authentication data, in analyzing cyberattacks. The aim of the research is to comprehensively understand social engineering attacks and justify effective protection measures against them.*

Keywords: *Social engineering, cyber threats, cybersecurity, phishing, digital evidence, digital forensics, log files, authentication, user security, cyberattacks.*

Аннотация: *В данной статье анализируются киберугрозы, основанные на социальной инженерии, их роль в современных информационных системах и механизмы их функционирования. Рассматриваются атаки, основанные на человеческом факторе, в частности фишинг и другие методы обмана, используемые для воздействия на пользователей. Также изучаются основные подходы к выявлению и предотвращению подобных киберугроз. Отдельное внимание уделяется роли цифровых доказательств, включая лог-файлы, сетевые следы и данные аутентификации, в анализе кибератак. Цель исследования заключается в комплексном понимании атак социальной инженерии и обосновании эффективных мер защиты.*

Ключевые слова: *Социальная инженерия, киберугрозы, кибербезопасность, фишинг, цифровые доказательства, цифровая криминалистика, лог-файлы, аутентификация, безопасность пользователей, кибератаки.*

Zamonaviy axborot jamiyati sharoitida internet tarmoqlari inson hayotining barcha sohalariga chuqur kirib borgan bo‘lib, bu holat bilan bir qatorda kiberxavfsizlik muammolari ham keskin dolzarblik kasb etmoqda. Bugungi kunda kibertahdidlar nafaqat texnik zaifliklar, balki inson omilidan foydalanishga asoslangan murakkab hujumlar orqali ham amalga oshirilmoqda. Ayniqsa, ijtimoiy muhandislik usullariga asoslangan hujumlar foydalanuvchilarning psixologik xususiyatlari, ishonuvchanligi va ehtiyotsizligidan foydalanib, maxfiy ma’lumotlarni qo‘lga kiritishga qaratilganligi bilan ajralib turadi.Ijtimoiy muhandislik asosidagi kibertahdidlar zamonaviy kiberjinoyatchilikning eng keng tarqalgan yo‘nalishlaridan biri bo‘lib, ular orqali tajovuzkorlar phishing xabarlari, soxta veb-saytlar, aldovli elektron pochta va boshqa usullar yordamida foydalanuvchilarni manipulyatsiya qiladi. Bunday hujumlar natijasida shaxsiy ma’lumotlar, moliyaviy axborotlar hamda tizimlarga kirish huquqlari qo‘lga kiritilishi mumkin. Ijtimoiy muhandislik o’zi nima?

Ijtimoiy muhandislik — bu odamlarga nisbatan biror xatti-harakatni amalga oshirish yoki maxfiy ma’lumotlarni oshkor qilish ma’nosidagi psixologik manipulyatsiya. [34] Ijtimoiy muhandislik faqat nazariya emas, balki u millionlab dollar zarar keltirgan. Quyida bunga misol sifatida bir necha mashhur holatlar keltirilgan:

Shark Tank, 2020: "Shark Tank" shousining ishtirokchisi Barbara Korkoran qariyb 400 000 AQSh dollari miqdoridagi fishing va ijtimoiy muhandislik firibgarligiga uchragan. Kiberjinoyatchi uning yordamchisiga o'xshagan e-pochta orqali hisobchiga ko'chmas mulk sarmoyalari bo'yicha to'lovni yangilash haqida xabar yuborgan. Firibgar legitim e-pochta manziliga o'xshash manzildan foydalangan. Firibgarlik faqat buxgalter yordamchisining to'g'ri manziliga tasdiqlash uchun yozganida aniqlangan. Zarar: 400 000 dollar. Bu holat oddiy e-pochta tekshiruvi qanchalik muhimligini ko'rsatadi.

Toyota, 2019: Avtomobil qismlari yetkazib beruvchisi Toyota Boshoku Corporation ijtimoiy muhandislik va BEC (Biznes elektron pochtasi buzilishi) hujumining qurboniga aylangan. Hujumchilar moliya rahbarini ishontirib, pul o'tkazmasida bank hisobini o'zgartirishga majbur qilgan. Zarar: 37 million dollar. Kompaniyalar ichki aloqalarni qanchalik ehtiyotkorlik bilan tekshirishi kerakligini eslatadi.

SMS va messenjerlar orqali phishing hamda “rasmiy tashkilot” nomidan aldash holatlari.

O‘zbekistonda keng tarqalgan ijtimoiy muhandislik hujumlaridan biri banklar bilan bir qatorda turli rasmiy tashkilotlar, jumladan ichki ishlar organlari nomidan yuboriladigan soxta SMS va xabarlar hisoblanadi. Bunday holatlarda tajovuzkorlar foydalanuvchiga “sizga nisbatan ma’muriy ish ochildi”, “jarimani to‘lash kerak” yoki “hisobingiz bloklanadi” kabi tahdidli va shoshilinch mazmundagi xabar yuboradi. Ba’zi holatlarda esa ular o‘zlarini ichki ishlar xodimi sifatida tanishtirib, “tekshiruv uchun karta ma’lumotlari yoki SMS kodni taqdim eting” kabi talablarni qo‘yadi. Ushbu usul foydalanuvchining qo‘rquv va rasmiy organlarga ishonish

[34] Wikipediya - https://uz.wikipedia.org/wiki/Ijtimoiy_muhandislik_(xavfsizlik)

psixologiyasidan foydalanishga asoslanadi va ko‘pincha soxta havolalar orqali ma’lumotlarni qo‘lga kiritish bilan yakunlanadi.

Telefon qo‘ng‘iroqlari va hujjatli aldovlar orqali ijtimoiy muhandislik. Yana bir keng tarqalgan ijtimoiy muhandislik usulida firibgarlar telefon qo‘ng‘iroqlari yoki messenjerlar orqali o‘zlarini bank xodimi, ichki ishlar organlari (IIO) xodimi yoki boshqa rasmiy tashkilot vakili sifatida tanishtiradi. Ular “sizning nomingizga jinoyat ishi ochilgan”, “shubhali tranzaksiya qayd etildi” yoki “xavfsizlik tekshiruvi uchun ma’lumotlarni tasdiqlang” kabi psixologik bosimga asoslangan ssenariylardan foydalanadi.

Bundan tashqari, hujumni ishonchli ko‘rsatish uchun tajovuzkorlar turli hujjatlarni ham yuboradi. Jumladan, soxta sud qarorlari, chaqiruv xatlari, ma’muriy qarorlar, MIB tomonidan yuborilgandek ko‘rsatilgan undirish hujjatlari yoki “rahbar nomidan” yozilgan soxta akkauntlar orqali xabarlar tarqatiladi.

Ushbu fayllar ko‘pincha zararli dastur (virus) bilan biriktirilgan bo‘lib, ularni ochish orqali qurilma yoki ma’lumotlarga ruxsatsiz kirish imkoniyati yaratiladi. Shuningdek, ayrim holatlarda tajovuzkorlar audio fayllar ko‘rinishida ham zararli kontent yuborishi mumkin.

Bunday fayllar “muhim eslatma”, “rasmiy ogohlantirish” yoki “tezkor ko‘rsatma” sifatida taqdim etilib, foydalanuvchini ochishga undaydi. Aslida esa bu ham zararli dastur yoki ma’lumot o‘g‘irlashga qaratilgan vosita bo‘lishi ehtimoli yuqori. Ushbu usullar foydalanuvchining rasmiy hujjatlarga bo‘lgan ishonchi va shoshilinch qaror qabul qilish psixologiyasidan foydalanadi.

Ijtimoiy muhandislik asosidagi kibertahdidlarni aniqlash jarayoni asosan foydalanuvchi xatti-harakatlari, texnik indikatorlar va aloqa kanallaridagi shubhali belgilarni tahlil qilishga asoslanadi. Bunday hujumlar ko‘pincha tashqi tomondan oddiy ko‘rinsa-da, ularning ichki tuzilmasida bir qator aniqlanadigan xavf signallari mavjud. Birinchi navbatda, elektron pochta va messenjer xabarlarida yuboruvchi manzilini tekshirish muhim hisoblanadi. Firibgarlar ko‘pincha rasmiy tashkilotlarga juda o‘xshash, lekin kichik farqlarga ega domenlardan foydalanadi. Masalan, harf almashtirish, qo‘shimcha belgilar yoki notanish domen zonalari shubhali holat hisoblanadi.

Masalan: Uzum Market (original) - Uzurn Market(soxta)

Ikkinchi muhim belgi — xabar mazmunidagi psixologik bosim elementlari. “Darhol harakat qiling”, “hisobingiz bloklanadi” yoki “tezda tasdiqlang” kabi jumlalar foydalanuvchini shoshilinch qaror qabul qilishga undaydi. Bu esa ijtimoiy muhandislik hujumlarining asosiy indikatorlaridan biri hisoblanadi. Uchinchi yo‘nalish texnik tahlil bilan bog‘liq bo‘lib, URL manzillarni tekshirish, domenning haqiqiyligini aniqlash hamda SSL sertifikatlar mavjudligini tahlil qilishni o‘z ichiga oladi. Shuningdek, shubhali fayllar (PDF, DOC, audio yoki arxivlar) ichida yashiringan zararli kodlar antivirus va sandbox muhitlari orqali aniqlanadi. Ijtimoiy muhandislik asosidagi kibertahdidlarning oldini olish kompleks yondashuvni talab qiladi, chunki bu turdagi hujumlar texnik tizimlardan ko‘ra ko‘proq inson omiliga qaratilgan bo‘ladi. Shu sababli himoya choralari ham texnik, tashkiliy va foydalanuvchi darajasida amalga oshirilishi lozim.

Birinchi navbatda, foydalanuvchilarning kiberxavfsizlik bo‘yicha savodxonligini oshirish muhim hisoblanadi. Foydalanuvchilar shubhali havolalarni ochmaslik, noma’lum

manbalardan kelgan fayllarni yuklab olmaslik va hech qachon SMS kodlar, parollar yoki PIN ma'lumotlarni uchinchi shaxslarga bermaslik kabi asosiy xavfsizlik qoidalarini bilishi kerak.

Ikkinchi yo'nalish — texnik himoya vositalaridan foydalanish. Bunga ikki bosqichli autentifikatsiya (2FA), antivirus dasturlar, firewall tizimlari hamda elektron pochta filtrlash tizimlari kiradi. Ushbu vositalar shubhali kirish urinishlarini erta bosqichda aniqlash va bloklash imkonini beradi.

Uchinchi muhim chora tashkiliy xavfsizlik siyosatlaridir. Tashkilotlarda ichki ma'lumot almashinuvi qat'iy nazorat qilinishi, moliyaviy operatsiyalar esa qo'shimcha tasdiqlash bosqichlaridan o'tishi kerak. Ayniqsa, "ikki tomonlama tasdiqlash" (dual verification) tizimi ijtimoiy muhandislik orqali amalga oshiriladigan pul o'g'irlash holatlarini kamaytiradi.

Ijtimoiy muhandislik hujumlarida raqamli izlar.

Ijtimoiy muhandislik hujumlari ko'pincha bevosita tizimni buzmasdan, foydalanuvchi orqali amalga oshirilgani sababli ular ortida qoladigan raqamli izlar alohida ahamiyatga ega hisoblanadi. Ushbu izlar hujumni aniqlash, uning ketma-ketligini tiklash va tajovuzkor harakatlarini tahlil qilish imkonini beradi.Eng asosiy raqamli izlardan biri — elektron aloqa yozuvlaridir.

Bunga yuborilgan va qabul qilingan email xabarlari, messenjer yozishmalari hamda ularning metadata ma'lumotlari kiradi. Metadata orqali yuboruvchining IP manzili, vaqt belgisi va xabar yo'nalishini aniqlash mumkin bo'ladi. Shuningdek, tizim log fayllari ham muhim manba hisoblanadi.

Login urinishlari, muvaffaqiyatli yoki muvaffaqiyatsiz autentifikatsiya jarayonlari, hamda g'ayrioddiy kirish vaqtlari hujum ehtimolini ko'rsatishi mumkin. Ayniqsa, bir nechta joydan bir vaqtning o'zida kirish urinishlari shubhali faoliyat sifatida baholanadi. Fayl tizimidagi o'zgarishlar ham muhim indikator hisoblanadi. Shubhali fayllarning yuklab olinishi, ochilishi yoki ishga tushirilishi tizimga zarar yetkazuvchi faoliyatni ko'rsatishi mumkin. Ayniqsa, phishing hujumlari orqali yuborilgan hujjatlar ichida yashiringan zararli kodlar ko'pincha shu bosqichda faollashadi. Umuman olganda, ijtimoiy muhandislik hujumlarida raqamli izlar hujumni to'liq rekonstruksiya qilish va uning manbasini aniqlashda asosiy rol o'ynaydi.

Ijtimoiy muhandislik asosidagi kibertahdidlarni samarali tahlil qilishda raqamli dalillarni to'g'ri yig'ish, ishonchli saqlash va professional tarzda tahlil qilish muhim bosqich hisoblanadi. Ushbu jarayon noto'g'ri bajarilsa, dalillarning huquqiy va texnik qiymati yo'qolishi mumkin. Raqamli dalillarni yig'ish jarayonida eng muhim talab — ma'lumotlarning asl holatini o'zgartirmaslikdir. Chunki har qanday o'zgarish dalilning ishonchliligiga salbiy ta'sir ko'rsatishi mumkin. Shu sababli maxsus forensik vositalar va himoyalangan usullar qo'llaniladi.

Yig'ilgan ma'lumotlar keyinchalik maxsus muhitda saqlanadi va ularning qayerdan, qachon va kim tomonidan olingani hujjatlashtirib boriladi. Tahlil bosqichida esa ushbu dalillar chuqur o'rganilib, shubhali login urinishlari, g'ayrioddiy tarmoq faolligi, zararli fayllar yoki phishing orqali kirib kelgan ma'lumotlar aniqlanadi.

Zamonaviy yondashuvlarda katta hajmdagi ma'lumotlarni tez tahlil qilish uchun avtomatlashtirilgan tizimlar va xavfsizlik monitoring platformalaridan ham foydalaniladi. Ijtimoiy muhandislik hujumlari amalda odatda foydalanuvchini ishonchga kirish orqali boshlanadi.Bunday holatlarda raqamli dalillar hujumni aniqlash va qayta tiklashda muhim rol o'ynaydi. Ijtimoiy muhandislik hujumlari texnik emas, balki psixologik zaifliklardan

foydalanishga asoslangan. Shu sababli ularga qarshi kurashishda nafaqat texnik himoya, balki foydalanuvchi xabardorligi ham muhim hisoblanadi.

Ushbu maqolada ijtimoiy muhandislik asosidagi kibertahdidlarning mohiyati, ularni aniqlash va oldini olish usullari tahlil qilindi. Natijalar shuni ko‘rsatadiki, bunday hujumlar asosan texnik zaifliklardan emas, balki inson psixologiyasi va ishonchidan foydalanishga asoslanadi. Shu sababli eng muhim himoya omili — foydalanuvchining o‘z ehtiyotkorligi va kiberxavfsizlik bo‘yicha ongli qaror qabul qilishidir.

Foydalanuvchi shubhali havolalarni ochmaslik, noma’lum fayllarni yuklab olmaslik, shaxsiy ma’lumotlarni uchinchi shaxslarga bermaslik kabi oddiy xavfsizlik qoidalariga amal qilishi zarur.

Bu o’rinda kiberjinoyatlardan ogohlikka chaqirish, aholining raqamli savodxonligini oshirish bo’yicha olib boriladigan targ’ibotlar, turli tadbirlar muhim ahamiyat kasb etadi.

FOYDALANILGAN ADABIYOTLAR:

1. O‘zbekiston Respublikasining Qonuni – “Kiberxavfsizlik to’g’risida”, O‘RQ – 764, 15.04.2022-yil

2. Abduraximov B.F. (professor). Kiberxavfsizlik va kriminalistika: Raqamli dalillarni tahlil qilish usullari. Muhammad al-Xorazmiy nomidagi Toshkent axborot texnologiyalari universiteti nashriyoti. 2023 y. (Kiberjinoyatlarda raqamli dalillarning o'ziga xosligi va forensika usullari).

3. UzCERT. Uzbekistan strengthened its position in the Global Cyber Security Index. 10.10.2025 y. (Kiberxavfsizlik hodisalari statistikasi)

4. ISO. ISO/IEC 27037:2012 – Information technology — Security techniques — Guidelines for identification, collection, acquisition and preservation of digital evidence. 2012 y.

5. O‘zbekiston Respublikasi Ichki ishlar vazirligi ATSJQK bo’lim va bo’linmalariga kiberjinoyatlar bo’yicha jabrlanuvchilardan tushayotgan murojaatlar tahlillari.

6. O‘zbekiston Respublikasi Axborot texnologiyalari va kommunikatsiyalarini rivojlantirish vazirligi materiallari.

7. Wikipediya onlayn erkin ensiklopediyasi - https://uz.wikipedia.org

8. Christopher Hadnagy - Social Engineering: The Science of Human Hacking - 2018