UNIVERSAL JOURNAL OF MATHEMATICAL THEORY AND COMPUTER SCIENCES
ISSN 2992 – 8788
https://sr-journals.org/index.php/UJMTCS

MOLIYAVIY TASHKILOTLARDA IJTIMOIY MUHANDISLIK HUJUMLARINI KO‘P MEZONLI RISK-BAHOLASH ASOSIDA ANIQLASH MODELI

Eshmurodov Alisher Akrom o’g’li
Muhammad al-Xorazmiy nomidagi Toshkent axborot texnologiyalari universiteti magistranti
alishereshmurodov61@gmail.com
Qudratov Ulug’bekxo’ja Ibodullo o’g’li
Muhammad al-Xorazmiy nomidagi Toshkent axborot texnologiyalari universiteti Axborot xavfsizligi kafedrasi stajiyor o’qituvchisi
qudratovulugbek0022@gmail.com

Annotatsiya: Mazkur maqolada moliyaviy tashkilotlarda uchraydigan ijtimoiy muhandislik hujumlarini aniqlashning ko‘p mezonli risk-baholash modeli taklif etiladi. Tadqiqotning dolzarbligi shundaki, zamonaviy kiberjinoyatchilar phishing, vishing, smishing, business email compromise va adversary-in-the-middle kabi usullarni inson omili bilan texnik zaifliklarni uyg‘unlashtirgan holda qo‘llamoqda. Moliyaviy sektor esa yuqori qiymatli ma’lumotlar, tezkor tranzaksiyalar va keng foydalanuvchi bazasi sababli bunday hujumlar uchun asosiy nishonlardan biri bo‘lib qolmoqda. ENISA ma’lumotlariga ko‘ra, 2023-yil yanvaridan 2024-yil iyunigacha Yevropa moliya sektoriga taalluqli 488 ta ommaviy xabar qilingan kiberhodisa tahlil qilingan, banklar esa eng ko‘p zararlangan subyektlar qatorida qayd etilgan. Verizon’ning 2025-yilgi moliya sektori bo‘yicha ko‘rinishida esa ijtimoiy muhandislik ushbu vertikalda asosiy buzilish naqshlaridan biri sifatida ko‘rsatilgan. Maqolada xabar matni, URL xususiyatlari, yuboruvchi identifikatori, foydalanuvchi xatti-harakati, vaqt omili va tranzaksion kontekst asosida ishlovchi ko‘p qatlamli model tavsiflanadi. Modelning ilmiy yangiligi ijtimoiy muhandislik hujumlarini faqat bitta indikator bilan emas, balki bir nechta semantik, texnik va xulqiy belgilar integratsiyasi orqali baholashga asoslanadi. Shuningdek, maqolada xavf darajasini hisoblash uchun ball beruvchi mexanizm, ogohlantirish chegaralari va amaliy tatbiq ssenariylari taklif etilgan. Tadqiqot natijalari moliyaviy muassasalarda adaptiv himoya tizimlarini yaratish, foydalanuvchi xatolarini kamaytirish va real vaqt rejimida shubhali xabarlarni filtrlash uchun nazariy hamda amaliy asos bo‘lib xizmat qiladi.

Kalit so‘zlar: ijtimoiy muhandislik, moliyaviy sektor, phishing, risk-baholash, kiberxavfsizlik, sun’iy intellekt, xulq-atvor tahlili, foydalanuvchi omili, BEC, tahdidlarni aniqlash.

Аннотация: В данной статье предлагается модель многокритериальной оценки риска для выявления атак социальной инженерии в финансовых организациях. Актуальность исследования обусловлена тем, что современные киберпреступники используют такие методы, как phishing, vishing, smishing, business email compromise и adversary-in-the-middle, комбинируя человеческий фактор с техническими уязвимостями. Финансовый сектор, в силу наличия высокоценных данных, быстроты транзакций и широкой пользовательской базы, остается одной из основных целей подобных атак.Согласно данным ENISA, в период с января 2023 года по июнь 2024 года было проанализировано 488 публично зарегистрированных киберинцидентов, связанных с финансовым сектором Европы, при этом банки оказались среди наиболее пострадавших субъектов. В обзоре Verizon за 2025 год также отмечается, что социальная инженерия является одним из ключевых паттернов нарушений в данном секторе. В статье описывается многоуровневая модель, основанная на анализе содержания сообщений, характеристик URL, идентификаторов отправителя, поведения пользователя, временного

фактора и транзакционного контекста. Научная новизна модели заключается в оценке атак социальной инженерии не по одному индикатору, а на основе интеграции семантических, технических и поведенческих признаков. Кроме того, в работе предлагается механизм расчета уровня риска, пороговые значения для формирования предупреждений и сценарии практического применения. Результаты исследования могут служить теоретической и практической основой для разработки адаптивных систем защиты в финансовых организациях, снижения пользовательских ошибок и фильтрации подозрительных сообщений в режиме реального времени.

Ключевые слова: социальная инженерия, финансовый сектор, фишинг, оценка риска, кибербезопасность, искусственный интеллект, поведенческий анализ, человеческий фактор, BEC, выявление угроз.

ABSTRACT: This article proposes a multi-criteria risk assessment model for detecting social engineering attacks in financial institutions. The relevance of the study is determined by the fact that modern attackers increasingly combine human manipulation with technical deception through phishing, vishing, smishing, business email compromise, and adversary-in-the-middle techniques. The financial sector remains one of the most attractive targets because of its high-value data, rapid transaction flows, and extensive customer infrastructure. According to ENISA, 488 publicly reported incidents affecting the European finance sector were analyzed for the period from January 2023 to June 2024, while Verizon's 2025 finance snapshot identifies social engineering as one of the dominant breach patterns in this industry. The paper describes a layered model that evaluates message content, URL features, sender identity, user behavior, temporal context, and transaction-related indicators. The novelty of the approach lies in integrating semantic, technical, and behavioral attributes into a unified risk score rather than relying on isolated indicators. A scoring mechanism, threshold-based warning logic, and practical implementation scenarios are also presented. The proposed model can serve as a theoretical and practical foundation for adaptive defense systems in financial organizations, reducing user error and improving early-stage detection of suspicious communications.

Keywords: social engineering, financial sector, phishing, risk assessment, cybersecurity, artificial intelligence, behavioral analysis, human factor, BEC, threat detection.

KIRISH (INTRODUCTION)

Raqamli transformatsiya moliyaviy xizmatlar ko‘lamini keskin kengaytirdi. Internet-banking, mobil ilovalar, masofaviy identifikatsiya, elektron to‘lov infratuzilmalari va fintech xizmatlarining ommalashuvi natijasida mijozlar uchun qulaylik oshgan bo‘lsa-da, hujum yuzasi ham sezilarli ravishda kengaydi. Bu sharoitda an’anaviy texnik himoya vositalari bilan bir qatorda inson omiliga yo‘naltirilgan firibgarlik usullariga qarshi kurashish alohida ahamiyat kasb etmoqda. NIST phishingni ishonchli manba ko‘rinishidagi aldov xabarlari orqali zararli havolani ochishga, faylni yuklab olishga yoki maxfiy ma’lumotni yuborishga majbur qiluvchi usul sifatida tavsiflaydi; ayniqsa bank yoki to‘lov tashkiloti nomidan yuborilgan soxta xabarlar moliyaviy sektorda xavfni kuchaytiradi.

So‘nggi yillarda ijtimoiy muhandislik hujumlari oddiy email firibgarligi darajasidan chiqib, ko‘p kanalli va moslashuvchan tahdidga aylandi. Endilikda hujumchilar elektron pochta, SMS, messenjer, telefon qo‘ng‘iroqlari, soxta autentifikatsiya oynalari va hatto MFA prompt bombing kabi usullarni uyg‘unlashtirgan holda foydalanuvchini noto‘g‘ri qaror qabul qilishga majbur qilmoqda. Verizon’ning 2025-yilgi hisobotida ijtimoiy muhandislik hodisalarida phishing va pretexting yetakchi usullar ekani, MFA prompt bombing esa sezilarli foizdagi hodisalarda uchrayotgani qayd etilgan. Xuddi shu hisobotda 2024-yilda BEC firibgarliklari doirasida 6,3 milliard dollardan ortiq mablag‘ ko‘chirilgani ko‘rsatiladi.Moliyaviy sektorning alohida zaifligi uning iqtisodiy qiymati, tranzaksion tezligi va foydalanuvchilarning doimiy “tezkor harakat” rejimida ishlashidadir. ENISA hisobotiga ko‘ra, 2023-yil yanvaridan 2024-yil iyunigacha tahlil qilingan 488 hodisa orasida banklar eng ko‘p zararlangan segment bo‘lib, ular umumiy holatlarning 46 foizida uchraydi. Bu raqamlar moliya sektorida ijtimoiy muhandislikka qarshi kurash faqat foydalanuvchi ogohligiga tayanib qolmasligi, balki tizimli risk-baholash modellarini joriy etishni talab qilishini ko‘rsatadi.

ADABIYOTLAR TAHLILI VA METOD

Ijtimoiy muhandislikni o‘rganishda tadqiqotchilar asosan uch yo‘nalishga e’tibor qaratadi: birinchisi — xabar mazmuni va til birliklariga asoslangan semantik aniqlash; ikkinchisi — URL, domen, yuboruvchi identifikatori, sertifikat va sarlavha kabi texnik belgilarga asoslangan filtrlash; uchinchisi esa foydalanuvchi xatti-harakatlarini modellashtirish orqali shubhali og‘ishlarni aniqlash. Mazkur yondashuvlarning har biri muayyan samaradorlikka ega bo‘lsa-da, ijtimoiy muhandislikning moslashuvchan tabiatini hisobga olganda, ularni alohida qo‘llash yetarli bo‘lmaydi. Chunki hujumchilar bir qatlamdagi himoyani aylanib o‘tish uchun boshqa qatlamdagi zaiflikdan foydalanadi.NIST Phish Scale foydalanuvchi phishing xabarini qanchalik qiyin aniqlashini baholashga mo‘ljallangan metodikani taklif etadi. Bu yondashuv juda muhim, chunki phishing samaradorligi ko‘p hollarda xabarning texnik zararli ekanidan ko‘ra, foydalanuvchi uni qanchalik ishonchli deb qabul qilishiga bog‘liq. Demak, zamonaviy modelda nafaqat xabarning o‘zi, balki uning qabul qiluvchi uchun qanchalik “ishonchli ko‘rinishi” ham o‘lchanishi lozim.

IBM X-Force’ning 2025-yilgi ma’lumotlari hujumchilar identity abuse va credential theft’dan tobora faolroq foydalanayotganini ko‘rsatadi. Hisobotda 2024-yilda infostealer tarqatuvchi email’lar 84 foizga oshgani, dastlabki 2025-yil ma’lumotlarida esa 2023-yilga nisbatan 180 foizgacha o‘sish kuzatilgani ta’kidlanadi. Bu holat ijtimoiy muhandislik hujumlari endi faqat oddiy phishing emas, balki keyingi bosqichdagi akkauntni egallab olish, sessiyani o‘g‘irlash va ichki tizimlarga kirish uchun start nuqtasi vazifasini ham bajarayotganini anglatadi. Shuningdek, Verizon’ning moliya sektori bo‘yicha 2025-yilgi tahlili Financial and Insurance vertikalida 3336 ta hodisa va 927 ta tasdiqlangan ma’lumotlar sizib chiqishi qayd etilganini, asosiy buzilish naqshlari esa System Intrusion, Social Engineering va Basic Web Application Attacks ekanini ko‘rsatadi. Demak, moliyaviy sohada ijtimoiy muhandislik ko‘pincha yakka hodisa emas, balki murakkab hujum zanjirining boshlang‘ich bosqichi sifatida namoyon bo‘ladi.

Mazkur tadqiqotda tizimli tahlil, qiyosiy tahlil, xavf indikatorlarini ajratish, ekspert-logik baholash va konseptual modellashtirish usullaridan foydalanildi. Dastlab moliyaviy sohada uchraydigan asosiy ijtimoiy muhandislik ssenariylari ajratildi: bank nomidan yuborilgan soxta xabarlar, login ma’lumotini so‘rovchi sahifalar, tranzaksiyani tasdiqlashni talab qiluvchi favqulodda bildirishnomalar, call-markaz operatori ko‘rinishidagi vishing, hamda korporativ hisoblar nomidan yuboriladigan BEC xabarlari. So‘ngra har bir ssenariy uchun indikatorlar to‘plami shakllantirildi. Taklif etilgan model oltita asosiy mezonga tayanadi. Birinchi mezon — matn semantikasi bo‘lib, unda shoshiltirish, qo‘rqitish, zudlik bilan harakat talab qilish, maxfiylikni buzishga undash va rasmiy uslubni sun’iy imitatsiya qilish kabi belgilar baholanadi. Ikkinchi mezon — texnik atributlar, bunda URL strukturasining shubhaliligi, domenning mos kelmasligi, yuboruvchi manzili va xat sarlavhasidagi anomaliyalar tekshiriladi. Uchinchi mezon — vizual ishonchlilik, ya’ni logotip, rang, korporativ til va interfeys imitasiya darajasi. To‘rtinchi mezon — foydalanuvchi xatti-harakati, masalan, odatda foydalanmaydigan qurilmadan tezkor login, noodatiy vaqt oralig‘idagi harakatlar yoki qisqa vaqt ichida ketma-ket havola ochish kabi holatlar. Beshinchi mezon — tranzaksion kontekst, oltinchisi esa avvalgi hodisalar bilan bog‘liqlikdir.

Modelning matematik ifodasi umumlashtirilgan xavf balli shaklida beriladi:

$$R = w_1 S + w_2 T + w_3 V + w_4 B + w_5 C + w_6 H$$

Bu yerda SSS — semantik risk, TTT — texnik risk, VVV — vizual imitatsiya darajasi, BBB — behavioral risk, CCC — kontekstual risk, HHH — tarixiy hodisalarga yaqinlik koeffitsienti, wiw_iwi esa ekspert va empirik sozlash asosida belgilanadigan og‘irlik koeffitsientlaridir. Mazkur formuladagi ustunlik shundaki, u qarorni izohlash imkonini beradi: tizim “xavfli” debgina javob bermaydi, balki aynan qaysi qatlamlar sabab xavf oshganini ham ko‘rsatadi. Bu moliyaviy tashkilotlarda audit va compliance jarayonlari uchun muhim. NIST’ning phishingni baholashga doir yondashuvlari ham izohlanadigan mezonlarga ehtiyoj borligini ko‘rsatadi. Taklif etilayotgan tizimga kiruvchi ma’lumotlar sifatida email, SMS, messenjer xabari, URL, QR-havola, autentifikatsiya oynasi haqidagi metadata va foydalanuvchi faoliyat loglari olinadi. Birinchi bosqichda normalizatsiya va

tozalash amalga oshiriladi: matn tokenlarga ajratiladi, URL qismlarga bo‘linadi, yuboruvchi identifikatorlari standart formatga keltiriladi. Ikkinchi bosqichda xususiyatlar ajratiladi. Bu bosqichda matndan buyruq ohangi, shoshiltirish iboralari, moliyaviy tasdiq so‘zlari, maxfiy ma’lumot talablari kabi semantik birliklar olinadi; URL’dan esa domen yoshi, subdomen chuqurligi, obfuskatsiya, typo-squatting ehtimoli va sertifikatga oid belgilar ajratiladi.Keyingi bosqichda foydalanuvchi harakatining kontekstual tahlili bajariladi. Masalan, xabar tungi vaqtda kelgan bo‘lsa, foydalanuvchi odatda tranzaksiya qilmaydigan geolokatsiyadan tizimga kirishga urinsa yoki bir necha soniya ichida ketma-ket linklarga bosilsa, model risk ballini oshiradi. Verizon hisobotida o‘g‘irlangan credential’lardan keyingi bosqichlarda keng foydalanilishi qayd etilganligi sababli, foydalanuvchi faolligini xabar tahlili bilan bog‘lash muhim hisoblanadi. Ijtimoiy muhandislik ko‘pincha yakka email emas, balki credential abuse’ga olib boruvchi zanjir bo‘lgani uchun riskni ketma-ketlik sifatida tahlil qilish zarur.Shundan so‘ng tizim ball beruvchi modulga o‘tadi. Har bir mezon uchun 0 dan 1 gacha oraliqda lokal xavf koeffitsienti aniqlanadi. Yakuniy R qiymati uch diapazonga bo‘linadi: past xavf, o‘rta xavf, yuqori xavf. Past xavf holatlarida tizim faqat jurnalga yozuv qoldiradi. O‘rta xavfda foydalanuvchiga ogohlantirish va qo‘shimcha tekshiruv ko‘rsatiladi. Yuqori xavfda esa xabar bloklanadi, sessiya vaqtincha muzlatiladi yoki tranzaksiya ikkilamchi verifikatsiyaga yuboriladi. Bunday ko‘p bosqichli javob modeli moliyaviy sektorda xato pozitiv va xato negativlar o‘rtasidagi muvozanatni ushlash uchun qulaydir.

MUHOKAMA (DISCUSSION)

Taklif etilgan modelning asosiy afzalligi shundaki, u ijtimoiy muhandislik hujumlarini faqat texnik zararli indikatorlar bilan cheklab qo‘ymaydi. An’anaviy antispam yoki blacklist yechimlari ko‘pincha URL yoki domen ma’lumotlari asosida ishlaydi. Biroq bugungi hujumchilar ishonchli brend imitasiya qilgan, yangi ochilgan, hali qora ro‘yxatga tushmagan domenlardan foydalana oladi. AI yordamida yozilgan matnlar esa grammatik jihatdan ancha toza va ishonchli bo‘lib bormoqda. NIST ham AI yordamida tobora ishontiruvchi phishing xabarlari yaratilayotganini ta’kidlaydi. Shu sababli faqat bitta signalga tayanish samarali emas.Ikkinchi afzallik — modelning izohlanishidir. Moliyaviy sektor uchun qaror qabul qiluvchi tizimlarda explainability muhim, chunki bloklangan tranzaksiya yoki karantin qilingan xabar bo‘yicha ichki audit, foydalanuvchi shikoyati yoki regulyator savoliga javob berish talab etilishi mumkin. Agar tizim “yuqori xavf” qarorini semantik tahdid 0.82, texnik tahdid 0.76 va xulqiy og‘ish 0.64 kabi ajratilgan ko‘rsatkichlar bilan asoslay olsa, u holda xavfsizlik bo‘limi ham, biznes bo‘limi ham qarorni tezroq qabul qiladi. Uchinchi jihat — model adaptiv tarzda o‘qitilishi mumkin. IBM X-Force ma’lumotlari hujumchilarning credential theft va infostealer kampaniyalariga tobora ko‘proq murojaat qilayotganini ko‘rsatgani sababli, tizimda vaqt o‘tishi bilan yangi patternlarni hisobga olish mexanizmi bo‘lishi kerak. Masalan, oldin kam uchragan MFA prompt bombing yoki AiTM ssenariylari keyinchalik yuqori og‘irlikka ega bo‘lishi mumkin. Demak, model statik emas, balki yangilanadigan tahdid razvedkasi bilan integratsiyalashgan bo‘lishi lozim. Shu bilan birga, modelning ayrim cheklovlari ham mavjud. Birinchidan, foydalanuvchi xulqini chuqur tahlil qilish maxfiylik va ma’lumotlarni himoya qilish talablarini kuchaytiradi. Ikkinchidan, juda qattiq thresholdlar foydalanuvchi tajribasini yomonlashtirishi mumkin. Uchinchidan, til va madaniy kontekst farqlari semantik tahlil modulining aniqligiga ta’sir qiladi. Shu bois modelni mahalliy bank amaliyoti, o‘zbek va rus tillaridagi real xabarlar, hamda tashkilotning ichki biznes-jarayonlariga moslab o‘qitish kerak bo‘ladi. ENISA ham moliya sektori uchun kiberbarqarorlikni oshirishda sektorga xos moslashtirilgan choralar zarurligini qayd etadi.

NATIJALAR (RESULTS)

Tadqiqot natijasida taklif etilayotgan ko‘p mezonli modelni banklar, mikroqarz tashkilotlari, to‘lov xizmatlari operatorlari va sug‘urta kompaniyalarida bir nechta qatlamda joriy etish mumkin. Birinchi qatlam — korporativ pochta va mijozlar bilan aloqa tizimlari; ikkinchi qatlam — internet-banking va mobil ilovalar; uchinchi qatlam — antifraud markazlari va SOC monitoring platformalari. Model ayniqsa “foydalanuvchi bosdi yoki bosmadi” degan sodda tekshiruvdan ko‘ra chuqurroq, kontekstga mos qaror chiqarishi bilan qimmatlidir. Verizon hisobotida moliya va sug‘urta sektorida buzilishlarning sezilarli qismi credentiallardan foydalanish bilan bog‘liq ekani ko‘rsatilgani sababli,

bunday model dastlabki aldov bosqichining o‘zida tahdidni ushlash imkonini beradi.Bundan tashqari, tizim foydalanuvchi xabardorligini oshirish vositasi sifatida ham ishlashi mumkin. Agar tizim xabarni bloklash bilan birga uning nima uchun xavfli ekanini — masalan, domen mos emasligi, shoshiltirish iboralari mavjudligi, yuboruvchi identifikatori qalbakilashtirilgani yoki noodatiy vaqt konteksti — ko‘rsatib bersa, foydalanuvchi asta-sekin tahdid alomatlarini mustaqil farqlashni o‘rganadi. Bu esa sof texnik himoyani insoniy immunitet bilan mustahkamlaydi. NIST Phish Scale’ning amaliy ahamiyati ham aynan shunda: phishingga qarshi kurashda faqat filtr emas, balki foydalanuvchining idrokini ham hisobga olish zarur.

XULOSA (CONCLUSION)

Mazkur maqolada moliyaviy tashkilotlarda ijtimoiy muhandislik hujumlarini aniqlash uchun ko‘p mezonli risk-baholash modeli taklif etildi. Tadqiqot davomida ijtimoiy muhandislikning zamonaviy shakllari, moliya sektorining zaif nuqtalari va mavjud yondashuvlarning chegaralari tahlil qilindi. Tahlillar shuni ko‘rsatdiki, moliyaviy sektor hali ham yuqori qiymatli nishon bo‘lib qolmoqda, ijtimoiy muhandislik esa ushbu sektordagi muhim buzilish naqshlaridan biri hisoblanadi. Taklif etilgan modelning ilmiy va amaliy qiymati uning bir vaqtning o‘zida semantik, texnik, vizual, xulqiy va kontekstual indikatorlarni yagona risk balliga birlashtirishidadir. Bunday yondashuv oddiy filtratsiyadan ko‘ra ancha moslashuvchan bo‘lib, nafaqat tahdidni erta aniqlash, balki qarorni izohlash imkonini ham beradi. Ayniqsa, AI yordamida tayyorlangan, ko‘proq ishonch uyg‘otuvchi phishing kampaniyalari ko‘payib borayotgan sharoitda, moliyaviy tashkilotlar uchun izohlanadigan va adaptiv himoya modellariga ehtiyoj yanada ortadi. Kelgusida ushbu modelni real bank loglari, ko‘p tilli xabarlar korpusi, tranzaksion anomaliyalar va foydalanuvchi profilingi bilan boyitish maqsadga muvofiq. Shuningdek, uni veb-ilova yoki antifraud platforma ko‘rinishida joriy etish orqali avvalgi maqolada taklif etilgan algoritmik asosning amaliy versiyasini yanada chuqurlashtirish mumkin. Shu ma’noda, ushbu maqola siz yuborgan oldingi ishning mantiqiy davomidir: birinchisida algoritm yaratish masalasi qo‘yilgan bo‘lsa, bu maqolada uning konseptual risk-arxitekturasi ilmiyroq asoslab berildi.

ADABIYOTLAR RO‘YXATI

1. ENISA. *Threat Landscape: Finance Sector (January 2023 to June 2024).* European Union Agency for Cybersecurity, 2025.
2. Verizon. *2025 Data Breach Investigations Report: Finance Snapshot.* 2025.
3. NIST. *Phish Scale User Guide.* National Institute of Standards and Technology, 2023.
4. NIST. *Phishing.* Small Business Cybersecurity Corner, 2021, updated guidance in use.
5. IBM. *2025 X-Force Threat Intelligence Index / Threat Index highlights.* 2025.
6. Stallings, W. *Network Security Essentials.* Pearson.