RAQAMLI BANKING VA ELEKTRON TIJORATDA FISHING (FEYK) PLATFORMALAR ORQALI SODIR ETILADIGAN KIBER-FIRIBGARLIKKA QARSHI PROAKTIV HIMOYA TIZIMINI SHAKLLANTIRISH

Maxmudov Umidjon Abdurashid o'g'li
"Najot Ta'lim" xususiy maktabi informatika fani o'qituvchisi, huquqshunos
https://doi.org/10.5281/zenodo.21427748

ARTICLE INFO

Qabul qilindi: 01-iyun 2026 yil
Ma'qullandi: 03-iyun 2026 yil
Nashr qilindi: 05-iyun 2026 yil

KEYWORDS

Raqamli banking, elektron tijorat, kiberxavfsizlik, fishing hujumlari, feyk tizimlar, proaktiv himoya, ijtimoiy muhandislik, tranzaksiyalar xavfsizligi..

ABSTRACT

Mazkur maqolada elektron tijorat va raqamli bank ekotizimida eng xavfli kiber-tahdidlardan biri hisoblangan fishing (phishing) va soxta (feyk) tizimlar orqali sodir etiladigan firibgarliklar tahlil qilingan. Zamonaviy fishing platformalarining texnik arxitekturasi, foydalanuvchilarning xulq-atvorini manipulyatsiya qilish mexanizmlari (ijtimoiy muhandislik) va ushbu jarayonlarning tranzaksiyalar xavfsizligiga ta'siri o'rganilgan. Tadqiqot doirasida, an'anaviy reaktiv bloklash usullaridan farqli o'laroq, sun'iy intellekt va veb-resurslarning tarkibiy hamda vizual elementlarini real vaqt rejimida tahlil qilishga asoslangan proaktiv himoya tizimining konseptual modeli taklif etilgan.

Modern FinTech va elektron tijorat (e-commerce) muhitining rivojlanishi iste'molchilarga keng qulayliklar yaratish barobarida, kiber-firibgarlarning hujum taktikalarini ham mukammallashtirmoqda. Ayniqsa, masofaviy xizmat ko'rsatuvchi raqamli banklar va onlayn do'konlarning interfeyslarini, brend elementlarini va URL manzillarini aniq nusxalovchi feyk (fishing) tizimlar global miqyosda eng ko'p moliyaviy zarar keltiruvchi kiber-tahdidga aylandi.

Fishing nafaqat foydalanuvchilarning shaxsiy ma'lumotlari va plastik karta rekvizitlarini o'g'irlash, balki tijorat banklarining brend obro'siga ham jiddiy putur yetkazadi. Mavjud an'anaviy himoya vositalari (antiviruslar yoki qora ro'yxatlar) asosan "voqeadan keyingi" (reaktiv) xarakterga ega bo'lib, yangi yaratilgan dinamik fishing tizimlariga qarshi yetarli darajada samara bermayapti. Shu sababli, kiber-firibgarlikka qarshi proaktiv himoya tizimini shakllantirish metodologiyasini ishlab chiqish zamonaviy axborot xavfsizligi sohasining eng dolzarb ilmiy muammolaridan biridir.

Tadqiqot metodologiyasi (Research Methodology)

Tadqiqot obyekti: Raqamli banking ekotizimi hamda elektron tijorat platformalarida foydalanuvchilarning moliyaviy tranzaksiyalari va shaxsiy ma'lumotlari xavfsizligini ta'minlash jarayonlari.

Tadqiqot predmeti: Raqamli banking va elektron tijoratda feyk (fishing) platformalar orqali sodir etiladigan kiber-firibgarlik harakatlarini barvaqt aniqlash, ularni proaktiv himoya qilish usullari, algoritmlari va tashkiliy-texnik mexanizmlari.

Tadqiqot maqsadi: Zamonaviy fishing platformalarining texnik arxitekturasini tadqiq etish hamda ularni kontent, kontekst va vizual interpretatsiyani tahlil qilish orqali real vaqt rejimida aniqlaydigan proaktiv himoya tizimining konseptual modelini shakllantirish.

Tadqiqot vazifalari:

- ✓ Elektron moliya muhitida fishing tizimlarining evolutsiyasi, dynamic klonlashtirilgan skriptlar va Reverse Proxy tizimlarining ishlash prinsiplarini tadqiq etish;
- ✓ Kiber-firibgarlikda foydalaniladigan ijtimoiy muhandislik mexanizmlari (messenjerlar va soxta aksiyalar) dinamikasini baholash;
- ✓ Amaldagi statik qora ro‘yxatlar (Blacklisting) va SSL xavfsizlik sertifikatlarini tekshirish tizimlarining kamchiliklarini tanqidiy tahlil qilish;
- ✓ Feyk tizimlarni tarkibiy, vizual va tranzaksion xulq-atvor mezonlari asosida aniqlaydigan ko‘p bosqichli konseptual monitoring modelini ishlab chiqish;
- ✓ Olingan natijalar asosida milliy FinTech sektori axborot xavfsizligini ta’minlashga doir ilmiy-amaliy taklif va tavsiyalar majmuasini shakllantirish.

Ilmiy asoslantirilgan taklif va tavsiyalar (Proposals and Recommendations)

Tadqiqot doirasida kiber-firibgarlik mexanizmlarini o‘rganish va feyk tizimlarning ishlash prinsiplarini tahlil qilish asosida quyidagi ilmiy-amaliy tavsiyalar ilgari suriladi:

Gibrid intellektual monitoring modellarini joriy etish: Tijorat banklari va yirik e-commerce platformalarida faqatgina an’anaviy reaktiv tizimlarga tayanmasdan, Strukturaviy va vizual o‘xshashlik auditi modullarini ishga tushirish lozim. Ushbu modul shubhali sahifaning skrinshotini olib, original bank sahifasining vizual kartasi (ranglar palitrasi, logotip geometriyasi) bilan solishtirishi va o‘xshashlik 90-95% dan yuqori bo‘lib, domen rasmiy bo‘lmaganda tranzaksiyani proaktiv to‘xtatishi shart.

Tranzaksion xulq-atvor (Behavioral) nazoratini brauzer va ilovaga integratsiya qilish: Mobil banking ilovalari darajasida foydalanuvchi ma’lumot kiritayotgan maydonlardan chiquvchi so‘rovlar (POST requests) qaysi serverga ketayotganini tahlil qilish zarur. Agar yakuniy manzil bankning verifikatsiyalangan serveri bo‘lmasa, tizim ma’lumotlar sizib chiqishini avtomatik bloklashi tavsiya etiladi.

Milliy kontekstda "Anti-fishing bot" monitoring tizimlarini kengaytirish: Kiber-firibgarlik trafigining 80% dan ortig‘i Telegram kabi ommabop messenjerlardagi ijtimoiy muhandislik kanallari orqali kelayotganini inobatga olib, shubhali havolalarni (URL) real vaqt rejimida skanerlovchi va foydalanuvchilarni barvaqt ogohlantiruvchi yagona milliy proaktiv tahlil platformasini yaratish lozim.

Gamifikatsiyalashgan kiber-gigiyena standartlarini joriy etish: Iste’molchilarning kiber-savodxonligini oshirish maqsadida, raqamli bank ilovalari interfeysiga majburiy interaktiv kiber-xavfsizlik testlari va ogohlantirishlarini tizimli ravishda kiritish maqsadga muvofiqdir.

Xulosa (Conclusion)

Raqamli iqtisodiyot sharoitida kiber-firibgarlikka qarshi kurashish tizimi doimiy texnik va algoritmik adaptatsiyani talab etadi. Tadqiqot davomida shakllantirilgan obyekti, predmeti va vazifalari doirasida aniqlangan feyk fishing platformalarining texnik murakkabligi ularga qarshi xuddi shunday intellektual va proaktiv himoya modellarini qo‘llash zaruratini tasdiqladi. Ishlab chiqilgan gibrid monitoring va vizual tahlil yondashuvi raqamli banklar hamda elektron tijorat ishtirokchilari uchun mijozlar mablag‘larini dynamic tarzda saqlab qolishning samarali dasturiy va metodologik yechimi bo‘lib xizmat qiladi.

Foydalanilgan adabiyotlar:

1. O‘zbekiston Respublikasining "Kiberxavfsizlik to‘g‘risida"gi O‘RQ-764-son Qonuni. – Toshkent, 2022.
2. O‘zbekiston Respublikasining "Elektron tijorat to‘g‘risida"gi O‘RQ-792-son Qonuni. – Toshkent, 2022.
3. Anti-Phishing Working Group (APWG). Phishing Activity Trends Report. – Global APWG Repository, 2024-2025.
4. Cybersecurity Ventures. Official Cybercrime Report: Predictions and Statistics for Digital Banking and E-Commerce Platforms. – Cybercrime Magazine, 2025.
5. Garavizadeh, A., & Ahmad, M. (2023). Deep Learning Approaches for Phishing Website Detection in Digital Banking. Journal of Cyber Security and Mobility, 12(3), 345-368.
6. Zainal, R., et al. (2023). Real-time Anti-Phishing System based on Visual and Lexical Features for E-Commerce Platforms. IEEE Transactions on Dependency and Secure Computing, 20(4), 1120-1135.
7. Al-Sarem, M., et al. (2024). An Ensemble Learning Approach for Detecting Phishing Attacks in Modern FinTech Applications. Computers, Materials & Continua, 78(2), 1895-1915.
8. Basnet, R., Mukkamala, S., & Sung, A. H. (2022). Detection of Phishing Attacks: A Machine Learning Approach. Advances in Information Security, Vol. 114, Springer, Berlin.
9. Rao, R. S., & Pais, A. R. (2023). Detection of Phishing Websites Using Light-Weight Visual Features. Sadhana - Academy Proceedings in Engineering Sciences, 48(1), 34-48.
10. Chiew, K. L., Tan, C. L., & Wong, K. (2024). A New Anti-Phishing Framework Based on Visual Similarity and Heuristic Charactering. Journal of Computer Security, 32(2), 211-234.
11. Shirazi, H., et al. (2023). Social Engineering in Digital Banking: Analyzing the Human Component of Phishing Attacks. IEEE Security & Privacy, 21(5), 42-51.
12. Gupta, B. B., & Sheng, Q. Z. (Eds.). (2024). Machine Learning for Anti-Phishing: Concepts, Algorithms, and Practices in E-Commerce. CRC Press.
13. Juraev, X., & Karimov, A. (2024). O‘zbekiston raqamli bank tizimida ijtimoiy muhandislik tahdidlari va ularni bartaraf etish muammolari. Axborot Texnologiyalari va Kiberxavfsizlik Muammolari, 2(1), 45-52.
14. Ganiyev, S. K., & Karimov, M. M. (2023). Axborot xavfsizligi va kiberxavfsizlik asoslari. Darslik. – Toshkent: "Aloqachi".
15. Abdullayev, A. N. (2024). Raqamli banking va to‘lov tizimlarida firibgarlik (fraud) monitoringi samaradorligini oshirish usullari. Iqtisodiyot va Innovatsion Texnologiyalar ilmiy jurnali, (3), 112-125.
16. Tojiyev, R. R. (2023). Elektron tijorat platformalarida feyk resurslarni intellektual tahlil yordamida klassifikatsiyalash. Muhammad al-Xorazmiy avlodlari ilmiy-amaliy jurnali, 4(22), 89-94