



TIJORAT BANKLARIDA FISHING HUJUMLARI XAVFI VA ULARNING BANK OPERATSIYALARIGA TA'SIRINI BAHOLASH METODOLOGIYASI

Xayrullayev Zuxriddin Akbar o'g'li

O'zbekiston Respublikasi Bank-moliya akademiyasi magistranti

<https://doi.org/10.5281/zenodo.18951212>

Annotatsiya: Mazkur maqolada tijorat banklari faoliyatida fishing (phishing) hujumlari xavfining ortib borish tendensiyalari hamda ularning bank operatsiyalarining xavfsizligiga ko'rsatadigan ta'siri ilmiy jihatdan tahlil qilinadi. Raqamli bank xizmatlari, internet-banking, mobil banking va elektron to'lov tizimlarining keng rivojlanishi sharoitida bank tizimi kiberxavfsizlik bilan bog'liq yangi tahdidlarga duch kelayotgani asoslab beriladi. Tadqiqot davomida fishing hujumlarining bank mijozlari ma'lumotlarini noqonuniy qo'lga kiritish, bank kartalari rekvizitlari va elektron to'lov tizimlariga kirish orqali moliyaviy operatsiyalarga zarar yetkazish mexanizmlari o'rganildi.

Kalit so'zlar: yashil iqtisodiyot, yashil loyihalar, yashil moliyalashtirish, yashil obligatsiyalar, yashil kreditlar, barqaror rivojlanish, qayta tiklanuvchi energiya, energiya samaradorligi, ekologik investitsiyalar, davlat-xususiy sherikchilik (DXSh), innovatsion moliyaviy instrumentlar, xalqaro moliya institutlari, fiskal rag'batlantirish, ekologik infratuzilma.

Kirish. Bugungi kunda global iqlim o'zgarishi, tabiiy resurslardan samarasiz foydalanish hamda ekologik muammolarning kuchayishi iqtisodiy rivojlanishning yangi, barqaror modelini shakllantirish zaruratini yuzaga keltirmoqda. Shu nuqtai nazardan, yashil iqtisodiyot tamoyillariga asoslangan loyihalarni moliyalashtirish masalasi xalqaro hamjamiyat hamda milliy iqtisodiyotlar uchun ustuvor yo'nalishlardan biriga aylanmoqda. Yashil loyihalar, xususan qayta tiklanuvchi energiya manbalarini rivojlantirish, energiya samaradorligini oshirish, ekologik toza texnologiyalarni joriy etish va atrof-muhitni muhofaza qilishga qaratilgan tashabbuslarni amalga oshirish uchun samarali moliyaviy mexanizmlarni yaratish muhim ahamiyat kasb etadi. Shu sababli yashil loyihalarni moliyalashtirishda innovatsion moliyaviy instrumentlardan foydalanish, davlat va xususiy sektor o'rtasidagi hamkorlikni rivojlantirish hamda mavjud institutsional va moliyaviy muammolarni aniqlash va bartaraf etish masalalarini ilmiy jihatdan o'rganish dolzarb hisoblanadi.

Xulosa. Xulosa qilib aytganda, tijorat banklarida fishing hujumlari xavfi bank operatsiyalarining xavfsizligi, moliyaviy barqarorligi hamda mijozlar ishonchiga bevosita ta'sir ko'rsatadigan muhim kiberxavfsizlik muammolaridan biri hisoblanadi. Shu sababli ushbu tahdidlarni samarali boshqarish uchun fishing



hujumlari xavfini kompleks baholash metodologiyasini qo'llash zarur bo'lib, bunda bank axborot tizimlarining zaif tomonlarini aniqlash, operatsion va moliyaviy zararlarni tahlil qilish, risk darajasini baholash hamda statistik monitoring usullaridan foydalanish muhim ahamiyat kasb etadi. Bundan tashqari, zamonaviy texnologiyalarni joriy etish, ko'p bosqichli autentifikatsiya tizimlarini qo'llash va mijozlarning kiberxavfsizlik bo'yicha xabardorligini oshirish orqali fishing hujumlarining oldini olish mumkin. Natijada tijorat banklarida elektron bank xizmatlarining ishonchliligi ortadi, bank operatsiyalarining xavfsizligi mustahkamlanadi hamda moliyaviy tizimning barqaror rivojlanishi ta'minlanadi.

Foydalanilgan adabiyotlar ro'yxati:

1. Karimov, B. (2021). Raqamli bank xizmatlari xavfsizligini ta'minlash masalalari. Toshkent: Iqtisodiyot nashriyoti.
2. Yuldashev, S. & Abdullayeva, M. (2022). Tijorat banklarida kiberxavfsizlik risklarini boshqarish masalalari. Bank va moliya tizimi tadqiqotlari jurnali, 3(2), 45–53.
3. Volkova, O.V. (2023). Phishing как угроза бизнесу и государству. Научные исследования экономики и управления, 4(2), 112–118.
4. O'g'li, A.R.N. (2024). Цифровые угрозы банковскому сектору и обеспечение безопасности банковских операций. Cyberleninka iqtisodiy tadqiqotlar jurnali, 6(1), 71–80.
5. Ali, M.M. (2024). Phishing – a cyber fraud: Types, implications and governance issues. Journal of Information Security, 18(2), 221–236.
6. Pinjarkar, L., Hete, P.R. & Agrawal, P. (2024). An examination of prevalent online scams: Phishing attacks, banking frauds and e-commerce deceptions. International Conference on Advances in Information Technology Proceedings, 145–152.
7. Kara, I. (2021). Detection and analysis of a real e-banking phishing attack. Journal of Digital Forensics, Security and Law, 16(2), 1–12.
8. Cele, N.N. (2023). Cybersecurity threats and their impact on digital banking systems. International Journal of Information Security Research, 9(3), 210–224.
9. Smaga, P. (2024). Profiling cyber risk and targeted attacks in commercial banks. Computers & Security, 142, 103–115.
10. Waliullah, M., George, M.Z.H., Hasan, M.T. & Alam, M.K. (2024). Assessing the influence of cybersecurity threats on digital banking adoption. Journal of Financial Technology Research, 11(4), 55–70.
11. Watters, P. (2019). Cybercrime and phishing detection in financial systems. Journal of Cybersecurity Studies, 7(1), 33–49.



POLAND

CURRENT APPROACHES AND NEW RESEARCH IN MODERN SCIENCES

International scientific-online conference



POLAND

12. Carpenter, P. (2020). Human risk management and phishing awareness in organizations. *Information Security Professional*, 22(5), 18–26.
13. Shapiro, S.J. (2023). *Fancy Bear Goes Phishing: The Dark History of the Information Age*. New York: Farrar, Straus and Giroux.