# MOLIYAVIY SAVODXONLIK DARAJASINING KIBERFIRIBGARLIKDAN HIMOYALANISHGA TA'SIRI O'ZBEKISTON MISOLIDA PEST TAHLILI

**Imomov Jamshidxon Odilovich**
Toshkent davlat iqtisodiyot universiteti
"Iqtisodiyot va moliyaviy xavfsizlik" kafedrasi
dotsenti, PhD.
E-mail: jamshidkhon@gmail.com

**Toshpo'latova Mohizodaxon Latifxon qizi**
Toshkent xalqaro universiteti
talabasi
Tel.: +998 50 889 25 88

**Annotatsiya**

Mazkur maqolada O'zbekistonda moliyaviy savodxonlik darajasining kiber-firibgarlikdan himoyalanishga ta'siri PEST tahlili asosida o'rganildi. Tadqiqotda plastik karta va mobil to'lovlardan foydalanish jarayonida yuzaga keladigan siyosiy, iqtisodiy, ijtimoiy va texnologik omillar tahlil qilindi. Natijalar an'anaviy moliyaviy bilimlar bilan bir qatorda raqamli xavfsizlik ko'nikmalari ham fuqarolarning firibgarlik xavfini kamaytirishda muhim ahamiyatga ega bo'lganini ko'rsatdi. Shuningdek, banklar, davlat institutlari va foydalanuvchilar o'rtasidagi hamkorlik moliyaviy himoya madaniyatini mustahkamlashga xizmat qilgani asoslandi.

**Kalit so'zlar:** moliyaviy savodxonlik, kiber-firibgarlik, PEST tahlili, raqamli xavfsizlik, plastik karta, mobil to'lovlar.

**Аннотация**

В статье было изучено влияние уровня финансовой грамотности на защиту от кибермошенничества в Узбекистане на основе PEST-анализа. В исследовании были рассмотрены политические, экономические, социальные и технологические факторы, возникающие при использовании банковских карт и мобильных платежей. Результаты показали, что наряду с традиционными финансовыми знаниями важную роль в снижении риска мошенничества сыграли навыки цифровой безопасности. Также было обосновано, что сотрудничество банков, государственных институтов и пользователей способствовало укреплению культуры финансовой защиты.

**Ключевые слова:** финансовая грамотность, кибермошенничество, PEST-анализ, цифровая безопасность, банковская карта, мобильные платежи.

**Abstract**

This article examined the impact of financial literacy on protection against cyber fraud in Uzbekistan using PEST analysis. The study analyzed political, economic, social, and technological factors related to the use of bank cards and mobile payment systems. The findings showed that, along with traditional financial knowledge, digital security skills played an important role in reducing fraud risks among users. The research also demonstrated that cooperation among banks, public institutions, and citizens contributed to strengthening a culture of financial protection. The study

confirmed the practical importance of digital financial literacy in improving cyber fraud prevention.

**Keywords:** financial literacy, cyber fraud, PEST analysis, digital security, bank card, mobile payments.

## KIRISH

Raqamli to‘lov texnologiyalarining keng tarqalishi bilan plastik karta va mobil to‘lovlar O‘zbekiston fuqarolarining kundalik hayotiga mustahkam kirib keldi. Milliy to‘lov tizimlari orqali amalga oshirilayotgan tranzaksiyalar hajmi yillik 40 foizdan ortiq o‘sish sur’atida oshmoqda. Biroq moliyaviy xizmatlarning raqamlashuvi bilan parallel ravishda kiber-firibgarlik ham ko‘lami va murakkabligi jihatidan tobora jiddiy tahdidga aylanmoqda. Nasdaq kompaniyasining 2024-yilgi global moliyaviy jinoyatlar hisobotiga ko‘ra, jahon miqyosida moliyaviy firibgarlikdan yetkazilgan zarar 485,6 milliard AQSh dollarini tashkil etdi. Kaspersky laboratoriyasining 2025-yilgi ma’lumotlariga ko‘ra esa, dunyo bo‘ylab 2 milliondan ortiq bank kartasi ma’lumotlari zararli dasturlar yordamida o‘g‘irlangan.

O‘zbekiston ushbu global tendentsiyadan mustasno emas. Markaziy bankning CERT-CBU kiberxavfsizlik markazi ma’lumotlariga ko‘ra, ijtimoiy injeneriya - psixologik manipulyatsiya orqali aldash - mamlakatimizda moliyaviy firibgarlikning eng keng tarqalgan usuli hisoblanadi. Firibgarlar fuqarolarning bank tizimiga ortiqcha ishonuvchanligidan va raqamli xavfsizlik ko‘nikmalari yetarli emasligidan foydalanib, karta mablag‘larini o‘g‘irlaydi.

Moliyaviy savodxonlikni oshirish kiber-firibgarlikka qarshi kurashning asosiy yo‘li sifatida ko‘p yillardan beri e’tirof etiladi. Biroq zamonaviy xalqaro tadqiqotlar bu munosabatning ancha murakkab ekanligini ko‘rsatmoqda. Ruiz (2026) 10 ta Yevropa mamlakatida 14 000 dan ortiq kishi orasida o‘tkazilgan tadqiqotida an’anaviy moliyaviy savodxonlik fishing va Ponzi sxemalariga qarshi sezilarli himoya ta’sirini bermasligini aniqladi. Asosiy himoya omili bo‘lib raqamli xavfsizlik ko‘nikmalari - parolni himoya qilish, shubhali saytlarni tanib olish, shaxsiy ma’lumotlarni oshkor qilmaslik - ekanligi isbotlandi.

Ushbu maqolaning maqsadi - O‘zbekiston plastik karta foydalanuvchilarining kiber-firibgarlikdan himoyalanish holatiga ta’sir etuvchi omillarni PEST tahlili (Political - siyosiy, Economic -iqtisodiy, Social - ijtimoiy, Technological - texnologik) orqali tizimli baholab, davlat siyosati va bank amaliyoti uchun amaliy tavsiyalar ishlab chiqishdir. PEST tahlili murakkab statistik hisob-kitoblarsiz, ammo tizimli va keng qamrovli baholashni ta’minlaydi, shuning uchun ijtimoiy-iqtisodiy tadqiqotlarda keng qo‘llaniladi.

## ADABIYOTLAR SHARHI

Moliyaviy savodxonlik va kiberxavfsizlik masalalari zamonaviy raqamli iqtisodiyot sharoitida ilmiy tadqiqotlarning muhim yo‘nalishlaridan biriga aylandi. Jahon amaliyotida moliyaviy savodxonlik fuqarolarning moliyaviy qarorlar qabul qilish sifati, moliyaviy xizmatlardan samarali foydalanishi va moliyaviy xavflardan himoyalanish darajasini belgilovchi asosiy omillardan biri sifatida e’tirof etiladi [1].

Moliyaviy savodxonlikning nazariy asoslari va uni baholash metodologiyasi OECD hamda INFE tomonidan ishlab chiqilgan yondashuvlarda keng yoritilgan bo‘lib, ularda moliyaviy bilim, xulq-atvor va moliyaviy munosabatlarning o‘zaro bog‘liqligi asoslab berilgan [2]. Tadqiqotlarda moliyaviy savodxonlik darajasi yuqori bo‘lgan aholining moliyaviy firibgarlik va tavakkalchiliklarga nisbatan barqarorroq ekanligi qayd etilgan [3].

Raqamli texnologiyalarning keng tarqalishi bilan kiber-firibgarlik muammosi ham dolzarb ahamiyat kasb eta boshladi. Anderson va hamkorlari kiberjinoyatlar iqtisodiy zararining ortib borayotganini ko‘rsatib, foydalanuvchilarning axborot xavfsizligi bo‘yicha bilimlari himoyalanish darajasiga bevosita ta’sir qilishini ta’kidlaganlar [4]. Hadnagy tomonidan olib borilgan tadqiqotlarda esa ijtimoiy injeneriya usullari orqali amalga oshiriladigan firibgarliklar inson omiliga asoslanishi va moliyaviy savodxonlikning bu xavflarni kamaytirishdagi o‘rni yoritilgan [5].

Kiberxavfsizlik va foydalanuvchi xulq-atvori o‘rtasidagi bog‘liqlik Albladi va Weir tadqiqotlarida ham tahlil qilingan bo‘lib, mualliflar raqamli savodxonlik darajasi oshgan sari fishing va boshqa firibgarlik usullariga nisbatan barqarorlik kuchayishini aniqlaganlar [6]. Shu bilan birga, moliyaviy texnologiyalar va mobil to‘lov tizimlarining rivojlanishi foydalanuvchilardan nafaqat moliyaviy bilim, balki raqamli xavfsizlik ko‘nikmalarini ham talab qilishi qayd etilgan [7].

PEST tahlili usuli iqtisodiy va boshqaruv tadqiqotlarida tashqi muhit omillarini tizimli baholash vositasi sifatida keng qo‘llaniladi. Kotler va Keller siyosiy, iqtisodiy, ijtimoiy hamda texnologik omillar tashkilotlar va iste’molchilar faoliyatiga sezilarli ta’sir ko‘rsatishini asoslab berganlar [8]. Ushbu yondashuv moliyaviy savodxonlik va kiber-firibgarlik o‘rtasidagi bog‘liqlikni kompleks baholash imkonini yaratadi.

O‘zbekistonda ham moliyaviy xizmatlarni raqamlashtirish, elektron to‘lov tizimlarini rivojlantirish va aholining moliyaviy savodxonligini oshirish bo‘yicha keng ko‘lamli islohotlar amalga oshirilmoqda [9]. Mazkur jarayonlar fuqarolarning moliyaviy xavfsizligini mustahkamlash va kiber-firibgarlik holatlarining oldini olish uchun yangi imkoniyatlar yaratmoqda [10].

## METODOLOGIYA

Tadqiqot ikki bosqichdan iborat. Birinchi bosqich - miqdoriy ma’lumot to‘plash. 2024-yilda Toshkent shahrida ijtimoiy-sotsiologik so‘rovnoma o‘tkazildi. So‘rovnomada 391 ta respondent ishtirok etdi (n=391). Anketa 44 ta savoldan iborat bo‘lib, barchasi 5 balli Likert shkalasida tuzilgan (1=mutlaqo roziman emasman, 5=mutlaqo roziman). Savollar 9 ta tematik blokni qamrab oladi: umumiy moliyaviy savodxonlik, raqamli ko‘nikmalar, kiberxavfsizlik bilimi, shaxsiy firibgarlik tajribasi, bank tizimiga ishonch, himoya choralarini amaliy qo‘llash, ijtimoiy injeneriya munosabati, raqamli to‘lov ilovalaridan foydalanish va umumiy qoniqish darajasi.

So‘rovnomaning ichki ishonchliligi Kronbax alfa koeffitsiyenti orqali tekshirildi. Natijalar: umumiy moliyaviy savodxonlik bloki a=0,891; raqamli ko‘nikmalar a=0,856; kiberxavfsizlik bilimi a=0,872; bank tizimiga ishonch a=0,919; himoya choralarini qo‘llash a=0,834. Barcha bloklar Nunnally mezoniga ko‘ra qoniqarli (>0,70) va yuqori (>0,80) ishonchlilik darajasini ko‘rsatdi.

Ikkinchi bosqich - PEST matritsa tuzish. So‘rovnoma natijalari va xalqaro ilmiy adabiyotlar (2014-2026-yillar, Scopus, Web of Science va ScienceDirect bazalari) tahlili asosida PEST matritsaning to‘rtta bo‘limi to‘ldirildi. Har bir bo‘lim uchun asosiy topilmalar va ularning amaliy ma’nosi aniqlab berildi. PEST omillar mazmunini boyitish uchun CERT-CBU kiberxavfsizlik markazi hisobotlari, Yevropa Markaziy banki va Yevropaning banklararo nazorat organi (ECB/EBA) hamda Nasdaq global firibgarlik hisobotlaridan foydalanildi.

PEST tahlili strategik menejmentda tashqi muhitni baholash uchun ishlab chiqilgan, biroq keyinchalik ijtimoiy-iqtisodiy tadqiqotlarda ham keng qo‘llanila boshlandi. Usul muammoga ta’sir etuvchi to‘rtta omil toifasini tizimli ko‘rib chiqishni taklif etadi: siyosiy omillar - qonunchilik, regulyatsiya, davlat siyosati, xalqaro hamkorlik; iqtisodiy omillar - bozor holati, daromad, moliyaviy tendensiyalar va yo‘qotishlar; ijtimoiy omillar - xulq-atvor, madaniyat, demografiya va jamiyatdagi ishonch darajasi; texnologik omillar - innovatsiyalar, raqamlashtirish, infratuzilma va yangi tahdidlar.

Moliyaviy savodxonlik va kiber-firibgarlik sohasida PEST tahlilining asosiy afzalligi shundaki, u muammoni faqat individual bilim darajasi nuqtai nazaridan emas, balki keng ijtimoiy, regulyativ va texnologik muhit bilan bog‘lab ko‘rishga imkon beradi. Bu yondashuv qonunchilar, nazorat organlari, banklar va ta’lim muassasalari uchun amaliy xulosalar chiqarishni osonlashtiradi.

## TAHLIL VA NATIJALAR

PEST tahlilini o‘tkazishdan oldin so‘rovnomaning miqdoriy natijalarini ko‘rib chiqish zarur - chunki ular, ayniqsa, PEST matritsasining ijtimoiy qismini isbotlovchi empirik asos bo‘lib xizmat qiladi.

**1-jadval**

**Asosiy ko‘rsatkichlar (n=391, Toshkent, 2026)[1]**

| Kod | Ko‘rsatkich | O‘rtacha (M) | Shkaladan | Daraja |
|---|---|---|---|---|
| S1 | Umumiy moliyaviy savodxonlik | 3,48 | 5,0 | O‘rta |
| S5 | Kiberxavfsizlik bo‘yicha bilim | 3,76 | 5,0 | O‘rta+ |
| S7 | Raqamli ko‘nikmalar darajasi | 3,35 | 5,0 | O‘rta |
| S12 | Himoya choralarini amalda qo‘llash | 3,21 | 5,0 | O‘rta |
| S19 | Bank kompensatsiyasiga ishonch | 1,70 | 5,0 | Past |
| GAP | Bilim-ishonch tafovuti (S5 − S19) | 2,06 | - | Yuqori |

1-jadvaldan ko‘rinib turibdiki, respondentlar kiberxavfsizlik bilimi bo‘yicha o‘rtacha 3,76 ball ko‘rsatdi - bu 5 ballik shkalada qoniqarli daraja. Biroq bank kompensatsiyasiga ishonch atigi 1,70 ballni tashkil etdi, ya’ni respondentlarning katta qismi firibgarlik yuz berganda bankdan yetarli yordam olishiga ishonmaydi. Ushbu ikki ko‘rsatkich orasidagi +2,06 birlik farq - “bilim-ishonch paradoksi” - maqolaning markaziy topilmasi bo‘lib, u PEST matritsasining ijtimoiy bo‘limida batafsil tahlil qilinadi.

[1] Manba: muallif, 2024-yilgi so‘rovnoma asosida (n=391, Toshkent).

PEST matritsa to‘rtta yo‘nalish bo‘yicha alohida ko‘rib chiqiladi. Har bir yo‘nalishda O‘zbekiston holati, xalqaro adabiyotlar bilan taqqoslama va amaliy xulosa beriladi.

*P - Siyosiy omillar (Political)* Siyosiy omillar moliyaviy savodxonlik va kiberxavfsizlik sohasidagi qonunchilik, davlat dasturlari, nazorat organlari faoliyati va xalqaro hamkorlikni qamrab oladi.

*Ijobiy holat.* O‘zbekistonda moliyaviy savodxonlikni oshirishga qaratilgan bir qator muhim hujjatlar qabul qilingan. 2022-yilgi “Yangi O‘zbekiston Taraqqiyot strategiyasi” moliyaviy savodxonlikni ustuvor yo‘nalish sifatida belgiladi. 2021-2026-yillarga mo‘ljallangan “Moliyaviy xizmatlar ommaboyligi milliy strategiyasi” fuqarolarning moliyaviy xizmatlardan foydalanish qobiliyatini oshirishni maqsad qilib qo‘ydi. CERT-CBU kiberxavfsizlik markazi banklar va to‘lov muassasalaridan firibgarlikka qarshi avtomatlashtirilgan tizimlarni joriy etishni, 24/7 rejimida faoliyat yuritishni va shubhali operatsiyalar reyestrini muntazam yuritishni majburiy ravishda talab qiladi. Markaz 2024-yil oktabr oyida OIC-CERT (31 davlatdan 65 tashkilot) a’zoligiga kirdi va Anti-Phishing Working Group (APWG) bilan hamkorlik o‘rnatdi - bu xalqaro tahdid ma’lumotlari bazasidan foydalanish imkonini beradi.

*Muammoli holat.* Biroq siyosiy muhitda muhim zaifliklar ham mavjud. O‘zbekiston qonunchiligi raqamli firibgarlikning yangi shakllarini - deepfake texnologiyasi asosida soxta qo‘ng‘iroq qilish, sun’iy intellekt yordamida tuzilgan fishing xabarlari, kripto-valyuta aldov sxemalari - to‘liq qamrab olmaydi. Yevropa Ittifoqida PSD2 direktivasi kuchli foydalanuvchi autentifikatsiyasini (Strong Customer Authentication, SCA) majburiy qilgan, biroq O‘zbekistonda bunday qonuniy talab hali joriy etilmagan. Bundan tashqari, mamlakat bo‘yicha firibgarlik holatlari to‘g‘risida ochiq, umumlashtiruvchi statistika mavjud emas - bu muammoning haqiqiy ko‘lamini baholashni qiyinlashtiradi.

*Siyosiy omil xulosasi.* Davlat moliyaviy savodxonlik siyosati mavjud va faol rivojlantirilayapti. Biroq raqamli firibgarlikning yangi avlodi qonunchilikdan tez ilgarilamoqda. Xalqaro hamkorlik orqali olinayotgan tahdid ma’lumotlarini tezroq me’yoriy hujjatlarga kiritish va kuchli autentifikatsiya talabini joriy etish ustuvor vazifa sifatida ko‘rinadi.

*E - Iqtisodiy omillar (Economic)*

Iqtisodiy omillar plastik karta bozorining holati, tranzaksiyalar hajmi, aholi daromadi tarkibi va firibgarlikning iqtisodiy oqibatlarini o‘z ichiga oladi.

*Bozor o‘sishining ikki tomoni.* O‘zbekistonda karta tranzaksiyalari yillik 40 foizdan ortiq sur’atda o‘sib bormoqda. Bu bir tomondan moliyaviy inklyuziyaning kuchayishini anglatsa, ikkinchi tomondan firibgarlar uchun potensial “bozor”ning kengayishini bildiradi. Karta egalarining ko‘payishi, ayniqsa moliyaviy xizmatlardan yangi foydalana boshlagan fuqarolar orasida, tajribasizlik va xavfsizlik odatlarining yo‘qligi bilan birga keladi.

*Daromad darajasi va xavf nisbati.* So‘rovnoma natijalariga ko‘ra, oylik daromadi o‘rta darajadagi (3-7 mln so‘m) respondentlar guruhi karta operatsiyalari bo‘yicha eng faol toifa hisoblanadi. Ruiz Yevropa tadqiqotida ham o‘rta daromadli guruh firibgarlik

qurboni bo‘lishning eng yuqori ehtimolini ko‘rsatdi: ular moliyaviy mahsulotlardan faol foydalanadi, biroq ularda to‘laqonli himoya ko‘nikmasi hali shakllanmagan. Kam daromadlilarda karta faoliyati past, yuqori daromadlilarda esa nisbatan kuchliroq moliyaviy savodxonlik mavjud.

*Iqtisodiy zarar va statistika muammosi.* Kaspersky ma’lumotlariga ko‘ra, 2 milliondan ortiq bank kartasi ma’lumotlari zararli dasturlar orqali o‘g‘irlangan - bu bevosita iqtisodiy zarar. O‘zbekistonda esa firibgarlik yo‘qotishlari bo‘yicha ochiq, tartibli milliy statistika mavjud emas. Statistikasiz muammoning ko‘lami baholanmaydi, moliyalashtirish to‘g‘ri yo‘naltirilmaydi va aholi xabardorligi oshirilmaydi. ECB/EBA Yevropa to‘lov tizimlarida firibgarlik hajmi oshib borayotganini qayd etdi - bu tendensiya O‘zbekistonda ham kuzatilayotganligi ehtimol yuqori.

*Iqtisodiy omil xulosasi.* Karta bozorining tez o‘sishi iqtisodiy siyosatdan tezkor javobni talab etadi: firibgarlik yo‘qotishlari bo‘yicha ochiq milliy ma’lumotlar bazasini yo‘lga qo‘yish va o‘rta daromadli foydalanuvchilarni maxsus himoya dasturlarining asosiy maqsad guruhi sifatida belgilash zarur.

*S - Ijtimoiy omillar (Social)*

Ijtimoiy omillar aholining bilim darajasi, xulq-atvori, institutlarga bo‘lgan ishonchi, demografik xususiyatlari va madaniy odatlarini qamrab oladi. Bu bo‘lim so‘rovnoma ma’lumotlari bilan eng to‘g‘ridan-to‘g‘ri bog‘langan.

*Bilim-ishonch paradoksi - asosiy ijtimoiy topilma.* So‘rovnoma natijalari shuni ko‘rsatdiki, respondentlar kiberxavfsizlik bilimi bo‘yicha o‘rtacha 3,76 ball (5 ballik shkalada), ammo bank kompensatsiyasiga ishonch bo‘yicha atigi 1,70 ball ko‘rsatdi. Ikkala ko‘rsatkich o‘rtasidagi +2,06 birlik tafovut - “bilim-ishonch paradoksi” - muhim ijtimoiy hodisa sifatida aniqlandi. Bu shuni anglatadiki, fuqarolar kiberxavfsizlik haqida yetarli bilimga ega, ammo firibgarlik yuz berganda bank ularni himoya qilishiga ishonmaydi. Bunday paradoks ikki salbiy oqibatga olib keladi: birinchidan, firibgarlik holati yuz berganda shikoyat qilinmaydi; ikkinchidan, muammo yashirinib qoladi va statistikada aks etmaydi.

*Bilim va xulq-atvor tafovuti.* Respondentlar kiberxavfsizlik bilimi bo‘yicha 3,76 ball ko‘rsatgan bo‘lsa-da, himoya choralarini kundalik hayotda amalda qo‘llash ko‘rsatkichi 3,21 ballni tashkil etdi - 0,55 birlikka past. Bu klassik “bilim-xulq” bo‘shliqni ko‘rsatadi: odam biladi, lekin qilmaydi. Chowdhury va hamkasblar (2026) tadqiqotida ham moliyaviy bilim va moliyaviy xulq-atvor o‘rtasidagi korrelyatsiya 0,10 dan past ekanligi aniqlandi - ya’ni bilim o‘z-o‘zicha xulq-atvorni o‘zgartirmaydi. Shu sababli ta’lim dasturlari bilim berishdan ko‘ra xulq-atvorni shakllantirishga ko‘proq yo‘naltirilishi kerak.

*Ijtimoiy injeneriya va psixologik zaiflik.* CERT-CBU ma’lumotlariga ko‘ra, ijtimoiy injeneriya O‘zbekistonda moliyaviy firibgarlikning eng keng tarqalgan usuli bo‘lib qolmoqda. Firibgarlar avtoritetga murojaat qilish (“Men Markaziy bank xodimiman”), sun’iy shoshilinchlik yaratish (“Kartangiz bloklanyapti, 5 daqiqada javob bering”) va qo‘rqitish kabi psixologik usullardan foydalanadi. Bunday hujumlar bilimli odamni ham aldashi mumkin, chunki ular kognitiv zaifliklardan foydalanadi -

moliyaviy bilimdan emas. Ruiz tadqiqotida aniqlangandek, ortiqcha o‘z-o‘ziga ishonch (overconfidence) firibgarlik xavfini 29-37 foizga oshiradi.

*Demografik jihat.* So‘rovnomada 18-35 yosh oralig‘idagi respondentlar raqamli ko‘nikmalar bo‘yicha eng yuqori natija ko‘rsatdi. Biroq ular bir vaqtning o‘zida onlayn faoliyati yuqoriligi sababli fishing va ijtimoiy injeneriya hujumlariga ham ko‘proq duchor keladi. Ruizda ham yoshlar (18-29 yosh) firibgarlik qurbonligi bo‘yicha eng yuqori ko‘rsatkichni berdi - raqamli faollik va tajribasizlikning uyg‘unligi natijasida. Keksa yoshdagilar esa past internet faolligi tufayli nisbatan kamroq qurbon bo‘lmoqda.

*Ijtimoiy omil xulosasi.* Ijtimoiy tahlil moliyaviy savodxonlik siyosatini uchta yo‘nalishda qayta ko‘rib chiqish zarurligini ko‘rsatadi: bilimdan xulq-atvorga o‘tish; institutlarga ishonchni alohida muammo sifatida ko‘rib chiqish; yosh guruhlariga qarab moslashtirilgan ta’lim yondashuvi.

*T - Texnologik omillar (Technological)*

Texnologik omillar raqamli infratuzilmaning holati, moliyaviy himoya tizimlari va firibgarlik texnologiyalarining rivojlanishini qamrab oladi.

*Himoya texnologiyalarining rivojlanishi.* Xalqaro miqyosda karta firibgarligiga qarshi kurashda ilg‘or texnologiyalar keng qo‘llanilmoqda. Fetaji va hamkasblar (IEEE Access) tomonidan ishlab chiqilgan FRAUD-X arxitekturasi sun’iy intellekt, blokcheyn va kiberxavfsizlikni birlashtirib, Shimoliy Makedoniya bank sektori ma’lumotlari asosida F1=85,9% aniqlik va nolinchi kun tahdidlari (zero-day threats) uchun 90% recall ko‘rsatkichiga erishdi. Har bir tranzaksiya 15,6 millisekund ichida tahlil qilinadi - bu real vaqt rejimida ishlash talablariga to‘la javob beradi. O‘zbekistonda ham tranzaksion monitoring, anomaliyalarni aniqlash va zudlik bilan ogohlantirishlar yuborish tizimlari joriy etilgan, ammo ularning samaradorligi xalqaro standartlarga nisbatan tekshirilmagan.

*Raqamli infratuzilmaning kengayishi.* Smartfon va internet qamrovining oshishi to‘lov texnologiyalari uchun qulay muhit yaratmoqda. Mobil bank ilovalari foydalanuvchilarga real vaqtda tranzaksiya tasdiqlash, ogohlantirishlar olish va xavfsizlik sozlamalarini boshqarish imkonini beradi. Basar va hamkasblar (2025) 12 mamlakatda o‘tkazilgan tadqiqotda raqamli infratuzilma va moliyaviy savodxonlik uyg‘unligining tejamkorlik xulq-atvoriga ijobiy ta’sirini ko‘rsatdi, biroq bu uyg‘unlik kiberxavfsizlik ongini ham o‘z ichiga olishi zarurligini ta’kidladi.

*Tahdid texnologiyalarining rivojlanishi.* Texnologik muhit bir vaqtning o‘zida muhim tahdidlar ham keltirib chiqarmoqda. Kaspersky ma’lumotlariga ko‘ra, stealer zararli dasturlar 2 milliondan ortiq karta ma’lumotini o‘g‘irladi. Bu dasturlar foydalanuvchi bilimi yoki ehtiyotkoriligidan qat’i nazar ishlaydi va texnik infratuzilma zaifliklaridan foydalanadi. Deepfake texnologiyasi bank xodimi nomidan soxta ovozli qo‘ng‘iroq qilishga imkon berib, ijtimoiy injeneriya hujumlarini yangi darajaga ko‘tardi. Fishing saytlar ham tobora ishonchli ko‘rinishga ega bo‘lmoqda: hatto tajribali foydalanuvchilar ham ularni haqiqiy bank saytidan ajrata olmaydi.

Texnologiya ikki tomonlama ta’sir ko‘rsatadi: himoya va tahdid texnologiyalari bir xil tezlikda rivojlanmoqda. Himoya tizimlari doimiy yangilanib borishi va foydalanuvchi ta’limi texnologik rivojlanish bilan parallel olib borilishi zarur.

Yuqoridagi to‘rtta yo‘nalish bo‘yicha o‘tkazilgan tahlilni umumlashtirish uchun quyida yaxlit PEST matritsa taqdim etiladi. Har bir omil bo‘yicha ijobiy holatlar va muammolar bir joyda ko‘rsatilgan.

**2-jadval**

**PEST matritsa: O‘zbekistonda moliyaviy savodxonlik va kiber-firibgarlikdan himoyalanish[1]**

| Omil | | Ijobiy holatlar va imkoniyatlar | Muammolar va tahdidlar |
|---|---|---|---|
| P | **SIYOSIY omillar** | - Yangi O‘zbekiston strategiyasida moliyaviy savodxonlik ustuvor yo‘nalish (2022)<br>- Moliyaviy xizmatlar ommaviyligi milliy strategiyasi (2021-2026)<br>- CERT-CBU tomonidan banklarga majburiy fraud-nazorat talablari<br>- OIC-CERT va APWG a’zoligi - xalqaro tahdid ma’lumotlari bazasi | - Raqamli firibgarlikning yangi shakllari (deepfake, kripto) qonunchilikda qamrab olinmagan<br>- Kuchli autentifikatsiya (SCA) talabi hali joriy etilmagan<br>- Firibgarlik holatlari bo‘yicha ochiq milliy statistika mavjud emas<br>- Me’yoriy yangilanish texnologiya rivojidan orqada qolmoqda |
| E | **IQTISODIY omillar** | - Karta tranzaksiyalari hajmi yillik 40%+ o‘sishi - moliyaviy inklyuziya kengaymoqda<br>- Maosh, nafaqa, stipendiyalarni kartaga o‘tkazish - foydalanuvchilar bazasi kengaymoqda<br>- Moliyaviy savodxonlik dasturlariga davlat e’tiborining oshib borayotganligi | - Firibgarlik yo‘qotishlari statistikasi yo‘q - muammoning ko‘lami noma’lum<br>- O‘rta daromadli guruh eng xavfli toifa: faol foydalanadi, ammo tajribasiz<br>- Kaspersky: 2 mln+ karta ma’lumoti o‘g‘irlangan - bevosita iqtisodiy zarar<br>- Kichik yo‘qotishlar e’tibordan chetda qoladi va yig‘ilib katta zarar beradi |
| S | **IJTIMOIY omillar** | - Kiberxavfsizlik bilimi qoniqarli (M=3,76/5,0)<br>- Yoshlar raqamli ko‘nikmalar bo‘yicha yuqori daraja ko‘rsatdi<br>- Respondentlarning 62%+ i 3 yildan ortiq karta tajribasiga ega<br>- Foydalanuvchilar o‘zlarini himoya qilmoqchi - himoyalanish istagi yuqori | - BILIM-ISHONCH PARADOKSI: bilim 3,76 - ishonch 1,70 - tafovut +2,06<br>- Bilim-xulq bo‘shliq: biladi (3,76) lekin qilmaydi (3,21) - 0,55 birlik farq<br>- Ijtimoiy injeneriya: psixologik manipulyatsiya bilimli odamni ham aldashi mumkin<br>- Ortiqcha o‘ziga ishonch - firibgarlik xavfini 29-37% oshiradi (Ruiz)<br>- Yoshlar eng raqamli faol - shu bilan birga eng ko‘p hujumga uchraydigan guruh |
| T | **TEXNOLOGIK omillar** | - Tranzaksion monitoring va anomaliyalarni aniqlash tizimlari mavjud<br>- Biometrik autentifikatsiya va ko‘p bosqichli tasdiqlash kengayib bormoqda<br>- FRAUD-X (Fetaji): AI+blokcheyn+kiberxavfsizlik - F1=85,9%, 15,6ms<br>- Smartfon va internet qamrovi kengayishi - ta’lim yetkazishni osonlashtiradi | - Stealer zararli dasturlar foydalanuvchi bilimidan qat’i nazar ishlaydi<br>- Deepfake texnologiyasi: soxta bank xodimi ovozi bilan qo‘ng‘iroq imkoni<br>- Fishing saytlar tobora ishonchli ko‘rinishga ega bo‘lmoqda<br>- Texnologik tahdidlar tezligi himoya tizimlaridan ustun chiqmoqda |

[1] Manba: muallif tahlili, 2026-yilgi so‘rovnoma, Bobojanov (2024), Fetaji va b. (2025), Kaspersky (2025), ECB/EBA (2024) asosida.

PEST tahlili siyosiy va iqtisodiy omillar o‘rtasida muhim bog‘liqlikni ko‘rsatdi. Karta bozorining jadal iqtisodiy o‘sishi bir tomondan moliyaviy inklyuziyani kuchaytirmoqda, ammo ikkinchi tomondan firibgarlik xavfi muhitini ham kengaytirmoqda. Iqtisodiy o‘sish siyosiy javob - yangi tartibga soluvchi hujjatlar, nazorat mexanizmlari, ochiq statistika tizimi - bilan uyg‘unlikda bo‘lishini talab etadi. Hozirgi holatda iqtisodiy o‘sish tezligi siyosiy reaksiyadan ancha yuqori.

Iqtisodiy jihatdan eng muhim muammo - firibgarlik yo‘qotishlarining ko‘rinmasligi. Statistika bo‘lmasa muammo ko‘lami baholanmaydi, moliyalashtirish to‘g‘ri yo‘naltirilmaydi, jamiyat xabardorligi oshirilmaydi. Yevropa tajribasida (ECB/EBA =) to‘lov tizimlari firibgarligi bo‘yicha yillik batafsil hisobotlar chiqarish odatiy amaliyotga aylangan. O‘zbekiston uchun shunday milliy hisobot tizimini yo‘lga qo‘yish ustuvor vazifadir.

PEST matritsasining ijtimoiy bo‘limidagi eng muhim topilma - bilim-ishonch paradoksi - faqat statistik ko‘rsatkich emas, balki moliyaviy ta’lim siyosatining asosiy muammosini ochib beruvchi hodisadir. Foydalanuvchi bilimli (3,76/5,0), biroq bank tizimi uni himoya qilishiga ishonmaydi (1,70/5,0). Bu ikki tomonlama muammo: birinchisi - banklar kompensatsiya mexanizmlari amalda qanchalik samarali ishlayotganligi; ikkinchisi - bu samaradorlik aholi tomonidan qanchalik his etilmoqda.

Chowdhury va hamkasblar Bangladesh tadqiqotida ham xuddi shunday xulosa chiqardi: institutsional ishonch (muhimlik=0,18) ta’lim darajasidan (0,09) kuchliroq prediktor. Demak, moliyaviy ta’lim dasturlari faqat bilim berishga qaratilsa, bilim-ishonch paradoksini bartaraf eta olmaydi. Banklar kompensatsiya mexanizmlarining shaffofligi va amaliy samaradorligi parallel tarzda mustahkamlanishi kerak.

Texnologik tahlil eng aniq ziddiyatni ko‘rsatdi: bir xil texnologik taraqqiyot ham himoya imkoniyati, ham yangi tahdid. Tranzaksion monitoring, biometrik autentifikatsiya va ko‘p qatlamli himoya tizimlari karta foydalanuvchilarini samarali himoya qilishi mumkin. Biroq ayni vaqtda stealer dasturlar va deepfake texnologiyasi firibgarlar arsenalini kengaytirib bormoqda. Fetaji va hamkasblar FRAUD-X arxitekturasida ko‘rsatgandek, bu raqobatda faqat ko‘p qatlamli, birlashtirilgan texnik yondashuv yetarlicha samarali bo‘lishi mumkin.

PEST tahlili natijalari asosida to‘rtta tomonga - davlat organlari, banklar, ta’lim muassasalari va kelajakdagi tadqiqotlar uchun - alohida tavsiyalar ishlab chiqildi.

**3-jadval**

**PEST omillariga asoslangan amaliy tavsiyalar**[1]

| PEST omili | Asosiy muammo | Tavsiyalar |
|---|---|---|
| P - Siyosiy | Qonunchilik raqamli firibgarlikning yangi shakllarini qamrab olmaydi | OIC-CERT va APWG ma’lumotlari asosida qonunchilikni yiliga kamida bir marta yangilash mexanizmini joriy etish; kuchli foydalanuvchi autentifikatsiyasi (SCA) talabini belgilash; firibgarlik statistikasi uchun ochiq milliy platforma yaratish va yillik hisobot chiqarish |
| E - Iqtisodiy | Firibgarlik ko‘lami noma’lum; o‘rta | Milliy firibgarlik ma’lumotlar bazasini va yillik ochiq hisobot tizimini yo‘lga qo‘yish; moliyaviy savodxonlik dasturlarida o‘rta daromadli karta egalarini asosiy maqsad |

[1] Manba: muallif tahlili asosida.

| PEST omili | Asosiy muammo | Tavsiyalar |
|---|---|---|
| | daromadli guruh eng xavfli | guruh sifatida belgilash va ularga maxsus yo‘naltirilgan ta’lim berish |
| S - Ijtimoiy | Bilim-ishonch paradoksi; bilim-xulq tafovuti; ijtimoiy injeneriya | Banklar kompensatsiya mexanizmlarini shaffoflashtirishi va soddalashtirilgan shikoyat tizimini joriy etishi; ta’lim dasturlarini bilim uzatishdan xulq-atvorni shakllantirish simulyatsiyalari, mashqlar orqali qayta yo‘naltirish; psixologik manipulyatsiya usullarini tanib olish bo‘yicha maxsus modul yaratish |
| T - Texnologik | Stealer dasturlar va deepfake; himoya va tahdid texnologiyalari poyga holatida | FRAUD-X tipidagi ko‘p qatlamli texnik himoya (AI, blokcheyn va kiberxavfsizlik) ni banklar uchun pilot loyiha sifatida joriy etish; biometrik va ko‘p bosqichli autentifikatsiyani kuchaytirish; foydalanuvchilarga yangi tahdidlar haqida tezkor ogohlantirish tizimini yo‘lga qo‘yish |

## XULOSA VATAKLIFLAR

Ushbu maqolada O‘zbekiston plastik karta foydalanuvchilarining moliyaviy savodxonlik darajasi va kiber-firibgarlikdan himoyalanish holati PEST tahlili orqali ko‘rib chiqildi. Tadqiqot to‘rtta mustaqil xulosaga keldi.

Birinchi xulosa - siyosiy jihat. O‘zbekistonda moliyaviy savodxonlikka oid me’yoriy baza mavjud va rivojlantirilmoqda - milliy strategiyalar, CERT-CBU faoliyati va xalqaro hamkorlik buning dalili. Biroq raqamli firibgarlikning yangi shakllari qonunchilik doirasidan tashqarida qolmoqda. Regulyativ yangilanish tezligi texnologik rivojlanish tezligiga mos kelishi uchun doimiy mexanizm zarur.

Ikkinchi xulosa - iqtisodiy jihat. Karta bozorining jadal o‘sishi moliyaviy inklyuziyani kuchaytirmoqda, ammo firibgarlik xavfi muhitini ham kengaytirmoqda. Firibgarlik yo‘qotishlari bo‘yicha ochiq milliy statistikaning yo‘qligi muammo ko‘lamini yashirib, samarali siyosat ishlab chiqishni qiyinlashtirmoqda. O‘rta daromadli foydalanuvchilar guruhining yuqori zaifligiga alohida e’tibor berish zarur.

Uchinchi xulosa - ijtimoiy jihat. “Bilim-ishonch paradoksi” (kiberxavfsizlik bilimi M=3,76, bank kompensatsiyasiga ishonch M=1,70, GAP=+2,06) tadqiqotning markaziy topilmasi hisoblanadi. Bu paradoks moliyaviy ta’lim siyosati bilim berishdan tashqari institutlarga ishonchni mustahkamlashni ham maqsad qilib olishi kerakligini ko‘rsatadi. Bundan tashqari, bilim va xulq-atvor o‘rtasidagi 0,55 birlik tafovut ta’lim dasturlarini amaliy simulyatsiyalarga yo‘naltirish zarurligini anglatadi.

To‘rtinchi xulosa - texnologik jihat. Texnologiya ikki tomonlama ta’sir ko‘rsatadi. Bir tomondan, zamonaviy tranzaksion monitoring, biometrik autentifikatsiya va ko‘p qatlamli himoya tizimlari karta xavfsizligini oshirishda muhim vosita. Ikkinchi tomondan, stealer dasturlar va deepfake texnologiyasi yangi tahdid avlodini keltirib chiqarmoqda. Texnologik poyga sharoitida texnik himoya va foydalanuvchi ta’limining parallel rivojlanishi strategik zaruriyatdir.

Kelgusi tadqiqotlar uchun ustuvor yo‘nalishlar quyidagilardan iborat: viloyatlar va qishloq hududlarini qamrab oluvchi kengaytirilgan so‘rovnoma o‘tkazish; bilim-ishonch paradoksining vaqt o‘tishi bilan qanday o‘zgarishini longitudinal kuzatish;

banklar kompensatsiya mexanizmlari shaffofligi va aholining unga bo‘lgan ishonchi o‘rtasidagi munosabatni alohida o‘rganish.

## FOYDALANILGAN ADABIYOTLAR RO‘YXATI

1. Basar, D., Keskin, H., Esen, E., Merter, A. K., & Balcioglu, Y. S. (2025). Digital financial literacy and savings behavior: A comprehensive cross-country analysis of FinTech adoption patterns and economic outcomes across 12 nations. Borsa Istanbul Review, 25(1), 59-72. https://doi.org/10.1016/j.bir.2025.09.004

2. Bobojanov, M. (2024). O‘zbekiston Respublikasi Markaziy banki banklar va to‘lov tizimlarida firibgarlikning oldini olishni qanday tartibga soladi. CERT-CBU Kiberxavfsizlik markazi ma’ruzasi. Toshkent.

3. Chowdhury, T. A., Chowdhury, M. A. H., Rahman, M. T., Ahmed, I., Ahmed, N., Tuhin, M. A. I., & Kafy, A. A. (2026). Modeling financial literacy through explainable machine learning and behavioral segmentation in emerging economies. Computers in Human Behavior Reports, 21, 100926. https://doi.org/10.1016/j.chbr.2025.100926

4. European Central Bank & European Banking Authority. (2024). 2024 Report on payment fraud. Frankfurt: ECB/EBA. https://www.ecb.europa.eu

5. Ferilli, G. B., Palmieri, E., Miani, S., & Stefanelli, V. (2024). The role of digital financial literacy in banking strategies and financial inclusion. Research in International Business and Finance, 69, 102218. https://doi.org/10.1016/j.ribaf.2024.102218

6. Fetaji, B., Fetaji, M., Hasan, A., Rexhepi, S., & Armenski, G. (2025). FRAUD-X: An integrated AI, blockchain, and cybersecurity framework with early warning systems for mitigating online financial fraud. IEEE Access, 13, 48068-48083. https://doi.org/10.1109/ACCESS.2025.3547285

7. Isaia, E., Oggero, N., & Sandretto, D. (2024). Is financial literacy a protection tool from online fraud in the digital era? Journal of Behavioral and Experimental Finance, 44, 100977. https://doi.org/10.1016/j.jbef.2024.100977

8. Kaspersky. (2025). Stealer malware leaked over 2 million bank cards. https://www.kaspersky.com/about/press-releases

9. Kieffer, C. N., & Mottola, G. R. (2017). Understanding and combating investment fraud. In O. S. Mitchell, P. B. Hammond & S. P. Utkus (Eds.), Financial decision making and retirement security in an aging world. Oxford University Press.

10. Li, J., Wei, X., & Zhao, H. (2024). Digital literacy and fraud vulnerability: Evidence from rural China. China Economic Review, 85, 102156.

11. Lusardi, A., & Mitchell, O. S. (2014). The economic importance of financial literacy: Theory and evidence. Journal of Economic Literature, 52(1), 5-44. https://doi.org/10.1257/jel.52.1.5

12. Nasdaq. (2024). Global Financial Crime Report 2024. Nasdaq Verafin.

13. OECD. (2021). G20/OECD INFE report on ensuring financial education and consumer protection for all in the digital age. Paris: OECD Publishing.

14. Ruiz, J. R. (2026). Who gets scammed? The roles of financial literacy, digital financial security, and overconfidence in Europe. International Review of Economics and Finance, 106, 104913. https://doi.org/10.1016/j.iref.2026.104913

15. Soriyev, S., & Tuychiyeva, N. (2022). Aholining moliyaviy savodxonligini oshirish va hududlarni iqtisodiy rivojlantirish omili. STARS International University Conference Proceedings, 5, 435-438.

16. Vahobov, A. V., & Dusmuhamedov, O. S. (2022). Moliyaviy savodxonlik tushunchasining nazariy asoslarini takomillashtirish. Iqtisod va moliya, 5(153), 21-

# Marketing

*ilmiy, amaliy va ommabop jurnali*





**2026-yil, may, 5-son**




Mazkur jurnalda maqolalar chop etish uchun quyidagi havolalarga murojaat qilish mumkin.
Ilmiy maqola, ommabop maqola, reklama, hikoya va boshqa ilmiy-ijodiy materiallar yuborishingiz mumkin.
Materiallar va reklamalar pullik asosda chop etiladi.


Elektron pochta: info@marketingjournal.uz
Bot: @marketinjournalbot
Tel.: +998977838464, +998939266610
Jurnalning rasmiy sayti: https://marketingjournal.uz



Marketing jurnali O‘zbekiston Respublikasi Oliy ta’lim, fan va innovatsiyalar vazirligi huzuridagi **Oliy attestatsiya komissiyasi rayosatining 2024-yil 04-oktabrdagi 332/5 sonli qarori** bilan milliy ilmiy nashrlar ro‘yxatiga kiritilgan

**“Marketing” ilmiy, amaliy va ommabop jurnali** 2024-yil 15-martdan O‘zbekiston Respublikasi Prezidenti Administratsiyasi huzuridagi Axborot va ommaviy kommunikatsiyalar agentligi tomonidan **C-5669517** reyestr raqami tartibi bo‘yicha ro‘yxatdan o‘tkazilgan. **Litsenziya raqami: №240874**

“Marketing” ilmiy, amaliy va ommabop jurnalining xalqaro darajasi: **9710.** ГОСТ 7.56-2002 " Seriyali nashrlarning xalqaro standart raqamlanishi" davlatlataro standartlari talablari. **Berilgan ISSN tartib raqami: 3060-4621**