MOLIYAVIY TEXNOLOGIYALARDA XAVFSIZLIK MASALALARI: RAQAMLI TO‘LOVLAR EKOTIZIMIDA RISKLAR, BOSHQARUV VA HIMOYA ARXITEKTURASI

Toshkent davlat iqtisodiyot universiteti

To‘rtko‘l fakulteti Soliq va soliqqa tortish

Yo‘nalishi 3-kurs bakalavriyat talabasi

Muhammadto‘xtasinov Ismoiljon Umidjon o‘g‘li

Toshkent davlat iqtisodiyot universiteti

To‘rtko‘l fakulteti Soliq va soliqqa tortish

Yo‘nalishi 3-kurs bakalavriyat talabasi

Ilxombekov Asadbek Baxtiyor o‘g‘li

Annotatsiya: Ushbu maqola moliyaviy texnologiyalar ekotizimida xavfsizlik muammolarini riskga yo‘naltirilgan yondashuv asosida tahlil qiladi. Tadqiqotda adabiyotlar sharhi, konseptual modellashtirish va qiyosiy tahlil metodlari qo‘llanildi. Natijalar tahdidlar zanjiri, zaifliklar manbalari hamda boshqaruv nazoratlari uyg‘unligini ko‘rsatadi. Ilmiy hissa sifatida fintech uchun ko‘p qatlamli himoya arxitekturasi asoslari tizimlashtirildi.

Kalit so‘zlar: Moliyaviy texnologiyalar, kiberxavfsizlik, raqamli to‘lovlar, identifikatsiya va autentifikatsiya, ma’lumotlar himoyasi, firibgarlik, risklarni boshqarish

Moliyaviy texnologiyalar so‘nggi o‘n yillikda bank xizmatlari, to‘lov tizimlari, mikromoliyalashtirish va investitsiya platformalarining mantiqiy arxitekturasini tubdan o‘zgartirib, mijoz tajribasini tezlik va qulaylik mezonlari bo‘yicha yangi bosqichga olib chiqdi. Biroq texnologik soddalashuv va masofaviy kanallarning kengayishi xavfsizlikning an’anaviy chegaralarini yemirib, ishonch kategoriyasini raqamli identifikatsiya, ma’lumotlar oqimi va uchinchi tomon integratsiyalarining barqarorligi bilan bevosita

bog‘ladi. Fintech ekotizimida qiymat yaratish mexanizmi ko‘pincha API asosidagi xizmatlar, bulut infratuzilmasi, mobil ilovalar, tezkor scoring, biometrik tekshiruvlar hamda real vaqt rejimidagi tranzaksiyalarni qayta ishlashga tayanadi; aynan shu elementlar hujumchilar uchun ko‘p vektorli imkoniyatlar eshigini ochadi. Shuning uchun moliyaviy texnologiyalarda xavfsizlik masalasi faqat texnik himoya choralariga emas, balki risklarni boshqarish, boshqaruv nazorati, muvofiqlik talablari, hamkorlar zanjiri va foydalanuvchi xulqi kabi omillarga tayangan kompleks ilmiy muammo sifatida ko‘rilishi lozim.

Ilmiy adabiyotlarda fintech xavfsizligi ko‘pincha alohida yo‘nalishlar bo‘yicha yoritiladi: kriptografik mexanizmlar, ma’lumotlarni himoyalash, firibgarlikni aniqlash, identifikatsiya va autentifikatsiya yoki regulyativ talablar doirasida. Biroq amaliyot shuni ko‘rsatadiki, real hodisalar aksariyat hollarda biror bitta zaiflik natijasi emas, balki biznes jarayonidagi noto‘g‘ri sozlama, integratsiya xatosi, inson omili va monitoring yetishmasligi kabi bir nechta bo‘g‘inlar ketma-ketligidan kelib chiqadi. Demak, mavjud tadqiqotlarda ko‘p uchraydigan bo‘shliq shundaki, fintech ekotizimida tahdidlarning zanjirli tabiati, aktivlar hayotiy sikli va boshqaruv nazoratlarining o‘zaro mosligi yagona tizimli model sifatida yetarlicha integratsiyalanmaydi. Xususan, tez o‘sayotgan startaplar muhitida “tez bozorga chiqish” strategiyasi xavfsizlik dizaynini keyinga surishi, natijada texnik qarzning xavfsizlik qarziga aylanishi haqida yetarli analitik xulosalar doim ham taqdim etilmaydi.

Ushbu maqolaning maqsadi moliyaviy texnologiyalar ekotizimida xavfsizlik muammolarini riskga yo‘naltirilgan yondashuv asosida tizimlashtirish, tahdidlar va zaifliklar manbalarini funksional qatlamlar kesimida ochib berish hamda ko‘p qatlamli himoya arxitekturasi uchun konseptual tamoyillarni asoslashdan iborat. Maqsadga erishish uchun quyidagi vazifalar qo‘yildi: birinchidan, fintechda asosiy aktivlar va hujum sirtini tahlil qilish; ikkinchidan, hujum ssenariylarini zanjirli mantiqda guruhlash va ularning ildiz omillarini aniqlash; uchinchidan, boshqaruv va texnik nazoratlarning uyg‘un modelini taklif etish; to‘rtinchidan, natijalarni xalqaro va mintaqaviy ilmiy yondashuvlar bilan qiyosiy muhokama qilish. Tadqiqotning ilmiy yangiligi fintech xavfsizligini “texnik

vositalar majmui” emas, balki “ekotizim risklari va nazoratlar arxitekturasi” sifatida bir butun konsepsiyada birlashtirishga urinish bilan izohlanadi.

Tadqiqot metodologiyasi ko‘p manbali nazariy-analitik yondashuvga asoslanadi. Birinchi bosqichda xalqaro standartlar va ilmiy manbalar asosida fintech xavfsizligining konseptual chegaralari aniqlashtirildi; bunda axborot xavfsizligi boshqaruvi, kiberxatarlarni baholash va raqamli ishonch infratuzilmasi haqidagi yondashuvlar umumlashtirildi [1; 2]. Ikkinchi bosqichda konseptual modellashtirish qo‘llanilib, fintech platformasining tipik arxitekturasi funksional qatlamlarga ajratildi: mijoz interfeysi va mobil kanal, identifikatsiya-autentifikatsiya, tranzaksiyalarni qayta ishlash, ma’lumotlar saqlash va tahlil, uchinchi tomon integratsiyalari hamda monitoring va javob qaytarish konturi. Ushbu qatlamlash hujum sirtini tizimli ko‘rish va nazoratlarning qaysi nuqtada uzilishi xavfni kuchaytirishini izohlash uchun tanlandi.

Uchinchi bosqich qiyosiy tahlilga bag‘ishlandi. Qiyosiy tahlilda bank sektori uchun shakllangan klassik xavfsizlik amaliyotlari bilan fintechning tez iterativ rivojlanish modeli taqqoslandi; bu taqqoslash xavfsizlikning “dizayn orqali” va “so‘ngdan qo‘shiladigan” yondashuvlari o‘rtasidagi farqlarni ochib berdi [3]. To‘rtinchi bosqichda sifatli tahlil usuli orqali ommaviy manbalarda qayd etilgan tipik hodisalar sinflari, xususan phishing va ijtimoiy muhandislik, hisob egallash, API suiiste’moli, ma’lumot sizishi, ichki xodimlar xavfi va uchinchi tomon provayderlari xatarlari bo‘yicha umumiy hujum zanjirlari rekonstruksiya qilindi. Bu yerda maqsad statistik umumlashtirish emas, balki sabab-oqibat bog‘lanishlarini nazariy asosda tartiblashdir. Nihoyat, normativ va tashkiliy nazoratlar tahlilida axborot xavfsizligi boshqaruvi bo‘yicha standartlashgan talablar hamda risklarni boshqarish konsepsiyalari tayanch sifatida olindi [1; 4]. Mazkur metodlar tanlovi maqola maqsadiga mos, chunki fintech xavfsizligida texnik va tashkiliy omillar bir-biridan ajralmagan, ularni kompleks ko‘rish esa faqat integrativ metodologiya bilan ta’minlanadi.

Tadqiqot natijalari fintech ekotizimida xavfsizlik muammolari uch darajali bog‘liqlikda namoyon bo‘lishini ko‘rsatdi: aktivlar va qiymat oqimi darajasi, texnologik arxitektura darajasi hamda boshqaruv va hamkorlar zanjiri darajasi. Aktivlar darajasida

asosiy himoya obyekti sifatida nafaqat mijoz mablag‘lari, balki tranzaksiya yaxlitligi, identifikatsiya atributlari, scoring modellari, shaxsiy ma’lumotlar va reputatsion kapital ham ko‘tariladi. Fintech biznes modeli ko‘pincha ma’lumotlar va tezkor qaror qabul qilishga tayanishi sababli, ma’lumotlarning maxfiyligi buzilishi bilan bir qatorda ularning yaxlitligi buzilishi ham iqtisodiy zarar mexanizmini keskin tezlashtiradi; masalan, scoring signallari manipulyatsiyasi kredit portfeli sifatini sekin emas, balki eksponentsial yomonlashtirishi mumkin.

Arxitektura darajasida hujum sirtining kengayishi uchta ustun omil bilan izohlandi. Birinchi omil mobil kanalning ustunligi bo‘lib, u qurilma xavfsizligi, ilova yangilanishlari, root yoki jailbreak holatlari va zararli dasturlar bilan bog‘liq risklarni kuchaytiradi. Ikkinchi omil API iqtisodiyoti bo‘lib, ochiq interfeyslar va hamkor servislar integratsiyasi autentifikatsiya, avtorizatsiya va tezlik cheklovlari noto‘g‘ri sozlanganda ekspluatatsiya uchun qulay sharoit yaratadi. Uchinchi omil bulut infratuzilmasi va mikroxizmatlar bo‘lib, konfiguratsiya boshqaruvi, maxfiy kalitlar aylanishi va loglash intizomi sust bo‘lsa, “ko‘rinmas” zaifliklar to‘planib boradi. Natijalarga ko‘ra, fintechdagi ko‘plab hodisalarning ildizi kriptografiya “kuchsizligi”dan ko‘ra ko‘proq identifikatsiya jarayonining bo‘shligi, sessiya boshqaruvi xatolari, ruxsatlar matritsasining murakkablashuvi va monitoringning fragmentatsiyasiga borib taqaladi.

Hujum ssenariylarining zanjirli modeli quyidagi tipik ketma-ketlikni ko‘rsatdi. Birinchi bo‘g‘in sifatida ijtimoiy muhandislik yoki credential stuffing orqali dastlabki kirish olinadi; ikkinchi bo‘g‘inda qurilma yoki sessiya darajasida tokenlar qo‘lga kiritiladi; uchinchi bo‘g‘inda tranzaksiya yo‘naltiriladi yoki hisobdan chiqarishlar maskirovka qilinadi; to‘rtinchi bo‘g‘inda esa izlarni yashirish uchun loglar bo‘yicha ko‘rinishni pasaytiruvchi harakatlar amalga oshiriladi. Bu zanjirda eng ko‘p uziladigan nazoratlar sifatida kuchli mijoz autentifikatsiyasi, riskga asoslangan tranzaksiya monitoringi va hodisalarga javob qaytarishning vaqt bo‘yicha kechikishi ajralib chiqdi. Ayniqsa real vaqt to‘lovlarida “tasdiqlash oynasi” qisqargani sababli, klassik antifraud qoidalari yetarli

bo‘lmay qolishi va xulq-atvor analitikasi hamda kontekstual signallar zarurligi aniqlashtirildi.

Boshqaruv darajasida muammolar uch guruhga jamlandi. Birinchi guruh tez rivojlanish sharoitida xavfsizlik talablarining mahsulot dizayniga kech integratsiyalanishi bilan bog‘liq bo‘lib, bu kod sifati, test qamrovi va xavfsiz konfiguratsiya intizomiga salbiy ta’sir qiladi. Ikkinchi guruh uchinchi tomon risklari bo‘lib, identifikatsiya provayderlari, bulut servislar, to‘lov shlyuzlari va analitik SDKlar orqali ma’lumot oqimlari ko‘payadi; bu oqimlar ustidan nazorat yetarli bo‘lmasa, tashkilotning xavfsizlik chegarasi amalda hamkorlar zanjiri bo‘ylab yoyilib ketadi. Uchinchi guruh inson omili va operatsion intizomga taalluqli bo‘lib, kirish huquqlarini minimallashtirish, maxfiy kalitlar bilan ishlash, o‘zgartirishlarni tasdiqlash va audit izlari muammolari ko‘p uchraydi. Natija sifatida fintech xavfsizligini ta’minlash uchun ko‘p qatlamli himoya arxitekturasi tamoyillari shakllantirildi: identifikatsiya va kirish boshqaruvi markazlashtirilgan bo‘lishi, ma’lumotlar hayotiy sikli bo‘yicha klassifikatsiya joriy etilishi, API va integratsiyalar uchun nol ishonchga yaqin yondashuv qo‘llanishi, monitoring esa biznes tranzaksiyalari semantikasini tushunadigan darajada qurilishi lozim.

Olingan natijalar fintech xavfsizligining markazida “ishonch”ni texnik komponent sifatida emas, balki boshqaruv, arxitektura va operatsion jarayonlar yig‘indisi sifatida ko‘rish zarurligini ko‘rsatadi. Axborot xavfsizligi boshqaruvi bo‘yicha xalqaro yondashuvlar xavfsizlikni doimiy takomillashtirish sikli sifatida belgilaydi va risklarni tizimli boshqarish talabini ilgari suradi [1]. Ushbu maqoladagi ko‘p qatlamli arxitektura tamoyillari aynan shu boshqaruv mantiqini fintechning tezkor iteratsiyalariga moslashtirishni ko‘zlaydi; ya’ni nazoratlar faqat tekshiruv nuqtalarida emas, balki dasturiy ta’minot yetkazib berish zanjirida ham uzluksiz ishlashi kerak.

Kiberxavfsizlikning asosiy risklari haqidagi ilmiy yondashuvlar tahdidlarning texnik evolyutsiyasi bilan bir qatorda iqtisodiy motivatsiya va tashkilot ichki jarayonlarini ham tahlil qiladi [2]. Natijalarimizdagi “zanjirli hujum” modeli shu nuqtai nazarni kuchaytiradi: hujumchi ko‘pincha bitta himoya devorini buzmaydi, balki bir nechta mayda bo‘shliqlarni

ketma-ket ulab, yakuniy zararli natijaga erishadi. Bu esa fintechda nazoratlarni alohida-alohida “chek-list” sifatida joriy qilish samarasizligini, ularni o‘zaro bog‘liq ekotizim sifatida dizaynlash zarurligini anglatadi.

To‘lov tizimlari va elektron to‘lovlar bo‘yicha rus tilidagi ilmiy-analitik manbalarda raqamli to‘lov muhitida ishonchlilik va xavfsizlikning muhim sharti sifatida identifikatsiya, protsessing barqarorligi hamda firibgarlikka qarshi mexanizmlarning institutsional uyg‘unligi ta’kidlanadi [3]. Bizning tahlilimiz bu fikrni fintech sharoitida kengaytiradi: protsessingning barqarorligi endi faqat markaziy tizim bilan cheklanmay, API asosidagi hamkorlar zanjiri, mobil qurilma muhiti va bulut konfiguratsiyalariga ham bog‘liq. Shu bois “institutsional uyg‘unlik” tushunchasi fintechda vendor va provayderlar bilan shartnomaviy boshqaruv, xizmat darajasi kelishuvlari, audit huquqi va hodisalarni birgalikda boshqarish protokollarini ham o‘z ichiga olishi kerak.

Risklarni boshqarish bo‘yicha klassik konsepsiyalar moliyaviy sohaga xos bo‘lgan operatsion risklar va axborot xavfsizligi risklari o‘rtasidagi uzviy aloqani ko‘rsatadi [4]. Tadqiqot natijalari ham shuni tasdiqlaydiki, fintechda kiberhodisa ko‘pincha operatsion uzilish, mijozlarga xizmat ko‘rsatishdagi pasayish va regulyativ jarimalar bilan bir vaqtda yuzaga keladi. Demak, xavfsizlikni alohida IT funksiyasi doirasida emas, balki korporativ risklar portfeli doirasida boshqarish metodik jihatdan to‘g‘riroq bo‘ladi. Bu yondashuv boshqaruv organlarining mas’uliyati, risk appetiti va nazoratlar samaradorligini o‘lchash mezonlarini aniqlashtirishni talab qiladi.

Zamonaviy amaliy tadqiqotlar fintech va bank tizimlarida firibgarlikning transformatsiyasini, xususan, masofaviy kanallar orqali hisob egallash va ijtimoiy muhandislikning kuchayishini qayd etadi [5]. Bizning natijalar phishing va credential stuffingning “kirish nuqtasi” sifatidagi rolini asoslab, keyingi bo‘g‘inlarda tokenlar va sessiyalarni boshqarish muhimligini alohida ko‘rsatdi. Bu esa himoyani faqat foydalanuvchiga “ogohlantirish” bilan cheklamasdan, autentifikatsiyani kontekstga bog‘lash, anomaliya aniqlashni kuchaytirish va tranzaksiya darajasida qo‘shimcha tekshiruvlarni dinamik qo‘llash zarurligini anglatadi.

Mintaqaviy ilmiy manbalarda raqamli iqtisodiyot va elektron xizmatlarda axborot xavfsizligi muammolari ko‘tarilar ekan, tashkiliy-texnik choralar bilan bir qatorda kadrlar salohiyati va standartlarga mos boshqaruv masalasi ham urg‘ulanadi [6]. Ushbu maqolada ham inson omili operatsion intizom orqali hujum zanjiriga “ko‘prik” bo‘lib xizmat qilishi ko‘rsatildi. Demak, fintech kompaniyalari uchun xavfsizlik madaniyati, DevSecOps ko‘nikmalari, audit izlari bilan ishlash va hodisalarga javob qaytarish treninglari texnik investitsiyalar bilan teng darajada strategik ahamiyatga ega.

Bulut xavfsizligi va konfiguratsiya boshqaruvi bo‘yicha zamonaviy ilmiy-texnik yondashuvlar noto‘g‘ri sozlamalar va maxfiy ma’lumotlar sizishi hodisalarining asosiy sabablari sifatida identifikatsiya siyosatlari, kalitlar boshqaruvi va kuzatuvchanlik yetishmasligini ajratadi [7]. Bizning arxitektura darajasidagi natijalar bu pozitsiyani fintech kontekstida tasdiqlab, mikroxizmatlar va uchinchi tomon integratsiyalarida kuzatuvchanlik biznes semantikasi bilan bog‘lanmasa, loglar ko‘pligi fonida signal yo‘qolib ketishini ko‘rsatdi. Shu nuqtada ilmiy bahs uchun muhim masala shundan iboratki, fintech monitoringi faqat infratuzilma metrikalariga emas, balki tranzaksiyaning iqtisodiy mantiqiga mos “xavf signalizatsiyasi”ni shakllantirishi kerak.

Maqola moliyaviy texnologiyalarda xavfsizlik masalalarini ekotizim risklari sifatida yoritib, aktivlar, arxitektura va boshqaruv darajalaridagi o‘zaro bog‘liqlikni tizimlashtirdi. Natijalar fintech hodisalari ko‘pincha zanjirli hujum ssenariylari ko‘rinishida kechishini, zaifliklar esa asosan identifikatsiya, integratsiyalar va monitoringdagi uzilishlar bilan kuchayishini ko‘rsatdi. Ilmiy hissa sifatida ko‘p qatlamli himoya arxitekturasi tamoyillari asoslandi va nazoratlar uyg‘unligini ta’minlash zarurligi konseptual jihatdan izohlandi. Amaliy jihatdan, fintech kompaniyalari uchun xavfsizlikni mahsulot dizayniga erta integratsiyalash, uchinchi tomon risklarini shartnomaviy va texnik nazoratlar bilan qamrab olish, tranzaksiya semantikasiga mos monitoring va tezkor javob qaytarish mexanizmlarini rivojlantirish muhimligi kelib chiqadi. Kelgusidagi tadqiqotlar real vaqt antifraud modellarining izohlanishi, maxfiylikni saqlovchi analitika usullari hamda ekotizim

hamkorlari o‘rtasida ishonchni taqsimlangan boshqarish mexanizmlarini baholashga qaratilishi maqsadga muvofiq.

Foydalanilgan adabiyotlar:

1. ISO. ISO/IEC 27001:2022 Information security, cybersecurity and privacy protection. Information security management systems. Requirements. Geneva: International Organization for Standardization, 2022. 34 p.

2. Schneier B. Data and Goliath: The Hidden Battles to Collect Your Data and Control Your World. New York: W. W. Norton and Company, 2015. 448 p.

3. Кузнецов В. А., Михайлов А. Ю. Платежные системы и электронные деньги. Москва: Юрайт, 2019. 354 с.

4. Lam J. Enterprise Risk Management: From Incentives to Controls. 2nd ed. Hoboken: John Wiley and Sons, 2014. 640 p.

5. Anderson R. Security Engineering: A Guide to Building Dependable Distributed Systems. 3rd ed. Hoboken: John Wiley and Sons, 2020. 1248 p.

6. G‘ulomov S. S., Xolmatov A. R. Raqamli iqtisodiyot sharoitida axborot xavfsizligini boshqarish. Toshkent: Iqtisodiyot, 2020. 216 b.

7. Гречишников Е. В. Облачные вычисления: безопасность и управление рисками. Санкт-Петербург: Питер, 2021. 288 с.

8. Karimov A. A., Raxmonov D. D. To‘lov tizimlari va raqamli bank xizmatlarida risklarni boshqarish. Toshkent: Moliya, 2021. 200 b.