TO‘LOV TIZIMLARIDA KIBERREZILIENTLIK VA OMMAVIY ISHONCH: PUL MUOMALASI BARQARORLIGIGA TAHDIDLAR VA BOSHQARUV YECHIMLARI

Xazratkulov O’ktamjon Xikmatullayevich
Guliston davlat universiteti tayanch doktoranti
https://doi.org/10.5281/zenodo.18629183

Annotatsiya. *Raqamli to‘lovlar ekotizimi kengaygani sayin pul muomalasi barqarorligi faqat emissiya, naqd pul massasi yoki inflyatsion kutilmalar bilan cheklanmaydi. Barqarorlikning amaliy o‘lchovi to‘lov infratuzilmasining uzluksiz ishlashi, tranzaksiyalar yakuniyligi, ma’lumotlar yaxlitligi va ommaviy ishonchning saqlanishi bilan bevosita bog‘lanadi. Mazkur maqolada kiberrezilientlik to‘lov tizimlari kontekstida kompleks tushuncha sifatida talqin qilinib, kiberxavfsizlik hodisalari pul muomalasiga ta’sir etishining asosiy kanallari yoritiladi.*

Kalit so‘zlar: *raqamli to‘lovlar, kiberrezilientlik, ommaviy ishonch, operatsion uzluksizlik, settlement yakuniyligi, antifrod.*

KIRISH

O‘zbekistonda raqamli to‘lov vositalari, mobil ilovalar, elektron hamyonlar va masofaviy xizmatlar kundalik iqtisodiy hayotning tezlashtiruvchi mexanizmiga aylanmoqda. Biroq tezlikning narxi bor: to‘lovlar tezlashgani sari xatolik ham tez tarqaladi, xavf ham tez ko‘payadi, eng muhimi, ishonch ham tez yo‘qolishi mumkin. Pul muomalasi barqarorligi ana shu nuqtada klassik monetar tushunchadan infratuzilmaviy tushunchaga yaqinlashadi: tizim ishlasa, muomala ishlaydi; tizim to‘xtasa, bozor ham “pauza”ga kiradi. Kiberrezilientlik esa shu muomalani “asabi” kabi: u bo‘lmasa, hatto eng yaxshi ilova ham foydalanuvchiga foyda bermaydi, faqat asabni “tezkor” qiladi.

Milliy tartibga solish doirasida to‘lov tizimlari bo‘yicha nazorat va kuzatuv mexanizmlarini belgilovchi hujjatlar Markaziy bankning axborot olish, tahlil qilish hamda qonunchilik talablari buzilganda choralar ko‘rish vakolatlarini aniq ko‘rsatadi [1]. Bu vakolatlar kiberrezilientlikni bozor intizomi sifatida shakllantirish uchun zarur, chunki to‘lov infratuzilmasida “xohlasam qilaman” degan yondashuv oxir-oqibat umumiy riskni oshiradi. Shuningdek, to‘lov tizimlari operatorlari va to‘lov xizmatlari provayderlari uchun axborot xavfsizligi hamda kiberxavfsizlik talablari alohida nizomda majburiy jarayonlar ko‘rinishida belgilangan bo‘lib, to‘lov axborotini himoyalash, shaxsga doir ma’lumotlar, insidentlarga munosabat va profilaktika yo‘nalishlari normativlashtirilgan [2].

ADABIYOTLAR SHARHI

Xalqaro adabiyotlarda to‘lov va bozor infratuzilmalari barqarorligi risklar orqali izohlanadi: operatsion uzilishlar, likvidlik dislokatsiyasi, huquqiy va kredit risklari bir-birini kuchaytirib, tizim orqali iqtisodiyotga tarqalishi mumkin [4]. Shu ramkada settlement yakuniyligi, operatsion riskni boshqarish va boshqaruv tamoyillari nafaqat texnik talab, balki moliyaviy barqarorlikning instrumenti sifatida ko‘riladi. Kiberxavflar esa aynan operatsion riskning zamonaviy va eng dinamik ko‘rinishi bo‘lib, to‘lov tizimlarida “ishonch”ni bevosita sinovdan o‘tkazadi. CPMI-IOSCOning kiberrezilientlik bo‘yicha qo‘llanmasi kiberrezilientlikni operatsion chidamlilikning hal qiluvchi qismi sifatida talqin qilib, boshqaruv, identifikatsiya, himoya, aniqlash, javob va tiklanish bloklari hamda test, situatsion xabardorlik, o‘rganish va evolyutsiya kabi transversal komponentlarni tavsiya

etadi [3]. Qo‘llanmada kritik operatsiyalarni tez tiklash bo‘yicha maqsadli yondashuvlar ham tilga olinadi, bu to‘lov tizimlari uchun “qanchalik tez tiklansak, shunchalik tez ishonch qaytadi” degan oddiy qoida bilan yakdil.

Ochiq moliya, APIlar va fintex integratsiyasi rivojlangani sari adabiyotlarda “attack surface” kengayishi muhokama qilinadi: to‘lovlar ko‘proq tizimlararo bog‘langan sari, zaif bo‘g‘in ham ko‘payadi. BISning open finance bo‘yicha hisobotida masofaviy identifikatsiya va autentifikatsiya, standartlashtirilgan API arxitekturasi, uchinchi tomonlar uchun texnik va tashkiliy talablar hamda markaziy validatorga o‘xshash yechimlar xavfsiz ekotizim sharti sifatida qayd etiladi [5]. Bu yondashuv ommaviy ishonchni “interfeys” emas, “arxitektura” ishlab chiqarishini ko‘rsatadi: foydalanuvchi qulay tugmani ko‘radi, lekin ishonch tugma ortidagi identifikatsiya, audit izi va javobgarlik zanjiridan tug‘iladi. Shu bilan birga, ISO 20022 kabi xabar standartlari strukturalangan va boy ma’lumotlar orqali monitoring, moslik nazorati va antifrod tahlilini kuchaytirish imkonini beradi, ya’ni xavfsizlikni “ma’lumot sifati” orqali ham qo‘llab-quvvatlaydi [7].

Milliy normativ manbalar esa kiberrezilientlikni sektor amaliyotiga tatbiq etish uchun institutsional asos beradi. Nazorat va kuzatuv nizomi Markaziy bankka to‘lov tizimi operatorlari hamda to‘lov tashkilotlari faoliyati bo‘yicha axborot yig‘ish va tahlil qilish imkonini beradi, bu esa riskka asoslangan kuzatuv modeliga o‘tishning huquqiy poydevoridir [1]. Axborot xavfsizligi va kiberxavfsizlik nizomi esa to‘lov axborotlarini himoya qilish, shaxsiy ma’lumotlar, insidentlar profilaktikasi va raqamli huquqbuzarliklarning oldini olish choralarini belgilab, operator va provayderlar uchun majburiy minimal standartni yaratadi [2]. CERT-CBU faoliyati haqidagi axborot to‘plami esa monitoring, audit, muhim infratuzilmani aniqlash va hamkorlik yo‘nalishlarini amaliy boshqaruv instrumentiga aylantirish tendensiyasini ko‘rsatadi [8]. Demak, adabiyotlar va normativ manbalar bir xulosaga olib keladi: rezilientlik – bu texnik himoya bilan birga boshqaruv, ma’lumot va hamkorlikni birlashtiradigan tizim.

TADQIQOT METODOLOGIYASI VA EMPIRIK TAHLIL

To‘lov tizimlaridagi kiberxavflarni pul muomalasi barqarorligiga ta’siri bo‘yicha uchta yadro kanalga ajratish mumkin: mavjudlik (availability) buzilishi, yaxlitlik (integrity) buzilishi va maxfiylik (confidentiality) buzilishi. Mavjudlik buzilganda tizim ishlashdan to‘xtaydi yoki sekinlashadi: tarmoqdagi DDoS, data markaz nosozligi, provayderdagi xato yangilanish, uchinchi tomon servislarining qulashlari natijasida to‘lovlar navbatga o‘tadi, yakuniy holat kechikadi, ayrim holatlarda “qayta urinib ko‘ring”ga aylanadi. Bu vaziyatning pul muomalasiga ta’siri darhol: savdo va xizmat ko‘rsatish kechikadi, naqd pulga talab oshadi, norasmiy hisob-kitoblar ko‘payadi, “tezkor” bo‘lishi kerak bo‘lgan tranzaksiya “kechikkan” iqtisodiy qarorga aylanadi. Shunday paytda odamlar pulni tizimga emas, qo‘liga yaqinlashtiradi, bu esa ommaviy ishonchni to‘g‘ridan-to‘g‘ri yemiradi.

Yaxlitlik buzilishi esa ko‘pincha ko‘rinmasroq, lekin xavfliroq: tranzaksiya rekvizitlarini almashtirish, to‘lov buyruqlarini soxtalashtirish, ichki tizimlarda ma’lumotlarni manipulyatsiya qilish, settlement yakuniyligini shubha ostiga qo‘yadigan nizolarni keltirib chiqaradigan holatlar. Xalqaro tamoyillar settlement yakuniyligi barqarorlik uchun markaziy ekanini urg‘ulaydi, chunki yakuniylik bo‘lmasa risklar qayta taqsimlanadi va ishtirokchilar likvidlikni “zaxira”ga yig‘ishni boshlaydi [4]. Kiberrezilientlik bo‘yicha qo‘llanma ham aynan yakuniylik va kritik operatsiyalarni tiklashni kiberrezilientlik maqsadlari bilan bog‘laydi [3]. Ya’ni, muammo faqat o‘g‘irlangan mablag‘ miqdorida emas: muammo shundaki, “yakuniy bo‘ldi” degan signalga ishonch pasaysa, muomala tezligi pasayadi, ehtiyotkorlik kuchayadi, iqtisodiy faollikda friksiya paydo bo‘ladi.

Maxfiylik buzilishi – ma'lumot sizishi, shaxsga doir ma'lumotlarning tarqalishi, kartalar va hisoblar bo'yicha rekvizitlarning fosh bo'lishi – pul muomalasiga ko'proq xulq-atvor orqali ta'sir qiladi. Ommaviy ishonchning iqtisodiy mexanizmi oddiy: foydalanuvchi riskni yuqori deb his qilsa, u odatini o'zgartiradi; odat o'zgarsa, muomala tuzilishi o'zgaradi. Tezkor to'lovlar bo'yicha World Bank materiali finality va real vaqtga yaqinlik ishonchni oshirishini qayd etadi [6], demak, uzilishlar va xavfsizlik muammolari bu afzallikni tez yo'qqa chiqaradi. Natijada odamlar raqamli to'lovdan vaqtincha chekinadi, biznes zaxira naqdni ko'paytiradi, provayderlar antifrod filtrlari va verifikatsiya bosqichlarini kuchaytiradi. Bu esa tranzaksiya "friksiya"sini oshirib, to'lovlar tezligi va qulayligini pasaytiradi, so'nggi hisobda pul muomalasi barqarorligiga bosim beradi.

NATIJALAR

Cyber guidance yondashuviga tayangan holda [3], to'lov tizimlari uchun yechimlar uch qatlamda takomillashtirilishi maqsadga muvofiq. Birinchi qatlam institut va boshqaruv: kiberrezilientlikni strategik risk sifatida rahbariyat darajasida ko'rish, insident boshqaruvi bo'yicha vakolatlar va qaror qabul qilish tartibini aniqlash, uchinchi tomonlar bilan shartnomalarda xavfsizlik majburiyatlari va audit huquqlarini mustahkamlash, sektor bo'yicha axborot almashinuvini yo'lga qo'yish. Milliy hujjatlar bu yo'nalishda nazorat-kuzatuv va kiberxavfsizlik talablarini belgilab, minimum standartni beradi [1], [2]. CERT-CBUning monitoring, audit va hamkorlik vazifalari esa muvofiqlashtirishni amaliy instrumentga aylantiradi [8]. Shu qatlamda eng katta "takomillashtirish zaxirasi" – talablarni bajarishni tekshirishdan ko'ra, rezilientlikni o'lchash va natija orqali boshqarishga o'tishdir.

Ikkinchi qatlam texnologiya va arxitektura: to'lov tizimlarida zaiflik ko'pincha integratsiya joyida namoyon bo'ladi. Open finance va APIlar bo'yicha BIS materiali xavfsiz identifikatsiya va autentifikatsiya, standartlashtirilgan arxitektura va uchinchi tomonlar uchun minimal talablar zarurligini ko'rsatadi [5]. Shu sabab, API xavfsizligi bo'yicha minimal paket sifatida kuchli autentifikatsiya, tranzaksion limitlar va rate limiting, tokenlarni boshqarish, audit loglar va anomaliyani aniqlash mexanizmlari, "least privilege" prinsipiga asoslangan ruxsatlar, yetkazib beruvchi zanjiri risklarini baholash, zaxira va avariya rejimlari ko'rilishi lozim. Bunga qo'shimcha ravishda, ISO 20022 kabi strukturalangan xabarlar standarti monitoring va antifrod analitikasini kuchaytirib, "nima bo'lyapti"ni tezroq tushunish imkonini beradi [7]. Ya'ni, ma'lumot sifati ham kiberrezilientlikning bir qismiga aylanadi: yomon ma'lumot – kechikkan qaror, kechikkan qaror – cho'zilgan uzilish.

Uchinchi qatlam xulq-atvor va ommaviy ishonch: kiberrezilientlikning yarmi texnikadan tashqarida, chunki tizimga kirish ko'pincha foydalanuvchi orqali sodir bo'ladi. Phishing, ijtimoiy muhandislik, soxta qo'ng'iroqlar va havolalar texnik himoyani aylanib o'tadi, natijada "tizim buzildi" emas, "foydalanuvchi aldandi" degan senariy ommaviy ko'lamga chiqadi. CERT-CBU axborot to'plamida hodisalarni aniqlash, oldini olish va ko'rsatmalar berish kabi vazifalar qayd etilgani bejiz emas [8]. Shu yo'nalishda banklar va to'lov tashkilotlari uchun yagona ogohlantirishlar, sodda va takroriy "kiber gigiyena" kampaniyalari, shikoyatlarni tez ko'rib chiqish va zararlarni adolatli kompensatsiya qilish mexanizmlari ommaviy ishonchni saqlashda texnik choralar qatori muhim.

XULOSA VA MUNOZARA

To'lov tizimlarida kiberrezilientlik ommaviy ishonchning texnik va institutsional poydevori bo'lib, u zaiflashsa pul muomalasi barqarorligi ham amaliyotda izdan chiqadi. Milliy normativ baza nazorat-kuzatuv hamda axborot xavfsizligi talablarini belgilab, bozor intizomini kuchaytirish va

risklarni boshqarish uchun huquqiy asos yaratadi. CERT-CBU faoliyati esa monitoring, audit, hodisalar oqibatini bartaraf etish va hamkorlik yo‘nalishlari orqali sektor darajasida rezilientlikni muvofiqlashtirish imkonini kuchaytiradi. Xalqaro ramkalar (PFMI va cyber guidance) kiberrezilientlikni moliyaviy barqarorlik bilan bevosita bog‘lab, operatsion uzluksizlik va settlement yakuniyligini asosiy tayanch sifatida ko‘rsatadi.

Amaliy taklif sifatida, O‘zbekiston sharoitida kiberrezilientlikni pul muomalasi barqarorligi bilan bog‘lovchi yagona boshqaruv konturi shakllantirilishi lozim: riskka asoslangan kuzatuvni rezilientlik indikatorlari paneli bilan to‘ldirish, tiklanish mezonlarini servis darajalariga aylantirish, uchinchi tomonlar va API integratsiyalar riskini standartlashtirish, ISO 20022 imkoniyatlarini monitoring va antifrod analitikasi bilan uyg‘unlashtirish, foydalanuvchi kiber savodxonligini tizimli oshirish. Bu chora-tadbirlar bitta maqsadga xizmat qiladi: raqamli to‘lovlar tez bo‘lishi yetarli emas, ular ishonchli bo‘lishi shart; aks holda “tezkor” tizim muomalani tezlashtirmaydi, balki xavotirni tezlashtiradi.

ADABIYOTLAR RO`YXATI

1. O‘zbekiston Respublikasi Markaziy banki boshqaruvining qarori. To‘lov tizimi operatorlarining va to‘lov tashkilotlarining faoliyatini nazorat qilish va kuzatuvni amalga oshirish tartibi to‘g‘risidagi nizomni tasdiqlash haqida: ro‘yxat raqami 3434, 15.05.2023 (kuchga kirishi 17.08.2023). – Toshkent, 2023. – Elektron manba.
2. O‘zbekiston Respublikasi Markaziy banki boshqaruvining qarori. To‘lov tizimlari operatorlari va to‘lov xizmatlarini yetkazib beruvchilarning to‘lov tizimlarida axborot xavfsizligi va kiberxavfsizlikni ta’minlash hamda raqamli texnologiyalar vositasida sodir etiladigan huquqbuzarliklarning oldini olish choralarini ko‘rish to‘g‘risidagi nizomni tasdiqlash haqida: ro‘yxat raqami 3513, 21.05.2024. – Toshkent, 2024. – Elektron manba.
3. CPMI-IOSCO. Guidance on cyber resilience for financial market infrastructures. – Basel: Bank for International Settlements, 2016. – 32 p.
4. CPSS-IOSCO. Principles for financial market infrastructures. – Basel: Bank for International Settlements, 2012. – 188 p.
5. BIS (CGIDE). Enabling open finance through APIs. – Basel: Bank for International Settlements, 2020. – 23 p.
6. World Bank Group. Fast Payment Systems: Preliminary Analysis of Global Developments (policy toolkit material). – Washington, DC: The World Bank, 2020. – 24 p.
7. ISO 20022 Registration Authority. ISO 20022: Universal financial industry message scheme (overview material). – Elektron manba, murojaat qilingan sana: 10.02.2026.
8. O‘zbekiston Respublikasi Markaziy banki. Bank va to‘lov tizimlarida axborot xavfsizligi va kiberxavfsizlikni ta’minlash hamda shubhali (frod) operatsiyalarni oldini olish bo‘yicha Markaziy bank “CERT-CBU” kiberxavfsizlik markazi tomonidan 2024-yilda amalga oshirilgan ishlar. – Toshkent, 2025. – 8 b.