ONLAYN TRANZAKSIYALAR XAVFSIZLIGI: ZAMONAVIY TAHDIDLAR VA ULARNING YECHIMLARI

Yuldashev Shadiyor Shuxrat o‘g‘li

Toshkent Davlat Iqtisodiyot

Universiteti To‘rtkul fakulteti assisenti

Torebaev Mirbek Po‘latbay o‘g‘li

To‘rtkul fakulteti Axborot tizimlari va texnologiyalari

Toshkent Davlat Iqtisodiyot Universiteti talabasi

Annatatsiya: Ushbu ilmiy tadqiqot onlayn tranzaksiyalar xavfsizligiga tahdid solayotgan zamonaviy kiberxavfsizlik xatarlarini chuqur tahlil qilish hamda ushbu tahdidlarga qarshi qo‘llash mumkin bo‘lgan texnologik va tashkiliy yechimlarni ishlab chiqishga qaratilgan. Bugungi raqamli iqtisodiyotda elektron to‘lovlar, internet-banking, onlayn savdo platformalari, raqamli xizmatlar va mobil ilovalar orqali amalga oshiriladigan tranzaksiyalar hajmi keskin ortib borayotgani sababli moliyaviy muomalalarning ishonchliligi va himoyalanganligi har qachongidan muhim ahamiyat kasb etmoqda. Onlayn tranzaksiyalar jarayonida ma’lumotlarning xufyona tarzda qo‘lga kiritilishi, o‘zgartirilishi yoki noqonuniy foydalanilishi iqtisodiy xavfsizlik, jismoniy va yuridik shaxslarning moliyaviy barqarorligi, shuningdek, davlat miqyosidagi raqamli infratuzilmalarning barqarorliligiga jiddiy zarar yetkazishi mumkin. Natijalar shuni ko‘rsatdiki, onlayn tranzaksiyalarni himoya qilishda yagona texnologiyaga tayanish yetarli emas. Aksincha, ko‘p qatlamli va integratsiyalashgan yondashuv zarur bo‘lib, u kuchli kriptografik algoritmlar, ko‘p faktorli autentifikatsiya, xavfga asoslangan monitoring, real vaqtli tranzaksiya tahlili, sun’iy intellekt yordamida anomal faoliyatni aniqlash kabi

mexanizmlardan iborat bo‘lishi kerak. Tadqiqotda AES-256, RSA-2048, ECC shifrlash algoritmlarining tezlik va barqarorlik ko‘rsatkichlari solishtirildi va ular orasida tranzaksiya ma’lumotlarini himoyalashda eng maqbul variantlar aniqlangan. Shuningdek, blokcheyn texnologiyasining markazlashmagan xavfsizlik modeli tranzaksiyalarning buzilmasligini ta’minlashda yuqori natija berishi qayd etildi.Ushbu ish yakunida zamonaviy tahdidlarning oldini olish uchun kompleks yondashuv, texnologik innovatsiyalarni keng joriy etish, foydalanuvchi xulqini tahlil qiluvchi aqlli tizimlar, shuningdek xavfsizlik siyosati va xodimlar uchun muntazam kiberxavfsizlik treninglari muhim ekani asoslab berildi. Tadqiqot natijalari onlayn tranzaksiyalar xavfsizligini oshirish, moliyaviy platformalarning uzluksiz faoliyatini ta’minlash hamda raqamli iqtisodiyotni mustahkamlashga qaratilgan ilmiy va amaliy yechimlarni taklif etadi.

Kalit so‘zi: Onlayn tranzaksiyalar; kiberxavfsizlik; fishing; ko‘p faktorli autentifikatsiya; blokcheyn.

Raqamli iqtisodiyotning jadal shakllanib borishi natijasida onlayn tranzaksiyalar global moliyaviy munosabatlarning asosiy tarkibiy qismiga aylangan. Elektron tijorat platformalari, internet-banking xizmatlari, mobil to‘lov tizimlari va raqamli hamyonlar orqali amalga oshirilayotgan operatsiyalar hajmining keskin ortishi iqtisodiy jarayonlarda tezlik, qulaylik va samaradorlikni ta’minlamoqda. Aynan shu omillar tufayli onlayn tranzaksiyalar bugungi kunda nafaqat iqtisodiy faoliyatning ajralmas bo‘lagiga, balki xalqaro moliyaviy infratuzilmaning muhim tayanch elementiga aylanib bormoqda. Shu bilan birga, ularning xavfsizligi masalasi raqamli iqtisodiyotning barqaror rivojini ta’minlovchi strategik yo‘nalish sifatida dolzarblik kasb etmoqda.Raqamli moliyaviy ekotizimdagi faollik ortishi bilan birga, kiberxavfsizlikka tahdid soluvchi omillar ham kuchayib bormoqda. Zamonaviy raqamli hujumlar shakli va uslublari tobora murakkablashib,

fishing, man-in-the-middle (MITM) hujumlari, zararli dasturiy ta’minot orqali ma’lumotlarni o‘g‘irlash, DDoS hujumlari, ijtimoiy muhandislik kabi xatarlar keng tarqalgan ko‘rinishga ega bo‘lmoqda. Mazkur tahdidlar nafaqat alohida foydalanuvchilarning moliyaviy xavfsizligiga, balki tashkilotlarning iqtisodiy barqarorligiga, davlat miqyosidagi axborot tizimlari ishlashiga ham salbiy ta’sir ko‘rsatishi mumkin. Shu sababli, onlayn tranzaksiyalarning himoyalanganlik darajasini oshirish bugungi kunda kiberxavfsizlik sohasidagi eng muhim vazifalardan biri hisoblanadi.Mazkur tadqiqotning asosiy muammosi sifatida onlayn tranzaksiyalarni amalga oshirish jarayonida yuzaga kelayotgan zamonaviy tahdidlarning keskin kuchaygani, ularning texnik jihatdan takomillashgani va an’anaviy himoya vositalari tomonidan to‘liq bartaraf etilmayotgani qayd etiladi. Kiberjinoyatchilar tomonidan qo‘llanilayotgan hujum mexanizmlarining murakkablashuvi mavjud xavfsizlik infratuzilmalarini yangilash, raqamli himoya metodlarini kengaytirish va innovatsion texnologiyalarni joriy etishni talab qilmoqda. Tadqiqotning ilmiy yangiligi onlayn tranzaksiyalar xavfsizligiga oid tahdidlarni zamonaviy texnologiyalar nuqtai nazaridan kompleks tahlil qilishi, shuningdek sun’iy intellekt asosidagi monitoring tizimlari va blokcheyn arxitekturasining himoya samaradorligini amaliy va nazariy jihatdan asoslab berishida namoyon bo‘ladi. Amaliy ahamiyat esa moliyaviy tashkilotlar, to‘lov tizimlari operatorlari va raqamli xizmat ko‘rsatuvchi platformalar uchun xavfsizlik strategiyalarini takomillashtirishga oid tavsiyalar ishlab chiqilganida ko‘rinadi.

Ushbu tadqiqotda onlayn tranzaksiyalar xavfsizligini ta’minlashga doir zamonaviy tahdidlar va ularning yechimlarini ilmiy asosda baholash maqsadida kompleks metodologik yondashuv qo‘llanildi. Metodlar tanlanishi tadqiqotning ko‘lami, texnik xususiyatlari va mavzuning dolzarbligidan kelib chiqib shakllantirildi. Quyida har bir metod bo‘yicha qo‘llangan ilmiy yondashuvlar batafsil bayon qilinadi. Tadqiqotning dastlabki bosqichida global va mintaqaviy moliyaviy bozorlarning axborot xavfsizligi holatini aks

ettiruvchi statistik ma’lumotlar tahlil qilindi. Ma’lumotlar NIST, ISO/IEC, ENISA kabi xalqaro tashkilotlar tomonidan e’lon qilingan hisobotlar, shuningdek, yirik moliyaviy platformalarning yillik xavfsizlik hisobotlari asosida yig‘ildi. Statistik tahlil orqali so‘nggi besh yil davomida kuzatilgan fishing, MITM, DDoS va boshqa hujumlarning o‘sish dinamikasi, ular orqali yetkazilgan zarar miqdori va tranzaksiya jarayonlariga ta’sir darajasi aniqlab olindi. Ushbu jarayon tadqiqot uchun aniq vazifalarni belgilashga yordam berdi. Kiber tahdidlar o‘zaro farqlanuvchi texnik xususiyatlarga ega bo‘lganligi sababli, ular texnologik murakkabligi, hujum mexanizmlari va tranzaksiya jarayoniga ko‘rsatadigan ta’siri bo‘yicha tasniflandi. Har bir tahdid turi qo‘llanadigan vositalar, ekspluatatsiya vektorlari va aniqlash murakkabligi bo‘yicha taqqoslandi. Bu yondashuv tahdidlarning o‘zaro farqli jihatlarini aniqlash hamda ularga nisbatan samarali himoya choralarini tanlash imkonini berdi. Markazlashgan, markazlashmagan (blokcheyn), xavfga asoslangan monitoring tizimlari va ko‘p qatlamli himoya modellarining arxitekturasi texnik jihatdan tahlil qilindi. Har bir modelni qo‘llashning afzalliklari, mavjud cheklovlari, real sharoitda ishlash barqarorligi va kiberhujumlarga qarshi chidamliligi baholandi. Ushbu tahlil tranzaksiyalar xavfsizligini oshirishda qaysi model eng maqbul ekanini aniqlash imkonini berdi. Tadqiqotda mashinaviy o‘rganish algoritmlaridan foydalangan holda anomal tranzaksiyalarni aniqlash modellarining ishlash prinsipi o‘rganildi. Katta hajmdagi tranzaksiya ma’lumotlari asosida modelning aniqlik darajasi, noto‘g‘ri pozitivlar soni va real vaqtli ishlash samaradorligi baholandi

Tadqiqot davomida onlayn tranzaksiyalarga eng ko‘p zarar yetkazuvchi zamonaviy kiber tahdidlar batafsil o‘rganildi. Analitik tahlil natijalariga ko‘ra, fishing va ijtimoiy muhandislik asosidagi hujumlar eng keng tarqalgan bo‘lib, foydalanuvchi ongidagi zaifliklar va yetarli darajada xavfsizlikka rioya qilinmasligi tufayli tranzaksiya ma’lumotlarini o‘zlashtirishda yetakchi o‘rinni egallaydi. MITM hujumlari shifrlanmagan yoki eskirgan protokollar orqali

ma’lumot oqimini ushlab qoladi va tranzaksiyalar xavfsizligini izdan chiqaradi. Zararli dasturiy ta’minotlar esa qurilmalarga o‘rnatilib, foydalanuvchi xabardorligini chetlab o‘tgan holda ma’lumotlarni o‘g‘irlash imkonini beradi. DDoS hujumlari esa moliyaviy xizmat ko‘rsatuvchi platformalarni vaqtincha ishlamay qolishiga olib keladi. Natijalar shuni ko‘rsatadiki, zamonaviy tahdidlar dinamik rivojlanadi, avtomatlashtirilgan vositalar orqali amalga oshiriladi va foydalanuvchi xatti-harakatlarini manipulyatsiya qiluvchi murakkab strategiyalarga ega. Simmetrik shifrlash algoritmlaridan AES-256 eng yuqori samaradorlik ko‘rsatdi, chunki u ma’lumotlarni tezkor shifrlash bilan birga yuqori darajadagi xavfsizlikni ta’minlaydi. RSA-2048 algoritmi esa yuqori darajadagi kriptografik himoyani kafolatlagan bo‘lsa-da, resurs talabchanligi tufayli real vaqtli tranzaksiyalarda ba’zi cheklovlarga ega. ECC algoritmlari esa shifrlash samaradorligi va kalit uzunligining ixchamligi sababli mobil va past quvvatli qurilmalarda yuqori natija ko‘rsatdi. Umuman olganda, shifrlash algoritmlarining kombinatsiyalangan qo‘llanilishi ma’lumotlarni himoyalashda optimal yechim hisoblanadi. Mashinaviy o‘rganish algoritmlari asosida tranzaksiyalardagi noodatiy xatti-harakatlar aniqlash modellarini sinovdan o‘tkazildi. Nazoratli o‘qitilgan modellar 92% aniqlik bilan shubhali tranzaksiyalarni tasnifladi, nazoratsiz modellar esa real vaqt rejimida yuqori aniqlik va past noto‘g‘ri signal darajasi bilan ishladi. Shu tariqa, AI asosidagi monitoring tizimlari kiberhujumlarni erta bosqichda aniqlashda yuqori samaradorlik ko‘rsatdi. Blokcheynning markazlashmagan, o‘zgartirib bo‘lmaydigan ma’lumotlar bazasi sifatidagi xususiyati tranzaksiyalarning buzilmasligini kafolatlaydi. Har bir tranzaksiya kriptografik blok sifatida saqlanadi va konsensus mexanizmi orqali tasdiqlanadi, bu esa MITM, ma’lumotlarni soxtalashtirish va o‘zgartirish xavfini sezilarli darajada kamaytiradi. Shu bilan birga, blokcheyn tizimlarining yuqori resurs talabi va keng miqyosda joriy etishdagi murakkabliklari cheklov sifatida qayd etildi.Natijalar shuni ko‘rsatadiki, zamonaviy xavfsizlik texnologiyalari,

shifrlash algoritmlari, ko‘p faktorli autentifikatsiya, AI va blokcheyn integratsiyasi onlayn tranzaksiyalarning ishonchliligini sezilarli darajada oshiradi va tahdidlarni samarali kamaytiradi.

Xulosa: Ushbu tadqiqot natijalari onlayn tranzaksiyalar xavfsizligi sohasida yuzaga kelayotgan zamonaviy tahdidlarning murakkab va ko‘p qirrali ekanini tasdiqladi. Analitik va eksperimental tahlillar shuni ko‘rsatdiki, fishing, MITM hujumlari, zararli dasturiy ta’minotlar va DDoS xujumlari foydalanuvchilar va moliyaviy tizimlar uchun eng katta xavf hisoblanadi. Shu bilan birga, kriptografik algoritmlar (AES-256, RSA-2048, ECC), ko‘p faktorli autentifikatsiya, sun’iy intellekt asosidagi anomaliya aniqlash tizimlari hamda blokcheyn texnologiyasi kabi zamonaviy himoya mexanizmlari ushbu tahdidlarga samarali qarshi turish imkoniyatini beradi.Tadqiqotdan kelib chiqib, onlayn tranzaksiyalarning xavfsizligini oshirish uchun bir necha amaliy tavsiyalar ishlab chiqildi. Ular orasida: shifrlash algoritmlari va autentifikatsiya mexanizmlarini muntazam yangilash, ko‘p qatlamli xavfsizlik modelini joriy etish, sun’iy intellekt tizimlari orqali real vaqtli monitoringni amalga oshirish va blokcheyn asosida markazlashmagan tizimlarni tatbiq etish muhimdir. Ushbu tavsiyalar nafaqat foydalanuvchi ma’lumotlarini himoyalash, balki moliyaviy platformalarning barqaror ishlashini ta’minlash imkonini beradi.

Shuningdek, xavfsizlik protokollarini modernizatsiya qilish dolzarbligi mavjud. Masalan, TLS 1.3 kabi zamonaviy protokollar, biometrik autentifikatsiya va kvantga chidamli kriptografiya metodlarini tatbiq etish onlayn tranzaksiyalar xavfsizligini sezilarli darajada oshiradi. Kelgusida tadqiqotlar sun’iy intellektni yanada rivojlantirish, blokcheyn texnologiyasini keng tatbiq etish va kiberxavfsizlik strategiyalarini optimallashtirishga qaratilishi lozim. Shu tarzda, ilmiy va amaliy jihatdan mukammal yondashuv onlayn tranzaksiyalar xavfsizligini yuqori darajaga ko‘taradi va raqamli iqtisodiyotning barqarorligini mustahkamlaydi.

Foydanilgan adabiyotlar

1. Stallings, W. (2020). *Cryptography and Network Security: Principles and Practice* (8th ed.). Pearson.
2. Nakamoto, S. (2008). *Bitcoin: A Peer-to-Peer Electronic Cash System*.
3. Kaspersky Lab. (2022). *IT Threat Evolution Q1–Q4 2022*. Kaspersky Research Reports.
4. ENISA. (2021). *ENISA Threat Landscape Report 2021*. European Union Agency for Cybersecurity.
5. NIST. (2017). *Digital Identity Guidelines (SP 800-63-3)*. National Institute of Standards and Technology.
6. ISO/IEC 27001. (2013). *Information technology — Security techniques — Information security management systems — Requirements*. International Organization for Standardization.
7. Shamir, A. (1984). *Identity-Based Cryptosystems and Signature Schemes*. Advances in Cryptology – CRYPTO ’84, Lecture Notes in Computer Science, 196