

**ELEKTRON SAVDO PLATFORMALARINI JORIY ETISHDA
KIBERXAVFSIZLIK MUAMMOLARINI HAL ETISH ISTIQBOLLARI****Yuldashev Shadiyor Shuxrat o'g'li***Toshkent Davlat Iqtisodiyot**Universiteti To'rtkul fakulteti assisenti***Xudayberganova Sohiba Hamid qizi***To'rtkul fakulteti Axborot tizimlari va texnologiyalari**Toshkent Davlat Iqtisodiyot Universiteti talabasi*

Annotatsiya Mazkur ilmiy tadqiqot elektron savdo platformalarini joriy etish jarayonida yuzaga kelayotgan kiberxavfsizlik muammolarini chuqur tahlil qilish hamda ularni samarali hal etish istiqbollarini ilmiy asosda o'rganishga bag'ishlangan. Bugungi kunda raqamli iqtisodiyotning jadal rivojlanishi natijasida elektron savdo global miqyosda muhim iqtisodiy mexanizmga aylanib bormoqda. Tovar va xizmatlarning masofadan turib sotilishi aholiga qulayliklar yaratish bilan birga, tadbirkorlik subyektlari uchun yangi bozor imkoniyatlarini ochib bermoqda. Biroq elektron savdo platformalarining kengayishi bilan bir qatorda kiberxavfsizlik bilan bog'liq tahdidlar ham keskin ortib bormoqda. Ayniqsa, foydalanuvchilarning shaxsiy ma'lumotlari, moliyaviy tranzaksiyalar va bank karta rekvizitlarining raqamli muhitda saqlanishi kiberjinoyatchilar uchun qulay nishon bo'lib xizmat qilmoqda. Tadqiqot davomida elektron savdo platformalarida uchraydigan asosiy kiberxavfsizlik tahdidlari, jumladan, phishing hujumlar, zararli dasturlar orqali ma'lumotlarni o'g'irlash, xizmat ko'rsatishni rad etish hujumlari (DDoS), shuningdek, ma'lumotlar bazalarining himoyasizligi natijasida yuzaga keladigan axborot sizib chiqishi holatlari atroflicha tahlil qilindi.

Tadqiqot natijalari shuni ko'rsatadiki, elektron savdo platformalarida kiberxavfsizlikni ta'minlash nafaqat texnik, balki tashkiliy va huquqiy mexanizmlarning uyg'un ishlashini ham talab etadi. Foydalanuvchilarning axborot xavfsizligi bo'yicha bilim va ko'nikmalarining yetarli darajada shakllanmaganligi ham kiberjinoyatchilikning keng tarqalishiga sabab bo'layotgan muhim omillardan biri hisoblanadi. Shu bois, texnik himoya vositalari bilan bir qatorda, foydalanuvchilar o'rtasida axborot xavfsizligi madaniyatini oshirish ham muhim strategik vazifa sifatida qaraladi. Mazkur tadqiqot natijalari asosida elektron savdo platformalarida kiberxavfsizlikni kuchaytirish bo'yicha bir qator amaliy taklif va tavsiyalar ishlab chiqildi. Xususan, himoya tizimlarini xalqaro standartlar asosida modernizatsiya qilish, kuchli kriptografik vositalardan foydalanish, real vaqt rejimida tahdidlarni aniqlovchi intellektual monitoring tizimlarini joriy etish hamda foydalanuvchilarning axborot xavfsizligi bo'yicha xabardorligini oshirish zarurligi ilmiy jihatdan asoslab berildi.

Ushbu tadqiqot natijalari elektron savdo sohasining barqaror va xavfsiz rivojlanishini ta'minlashga xizmat qiladi.

Kalit so'zlar: Elektron savdo, kiberxavfsizlik, axborot xavfsizligi, elektron to'lovlar, kiberhujumlar, ma'lumotlar himoyasi, kriptografiya.

So'nggi yillarda raqamli iqtisodiyotning jadal rivojlanishi natijasida elektron savdo (e-commerce) O'zbekiston iqtisodiyotida muhim o'rin egallay boshladi. Davlat tomonidan raqamli transformatsiya va "Elektron hukumat" dasturlarini amalga oshirish orqali onlayn savdo platformalari aholiga xizmat ko'rsatishning samarali va qulay vositasiga aylantirilmoqda. Ayniqsa, Prezidentning 2019-yil 5-fevraldagi "Raqamli iqtisodiyotni rivojlantirish konsepsiyasini tasdiqlash to'g'risida"gi qarori va 2021-yil 30-martdagi "Elektron tijoratni rivojlantirish chora-tadbirlari to'g'risida"gi qarorlari elektron savdo infratuzilmasini modernizatsiya qilish, platformalarning xavfsizlik tizimini takomillashtirish va foydalanuvchilar ma'lumotlarini himoya qilishni ustuvor vazifa sifatida belgiladi. Ushbu hujjatlar nafaqat raqamli iqtisodiyotni rivojlantirishga, balki xalqaro standartlarga mos keladigan xavfsizlik mexanizmlarini joriy etishga ham katta e'tibor qaratadi. O'zbekiston sharoitida elektron savdo platformalarining rivojlanish tendensiyalari ijobiy bo'lishiga qaramay, ular bilan birga turli kiberxavfsizlik muammolari ham yuzaga kelmoqda. Jumladan, foydalanuvchilarning shaxsiy ma'lumotlari, bank rekvizitlari va moliyaviy tranzaksiyalar onlayn tizimlarda saqlanishi kiberjinoyatchilar uchun jozibador nishonga aylanmoqda. Phishing hujumlar, zararli dasturlar, DDoS xujumlar, shuningdek, ma'lumotlar bazalarining yetarlicha himoyalanganligi oqibatida yuzaga keladigan ma'lumotlar sizib chiqishi holatlari elektron savdo tizimlarining ishonchliligiga sezilarli xavf tug'dirmoqda. Shu sababli platformalarning xavfsizlik darajasini oshirish davlat siyosati darajasida ham muhim vazifa sifatida ko'rilmoqda.

Mazkur tadqiqotning **asosiy maqsadi** – O'zbekiston sharoitida elektron savdo platformalarini joriy etishda uchraydigan kiberxavfsizlik muammolarini aniqlash va ularni hal etish istiqbollari ilmiy asosda o'rganishdir. Tadqiqot vazifalari sifatida quyidagilar belgilandi: kiberxavflarni aniqlash, zamonaviy himoya texnologiyalari va xalqaro xavfsizlik standartlarini tahlil qilish hamda amaliy tavsiyalar ishlab chiqish. Tadqiqotning **ilmiy yangiligi** shundaki, u Prezident qarorlari asosida mamlakat sharoitiga moslashtirilgan xavfsizlik chora-tadbirlarini ilmiy tahlil qiladi va elektron savdo tizimlarining samaradorligini oshirishga yo'naltirilgan. Shu bilan birga, tadqiqotning **amaliy ahamiyati** elektron tijoratni rivojlantirish, foydalanuvchi ma'lumotlarini himoya qilish va O'zbekistonning raqamli iqtisodiyotini barqaror rivojlantirishga xizmat qiladi.

O'zbekiston sharoitida elektron savdo platformalarini joriy etishda yuzaga keladigan kiberxavfsizlik muammolarini aniqlash va ularni samarali hal etish

istiqbollarini o‘rganishdir. Tadqiqot metodologiyasi **kompleks ilmiy yondashuv**ga asoslandi va quyidagi usullarni o‘z ichiga oladi: **tahlil, taqqoslash, kuzatuv va statistik ma’lumotlarni umumlashtirish**. Ushbu yondashuv platformalarning xavfsizlik darajasini baholash va tahdidlarni aniqlash imkonini beradi. Axborot manbalari sifatida ilmiy maqolalar, monografiyalar, xalqaro standartlar, shuningdek, O‘zbekiston Respublikasi Prezidentining 2019–2022 yillardagi qarorlari, jumladan, “Raqamli iqtisodiyotni rivojlantirish konsepsiyasi” va “Elektron tijoratni rivojlantirish chora-tadbirlari” tahlil qilindi. Bundan tashqari, elektron savdo platformalarining amaliy faoliyati va foydalanuvchi statistikasi ham o‘rganildi. Ushbu manbalarni tahlil qilish orqali kiberxavflar va ularni oldini olish imkoniyatlari aniqlangan. Tadqiqot davomida **ISO/IEC 27001** va **PCI DSS** xalqaro kiberxavfsizlik standartlari o‘rganildi. Ushbu standartlar platformalarda axborot xavfsizligini ta’minlash va foydalanuvchi ma’lumotlarini himoya qilishga yo‘naltirilgan. Shuningdek, elektron savdoda xavfsizlikni ta’minlash texnologiyalari — kriptografik algoritmlar, ikki bosqichli autentifikatsiya, biometrik identifikatsiya va sun’iy intellekt asosidagi monitoring tizimlari tahlil qilindi. Ushbu texnologiyalar O‘zbekiston sharoitida platformaning xavfsizlik darajasini oshirishga qanchalik samarali ekanligi baholandi. Natijada qo‘llanilgan usullar kompleks yondashuvni ta’minlab, elektron savdo platformalarini kiberxavfsizlik nuqtai nazaridan chuqur tahlil qilish imkonini berdi. Tadqiqot natijalari O‘zbekiston sharoitida platformalarning xavfsizligini oshirish va foydalanuvchi ma’lumotlarini himoya qilish bo‘yicha amaliy tavsiyalar ishlab chiqishga xizmat qiladi.

O‘zbekiston sharoitida elektron savdo platformalarida eng ko‘p uchraydigan kiberxavfsizlik tahdidlari quyidagilardan iborat. Birinchi navbatda, **phishing hujumlar** foydalanuvchilarning shaxsiy ma’lumotlarini va moliyaviy tranzaksiyalarini aldov yo‘li bilan qo‘lga kiritishga qaratilgan. Ushbu hujumlar, ayniqsa, oddiy parol tizimidan foydalanadigan foydalanuvchilar orasida keng tarqalgan. Ikkinchi muhim tahdid — **zararli dasturlar (malware)**, ular platforma tizimlariga zarar yetkazish va maxfiy ma’lumotlarni yashirin ravishda uzatish orqali foydalanuvchilarga va platformalarga jiddiy moliyaviy zarar yetkazadi. Shuningdek, **DDoS hujumlar** elektron savdo saytlarining faoliyatini vaqtincha to‘xtatish orqali savdo operatsiyalarining uzilishiga olib keladi va foydalanuvchilarda ishonchsizlikni keltirib chiqaradi. To‘rtinchi eng keng tarqalgan tahdid — **ma’lumotlar sizib chiqishi**, ya’ni himoyaning sustligi sababli foydalanuvchilarning shaxsiy va moliyaviy ma’lumotlari uchinchi shaxslarga tushib qolishi. Tadqiqot natijalari shuni ko‘rsatdiki, bunday hodisalar nafaqat platformaning obro‘sig, balki foydalanuvchilarning moliyaviy xavfsizligiga ham jiddiy ta’sir qiladi. Kiberhujumlarning foydalanuvchilar va tashkilotlarga yetkazadigan zarari ham tahlil qilindi. Phishing va malware hujumlari natijasida foydalanuvchilarning shaxsiy ma’lumotlari o‘g‘irlanadi, moliyaviy

tranzaksiyalar buziladi, DDoS hujumlari esa platformaning ish faoliyatini to'xtatadi. Bu esa nafaqat moliyaviy yo'qotishlarga, balki platformaning xizmat ko'rsatish qobiliyatining pasayishiga olib keladi. Shu bilan birga, ma'lumotlar sizib chiqishi ishonchni pasaytiradi va mijozlar bazasining qisqarishiga sabab bo'ladi.

Tahlillar shuni ko'rsatdiki, **himoya darajasining hozirgi holati** O'zbekistonda yetarli darajada mukammal emas. Ko'plab platformalarda autentifikatsiya tizimlari sodda, ikki bosqichli himoya va zamonaviy kriptografik usullar yetarlicha qo'llanmayapti. Shu bilan birga, **amaldagi xavfsizlik tizimlarining samaradorligi** turlicha bo'lib, ayrim platformalarda zamonaviy texnologiyalar — biometrik autentifikatsiya, sun'iy intellekt asosida tahdidlarni aniqlash tizimlari va real vaqt rejimida monitoring tizimlari qo'llanilgan bo'lsa-da, ko'pchilik platformalarda ular yetarli darajada tatbiq etilmagan. Umuman olganda, tadqiqot natijalari shuni ko'rsatadiki, O'zbekiston sharoitida elektron savdo platformalarining xavfsizlik tizimini kuchaytirish, foydalanuvchilarning ma'lumotlarini himoya qilish va xalqaro standartlarga mos infratuzilmani joriy etish zarurati mavjud. Bu esa nafaqat texnik himoya, balki foydalanuvchi savodxonligi va tashkiliy chora-tadbirlarni ham o'z ichiga oladi. Olingan natijalar shuni ko'rsatadiki, O'zbekiston sharoitida elektron savdo platformalarida kiberxavfsizlik tahdidlari keng tarqalgan va ular foydalanuvchilar hamda platformalarga sezilarli zarar yetkazmoqda. Tadqiqot davomida aniqlangan phishing hujumlari, zararli dasturlar, DDoS xujumlar va ma'lumotlar sizib chiqishi holatlari platformalarning ishonchliligini pasaytiradi hamda foydalanuvchilar o'rtasida xavfsizlik bo'yicha ishonchsizlikni oshiradi. Shu bilan birga, himoya tizimlarining yetarli darajada ishlayotgani kiberhujumlarning muvaffaqiyatli amalga oshishiga zamin yaratmoqda. Mavjud muammolarning kelib chiqish sabablari asosan uch omilga bog'liq: birinchidan, ko'plab platformalarda autentifikatsiya va himoya tizimlari oddiy va eskirgan; ikkinchidan, foydalanuvchilarning axborot xavfsizligi bo'yicha savodxonligi past; uchinchidan, elektron savdoni tartibga soluvchi normativ-huquqiy bazaning yetarlicha rivojlanmaganligi kiberhujumlarni amalga oshirish imkoniyatini oshiradi. Xususan, ma'lumotlar bazalarining yetarlicha himoyalanganligi va ikki bosqichli autentifikatsiya tizimlarining cheklangan qo'llanilishi bu muammolarning asosiy sabablaridan biridir. Mahalliy tajribani xorijiy tajriba bilan solishtirish natijalari shuni ko'rsatadiki, ilg'or mamlakatlarda elektron savdo platformalari kiberxavfsizlikni ta'minlash uchun zamonaviy texnologiyalarni keng qo'llaydi. Kriptografik himoya, sun'iy intellekt asosida tahdidlarni aniqlash tizimlari va biometrik autentifikatsiya O'zbekiston sharoitida ham samarali qo'llanilishi mumkin bo'lgan asosiy vositalar hisoblanadi. Xorijiy tajribalar shuni ko'rsatadiki, bu texnologiyalar platformaning xavfsizlik darajasini sezilarli darajada oshiradi va foydalanuvchi ma'lumotlarini himoya qiladi.

Kriptografiya foydalanuvchi ma'lumotlarini shifrlash va tranzaksiyalarni xavfsiz amalga oshirish imkonini beradi. Sun'iy intellekt esa real vaqt rejimida kiberhujumlarni aniqlash va ularni avtomatik bartaraf etishga xizmat qiladi. Biometrik autentifikatsiya esa foydalanuvchini noyob identifikatsiya qilish orqali kirish xavfsizligini oshiradi. Tadqiqot natijalari shuni ko'rsatadiki, ushbu texnologiyalarni birgalikda qo'llash elektron savdo platformalarida kiberxavfsizlikni sezilarli darajada kuchaytiradi. Shuningdek, O'zbekiston sharoitida Prezidentning "Raqamli iqtisodiyotni rivojlantirish konsepsiyasi" va "Elektron tijoratni rivojlantirish chora-tadbirlari to'g'risida"gi qarorlari ilg'or texnologiyalarni joriy etish uchun normativ-huquqiy baza sifatida xizmat qilishi mumkin. Shu bois, zamonaviy texnologiyalarni tatbiq etish, foydalanuvchilarning axborot xavfsizligini oshirish va platformalarni xalqaro standartlarga moslashtirish amaliy jihatdan muhim ahamiyatga ega. Umuman olganda, tadqiqot natijalari elektron savdo platformalarida kiberxavfsizlikni mustahkamlash uchun zamonaviy texnologiyalarni qo'llash zarurligini ilmiy asoslaydi va amaliy tavsiyalar ishlab chiqishga imkon yaratadi.

Xulosa: Tadqiqot shuni ham ko'rsatdiki, hozirgi vaqtda ko'plab elektron savdo platformalarida xavfsizlik tizimlari yetarlicha yuqori darajada yo'lga qo'yilmagan. Elektron savdo platformalarida kiberxavfsizlikni kuchaytirish uchun bir qator **amaliy tavsiyalar** ishlab chiqildi. Jumladan, platformalarda ikki bosqichli autentifikatsiyani majburiy joriy etish, foydalanuvchi ma'lumotlarini zamonaviy kriptografik algoritmlar asosida shifrlash, real vaqt rejimida ishlovchi sun'iy intellekt asosidagi monitoring tizimlaridan foydalanish zarur. Shuningdek, biometrik autentifikatsiya texnologiyalarini bosqichma-bosqich joriy etish platformalarning himoya darajasini sezilarli oshirishi mumkin. Texnik chora-tadbirlar bilan bir qatorda, foydalanuvchilarning axborot xavfsizligi bo'yicha bilimlarini oshirish, ularni kiberxavflardan ogoh qilish ham muhim ahamiyatga ega. Bundan tashqari, elektron savdoni tartibga soluvchi normativ-huquqiy bazani yanada takomillashtirish ham zamon talabi hisoblanadi. Tadqiqot natijalariga asosanib, elektron savdo sohasining **istiqbolli rivojlanish yo'nalishlari** sifatida raqamli xavfsizlik infratuzilmasini mustahkamlash, xalqaro kiberxavfsizlik standartlarini keng joriy etish, sun'iy intellektga asoslangan himoya tizimlarini rivojlantirish va fintech texnologiyalar bilan integratsiyani chuqurlashtirishni ko'rsatish mumkin. Ushbu yo'nalishlarning izchil amalga oshirilishi O'zbekistonning raqamli iqtisodiyotini barqaror rivojlantirish, elektron savdo tizimlarining ishonchligini ta'minlash hamda foydalanuvchilar manfaatlarini to'liq himoya qilishga xizmat qiladi.

Foydanilgan adabiyotlar

1. O'zbekiston Respublikasi Raqamli texnologiyalar vazirligi. (2024). Elektron tijorat statistikasi 2023. Toshkent.

2. Cybersecurity Ventures. (2024). Cybercrime Report: E-commerce Security Statistics. *Official Annual Cybercrime Report*.
3. O'zbekiston Respublikasi. (2022). Kiberxavfsizlik to'g'risidagi Qonun. O'RQ-764-son. Toshkent.
4. Smith, J. A., & Davis, R. M. (2023). Evolution of cyber threats in e-commerce: A comprehensive analysis. *Journal of Cybersecurity Research*, 18(3), 245-267.
5. Kumar, S., Patel, R., & Zhang, L. (2023). Blockchain technology for securing electronic payment systems. *International Journal of Information Security*, 22(4), 891-915.
6. Karimov, A. R., & Azizov, B. T. (2024). Kiberxavfsizlik holati: O'zbekiston elektron savdo platformalari tahlili. *O'zbekiston Iqtisodiyot va Ta'lim Jurnal*i, 5(2), 78-95.