ELEKTRON TIJORAT PLATFORMALARINING XAVFSIZLIK JIXATLARI TAHLILI

Maxmudov Lazizbek Ubaydullo o‘g‘li
i.f.f.d., (Phd)
Samarqand iqtisodiyot va servis instituti, “Real iqtisodiyot” kafedrasi dotsenti
lazizmakhmudov90@gmail.com
+99897 913 60 19
ORCID: 0000-0002-6819-6543

Annotatsiya: *Maqola elektron tijorat platformalarining xavfsizlik jihatlarini tahlil qiladi. Kiberhujumlar, ma’lumotlar maxfiyligi va firibgarlik kabi tahdidlarning turlari va tasnifi ko‘rib chiqiladi. Shifrlash protokollari, ko‘p faktorli autentifikatsiya, to‘lov shlyuzlari va boshqa xavfsizlik tizimlarining roli yoritiladi. Mijozlar ishonchini oshirish, raqobatbardoshlikni ta’minlash va iqtisodiy samaradorlikka erishish uchun xavfsizlik choralarining ahamiyati ta’kidlanadi. O‘zbekistonda huquqiy bazani takomillashtirish va raqamli savodxonlikni oshirish bo‘yicha tavsiyalar beriladi.*

Kalit so‘zlar: *elektron tijorat, xavfsizlik tizimlari, kiberhujumlar, ma’lumotlar maxfiyligi, mijozlar ishonchi, shifrlash protokollari, ko‘p faktorli autentifikatsiya, to‘lov shlyuzlari, firibgarlik, raqamli savodxonlik, huquqiy asoslar, DDoS hujumlari, SQL in'ektsiyalari, saytlararo skript, yashil logistika.*

Kirish. Hozirgi kunda elektron tijorat dunyo bo‘ylab iqtisodiyotning ajralmas qismiga aylanib bormoqda. Foydalanuvchilarning tovar va xizmatlarga onlayn buyurtma berishi odat tusiga kirayotgan bir davrda, elektron tijorat platformalari mijozlarga qulaylik yaratish bilan birga, xavfsizlik masalalariga ham alohida e’tibor qaratishi zarur bo‘lib qolmoqda.

Xavfsizlik masalalari nafaqat foydalanuvchilarning shaxsiy ma’lumotlarini himoya qilish, balki ular orasida ishonchni mustahkamlash va raqobatbardoshlikni oshirish uchun ham zarurdir. Ma’lumotlarning buzilishi, kiberhujumlar va firibgarlik holatlari platformalar uchun katta xavf tug‘diradi. Shu bois, xavfsizlik bo‘yicha chuqur tahlil olib borish nafaqat xavf-xatarlarni aniqlash, balki ularning oldini olishga qaratilgan samarali chora-tadbirlarni ishlab chiqish imkonini beradi.

Adabiyotlar sharhi. Elektron tijorat platformalarining xavfsizlik jihatlari tahlil qilinishi zarur, chunki bu jarayon bir qator muhim sabablarni o‘z ichiga oladi:

1. Ma’lumotlarning maxfiyligi va yaxlitligi[23]. Elektron tijoratda ma’lumotlar, masalan, mijozlarning shaxsiy va moliyaviy ma’lumotlari, doimiy ravishda xavf ostida bo‘ladi. Xavfsizlik modellarini tahlil qilish orqali ma’lumotlarning maxfiyligini ta’minlash va ularni ruxsatsiz kirishdan himoya qilish mumkin. Bu, o‘z navbatida, mijozlar ishonchini oshiradi va platformaning obro‘sini saqlab qolishga yordam beradi.

2. Tahdidlar va hujumlar. Elektron tijorat platformalari turli xil tahdidlarga duch keladi, jumladan, kiberhujumlar, viruslar va boshqa zararli dasturlar[24]. Xavfsizlik jihatlarini tahlil qilish orqali bu tahdidlarga qarshi samarali himoya choralarini ishlab chiqish mumkin bo‘ladi.

[23] Maxmudov L.U. Xizmat ko‘rsatish sohasida elektron tijorat operatsiyalarini amalga oshirishning konseptual modellari. /https://cyberleninka.ru/article/n/xizmat-ko-rsatish-sohasida-elektron-tijorat-operatsiyalarini-amalga-oshirishning-konseptual-modellari/viewer

[24] https://srcyrl.goldenwellgermany.com/news/risks-and-avoidance-of-my-country-s-foreign-tr-68900033.html

3. Huquqiy va tartibga solish masalalari. O‘zbekistonda elektron tijoratni tartibga soluvchi qonunlar mavjud bo‘lsa-da, ularda hali ham bo‘shliqlar mavjud[25]. Xavfsizlik jihatlarini tahlil qilish orqali qonunchilikni takomillashtirish va yangi xavfsizlik standartlarini joriy etish uchun zarur bo‘lgan tavsiyalar ishlab chiqilishi mumkin.

4. Mijozlar ishonchi. Mijozlar onlayn xarid qilishda xavfsizlikni birinchi o‘ringa qo‘yadilar. Agar platforma xavfsizlikni ta’minlasa, bu mijozlarning ishonchini oshiradi va xarid qilish faoliyatini kengaytiradi[26]. Tahlil natijalari asosida mijozlarni xabardor qilish va ularning xavfsizligini ta’minlash uchun strategiyalar ishlab chiqilishi mumkin.

5. Raqobatbardoshlik. Hozirgi raqobat yuqori bo‘lgan bozor sharoitida elektron tijorat platformalari o‘z xavfsizlik darajalarini oshirish orqali raqobat ustunligini qo‘lga kiritishi mumkin[27]. Tahlil qilish orqali eng yaxshi amaliyotlarni aniqlash va joriy etish mumkin. Elektron tijorat platformalarining xavfsizlik jihatlarini tahlil qilish nafaqat ma’lumotlarni himoya qilish, balki biznesning muvaffaqiyatli ishlashi uchun ham muhimdir. Bu jarayon orqali xavf-xatarlarni aniqlash, mijoz ishonchini oshirish va raqobatbardoshlikni ta’minlash mumkin bo‘ladi.

O‘zbekistonda elektron tijoratni tartibga soluvchi qonunchilikning rivojlanayotganiga qaramay, xavfsizlik masalalarida hali ko‘plab bo‘shliqlar mavjud. Ushbu maqola elektron tijorat platformalarining xavfsizlik jihatlarini tahlil qilish, asosiy tahdidlar va himoya choralarini aniqlash hamda O‘zbekiston sharoitida xavfsizlik tizimlarini takomillashtirish bo‘yicha tavsiyalar ishlab chiqishga qaratilgan. Tadqiqotda kiberxavfsizlikning zamonaviy texnologiyalari, huquqiy asoslar va foydalanuvchilarning raqamli savodxonligini oshirish masalalari muhokama qilinadi.

Tadqiqot metodologiyasi. Ushbu tadqiqotda elektron tijorat platformalarining xavfsizlik jihatlarini tahlil qilish uchun kompleks metodologik yondashuv qo‘llanildi. Asosiy metod sifatida tahliliy va tasniflash yondashuvlari ishlatildi, bu esa kiberxavfsizlik tahdidlarini turlarga ajratish va ularning platformalarga ta’sirini baholash imkonini berdi. Xavfsizlik tizimlarini baholashda funksionallik, joylashuv va ishlash prinsipi bo‘yicha tasniflash amalga oshirildi, bu tizimlarning samaradorligini aniqlashga xizmat qildi. Tadqiqotda shifrlash protokollari (SSL/TLS), ko‘p faktorli autentifikatsiya, to‘lov shlyuzlari va boshqa xavfsizlik choralarining texnik xususiyatlari tahlil qilindi. O‘zbekistonda xavfsizlik masalalarini o‘rganish uchun normativ-huquqiy hujjatlar, xususan, “Elektron tijorat to‘g‘risida”gi Qonun va shaxsiy ma’lumotlarni himoya qilish bo‘yicha qonunchilik tahlil qilindi. Bundan tashqari, global miqyosda qo‘llaniladigan xavfsizlik standartlari (masalan, PCI DSS) va ularning O‘zbekiston sharoitida qo‘llanilishi ko‘rib chiqildi. Ma’lumotlar manbai sifatida ilmiy adabiyotlar, statistik ma’lumotlar va elektron tijorat platformalarining amaliy

[25] Mustafayeva F.Sh. O‘zbekistonda elektron tijorat tizimlari qo‘llanilishining joriy holatini tahlil qilish (“foton” aj misolida). Raqamli iqtisodiyot (Цифровая экономика). / 2024 / https://cyberleninka.ru/article/n/o-zbekistonda-elektron-tijorat-tizimlari-qo-llanilishining-joriy-holatini-tahlil-qilish-foton-aj-misolida

[26] https://sciencebox.uz/index.php/sjeg/article/view/5237

[27] Mustafayeva F.Sh. O‘zbekistonda elektron tijorat tizimlari qo‘llanilishining joriy holatini tahlil qilish (“foton” aj misolida). Raqamli iqtisodiyot (Цифровая экономика). / 2024 / https://cyberleninka.ru/article/n/o-zbekistonda-elektron-tijorat-tizimlari-qo-llanilishining-joriy-holatini-tahlil-qilish-foton-aj-misolida

tajribalari (masalan, Uzum Market, Click, PayMe) ishlatildi. Foydalanuvchilar xavfsizligini ta’minlash bo‘yicha tavsiyalar ishlab chiqishda xaridorlarning raqamli savodxonligini oshirish va kiberxavfsizlik bo‘yicha treninglarning ahamiyati alohida e’tiborga olindi. Ushbu metodlarning kombinatsiyasi orqali elektron tijorat platformalarining xavfsizlik jihatlari chuqur tahlil qilinib, O‘zbekistonda sohani rivojlantirish uchun amaliy yechimlar taklif etildi.

Tahlil va natijalar. Tahdidlar kiber jinoyatchilar tomonidan amalga oshiriladigan hujumlar va firibgarliklarni o‘z ichiga oladi. Quyida elektron tijoratda ko‘p uchraydigan asosiy tahdidlar batafsil keltirilgan:

1. Hisobni qo‘lga olish (Account Take Over - ATO). ATO foydalanuvchi hisoblarini egallash uchun login ma’lumotlarini o‘g‘irlashni o‘z ichiga oladi. Bu usul orqali jinoyatchilar karta ma’lumotlarini olish yoki foydalanuvchi hisobidan ruxsatsiz xaridlar qilish imkoniyatiga ega bo‘lishadi. “ATO barcha firibgarlik yo‘qotishlarining taxminan 29.8 foizni ga tengdir”[28].

2. Chatbot imposteri. Firibgarlar soxta chatbotlarni yaratib, foydalanuvchilardan shaxsiy ma’lumotlarni olishga harakat qiladilar. Foydalanuvchilar qonuniy va soxta chatbotlar orasidagi farqni ajrata olmaydi. “Bunday firibgarlik harakatlari barcha firibgarliklarning 24.1 foizini tashkil etadi”[29].

3. Orqa eshik fayllari. Kiber jinoyatchilar zararli dasturlarni kiritish uchun eskirgan plaginlar yoki himoyalanmagan kirish nuqtalaridan foydalanadilar. Bu orqali ular kompaniyaning barcha ma’lumotlariga, shu jumladan mijozlarning shaxsiy ma’lumotlariga kirish huquqiga ega bo‘lishadi. “Barcha hujumlarning 6.4 foizni orqa eshik fayllaridan kelib chiqadi”[30].

4. SQL injection. Hujumchilar onlayn shakllar va URL so‘rovlaridan foydalanib, ma’lumotlar bazasiga ruxsatsiz kirishga harakat qiladilar. Bu usul orqali shaxsiy ma’lumotlarni o‘g‘irlash mumkin. “SQL injection hujumlari barcha hujumlarning 8.2 foizni ni tashkil etadi”[31].

5. Saytlararo skript (Cross-Site Scripting - XSS). “XSS hujumlari xakerlarga foydalanuvchi brauzeri orqali boshqa foydalanuvchilar tomonidan ko‘riladigan veb-sahifalarga zararli skriptlarni kiritishga imkon beradi. Bu xakerlarga kirish boshqaruvlarini chetlab o‘tish va shaxsiy ma’lumotlarga kirish imkonini beradi”[32].

6. Ransomware (tovlamachi-viruslar). “Ransomware zararli dasturlari foydalanuvchilarning ma’lumotlarini shifrlab, ularni qaytarish uchun pul talab qiladi. Ushbu viruslar ko‘pincha fishing xatlari orqali tarqatiladi. Tashkilotlarning axborot tizimlariga ruxsatsiz kirish va buzg‘unchilik maqsadida foydalaniladi”[33].

7. IOT qurilmalariga hujum. “Internetga ulangan qurilmalar (masalan, kameralar va sensorlar) orqali amalga oshiriladigan hujumlar, bu qurilmalar ko‘pincha

[28] https://uz.martech.zone/top-ecommerce-attacks-fraud-security/
[29] https://uz.martech.zone/top-ecommerce-attacks-fraud-security/
[30] https://uz.martech.zone/top-ecommerce-attacks-fraud-security/
[31] https://uz.martech.zone/top-ecommerce-attacks-fraud-security/
[32] https://uz.martech.zone/top-ecommerce-attacks-fraud-security/
[33] Akbarova M.R., Akbarov J.M. / Axborot xavfsizligiga bo’ladigan tahdidlar. / "Экономика и социум" №6(85) ч.1 2021// https://cyberleninka.ru/article/n/axborot-xavfsizligiga-bo-ladigan-tahdidlar

xavfsizlik choralariga ega emas. Bu turdagi tahdidlar tashkilotlarning axborot tizimlariga ruxsatsiz kirishga olib kelishi mumkin”[34].

Elektron tijoratdagi tahdidlarni bartaraf etish uchun elektron tijorat kompaniyalari xavfsizlik choralarini kuchaytirishi va foydalanuvchilarga shubhali faoliyatlardan ehtiyot bo‘lishni tavsiya qilishi zarurdir. Xaridorning malakasi elektron tijoratdan xavfsiz foydalanishda muhim ahamiyatga ega. O‘zbekiston hamda boshqa mamlakatlarda ham elektron tijoratning rivojlanishi bilan birga, xaridorlarning raqamli savodxonligi va kiberxavfsizlik bo‘yicha bilimlarini oshirib borish zarur. Malakali xaridorlar onlayn muhitda firibgarlik va kiberhujumlardan o‘zlarini himoya qilishda, to‘g‘ri va ishonchli ma’lumotlarni tanlashda, shuningdek, xavfsiz to‘lov tizimlaridan foydalanishda tajribali bo‘lishadi. Bunday xaridorlar, shuningdek, elektron tijorat platformalarini samarali va xavfsiz ishlatish uchun zarur bo‘lgan texnik ko‘nikmalarga ega bo‘lib, bu esa ularning onlayn xarid qilish tajribasini yaxshilaydi va umumiy xavfsizlikni oshiradi. Shunday qilib, xaridorning malakasi nafaqat individual foydalanuvchining manfaatlariga, balki elektron tijorat ekotizimining barqarorligiga ham ijobiy ta'sir ko‘rsatadi.

[34] Akbarova M.R., Akbarov J.M. / Axborot xavfsizligiga bo’ladigan tahdidlar. / "Экономика и социум" №6(85) ч.1 2021// https://cyberleninka.ru/article/n/axborot-xavfsizligiga-bo-ladigan-tahdidlar

Xavfsizlikni ta’minlovchi texnologiyalar va amaliyotlar	•HTTPS va SSL/TLS sertifikatlari bilan himoyalangan saytlarni tanlash •Ikki faktorli autentifikatsiya (2FA) •Zararli dasturlardan himoya
Parolni boshqarish va hisobni himoyalash	•Kuchli va noyob parollardan foydalanish •Parol menejerlari •Hisob ma’lumotlarini maxfiy saqlash
Ishonchli platformalar va sotuvchilarni tanlash	•Reyting va sharhlarni tekshirish •Taniqli platformalardan foydalanish •Firibgarlikdan ehtiyot bo‘lish
To‘lov jarayonida xavfsizlik choralarini ko‘rish	•Xavfsiz to‘lov usullaridan foydalanish •Virtual kartalar va limitlangan hisoblar •To‘lovlarni tasdiqlash uchun ikki faktorli tizim
Xarid jarayonida e’tiborli bo‘lish	•Sayt manzilini tekshirish •Mahsulotning to‘liq tavsifini o‘qish •Cheklovlarni tushunish
Foydalanuvchilar xabardorligini oshirish	•Kiberxavfsizlik bo‘yicha bilimlarni kengaytirish •Firibgarlik sxemalari haqida ogohlantirishlardan foydalanish •Spam va phishing xabarlardan ehtiyot bo‘lish
Savdolardan so‘nggi choralar	•Hisobni muntazam nazorat qilish •Shikoyat qilish tartibini bilish •Shaxsiy ma’lumotlarni yangilash

1-rasm. Elektron tijoratdan xavfsiz xaridni amalga oshirish mexanizmi

1. **Texnologik xavfsizlik choralarini qo‘llash.** HTTPS va SSL/TLS sertifikatlari bilan himoyalangan saytlar orqali xarid qilish ma’lumotlarning shifrlanishini ta’minlaydi. Masalan, Amazon yoki O‘zbekistondagi Click tizimlari HTTPS protokolidan foydalanadi. Brauzerda “Not secure” belgisi paydo bo‘lsa, bu saytlardan foydalanish tavsiya etilmaydi. Ikki faktorli autentifikatsiya (2FA) tizimi, masalan, PayPal orqali SMS-kod bilan hisobga kirish, hisob xavfsizligini oshiradi.
2. **Parollarni boshqarish va hisob xavfsizligini ta'minlash.** Oddiy parollar (masalan, “12345”) o‘rniga murakkab parollar (“As foizni29_LmtF”) tavsiya etiladi. LastPass yoki 1Password kabi parol menejerlari parollarni xavfsiz saqlash va eslab qolishda yordam beradi. Login va parollarni brauzerda saqlash tavsiya etilmaydi, ayniqsa umumiy kompyuterlarda.
3. **Ishonchli platforma va sotuvchilarni tanlash.** Xariddan avval sotuvchining reytingi va mijozlar sharhlarini o‘rganish lozim. Masalan, AliExpressda xarid qilishdan oldin izohlar orqali firibgarlik xavfini kamaytirish mumkin. Bozor narxidan ancha arzon mahsulotlar, masalan, $150 evaziga iPhone 15 taklif etilishi firibgarlik belgisi bo‘lishi mumkin.

4. **To‘lov xavfsizligini ta’minlash.** Visa, MasterCard kabi ishonchli to‘lov tizimlari orqali to‘lovlar amalga oshirilganda tranzaksiya himoyasi va mablag‘ni qaytarib olish imkoniyati mavjud. Virtual kartalardan (Kapitalbank, Humo) foydalanish asosiy hisobni himoyalaydi. Click yoki PayMe kabi tizimlar orqali ikki faktorli tasdiqlash foydalidir.

5. **Xarid jarayonida ehtiyotkorlik.** Sayt manzillarining aniqligiga e’tibor berish zarur. Masalan, “www.amazonn.com” kabi qalbaki manzillar asl saytdan farqlanadi. Tovar tavsifi va kafolat shartlarini diqqat bilan o‘rganish, sotuvchining qaytarib berish siyosatini tushunish muhim.

6. **Foydalanuvchilar xabardorligini oshirish.** Google Security Checkup kabi xizmatlar hisob xavfsizligini baholashda yordam beradi. Davlat xavfsizlik organlarining ogohlantirishlari, spam va fishing xabarlardan ehtiyot bo‘lish, kiberjinoyatlarning oldini olishga xizmat qiladi.

7. **Xariddan so‘nggi nazorat choralari.** Bank hisobini muntazam tekshirib borish, shubhali tranzaksiyalar aniqlansa zudlik bilan bankka murojaat qilish lozim. Firibgarlik holatida PayPal yoki Click orqali shikoyat yuborish va mablag‘ni qaytarish imkoniyati mavjud. Login va parollarni davriy yangilab borish shaxsiy ma’lumotlarning xavfsizligini oshiradi.

Elektron tijorat platformalarining xavfsizlik jihatlarini mustahkamlash iqtisodiy samaradorlikka bir qator ijobiy ta'sir ko‘rsatadi. Birinchidan, xavfsizlikni ta’minlash xaridorlar o‘rtasida ishonchni oshiradi, bu esa onlayn xaridlarni ko‘paytiradi va sotuvlarning o‘sishiga olib keladi. Xaridorlar xavfsiz muhitda xarid qilishni afzal ko‘rishadi, bu esa kompaniyalarni raqobatbardosh qilishga yordam beradi. Ikkinchidan, mustahkam xavfsizlik choralari kiberjinoyatlardan himoya qiladi, bu esa moliyaviy yo‘qotishlarni kamaytiradi. Kiberhujumlar natijasida yuzaga keladigan zararlar, masalan, ma’lumotlarning o‘g‘irlanishi yoki moliyaviy firibgarlik, kompaniyalar uchun katta iqtisodiy xarajatlarni keltirib chiqarishi mumkin. Bunday yo‘qotishlarni oldini olish orqali kompaniyalar o‘z resurslarini samarali ravishda rivojlantirishga yo‘naltirishi mumkin bo‘ladi. Uchinchidan, xavfsizlikning yuqori darajasi kompaniyaning obro‘sini oshiradi va brend sodiqligini kuchaytiradi. Mijozlar ishonchli va xavfsiz xizmatlardan foydalanishni afzal ko‘radilar, bu esa takroriy xaridlarni rag‘batlantiradi va mijozlar bazasini kengaytiradi. Natijada, elektron tijorat platformalarining xavfsizlik jihatlarini mustahkamlash iqtisodiy samaradorlikni oshirishga, raqobatbardoshlikni kuchaytirishga va moliyaviy yo‘qotishlarni kamaytirishga yordam beradi.

Elektron tijorat platformalarining xavfsizligiga tahdidlar xilma-xil shakllar va ko‘rinishlarda namoyon bo‘lib, ularning har biri platformalarning barqaror faoliyatiga va foydalanuvchilarning ma’lumotlariga jiddiy zarar yetkazishi mumkin. Tahdidlarni tahlil qilishda ularni asosiy turlarga bo‘lish imkonini beruvchi klassifikatsiya muhim ahamiyatga ega.

1-jadval

Elektron tijoratdagi asosiy tahdidlar turlari

№	Turkumlar	Turlari	Tavsifi
1.	Ma’lumotlarga tahdidlar[35]	Ma’lumotlarni o‘g‘irlash	Buzg‘unchilar kredit karta raqamlari, manzillar, parollar va h.k. kabi nozik ma’lumotlarni o‘g‘irlash uchun mijozlar ma’lumotlar bazasiga kirishga intiladi.
		To‘lov firibgarligi	Kiberjinoyatchilar mijozlarni aldash va ularning to‘lov mablag‘lariga ruxsatsiz kirish uchun turli usullardan foydalanadilar.
		Fishing	Buzg‘unchilar foydalanuvchilarni aldash maqsadida qonuniy onlayn-do‘konlarga taqlid qiluvchi soxta veb-saytlarni yaratadilar.
2.	Mavjudlikka tahdidlar[36]	DDoS hujumlari	Xizmatni rad etishning taqsimlangan hujumlari onlayn-do‘kon serverlarini ortiqcha yuklashga qaratilgan bo‘lib, bu sayt xizmati foydalanuvchilar uchun mavjud bo‘lmasligiga olib keladi.
		Zararli dasturlar	Buzg‘unchilar onlayn-do‘kon serverlariga saytni buzishi yoki keyingi hujumlar uchun ishlatilishi mumkin bo‘lgan zararli dasturlar bilan zararlanishi mumkin.
3.	Yaxlitlikka tahdidlar[37]	SQL in’ektsiyalari	Buzg‘unchilar ma’lumotlar bazasiga ruxsatsiz kirish uchun veb-sayt ma’lumotlarini kiritish shakllariga zararli kodni kiritishlari mumkin.
		Saytlararo skript (XSS)	Bu hujum tajovuzkorlarga foydalanuvchi ma’lumotlarini o‘g‘irlash yoki boshqa zararli harakatlarni amalga oshirish uchun veb-sahifalarga kod kiritish imkonini beradi.

Yuqoridagi ro‘yxatda ko‘rib turganingizdek, elektron tijorat platformalari uchun xavfsizlik tahdidlari xilma-xil va doimiy ravishda rivojlanib bormoqda. Ushbu tahdidlardan muvaffaqiyatli himoyalanish uchun texnik xavfsizlik choralarini ham, tashkiliy va huquqiy choralarni ham o‘z ichiga olgan kompleks yechim talab qilinadi.

Elektron tijorat murakkab ekotizim bo‘lib, unda xaridorlar, sotuvchilar va to‘lov protsessorlari o‘zaro ta’sir qiladi. Bunda, xavfsizlik tahdidlarini bir nechta mezonlar bo‘yicha tasniflash mumkin.

2-jadval

Elektron tijoratning xavfsizlikka tahdid guruhlari tasnifi

Kategoriya	Tur	Tavsif
Rejalashtirilishi bo‘yicha	Qasddan bo‘lmagan tahdidlar	Texnik nosozliklar yoki foydalanuvchi xatolari (masalan, server ishlamay qolishi)
	Qasddan qilingan tahdidlar	DDoS hujumlari kabi ataylab qilingan zararli harakatlar
Manbasi bo‘yicha	Ichki tahdidlar	Xodimlarning beparvoligi yoki ma’lumot o‘g‘irlash kabi harakatlari

[35] Оладько В.С. Угрозы информационной безопасности в системах электронной коммерции. Экономика и социум. 2015. / https://cyberleninka.ru/article/n/ugrozy-informatsionnoy-bezopasnosti-v-sistemah-elektronnoy-kommertsii
[36] https://www.ptsecurity.com/ru-ru/research/analytics/information-security-threats-in-ecommerce/
[37] https://www.ptsecurity.com/ru-ru/research/analytics/retail-cybersecurity-threatscape-2023/

	Tashqi tahdidlar	Fishing, zararli dasturlar, DDoS hujumlari va firibgarlik
Maqsadi bo‘yicha	Moliyaviy	Soxta tranzaksiyalar va to‘lov ma’lumotlarini o‘g‘irlash
	Obro‘-e’tiborga tahdid	Mijoz ma’lumotlari buzilishi yoki xizmatdagi uzilishlar
	Operatsion	Texnik nosozliklar va xizmatni rad etish hujumlari (DDoS)
Usullari bo‘yicha	Ijtimoiy muhandislik	Fishing va manipulyatsiya orqali tizimga ruxsatsiz kirish
	Texnik hujumlar	Viruslar, troyanlar va zararli dasturlar orqali tizimga zarar yetkazish

Elektron tijorat platformalarining xavfsizlik tizimlari turli tahdidlarga qarshi himoya qilish uchun keng qamrovli va ko‘p qatlamli yondashuvlardan foydalanadi. Bu tizimlar nafaqat texnik jihatdan, balki tashkiliy va operatsion xavfsizlikni ham o‘z ichiga oladi. Shunday qilib, elektron tijorat platformalari uchun xavfsizlik tizimlari bir nechta mezonlarga ko‘ra tasniflanishi mumkin.

1. Funksionalligi bo‘yicha. ***Xujumlarni oldini olish tizimlari (IPS):*** tarmoq trafigini tahlil qilib, xakerlik urinishlari, portlarni skanerlash va boshqa hujumlar kabi shubhali harakatlarni bloklashga qaratilgan bo‘ladi. ***Xujumlarni aniqlash tizimlari (IDS):*** tarmoqni passiv ravishda kuzatib borib, potentsial tahdidlar haqida ogohlantiradi. ***Fayervollar:*** kiruvchi va chiquvchi tarmoq trafigini boshqaradi, ruxsatsiz kirishni bloklaydi. ***Veb zaiflikdan himoya qilish (WAF) tizimlari:*** veb-ilovalarni SQL injection, XSS va boshqalar kabi keng tarqalgan hujumlardan himoya qiladi. ***Anomaliyalarni aniqlash tizimlari:*** foydalanuvchilar va tizimlarning xatti-harakatlarini tahlil qilib, normal sharoitlardan og‘ishlarni aniqlaydi. ***DDoS hujumidan himoya qilish tizimlari:*** serverlarni haddan tashqari yuklanishiga va ularni ishlamay qolishiga qaratilgan tarqatilgan hujumlardan himoya qiladi.

2. Joylashuvi bo‘yicha. ***Tarmoq:*** tarmoq perimetri va serverlarini himoya qiladi. ***Xost:*** shaxsiy serverlar va ish stantsiyalarida o‘rnatilgan bo‘ladi. ***Bulutli:*** xizmat sifatida taqdim etiladi va bulutli infratuzilmalarni himoya qilish imkonini beradi.

3. Ishlash prinsipiga ko‘ra. ***Faol:*** real vaqtda tahdidlarni bloklashga qaratilgan ximoya tizimlari bo‘ladi. ***Passiv:*** tarmoqni kuzatib boradi va ogohlantiradi.

Maksimal himoyani ta’minlash uchun turli xil texnik va tashkiliy chora-tadbirlarni o‘z ichiga olgan kompleks yondashuvdan foydalanish kerak. Tahdidlarni muntazam tahlil qilish va xavfsizlik tizimini o‘zgaruvchan sharoitlarga moslashtirish muvaffaqiyatning asosiy omillari hisoblanadi.

Elektron tijorat platformalaridagi xavfsizlik tizimlari foydalanuvchi ma’lumotlarini, moliyaviy operatsiyalarni va biznesdagi obro‘sini himoya qilishda asosiy rol o‘ynaydi. Kibertahdidlar va firibgarlikning kuchayishi bilan samarali xavfsizlik tizimlari zaruratga aylanib bormoqda. Quyida elektron tijoratda foydalaniladigan xavfsizlik tizimlarining asosiy turlari, shuningdek, ularning funksional xususiyatlari keltirilgan.

1. Shifrlash protokollari. Secure Sockets Layer (SSL) va Transport Layer Security (TLS) protokollari mijoz va server o‘rtasida uzatiladigan ma’lumotlarni

shifrlashni ta’minlaydi. Bu karta raqamlari va foydalanuvchi shaxsiy ma’lumotlari kabi nozik ma’lumotlarini ushlashdan himoya qiladi. Barcha zamonaviy onlayn-do‘konlar HTTPS (xavfsiz HTTP) dan foydalanishi kerak, bu veb-trafikni himoya qilish uchun standart protokoldir.

2. To‘lov shlyuzlari. PayPal yoki Stripe kabi to‘lov shlyuzlari ma’lumotlarning buzilishi xavfini minimallashtirib, xavfsiz to‘lovlarni qayta ishlashni taklif qiladi. Ushbu tizimlar shifrlash va tokenizatsiyani o‘z ichiga olgan ko‘p qatlamli xavfsizlik mexanizmlaridan foydalanadi. Uchinchi tomon to‘lov shlyuzlaridan foydalanishda karta ma’lumotlarini o‘z serverlarida saqlashdan qochish imkonini beradi, bu esa o‘g‘rilik xavfini kamaytiradi.

3. Ko‘p faktorli autentifikatsiya (MFA). Ko‘p faktorli autentifikatsiya foydalanuvchilardan hisobga kirishdan oldin bir nechta identifikatsiya shakllarini taqdim etishlarini talab qiladi. Bu parollar, SMS kodlari yoki biometrik ma’lumotlarni o‘z ichiga olishi mumkin. Ko‘pgina e-tijorat platformalari foydalanuvchi hisoblarini ruxsatsiz kirishdan himoya qilish uchun MFAni qo‘llaydi.

4. Antivirus dasturlari va ruxsatsiz kirishni oldini olish tizimlari (IPS). Antivirus dasturlari tizimlarni zararli dasturlardan himoya qiladi va IPS tarmoq trafigini shubhali harakatlar uchun nazorat qiladi hamda real vaqtda hujumlarning oldini oladi. Antivirus yechimlari va IPS-dan foydalanish onlayn-do‘kon serverlarini DDoS yoki SQL injectionlari kabi hujumlardan himoya qilishga yordam beradi.

5. Fayervollar. Fayervollar kiruvchi va chiquvchi trafikni nazorat qiladi, potentsial xavfli ulanishlarni filtrlaydi. Ular apparat yoki dasturiy ta’minot bo‘lishi mumkin. E-tijorat serverlarida xavfsizlik devorlarini sozlash ichki tizimlarga ruxsatsiz kirishni oldini olishga yordam beradi.

6. Xodimlar va mijozlarni o‘qitish. Xodimlarni kiberxavfsizlik asoslariga o‘rgatish, mijozlarni fishing xatarlari va boshqa tahdidlar haqida xabardor qilish ham xavfsizlik tizimining muhim qismidir. Fishing hujumlarini aniqlash bo‘yicha xodimlarni muntazam ravishda o‘qitish ma’lumotlar sizib chiqishi xavfini sezilarli darajada kamaytiradi.

7. Tartibga solish va muvofiqlik. PCI DSS (Payment Card Industry Data Security Standard) kabi xalqaro ma’lumotlar xavfsizligi standartlariga muvofiqlik to‘lov ma’lumotlarini himoya qilish uchun zarur. E-tijorat kompaniyalari PCI DSS talablariga muvofiqligini tasdiqlash uchun muntazam tekshiruvdan o‘tishi kerak.

Xulosa va takliflar. Kiberjinoyatlar ko‘payishi va mijoz ishonchini saqlash zarurati platformalar uchun xavfsizlikni ustuvor vazifa etib belgilaydi. Ishonchli muhit yaratish nafaqat platformalar, balki foydalanuvchilar uchun ham muhim, chunki ularning e’tiborsizligi moliyaviy yo‘qotishlarga olib kelishi mumkin. Shu bilan birga, elektron tijoratni tartibga soluvchi huquqiy bazani takomillashtirish ham dolzarb masalalardan biridir.

Xavfsizlikni ta’minlash uchun platformalar shifrlash texnologiyalaridan foydalanishi, ikki faktorli autentifikatsiya va kuchli parol tizimlarini joriy qilishi, muntazam yangilanishlarni amalga oshirishi lozim. Xaridorlarni firibgarliklardan himoya qilish uchun ularni xabardor qilish va zarur maslahatlar berish ham samarali

choradir. Elektron tijoratning barqaror rivojlanishi xavfsizlik choralariga bevosita bog‘liq bo‘lib, bu nafaqat platformalar, balki butun sohaning ishonchliligini oshiradi.

3-jadval

Elektron tijorat foydalanuvchilari eng ko‘p duch kelishi mumkin bo‘lgan tahdidlar[38]

№	Tahdidlar guruhlari	Tahdidlar turlari	Tavsifi
1.	**Ma’lumotlarning o‘g‘irlanishi va shaxsiy xavfsizlikka tahdidlar**	**Shaxsiy ma’lumotlarning o‘g‘irlanishi**	Xaridorning ism-sharifi, manzili, telefon raqami kabi ma’lumotlar xavfsizlik devorlarining buzilishi yoki fishing hujumlari natijasida o‘g‘irlanishi mumkin.
		Moliyaviy ma’lumotlarning buzilishi	Karta raqamlari, bank hisoblari yoki elektron hamyon ma’lumotlari firibgarlik uchun asosiy nishonga aylanishi mumkin.
		Shaxsiy hayotga tajovuz	Xaridorning xaridlar tarixini kuzatish yoki ma’lumotlarni reklama maqsadida noqonuniy ishlatish.
2.	**Firibgarlik va soxta operatsiyalar**	**Fishing (soxta veb-saytlar)**	Xaridorni haqiqiy platformadan farq qilmaydigan soxta saytga yo‘naltirish orqali login va parollarni o‘g‘irlash.
		Qalbaki to‘lov sahifalari	To‘lov paytida haqiqiy emas, soxta tizimlarga yo‘naltirilish.
		Qalbaki tovarlar va xizmatlar	Ishonchsiz sotuvchilar tomonidan sifatli tovarlar nomidan sifatsiz yoki mavjud bo‘lmagan tovarlar taklif qilinishi.
		To‘lovlar qaytarilmasligi	Xaridor pulni to‘laganidan keyin tovar yoki xizmatni olmasligi va pullarni qaytarib ololmasligi.
3.	**Tizim va texnologik tahdidlar**	**Kiberhujumlar va xakerlik**	Elektron tijorat platformalariga qarshi kiberhujumlar, masalan, DDoS hujumlar orqali tizimlarning ishdan chiqishi yoki ma’lumotlarning buzilishi.
		Texnologik nosozliklar	To‘lov tizimlarida yoki platforma infratuzilmasida yuzaga kelgan muammolar, ma’lumotlarning yo‘qolishiga olib kelishi mumkin.
		Zararli dasturlar	Xaridor qurilmalariga zarar yetkazadigan viruslar yoki troyan dasturlar orqali ma’lumotlarni o‘g‘irlash.
4.	**Yetkazib berish va kafolat bilan bog‘liq muammolar**	**Sifatsiz yoki noto‘g‘ri tovar yetkazib berish**	Xaridor tomonidan buyurtma qilingan tovarning sifat yoki miqdor jihatdan talabga javob bermasligi.
		Yetkazib berilmagan tovarlar	To‘lov amalga oshirilgan bo‘lsa ham, tovar yetkazilmasligi.
		Kafolat va qo‘llab-quvvatlashning yetarli emasligi	Xaridorlar muammoga duch kelganida platforma tomonidan yordam yoki muammo hal qilinmasligi.

[38] Ma’lumotlar asosida muallif tomonidan ishlab chiqildi

5.	**Xaridorlarni chalg‘ituvchi axborot va noto‘g‘ri baholashlar**	**Noto‘g‘ri yoki yolg‘on ma’lumotlar**	Tovar yoki xizmatning real tavsifi bilan mos kelmaydigan axborot berilishi.
		Reklama va baholar bilan aldash	Tovarlar haqida soxta ijobiy baholar berilishi yoki kamchiliklarni yashirish uchun yolg‘on reklama ma’lumotlarining taqdim etilishi.
6.	**Huquqiy va siyosiy tahdidlar**	**Xalqaro operatsiyalar bilan bog‘liq muammolar**	Turli mamlakatlarda xarid qilishda bojxona qoidalari yoki soliqlar bilan bog‘liq murakkabliklar.
		Huquqiy himoya yo‘qligi	Xaridorning qonuniy huquqlarini himoya qiluvchi mexanizmlarning mavjud emasligi yoki samarali ishlamasligi.
7.	**Ijtimoiy va psixologik tahdidlar**	**Ijtimoiy muammolar**	Xarid qilish jarayonida manipulyatsiya qiluvchi reklama texnologiyalari sabab xaridor o‘zi istamagan narsani xarid qilishga majbur bo‘lishi.
		Psixologik bosim	Foydalanuvchining qarorlarini boshqarish uchun yaratilgan sun'iy chegirmalar yoki vaqt cheklovlari orqali xarid qilishga majbur qilish.

Ushbu barcha tahdidlar elektron tijoratda foydalanuvchilar xavfsizligini ta’minlashga bo‘lgan ehtiyojni oshiradi va bu borada xavfsizlik choralarini kuchaytirish muhimligini ta'kidlaydi.

Xaridorlar o‘zlarini tahdidlardan himoya qilish uchun ehtiyotkorlik choralarini ko‘rishi zarur. Shu bilan birga, platformalar o‘z mijozlariga xavfsiz muhit yaratishni ustuvor vazifa qilib belgilashlari kerak. Kiberxavfsizlik sohasidagi islohotlar va ilg‘or texnologiyalarni joriy etish elektron tijoratning barqaror rivojlanishiga xizmat qiladi.

Foydalanilgan adabiyotlar ro‘yxati

1. Akbarova M.R., Akbarov J.M. Axborot xavfsizligiga bo‘ladigan tahdidlar / M.R. Akbarova, J.M. Akbarov // Экономика и социум. – 2021. – №6(85), ч.1. – URL: https://cyberleninka.ru/article/n/axborot-xavfsizligiga-bo-ladigan-tahdidlar.

2. Maxmudov L.U. Xizmat ko‘rsatish sohasida elektron tijorat operatsiyalarini amalga oshirishning konseptual modellari / L.U. Maxmudov // Raqamli iqtisodiyot. – 2024. – URL: https://cyberleninka.ru/article/n/xizmat-ko-rsatish-sohasida-elektron-tijorat-operatsiyalarini-amalga-oshirishning-konseptual-modellari/viewer.

3. Mustafayeva F.Sh. O‘zbekistonda elektron tijorat tizimlari qo‘llanilishining joriy holatini tahlil qilish (“Foton” AJ misolida) / F.Sh. Mustafayeva // Raqamli iqtisodiyot (Цифровая экономика). – 2024. – URL: https://cyberleninka.ru/article/n/o-zbekistonda-elektron-tijorat-tizimlari-qo-llanilishining-joriy-holatini-tahlil-qilish-foton-aj-misolida.

4. Оладько В.С. Угрозы информационной безопасности в системах электронной коммерции / В.С. Оладько // Экономика и социум. – 2015. – №2(15). – URL: https://cyberleninka.ru/article/n/ugrozy-informatsionnoy-bezopasnosti-v-sistemah-elektronnoy-kommertsii.

5. Risks and avoidance of my country’s foreign trade e-commerce platform under cross-border e-commerce model / Goldenwell Germany. – 2024. – URL:

https://srcyrl.goldenwellgermany.com/news/risks-and-avoidance-of-my-country-s-foreign-tr-68900033.html.

6. Top e-commerce attacks, fraud, and security / Martech Zone. – 2024. – URL: https://uz.martech.zone/top-ecommerce-attacks-fraud-security/.

7. Uslubiy qo‘llanma: O‘zbekiston Respublikasida raqamli iqtisodiyotni rivojlantirishning dolzarb masalalari / ScienceBox. – 2023. – URL: https://sciencebox.uz/index.php/sjeg/article/view/5237.

8. Информационная безопасность в электронной коммерции / Positive Technologies. – 2023. – URL: https://www.ptsecurity.com/ru-ru/research/analytics/information-security-threats-in-ecommerce/.

9. Киберугрозы в розничной торговле 2023 / Positive Technologies. – 2023. – URL: https://www.ptsecurity.com/ru-ru/research/analytics/retail-cybersecurity-threatscape-2023/.