ELEKTRON TIJORATDA AXBOROT XAVFSIZLIGINI TA’MINLASh USULLARI

Doniyorov Shoxrux Rustamovich
O‘zbekiston Respublikasi Vazirlar Mahkamasi huzuridagi "Biznes va tadbirkorlik oliy maktabi" magistr tinglovchisi

Annotatsiya: *Elektron tijorat platformalarida axborot xavfsizligi nafaqat texnik muhofaza, balki boshqaruv, huquqiy muvofiqlik va inson omilini qamrab oladigan kompleks tizim sifatida qaralishi zarur. Maqolada elektron tijoratda axborot xavfsizligini ta’minlashning asosiy usullari riskka asoslangan yondashuvda tizimlashtirildi. Tadqiqotda xalqaro me’yoriy yondashuvlar (ISMS, kiberbarqarorlik funksiyalari, veb-ilova risklari, to‘lov ma’lumotlari xavfsizligi) qiyosiy tahlil qilindi hamda elektron tijorat uchun “qatlamli himoya” (defense-in-depth) modeli asosida tavsiyalar ishlab chiqildi. Natijada tashkilot darajasidagi boshqaruv mexanizmlari, texnik nazorat choralari (kriptografiya, autentifikatsiya, jurnallash, monitoring, segmentatsiya), operatsion tayyorgarlik (insidentlarga javob, rezerv nusxa, tiklash) va ta’minot zanjiri xavflarini kamaytirish bo‘yicha amaliy yo‘l xaritasi taklif etildi. Maqola elektron tijorat sub’ektlari uchun xavfsizlikni baholash indikatorlari va joriy etish bosqichlarini belgilashda uslubiy asos bo‘lib xizmat qiladi.*

Kalit so‘zlar: *elektron tijorat, axborot xavfsizligi, risk-menejment, ISO/IEC 27001, NIST CSF 2.0, OWASP Top 10, PCI DSS, kriptografiya, mnogofaktorli autentifikatsiya, insident menejmenti.*

Annotation: *Information security in e-commerce should be treated as an integrated system that combines technical controls, governance mechanisms, legal compliance, and human factors. This article systematizes key methods for ensuring information security in e-commerce through a risk-based approach. The study compares widely used international frameworks for information security management, cybersecurity functions, web application risks, and payment-data protection, and proposes a defense-in-depth model tailored to e-commerce environments. The results include practical recommendations covering organizational governance, technical safeguards (cryptography, authentication, logging, monitoring, segmentation), operational readiness (incident response, backup, recovery), and supply-chain risk reduction. An implementation roadmap and evaluation indicators are suggested to support phased deployment and continuous improvement. The article can serve as a methodological basis for e-commerce entities to prioritize controls, assess maturity, and strengthen cyber resilience.*

Keywords: *e-commerce, information security, risk management, ISO/IEC 27001, NIST CSF 2.0, OWASP Top 10, PCI DSS, cryptography, multi-factor authentication, incident response.*

Kirish

Elektron tijorat raqamli iqtisodiyotning tez o‘sib borayotgan segmenti sifatida katta hajmdagi ma’lumotlar aylanmasiga tayanadi. Onlayn savdo jarayonida mijozning shaxsiy ma’lumotlari, to‘lov rekvizitlari, buyurtma tarixi, logistika ma’lumotlari, marketing analitikasi va idora etish panellari orqali yuritiladigan xizmat ma’lumotlari kabi turli toifadagi axborot aktivlari shakllanadi va saqlanadi. Shu sababli elektron tijorat tizimlari kiberxujumlar uchun yuqori qiymatli nishon hisoblanadi: ma’lumotlarni o‘g‘irlash, akkauntlarni egallab olish, to‘lovlarda firibgarlik, veb-ilova va API orqali zaifliklardan foydalanish, ta’minot zanjiri orqali zararli kod kirishi, DDoS hujumlari tufayli xizmat ko‘rsatishning izdan chiqishi kabi holatlar biznesning moliyaviy barqarorligi va obro‘siga bevosita ta’sir ko‘rsatadi.

Amaliyotda axborot xavfsizligi faqat texnik vositalar majmuasi emas, balki boshqaruv, huquqiy muvofiqlik, inson omili va operatsion tayyorgarlikni birlashtiruvchi kompleks tizim sifatida qaralishi zarur. Mazkur maqolada elektron tijoratda axborot xavfsizligini ta’minlash usullari riskka asoslangan yondashuv nuqtai nazaridan tizimlashtiriladi hamda qatlamli himoya (defense-in-depth) tamoyili asosida joriy etishga yo‘naltirilgan amaliy tavsiyalar bayon qilinadi.

Elektron tijoratda axborot xavfsizligi, avvalo, maxfiylik, yaxlitlik va mavjudlik tamoyillarini ta’minlashga qaratilgan bo‘lishi kerak. Maxfiylik mijoz ma’lumotlarining ruxsatsiz oshkor bo‘lishini cheklashni, yaxlitlik buyurtma, to‘lov va narxlarga oid ma’lumotlar buzilmasdan saqlanishini, mavjudlik esa platforma uzluksiz ishlashini anglatadi. Shu uch tamoyil elektron tijoratda risklarni boshqarish uchun mezon vazifasini bajaradi. Risk odatda tahdid, zaiflik va oqibat (ta’sir) o‘zaro ko‘payishi natijasida yuzaga keladi, demak xavfsizlikni ta’minlashning to‘g‘ri yo‘li zaifliklarni kamaytirish, tahdidlarni erta aniqlash va oqibatni cheklash choralarini bir vaqtning o‘zida qo‘llashdan iborat. Bunday yondashuvda xalqaro amaliyotda qabul qilingan kiberbarqarorlik funksiyalari va axborot xavfsizligi menejmenti tizimiga tayanish maqsadga muvofiq, chunki ular xavfsizlikni boshqaruvdan tortib texnik nazoratlargacha bo‘lgan butun siklda tashkil etishga yordam beradi.

Tashkiliy darajada elektron tijorat sub’ektlari axborot aktivlarini aniq ro‘yxatga olishi, ma’lumotlarni toifalarga ajratishi va himoya darajalarini belgilashi lozim. Bu jarayonda axborot xavfsizligi siyosati, rollar va javobgarliklar, minimal huquq (least privilege)

tamoyili, kirish huquqlarini berish-olish tartiblari, parol va autentifikatsiya talablari, jurnallash va monitoring qoidalari rasmiylashtiriladi. Xavfsizlikni faqat IT bo‘limi zimmasiga yuklash amalda samara bermaydi; elektron tijoratda xavfsizlik biznes-protsessning o‘z ichiga kiritilgan qismi bo‘lishi kerak. Shuning uchun xavflarni baholash, ustuvor risklarni tanlash va resurslarni taqsimlash boshqaruv qarorlarining ajralmas elementiga aylantiriladi. Risk-baholash natijalari asosida birinchi navbatda to‘lov nuqtalari, ma’muriy panellar, API integratsiyalar, mijoz ma’lumotlari bazasi, logistika va ombor tizimiga bog‘langan modullar kabi “tanqidiy aktivlar” uchun alohida himoya profili shakllantiriladi.

Texnik darajada elektron tijoratdagi eng muhim masalalardan biri autentifikatsiya va avtorizatsiyaning kuchaytirilishi hisoblanadi. Akkauntlarni egallab olish va ma’muriy huquqlarni qo‘lga kiritish ko‘p holatlarda oddiy parollar, qayta-qayta ishlatiladigan parollar yoki fishing orqali sodir bo‘ladi. Shu sababli mnogofaktorli autentifikatsiya, ayniqsa adminlar va operatorlar uchun, majburiy standart sifatida joriy etilishi zarur. Rolga asoslangan ruxsatlar, yuqori riskli amallar (qaytarim, promokod, narxni o‘zgartirish, yetkazib berish manzilini almashtirish) uchun qo‘shimcha tasdiq mexanizmlari, sessiya xavfsizligi (inactivity timeout, session rotation) kabi choralar akkaunt xavfini sezilarli pasaytiradi. Shu bilan birga ma’lumotlarni kriptografik himoya qilish elektron tijoratdagi asosiy tayanch choralardan hisoblanadi. Ma’lumotlar tranzitda TLS orqali himoya qilinishi, server va bazada saqlanuvchi hassos ma’lumotlar shifrlanishi, rezerv nusxalar ham shifrlangan holda saqlanishi kerak. Kalitlarni boshqarish masalasi ham alohida ahamiyatga ega: kalitlarning aylantirilishi, huquqlarni cheklash, markazlashgan KMS/HSM yechimlaridan foydalanish kriptografiyaning samarasini belgilaydi. To‘lov ma’lumotlari bilan ishlovchi tizimlarda tokenizatsiya va PCI talablariga mos jarayonlarni tashkil etish orqali karta ma’lumotlariga to‘g‘ridan-to‘g‘ri ishlov berish hajmi qisqartiriladi va muvofiqlik riski kamayadi.

Elektron tijorat veb-ilova va APIlarga tayanadigani uchun veb xavfsizlik amallari alohida yo‘nalish sifatida yo‘lga qo‘yiladi. Kod yozishdan boshlab xavfsizlik talablarini kiritish, kodni tekshirish, statik va dinamik testlar, dependency scanning, konfiguratsiyani mustahkamlash kabi DevSecOps amaliyotlari zaifliklarni erta bosqichda aniqlashga yordam beradi. Veb-ilova darajasida WAF va API gateway orqali rate limiting, bot-trafikni cheklash, in’eksiya va skanerlash urinishlarini to‘sish mumkin. Input validation va output encoding, CSRF muhofazasi, CORS siyosati, secure headers, maxfiy kalitlar va tokenlarning repozitoriyga chiqib ketmasligini ta’minlovchi secrets management amaliyotlari veb-ilovani texnik zaifliklardan himoya qilishda muhim hisoblanadi.

Infratuzilma va tarmoq darajasida segmentatsiya elektron tijoratning ichki tarkibiy qismlarini ajratib, buzilish sodir bo‘lganda zararning tarqalishini cheklaydi. Veb-qatlam, ilovalar qatlami va ma’lumotlar bazasi qatlamining izolyatsiyasi, ma’muriy kirish nuqtalarini VPN yoki maxsus jump-host orqali berish, standart “default” konfiguratsiyalarni mustahkamlash, doimiy yangilash va patch-menejmentni yo‘lga qo‘yish kiberxavflarni pasaytiradi. Shu bilan birga xizmat uzluksizligi uchun DDoS muhofazasi, CDN, autoscaling va upstream filtering kabi arxitektura yechimlari ishonchli ishlashni ta’minlaydi.

Axborot xavfsizligining samarasi faqat “hujumni kiritmaslik” bilan emas, balki hujum sodir bo‘lganida uni tez aniqlash va ta’sirini cheklash qobiliyati bilan ham o‘lchanadi. Shu nuqtai nazardan jurnallash va monitoring elektron tijoratda markaziy o‘rin tutadi. Ma’muriy amallar, autentifikatsiya urinishlari, to‘lov statuslari, shubhali tranzaksiyalar, bir IPdan ko‘p akkauntga kirish, ko‘p marotaba parol xato kiritish, g‘ayritabiiy geografiyadan kirish urinishlari kabi ssenariylar avtomatik alertlar orqali nazorat qilinadi. SIEM va tahlil vositalari shubhali xulq-atvorni aniqlashda qo‘l keladi, integrity monitoring esa veb-kontentdagi noqonuniy o‘zgarishlarni tez ilg‘ab olishga yordam beradi.

Operatsion tayyorgarlik qismida rezerv nusxa olish, tiklanish rejalari va insidentlarga javob berish tartibi shakllantirilmasa, hatto kuchli texnik himoya ham yetarli bo‘lmasligi mumkin. Shu bois rezerv nusxa olishning 3-2-1 tamoyili, tiklanish vaqti (RTO) va ma’lumot yo‘qotish chegarasi (RPO) ko‘rsatkichlarini belgilash, insidentga javob berish ssenariylari bo‘yicha mas’ullar, aloqa kanallari va birinchi qadamlar chek-listini tayyorlash elektron tijorat barqarorligini ta’minlaydi.

Nihoyat, ta’minot zanjiri xavflari elektron tijoratda alohida dolzarbdir, chunki platforma ko‘pincha tashqi plaginlar, analitika skriptlari, to‘lov provayderlari, logistika agregatorlari va boshqa integratsiyalarga bog‘lanadi. Vendorlarni baholash, kelishuvlarda xavfsizlik talablarini aniq belgilash, tashqi komponentlarni minimallashtirish va doimiy kuzatuv elektron tijorat muhitida supply chain risklarini kamaytirishga xizmat qiladi. Shu tarzda tashkiliy boshqaruv, texnik nazoratlar va barqarorlik mexanizmlari bir butun tizimga aylantirilsa, elektron tijoratda axborot xavfsizligini ta’minlash “reaktiv” emas, balki “proaktiv” va uzluksiz takomillashuvchi jarayon sifatida shakllanadi.

Xulosa: Elektron tijoratda axborot xavfsizligini ta’minlash — texnik vositalar yig‘indisi emas, balki riskka asoslangan boshqaruv, qatlamli nazoratlar va barqarorlikni birlashtiruvchi tizimdir. Maqolada elektron tijorat uchun dolzarb xavflar va ularga mos tashkiliy-texnik usullar tizimlashtirildi. Integral yondashuv sifatida: (1) boshqaruv va siyosatlar, (2) veb-ilova/API va ma’lumotlarni himoya qiluvchi nazoratlar, (3) monitoring va tiklanish qobiliyati bir butun siklda qurilishi lozimligi asoslandi. Amaliyotga joriy etishda bosqichma-bosqich yo‘l xaritasi hamda xavf–nazorat xaritasi elektron tijorat

sub’ektlariga resurslarni to‘g‘ri taqsimlash, ustuvor risklarni birinchi bo‘lib yopish va kiberbarqarorlikni oshirish imkonini beradi.

REFERENCES

1. SO/IEC 27001:2022. Information security management systems — Requirements. ISO, 2022.
2. NIST. The NIST Cybersecurity Framework (CSF) 2.0. NIST CSWP 29, 26 February 2024.
3. NIST. NIST releases version 2.0 of the Cybersecurity Framework. 26 February 2024.
4. OWASP Foundation. OWASP Top 10:2025 (Web Application Security Risks).
5. PCI Security Standards Council. PCI DSS v4.0.1 haqida rasmiy izohlar va yangi talablar muddati (31 March 2025).
6. PCI Security Standards Council. PCI DSS v4.0 o‘tish davri va taymlayn bo‘yicha rasmiy ma’lumot.
7. Suyunova D.D. Corporate in joint stock companies ways to use digital technologies to improve management.European Journal of Research Development and Sustainability (EJRDS), Available Online at: https://www.scholarzest.com Vol. 4 No 09. September 2023 ISSN:2660-5570.
8. Suyunova D.D. Korporativ boshqaruvning samaradorligini oshirishda raqamli texnolgiyalardan foydalanish masalasiga ilmiy qarashlar.Iqtisodiy tarqqiyot va tahlil ilmiy elektron jurnali, 2024 yil 31 iyul.https://e-itt.uz/index.php/eitt/article/view/1472/1379.
9. Suyunova D.D. Raqamli texnologiyalardan foydalanish asosida korporativ boshqaruvning samaradorligini oshirish masalasiga ilmiy yondashuv.(Raqamli iqtisodiyot sharoitida biznes va tadbirkorlikni rivojlantirishning dolzarb muammolari, xalqaro ilmiy-amaliy konferensiya, 2022 yil 23 dekabr.)
10. Suyunova D.D. Aksiyadorlik jamiyatlarida korporativ boshqaruvni joriy qilishning raqamli transformatsiyasini amalga oshirishga ilmiy-nazariy yondashuv. (Raqamli iqtisodiyot sharoitida biznes va tadbirvorlikni rivojlantirishning dolzarb muammolari, xalqaro ilmiy-amaliy konferensiya, 2022 yil 23 dekabr).