



RAQAMLI LOGISTIKADA XAVFSIZLIK MUAMMOLARI VA ULARNI BARTARAF ETISH USULLARI

PhD, dots. **Uzaqov Ortik**
Qarshi davlat texnika universiteti
ORCID: 0009-0005-0456-1432
uzaqovortiq@gmail.com

Annotatsiya. Ushbu maqolada raqamli logistik tizimlarda uchraydigan asosiy xavfsizlik muammolari va ularni bartaraf etish usullari tahlil qilingan. Raqamli texnologiyalarning logistikaga keng joriy etilishi natijasida axborot xavfsizligi, tizimga noqonuniy kirishlar, ma'lumotlarning maxfiyligi va uzluksizligi kabi masalalar dolzarb bo'lib bormoqda. Tadqiqotda mavjud tahdidlar, ularning oqibatlari va zamonaviy himoya texnologiyalari, jumladan, kriptografik usullar, kirishni boshqarish tizimlari, xavfsizlik devorlari (Firewall), SIEM tizimlari va boshqa ilg'or yechimlar yoritilgan. Shu orqali logistikada raqamli infratuzilmaning barqarorligi va ishonchliligi ta'minlanishi mumkinligi ko'rsatib beriladi.

Kalit so'zlar: raqamli logistika, axborot xavfsizligi, kiberxavf, kiberxavfsizlik, tahdidlarni aniqlash, SIEM tizimlari, kriptografiya, xavfsizlik siyosati.

ПРОБЛЕМЫ БЕЗОПАСНОСТИ В ЦИФРОВОЙ ЛОГИСТИКЕ И МЕТОДЫ ИХ УСТРАНЕНИЯ

PhD, доц. **Узаков Ортик**
Каршинский государственный технический университет

Аннотация. В данной статье проанализированы основные проблемы безопасности в цифровых логистических системах и способы их устранения. Широкое внедрение цифровых технологий в логистику делает особенно актуальными вопросы информационной безопасности, несанкционированного доступа к системам, конфиденциальности и непрерывности данных. В исследовании рассмотрены существующие угрозы, их последствия и современные технологии защиты, включая криптографические методы, системы управления доступом, межсетевые экраны (Firewall), системы обнаружения угроз (SIEM) и другие передовые решения. Показано, что обеспечение устойчивости и надежности цифровой инфраструктуры играет ключевую роль в логистике.

Ключевые слова: цифровая логистика, информационная безопасность, киберугрозы, кибербезопасность, обнаружение угроз, SIEM-системы, криптография, политика безопасности.

SECURITY PROBLEMS IN DIGITAL LOGISTICS AND METHODS TO ELIMINATE THEM

PhD, assoc. prof. **Uzakov Ortik**
Karshi State Technical University

Abstract. This article analyzes the main security issues in digital logistics systems and the methods to eliminate them. The widespread adoption of digital technologies in logistics has made information security, unauthorized access, data confidentiality, and continuity highly relevant. The study examines existing threats, their impacts, and modern protection technologies, including cryptographic methods, access control systems, firewalls, SIEM systems, and other advanced solutions. The research demonstrates that ensuring the stability and reliability of digital infrastructure is crucial for effective logistics operations.

Keywords: digital logistics, information security, cyber threats, cyber security, threat detection, SIEM systems, cryptography, security policy.

Kirish.

Raqamli texnologiyalar zamonaviy logistikani tubdan o'zgartirib, yuk tashish, omborxona boshqaruvi, yetkazib berish zanjirlari va boshqa jarayonlarni avtomatlashtirish va optimallashtirish imkonini berdi. Shu bilan birga, logistika sohasining raqamlashtirilishi yangi xavfsizlik tahdidlarini yuzaga keltirdi. Ma'lumotlarning katta qismi bulutli tizimlarda saqlanishi, real vaqt rejimidagi monitoring va masofaviy boshqaruv tizimlarining keng qo'llanilishi raqamli logistikani kibertahdidlarga nisbatan yanada zaif qiladi. Axborotlarning maxfiyligi, butunligi va mavjudligini ta'minlash masalalari bugungi kunda logistik tashkilotlar uchun eng dolzarb muammolardan biriga aylangan. Shu sababli, raqamli logistik tizimlarda xavfsizlikni ta'minlash bo'yicha samarali yondashuvlarni ishlab chiqish va joriy etish zarurati ortib bormoqda. Ushbu maqolada aynan shu muammolar yoritiladi va ularni bartaraf etishning texnik hamda tashkiliy usullari ko'rib chiqiladi. Tadqiqotning maqsadi - logistikadagi raqamli xavfsizlikka tahdid soluvchi asosiy omillarni aniqlash hamda ularning oldini olish bo'yicha samarali choralarni tavsiya qilishdan iborat (Rouse, 2021).

Zamonaviy logistika sohasida raqamli texnologiyalarning keng joriy etilishi ishlab chiqarishdan tortib iste'molchigacha bo'lgan barcha jarayonlarni optimallashtirish va nazorat qilish imkonini bermoqda. Avtomatlashtirilgan omborxona tizimlari, GPS asosidagi kuzatuv texnologiyalari, elektron hujjatlashtirish, bulutli platformalar orqali boshqariladigan yetkazib berish tarmoqlari logistikaning tezkorligi, aniqligi va samaradorligini sezilarli darajada oshirdi. Biroq bu raqamli imkoniyatlar ortidan logistik infratuzilmalar yangi turdagi xavfsizlik tahdidlariga duch kelmoqda. Axborot xavfsizligini ta'minlash, tizimlar o'zaro uzluksiz ishlashi va ma'lumotlarning yaxlitligi hozirgi davrning eng muhim talablaridan biri bo'lib qolmoqda.

Raqamli logistik tizimlar asosan ochiq tarmoqlarda ishlaydi, turli tashqi xizmatlar bilan integratsiyalashgan bo'ladi va bu esa kiberhujumlar uchun yangi imkoniyatlar yaratadi. Tahdidlar ichida zararli dasturlar, xizmatdan foydalanishni rad etish (DoS/DDoS) hujumlari, ma'lumotlarni noqonuniy yig'ish va o'g'irlash, tarmoq orqali tizimlarga noqonuniy kirish kabi holatlar eng ko'p uchraydi. Ayniqsa, yetkazib berish zanjiri orqali harakatlanayotgan ma'lumotlar va yuklar haqidagi real vaqt ma'lumotlari o'g'irlangan taqdirda, kompaniya uchun moliyaviy, huquqiy va obro' jihatdan jiddiy zararlar keltirishi mumkin.

Shuningdek, ko'plab kompaniyalar axborot xavfsizligiga texnik emas, balki ikkinchi darajali masala sifatida yondashadi. Natijada zamonaviy tahdidlarga qarshi zaif bo'lgan arxitektura va siyosatlar shakllanadi. Shuning uchun raqamli logistikada axborot xavfsizligini ta'minlash tizimga yondashuvni, ya'ni texnologik vositalar bilan bir qatorda tashkiliy, huquqiy va inson omiliga asoslangan strategiyalarni ham o'z ichiga olishi lozim.

Logistik jarayonlarda uchraydigan raqamli xavfsizlik muammolari chuqur tahlil qilinadi. Xususan, mavjud tahdidlar va ularning oqibatlari, hozirgi kundagi ilg'or himoya texnologiyalari,

ularni joriy etishdagi amaliy tajribalar va kelgusidagi rivojlanish istiqbollari yoritiladi. Tadqiqotning asosiy maqsadi - logistik tizimlar xavfsizligini ta'minlash yo'llarini aniqlash, tahdidlarni erta bosqichda aniqlash va ularni bartaraf etish bo'yicha amaliy va samarali yechimlar ishlab chiqish hisoblanadi.

Adabiyotlar sharhi.

Axborotlashgan jamiyatni shakllantirish, AKTdan milliy iqtisodiyotimizning turli sohalarida foydalanish muammolari yetakchi iqtisodchi olimlar va mutaxassislar, iqtisodiy informatika va avtomatlashtirilgan boshqaruv axborot tizimlari sohasida bir qator iqtisodchi olimlarning fikrlari keltirib o'tilgan. Iqtisodiy informatika va avtomatlashtirilgan boshqaruv tizimlari sohasidagi taniqli olimlar, xususan, G'ulomov tadqiqotlari milliy iqtisodiyotning turli sohalarida AKTdan foydalanish va joriy etish samaradorligini oshirish masalalariga bag'ishlangan. Begalov AKTning shakllanib borishi, uning texnologik asoslari, jahonda va O'zbekistonda raqamli iqtisodiyotning shakllanishi, korxonalarda AKT joriy etish ilmiy ishlarida keng ko'rib chiqilgan (Zhang and Lee, 2020).

Odilovning ilmiy ishlarida kompaniya logistik jarayonlarini AKTlari asosida takomillashtirish bo'yicha yondoshuvlar va takliflar berilgan (Zaynutdinov va Norov, 2022).

Medvedev va Prisyajnyuklar logistika operatsiyalari bilan bog'liq asosiy axborot jarayonlariga quyidagilar kiradi: mahsulotlar assortimenti, tashuvchilar, yuk jo'natuvchilar va qabul qiluvchilar, yo'nalishlar, ta'riflar, normativ-huquqiy baza va boshqa biznes ma'lumotlari bo'yicha yagona ma'lumot bazasini yuritish va yangilash, elektron xaritalar va joylashishni aniqlash va navigatsiya tizimlarini qo'llab-quvvatlagan holda yuk monitoringi, buyurtmani amalga oshirish jarayonida turli jarayonlarni kuzatish (nazorat qilish va yuklashni optimallashtirish va boshqalar), boshqa dasturiy ilovalardan ma'lumotlarni import va eksport qilish, tahlil qilish, tashish uchun buyurtmalarni qabul qilish va qayta ishlash, mijozlar, hamkorlar va xodimlarga buyurtmaning borishi haqidagi ma'lumotlardan foydalanish imkoniyatini ta'minlaydi deb, logistika operatsiyalari bilan bog'liq asosiy axborot jarayonlariga o'zlarining o'quv qo'llanmalarida logistika axborot tizimlari bo'yicha o'zlarining yondoshuvlari va takliflarini berishgan (Uzbekov, 2019).

Sergeyevga ko'ra, logistika axborot tizimlari logistikasining bir qismi bo'lib, uning harakati davomida moddiy oqimga hamroh bo'ladigan axborot oqimini tashkil qiladi. Olimlar axborot logistikasini korxonaga yetkazib berish, yaratish va sotish o'rtasidagi bog'liqlik sifatida belgilaydilar deb, o'zlarining biznesda logistika o'quv qo'llanmalarida yondoshuv va takliflarini berishgan (Conti et al., 2018).

Kallahan o'zining adabiyotlarida raqamli logistika va uning global biznesdagi ahamiyati haqida batafsil tushunchalar bergan. U raqamli logistika orqali korxonalar qanday qilib o'z jarayonlarini optimallashtirishlari va xarajatlarni kamaytirishlari mumkinligini ko'rsatib o'tadi. Raqamli logistika orqali xizmatlar sifatini oshirish va bozorning o'zgaruvchan talablariga tezda javob berish imkoniyatlari haqida ham so'z yuritadi. Tashqi provayderlar bilan hamkorlik qilishda yuzaga keladigan xavf-xatarlar va bu muammolarni qanday hal qilish mumkinligi haqida fikrlar mavjud.

Hossain esa raqamli logistika va ta'minot zanjirining global miqyosdagi o'rni haqida chuqur tahlil taqdim etadi. Muallif, outsorsing va offshoring jarayonlarining biznesni global miqyosda boshqarishdagi o'zgarishlarga qanday ta'sir qilayotganini ko'rib chiqadi. Unda raqamli logistikasi orqali kompaniyalar qanday qilib yangi bozorlarni zabt etish va mavjud resurslardan maksimal darajada foydalanishlari mumkinligi haqida batafsil ma'lumot berilgan. Shuningdek, global raqobat va iqtisodiy o'zgarishlar natijasida raqamli logistika qanday yangi tendensiyalarni shakllantirayotganini tahlil qiladi.

Sharma o'zining ilmiy maqolasida, texnologiyaning raqamli logistika sohasida qanday ta'sir qilayotganini o'rganadi. U raqamli texnologiyalar, sun'iy intellekt (SI), Internet uskunalari ("IoT" - Internet of Things bu bir-biri bilan yoki tashqi muhit bilan o'zaro ta'sir qilish uchun

o'rnatilgan vositalar va texnologiyalar bilan jihozlangan jismoniy obyektlar o'rtasida ma'lumotlarni uzatish tarmog'i tushunchasi) va blokcheyn ("blockchain" - bu barcha uchun ochiq va o'zgaras bo'lgan ma'lumotlar bazasi) kabi zamonaviy texnologiyalarni raqamli logistika jarayonlariga qo'llashning afzalliklarini muhokama qiladi.

Tadqiqot metodologiyasi.

Tadqiqot olib borish davomida monografik, ekspert va tizimli tahlil usullaridan foydalangan holda korxonalarda logistika axborot tizimlarini joriy qilish bo'yicha logistika operatsiyalarini amalga oshirish, korxonalar harakatlarining asosiy yo'nalishlari, logistika axborot tizimlarini shakllantirish va boshqarish jarayonlari va ularning faoliyat iqtisodiy mexanizmlarini takomillashtirish hamda korxonalar logistika axborot tizimlari jarayonlarini samarali tashkil etish bo'yicha muammolarni aniqlanib, axborot xavfsizligini ta'minlashning samarali yechimlari bo'yicha takliflar tayyorlandi.

Tahlil va natijalar muhokamasi.

Raqamli logistik tizimlarning xavfsizligi turli darajadagi tahdidlar bilan chambarchas bog'liq bo'lib, ular tizimlarning samarali faoliyat yuritishiga bevosita ta'sir ko'rsatadi. Mavjud tahdidlar orasida eng asosiylari - kiberhujumlar, zararli dasturlar, ma'lumotlarni yo'qotish yoki o'g'irlash, tizimga ruxsatsiz kirishlar va axborotni soxtalashtirish holatlaridir. Ayniqsa, logistika zanjiri bir nechta tashqi ishtirokchilar (transport kompaniyalari, omborlar, brokerlar va mijozlar) orqali amalga oshirilgani sababli, bu zanjirdagi har qanday zaif nuqta umumiy tizim xavfsizligiga tahdid solidi(1-jadval).

1-jadval

Raqamli logistikada asosiy tahdidlar va oqibatlar

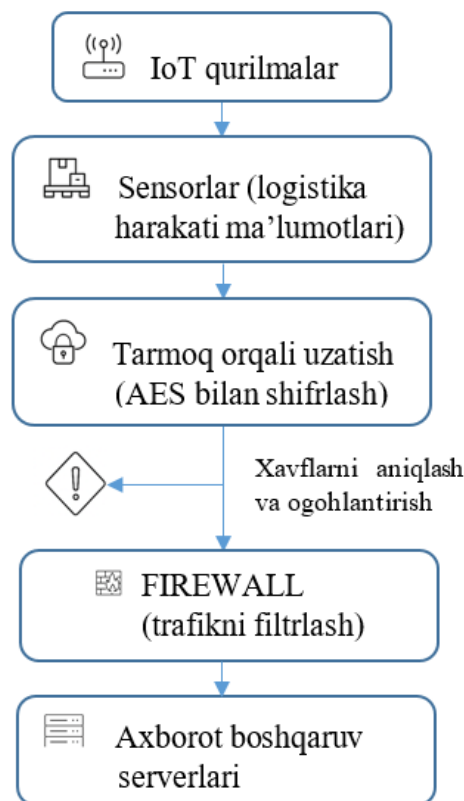
Tahdid turi	Ta'siri	Misollar
DDoS hujumi	Tizim faoliyatining to'xtashi	Yetkazib berishdagi uzilishlar
Ma'lumotlar o'g'irlanishi	Maxfiylik buzilishi, huquqiy muammolar	Mijozlar ma'lumotlarining tarqalishi
Zararli dasturlar (malware)	Tizimning buzilishi, ma'lumotlarning yo'qolishi	NotPetya, WannaCry
Noqonuniy kirishlar	Tashqi aralashuvlar orqali manipulyatsiya	Yuk marshrutini o'zgartirish
Inson xatolari	Ma'lumotlar noto'g'ri kiritilishi yoki tarqalishi	Xodimlar orqali tasodifiy buzilishlar

Logistika sohasida yuz beradigan DoS (Denial of Service) yoki DDoS (Distributed Denial of Service) hujumlari kompaniya serverlarini ishdan chiqarib, real vaqt rejimidagi operatsiyalarning to'xtashiga olib keladi. Bu esa yetkazib berishdagi kechikishlar, moliyaviy yo'qotishlar va mijozlar ishonchini yo'qotishga sabab bo'ladi. Shuningdek, SI asosida ishlab chiqilgan zararli dasturlar orqali avtomatlashtirilgan tizimlarga kirib, yuklar yo'nalishini o'zgartirish yoki ombor ma'lumotlarini buzish holatlari ham kuzatilmoqda (ISO/IEC, 2022).

Mazkur tahdidlarga qarshi kurashish uchun bir nechta zamonaviy texnologik vositalar mavjud. Ulardan biri kriptografik himoya usullari bo'lib, ular ma'lumotlarning shifrlanishi orqali ularning maxfiyligini ta'minlaydi. Xususan, RSA va AES algoritmlari ma'lumotlarni uzatish jarayonida ishonchlilik darajasini oshiradi. Shuningdek, kirishni boshqarish tizimlari (Access Control Systems) foydalanuvchilarni autentifikatsiya qilish orqali tizimga faqat vakolatli shaxslarning kirishini ta'minlaydi.

SIEM (Security Information and Event Management) tizimlari esa turli axborot manbalaridan xavfsizlik hodisalarini real vaqt rejimida yig'ib, ularni tahlil qiladi. Bu tizimlar yordamida kiberhujumlar erta aniqlanib, avtomatik ogohlantirishlar orqali tezkor choralar ko'riladi. Xavfsizlik devorlari (Firewall) va IDS/IPS tizimlari esa tarmoq darajasida kiruvchi va chiquvchi trafikni nazorat qilish orqali zararli harakatlarning oldini oladi (1-rasm).

Amaliy tajriba sifatida, yirik logistika kompaniyalari DHL, Maersk, FedEx - o'z infratuzilmasiga ilg'or xavfsizlik tizimlarini joriy qilgan. Masalan, Maersk kompaniyasi 2017-yilda yuz bergan NotPetya zararli dasturi orqali tizimining falaj bo'lishidan so'ng, o'zining xavfsizlik strategiyasini to'liq qayta ko'rib chiqdi va bulutli SIEM platformasiga o'tdi. FedEx esa yuklarni real vaqt rejimida kuzatishda IoT qurilmalari bilan birga o'z tarmoqlarini kriptografik darajada shifrlash bilan himoyalaydi (Zaynutdinov va Norov, 2022).



1-rasm. IoT bilan bog'liq logistik xavfsizlik arxitekturası

Shuningdek, xavfsizlikni faqat texnologiyalar orqali emas, balki **tashkiliy va huquqiy yondashuvlar** orqali ham mustahkamlash zarur. Kompaniyalar ichki xavfsizlik siyosatini ishlab chiqishi, xodimlar uchun muntazam treninglar o'tkazishi va favqulodda holatlarda harakat algoritmlarini ishlab chiqishi muhim sanaladi. Inson omili ko'plab xavfsizlik buzilishlarining asosiy sababi bo'lganligi uchun, xodimlar ongini oshirish va xatolarning oldini olish - muvaffaqiyat kaliti hisoblanadi.

Xulosa va takliflar.

Raqamli logistik tizimlarda xavfsizlikni ta'minlash masalasi zamonaviy texnologik taraqqiyot sharoitida tobora dolzarb bo'lib bormoqda. O'tkazilgan tahlillar shuni ko'rsatdiki, kiber xavf-xatarlar nafaqat texnik darajada, balki tashkiliy va insoniy omillar nuqtai nazaridan ham chuqur o'rganilishi lozim.

Kiberhujumlar, zararli dasturlar, ruxsatsiz kirishlar va ma'lumotlar o'g'irlanishi kabi xavflar raqamli logistik jarayonlarning izchil ishlashiga jiddiy to'siq bo'lishi mumkin. Bunday

tahdidlarni bartaraf etish uchun kriptografik himoya, SIEM tizimlari, kirish nazorati va xavfsizlik devorlari kabi ilg'or texnologiyalarni qo'llash muhim sanaladi.

IoT qurilmalari bilan integratsiyalashgan tizimlar yordamida real vaqt rejimidagi monitoring va tezkor javob choralari yo'lga qo'yish imkoniyati mavjud. Bu esa logistika zanjirining ishonchliligini oshirish va kutilmagan xavflarni bartaraf etishda muhim omil hisoblanadi.

Xulosa qilib aytganda, raqamli logistikada xavfsizlikni ta'minlash kompleks yondashuvni talab etadi: bu texnologik, tashkiliy va ma'naviy jihatlardan bir butun sifatida qaralishi kerak. Kompaniyalar o'z xavfsizlik strategiyalarini qayta ko'rib chiqishlari, xodimlarni muntazam o'qitishlari hamda real tahdidlar asosida testlash tizimlarini joriy etishlari muhimdir. Faqat shundagina logistika jarayonlari xavfsiz, samarali va barqaror bo'lishi mumkin deb hisoblaymiz.

Adabiyotlar/Jumepamypa/References:

Conti, M., et al. (2018). *Internet of Things Security and Forensics: Challenges and Opportunities*. Elsevier.

ISO/IEC 27001: (2022). *Information Security Management Systems - Requirements*. International Organization for Standardization.

Rouse, M. (2021). *Digital Logistics and Cybersecurity: A New Paradigm*. TechTarget Publishing.

Uzbekov, F. A. (2019). *Axborot xavfsizligi asoslari*. Toshkent: Innovatsiya nashriyoti.

Zaynutdinov, R. M., & Norov, B. B. (2022). *Raqamli iqtisodiyot va logistika tarmoqlarida axborot xavfsizligi muammolari*. O'zbekiston elektron jurnalida chop etilgan maqola.

Zhang, Y., & Lee, J. (2020). *IoT Security in Logistics Systems*. *International Journal of Logistics Research and Applications*, 23(4), 405-420.