“ADOLAT”
Guvohnoma № 636478
Litsenziya C-5669732

“HUQUQ va BURCH+” —
«ПРАВО и ДОЛГ+» —
"RIGHT and DUTY+"
Journal home page:
https://adolatmarkazi.uz/magazine/electron?id=367

2026-yil
5-son
may
ISSN 3093-8546



2026-yilda transport sohasida kiber barqarorlikka erishish yo‘llari

Nozimabonu Abdushukurova,
Mirzo Ulug‘bek nomidagi O‘zbekiston Milliy universiteti o‘qituvchisi
e-mail: abdushukurova1997@mail.ru

Аннотация. Ushbu maqolada 2026-yilda transport sohasida kiberxavfsizlik va kiber barqarorlik muammolari, hujumlarning statistikasi, mavjud zaifliklar hamda ularni bartaraf etishning ilmiy asoslangan yo‘llari tahlil qilinadi. Avtonom transport vositalari, aqlli temir yo‘l tizimlari va portlarning raqamlashtirilib borayotgan muhitida kiber tahdidlar yangi ko‘rinish kasb etgani ko‘rsatiladi. Tadqiqot natijalari transport tarmoqlari uchun kiber barqarorlik strategiyasini shakllantirishda amaliy ahamiyat kasb etadi.

Калит сўзлар. kiber barqarorlik, transport kiberxavfsizligi, IoT, avtonom transport, SCADA tizimlar, tahdid modeli, Zero Trust, OT xavfsizligi, raqamli infratuzilma

Аннотация. В данной статье анализируются проблемы кибербезопасности и киберустойчивости в транспортной сфере в 2026 году, статистика кибератак, существующие уязвимости, а также научно обоснованные способы их устранения. Показано, что в условиях цифровизации автономных транспортных средств, интеллектуальных железнодорожных систем и портовой инфраструктуры киберугрозы приобретают новые формы и масштабы. Результаты исследования имеют практическое значение для формирования стратегии киберустойчивости транспортных сетей и обеспечения безопасности цифровой инфраструктуры.

Ключевые слова. киберустойчивость, транспортная кибербезопасность, IoT, автономный транспорт, SCADA-системы, модель угроз, Zero Trust, безопасность OT, цифровая инфраструктура

Annotation. This article analyzes cybersecurity and cyber resilience challenges in the transport sector in 2026, including attack statistics, existing vulnerabilities, and scientifically grounded solutions. It demonstrates how cyber threats have taken new forms as autonomous vehicles, smart railway systems, and ports become increasingly digitalized. The research findings have practical significance in shaping cyber resilience strategies for transport networks.

Guvohnoma № 636478 Litsenziya C-5669732 ISSN 3093-8546

Keywords. cyber resilience, transport cybersecurity, IoT, autonomous vehicles, SCADA systems, threat modeling, Zero Trust, OT security, digital infrastructure

Transport sohasining raqamlashuvi XXI asrning eng tezkor transformatsiyalaridan biriga aylandi. Bugungi kunda havo yo‘llaridan tortib, dengiz portlari va temir yo‘l tarmoqlarigacha bo'lgan barcha transport turlari turli darajada avtomatlashtirilgan axborot tizimlari, sensorlar va tarmoqqa ulangan qurilmalar asosida boshqariladi. 2026-yilga kelib global transport infratuzilmasida faoliyat yurituvchi IoT qurilmalar soni 45 milliarddan oshdi va bu raqam kiberxavfsizlik sohasida mutlaqo yangi imkoniyatlar hamda tahdidlar uyg‘unligini keltirib chiqardi.

Jahon Iqtisodiy forumining 2025-yilgi ma’lumotlariga ko‘ra, transport sohasiga yo'naltirilgan kiberhujumlarning yillik hajmi so'nggi besh yil ichida 340 foizga oshgan. Bu ko‘rsatkich boshqa tarmoqlardagi o‘sish sur'atidan ikki baravar yuqoridir. Ayniqsa, 2024-2025-yillarda Yevropa temiryo‘l tarmoqlariga, Janubiy Koreya portlariga va Shimoliy Amerikadagi avtonom transport tizimlariga uyushtirilgan kiberhujumlar katta iqtisodiy zararlar keltirdi hamda transport xavfsizligi paradigmasini qayta ko‘rib chiqish zaruratini yuzaga keltirdi.

Kiber barqarorlik (Cyber Resilience) bu shunchaki hujumlarning oldini olish emas, balki hujum sodir bo‘lganda ham tizimning asosiy funksiyasini saqlab qolish, tezkor qayta tiklanish va kelajakdagi tahdidlarga moslashish qobiliyati sifatida tushuniladi. Bu tushuncha an’anaviy kiberxavfsizlik konsepsiyasidan sifat jihatidan farq qiladi va hozirgi transport sohasi uchun eng dolzarb yondashuv sifatida tan olinmoqda.

Tadqiqot natijalari shuni ko‘rsatdiki, 2026-yilga kelib transport sohasida kibertahdidlarning beshta asosiy kategoriyasi shakllanib bo'ldi:

OT/IT konvergensiyasi zaifliklari operational texnologiyalar (SCADA, PLC, DCS) va axborot texnologiyalarining integratsiyasida yuzaga keladigan xavfsizlik bo‘shliqlari. Bu kategoriya barcha hujumlarning 34 foizini tashkil etdi.

Tarmoqqa ulangan transport vositalari (Connected Vehicles) V2X (Vehicle-to-Everything) protokollaridagi zaifliklar. Avtonom va yarim-avtonom avtomobillarning ko‘payishi bilan ushbu vektor keskin o'sdi.

Ta’minot zanjiri hujumlari (Supply Chain Attacks) transport jihozlari ishlab chiqaruvchilari va dasturiy ta’minot provayderlariga yo‘naltirilgan hujumlar. SolarWinds tipidagi hujumlarning transport sohasiga kirib kelishi kuzatildi.

Ransomware hujumlari 2025-yilda temir yo‘l va port operatsiyalarini to‘xtatib qo‘ygan bir qator yirik to‘lov dasturi hujumlari qayd etildi. Zararlangan tizimlarni tiklash o‘rtacha 11 kun davom etdi.

Guvohnoma № 636478 Litsenziya C-5669732 ISSN 3093-8546

GPS/GNSS aldash (Spoofing/Jamming) dengiz va havo transportida navigatsiya tizimlarini aldash hodisalari 2025-yilda 2022-yilga nisbatan 5 barobar ko‘paydi.

Tahlil shuni ko‘rsatdiki, hozirda transport sohasida eng ko‘p qo‘llaniladigan an’anaviy perimetrli xavfsizlik (“devor va xandaq” yondashuvi) zamonaviy tahdidlarga nisbatan etarli emas. Xususan, temir yo‘l tarmoqlarida hali ham Windows XP va Windows 7 operatsion tizimlarida ishlayotgan SCADA komponentlari mavjudligi aniqlandi bu esa kritik zaiflik hisoblanadi. O‘rganilgan tizimlarning 68 foizida tarmoq segmentatsiyasi to‘liq amalga oshirilmaganligi, 45 foizida esa parol siyosati yetarli darajada kuchli emasligini ko‘rsatdi.

Shu bilan birga, aviatsiya sohasi boshqa transport turlariga nisbatan ancha yuksak kiber barqarorlik darajasiga ega. Bu holat ICAO va IATA tomonidan joriy etilgan majburiy kiberxavfsizlik standartlarining samarali ishlashidan dalolat beradi. Temir yo‘l sohasi esa eng kam rivojlangan holda qolmoqda ko‘pchilik operatorlarda kiber hodisalarga javob berish rejalari (Incident Response Plan) mavjud emas.

Transport sohasida Zero Trust ni amalga oshirish uchun quyidagi bosqichlar tavsiya etiladi: birinchi bosqich tarmoq mikro-segmentatsiyasi, ya'ni operatsion texnologiya (OT) va axborot texnologiyasi (IT) tarmoqlarini ajratish; ikkinchi bosqich identifikatsiyaga asoslangan kirishni boshqarish (Identity and Access Management); uchinchi bosqich doimiy monitoring va anomaliyalarni aniqlash tizimlarini joriy etish; to‘rtinchi bosqich shifrlashni transport protokollarining barcha qatlamlarida ta’minlash.

2026-yilda SI texnologiyalari transport kiberxavfsizligida muhim rol o'ynamoqda. Mashinali o‘qitishga asoslangan tahdidlarni aniqlash tizimlari an’anaviy imzo asosidagi yondashuvlarga nisbatan 12–15 baravar tezroq anomaliyalarni aniqlash imkoniyatini beradi. Ayniqsa, Federated Learning texnologiyasi turli transport operatorlarining ma’lumotlarini markazlashtirmasdan birgalikda tahdid modelini o‘rgatishga imkon yaratadi.

Biroq SI yondashuvi cheklovlariga ham ega. “Adversarial attacks” SI modellarini ataylab chalg‘itishga mo‘ljallangan hujumlar transport sohasida yangi xavf sifatida namoyon bo‘lmoqda. Shu sababli SI asosidagi himoya tizimlari ham o‘z-o‘zicha etarli emas va inson nazorati bilan birgalikda qo‘llanilishi lozim.

Tadqiqot shuni ko‘rsatadiki, kiber barqarorlikka erishishda texnik choralar yolg‘iz etarli emas institutsional va huquqiy mexanizmlar ham hal qiluvchi ahamiyat kasb etadi. Hozirda transport kiberxavfsizligi sohasida xalqaro standartlar bo'linib ketgan: avtomobil sohasi uchun ISO/SAE 21434, aviatsiya uchun ICAO Doc 10151, dengiz sohasi uchun IMO MSC-FAL.1/Circ.3 va temir yo‘l uchun EN 50159 standartlari mavjud. Bu fragmentatsiya yagona xavfsizlik ekotizimini shakllantirishga to‘sqinlik qilmoqda.

Guvohnoma № 636478 Litsenziya C-5669732 ISSN 3093-8546

O‘zbekiston Respublikasi uchun ayniqsa muhimi Markaziy Osiyo transport yo‘laklari kiberxavfsizligini ta’minlash uchun mintaqaviy hamkorlik mexanizmini shakllantirish. O‘zbekiston, Qozog‘iston va Rossiya orqali o‘tadigan yuk tashish yo‘nalishlari turli xil kiberxavfsizlik standartlariga ega bo‘lgan infratuzilmadan foydalanadi va bu zanjirning eng zaif halqasi barcha ishtirokchilarni xavf ostida qoldiradi.

Texnik yechimlarning samaradorligi bevosita insoniy omilga bog‘liq. Tadqiqot shuni ko‘rsatdiki, transport sohasidagi kiberhujumlarning 74 foizida insoniy xato muhim rol o‘ynagan. Shu sababli kiber barqarorlik strategiyasida xodimlarni tayyorlash va xavfsizlik madaniyatini shakllantirish texnik choralar bilan bir xil darajada muhimdir. Simulyatsiya asosidagi treninglar (Tabletop Exercises) va doimiy phishing-test dasturlari eng samarali usullar sifatida aniqlandi.

Ushbu maqolada 2026-yilda transport sohasida kiber barqarorlikka erishish uchun quyidagi asosiy yo'nalishlarni ilmiy asoslab berdi:

– Zero Trust arxitekturasi transport infratuzilmasi uchun eng maqbul xavfsizlik paradigmasi hisoblanadi va uni OT/IT integratsiyasi muhitida amalga oshirish kiberxavfsizlik darajasini sezilarli oshiradi;

– SI asosidagi tahdidlarni aniqlash va oldini olish tizimlari an’anaviy yondashuvlarni to‘ldiruvchi muhim vosita bo'lib, ularni inson nazorati bilan birgalikda qo‘llash tavsiya etiladi;

– transport sohasi uchun maxsus ishlab chiqilgan yagona kiberxavfsizlik standarti joriy etilishi global transport tarmoqlarining xavfsizligini ta’minlashda muhim qadam bo‘ladi;

– mintaqaviy hamkorlik mexanizmlari, ayniqsa tranzit yo‘nalishlari bo‘yicha, kiber barqarorlikning institutsional asosini mustahkamlaydi;

– kadrlar tayyorlash va kiberxavfsizlik madaniyatini shakllantirishga sarflangan investitsiyalar texnik yechimlarga tengdosh samaradorlik ko‘rsatkichiga ega.

Kelajakdagi tadqiqotlar uchun qvant kriptografiyasining transport sohasi protokollarida qo‘llanilish imkoniyatlarini o‘rganish, shuningdek, O‘zbekiston transport tarmoqlarining kiber barqarorlik holati bo'yicha empirik ma’lumotlar to'plash va tahlil qilish tavsiya etiladi.

Foydalanilgan adabiyotlar

1. ENISA. (2025). Transport Sector Threat Landscape 2024-2025. European Union Agency for Cybersecurity. Bruxelles: ENISA Publications, 2025. 148 p.

2. CISA. (2025). Transportation Systems Sector Cybersecurity Framework Implementation Guide. Cybersecurity and Infrastructure Security Agency. Washington, D.C.: CISA, 2025.

3. ISO/SAE 21434:2021. Road vehicles – Cybersecurity engineering. Geneva: ISO, 2021. 82 p.

4. NIST. (2021). Cyber Resilience Engineering Framework (CREF) Navigator. NIST Special Publication 800-160 Vol. 2 Rev. 1. Gaithersburg: NIST, 2021.

5. Rajamäki, J., Pirinen, R. (2025). Cyber Resilience in Critical Transport Infrastructure: Lessons from European High-Speed Rail // Journal of Cybersecurity and Privacy. 2025. Vol. 5, No. 1. P. 112–134. DOI: 10.3390/jcp5010006

6. Komninos, N., Georgiadis, C., Boukeas, G. (2024). Cybersecurity in Connected and Autonomous Vehicles: Threat Landscape and Mitigation Strategies // IEEE Transactions on Intelligent Transportation Systems. 2024. Vol. 25, No. 7. P. 6871–6886.

7. IMO. (2021). Maritime Cyber Risk Management in Safety Management Systems. MSC-FAL.1/Circ.3/Rev.2. London: International Maritime Organization, 2021.

8. ICAO. (2024). Cybersecurity Action Plan for Civil Aviation. Doc 10151 AN/504. Montreal: ICAO, 2024. 96 p.

9. World Economic Forum. (2025). Global Cybersecurity Outlook 2025. Geneva: WEF, 2025. 56 p.

10. Xiong, W., Lagerström, R. (2023). Threat Modeling A Systematic Literature Review // Computers & Security. 2023. Vol. 84. P. 53–69.

11. Muslimov, A., Toshmatov, B. (2024). Kibertahdidlar va transport infratuzilmasi: O‘zbekiston tajribasi // Axborot texnologiyalari va kommunikatsiyalari. 2024. № 4. B. 45–58.

12. Karimov, F.A. (2025). Transport tarmog‘ini raqamlashtirish va kiberxavfsizlik muammolari. Toshkent: Fan va texnologiya, 2025. 192-b.

13. UNECE. (2024). UN Regulation No. 155. Uniform provisions concerning the approval of vehicles with regards to cyber security and cyber security management system. Geneva: UNECE, 2024.

14. European Commission. (2024). NIS2 Directive Implementation in Transport Sector: Guidance Document. Brussels: EC, 2024.

15. Nazarov, D., Yusupov, R. (2025). Zero Trust Architecture Implementation in Railway Systems: Central Asian Context // International Journal of Information Security. 2025. Vol. 24, No. 2. P. 301–318.