“ADOLAT”
MILLIY HUQUQIY AXBOROT MARKAZI
Guvohnoma № 636478
Litsenziya C-5669732

“HUQUQ va BURCH+” —
«ПРАВО и ДОЛГ+» —
"RIGHT and DUTY+"
Journal home page:
https://adolatmarkazi.uz/magazine/electron?id=388

2026-yil
9-son
sentabr
ISSN 3093-8546



Transport sohasida kiberhujumlar: tarixi, vujudga kelishi va rivojlanishi

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

Аннотация. Ushbu maqola transport sohasida kiberhujumlarning kelib chiqishi, rivojlanishi va hozirgi kundagi holati haqida keng qamrovli tahlil taqdim etadi. Maqolada avtomobil, temiryo‘l, aviatsiya va dengiz transporti tizimlarida yuz bergan yirik kiber voqealar, ularning sabablari va oqibatlari ko‘rib chiqiladi. Ishning maqsadi transport infratuzilmasida kibertahdidlar qanday shakllanganini va ulardan himoyalanish yo‘llarini aniqlashdan iborat. Erishilgan natijalar shuni ko‘rsatadiki, raqamlashtirish va“aqlli”tizimlarning kengayishi transport sohasini kiberhujumlarga yanada zaifroq qilmoqda. Ishning ilmiy yangiligi shundaki, maqolada transport tarmoqlarida kiberhujumlarning xronologik tasviri, texnik mexanizmlari va profilaktik chora-tadbirlari birinchi marta o‘zbek tilidagi adabiyotlarda tizimli tarzda yoritilgan.

Калит сўзлар. kiberhujum, transport xavfsizligi, kiber tahdid, SCADA tizimi, avtomobil kiberxavfsizligi, aviatsiya kibertahdidlari, temiryo‘l kiberhujumi

Аннотация. В данной статье представлен всесторонний анализ возникновения, развития и современного состояния кибератак в транспортной отрасли. Рассматриваются крупные киберинциденты в системах автомобильного, железнодорожного, авиационного и морского транспорта, их причины и последствия. Цель работы определить, как формировались киберугрозы в транспортной инфраструктуре и каковы пути защиты от них. Полученные результаты свидетельствуют о том, что цифровизация и распространение «умных» систем делают транспортный сектор всё более уязвимым для кибератак. Научная новизна работы состоит в том, что в ней впервые в узбекоязычной литературе системно изложены хронология, технические механизмы и профилактические меры в области кибератак на транспортные сети.

Ключевые слова. кибератака, транспортная безопасность, киберугроза, система SCADA, кибербезопасность автомобилей, авиационные киберугрозы, кибератака на железную дорогу

Guvohnoma № 636478 Litsenziya C-5669732 ISSN 3093-8546

Annotation. This article provides a comprehensive analysis of the origin, development, and current state of cyberattacks in the transport sector. Major cyber incidents in road, rail, aviation, and maritime transport systems are examined, along with their causes and consequences. The aim of the study is to identify how cyber threats have evolved in transport infrastructure and to determine protective measures. The results demonstrate that digitalization and the expansion of 'smart' systems are making the transport sector increasingly vulnerable to cyberattacks. The scientific novelty of this work lies in the fact that, for the first time in Uzbek-language literature, the chronology, technical mechanisms, and preventive measures related to cyberattacks on transport networks are systematically presented.

Keywords. cyberattack, transport security, cyber threat, SCADA system, automotive cybersecurity, aviation cyber threats, railway cyberattack

Raqamlashtirishning jadal rivojlanishi va axborot-kommunikatsiya texnologiyalarining transport sohasiga chuqur integratsiyasi bu tarmoqni nafaqat samaraliroq, balki kiberhujumlarga nisbatan ancha zaifroq qilmoqda. Zamonaviy avtomobillar, poyezdlar, samolyotlar va kemalar endi minglab sensorlar, tarmoqqa ulangan qurilmalar va avtomatlashtirilgan boshqaruv tizimlaridan iborat murakkab kiber-fizik tizimlarga aylanib bormoqda. Bunday muhitda kiberhujumlar nafaqat iqtisodiy zarar keltiradi, balki insonlar hayotiga bevosita xavf soladi.

Transport sohasidagi kibertahdidlar tarixi 1990-yillardan boshlangan bo‘lsa-da, bu muammo 2010-yillardan boshlab keskin dolzarb tus oldi. Xususan, Stuxnet, BlackEnergy, WannaCry kabi global kiber qurollarning transport infratuzilmalariga ta’siri bu sohadagi xavfning global miqyosini ochib berdi. O‘zbekistonda ham transport sohasining raqamlashuvi tezlashib borishi bilan kiberhujumlardan himoyalanish masalasi tobora muhim ahamiyat kasb etmoqda.

Ushbu maqolada transport sohasida kiberhujumlarning kelib chiqishi, rivojlanish bosqichlari, texnik mexanizmlari va profilaktika choralari xronologik va tizimli tarzda tahlil qilinadi.

Kiberhujum axborot tizimlariga, tarmoqlarga yoki qurilmalarga niyatli ravishda zarar yetkazish, ularni buzish yoki noqonuniy nazorat qilish maqsadida amalga oshiriladigan harakatlar majmuyidir [1]. Transport sektorida bunday hujumlar quyidagi asosiy komponentlarga yo‘naltirilishi mumkin: boshqaruv va nazorat tizimlari (SCADA, ICS), aloqa va navigatsiya tizimlari (GPS, ADS-B, GSM-R), yo‘lovchilar va yuk axborot tizimlari, hamda texnik xizmat ko‘rsatish va ta’mirlash tizimlariga yo‘naltirilishi mumkin [2].

Transport sohasidagi zaifliklarning asosiy sabablari quyidagilar bilan izohlanadi. Birinchidan, “meros” (legacy) tizimlari: ko‘plab transport tashkilotlari hali ham yangilanmagan, zamonaviy kiberxavfsizlik talablariga javob bermaydigan eski dasturiy va apparat vositalaridan foydalanmoqda. Ikkinchidan, tarmoqqa ulanishning kengayishi: zamonaviy transport tizimlari internet va

Guvohnoma № 636478 Litsenziya C-5669732 ISSN 3093-8546

boshqa tarmoqlarga tobora ko‘proq ulanganligi ularga kirish nuqtalarini ko‘paytiradi. Uchinchidan, standartizatsiya etishmasligi: turli transport turlari va davlatlar o‘rtasida kiberxavfsizlik standartlari yetarli darajada uyg‘unlashtirilmagan [3].

Dastlabki bosqich (1990–2000-yillar)- Transport sohasida birinchi hujumlar asosan kompyuter viruslari orqali amalga oshirilgan. 1997-yilda Worchester, Massachusetts shtatida bir xaker mintaqaviy aeroportning boshqaruv tizimiga kirdi va uning aloqa qurilmalarini o‘chirib qo‘ydi. Bu voqea aviasiyadagi kibertahdidlarning real ekanligini birinchi marta ko‘rsatdi [4]. 2000-yilda Avstraliyada Maroochy Water Services hodisasi sodir bo‘ldi. Bu transport infratuzilmasiga emas, lekin sanoat boshqaruv tizimlariga (SCADA) birinchi yirik hujumlardan biri bo‘lib, keyinchalik transport sektoriga oid tahdidlarni prognoz qilishda muhim ibrat bo‘lib qoldi.

Rivojlanish bosqichi (2010–2015-yillar). 2010-yil transport kibertahdidlari tarixida alohida o‘rin tutadi. Stuxnet zararli dasturining kashf etilishi sanoat boshqaruv tizimlariga (ICS/SCADA) maqsadli hujumlar davri boshlanganligini bildirdi. Garchi u transport tizimlariga bevosita yo‘naltirilmagan bo‘lsa-da, uning mexanizmlari keyingi transport hujumlarining asosini tashkil etdi [5].

2013-yilda tadqiqotchilar Charlie Miller va Chris Valasek Toyota Prius va Ford Escape avtomobillariga noutbuk orqali ulanib, tormoz va rul tizimlarini masofadan boshqara olganliklarini namoyish etdilar. Bu avtomobil kiberxavfsizligi sohasida burilish nuqtasi bo‘ldi va sanoatni jiddiy xavf oldida qoldirdi [6].

2015-yilda aynan shu tadqiqotchilar Jeep Cherokee avtomobiliga masofadan hujum qilib, uni yo‘lda haydab borayotganida to‘xtatishga muvaffaq bo‘ldilar. Bu holat Chrysler kompaniyasini 1,4 million avtomobilni qaytarib olib, dasturiy yangilanishlar o‘tkazishga majbur qildi [7].

Global miqyosli hujumlar davri (2016–2020-yillar). 2016-yilda Ukraina elektr tarmog‘iga BlackEnergy zararli dasturi orqali amalga oshirilgan hujum transport tizimlariga ham salbiy ta’sir ko‘rsatdi, chunki mamlakat transport boshqaruv tizimlari ham shu tarmoqqa bog‘liq edi. Bu hujum davlat infratuzilmasiga uyushtirilgan kiber urushning yangi davrini boshlab berdi [8].

2017-yilda WannaCry ransomware hujumi butun dunyo bo‘ylab temir yo‘l kompaniyalarini ham qamrab oldi. Xususan, Buyuk Britaniyaning Deutsche Bahn hamkor tarmog‘i va bir qator Yevropa temir yo‘l operatorlari tizimlarini vaqtincha to‘xtatishga majbur bo‘ldilar. Bir xil yil ichida Not-Petya hujumi Maersk dengiz kompaniyasiga taxminan 300 million dollar zarar yetkazdi va global yuk tashish tizimini bir necha hafta davomida falaj qildi [9].

2020-yilda SITA aviatsiya ma’lumotlari provayderi kiberhujumga uchradi va Star Alliance, Oneworld kabi yirik aviakoalitsiya a’zolarining yo‘lovchi ma’lumotlari xavf ostida qoldi. Bu hodisa aviatsiya sektoridagi ta’minot zanjiri hujumlarining (supply chain attack) xavfini ko‘rsatdi [10].

Guvohnoma № 636478 Litsenziya C-5669732 ISSN 3093-8546

Zamonaviy holat (2021-yildan hozirga). 2021-yilda Florida shtati, Oldsmar shahrida suv taqsimlash tizimiga masofadan hujum qilingan voqeasi, garchi to‘g‘ridan-to‘g‘ri transport bilan bog‘liq bo‘lmasa-da, zamonaviy infratuzilma hujumlarining qanchalik oson amalga oshirilishi mumkinligini ko‘rsatdi. Shu yili avtomobil sanoatida Tesla, Honda, Volkswagen kompaniyalarida bir nechta jiddiy zaifliklar aniqlandi [11].

2022-yilda Rossiya-Ukraina urushi bilan bir qatorda kibermakon ham asosiy jangovar maydonlardan biriga aylandi. Ukraina temiryo‘l tizimi (Ukrzaliznytsia) va port infratuzilmasi bir necha bor kuchli DDoS hujumlariga uchradi. Xitoyning BYD, Tesla va boshqa elektr avtomobillarida ma’lumot yig‘ish va masofadan boshqarish imkoniyatlari kiberxavfsizlik ekspertlari tomonidan chuqur o‘rganildi [12].

Avtomobil transporti. Zamonaviy avtomobillar o‘rtacha 100 million qator dasturiy kod va 100 dan ortiq elektron boshqaruv bloki (ECU) bilan jihozlangan. Bluetooth, Wi-Fi, hujayraviy tarmoq, USB portlari orqali potentsial kirish nuqtalari tobora ko‘paymoqda. Hujumchilar odatda OBD-II diagnostika porti, infoteyment tizimi, TPMS (shinalar bosimi monitoringi) va telematikamodullari orqali avtomobillarga kirishga urinadi [13].

Milliy texnologiyalar instituti (NIST) va avtomobil sanoati uyushmalarining (ISAC) ma’lumotlariga ko‘ra, 2020–2024-yillarda avtomobil kiberxavfsizligi hodisalari soni 225 foizga oshgan. Eng xavfli ssenariylar qatoriga masofadan tormoz va rulni buzib qo‘yish, GPS firibgarligi (GPS spoofing) va avtopilot tizimlarini aldash kiradi [14].

Temiryo‘l transporti. Temiryo‘l tarmoqlari asosan uchta qatlamda zaiflikka ega: signalizatsiya va dispetcherlik tizimlari, yo‘lovchi axborot tizimlari, hamda haydovchi yordamchi tizimlar. Polsha temiryo‘lida 2023-yilda aniqlangan zaiflik hujumchilarning faqat radio to‘lqinlari orqali poyezdlarni to‘xtatishi mumkinligini ko‘rsatdi. Bu ETCS (Yevropa poyezd nazorat tizimi) protokolining zaif nuqtalaridan foydalanish edi [15].

Aviatsiya. Aviatsiya kibertahdidlari ayniqsa xavfli hisoblanadi, chunki bitta samolyotdagi nosozlik yuzlab odamning hayotiga xavf solib, milliardlab dollar zarar keltirishi mumkin. Asosiy zaif nuqtalar: ADS-B (Automatic Dependent Surveillance-Broadcast) tizimining kriptografik himoyasizligi, samolyot texnik xizmat ko‘rsatish tizimlariga masofadan kirish, aeroportning xavfli tarmoq integratsiyasi va yo‘lovchi Wi-Fi orqali bortkompyuterga kirish imkoniyatlari hisoblanadi [4].

2019-yilda Boing 737 MAX fojialari bevosita kiberxavfsizlik masalasi emas edi, ammo MCAS tizimining dasturiy kamchiliklari havo kemasi kiberxavfsizligiga yangicha nuqtayi nazardan qarashni taqozo etdi. FAA va EASA bunga javoban aviatsiya dasturiy ta’minot xavfsizligi standartlarini yangiladilar [5].

Dengiz transporti. Dengiz transportida kibertahdidlar asosan to‘rtta yo‘nalishda namoyon bo‘ladi: GPS firibgarligi (GPS Spoofing)

yordamida kemalarni noto‘g‘ri yo‘llarga yo'naltirish, AIS (Avtomatik identifikatsiya tizimi) manipulyatsiyasi, port operatsion tizimlariga hujumlar va yuk boshqaruv tizimlariga ruxsatsiz kirish. 2017-yilda O‘rta dengizda bir qator kemalarning GPS signallari soxtalashtirilgani va ular to‘g‘ri yo‘ldan ozib ketganligi qayd etildi[9].

Transport sohasidagi kiberhujumlarda qo‘llanadigan asosiy texnik usullar quyidagilar: Man-in-the-Middle (MitM) hujumlari – aloqa kanallarini o‘rtada ushlab qolish; Ransomware – tizimlarni shifrlash va to‘lov talab qilish; DDoS hujumlari – xizmatni ishdan chiqarish; Zero-day zaifliklari – hali yamoqlanmagan kamchiliklardan foydalanish; Fishing va ijtimoiy muhandislik – xodimlar orqali tizimga kirish; Ta’minot zanjiri hujumlari (Supply Chain Attack) – uchinchi tomon dasturlari orqali kirib borish [2, 3].

SCADA/ICS tizimlariga hujumlar alohida e’tiborni talab qiladi. Bu tizimlar ko‘pincha eski protokollar (Modbus, DNP3) asosida ishlaydi va dastlab tarmoqdan izolyatsiya qilingan bo‘lishga mo‘ljallangan edi. Zamonaviy integratsiya ularni internet bilan bog‘lab qo‘ydi, ammo xavfsizlik yangilanishlari ko‘p hollarda kechikib qolmoqda [8].

Transport sohasidagi kiberhujumlarning oqibatlari bir necha toifaga bo‘linadi. Iqtisodiy zararlar nuqtayi nazaridan Not-Petya hujumi Maersk kompaniyasiga 300 million dollar, WannaCry esa jami dunyoga taxminan 4 milliard dollar zarar yetkazdi [9]. Insonlar hayotiga xavf jihatidan masofadan avtomobil boshqaruvini egallash va poyezdlarni to‘xtatish voqealari bevosita yo‘lovchi va yo‘l foydalanuvchilari xavfsizligiga tahdid soldi. Ma’lumotlar oqishi sohasida SITA hodisasi millionlab yo‘lovchilarning shaxsiy ma’lumotlarini oshkor qildi [10]. Infratuzilma ishdan chiqishi borasida bir nechta yirik portlar va aeroportlar hujumlar oqibatida ishini to‘xtatishga majbur bo‘ldi.

Transport sohasini kiberhujumlardan himoya qilish uchun ko‘p qatlamli yondashuv talab etiladi. Texnik choralar sifatida tarmoqlarni segmentlash (Network Segmentation) orqali hujum tarqalishini cheklash, muntazam xavfsizlik auditlari va zaifliklarni skanerlash, kriptografik protokollarni joriy etish, real vaqt rejimida monitoring tizimlarini qo‘llash amalga oshirilishi zarur [11, 12].

Tashkiliy choralar doirasida xodimlarga kiberxavfsizlik bo‘yicha muntazam treninglar o‘tkazish, insident javob rejalarini ishlab chiqish va mashq qilish, ta’minot zanjiri xavfsizligini nazorat qilish, hamda davlat-xususiy hamkorlikni mustahkamlash tavsiya etiladi [13, 14].

Huquqiy va standartlashtirish choralariga kelsak, Yevropa ittifoqi 2022-yilda NIS2 direktivasini qabul qilib, transport sektorini muhim infratuzilma sifatida majburiy kiberxavfsizlik talablari doirasiga kiritdi. ENISA (Yevropa kiberxavfsizlik agentligi) transport kiberxavfsizligi bo‘yicha maxsus yo‘riqnomalar ishlab chiqqan [15].

O‘zbekistonda “Raqamli O‘zbekiston–2030” strategiyasi doirasida transport sohasida raqamlashtirishning kengayishi kibertahdidlarni ham dolzarb muammoga aylantirmoqda.

Guvohnoma № 636478 Litsenziya C-5669732 ISSN 3093-8546

Respublikada “aqlli” shaharsozlik tizimlarining joriy etilishi, temiryo‘l avtomatizatsiyasining kuchayishi va havo transportining modernizatsiyasi bilan bir qatorda kiberxavfsizlik infratuzilmasini rivojlantirish ham ustuvor vazifaga aylanib bormoqda.

O‘zbekistonning “Kiberxavfsizlik to‘g‘risida”gi qonuni (2022-yil) va Kiberxavfsizlik markazi transport tizimlarini kibertahdidlardan himoya qilishda muhim rol o‘ynaydi. Biroq global tajriba shuni ko‘rsatadiki, faqat qonunchilik choralarining o‘zi yetarli emas. Texnik va tashkiliy chora-tadbirlarni ham bir tizimda amalga oshirish zarur [1, 5].

Transport sohasidagi kiberhujumlar tarixi va rivojlanishini o‘rganish bir qator muhim xulosalar chiqarishga imkon beradi. Birinchidan, kibertahdidlar transport sohasida tobora murakkablashib va maqsadliroq bo‘lib bormoqda. Ikkinchidan, raqamlashuv va IoT qurilmalarining tarqalishi hujum yuzasini sezilarli darajada kengaytirmoqda. Uchinchidan, transport kiberhujumlari nafaqat iqtisodiy, balki insonlar hayotiga bevosita xavf soluvchi hodisalarga aylanishi mumkin. To‘rtinchidan, himoya ko‘p qatlamli, proaktiv va xalqaro hamkorlikka asoslanishi lozim.

O‘zbekiston uchun global tajribani o‘rganish va milliy kiberxavfsizlik salohiyatini mustahkamlash transport sohasining barqaror rivojlanishini ta’minlashda strategik ahamiyat kasb etadi.

Foydalanilgan adabiyotlar

1. Anderson R. Security Engineering: A Guide to Building Dependable Distributed Systems. Wiley, 2020. 1232 p. (Андерсон Р. Инженерия безопасности: Руководство по созданию надёжных распределённых систем. Уайли, 2020. 1232 с.)

2. Checkoway S. et al. Comprehensive Experimental Analyses of Automotive Attack Surfaces // USENIX Security Symposium. 2011. P. 1–16. (Чекоуэй С. и др. Комплексный экспериментальный анализ поверхностей атак в автомобилях // Симпозиум по безопасности USENIX. 2011. С. 1–16.)

3. ENISA. Cybersecurity in the Transport Sector. - European Union Agency for Cybersecurity, 2023. - 98 p. (ЭНАСА. Кибербезопасность в транспортном секторе. - Агентство Европейского Союза по кибербезопасности, 2023. 98 с.)

4. Costin A. Security of COTS IoT Products - Revisited // Black Hat Europe. - 2018. - P. 1–20. (Костин А. Безопасность коммерческих устройств IoT - пересмотр // Black Hat Европа. 2018. С. 1–20.)

5. Langner R. Stuxnet: Dissecting a Cyberwarfare Weapon // IEEE Security & Privacy. 2011. - Vol. 9, № 3. P. 49–51. (Лангнер Р. Stuxnet: Анатомия кибервоенного оружия // IEEE Безопасность и конфиденциальность. 2011. - Т. 9, № 3. С. 49–51.)

6. Miller C., Valasek C. Adventures in Automotive Networks and Control Units // DEF CON. 2013. P. 1–91. (Миллер К., Валасек К. Приключения в автомобильных сетях и блоках управления // DEF CON. 2013. С. 1–91.)

7. Miller C., Valasek C. Remote Exploitation of an Unaltered Passenger Vehicle // Black Hat USA. - 2015. - P. 1–92. (Миллер К.,

Валасек К. Удалённая эксплуатация неизменённого пассажирского автомобиля // Black Hat США. 2015. С. 1–92.)

8. Lee R. M., Assante M. J., Conway T. ICS CP/PE (Cyber-to-Physical or Process Effects) Case Study Paper – Ukraine Cyber Attack on the Power Grid. - SANS ICS, 2016. - 42 p. (Ли Р. М., Ассанте М. Дж., Конвей Т. Тематическое исследование кибератак на энергосистему Украины. - SANS ICS, 2016. 42 с.)

9. Greenberg A. Sandworm: A New Era of Cyberwar and the Hunt for the Kremlin's Most Dangerous Hackers. - Doubleday, 2019. 368 p. (Гринберг Э. Червь Sandworm: Новая эра кибервойны. Даблдэй, 2019. - 368 с.)

10. SITA. SITA Passenger Service System Data Security Incident, 2021. URL: https://www.sita.aero (Пресс-релиз по инциденту безопасности данных SITA, 2021.)

11. Upstream Security. Global Automotive Cybersecurity Report 2024. Tel Aviv: Upstream Security, 2024. 112 p. (Апстрим Секьюрити. Глобальный отчёт по кибербезопасности автомобилей 2024. - Тель-Авив: Апстрим Секьюрити, 2024. - 112 с.)

12. Wired. How Hackers Could Attack Freight Railways to Cause Chaos. 2023. URL: https://www.wired.com

13. NIST. Cybersecurity Framework for Transportation. National Institute of Standards and Technology, 2022. - 55 p. (НИСТ. Система кибербезопасности для транспорта. - Национальный институт стандартов и технологий, 2022. - 55 с.)

14. ISO/SAE 21434:2021. Road Vehicles - Cybersecurity Engineering. ISO, 2021. - 110 p. (ИСО/САЭ 21434:2021. Дорожные транспортные средства – Инжиниринг кибербезопасности. ИСО, 2021. - 110 с.)

15. European Union Agency for Cybersecurity (ENISA). Railway Cybersecurity - Security Measures in the Railway Sector. - ENISA, 2022. 132 p. (Агентство Европейского Союза по кибербезопасности. Кибербезопасность железных дорог. ЭНАСА, 2022. 132 с.)