ISSN: 2181-3906 2026

International scientific journal
«MODERN SCIENCE AND RESEARCH»
VOLUME 5 / ISSUE 4 / UIF:8.2 / MODERNSCIENCE.UZ

YO'L HARAKATI XAVFSIZLIGINI TA'MINLASHDA INTELLEKTUAL TRANSPORT TIZIMLARI (ITS) VA ULARNING KIBERXAVFSIZLIK MUAMMOLARI

Toxirov Asrorjon Axrorjon o'g'li
Huquqni muhofaza qilish akademiyasi
Magistratura fakulteti tinglovchisi.

https://doi.org/10.5281/zenodo.19594241

Annotatsiya. *Ushbu maqolada intellektual transport tizimlari (ITS) ning yo'l harakati xavfsizligini ta'minlashdagi roli va ushbu tizimlar bilan bog'liq kiberxavfsizlik muammolari ilmiy jihatdan tahlil etilgan. Zamonaviy transport infratuzilmasida ITS texnologiyalarining keng qo'llanilishi yo'l-transport hodisalari sonini kamaytirish, harakatni tartibga solish va favqulodda vaziyatlarga tezkor munosabat bildirish imkoniyatlarini sezilarli darajada oshirmoqda. Biroq, ushbu tizimlarning raqamli tarmoqlarga ulanishi yangi kiberxavfni vujudga keltirmoqda.*

Maqolada ITS komponentlari jumladan, aqlli svetoforlar, avtomatlashtirilgan yo'l belgilari, transport vositalararo aloqa tizimlari (V2X), yo'l kameralar va markaziy boshqaruv tizimlari - kiberxavfsizlik nuqtai nazaridan tahlil qilingan. Tadqiqot natijalari shuni ko'rsatadiki, ITS tizimlariga uyushtirilgan kiberhujumlar transport xavfsizligiga jiddiy tahdid solishi va inson hayotiga xavf tug'dirishi mumkin.

Kalit So'zlar: *intellektual transport tizimlari (ITS), kiberxavfsizlik, yo'l harakati xavfsizligi, V2X aloqa, aqlli transport infratuzilmasi, kiberhujumlar, axborot xavfsizligi, avtomatlashtirilgan boshqaruv tizimlari, transport telematikasi, tarmoq xavfsizligi.*

Abstract. *This article scientifically analyzes the role of intelligent transport systems (ITS) in ensuring road safety and the cybersecurity problems associated with these systems. The widespread use of ITS technologies in modern transport infrastructure significantly increases the ability to reduce the number of road accidents, regulate traffic, and respond quickly to emergencies. However, the connection of these systems to digital networks creates new cyber risks.*

The article analyzes ITS components, including smart traffic lights, automated road signs, vehicle-to-vehicle communication systems (V2X), road cameras, and central control systems, from a cybersecurity perspective. The results of the study show that cyberattacks on ITS systems can pose a serious threat to transport safety and endanger human life.

Keywords: *intelligent transportation systems (ITS), cybersecurity, road safety, V2X communication, smart transportation infrastructure, cyberattacks, information security, automated control systems, transportation telematics, network security.*

Аннотация. *В данной статье проводится научный анализ роли интеллектуальных транспортных систем (ИТС) в обеспечении безопасности дорожного движения и проблем кибербезопасности, связанных с этими системами. Широкое использование технологий ИТС в современной транспортной инфраструктуре значительно повышает возможности снижения числа дорожно-транспортных происшествий, регулирования движения и быстрого реагирования на чрезвычайные ситуации. Однако подключение этих систем к цифровым сетям создает новые киберриски. В статье анализируются компоненты ИТС, включая интеллектуальные светофоры, автоматизированные дорожные знаки, системы связи между транспортными средствами (V2X), дорожные камеры и централизованные системы управления, с точки зрения кибербезопасности.*

Результаты исследования показывают, что кибератаки на системы ИТС могут представлять серьезную угрозу безопасности дорожного движения и угрожать жизни людей.

Ключевые слова: *интеллектуальные транспортные системы (ИТС), кибербезопасность, безопасность дорожного движения, связь V2X, интеллектуальная транспортная инфраструктура, кибератаки, информационная безопасность, автоматизированные системы управления, транспортная телематика, сетевая безопасность.*

KIRISH

XXI asrning ikkinchi yarmiga kelib, shaharlar va mamlakatlar transport tizimlarini raqamlashtirish va intellektuallashtirish yo'lini tanlamoqda.

Intellektual transport tizimlari (ITS — Intelligent Transportation Systems) - bu axborot-kommunikatsiya texnologiyalari, sun'iy intellekt, sensor tarmoqlar va ma'lumotlar tahlilini transport infratuzilmasi bilan birlashtiruvchi kompleks yechimlar majmuasidir. Jahon sog'liqni saqlash tashkilotining (JST) ma'lumotlariga ko'ra, yo'l-transport hodisalari har yili dunyo bo'yicha 1,19 million kishining hayotiga zomin bo'lmoqda va 20-50 million kishini nogironlikka olib kelmoqda. [1] Ushbu ko'rsatkichlarni kamaytirish maqsadida ko'plab davlatlar ITS texnologiyalarini joriy etishni davlat siyosatining ustuvor yo'nalishi sifatida belgilagan.

O'zbekiston Respublikasida ham ushbu global tendentsiya davlat siyosati darajasida qo'llab-quvvatlanmoqda. Prezident Shavkat Mirziyoyev tomonidan 2020 yilda e'lon qilingan "Raqamli O'zbekiston - 2030" strategiyasi mamlakatni raqamli iqtisodiyotga o'tkazishning yo'l xaritasini belgilab, transport sohasini raqamlashtirish vazifasini ustuvorlar qatoriga qo'ydi.[2] Ushbu strategiya doirasida Toshkent, Samarqand, Buxoro, Namangan va boshqa yirik shaharlarda aqlli svetoforlar, tezlikni nazorat qiluvchi kameralar, avtomatlashtirilgan yo'l harakati boshqaruv tizimlari (ATMS) va elektron to'lov infratuzilmasi joriy etildi. Biroq, akademik A.A. Abduqodirov va professor R.X. Yunusovlarning fundamental "Axborot xavfsizligi asoslari" darsligida ta'kidlanganidek: "Har qanday tizimning raqamli tarmoqlarga ulanishi uning xavfsizligi uchun yangi zaiflik vektorlarini vujudga keltiradi. Raqamlashtirish va kiberxavfsizlik bir tanganing ikki tomoni bo'lib, birgalikda ko'rib chiqilmasa, kutilgan natijaga erishib bo'lmaydi". [3] Ushbu mulohaza ITS uchun ayniqsa dolzarb, chunki ushbu tizimlar to'g'ridan-to'g'ri inson hayoti va xavfsizligi bilan bog'liq.

ITS tizimlarining kiberxavfsizlik muammosi bir necha jihatdan o'ziga xos murakkablikka ega: birinchidan, oddiy axborot tizimiga kiberhujum ma'lumot yo'qotilishiga olib keladi. ITS ga kiberhujum esa svetofor tizimini izdan chiqarishi, yo'l-transport hodisasiga, hattoki odamlar hayotiga xavf tug'dirishi mumkin. Ikkinchidan, tizimning tarqoq va murakkab tuzilishi.

[1] World Health Organization. (2023). Global status report on road safety 2023. Olingan manzil: Global status report on road safety 2023

[2] "Raqamli O'zbekiston — 2030" strategiyasi, PF-6079-sonli Farmon (2020). Olingan manzil: https://lex.uz/docs/5031048

[3] Abduqodirov A.A., Yunusov R.X. Axborot xavfsizligi asoslari: Darslik (3-nashr). — Toshkent: TATU nashriyoti, 2021. — 412 b.

ITS bir nechta o’zaro ulangan kichik tizimlardan iborat: svetoforlar, yo’l kameralari, V2X aloqa qurilmalari, markaziy serverlar, mobil ilovalar. Bunday murakkab tarqoq tizimlarning kiberxavfsizligini ta’minlash oddiy tarmoqqa qaraganda qiyinroq hisoblanadi. Uchinchidan, milliy qonunchilikdagi normativ bo’shliqlar. O’zbekistonda axborot xavfsizligi sohasida bir qator qonunlar mavjud bo’lsa-da, ITS ga xos kiberxavfsizlik talablari hali to’liq shakllanmagan. Bu esa amaliy jihatdan himoya choralarini belgilashda noaniqlik tug’dirmoqda.

METODOLOGIYA VA ADABIYOTLAR TAHLILI

Mazkur tadqiqotda metodologik asos sifatida ilmiy adabiyotlar sharhi bilan bir qatorda O’zbekiston Respublikasining amaldagi normativ-huquqiy hujjatlari ham tahlil qilindi. Xususan, yo’l harakati xavfsizligi, transportni raqamlashtirish, axborot tizimlari muhofazasi, kiberxavfsizlik va shaxsga doir ma’lumotlarni qayta ishlashga oid qonunlar o’rganildi. Ushbu yondashuv ITSni xalqaro tajriba va milliy huquqiy mexanizmlar kesimida kompleks baholash imkonini berdi.

“Yo‘l harakati to‘g‘risida”gi Qonunda esa yo‘l harakati monitoringi axborotni hisobga olish, umumlashtirish, qayta ishlash va tahlil qilish jarayoni sifatida talqin qilingan. Bundan tashqari, yo‘l harakatini boshqarishning avtomatlashtirilgan tizimlarini joriy etish, yirik shaharlarda tirbandliklarning oldini olishga qaratilgan avtomatlashtirilgan axborot tizimlarini yaratish nazarda tutilgan.[4] Mazkur qoidalar ITSning milliy darajada amaliy joriy etilishi uchun to‘g‘ridan-to‘g‘ri normativ poydevor vazifasini bajaradi. Kiberxavfsizlik nuqtai nazaridan “Kiberxavfsizlik to‘g‘risida”gi Qonun alohida ahamiyatga ega. Unda transport sohasi muhim axborot infratuzilmasi obyektlari qatoriga kiritilgan. Shu sababli transportdagi axborot tizimlari operatorlari uzluksiz ishlashni ta’minlashi, monitoring tizimlarini joriy etishi, kiberhodisalar haqida vakolatli organga xabar berishi va belgilangan xavfsizlik talablariga rioya qilishi shart. Bu talablar ITS operatorlari uchun bevosita majburiy kiberxavfsizlik standartlarini shakllantiradi.[5]

“Axborotlashtirish to‘g‘risida”gi Qonunda axborot tizimlari va axborot resurslarini muhofaza qilishning asosiy maqsadlari belgilangan bo‘lib, ular orasida axborotning tarqalib ketishi, o‘g‘irlanishi, yo‘qotilishi, buzib talqin etilishi, to‘sib qo‘yilishi va qalbakilashtirilishining oldini olish ko‘rsatilgan.[6] ITS tarkibidagi markazlashgan boshqaruv platformalari, ma’lumotlar bazalari va sensor tarmoqlari aynan shu himoya talablariga mos ravishda loyihalanishi lozim. Agar ITS videokuzatuv, raqamli identifikatsiya, avtomatik jarima tizimlari yoki haydovchi va yo‘lovchilarga doir ma’lumotlarni qayta ishlasa, “Shaxsga doir ma’lumotlar to‘g‘risida”gi Qonun talablari ham tatbiq etiladi. Ayniqsa, biometrik ma’lumotlar va shaxsni aniqlashga xizmat qiluvchi tasvirlar bilan ishlashda rozilik, qonuniy asos va ma’lumotlarni O‘zbekiston hududida saqlash talablari dolzarb hisoblanadi. “Transport to‘g‘risida”gi Qonun esa transport faoliyatining asosiy prinsiplari sifatida qonuniylik, xavfsizlik, ochiqlik va shaffoflikni belgilaydi hamda transport tizimini zamonaviy innovatsion va axborot-kommunikatsiya texnologiyalari asosida raqamlashtirish choralarini nazarda tutadi.[7] Shu jihatdan mazkur qonun ITSni transport xizmatlarining ishonchliligi va boshqaruv samaradorligini oshiruvchi mexanizm sifatida huquqiy jihatdan mustahkamlaydi.

[4] “Yo’l harakati to’g’risida”gi qonun. Olingan manzil: https://lex.uz/docs/-6764454
[5] “Kiberxavfsizlik to’g’risida”gi qonun. Olingan manzil: https://lex.uz/uz/docs/-5960604
[6] “Axborotlashtirish to’g’rsida”gi qonun. Olingan manzil: https://lex.uz/docs/-83472
[7] “Transport to’g’risida”gi qonun. Olingan manzil: https://lex.uz/uz/docs/-5563039

Intellektual transport tizimlari (ITS) xavfsizlik, samaradorlik va barqarorlikni yaxshilash uchun ilg'or texnologiyalarni transport infratuzilmasi va transport vositalariga integratsiyalashni anglatadi. Sun'iy intellekt, IoT (narsalar interneti), katta ma'lumotlar tahlili va simsiz aloqa kabi innovatsiyalardan foydalanib, ITS trafikni oqilona boshqarish, real vaqtda monitoring va avtomatlashtirilgan qarorlar qabul qilish imkonini beradi. Ushbu tizimlar tirbandlikni kamaytirishga, yo'l harakati xavfsizligini oshirishga, chiqindilarni kamaytirishga yordam beradi va shahar va qishloq muhitlari uchun uzluksiz harakatlanish echimlarini taqdim etadi.[8]

Umuman olganda, mavjud tahlillar ITSning yo‘l harakati xavfsizligini ta’minlashdagi ahamiyatini keng yoritgan bo‘lsa-da, aynan kiberxavfsizlik muammolarini kompleks yondashuv asosida o‘rganish yetarli darajada rivojlanmagan. Shu bois, mazkur tadqiqot ushbu bo‘shliqni to‘ldirishga qaratilgan.

NATIJALAR VA MUHOKAMA

Tahlil natijalariga ko‘ra, ITS yo‘l harakati xavfsizligini oshirishda uchta asosiy mexanizm orqali samarali ishlaydi: vaziyatni tezkor aniqlash, qaror qabul qilishni avtomatlashtirish va ishtirokchilar o‘rtasida tezkor axborot almashinuvi. Sensorlar, kameralar, radarlar va ulanish modullari yordamida yo‘ldagi real holat to‘g‘risidagi ma’lumotlar markaziy tizimlarga uzatiladi; natijada tirbandliklar, avariya xavfi, yo‘l sharoiti yoki qoidabuzarliklar erta aniqlanadi. V2X aloqa esa transport vositalari va infratuzilma o‘rtasida xavfsizlikka doir xabarlarni uzatib, to‘qnashuvlar ehtimolini kamaytiradi. Biroq aynan shu bog‘liqlik ITSni cyber-physical tizimga aylantiradi va kiberhujum oqibatlarini jismoniy xavfga olib chiqadi. Agar hujumchi xavfsizlik xabarlarini qalbakilashtirsa, noto‘g‘ri tirbandlik yoki xavf ogohlantirishlarini tarqatsa, GPS signalini chalg‘itsa yoki markaziy boshqaruv tizimiga kirsa, transport oqimlari noto‘g‘ri boshqarilishi, favqulodda yordam marshrutlari to‘silishi yoki foydalanuvchilarga yolg‘on ko‘rsatmalar berilishi mumkin.[9] Bundan shuni xulosa qilish mumkin, ITSda axborot yaxlitligi va autentikligi yo‘l xavfsizligining bevosita shartiga aylanadi.

Sun’iy intellekt asosidagi ITS komponentlarida xavf yanada murakkablashadi. Avtonom yoki yarim avtonom transport tizimlarida mashinaviy o‘rganish modellariga adversarial hujumlar orqali obyektlar noto‘g‘ri tanilishi, belgilar yanglish talqin qilinishi yoki qaror qabul qilish tizimlari chalg‘itilishi mumkin. Bu esa odatiy IT-himoya choralari bilan to‘liq bartaraf etilmaydigan, ma’lumotlar tozaligi, model validatsiyasi, izohlanish va audit talab qiladigan yangi xavf maydonini yaratadi. ENISA Natijalar shuni ham ko‘rsatadiki, ITSda samarali himoya faqat bitta texnologik vosita bilan ta’minlanmaydi. Amaliy tavsiyalar qatlamli xavfsizlik arxitekturasi, tarmoq segmentatsiyasi, kuchli autentifikatsiya, sertifikat infratuzilmasi, trafikni shifrlash, qurilmalarni inventarizatsiya qilish, xavfsiz firmware va zaifliklarni boshqarish tizmlarini joriy etishni talab qiladi.[10] Yo‘l harakati xavfsizligi texnologiyalari: ITS doirasida avariya va hodisalarni oldini olish, ularga tezkor javob berish texnologiyalari rivojlanmoqda. Masalan, maxsus favqulodda xizmat transportiga ustunlik berish qurilmalari svetoforlarda tez yordam va yong‘in mashinalariga yashil chiroq yoqib, ularning kechikmasdan o‘tishini ta‘minlaydi.

[8] Intellektual transport tizimlari. Olingan manzil: https://fiberroad.com/uz/intelligent-transportation-systems/
[9] ITS Cybersecurity. Olingan manzil: ITS Cybersecurity | ITS Deployment Evaluation
[10] Cybersecurity Best Practices for the Safety of Modern Vehicles. Release 2022.

Yevropa Ittifoqida esa barcha yangi yengil mashinalar uchun avtomatik eCall tizimi majburiy joriy etilib, avariya sodir bo‘lsa avtomatik tarzda 112 xizmatiga joylashuv ma‘lumotlarini uzatish talabi qo‘yilgan (2018-yildan boshlab). Transport vositalaridagi to‘qnashuv oldi ogohlantirish sistemalari, yo‘l bo‘ylab piyodalarni aniqlash sensorlari, tezlikni avtomatik cheklovchi qurilmalar ham shu toifa texnologiyalarga kiradi.[11] Shu nuqtai nazardan, ITS uchun eng muhim ilmiy-amaliy xulosa shuki, kiberxavfsizlik transport tizimiga keyinchalik qo‘shiladigan yordamchi modul emas. U transport xavfsizligi me’yorlari, tizim dizayni, ekspluatatsiya, monitoring va modernizatsiya jarayonlari bilan integratsiyalashgan holda boshqarilishi zarur. Aks holda, aqlli transport texnologiyalarining xavfsizlikka keltiradigan ijobiy samarasi kiberxatarlar tufayli sezilarli darajada pasayishi mumkin.

XULOSA

Xulosa qilib aytganda, intellektual transport tizimlari yo‘l harakati xavfsizligini oshirish, tirbandliklarni kamaytirish, favqulodda holatlarni tez aniqlash va boshqaruv sifatini yaxshilashda katta salohiyatga ega. Biroq ITSning samaradorligi uning raqamli ishonchliligiga chambarchas bog‘liq. V2X aloqa, aqlli infratuzilma, markaziy boshqaruv markazlari va AI-modullar kiberhujumlardan yetarli darajada himoyalanmasa, ular xavfsizlikni oshiruvchi vosita o‘rniga qo‘shimcha xavf manbaiga aylanishi mumkin. Shuning uchun ITSni joriy etishda texnologik innovatsiyalar bilan bir qatorda kiberbardoshlilik ham ustuvor vazifa bo‘lishi kerak. Xususan, xavfsizlikni loyihalash bosqichidan integratsiya qilish, standartlarga tayangan boshqaruv, doimiy risk baholash, segmentatsiya, identifikatsiya va autentifikatsiya va insidentlarga tayyorgarlik kelajakdagi ITS ekotizimining ishonchliligini belgilab beradi. Ilmiy nuqtai nazardan esa keyingi tadqiqotlar real shahar infratuzilmasida kiberbardoshlilik ko‘rsatkichlarini baholash, AI-modullarni verifikatsiya qilish va rivojlanayotgan mamlakatlar sharoitiga mos model ishlab chiqishga qaratilishi maqsadga muvofiq bo’ladi.

Xulosa qilib aytganda, O‘zbekiston Respublikasining milliy qonunchiligi intellektual transport tizimlarini joriy etish va ularning xavfsiz ishlashini ta’minlash uchun yetarlicha muhim normativ asoslarni o‘z ichiga oladi. “Yo‘l harakati xavfsizligi to‘g‘risida”gi, “Yo‘l harakati to‘g‘risida”gi, “Kiberxavfsizlik to‘g‘risida”gi, “Axborotlashtirish to‘g‘risida”gi va “Transport to‘g‘risida”gi qonunlar ITSni joriy etish, monitoring qilish, himoyalash va ma’lumotlarni qonuniy qayta ishlashning asosiy huquqiy tayanchlarini belgilaydi. Shu sababli ilmiy maqolada ITS masalasini faqat texnologik nuqtai nazardan emas, balki milliy huquqiy tartibga solish nuqatai nazardan ham yoritilishi maqsadga muvofiqdir. Bu maqolaning dolzarbligi, ilmiy asoslanganligi va O‘zbekiston amaliyotiga mosligini sezilarli oshiradi.

FOYDALANILGAN ADABIYOTLAR

1. World Health Organization. (2023). Global status report on road safety 2023. Olingan manzil: Global status report on road safety 2023
2. “Raqamli O’zbekiston — 2030” strategiyasi, PF-6079-sonli Farmon (2020). Olingan manzil: https://lex.uz/docs/5031048

[11] Rivojlangan davlatlarda intellectual transport tizimlari: tajriba, samaradorlik va istiqbollar. Quljanov Farhod Berdiyorovich. [maqola].

3. Abduqodirov A.A., Yunusov R.X. Axborot xavfsizligi asoslari: Darslik (3-nashr). — Toshkent: TATU nashriyoti, 2021. — 412 b.
4. “Yo’l harakati to’g’risida”gi qonun. Olingan manzil: https://lex.uz/docs/-6764454
5. “Kiberxavfsizlik to’g’risida”gi qonun. Olingan manzil: https://lex.uz/uz/docs/-5960604
6. “Axborotlashtirish to’g’rsida”gi qonun. Olingan manzil: https://lex.uz/docs/-83472
7. “Transport to’g’risida”gi qonun. Olingan manzil: https://lex.uz/uz/docs/-5563039
8. Intellektual transport tizimlari. Olingan manzil: https://fiberroad.com/uz/intelligent-transportation-systems/
9. ITS Cybersecurity. Olingan manzil: ITS Cybersecurity | ITS Deployment Evaluation
10. Cybersecurity Best Practices for the Safety of Modern Vehicles. Release 2022.
11. Rivojlangan davlatlarda intellectual transport tizimlari: tajriba, samaradorlik va istiqbollar. Quljanov Farhod Berdiyorovich. [maqola].