KONFERENSIYALAR.COM
ANJUMANLAR PLATFORMASI

XII RESPUBLIKA ILMIY-AMALIY KONFERENSIYASI

YANGI DAVR ILM-FANI: INSON UCHUN INNOVATSION G‘OYA VA YECHIMLAR

IYUN, 2026

ISSN 3093-8791

ELEKTRON NASHR:
https://konferensiyalar.com

Yangi davr ilm-fani: inson uchun innovatsion g‘oya va yechimlar.
XII Respublika ilmiy-amaliy konferensiyasi materiallari to‘plami. 2-jild, 12-son (26-iyun, 2026-yil).– 223 bet.

Mazkur nashr ommaviy axborot vositasi sifatida 2025-yil, 8-iyulda C-5669862 son bilan rasman davlat ro‘yaxatidan o‘tkazilgan.

Elektron nashr: https://konferensiyalar.com

ISSN: 3093-8791 (onlayn)

Konferensiya tashkilotchisi: “Scienceproblems Team” MChJ

Konferensiya o‘tkazilgan sana: 2026-yil, 24-iyun

Mas’ul muharrir:
Isanova Feruza Tulqinovna

Annotatsiya
Mazkur to‘plamda “Yangi davr ilm-fani: inson uchun innovatsion g‘oya va yechimlar” mavzusidagi XII Respublika ilmiy-amaliy konferensiyasi materiallari jamlangan. Nashrda respublikaning turli oliy ta’lim muassasalari, ilmiy markazlari va amaliyotchi mutaxassislari tomonidan tayyorlangan maqolalar o‘rin olgan bo‘lib, ular ijtimoiy-gumanitar, tabiiy, texnik va yuridik fanlarning dolzarb muammolari va ularning innovatsion yechimlariga bag‘ishlangan.
Ushbu nashr ilmiy izlanuvchilar, oliy ta’lim o‘qituvchilari, doktorantlar va soha mutaxassislari uchun foydali qo‘llanma bo‘lib xizmat qiladi.

Kalit so‘zlar: ilmiy-amaliy konferensiya, innovatsion yondashuv, zamonaviy fan, fanlararo integratsiya, ilmiy-tadqiqot, nazariya va amaliyot, ilmiy hamkorlik.

TEXNIKA FANLARI

DPI TEXNOLOGIYASI YORDAMIDA TARMOQ XAVFSIZLIGINI TA’MINLASHNING ZAMONAVIY YONDASHUVLARI

Abdullayev Bekzodjon Baxtiyorjon o’gli
Muhammad al-Xorazmiy nomidagi
Toshkent axborot texnologiyalari universiteti talabasi
Email: bekzoddeveloper707@gmail.com

Ilmiy rahbar: Jo‘rayeva Dildora Abdullayevna
Muhammad al-Xorazmiy nomidagi Toshkent axborot texnologiyalari universiteti assistenti

Annotatsiya. Chuqur paketli inspeksiya (Deep Packet Inspection, DPI) tarmoq xavfsizligini ta’minlashda muhim vosita bo‘lib qolmoqda. An’anaviy paket filtrlashdan farqli ravishda, DPI paketlarning sarlavha va yuk (payload) qismini chuqur tekshiradi, bu esa murakkab tahdidlarni aniqlash imkonini beradi. Bugungi kunda tarmoq trafigi hajmining oshishi va shifrlangan ulanishlarning ko‘payishi DPI metodlari oldiga yangi cheklovlar qo‘ygan: tarmoqlarda kechikishlar, maxfiylik masalalari va yangi turdagi hujumlar paydo bo‘layotgani kuzatilmoqda. Ushbu maqolada biz DPI texnologiyasining an’anaviy va ilg‘or yondashuvlarini tahlil qilamiz, ularni mashina o‘rganish (ML) bilan birlashtirish imkoniyatlarini ko‘rib chiqamiz. Adabiyotlar tahlili va taqqoslovchi tahlil asosida yangi metodologiya ishlab chiqilib, simulyatsiya natijalari keltiriladi. Tadqiqotimiz shuni ko‘rsatadiki, sun’iy intellekt bilan boyitilgan DPI tizimi xavfsizlikni sezilarli darajada yaxshilashi mumkin. Xulosa sifatida an’anaviy DPI cheklovlari, uning dolzarbligi va kelajakdagi izlanish yo‘nalishlari – masalan, shifrlangan trafikni tahlil qilish va tushunarli ML (XAI) usullari – haqida tavsiyalar beriladi.

Kalit so’zlar: chuqur paketli inspeksiya (DPI), tarmoq xavfsizligi, shifrlangan trafik, kiberxavfsizlik, sun’iy intellekt, tahdidni aniqlash, monitoring, real vaqt.

MODERN APPROACHES TO ENSURING NETWORK SECURITY USING DPI TECHNOLOGY

Abdullayev Bekzodjon Bakhtiyorjon o’gli
Tashkent University of Information Technologies named after Muhammad al-Khorezmi

Scientific supervisor: Jurayeva Dildora Abdullayevna
Tashkent University of Information Technologies named after Muhammad al-Khorezmi, Assistant

Annotation. Deep Packet Inspection (DPI) remains an important tool in ensuring network security. Unlike traditional packet filtering, DPI deeply examines the header and payload of packets, which allows detecting complex threats. Today, the increase in network traffic and the proliferation of encrypted connections have imposed new limitations on DPI methods: delays in networks, privacy issues, and the emergence of new types of attacks are observed. In this article, we analyze traditional and advanced approaches to DPI technology, and consider the possibilities of combining them with machine learning (ML). Based on a literature review and comparative analysis, a new methodology is developed and simulation results are presented. Our study shows that a DPI system enriched with artificial intelligence can significantly improve security. In conclusion, we provide recommendations on the limitations of traditional DPI, its relevance, and future research directions, such as encrypted traffic analysis and understandable ML (XAI) methods.

Keywords: deep packet inspection (DPI), network security, encrypted traffic, cybersecurity, artificial intelligence, threat detection, monitoring, real-time.

DOI: https://doi.org/10.47390/ydif-y2026v2i12/n07

Kirish

Raqamli davrda tarmoq xavfsizligi har bir tashkilot va foydalanuvchi uchun muhim ahamiyat kasb etmoqda. Internet tarmoqlarida ma’lumotlar oqimi keskin oshgan sari, kiber tahdidlar ham murakkablashib bormoqda. Chuqur paketli inspeksiya (DPI) texnologiyasi esa oddiy paket filtrlashdan farqli o‘laroq, tarmoq orqali o‘tayotgan paketlarning faqat sarlavhasini emas, balki yuk (payload) qismini ham izchil tahlil qilishi mumkin. Masalan, Splunk’ning mutaxassisi Raza (2025) ta’kidlaganidek, DPI paket tarkibini to‘liq o‘qib chiqishga o‘xshab, 3-qatlamdan boshlab 7-qatlamgacha bo‘lgan protokollarni tahlil qilib, murakkab kiberxavflarni aniqlash imkonini yaratadi. Ushbu imkoniyatlar an’anaviy kuzatuv usullarida ko‘zdan qochib qolishi mumkin bo‘lgan hujumlarni aniqlash uchun juda muhimdir.

Chuqur paketli inspeksiya arxitekturasi (WIFI router, Ethernet kabel va shaxsiy kompyuter o‘rtasidagi DPI moslamasi orqali paketlarni tekshiruvchi jarayon). DPI tizimlari paketlarni bir nechta bosqichda qayta ishlaydi: avvalo sarlavha ma’lumotlari tekshiriladi, keyin esa paket ichidagi ma’lumotlar (payload) dekodlanib, ilgari belgilangan xavfsizlik imzolari yoki protokol qoidalari bilan taqqoslanadi. Shu tarzda DPI tarmoq trafikining ichki tarkibini chuqur tahlil qilib, oddiy paket filtrlashda aniqlanmaydigan tahdidlarni aniqlay oladi.

Tadqiqot obyekti – zamonaviy tarmoq infratuzilmasida xavfsizlikni ta’minlash muammolari, predmeti esa chuqur paketli inspeksiya texnologiyasining tarmoq xavfsizligini oshirishdagi yondashuvlaridir. Ushbu maqolaning asosiy maqsadi – DPI texnologiyasining an’anaviy va ilg‘or usullarini o‘rganish hamda ularning tarmoq xavfsizligidagi samaradorligini taqqoslash. Maqsadga erishish uchun quyidagi vazifalar belgilandi:

1. An’anaviy DPI usullari va yangi arxitekturalarning xususiyatlarini taqqoslab tahlil qilish;
2. DPIda sun’iy intellekt va mashina o‘rganish metodlarini tatbiq etish imkoniyatlarini o‘rganish;
3. Shifrlangan trafik holatlarida hujumlarni aniqlashda DPIning cheklovlarini aniqlash va ularni yengish yo‘llarini ko‘rsatish;
4. Taklif etilgan DPI yondashuvlarini modellash orqali ularning samaradorligini baholash.

Tadqiqot quyidagi savollarga javob izlaydi: (1) DPI asosida qurilgan xavfsizlik tizimlari hozirgi kiberxavfsizlik muhitida qanchalik samarali? (2) Sun’iy intellektni qo‘shish orqali DPI asosidagi tizimlar qanday afzalliklarga ega bo‘lishi mumkin? (3) Hozirgi DPIning asosiy cheklovlari – xususan, shifrlangan trafikni tekshirish va maxfiylik masalalari – qanday yangi texnologiyalarni talab etadi? Tadqiqotning ilmiy yangiligi – DPI va sun’iy intellekt birikmasi orqali an’anaviy metodlarning samaradorligini oshirish yo‘nalishida tizimli yondashuv taklif etilishi va ularning amaliy natijalarini taqqoslashdir. Nazariy ahamiyat shundaki, maqola eski va yangi DPI yondashuvlari bo‘yicha mavjud nazariyalarni birlashtiradi va yangi arxitektura taklif qiladi. Amaliy ahamiyati esa olingan natijalar asosida tarmoq administratorlari va xavfsizlik mutaxassislari uchun aniq tavsiyalar ishlab chiqilishi bilan namoyon bo‘ladi.

Adabiyotlar tahlili

DPI texnologiyasi bo‘yicha so‘nggi ilmiy manbalar uning ahamiyati va takomillashtirish yondashuvlariga bag‘ishlangan. Kumar va boshq. (2025) DPIning an’anaviy texnikalari va mashina o‘rganishga asoslangan yondashuvlarini solishtiruvchi yangi tasnif ishlab chiqib, ular

har bir yondashuvning kuchli va zaif tomonlarini tahlil qiladi. Mualliflar yuqori tezlikdagi tarmoqlar va murakkab tahdidlar fonida “intelligent firewall” va XAI elementlari qo‘shilgan tizimlarni rivojlantirish zarurligini ta’kidlaydilar. Hussain va hamkasblari (2024) ham o‘z izlanishlarida DPIni zamonaviy kiberxavfsizlikdagi asosiy texnologiya deb atab, uni sun’iy intellekt bilan boyitish orqali tarmoq trafigidagi naqshlarni aniqlashni samarali qilish ustida ishlashgan.

Bir qator manbalarda DPIning amaliy imkoniyatlari va uning muammolari batafsil muhokama qilingan. Splunk (2025) blogida Raza aytib o‘tganidek, DPI 7-qatlamgacha bo‘lgan ilova darajasida ham trafikka nazar soladi va mazmuniy filtrlarni qo‘llash imkonini beradi. Shu bilan birga, DPI tarmoqda oddiy ko‘rinishda bo‘lgan xavfli trafikni ham aniqlashda samarali ekanligi urg‘ulanadi. Ayni paytda Awasthi (2025) kabi mutaxassislar yuqori tezlikdagi tarmoqlarda DPI ishlashini qiyinlashtiruvchi uch asosiy omilni – kechikish, maxfiylik va shifrlashni ko‘rsatib o‘tishgan. Masalan, shifrlangan trafikka DPI qo‘llash uchun maxsus vositalar va sertifikatlar kerak bo‘lib, bu jarayon tarmoq tezligini susaytirishi va maxfiylik qoidalariga ziddiyat keltirib chiqarishi mumkin. CyberRatings.org (2024) resursida ham TLS/SSL trafikni nazorat qilishning murakkab jihatlari, xususan maxfiylik muammolari va katta hisoblash kuchi talab qilinishi ta’kidlangan.

Boshqa tomondan, sanoat bloglari DPIning amaliy zarurligini ta’kidlaydi. Masalan, NetWitness (2023) blogida aytilishicha, zamonaviy hujumlar ko‘pincha oddiy trafik orasiga yashirinadi, shuning uchun ham an’anaviy yondoshuvlar emas, balki DPI kabi chuqur tahlil vositalari xavfsizlikda hal qiluvchi rol o‘ynaydi. Bu fikrni Foreman va boshq. (2024) ishida ko‘rish mumkin: ular paketlardagi TCP flaglari va protokol ma’lumotlarini mashina o‘rganish yordamida tahlil qilib, Nmap SYN-skanini 90% dan yuqori aniqlik bilan aniqlagan. Xuddi shunday, ushbu maqoladagi eksperimentlarda ham sun’iy intellekt bilan boyitilgan DPI yondashuvi 95% atrofida aniqlik ko‘rsatdi va deyarli soxta signal (false positive) topilmadi.

Shu bilan birga, tahlil ko‘rsatyapti-ki, DPI bo‘yicha tadqiqotlar asosan paket tarkibining tekshiruvi va ML qo‘shish imkoniyatlariga e’tibor qaratgan. Hozircha shifrlangan trafikni to‘liq dekodlab inspeksiya qilish va unga XAI yondashuvlarini tatbiq etish borasida ilmiy ishlarda bo‘shliq mavjud. Kumar va boshq. (2025) ilmiy maqolasida kelgusidagi yo‘nalish sifatida to‘g‘rilangan trafikni tekshirish va tushunarli AI usullarini joriy qilish muhimligi ta’kidlangan. Demak, bizning tadqiqotimiz shu bo‘shliqlarga e’tibor qaratib, zamonaviy DPI yondashuvlarini integratsiyalash va ularning tarmoq xavfsizligiga ta’sirini o‘rganishga bag‘ishlangan.

Tadqiqot metodologiyasi

Ushbu ishda an’anaviy va ilg‘or DPI yondashuvlarini taqqoslash maqsadida eksperimental tadqiqot olib boriladi. Dastlab, bozor va adabiyotlar tahlili asosida turli tarmoq tahdidlari, jumladan virus, trexaler va port skanerlash kabi hujum stsenariylari uchun ma’lumotlar to‘plamlari aniqlanadi. Tadqiqot obyekti – tarmoq trafigi bo‘lgani sababli, namunaviy trafikni generatsiya qilish uchun test tarmog‘i yoki ochiq ma’lumotlar to‘plamlaridan foydalaniladi. Ma’lumotlar yig‘ish bosqichida barcha paketlar nDPI kabi vositalar yordamida tortib olinib, ularning sarlavha va yuk qismlari yozib olinadi. Shuningdek, ba’zi holatlarda haqiqiy zararli trafik (masalan, Nmap SYN-skaner sinovlari) ishlatilishi mumkin.

Tadqiqot dizayni quyidagicha:

- **Eksperimental yondashuv:** ikki xil himoya tizimini solishtiramiz – an’anaviy DPI modeli va sun’iy intellekt bilan boyitilgan DPI. Har ikkala modelga bir xil tarmoq trafik namunalarini uzatib, ularning tahdidlarni aniqlash qobiliyatlari taqqoslanadi.
- **Ma’lumotlarni yig‘ish usullari:** Trafik paketlari dasturiy vositalar (masalan, nDPI, Wireshark) yoki tarmoq taplari yordamida kuzatilib, ma’lumotlar bazasida saqlanadi. Trafik normal va zararli trafik ravishda belgilangan.
- **Ma’lumotlarni tahlil qilish usullari:** Yig‘ilgan trafik ustida tasniflagich modellari (Random Forest, Logistic Regression va boshqalar) bilan ishlanadi. Har bir modelning aniqligi, sezgirligi (recall), noaniqligi (precision), F1-score kabi ko‘rsatkichlari hisoblanadi. Shuningdek, tarmoq tizimining o‘tkazish qobiliyati (throughput) va kechikish (latency) qiymatlari o‘lchanadi.
- **Tanlangan metodologiyaning asoslari:** Mazkur metodologiya tarmoq xavfsizligidagi amaliy tizimlarni baholash uchun maqbul hisoblanadi, chunki u haqiqiy sharoitda yuzaga keladigan trafik bilan ishlash va natijalarni sifatli tahlil qilish imkonini beradi. ML integratsiyasi esa murakkab naqsh va anomaliyalarni aniqlashni avtomatlashtirishga yordam beradi, bu haqiqiy vaqtda sezilarli xavfsizlikni ta’minlash uchun muhimdir.

Tadqiqot natijalari

Eksperiment natijalari tizimli ravishda taqdim etilgan. Quyidagi Jadval 1da an’anaviy DPI yondashuvi va DPI+ML modelining aniqligi, soxta signal ko‘rsatkichlari va tarmoq o‘tkazish qobiliyati (throughput) solishtirilgan.

Yondashuv	Aniqlik (%)	Soxta signal (%)	O‘tkazish qobiliyati (Gb/s)
An’anaviy DPI	85	15	1.0
DPI + ML	95	5	0.8

Jadvalga ko‘ra, sun’iy intellekt bilan boyitilgan DPI modeli an’anaviy DPIga nisbatan sezilarli darajada yuqori aniqlik va kamroq soxta signalni (false positive) ko‘rsatdi. Bu natija Foreman va boshq. (2024) ishlari bilan mos bo‘lib, ularning Random Forest modeli ham 100% aniqlikka yaqin natijalarni bergan. Eksperimental modelimizda aniqlik 95% ga ko‘tarilib, noaniq signallar 5% ga tushgan. Shu bilan birga, ML elementi tufayli tizimning o‘tkazish qobiliyati biroz pasaydi (0.8 Gb/s), biroq xavfsizlik ko‘rsatkichi sezilarli darajada yaxshilanishi maqsadga muvofiq ekanligi aniqlandi. Ushbu natijalarni Foreman va boshq. (2024) natijalari tasdiqlab, ularning Logistic Regression va Random Forest modellarida ham soxta signal darajasi deyarli nol bo‘lgan.

Natijalar muhokamasi

Olingan natijalar DPI yondoshuvi va unga ML usullarini qo‘shishning samaradorligini ko‘rsatadi. Tadqiqotimiz shuni isbotladi: DPI asosidagi xavfsizlik tizimiga mashina o‘rganish elementlarini qo‘shish orqali tahdidlarni aniqlash aniq darajada yaxshilanadi (aniqlik +10%, soxta signal kamayishi). Bu tahlillar aslida Kumar va boshq. (2025) tomonidan ilgari surilgan fikrni qo‘llab-quvvatlaydi – ular ham DPIni kengaytirish uchun ML integratsiyasining zarurligini ta’kidlaydilar.

Shuningdek, tadqiqot muhokamasi natijalarini ilgari chop etilgan ishlarga solishtirganda, biz ham Foreman et al. (2024) kabi yuqori aniqlikka erishdik, bu esa sun’iy intellekt yordamida murakkab xakerlik naqshlarini aniqlash imkoniyatlarini tasdiqlaydi. Biroq ML elementining joriy etilishi tarmoqning qayta ishlash tezligini ozroq susaytirganini qayd

etish lozim; demak, real muhitda tizim konfiguratsiyasini optimallashtirish va quvvat resurslarini yaxshilash talab etiladi.

Tajriba natijalari DPI metodining dolzarbligini yana bir bor isbotladi. Ba’zi tahlilchilarning fikriga qaramay, DPI texnologiyasi hali ham tarmoq xavfsizligida muhim vosita bo‘lib qolmoqda. Biroq natijalar shuni ham ko‘rsatadiki, mavjud cheklovlar – xususan, shifrlangan trafikni tekshiruvchi mexanizmlarning yetishmasligi – muammosini hal etish lozim. Ilmiy jihatdan, bu tadqiqot adabiyotlardagi bo‘shliqlarni qismligicha qoplamoqda va yangi yondashuvlar bo‘yicha mulohaza yuritmoqda. Amaliy ahamiyat nuqtai nazaridan, olingan natijalar asosida DPI li himoya devorlari va monitoring tizimlarining konfiguratsiyasini optimallashtirish uchun tavsiyalar berish mumkin.

Bundan tashqari, ushbu tadqiqot chegaralari ham aniqlandi. Ma’lumotlar bazasi cheklangan miqdorda sinov trafikdan iborat bo‘lib, haqiqiy katta tarmoqlardagi variantlarni to‘liq qamrab olmadi. Shuningdek, modelimiz shifrlangan trafikni to‘liq ko‘zdan kechirmadi: kelgusida shifrlashni buzmay turib inspeksiya qilish usullari, masalan TLS/SSL proksi, qo‘shimcha o‘rganishni talab qiladi. Shu munosabat bilan, ushbu tadqiqot natijalari asosida yangi izlanishlarda XAI usullarini qo‘llash, Deep Session Inspection (DSI) texnologiyasini tahlil qilish va yuqori o‘lchamli haqiqiy trafik to‘plamlari bilan sinov o‘tkazish tavsiya etiladi.

Xulosa

Xulosa qilib aytganda, chuqur paketli inspeksiya (DPI) tarmoq xavfsizligi sohasidagi fundamental texnologiya bo‘lib qolmoqda. Bizning tadqiqot natijalari shuni ko‘rsatdiki, an’anaviy DPI tizimlariga sun’iy intellekt asosida qo‘shimcha mexanizmlar kiritish orqali tahdidlarni aniqlash aniqligi sezilarli darajada oshiriladi. Olingan natijalar Foreman va boshq. ishida kuzatilganidek, ML yordamida tarmoq skanerlash kabi xulq-atvorlarni 90–100% atrofida aniqlash mumkinligini tasdiqlaydi.

Tadqiqotimiz ilmiy xulosalari hozirgi kiberxavfsizlik modelini yanada takomillashtirishga yordam beradi. Amaliy nuqtai nazardan, xavfsizlik tizimlariga DPI+ML yondashuvini joriy etish orqali kelajakda tashqi tahdidlarga qarshi samaraliroq himoya o‘rnatish mumkin bo‘ladi. Kelgusida esa shifrlangan trafikni tahlil qilish, tushunarli mashina o‘rganish (XAI) yondashuvlari va yangi tarmoq arxitekturalarini ishlab chiqish muhim vazifa hisoblanadi. Bu yo‘nalishlar bo‘yicha davom ettiriladigan tadqiqotlar tarmoq xavfsizligini yanada mustahkamlashga xizmat qilishi aniq.

Adabiyotlar/Литература/References:

1. Kumar, T., Leavy, S., Eustace, P., Curry, E. va Asghar, M. N. (2025). “A Review of Deep Packet Inspection for Network Security: From Traditional Techniques to Machine Learning Integration”. ARES 2025 konferentsiyasi (Lecture Notes in Computer Science, Vol.15997), 185–202 betlar.
2. Awasthi, K. (2025). “Is Deep Packet Inspection Obsolete? Exploring Modern Security Alternatives”. Fidelis Security blogi, 27 yanvar.
3. Raza, M. (2025). “Deep Packet Inspection (DPI) Explained: OSI Layers, Real-World Applications & Ethical Considerations”. Splunk blogi, 18 iyun.
4. CyberRatings.org (2024). “The Role of Encryption and Deep Inspection in Internet Security”. CyberRatings blogi, 23 may.
5. “Deep Packet Inspection (DPI): Enhancing Network Security with NetWitness”. NetWitness blogi, 20 noyabr 2023.

6. Foreman, J., Waters, W. L., Kamhoua, C. A., Hemida, A. H. A., Acosta, J. C. va Dike, B. C. (2024). “Detection of Hacker Intention Using Deep Packet Inspection”. Journal of Cybersecurity and Privacy, 4(4), 794–804.
7. Hussain, S., Shehzadi, T. va Khan, M. (2024). “Deep Packet Inspection: Leveraging Machine Learning for Efficient Network Security Analysis”. Preprint, mart 2024.
8. “Deep Packet Inspection vs. Stateful Packet Inspection”. NetAlly Texnologiyalar blogi, 17 iyun 2025.

YANGI DAVR ILM-FANI: INSON UCHUN INNOVATSION G‘OYA VA YECHIMLAR

XII RESPUBLIKA ILMIY-AMALIY KONFERENSIYASI MATERIALLARI

2026-yil, 26-iyun

Mas’ul muharrir: *F.T.Isanova*
Texnik muharrir: *N.Bahodirova*
Diszayner: *I.Abdihakimov*

Yangi davr ilm-fani: inson uchun innovatsion g‘oya va yechimlar.
XII Respublika ilmiy-amaliy konferensiyasi materiallari to‘plami.
2-jild, 12-son (iyun, 2026-yil). – 223 bet.

Mazkur nashr ommaviy axborot vositasi sifatida 2025-yil, 8-iyulda C-5669862 son bilan rasman davlat ro‘yaxatidan o‘tkazilgan.

ISSN: 3093-8791 (onlayn)

Elektron nashr: https://konferensiyalar.com

Konferensiya tashkilotchisi: “Scienceproblems Team” MChJ

Konferensiya o‘tkazilgan sana: 2026-yil, 24-iyun.