JOURNAL OF TRANSPORT

ISSUE 3, 2025 vol. 2
E-ISSN: 2181-2438
ISSN: 3060-5164

SLIB.UZ
Scientific library of Uzbekistan

RESEARCH, INNOVATION, RESULTS

TOSHKENT DAVLAT TRANSPORT UNIVERSITETI
Tashkent state transport university

JOURNAL OF TRANSPORT

RESEARCH, INNOVATION, RESULTS

E-ISSN: 2181-2438
ISSN: 3060-5164
VOLUME 2, ISSUE 3
SEPTEMBER, 2025

jot.tstu.uz

TASHKENT STATE TRANSPORT UNIVERSITY

JOURNAL OF TRANSPORT

SCIENTIFIC-TECHNICAL AND SCIENTIFIC INNOVATION JOURNAL

VOLUME 2, ISSUE 3 SEPTEMBER, 2025

The **"Journal of Transport"** established by Tashkent State Transport University (TSTU), is a prestigious scientific-technical and innovation-focused publication aimed at disseminating cutting-edge research and applied studies in the field of transport and related disciplines. Located at Temiryo'lchilar Street, 1, office 465, Tashkent, Uzbekistan (100167), the journal operates as a dynamic platform for both national and international academic and professional communities. Submissions and inquiries can be directed to the editorial office via email at jot@tstu.uz.

The Journal of Transport showcases groundbreaking scientific and applied research conducted by transport-oriented universities, higher educational institutions, research centers, and institutes both within the Republic of Uzbekistan and globally. Recognized for its academic rigor, the journal is included in the prestigious list of scientific publications endorsed by the decree of the Presidium of the Higher Attestation Commission No. 353/3 dated April 6, 2024. This inclusion signifies its role as a vital repository for publishing primary scientific findings from doctoral dissertations, including Doctor of Philosophy (PhD) and Doctor of Science (DSc) candidates in the technical and economic sciences.

Published quarterly, the journal provides a broad spectrum of high-quality research articles across diverse areas, including but not limited to:

- Economics of Transport
- Transport Process Organization and Logistics
- Rolling Stock and Train Traction
- Research, Design, and Construction of Railways, Highways, and Airfields, including Technology
- Technosphere Safety
- Power Supply, Electric Rolling Stock, Automation and Telemechanics, Radio Engineering and Communications
- Technological Machinery and Equipment
- Geodesy and Geoinformatics
- Automotive Service
- Air Traffic Control and Aircraft Maintenance
- Traffic Organizatsion
- Railway and Road Operations

The journal benefits from its official recognition under Certificate No. 1150 issued by the Information and Mass Communications Agency, functioning under the Administration of the President of the Republic of Uzbekistan. With its E-ISSN 2181-2438, ISSN 3060-5164 the publication upholds international standards of quality and accessibility.

Articles are published in Uzbek, Russian, and English, ensuring a wide-reaching audience and fostering cross-cultural academic exchange. As a beacon of academic excellence, the "Journal of Transport" continues to serve as a vital conduit for knowledge dissemination, collaboration, and innovation in the transport sector and related fields.

Modern approaches to enhancing communication security in telecommunication infrastructure

A.Sh. Khurramov[1][a], N.N. Irgashev[1][b]

[1]Tashkent state transport university, Tashkent, Uzbekistan

Abstract: This article analyzes modern approaches to ensuring communication security in telecommunication infrastructure. In recent years, the widespread adoption of information and communication technologies, particularly IP telephony, mobile communications, and fiber-optic networks, has brought the issue of enhancing cybersecurity to the forefront. The study examines cyber threats specific to telecommunication networks, including DoS/DDoS attacks, data interception (sniffing, eavesdropping), call redirection (hijacking), and fraudulent schemes (vishing). The effectiveness of various protection measures was evaluated, such as cryptographic methods (TLS, SRTP, VPN), network security tools (firewall, IDS/IPS, VLAN), and organizational measures (user authentication, password policies, staff training). The findings indicate that implementing a comprehensive approach to protective measures significantly increases the stability and reliability of telecommunication systems. The proposed solutions hold practical significance for the development of the national telecommunication infrastructure within the framework of the "Digital Uzbekistan – 2030" strategy.

Keywords: telecommunication infrastructure, IP telephony, cybersecurity, TLS, SRTP, VPN, IDS/IPS, communication security

Telekommunikatsiya infratuzilmasida aloqa xavfsizligini oshirishning zamonaviy yondashuvlari

Xurramov A.Sh.[1][a], Irgashev N.N.[1][b]

[1]Toshkent davlat transport universiteti, Toshkent, O‘zbekiston

Annotatsiya: Ushbu maqolada telekommunikatsiya infratuzilmasida aloqa xavfsizligini ta’minlashning zamonaviy yondashuvlari tahlil qilinadi. So‘nggi yillarda axborot-kommunikatsiya texnologiyalarining keng qo‘llanilishi, xususan, IP-telefoniya, mobil aloqa va optik tolali tarmoqlarning joriy etilishi bilan bir qatorda ularning kiberxavfsizlik darajasini oshirish dolzarb masalaga aylandi. Tadqiqotda telekommunikatsiya tarmoqlariga xos kiber tahdidlar - DoS/DDoS hujumlari, ma’lumotlarni tinglash (sniffing, eavesdropping), qo‘ng‘iroqlarni yo‘naltirish (hijacking) hamda firibgarlik usullari (vishing) batafsil o‘rganildi. Aloqa xavfsizligini oshirishda qo‘llaniladigan kriptografik usullar (TLS, SRTP, VPN), tarmoq himoyasi vositalari (firewall, IDS/IPS, VLAN) hamda tashkiliy choralar (foydalanuvchi autentifikatsiyasi, parol siyosati, xodimlarni o‘qitish) samaradorligi baholandi. Natijalar shuni ko‘rsatadiki, kompleks yondashuv asosida himoya choralarini joriy etish telekommunikatsiya tizimlarining barqarorligi va ishonchliligini sezilarli darajada oshiradi. Taklif etilgan yechimlar “Raqamli O‘zbekiston - 2030” strategiyasi doirasida milliy telekommunikatsiya infratuzilmasini rivojlantirish uchun amaliy ahamiyat kasb etadi.

Kalit so‘zlar: telekommunikatsiya infratuzilmasi, IP-telefoniya, kiberxavfsizlik, TLS, SRTP, VPN, IDS/IPS, aloqa xavfsizligi

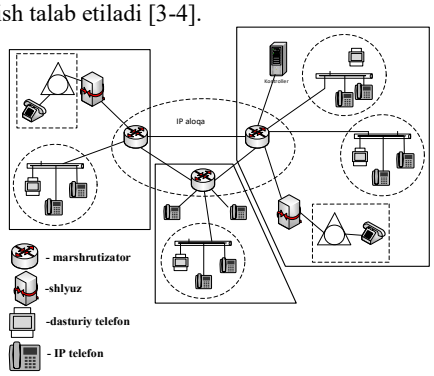
1. Kirish

Bugungi kunda telekommunikatsiya infratuzilmasi global iqtisodiyotning barcha sohalarida muhim ahamiyat kasb etib, jamiyatning axborot almashinuvi, xavfsizlik va boshqaruv jarayonlarining ajralmas qismi sifatida faoliyat yuritmoqda. Internet, mobil aloqa, optik tolali tarmoqlar va IP-telefoniya kabi texnologiyalarning jadal rivojlanishi axborot uzatish samaradorligini keskin oshirdi. Shu bilan birga, mazkur tizimlarning kiberxavfsizlik darajasini ta’minlash masalasi dolzarb muammo sifatida shakllandi [1-2]. IP-telefoniyani tashkil etishning tuzilmaviy sxemasi 1-rasmda keltirilgan.

Telekommunikatsiya tizimlarida yuzaga keladigan xavf-xatarlar turlicha bo‘lib, ularga xizmat ko‘rsatishni rad etish (DoS/DDoS) hujumlari, ma’lumotlarni noqonuniy tinglash (sniffing, eavesdropping), qo‘ng‘iroqlarni o‘g‘irlash (hijacking) hamda firibgarlik usullari (vishing) kiradi. Bunday tahdidlar nafaqat alohida foydalanuvchilar, balki butun milliy infratuzilma xavfsizligi uchun ham jiddiy xatar tug‘diradi. Shu sababli telekommunikatsiya sohasida aloqa

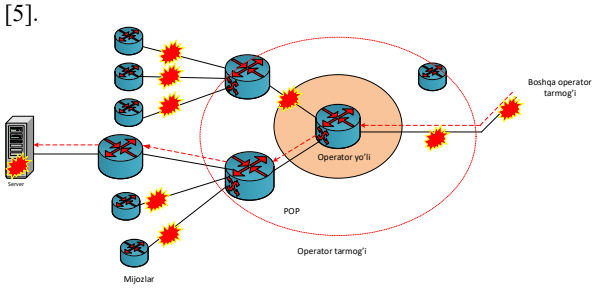
[a] https://orcid.org/0000-0002-8443-9250
[b] https://orcid.org/0009-0000-3736-1748

tizimlarini himoyalash bo‘yicha zamonaviy yondashuvlarni joriy etish talab etiladi [3-4].



1-rasm. IP-telefoniyani tashkil etish tamoyillari

Oxirgi yillarda axborot xavfsizligini ta’minlashda kriptografik protokollar (TLS, SRTP, VPN), tarmoq himoyasi vositalari (firewall, IDS/IPS, VLAN) va tashkiliy choralar (parol siyosati, foydalanuvchini autentifikatsiya qilish, xodimlarni maxsus tayyorlash) keng qo‘llanila boshlandi. Shu bilan birga, sun’iy intellekt asosida ishlovchi tarmoq monitoring tizimlari, 5G va 6G tarmoqlarida xavfsizlikni mustahkamlash, shuningdek, kvant kriptografiya kabi istiqbolli yondashuvlar ham tadqiqotlarning asosiy yo‘nalishlaridan biriga aylanmoqda [5].



2-rasm. IP-telefoniya tarmog‘iga kiber ta’sirlar

Mazkur tadqiqotning asosiy maqsadi telekommunikatsiya infratuzilmasida aloqa xavfsizligini oshirishga xizmat qiluvchi zamonaviy yondashuvlarni tahlil qilish va ularning amaliy samaradorligini baholashdan iborat. Olingan natijalar milliy raqamli infratuzilmani mustahkamlash va “Raqamli O‘zbekiston – 2030” strategiyasida belgilangan ustuvor yo‘nalishlarga muvofiq telekommunikatsiya tizimlarini yanada rivojlantirishga xizmat qiladi.

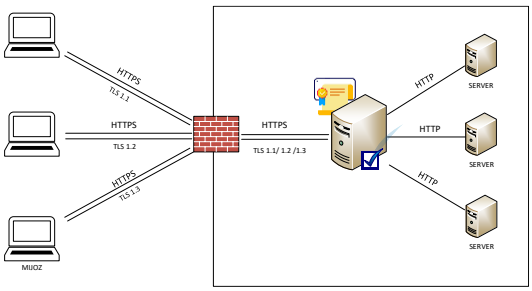
2. Tadqiqot metodologiyasi

Telekommunikatsiya infratuzilmasida aloqa xavfsizligini oshirish bo‘yicha tadqiqotda kompleks yondashuv qo‘llanildi. Avvalo, mavjud tarmoqlar arxitekturasi, jumladan, IP-telefoniya, mobil aloqa, optik tolali tarmoqlar hamda korporativ LAN/WAN tizimlari nazariy jihatdan tahlil qilindi. Shu asosda paket kommutatsiyasi, trafik oqimlari va xizmatlar integratsiyasi sxematik modellashtirildi [6-7].

Keyingi bosqichda telekommunikatsiya tizimlariga xos bo‘lgan kiberxavf-xatarlar, jumladan, xizmat ko‘rsatishni rad etish (DoS/DDoS) hujumlari, ma’lumotlarni noqonuniy tinglash (sniffing, eavesdropping), qo‘ng‘iroqlarni o‘g‘irlash (hijacking) va firibgarlikning ovozli usullari (vishing) o‘rganilib, ularning aloqa sifati va barqarorligiga ta’siri modellashtirildi.

Tadqiqot davomida aloqa xavfsizligini oshirishda qo‘llaniladigan texnologik yondashuvlar ham atroflicha o‘rganildi. Xususan, kriptografik protokollar - TLS, SRTP, IPsec va VPN orqali ma’lumotlarning maxfiyligi, yaxlitligi va autentifikatsiyasi ta’minlandi [8]. Shu bilan birga, tarmoq himoyasi vositalari - apparat va dasturiy firewalls, IDS/IPS tizimlari (Snort, Suricata), VLAN texnologiyasi hamda Session Border Controller (SBC) kabi yechimlar tahlil qilinib, ularning samaradorligi paketlarni filtrlash, zararli trafikni aniqlash va bloklash tezligi, noto‘g‘ri ogohlantirishlar chastotasi kabi ko‘rsatkichlar asosida baholandi.

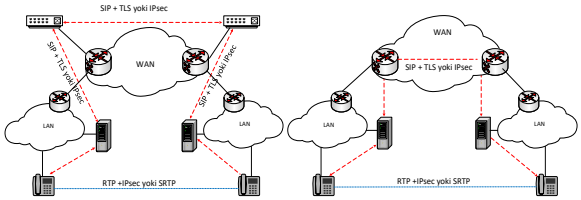
Metodologiyada texnologik yondashuvlardan tashqari tashkiliy choralar ham alohida ahamiyat kasb etdi. Kuchli parol siyosati, ikki bosqichli autentifikatsiya (2FA), muntazam audit va tizim yangilanishlari, xodimlarni kiberxavfsizlik bo‘yicha tayyorlash, real vaqt rejimidagi monitoring va log tahlili aloqa tizimlarida xavfsizlikni mustahkamlashning samarali yo‘llari sifatida qo‘llanildi.



3-rasm. Tizim himoyalash arxitekturasi diagrammasi

Baholash jarayonida qiyosiy tahlil, simulyatsiya va statistik usullardan foydalanildi: TLS, SRTP va VPN protokollarining samaradorligi solishtirildi, DDoS hujumlarining tarmoqqa ta’siri modellashtirildi, paket yo‘qotish darajasi, kechikish va throughput kabi ko‘rsatkichlar hisoblab chiqildi. Bundan tashqari, ekspert bahosi asosida tashkiliy choralar amaliy jihatdan tekshirildi [9-10].

RTP (Real-Time Transport Protocol) - bu IP tarmoq orqali, ayniqsa UDP transport qatlami asosida, real vaqt rejimidagi ma’lumotlarni, masalan, audio va video kabi oqimlarni uzatish uchun ishlab chiqilgan protokol (standart RFC 3550). Ushbu protokolning xavfsizligi ta’minlangan versiyasi SRTP (Secure RTP) deb ataladi va u RFC 3711 hujjatida tasvirlangan.



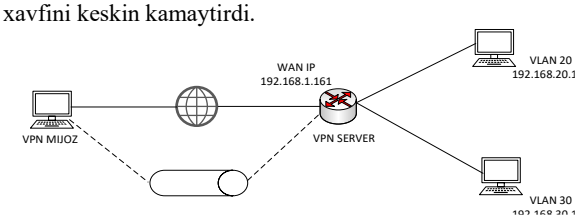
4-rasm. IP-telefoniya tarmog‘ida signal va media oqimlarini himoyalash sxemasi

Shu tariqa, metodlar qismida nazariy modellashtirish, kriptografik va tarmoq himoyasi protokollarini o‘rganish, simulyatsiya asosida tahdidlarni baholash hamda tashkiliy yechimlarni tatbiq etish orqali telekommunikatsiya infratuzilmasida aloqa xavfsizligini ta’minlash uchun kompleks metodologiya ishlab chiqildi.

3. Natijalar

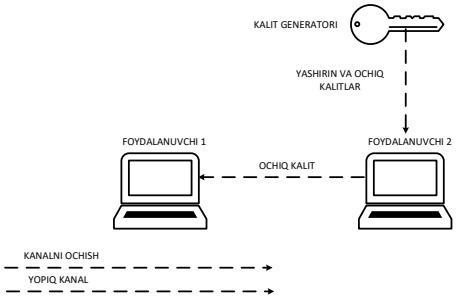
O‘tkazilgan tadqiqotlar natijasida telekommunikatsiya infratuzilmasida aloqa xavfsizligini oshirish uchun qo‘llaniladigan texnologik va tashkiliy yondashuvlarning samaradorligi baholandi. Kriptografik protokollar bo‘yicha olib borilgan tahlillar shuni ko‘rsatdiki, TLS transport darajasida sessiya xavfsizligini ta’minlashda yuqori darajada samarali bo‘lib, autentifikatsiya jarayonida ma’lumotlarning yaxlitligini kafolatladi. SRTP protokoli ovoz va video oqimlarida shifrlashni ta’minlab, “eavesdropping” tahdidlariga qarshi samarali himoya berdi. VPN va IPsec texnologiyalari esa segmentlararo aloqada yuqori darajada maxfiylikni ta’minladi, biroq ularning qo‘llanilishi hisoblash resurslari sarfini oshirishi aniqlangan [11].

Tarmoq darajasidagi himoya vositalari samaradorligi bo‘yicha o‘tkazilgan tajribalar shuni ko‘rsatdiki, apparat va dasturiy firewalllar orqali trafikni filtrlash DDoS hujumlariga qarshi birlamchi himoya sifatida muhim rol o‘ynaydi. IDS/IPS tizimlari (Snort, Suricata) real vaqt rejimida hujumlarni aniqlash va bloklashda yuqori aniqlikka ega bo‘ldi, lekin noto‘g‘ri signal (false positive) chastotasi 5–7% atrofida qayd etildi. VLAN asosida segmentatsiya esa tarmoq yuklamasini kamaytirib, paketlarni mantiqiy bo‘linmalarga ajratish orqali xavfsizlikni oshirdi. Session Border Controller (SBC) VoIP seanslarini himoyalashda samarali bo‘lib, qo‘ng‘iroqlarni o‘g‘irlash (hijacking) xavfini keskin kamaytirdi.



5-rasm. VPN Server va VLANlar bilan tarmoqning ulanish konfiguratsiyasi

Tashkiliy choralar bo‘yicha olib borilgan baholash natijalarida muntazam audit va tizim yangilanishlari, foydalanuvchilarni ikki bosqichli autentifikatsiya orqali tizimga kiritish hamda xodimlarni muntazam ravishda kiberxavfsizlik bo‘yicha o‘qitish xavfsizlik darajasini oshirishda muhim omil ekanligi tasdiqlandi. Ayniqsa, log fayllarni real vaqt rejimida monitoring qilish orqali hujumlarni dastlabki bosqichida aniqlash mumkinligi kuzatildi.

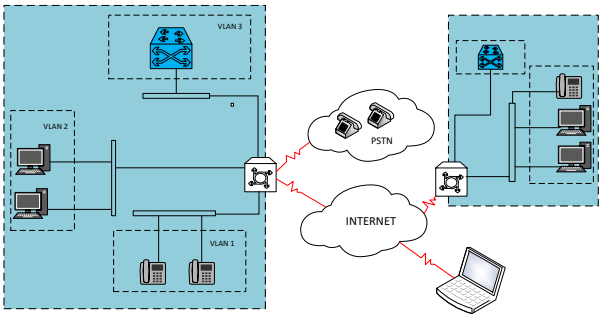


6-rasm. Assimetrik shifrlash uchun kalitlarni taqsimlash sxemasi

Simulyatsiya asosida o‘tkazilgan tajribalar shuni ko‘rsatdiki, DDoS hujumlari paytida himoyasiz tarmoqda paket yo‘qotish darajasi 35–40% gacha oshsa, firewall va IDS/IPS tizimlari qo‘llangan holda bu ko‘rsatkich 10–12% gacha kamaydi. Kriptografik protokollar qo‘llanilgan tarmoqlarda ma’lumotlarning maxfiyligi va yaxlitligi to‘liq saqlandi, biroq qo‘shimcha kechikish 20–40 millisekundni tashkil etdi. Bu ko‘rsatkich telekommunikatsiya xizmatlari sifati uchun qabul qilinadigan darajada ekanligi qayd etildi.

Umuman olganda, natijalar shuni tasdiqladiki, telekommunikatsiya infratuzilmasida xavfsizlikni ta’minlashda yagona bir texnologiya yetarli emas, balki kriptografik protokollar, tarmoq himoyasi vositalari va tashkiliy choralarni kompleks qo‘llash eng yuqori samaradorlikni beradi. Mazkur yondashuv aloqa tizimlarining barqarorligini, uzluksizligini va ishonchliligini sezilarli darajada oshiradi.

Natijalarni boshqa ilmiy ishlanmalar bilan solishtirganda ham o‘xshash xulosalarga kelindi. Masalan, xalqaro tadqiqotlarda SRTP protokoli ovozli trafikni himoyalashda samarali ekanligi qayd etilgan bo‘lsa, bizning simulyatsiya tajribalarimiz ham aynan shu natijani tasdiqladi. Bundan tashqari, DDoS hujumlariga qarshi faqat apparat darajasida emas, balki tarmoq segmentatsiyasi va trafikni boshqarish mexanizmlarini qo‘llash yanada yuqori darajadagi barqarorlikni ta’minlashi aniqlangan.



7-rasm. Taklif etilayotgan himoya tizimini tashkil qilish tuzilmaviy sxemasi

Kelajak istiqbollari nuqtai nazaridan, telekommunikatsiya infratuzilmasida xavfsizlikni oshirishda yangi avlod texnologiyalari muhim o‘rin tutadi. 5G va 6G tarmoqlarining keng joriy etilishi, ularda ko‘p sonli qurilmalar va xizmatlarning ulanishi xavfsizlik masalalarini yanada dolzarb qiladi.

Umuman olganda, tadqiqot natijalari shuni ko‘rsatadiki, telekommunikatsiya infratuzilmasida aloqa xavfsizligini ta’minlashning eng samarali yo‘li - bu texnologik vositalar va tashkiliy choralarni uyg‘unlashtirgan kompleks yondashuvni amaliyotga joriy etishdir.

4. Xulosa

Tadqiqot natijalari shuni ko‘rsatadiki, telekommunikatsiya infratuzilmasida aloqa xavfsizligini ta’minlash murakkab va ko‘p qirrali jarayon bo‘lib, u yagona texnologiya yoki yechimga tayanish orqali to‘liq amalga oshirilmaydi. Kriptografik protokollar -TLS, SRTP, VPN va IPsec - ma’lumotlarning maxfiyligi, yaxlitligi va autentifikatsiyasini ta’minlashda muhim vositalar hisoblanadi. Shu bilan birga, tarmoq darajasidagi himoya vositalari firewall, IDS/IPS tizimlari, VLAN asosida segmentatsiya va Session Border Controller kabi yechimlar hujumlarning oldini olishda va ularni tezkor aniqlashda samarali ekanligi isbotlandi.

https://doi.org/10.56143/2181-2438-2025-3-45-48 Research, Innovation, Results

Biroq, texnologik choralar bilan cheklanib qolish yetarli emasligi aniqlandi. Aloqa xavfsizligini oshirish uchun tashkiliy choralar - foydalanuvchilarni autentifikatsiya qilish, kuchli parol siyosatini joriy etish, muntazam audit va yangilanishlar, xodimlarni kiberxavfsizlik bo‘yicha tayyorlash texnologik vositalar bilan uyg‘unlashtirilgan holda qo‘llanganda eng yuqori samaraga erishiladi.

Simulyatsiya va tahlillar natijasida aniqlanishicha, kompleks yondashuv asosida himoya choralarini joriy etish telekommunikatsiya tizimlarida paket yo‘qotish darajasini kamaytiradi, DDoS hujumlarining ta’sirini sezilarli darajada pasaytiradi hamda ma’lumotlarning maxfiyligi va yaxlitligini kafolatlaydi. Natijalar shuni ko‘rsatadiki, telekommunikatsiya infratuzilmasida aloqa xavfsizligini oshirishning zamonaviy yondashuvlari tizimning barqarorligi, uzluksizligi va ishonchliligini oshirish bilan birga, foydalanuvchi tajribasini yaxshilashga ham xizmat qiladi.

Tadqiqotdan kelib chiqadigan asosiy xulosa shundaki, kelajakda telekommunikatsiya tizimlarini rivojlantirishda sun’iy intellekt asosida ishlovchi monitoring tizimlari, 5G/6G tarmoqlarida xavfsizlikni mustahkamlash hamda kvant kriptografiya kabi istiqbolli texnologiyalarni joriy etish dolzarb ahamiyat kasb etadi. Ushbu yondashuvlar “Raqamli O‘zbekiston – 2030” strategiyasi doirasida milliy raqamli infratuzilmani yanada kuchaytirish uchun muhim poydevor bo‘lib xizmat qiladi.

Foydalangan adabiyotlar / References

[1] Бахраев Р.Ш. IP-телефония: технологии и защита. – Москва: Солон-Пресс, 2020. – 224 с.

[2] Карпов А.В. IP телефония и мультимедийные технологии связи. – Санкт-Петербург: Питер, 2021. – 288 с.

[3] Соловьев А.В. Технологии VoIP и построение IP-сетей. – Казань: Техносфера, 2020. – 240 с.

[4] Касымхан Н.Е. Анализ обеспечения безопасности в IP-телефонии: Дипломная работа. – Алматы: КазНИТУ, 2022. – 56 с.

[5] Молчанов И.В. Киберугрозы в IP-сетях и методы защиты. – Москва: ДМК Пресс, 2021. – 304 с.

[6] Шахов И.В. Информационная безопасность с pfSense и Snort. – Москва: БХВ-Петербург, 2020. – 352 с.

[7] Чиркин С.Л. VLAN технологии и изоляция трафика. – Минск: РадиоСофт, 2021. – 256 с.

[8] Павлов С.Н. Системный подход к защите IP-телефонии. – Москва: Инфра-М, 2020. – 196 с.

[9] Cisco Systems. VoIP Essentials and Fundamentals Guide. – Cisco Press, 2022. – 196 p.

[10] Dierks T., Rescorla E. The Transport Layer Security (TLS) Protocol Version 1.2: RFC 5246. – IETF, 2021. – 74 p.

[11] Хуррамов А. Ш., Уроков О. Х., Иргашев Н. Н. Анализ и оценка факторов, влияющих на сеть оперативной технологической радиосвязи на основе IP-радиотерминалов // Транспорт: наука, техника, управление. – 2024. – № 5. – DOI: 10.36535/0236-1914-2024-05-4.

Mualliflar to‘g‘risida ma’lumot/ Information about the authors

Xurramov Asliddin / Khurramov Asliddin	Toshkent davlat transport universiteti “Radioelektron qurilmalar va tizimlar” kafedrasi dotsent v.b., t.f.f.d., (PhD) E-mail: asliddinxurramov703@gmail.com https://orcid.org/0000-0002-8443-9250
Irgashev Nuriddin / Nuriddin Irgashev	Toshkent davlat transport universiteti “Radioelektron qurilmalar va tizimlar” kafedrasi assistenti E-mail: irgashev_nn@bk.ru https://orcid.org/0009-0000-3736-1748

CONTEXT / MUNDARIJA