ISSN: 2181-3906 2025

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

# TELEKOMMUNIKATSIYA TARMOQLARINI MONITORING VA NAZORAT QILISH DASTURIY VOSITALARI

**Narzullayev Sherbek Nematullayevich**
University of Management and Future Technologies
Telekommunikatsiya injiniringi magistranti.
***https://doi.org/10.5281/zenodo.15372323***

***Annotatsiya.*** *Ushbu maqolada telekommunikatsiya tarmoqlarining barqaror va xavfsiz ishlashini ta'minlashda monitoring va nazorat tizimlarining tutgan o'rni chuqur tahlil qilinadi.*

*Telekommunikatsiya tarmog'i komponentlarining holatini real vaqt rejimida kuzatish, nosozliklarni tezda aniqlash va bartaraf etish, trafikni boshqarish hamda xavfsizlik tahdidlarini oldindan aniqlash uchun qo'llaniladigan zamonaviy dasturiy vositalar turlari o'rganiladi.*

*Maqolada ochiq kodli (open source) va tijorat (commercial) monitoring vositalari solishtirilib, ularning funksional imkoniyatlari, afzalliklari va cheklovlari batafsil ko'rib chiqiladi. Bundan tashqari, Software-Defined Networking (SDN) texnologiyasining monitoring jarayonlariga ta'siri, sun'iy intellekt asosidagi tahlil va avtomatik javob berish mexanizmlari, hamda real amaliyotdagi ilg'or tajribalar haqida ham fikr yuritiladi. Maqola yakunida monitoring tizimini tanlash mezonlari va uni samarali joriy etish bo'yicha amaliy tavsiyalar beriladi.*

***Kalit so'zlar:*** *Telekommunikatsiya tarmoqlari, tarmoq monitoringi, nazorat tizimlari, dasturiy vositalar, Zabbix, Nagios, Prometheus, PRTG, SolarWinds, tarmoq xavfsizligi, SNMP, NetFlow, real vaqt monitoring, ochiq kodli tizimlar, tijorat dasturlari, SDN (Software-Defined Networking), tarmoq boshqaruvi, sun'iy intellekt, trafik tahlili, IoT monitoringi, avtomatlashtirilgan nazorat, bulutli monitoring, tarmoq infrastrukturasi, tizim integratsiyasi.*

# SOFTWARE TOOLS FOR MONITORING AND CONTROL OF TELECOMMUNICATION NETWORKS

***Abstract.*** *This article provides an in-depth analysis of the role of monitoring and control systems in ensuring the stable and secure operation of telecommunication networks. The types of modern software tools used to monitor the state of telecommunication network components in real-time, quickly identify and eliminate faults, manage traffic, and identify security threats in advance are studied. The article compares open source and commercial monitoring tools and examines their functional capabilities, advantages, and limitations in detail. In addition, the impact of Software-Defined Networking (SDN) technology on monitoring processes, artificial intelligence-based analysis and automatic response mechanisms, and best practices in real practice are discussed. At the end of the article, the criteria for selecting a monitoring system and practical recommendations for its effective implementation are given.*

***Keywords:*** *Telecommunications networks, network monitoring, control systems, software tools, Zabbix, Nagios, Prometheus, PRTG, SolarWinds, network security, SNMP, NetFlow, real-time monitoring, open source systems, commercial software, SDN (Software-Defined Networking), network management, artificial intelligence, traffic analysis, IoT monitoring, automated control, cloud monitoring, network infrastructure, system integration.*

ISSN: 2181-3906 2025

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

# ПРОГРАММНЫЕ СРЕДСТВА ДЛЯ МОНИТОРИНГА И УПРАВЛЕНИЯ ТЕЛЕКОММУНИКАЦИОННЫМИ СЕТЯМИ

***Аннотация.*** *В статье дается углубленный анализ роли систем мониторинга и управления в обеспечении стабильной и безопасной работы телекоммуникационных сетей. Будут изучены типы современных программных средств, используемых для мониторинга состояния компонентов телекоммуникационных сетей в режиме реального времени, быстрого выявления и устранения неисправностей, управления трафиком и упреждающего выявления угроз безопасности. В статье сравниваются открытые и коммерческие средства мониторинга, а также подробно рассматриваются их функциональные возможности, преимущества и ограничения. Кроме того, обсуждается влияние технологии программно-определяемых сетей (SDN) на процессы мониторинга, анализ на основе искусственного интеллекта и механизмы автоматического реагирования, а также передовой опыт в реальной практике. В заключение статьи приводятся критерии выбора системы мониторинга и практические рекомендации по ее эффективному внедрению.*

***Ключевые слова:*** *Телекоммуникационные сети, сетевой мониторинг, системы управления, программные инструменты, Zabbix, Nagios, Prometheus, PRTG, SolarWinds, сетевая безопасность, SNMP, NetFlow, мониторинг в реальном времени, системы с открытым исходным кодом, коммерческое программное обеспечение, SDN (программно-определяемые сети), управление сетями, искусственный интеллект, анализ трафика, мониторинг IoT, автоматизированное управление, облачный мониторинг, сетевая инфраструктура, системная интеграция.*

## KIRISH

Telekommunikatsiya tarmoqlari bugungi raqamli jamiyatning asosi hisoblanadi. Internet, mobil aloqa, korporativ LAN va WAN tarmoqlari, davlat boshqaruvi tizimlari, moliyaviy institutlar, sanoat avtomatizatsiyasi – bularning barchasi zamonaviy va barqaror telekommunikatsiya infratuzilmasiga tayanadi. Bu tarmoqlarning uzluksiz ishlashi texnik va axborot xavfsizligi nuqtayi nazaridan nihoyatda muhim bo‘lib, ularda yuzaga keladigan har qanday nosozliklar katta moliyaviy va axboriy yo‘qotishlarga olib kelishi mumkin.

Shu bois, tarmoqlar faoliyatini real vaqt rejimida nazorat qilish, ishlash samaradorligini tahlil etish, nosozliklarga tezkor javob berish va tahdidlarning oldini olish uchun monitoring va nazorat qilish tizimlari zarurdir. Monitoring vositalari nafaqat mavjud muammolarni aniqlash, balki kelajakdagi ehtimoliy nosozliklarni prognoz qilishga ham xizmat qiladi. Ayniqsa, yirik va murakkab infratuzilmaga ega bo‘lgan tarmoqlarda bu vositalarsiz samarali boshqaruvni tasavvur etib bo‘lmaydi.

Ushbu maqolada tarmoq monitoringi va nazorati jarayonlarining mazmuni, ularni amalga oshiruvchi zamonaviy dasturiy vositalar, ularning turlari, texnik imkoniyatlari va qo‘llanilish doirasi chuqur tahlil qilinadi. Shuningdek, Software-Defined Networking (SDN), sun’iy intellekt texnologiyalari va IoT qurilmalarining monitoring tizimlariga integratsiyasi haqida ham batafsil fikr yuritiladi.

***Tarmoq monitoringi va nazorati nima?***

Tarmoq monitoringi – bu tarmoq infratuzilmasining holatini real vaqt rejimida doimiy kuzatish, trafik oqimlarini tahlil qilish, aloqa sifati va yuklamani baholash jarayonidir. U orqali foydalanuvchilarning ulanish sifati, qurilmalarning ishlash holati, tarmoq xizmatlarining uzluksizligi kabi muhim ko‘rsatkichlar nazorat qilinadi. Monitoring tizimlari tarmoqda sodir bo‘layotgan barcha texnologik jarayonlar haqida to‘liq axborot taqdim etadi.

Tarmoq nazorati esa – monitoring natijalari asosida tarmoqning ishlashiga faol ta’sir o‘tkazish, ya’ni nosozliklarni bartaraf etish, tarmoq siyosatlarini (QoS, ACL, firewall qoidalari) o‘zgartirish, qurilmalarni qayta sozlash yoki yangilash kabi chora-tadbirlarni o‘z ichiga oladi.

Monitoring va nazorat bir-biri bilan chambarchas bog‘liq bo‘lib, ular orqali tarmoqni:

- Optimallashtirish;
- Nosozliklarga tezkor javob berish;
- Tarmoq resurslarini samarali taqsimlash;
- Xavfsizlikni ta’minlash imkonini beradi.

Monitoringning asosiy komponentlari quyidagilardan iborat:

- Topologiyani kuzatish (qurilmalar joylashuvi va ularning bog‘lanishi);
- Trafik tahlili (tarmoqdan qanday axborot oqimi o‘tmoqda);
- Xizmatlarning holatini kuzatish (web-server, email-server va h.k.);
- Nosozlik aniqlash va ogohlantirish tizimi (trublshooting);
- Statistik ma’lumotlarni yig‘ish va vizualizatsiya qilish (grafik interfeys, jadvallar, tarixiy ma’lumotlar bazasi).

Bularning barchasi tarmoq administratoriga doimiy nazoratni amalga oshirish va tezkor qarorlar qabul qilish imkonini beradi.

***Dasturiy vositalarning tasnifi***

Tarmoq monitoringi va nazorati uchun ishlab chiqilgan dasturiy vositalar juda xilma-xil bo‘lib, ularni bir nechta asosiy guruhlarga bo‘lish mumkin. Tasniflashda dasturiy vositaning litsenziya turi, funksional imkoniyatlari, qo‘llash sohasi va texnik moslashuvchanligi inobatga olinadi.

*Ochiq kodli (Open Source) dasturiy vositalar*

Bu turdagi vositalar bepul bo‘lib, ularni erkin sozlash va kengaytirish imkoniyati mavjud. Asosan kichik va o‘rta miqyosdagi tarmoqlar uchun mos.

*Zabbix*

- Monitoring va ogohlantirish tizimi sifatida kuchli imkoniyatlarga ega.
- Agent va agentless monitoring, SNMP, IPMI, JMX protokollarini qo‘llab-quvvatlaydi.
- Ma’lumotlar bazasiga asoslangan tizim: grafik, jadvallar, tarixiy tahlil.
- Avtomatik aniqlash va o‘zgarishlarga moslashuv funksiyasi mavjud.

*Nagios*

- Klassik monitoring tizimi, plaginlar orqali kengaytiriladi.
- Har qanday xizmat yoki qurilmani kuzatish mumkin.
- Ko‘p sonli hamjamiyat va keng hujjatlashtirishga ega.

*Prometheus*

- “Time-series” ma’lumotlar yig‘ish texnologiyasi asosida ishlaydi.

- Grafana bilan integratsiya qilinadi, kuchli grafik interfeysga ega.
- Kubernetes va Docker kabi zamonaviy infratuzilmalarga moslashgan.

*Cacti*

- SNMP asosida grafik holatda tarmoq holatini ko‘rsatadi.
- RRDTool (Round Robin Database) asosida ishlaydi.
- Asosan trafik monitoringi uchun mos.

*Tijorat (Commercial) dasturiy vositalar*

Pullik va ko‘p hollarda professional xizmatlar bilan birga taqdim etiladi. Katta hajmli, xavfsizlikka yuqori talab qo‘yiladigan va tarmoq ishonchliligi muhim bo‘lgan tizimlar uchun mos.

*PRTG Network Monitor*

- 10 000+ sensor monitoring imkoniyati.
- SNMP, NetFlow, WMI va boshqa protokollarni qo‘llab-quvvatlaydi.
- Avtomatik topologiya yaratish va ogohlantirish tizimi mavjud.

*SolarWinds Network Performance Monitor*

- Tarmoqning ishlash holatini interaktiv xarita shaklida ko‘rsatadi.
- NetFlow, J-Flow, sFlow tahlillari orqali chuqur trafik kuzatuvi.
- Oson sozlanadigan ogohlantirish tizimi va muammolarni avtomatik tahlil qilish imkoniyati mavjud.

*ManageEngine OpManager*

- Tizim va tarmoq monitoringini birlashtiradi.
- Real vaqtli grafiklar, 3D topologik xaritalar.
- Virtual muhit (VMware, Hyper-V) monitoringini qo‘llab-quvvatlaydi.

*SDN va AI asosidagi monitoring vositalari*

Software-Defined Networking asosida monitoring tizimlari tarmoqni markazlashtirilgan holda boshqaradi, avtomatik sozlash va tahlil qilish imkonini beradi.

AI (sun’iy intellekt) yordamida anomal holatlarni oldindan aniqlash va prognozlash imkoniyati kengaymoqda. Masalan:

- Cisco DNA Center
- Juniper HealthBot
- IBM SevOne Network Performance Monitoring

*Zamonaviy yondashuvlar: SDN asosidagi monitoring*

An’anaviy tarmoq infratuzilmasida monitoring tizimlari har bir qurilma yoki segment darajasida alohida ishlaydi. Bunday holatda umumiy tarmoq holatini real vaqt rejimida kuzatish va boshqarish qiyin kechadi. Shuning uchun so‘nggi yillarda **Software-Defined Networking (SDN)** texnologiyasi asosida markazlashtirilgan monitoring va boshqaruv tizimlariga bo‘lgan talab ortib bormoqda.

*SDN monitoringining asosiy afzalliklari:*

- Markazlashtirilgan nazorat: barcha tarmoq qurilmalari yagona boshqaruv tizimiga ulanadi. Bu esa monitoring jarayonini soddalashtiradi va avtomatlashtiradi.
- Dinamik tarmoq sozlamalari: tarmoqdagi yuklama yoki xavf holatiga qarab konfiguratsiyalar avtomatik o‘zgaradi.

- Real vaqtli tahlil: SDN boshqaruv qurilmasi (controller) tarmoqdagi har bir hodisani tezda aniqlaydi va tegishli javobni beradi.
- Ortiqcha yuklamani balanslash: trafik oqimlarini aqlli tarzda boshqarish orqali tarmoq resurslaridan samarali foydalanish imkoniyati yaratiladi.

*SDN monitoringi uchun vositalar misollari:*

*OpenDaylight*

- Ochiq kodli SDN controller bo‘lib, tarmoq monitoringi va boshqaruvini markazlashtirish imkonini beradi.
- REST API orqali boshqa tizimlar bilan integratsiya qilinadi.

*ONOS (Open Network Operating System)*

- Masshtablanadigan va barqaror monitoring va boshqaruv imkoniyatlariga ega.
- Telecommunication-scale SDN monitoring tizimlarida keng qo‘llaniladi.

*Cisco Digital Network Architecture (DNA) Center*

- Sun’iy intellekt yordami bilan tarmoqdagi harakatlarni tahlil qiladi.
- Potensial nosozliklar, xavfsizlik tahdidlari va trafikdagi g‘ayritabiiy holatlarni oldindan aniqlaydi.

*Juniper HealthBot*

- Tarmoq sog‘ligini sun’iy intellekt yordamida doimiy kuzatadi.
- Ma’lumotlar analitikasi asosida ogohlantirish va tahlil xizmatlarini taqdim etadi.

*SDN monitoringi* ayniqsa katta hajmdagi ma’lumot oqimlarini boshqarishda, xizmat sifatini kafolatlashda (QoS) va avtomatlashtirilgan xavfsizlik choralarini ko‘rishda samarali yechim hisoblanadi.

*Monitoring tizimlarini tanlash mezonlari*

Monitoring tizimini tanlashda har bir tashkilot yoki operator o‘zining texnik, moliyaviy va xavfsizlik ehtiyojlaridan kelib chiqishi kerak. Quyida monitoring dasturiy vositasini tanlashda hisobga olinadigan asosiy mezonlar keltirilgan:

*Tarmoqning o‘lchami va murakkabligi*

- Kichik va o‘rta miqyosli tarmoqlar uchun Zabbix, PRTG yoki Cacti yetarli bo‘lishi mumkin.
- Katta korporativ yoki davlat miqyosidagi tarmoqlar uchun SolarWinds, ManageEngine yoki Cisco DNA kabi tizimlar afzalroq.

*Litsenziya va xarajatlar*

- Ochiq kodli tizimlar bepul, lekin texnik xizmat ko‘rsatish resurslari talab etiladi.
- Tijorat tizimlari yuqori sifatli texnik qo‘llab-quvvatlashni taqdim etsa-da, ularning xarajati ancha yuqori.

*Protokollarni qo‘llab-quvvatlash darajasi*

- SNMP, NetFlow, J-Flow, sFlow, ICMP, WMI va boshqa standart protokollar bilan ishlay olish qobiliyati muhimdir.

*Vizualizatsiya va foydalanuvchi interfeysi*

- Grafiklar, xaritalar, diagrammalar orqali aniq, tushunarli monitoring natijalarini taqdim etish foydalanuvchi samaradorligini oshiradi.

Xavfsizlik imkoniyatlari

• Monitoring tizimi o‘zi ham hujumlarga qarshi himoyalangan bo‘lishi kerak (autentifikatsiya, loglash, shifrlash).

*Integratsiya imkoniyatlari*

• Dastur boshqa tizimlar (SDN controller, SIEM, ticketing system, ITSM) bilan bog‘lana olishi zarur.

*Avtomatlashtirish darajasi*

• AI va ML asosida nosozliklarni aniqlash, ogohlantirish yuborish, avtomatik javob choralari ko‘rish imkoniyatlari bo‘lishi samaradorlikni oshiradi.

*Ilg‘or amaliyotlar va tendensiyalar*

Bugungi kunda telekommunikatsiya tarmoqlarini monitoring va nazorat qilish sohasida bir qancha ilg‘or amaliyotlar shakllangan bo‘lib, ular tarmoq ishonchliligi, xavfsizligi va optimal ishlashini ta’minlashga qaratilgan. Shu bilan birga, global texnologik tendensiyalar tarmoq monitoringi konsepsiyalarini tubdan o‘zgartirmoqda. Quyida eng dolzarb yo‘nalishlar va amaliyotlar yoritib beriladi.

*Sun’iy intellekt va mashinali o‘qitish asosidagi monitoring*

So‘nggi yillarda sun’iy intellekt (AI) va mashinali o‘qitish (ML) texnologiyalarining monitoring tizimlariga integratsiyasi tarmoq holatini chuqur tahlil qilish va anomal holatlarni prognozlash imkonini bermoqda.

*Afzalliklari:*

- Tarmoq trafikidagi g‘ayritabiiy holatlarni avtomatik aniqlash.
- Nosozliklar yuzaga kelishidan oldin ogohlantirish.
- Dinamik tarmoq sozlamalarini avtomatlashtirish orqali yuklamani muvozanatlash.

Misol: *Cisco AI Network Analytics, Juniper Mist AI, IBM SevOne NPM* kabi tizimlar AI asosida ishlaydi va real vaqtli analizni ta’minlaydi.

*Bulutli monitoring (Cloud-based Monitoring)*

An’anaviy monitoring tizimlari mahalliy (on-premise) infratuzilmalarda joylashgan bo‘lsa, hozirgi tendensiya bulutga asoslangan monitoring xizmatlariga o‘tishni ko‘rsatmoqda.

*Afzalliklari:*

- Moslashuvchanlik: istalgan joydan monitoringga ulanish.
- Masshtablilik: trafik ortgani sayin resurslar avtomatik kengayadi.
- Kam xarajat: jismoniy serverlar va texnik xizmatga ehtiyoj kamayadi.

Xizmatlar misoli: *Datadog, Amazon CloudWatch, Microsoft Azure Monitor, Google Cloud Operations Suite* (Stackdriver).

*Tarmoqda avtomatlashtirilgan xatti-harakat (Network Automation & Self-Healing)*

Tarmoq monitoringi tizimlari endilikda faqat holatni aniqlash bilan cheklanmayapti, balki muammoni avtomatik tarzda hal qilish imkonini bermoqda.

Masalan:

• Tarmoqdagi port nosoz bo‘lsa, tizim avtomatik boshqa portni faollashtiradi.

• DoS/DDoS hujumi aniqlansa, avtomatik filtr yoki bloklash harakati amalga oshiriladi.

Bu “self-healing network” (o‘z-o‘zini tiklovchi tarmoq) kontseptsiyasining rivojlanishidir.

*Tahliliy vositalar va prognozlash*

Monitoring tizimlari real vaqtli ma’lumotlarni to‘plash bilan birga, uzoq muddatli statistik tahlil, trafik tendensiyalari va prognozlash imkoniyatlarini ham taqdim eta boshladi.

*Amaliy misollar:*

- Trafik yuklamasining eng yuqori vaqtlarini aniqlash.
- Ma’lumotlar oqimi asosida xizmatlar sifati (QoS) darajasini prognozlash.
- Uzoq muddatli saqlanayotgan log ma’lumotlari asosida audit va xavfsizlikni mustahkamlash.

*Tarmoq segmentatsiyasi va mikrosementatsiya*

Tarmoq xavfsizligi va monitoringini yaxshilash maqsadida zamonaviy amaliyotlar tarmoqlarni lozim darajada segmentatsiyalashni taklif qilmoqda. Bu orqali har bir segment alohida monitoring qilinadi.

*Afzalliklari:*

- Har bir tarmoq zonasi bo‘yicha aniqlik va nazorat ortadi.
- Virus yoki tahdid bo‘lsa, faqat bitta segmentga zarar yetadi.
- Xavfsizlik devorlarini tarmoq ichida ham yaratish mumkin (microsegmentation).

*Ochiq manbali monitoring vositalarini moslashtirish*

Ko‘plab tashkilotlar Zabbix, Prometheus, Grafana, Telegraf kabi ochiq kodli vositalarni o‘z ehtiyojlariga moslab moslashtirishmoqda.

*Afzalliklari:*

- Arzon va moslashuvchan.
- Yangi plaginlar yoki modullar orqali qo‘shimcha funksiyalar qo‘shish mumkin.
- Keng jamoa qo‘llab-quvvatlovi mavjud.

*Integratsiyalashgan IT infratuzilma monitoringi*

Tarmoq monitoringi boshqa tizimlar — serverlar, virtual mashinalar, ma’lumotlar bazalari, xavfsizlik vositalari bilan birgalikda yagona monitoring platformasida olib boriladi.

Misol: *ManageEngine OpManager, SolarWinds Orion Platform* — barcha IT aktivlarni bitta interfeysda kuzatish imkonini beradi.

*Tendensiyalar yakuni:*

Monitoring texnologiyalarining kelajagi avtomatlashtirish, sun’iy intellekt va keng ko‘lamli integratsiya tomon harakat qilmoqda. Tarmoq infratuzilmasi murakkablashgani sari, monitoring vositalarining aqlli, kontekstli va o‘zgaruvchan holatlarga mos ishlashi talabi oshib bormoqda.

**XULOSA**

Telekommunikatsiya tarmoqlarining uzluksiz va ishonchli ishlashi zamonaviy infratuzilmalar, axborot xizmatlari va raqamli iqtisodiyotning barqaror faoliyati uchun muhim omildir. Ushbu maqolada tarmoq monitoringi va nazorati vositalarining roli, ularning funksional imkoniyatlari, zamonaviy texnologiyalar bilan integratsiyasi va tanlash mezonlari batafsil yoritildi.

Monitoring tizimlari tarmoq infratuzilmasidagi istalgan o‘zgarish, nosozlik yoki xavfsizlik tahdidini oldindan aniqlash imkonini berib, tezkor va samarali boshqaruvni ta’minlaydi.

Ayniqsa, Software-Defined Networking (SDN) va sun’iy intellekt (AI) kabi ilg‘or yondashuvlarning monitoring jarayonlariga joriy etilishi ushbu sohaga yangicha sifat va samaradorlik olib kirmoqda.

**REFERENCES**

1. Кук, Ричард. *Network Monitoring and Analysis: A Protocol Approach to Troubleshooting*. McGraw-Hill, 2020.
2. Cisco Systems. *Cisco Digital Network Architecture Overview*, 2022. https://www.cisco.com
3. Zabbix Documentation. *Zabbix Monitoring Solution Manual*, 2023. https://www.zabbix.com/documentation
4. Nagios Enterprises. *Nagios Core Documentation*, 2022. https://www.nagios.org
5. SolarWinds. *Network Performance Monitor Product Guide*, 2023. https://www.solarwinds.com
6. Open Networking Foundation. *Software-Defined Networking (SDN) Architecture*, ONF White Paper, 2021.
7. Prometheus Authors. *Prometheus Monitoring Guide*, 2023. https://prometheus.io/docs
8. ManageEngine. *OpManager Network Monitoring Guide*, 2022. https://www.manageengine.com
9. Juniper Networks. *HealthBot AI Monitoring Platform*, 2023.
10. IBM. *SevOne Network Performance Monitoring Platform Overview*, 2022.