ISSN 3060-4567

KOMPYUTER TARMOQLARINI ADMINISTRATORLASH: NAZARIY VA AMALIY JIHATLAR

Andijon shahar 1 son politexnikumi

Ichlab chiqarish ta‘lim ustasi Kompyuter tarmoqlari operatori

Mavlyanova Soxibaxon Axatovna

Tel: +998 91 607 47 83

Pochta: SoxibaxonMavlaynova@gmail.com

Annotatsiya: *Ushbu ilmiy maqola zamonaviy axborot texnologiyalari davrida kompyuter tarmoqlarini administratorlashning nazariy asoslari va amaliy jihatlarini atroflicha tahlil qiladi. Maqolada tarmoq administratorining vazifalari, tarmoq infratuzilmasini loyihalash, o'rnatish, sozlash, monitoring qilish va xavfsizligini ta'minlash bo'yicha asosiy tamoyillar yoritilgan. Shuningdek, tarmoqni boshqarishda qo'llaniladigan zamonaviy texnologiyalar, dasturiy va apparat vositalari, nosozliklarni bartaraf etish usullari hamda kiberxavfsizlikning dolzarb masalalariga alohida e'tibor qaratilgan. Bulutli hisoblashlar, virtuallashtirish, dasturiy ta'minot bilan aniqlangan tarmoqlar (SDN) kabi yangi tendensiyalar va ularning tarmoq administratsiyasiga ta'siri ham ko'rib chiqilgan. Maqola axborot texnologiyalari sohasi mutaxassislari, talabalar, tadqiqotchilar va tarmoq administratsiyasi bilan qiziquvchi keng jamoatchilik uchun mo'ljallangan bo'lib, sohadagi bilim va ko'nikmalarni chuqurlashtirishga yordam beradi.*

Kalit so'zlar: *Kompyuter tarmoqlari, tarmoq administratsiyasi, tarmoq infratuzilmasi, kiberxavfsizlik, tarmoq monitoringi, nosozliklarni bartaraf etish, router, switch, server, IP-manzil, DNS, DHCP, VPN, firewall, virtuallashtirish, bulutli hisoblashlar, SDN.*

Kirish

Bugungi kunda axborot texnologiyalari har qanday tashkilot, korxona va ijtimoiy hayotning ajralmas qismiga aylangan. Global axborot makonining kengayishi va raqamli iqtisodiyotning shakllanishi bilan kompyuter tarmoqlari zamonaviy

ISSN 3060-4567

jamiyatning "qon tomirlari" vazifasini bajarmoqda. Elektron pochta, veb-ilovalar, bulutli xizmatlar, onlayn savdo, masofaviy ish va ta'lim kabi ko'plab jarayonlar tarmoq infratuzilmasining uzluksiz va samarali ishlashiga bog'liq. Tarmoqlarning uzluksiz, samarali va xavfsiz ishlashini ta'minlash esa malakali tarmoq administratorlarining zimmasidagi asosiy vazifadir.

Kompyuter tarmoqlarini administratorlash – bu tarmoq infratuzilmasini loyihalash, o'rnatish, konfiguratsiya qilish, boshqarish, monitoring qilish, nosozliklarni bartaraf etish va xavfsizligini ta'minlashni o'z ichiga olgan murakkab jarayonlar majmuidir. Bu jarayon nafaqat texnik bilimlarni, balki tizimli fikrlash, muammolarni hal qilish qobiliyati va doimiy o'rganishni ham talab qiladi. Ushbu maqola kompyuter tarmoqlarini administratorlashning asosiy nazariy va amaliy jihatlarini ko'rib chiqishga, tarmoq administratorining zamonaviy sharoitlardagi rolini yoritishga, shuningdek, sohadagi yangi tendensiyalarni tahlil qilishga qaratilgan.

Tarmoq administratorining vazifalari va mas'uliyatlari

Tarmoq administratori – bu tashkilotning kompyuter tarmoqlari infratuzilmasini boshqaruvchi va texnik jihatdan qo'llab-quvvatlovchi mutaxassis. Uning asosiy vazifalari quyidagilardan iborat:

1. **Tarmoqni loyihalash va o'rnatish:**

Tashkilotning joriy va kelajakdagi ehtiyojlaridan kelib chiqqan holda tarmoq topologiyasini (yulduz, halqa, shina, to'r) tanlash va loyihalash.

IP-manzillash sxemasini (IPv4, IPv6, subnetting) rejalashtirish va amalga oshirish.

Tarmoq uskunalarini (routerlar, switchlar, serverlar, kirish nuqtalari, faervollar) tanlash, sotib olish va fizik jihatdan o'rnatish.

Kabel tizimlarini (strukturaviy kabellash, optik tolali kabellar, simsiz tarmoqlar) yotqizish va ulash.

Tarmoq diagrammalarini va hujjatlarini yaratish.

2. **Tarmoqni konfiguratsiya qilish:**

ISSN 3060-4567

Tarmoq qurilmalarini (routerlar, switchlar, simsiz kirish nuqtalari) to'g'ri sozlash, jumladan, asosiy konfiguratsiyalar, yo'naltirish protokollari (RIP, OSPF, EIGRP, BGP), VLAN (Virtual Local Area Network) larni yaratish va boshqarish.

Tarmoq protokollarini (TCP/IP, DNS, DHCP, HTTP/HTTPS, FTP, SSH) konfiguratsiya qilish.

Xizmat sifati (QoS) mexanizmlarini sozlash orqali muhim trafikka ustuvorlik berish.

3. **Serverlarni boshqarish:**

Fayl serverlari, veb-serverlar (Apache, Nginx, IIS), pochta serverlari (Exchange, Postfix), ma'lumotlar bazasi serverlari (MySQL, PostgreSQL, SQL Server) kabi turli xil server operatsion tizimlarini (Windows Server, Linux distributivlari - Ubuntu Server, CentOS, Red Hat) o'rnatish, sozlash va ularning uzluksiz ishlashini ta'minlash.

Virtualizatsiya texnologiyalaridan (VMware vSphere, Microsoft Hyper-V, KVM) foydalanib, virtual serverlarni yaratish va boshqarish.

Bulutli platformalarda (AWS, Azure, Google Cloud) virtual mashinalar va konteynerlarni (Docker, Kubernetes) boshqarish.

4. **Foydalanuvchilarni boshqarish:**

Tarmoq resurslariga kirish huquqlarini belgilash va boshqarish (Access Control Lists - ACLs).

Foydalanuvchi hisoblarini yaratish, o'zgartirish va o'chirish.

Katalog xizmatlarini (Active Directory, LDAP) sozlash va boshqarish.

Guruh siyosatlarini (Group Policy Objects - GPO) joriy etish va qo'llash.

5. **Tarmoq monitoringi:**

Tarmoq trafigini kuzatish va tahlil qilish (SNMP, NetFlow, sFlow).

Tarmoq qurilmalarining holatini (CPU yuklanishi, xotira ishlatilishi, interfeys holati) tekshirish.

Ish faoliyatini tahlil qilish va potentsial muammolarni oldindan aniqlash. Buning uchun turli monitoring dasturlari (masalan, Zabbix, Nagios, PRTG, SolarWinds) qo'llaniladi.

Log-fayllarni yig'ish va tahlil qilish.

6. **Nosozliklarni bartaraf etish:**

Tarmoqdagi nosozliklarni (masalan, ulanish yo'qligi, sekin ishlash, ma'lumotlar yo'qolishi, server ishdan chiqishi) aniqlash, tashxislash va qisqa muddatda bartaraf etish.

Diagnostika vositalari (ping, tracert, ipconfig/ifconfig, netstat, nslookup, Wireshark, Nmap) yordamida muammoning ildiz sababini topish.

7. **Kiberxavfsizlikni ta'minlash:**

Tarmoqni ruxsatsiz kirish, viruslar, zararli dasturlar (malware), fishing hujumlari va kiberhujumlardan himoya qilish.

Faervollarni (Firewall) sozlash va boshqarish (paket filtrlash, holatli tekshirish, ilova darajasidagi faervollar).

VPN (Virtual Private Network) larni o'rnatish va boshqarish orqali masofaviy foydalanuvchilar va filiallar uchun xavfsiz ulanishni ta'minlash.

Intrusion Detection Systems (IDS) va Intrusion Prevention Systems (IPS) larni joriy etish va boshqarish.

Xavfsizlik siyosatlarini ishlab chiqish va joriy etish, foydalanuvchilarni xavfsizlik qoidalari bo'yicha o'qitish.

Muntazam xavfsizlik auditlari va zaifliklarni baholashni o'tkazish.

Ma'lumotlarni shifrlash (encryption) va autentifikatsiya mexanizmlarini qo'llash (RADIUS, TACACS+).

8. **Ma'lumotlarni zaxiralash va tiklash:**

Muhim ma'lumotlarning (serverlar, ma'lumotlar bazalari, konfiguratsiya fayllari) zaxira nusxalarini yaratish va ularni xavfsiz joyda saqlash.

Favqulodda vaziyatlarda (apparat nosozligi, ma'lumotlar yo'qolishi, kiberhujum) ma'lumotlarni tez va samarali tiklash tizimini yo'lga qo'yish.

9. **Hujjatlashtirish:**

Tarmoq konfiguratsiyasi, topologiyasi, IP-manzillash sxemasi, xavfsizlik siyosatlari, server sozlamalari, nosozliklarni bartaraf etish tartiblari va boshqa muhim

ISSN 3060-4567

ma'lumotlarni batafsil hujjatlashtirish. Bu tarmoqni boshqarishda va yangi xodimlarni o'qitishda muhim ahamiyatga ega.

10. **Avtomatlashtirish:**

Takrorlanuvchi vazifalarni (masalan, konfiguratsiya o'zgarishlari, monitoring skriptlari, dasturiy ta'minotni yangilash) avtomatlashtirish uchun skriptlar (Python, PowerShell, Bash) va avtomatlashtirish vositalaridan (Ansible, Puppet, Chef) foydalanish.

Tarmoq infratuzilmasi komponentlari

Kompyuter tarmoqlari turli komponentlardan tashkil topgan murakkab tizimlardir. Ularning to'g'ri ishlashi va o'zaro aloqasi tarmoq administratorining asosiy vazifasidir.

- **Routerlar (marshrutizatorlar):** Turli tarmoqlarni (masalan, ichki lokal tarmoqni internetga) bir-biriga bog'laydigan va ma'lumot paketlarini optimal yo'nalish bo'yicha yo'naltiruvchi qurilmalar. Ular IP-manzillar asosida ishlaydi va tarmoqlararo aloqani ta'minlaydi. Routerlar statik yoki dinamik yo'naltirish protokollari (RIP, OSPF, EIGRP, BGP) yordamida yo'naltirish jadvallarini tuzadi.
- **Switchlar (kommutatorlar):** Lokal tarmoq ichidagi qurilmalarni (kompyuterlar, serverlar, printerlar) bir-biriga bog'laydigan va ma'lumot paketlarini MAC-manzillar asosida yetkazib beruvchi qurilmalar. Switchlar ma'lumotlarni faqat kerakli portga yuborish orqali tarmoq samaradorligini oshiradi. Ular boshqariladigan (managed) va boshqarilmaydigan (unmanaged) turlarga bo'linadi. Boshqariladigan switchlar VLAN, QoS, port xavfsizligi kabi funksiyalarni qo'llab-quvvatlaydi.
- **Serverlar:** Tarmoq foydalanuvchilariga turli xizmatlar (fayl saqlash, veb-sayt joylashtirish, elektron pochta, ma'lumotlar bazasi, DNS, DHCP, domen xizmatlari) taqdim etuvchi kuchli kompyuterlar. Serverlar odatda yuqori unumdorlik, ishonchlilik va xavfsizlik talablariga javob beradi.
- **Ishchi stansiyalar:** Tarmoqqa ulangan foydalanuvchi kompyuterlari, ular orqali foydalanuvchilar tarmoq resurslariga kirishadi.
- **Kabel tizimlari:** Ma'lumotlarni uzatish uchun ishlatiladigan fizik muhit. Bularga misol qilib, burama juft kabellar (Cat5e, Cat6, Cat7), optik tolali kabellar

(multimode, single-mode) va simsiz tarmoqlar (Wi-Fi) kiradi. Kabel tizimining to'g'ri loyihalashtirilishi va o'rnatilishi tarmoqning ishonchliligi va tezligini ta'minlaydi.

- **Tarmoq dasturiy ta'minoti:** Tarmoq operatsion tizimlari (masalan, Windows Server, Linux distributivlari), tarmoq xizmatlari (DNS, DHCP), monitoring va boshqaruv dasturlari, xavfsizlik dasturlari (antivirus, IDS/IPS).
- **Faervollar (Firewall):** Tarmoqqa kiruvchi va chiquvchi trafikni nazorat qiluvchi, ruxsatsiz kirishlarni bloklovchi dasturiy yoki apparat qurilmalar.
- **Kirish nuqtalari (Access Points):** Simsiz qurilmalarni (smartfonlar, noutbuklar) simsiz tarmoqqa ulash imkonini beruvchi qurilmalar.
- **Yuk balanserlari (Load Balancers):** Kiruvchi trafikni bir nechta serverlar o'rtasida taqsimlash orqali tarmoqning unumdorligi va ishonchliligini oshiruvchi qurilmalar.

Tarmoq xavfsizligi

Tarmoq xavfsizligi – bu tarmoq resurslarini ruxsatsiz kirish, foydalanish, o'zgartirish, yo'q qilish yoki oshkor qilishdan himoya qilishni ta'minlovchi chora-tadbirlar majmuidir. Tarmoq administratorining eng muhim vazifalaridan biri kiberxavfsizlikni ta'minlashdir.

- **Faervollar (Firewall):** Tarmoqqa kiruvchi va chiquvchi trafikni belgilangan qoidalar asosida filtrlash orqali tarmoqni himoya qiladi. Ular paket filtrlash, holatli tekshirish (stateful inspection) va ilova darajasidagi filtrlash (application-level filtering) kabi funksiyalarni bajarishi mumkin.
- **VPN (Virtual Private Network):** Ochiq tarmoq (masalan, internet) orqali xavfsiz va shifrlangan (IPsec, SSL/TLS) ulanishni yaratish imkonini beradi. Bu masofaviy foydalanuvchilar yoki filiallar uchun korporativ tarmoqqa xavfsiz kirishni ta'minlaydi.
- **Antivirus va zararli dasturlarga qarshi vositalar:** Tarmoqqa kiruvchi va chiquvchi fayllarni skanerlash, viruslar, troyanlar, shpion dasturlar va boshqa zararli dasturlarni aniqlash va yo'q qilish. Endpoint Detection and Response (EDR) tizimlari ham keng qo'llaniladi.

ISSN 3060-4567

- **Kirishni boshqarish (Access Control):** Foydalanuvchilarni autentifikatsiya qilish (ularning kimligini tasdiqlash, masalan, parol, ikki faktorli autentifikatsiya) va avtorizatsiya qilish (ularga qanday resurslarga kirishga ruxsat berish) mexanizmlari. Rolga asoslangan kirishni boshqarish (Role-Based Access Control - RBAC) keng tarqalgan.
- **Intrusion Detection Systems (IDS) va Intrusion Prevention Systems (IPS):** Tarmoq trafigini shubhali faoliyat yoki hujum belgilari uchun kuzatuvchi tizimlar. IDS faqat ogohlantirish beradi, IPS esa shubhali trafikni bloklaydi.
- **Xavfsizlik siyosatlari:** Tashkilot ichida xavfsizlik qoidalarini belgilovchi va ularga rioya etilishini ta'minlovchi hujjatlar. Masalan, parol siyosati, ma'lumotlardan foydalanish siyosati, mobil qurilmalar siyosati.
- **Muntazam yangilanishlar (Patch Management):** Operatsion tizimlar, dasturiy ta'minot va tarmoq qurilmalarining dasturiy ta'minotini muntazam yangilab borish, xavfsizlikdagi zaifliklarni (vulnerabilities) bartaraf etish.
- **Ma'lumotlarni shifrlash (Data Encryption):** Ma'lumotlarni uzatish va saqlashda ularni shifrlash orqali ruxsatsiz kirishdan himoya qilish.
- **Xavfsizlik axborot va hodisalarni boshqarish (SIEM - Security Information and Event Management):** Tarmoq qurilmalari va serverlardan log-fayllarni yig'ish, tahlil qilish va xavfsizlik hodisalarini aniqlash uchun markazlashtirilgan tizim.
- **DDoS hujumlaridan himoya:** Tarmoqni taqsimlangan xizmatdan voz kechish (DDoS) hujumlaridan himoya qilish mexanizmlari.

Nosozliklarni bartaraf etish metodologiyasi

Tarmoq administratorining muhim ko'nikmalaridan biri – tarmoqdagi nosozliklarni tez va samarali bartaraf etishdir. Buning uchun tizimli yondashuv va aniq metodologiya talab etiladi. Ko'pincha, OSI (Open Systems Interconnection) modelining yetti qatlami nosozliklarni bartaraf etishda asosiy yo'riqnoma bo'lib xizmat qiladi.

1. **Muammoni aniqlash:**
   - Foydalanuvchilarning shikoyatlarini tinglash va ularni to'g'ri tushunish.

ISSN 3060-4567

- Tarmoq monitoringi tizimlaridan (Zabbix, Nagios) ogohlantirishlarni tekshirish.
- Muammoning ko'lami va ta'sirini aniqlash (bir foydalanuvchiga ta'sir qiladimi yoki butun tarmoqqa).

2. **Ma'lumotlarni yig'ish:**

- Nosozlik haqida batafsil ma'lumot to'plash: qachon boshlangan, qanday o'zgarishlar sodir bo'lgan, qaysi qurilmalar yoki xizmatlar ta'sirlangan.
- Qurilmalarning log-fayllarini, konfiguratsiya ma'lumotlarini tekshirish.
- Foydalanuvchidan qo'shimcha ma'lumotlarni so'rash.

3. **Gipoteza yaratish:**

- Muammoning mumkin bo'lgan sabablari haqida farazlar ilgari surish. Masalan, "kabel uzilgan", "IP-manzil konflikti", "DNS server ishlamayapti", "faervol bloklayapti".
- Eng oddiy va ehtimoliy sabablardan boshlash.

4. **Gipotezani tekshirish:**

- Farazlarni tekshirish uchun diagnostika vositalari va testlarni qo'llash.
- **OSI modeliga asoslangan tekshirish:**
  - **1-qavat (Fizik):** Kabel ulanishini, LED indikatorlarini, tarmoq kartasining holatini tekshirish. (ping buyrug'i bilan ulanishni tekshirish).
  - **2-qavat (Kanal):** MAC-manzillarni, switchning MAC-jadvalini, VLAN sozlamalarini tekshirish. (arp -a, show mac address-table (Cisco) buyruqlari).
  - **3-qavat (Tarmoq):** IP-manzillar, subnet maskalar, shlyuz (gateway) sozlamalarini tekshirish. (ipconfig /all (Windows), ifconfig (Linux), route print, traceroute/tracert buyruqlari).
  - **4-qavat (Transport):** Portlar, TCP/UDP ulanishlarini tekshirish. (netstat, telnet buyruqlari).
  - **5-7-qavatlar (Sessiya, Taqdimot, Ilova):** Ilova darajasidagi xizmatlarning (DNS, HTTP, FTP) ishlashini tekshirish. (nslookup, dig, veb-brauzer orqali kirish).
- Paket analizatorlari (Wireshark) yordamida trafikni tahlil qilish.

- Tarmoq skanerlari (Nmap) yordamida ochiq portlar va xizmatlarni aniqlash.

5. **Yechimni amalga oshirish:**

- Muammoning sababi aniqlangach, uni bartaraf etish uchun tegishli chora-tadbirlarni qo'llash (masalan, kabelni almashtirish, IP-manzilni to'g'irlash, DNS serverni qayta ishga tushirish, faervol qoidalarini o'zgartirish).
- O'zgarishlarni amalga oshirishdan oldin zaxira nusxasini olish.

6. **Tekshirish:**

- Muammo bartaraf etilganligiga ishonch hosil qilish.
- Tarmoqning normal ishlashini, ta'sirlangan xizmatlarning tiklanganligini tekshirish.
- Foydalanuvchidan muammoning hal bo'lganligini tasdiqlashini so'rash.

7. **Hujjatlashtirish:**

- Muammo, uning sababi, bartaraf etish yo'llari va amalga oshirilgan o'zgarishlarni batafsil hujjatlashtirish. Bu kelajakda shunga o'xshash vaziyatlarning oldini olish va tezroq hal qilish uchun muhim ma'lumot bazasini yaratadi.

Yangi tendensiyalar va kelajak

Kompyuter tarmoqlari sohasi doimiy rivojlanishda bo'lib, tarmoq administratsiyasiga ham yangi tendensiyalar ta'sir ko'rsatmoqda:

- **Bulutli hisoblashlar (Cloud Computing):** Tashkilotlar infratuzilmasining bir qismi yoki to'liq qismi bulutga ko'chirilmoqda (IaaS, PaaS, SaaS). Tarmoq administratorlari endi nafaqat lokal tarmoqlarni, balki bulutli tarmoqlarni (Virtual Private Cloud - VPC) ham boshqarishlari kerak.
- **Virtuallashtirish (Virtualization):** Serverlar, saqlash tizimlari va tarmoq funksiyalarini virtuallashtirish (NFV - Network Function Virtualization) tarmoqni boshqarishni yanada moslashuvchan va samarali qiladi.
- **Dasturiy ta'minot bilan aniqlangan tarmoqlar (SDN - Software-Defined Networking):** Tarmoq boshqaruvini apparatdan ajratish orqali tarmoqni markazlashtirilgan dasturiy ta'minot yordamida boshqarish imkonini beradi. Bu tarmoqni avtomatlashtirish va konfiguratsiya qilishni soddalashtiradi.

- **DevOps va NetDevOps:** Dasturiy ta'minotni ishlab chiqish (DevOps) amaliyotlarini tarmoq administratsiyasiga qo'llash, tarmoq konfiguratsiyasini kod sifatida boshqarish (Infrastructure as Code) va avtomatlashtirish.
- **Kiberxavfsizlikning murakkablashuvi:** Kiberhujumlarning tobora murakkablashib borishi tarmoq administratorlaridan doimiy ravishda yangi himoya mexanizmlarini o'rganish va joriy etishni talab qiladi. Sun'iy intellekt va mashinani o'rganish kiberxavfsizlikda ham qo'llanilmoqda.
- **IoT (Internet of Things) va Edge Computing:** Ko'plab qurilmalarning tarmoqqa ulanishi va ma'lumotlarni tarmoq chetida (edge) qayta ishlash zarurati tarmoq infratuzilmasiga yangi talablar qo'ymoqda.

Xulosa

Kompyuter tarmoqlarini administratorlash zamonaviy axborot jamiyatida hal qiluvchi ahamiyatga ega bo'lgan murakkab va mas'uliyatli sohadir. Tarmoq administratorlari tashkilotlarning raqamli infratuzilmasining uzluksiz, samarali va xavfsiz ishlashini ta'minlashda muhim rol o'ynaydi. Ushbu sohada muvaffaqiyatga erishish uchun nazariy bilimlarni chuqur o'zlashtirish bilan birga, doimiy amaliy ko'nikmalarni rivojlantirish, zamonaviy texnologiyalardan xabardor bo'lish va kiberxavfsizlikka alohida e'tibor qaratish zarur.

Kelajakda tarmoq administratsiyasi bulutli hisoblashlar, virtuallashtirish, dasturiy ta'minot bilan aniqlangan tarmoqlar (SDN) va avtomatlashtirish texnologiyalari bilan yanada integratsiyalashib boradi. Bu esa tarmoq administratorlaridan yangi ko'nikmalar va doimiy malaka oshirishni talab qiladi. Ushbu maqolada keltirilgan ma'lumotlar tarmoq administratsiyasi sohasiga qiziquvchilar va mutaxassislar uchun foydali bo'ladi degan umiddamiz, shuningdek, ularni sohadagi bilim va ko'nikmalarini yanada chuqurlashtirishga undaydi.

FOYDALANILGAN ADABIYOTLAR

1. Tanenbaum, A. S., & Wetherall, D. J. (2011). *Computer Networks* (5th ed.). Pearson Education.
2. Odom, W. (2013). *CCNA Routing and Switching Official Cert Guide, Volume 1*. Cisco Press.

ISSN 3060-4567

3. Zucker, S. (2017). *CompTIA Network+ N10-007 Cert Guide*. Pearson Education.

4. Stallings, W. (2017). *Network Security Essentials: Applications and Standards* (6th ed.). Pearson.

5. Chapple, M. (2018). *CompTIA Security+ SY0-501 Cert Guide*. Pearson Education.

6. O'zbekiston Respublikasining "Axborotlashtirish to'g'risida"gi Qonuni (2004).

7. International Journal of Network Security. (Turli sonlar).

8. Goralski, W. (2017). *Software Defined Networking (SDN) and OpenFlow: A Practical Guide to Evolving Network Technologies*. McGraw-Hill Education.

9. Kim, G. (2018). *The Phoenix Project: A Novel About IT, DevOps, and Helping Your Business Win*. IT Revolution Press.

10. Cisco Systems. (Turli texnik hujjatlar va o'quv materiallari).