



TOSHKENT DAVLAT IQTISODIYOT UNIVERSITETI

**SUN'IY INTELLEKT NAZARIYASI VA AMALIYOTI:
TAJRIBALAR, MUAMMOLAR VA ISTIQBOLLAR**

**RESPUBLIKA ILMIY-AMALIY KONFERENSIYASI
MA'RUZALAR TO'PLAMI**

**21-22 MAY
2024 YIL**

Toshkent 2024

**O‘ZBEKISTON RESPUBLIKASI
OLIIY TA‘LIM, FAN VA INNOVATSIYALAR VAZIRLIGI
TOSHKENT DAVLAT IQTISODIYOT UNIVERSITETI**



**SUN‘IY INTELLEKT NAZARIYASI VA AMALIYOTI:
TAJRIBALAR,
MUAMMOLAR VA ISTIQBOLLAR**

**Respublika ilmiy-amaliy konferensiyasi ma‘ruzalar to‘plami
(1-qism)**

2024 yil 21-22-may

Toshkent shahri

Kaxorov A., Xayrullayev M. Online buyurtma qilishda chatbotlar va yetkazib berish xizmatlaridan foydalanish va uning afzalliklari.....	157
Khasanov D., Shirinboyev R. The main theory of linear regression models in data mining	160
Mamagapurova Sh. Steganography techniques and types of stenography	165
Mamanazirova S. Biznesni rivojlantirish uchun marketing modelini yaratishda sun'iy intellekt imkoniyatlaridan foydalanish.....	168
Mavlonova M. Globallashuv davrida biznes jarayonlarni modellashtirishda strategik boshqaruv usullaridan foydalanish	173
Mutalibov M.Sh. Biznes jarayonlarini optimallashtirish uchun robotlar va sun'iy intellektning afzalliklari	176
Norqulova D.R. Sun'iy intellekt yordamida ishlab chiqarish jarayonlarini avtomatlashtirish va optimallashtirish	178
Pattayeva S.B. Cisco Tarmoq Xavfsizligi: Zaruratlar va Yechimlar	181
Rahmatullayeva S.G'. Развитие искусственного интеллекта основа четвертой индустриальной революции.....	184
Rahmonov S.K., Rahmatullayeva S.G'., Yunusova S.F., Olimjonova D.O. Ривожланаётган мамлакатларда сунъий интеллектнинг тараккиётдаги ўрни	189
Shukurova M.E. O'zaro dinamik aloqadagi g'ovak muhitda neft va gazlarning filtratsiya jarayoni hisoblashlarni vizuallashtirish.....	192
Sunatov J. T. Sun'iy intellektning biznes jarayonlarini modellashtirishdagi ahamiyati.....	195
Toshpo'latova M.A., Belalova G.A. Sun'iy intellekt, uning iqtisodiyot va biznesga ta'siri.....	200
Xusenov Sh.Sh. Sun'iy intellektni biznes jarayonlarini modellashtirish va strategik boshqarishda qo'llash	202
Yoqubjonov F.N. Sinfdagi obyektlardan lokal metrika bo'yicha mantiqiy qonuniyatlarni topish va uning yechimi.....	205
Yusupova D.M. Sanoat korxonalarida sun'iy intellektning strategik jarayondagi o'rni.	210
Алиева Э.А. Искусственный интеллект в повышении активности инновационной деятельности.....	215
Ёқубжонов Ф.Н. Минимал конфигурацияли сунъий нейрон тўри асосида танлов қопламасини куришнинг математик модели.....	219

yordam beradi. Bu, biznes rivojlanishini o'rganishda yordam beradi va biznesning eng samarali yo'nalishlari va ilg'or mahsulotlari aniqlashda imkoniyatini yaratadi.

Foydalanilgan adabiyotlar ro'yxati.

1. H.Zhang. "Intelligent Control of Automated Microelectronic Production Lines Based on Artificial Intelligence" 2023 International Conference on Applied Intelligence and Sustainable Computing (ICAISC), Dharwad, India, 2023, -pp. 1-6.
2. G.Chen and Q. Yuan. "Application and existing problems of computer network technology in the field of artificial intelligence" 2021 2nd International Conference on Artificial Intelligence and Computer Engineering (ICAICE), Hangzhou, China, 2021, pp. 139-142.
3. Z.R.Rakhmonov, G.A.Pardaeva. Steps Of Organizing The Methodology Of Improvement Of Methods Of Distance Learning Of Students. 2021 International Conference on Information Science and Communications Technologies (ICISCT). Tashkent, Uzbekistan. (SCOPUS) 3-5 Nov. 2021.
4. F.A.Norqobilova. "Xizmat ko'rsatish tarmoqlarini modellashtirishda tizimli tahlil qilish, sintezlash va optimallashtirish" International journal of conference series on education and social sciences (Online). Vol. 1. No. 2. 2021.
5. Z.R.Rakhmonov, G.A.Pardaeva Mobile application development education methodology with integrated distance learning environment. Central Asian Journal of Education and Computer Sciences VOLUME 1, ISSUE 2, APRIL 2022 (CAJECS).
6. Kh.S.Mukhitdinov and F.A.Norqobilova. "Prospects Of Digitalization Of Craftsmanship Development In The Region" Journal of Pharmaceutical Negative Results (2022): -pp.345-352.

"CISCO TARMOQ XAVFSIZLIGI: ZARURATLAR VA YECHIMLAR"

Pattayeva Sevinch Baxtiyor qizi, Muhammad al-Xorazmiy nomidagi Toshkent Axborot Texnologiyalari universiteti Nurafshon filiali "Kompyuter injineriing" fakulteti 3-kurs talabasi.

Annotatsiya: "Cisco Tarmoq Xavfsizligi: Zaruratlar va Yechimlar" tarmoq xavfsizligining muhimligi va uni ta'minlash uchun zaruratlar va yechimlar haqida ma'lumot beradi. Maqola, tarmoq xavfsizligining muhimiyatiga e'tibor qaratiladi va xavfsizlik muammolari, ularning kelajakdagi tasirini, va ularga qarshi kurashishning muhimligi ko'rsatiladi.

Kalit so'zlar: Tarmoq xavfsizligi, tarmoqni hujjatlarini va ma'lumotlarini to'g'ridan-to'g'riroq va muxofaza qilishni ta'minlaydi.

"Cisco Network Security: Ehtiyojlar va yechimlar" - Bu sarlavha tarmoq xavfsizligi sohasidagi talablar va himoya vositalarini o'rganishni taklif qiladi, ehtimol Cisco kompaniyasining ushbu ehtiyojlarni qondirishga bo'lgan yondashuviga e'tibor qaratadi. Maqolada tarmoqlar duch keladigan turli xil xavfsizlik muammolari va Cisco xavflarni kamaytirish va tahdidlardan himoyalani uchun qanday yechimlar taqdim etishini ko'rib chiqishi mumkin.

U xavfsizlik devorini joriy etish, oldini olish tizimlari, xavfsiz kirishni boshqarish, shifrlash texnologiyalari, tahdidlarni aniqlash va tarmoq monitoringi

amaliyoti kabi mavzularni qamrab olishi mumkin. Bundan tashqari, u “ Cisco ”ning xavfsizlik mahsulotlari, xizmatlari portfelini va tarmoq xavfsizligi holatini yaxshilash bo‘yicha eng yaxshi amaliyotlarni muhokama qilishi mumkin.

Xavfsizlikning zarurligi: Maqola tarmoq xavfsizligining qanday muhim ahamiyatga ega ekanligini ta’kidlaydi. Tarmoq xavfsizligi muammatlari, yutuqlar, vaqt va pul yo‘qotishlari va kompaniyalarga katta zarar yetkazishi mumkinligini ko‘rsatadi.[1]

1.Ahamiyati: Tarmoq xavfsizligi kompaniyalar uchun juda muhimdir, chunki xavfsizlik muammatlari tarmoqdagi ma’lumotlar va tizimlar uchun katta kutilmagan zararlar yetkazishi mumkinligini o‘z ichiga oladi.

2.Muommolar: Tarmoq xavfsizligi muommolari, masalan, ma’lumot yo‘qotish, hujjatlarni yoki xavfsizlikni buzish, kompaniyalar uchun katta kutilmagan zararlar tug‘dirishi mumkinligini ta’kidlaydi.

3.Yutuqlar: Tarmoq xavfsizligi yutuqlari,tarmoqdagi ma’lumotlarni uchratilishi va undan foydalanilishi uchun berilgan imkoniyatlarni ta’kidlaydi.

4.Yo‘qotish: Tarmoq xavfsizligi yo‘qotishlari, kompaniyalarga vaqt va pul yo'qotishiga olib kelishi mumkin, chunki bu yo‘qotishlar tarmoqdagi faollikni to‘xtatishi va ma’lumot yo‘qotishiga olib kelishi mumkin.

5.Katta zarar: Tarmoq xavfsizligi muommolari yuzaga kelsa, kompaniyalarga katta zarar yetkazishi mumkinligini ta'kidlaydi, chunki bu muommolarin ma’lumotlar va operatsiyalarga ta’sir qilishi mumkin.

Xavfsizlik so‘rovlarining yechimlari: Cisco tarmoqlarida xavfsizlikni ta’minlash uchun muhim bo‘lgan asosiy yechimlar, masalan, kamchiligini tasdiqlash, ma’lumotlarni shifrlash, tarmoq trafiklarini monitoring qilish va oddiyroq xavfsizlik so‘rovlarini o‘rnatishni qanday amalga oshirishni o‘rganishga yordam beradi.[2]

1.Ma’lumotlarni shifrlash: Ma’lumotlarni shifrlash, tarmoqda uzatilayotgan ma’lumotlarni himoya qilishning asosiy usuli. Bu yechim, ma’lumotlarni sirli alifbo yordamida kodlash orqali ma’lumotlarni himoya qilishni ta’minlaydi.

2.Tarmoq trafiklarini monitoring qilish: Tarmoq trafiklarini monitoring qilish, tarmoqdagi faoliyatni kuzatish va g‘ayrioddiy holatlarni aniqlash uchun muhimdir. Bu yechim, tarmoqda yo‘l topishini va shuningdek tarmoqdagi qurilmalar orasidagi aloqani nazorat qilishni osonlashtiradi.

3.Oddiyroq xavfsizlik so‘rovlarini o‘rnatish: Oddiy xavfsizlik so‘rovlarini o‘rnatish, tarmoqdagi oddiy xavfsizlik muammatlarni hal qilishga yordam beradi. Bu yechim, oddiyroq xavfsizlik so‘rovlarini o‘rnatish, tarmoqda asosiy xavfsizlikni ta’minlash uchun qo‘llaniladi.

Ushbu yechimlar tarmoq xavfsizligini ta’minlashda asosiy bo‘lib, Cisco tarmoqlarida amalga oshiriladigan xavfsizlik so‘rovlarini yaratish va o‘rnatishda kritish ahamiyatga ega.

Bu yechimlar tarmoq administratorlari va xavfsizlik mutaxassislariga tarmoq xavfsizligini oshirish va uni boshqarishda yordam beradi.

“Xavfsizlik muammolari yechimlari” mavzusida Cisco tarmoqlarida xavfsizlikni ta’minlash uchun muhim bo‘lgan asosiy yechimlar yoritilgan.

Maqolaning “Xavfsizlik muammolari yechimlari” bo‘limi Cisco tarmoqlari ,Xavfsizlik muammolari ,yechimlar ,tarmoq xavfsizligi ,kiberxavfsizlik choralari ,tahdidni yumshatish ,risklarni boshqarish ,xavfsizlik yechimlari ,hodisaga javob ,kirish nazorati ,bosqinni aniqlash ,ma'lumotlarni shifrlash ,xavfsizlik siyosatini amalga oshirish ,zaifliklarni boshqarish ,muvofiqlik monitoringi.

“Xavfsizlik protokollari”Cisco tarmoqlarida amalga oshiriladigan asosiy xavfsizlik protokollarini ta’kidlaydi. Bu protokollar masalan, IPsec (Internet Protocol Security), SSL/TLS (Secure Sockets Layer/Transport Layer Security), AAA (Authentication, Authorization, and Accounting) va tarmoqni monitoring qilish uchun ushbu protokollar yoki vositalardan foydalanishni ta’kidlaydi:

IPsec (Internet Protocol Security): IPsec, internet protokolni himoya qilish uchun ishlatiladigan protokollar to‘plamidir. U, ma'lumotlarni shifrlash, kimlik tasdiqlash va integritetni ta'minlash uchun foydalaniladi. Cisco tarmoqlarida IPsec protokollari o‘rnatilishi tarmoq xavfsizligini oshirishda juda muhimdir.

1.SSL/TLS (Secure Sockets Layer/Transport Layer Security): SSL/TLS, internet tarmoq bo‘ylab ma'lumot almashishni shifrlash uchun ishlatiladi. Bu protokollar, veb saytlar, elektron pochta xabarlar va boshqa tarmoq ilovalari o‘rtasida xavfsiz almashishni ta'minlaydi. Cisco tarmoqlarida SSL/TLS protokollaridan foydalanish, masalan, HTTPS tarmoq xavfsizligini oshirishda kreativ.[3]

2.AAA (Authentication, Authorization, and Accounting): AAA protokollari, foydalanuvchilar kimligini tasdiqlash, ularning yo‘nalishlariga ruxsat etish va ulardagi faoliyatni nazorat qilish uchun ishlatiladi. Bu protokollar, tarmoqdagi resurslarga kirishni nazorat qilish, foydalanuvchilarga moslashtirilgan huquqlarni berish va faoliyatlarini nazorat qilishga imkon beradi.

3.Tarmoqni monitoring qilish uslublari: Tarmoqni monitoring qilish uchun mo‘ljallangan protokollar va vositalar, tarmoqdagi trafikni nazorat qilish va yozilgan ma'lumotlarni analiz qilish uchun foydalaniladi. Cisco tarmoqlarida amalga oshiriladigan tarmoqni monitoring qilish uslublari tarmoqni xavfsizligini ta'minlashda juda muhimdir.

Ushbu protokollar va vositalar, Cisco tarmoqlarida amalga oshiriladigan xavfsizlikni ta'minlashda muhim ahamiyatga ega. Bu protokollar tarmoq administratorlari va xavfsizlik mutaxassislariga tarmoq xavfsizligini oshirish va uni boshqarishda yordam beradi.[4]

“Xavfsizlik so'rovlarining amalga oshirilishi” mavzusidagi , tarmoq xavfsizligini ta'minlash uchun qanday protsesslarni o‘tkazish, xavfsizlikni nazorat qilish, hujjatlarni yuritish va xavfsizlik so‘rovlarini ishlab chiqishni amalga oshirishning muhimligi haqida ma'lumot beradi.

1.Xavfsizlik protsesslarini o‘tkazish: Tarmoq xavfsizligini ta'minlash uchun protsesslarni o‘tkazishning muhimligini ta’kidlaydi. Bu protsesslar foydalanuvchilar kimligini tasdiqlash, ma'lumotlarni shifrlash, tarmoq trafikini nazorat qilish va hujjatlarni yuritishni o‘z ichiga oladi.

2.Xavfsizlikni nazorat qilish: Xavfsizlikni nazorat qilish, tarmoqda oddiyroq xavfsizlik so‘rovlarini yuritish, tarmoq trafikini kuzatish, holatlarni aniqlash va dastlabki taqiqlovlar va hal qilishlarni amalga oshirishni o‘z ichiga oladi.

3.Hujjatlarni yuritish: Hujjatlarni yuritish, tarmoq xavfsizligi muammoatlarini hal qilish uchun zarur bo‘lgan protsesslarni amalga oshirishni ta‘minlaydi. Bu jarayon, xavfsizlikni nazorat qilish, identifikatsiyani va yetkazib berishni ta‘minlash,

Ma‘lumotlarni himoya qilish va tarmoq trafikini kuzatishni o‘z ichiga oladi.

4.Xavfsizlik so‘rovlarini ishlab chiqish: Xavfsizlik so‘rovlarini ishlab chiqishning muhimligini ta‘kidlaydi. Bu so‘rovlar, tarmoqdagi xavfsizlik muammoatlarini aniqlash, tahlil qilish, dastlabki taqiqlovlar va hal qilishlar uchun muhimdir.

Ushbu protsesslar, tarmoq xavfsizligini oshirish va uni boshqarish uchun asosiy bo‘lib, tarmoq administratorlari va xavfsizlik mutaxassislariga qanday qilib tarmoq xavfsizligini oshirish va muammolarni hal qilishda yordam beradi.[5]

Foydalanilgan adabiyotlar.

1. Omar Santos va Jon Stuppi tomonidan “ CCNA Security 210-260 rasmiy sertifikat qo‘llanmasi”: Ushbu rasmiy qo‘llanma CCNA Security sertifikatlash imtihonlari mavzularini qamrab oladi va Cisco tarmoqlarini himoya qilish bo‘yicha keng qamrovli ma‘lumotlarni taqdim etadi.

2. Jazib Frahim, Omar Santos va Endryu Ossipovning “Cisco ASA: Barchasi birda yangi avlod xavfsizlik devori, IPS va VPN xizmatlari”: Ushbu kitob Cisco Adaptive Security Appliance (ASA) xavfsizlik devori, IPS va VPN haqida batafsil ma‘lumot beradi. xizmatlar, jumladan, konfiguratsiya, muammolarni bartaraf etish va eng yaxshi amaliyotlar.

3. Ketrin Paquet tomonidan “Cisco IOS Network Security (IINS 640-554) Foundation o‘quv qo‘llanmasini amalga oshirish”: Ushbu qo‘llanma AAA, ACL, VPN va boshqalar kabi mavzularni qamrab olgan.Cisco routerlari va kalitlari yordamida xavfsizlik xususiyatlari va texnologiyalarini joriy etishga qaratilgan.

4. Nazmul Rajib tomonidan “Cisco Firepower Threat Defense (FTD): Yangi avlod xavfsizlik devori (NGFW), yangi avlod hujumlarini oldini olish tizimi (NGIPS) va ilg‘or zararli dasturlardan himoya qilish (AMP) uchun konfiguratsiya va muammolarni bartaraf etishning eng yaxshi amaliyotlari”: Ushbu qo‘llanma keng qamrovli ma‘lumotlarni taqdim etadi. Kengaytirilgan tarmoq xavfsizligi uchun Cisco Firepower Threat Defense (FTD) yechimlarini sozlash va muammolarni bartaraf etish bo'yicha qo‘llanma.

5. Mohamed Elmahdi, Umar Santos va Massimo Neri tomonidan yozilgan “Raqamli transformatsiya uchun Cisco xavfsizlik echimlari”: Bu kitob Cisco xavfsizlik yechimlari va raqamli transformatsiyani faollashtirish va mustahkam kiberxavfsizlik holatini ta‘minlash strategiyalarini o‘rganadi.