TARMOQLARDA UZATILADIGAN MA’LUMOTLARNI XATOLIKLARINI BARTARAF ETISH USULLARI

Boymuratov Erkin Kamolovich
Farg‘ona ICHSHUI kasb-hunar maktabi maxsus fan o‘qituvchisi

Annotatsiya: *Tarmoqlarda uzatiladigan ma’lumotlarni xatoliklarini bartaraf etish usullari xaqida ma’lumotlar berilgan.*

Kalit so‘zlar: *tarmoqlarda uzatiladigan ma’lumotlarni xatoliklar, kompyuter tarmoqlar, Muammolarni bartaraf etish, yuqoridan pastga, pastdan yuqoriga, SNMP, Netflow, ping.*

Kompyuter tarmoqlardan foydalanuvchilar tarmoqdagi axborot almashuv vositasi va kimmatbaxo apparat vositalari, dasturiy, axboriy resurslardan jamoa

bo‘lib foydalanish imkoniga ega bo’lishadi. Bu imkoniyatlarni esa tarmoqlar taqdim etishi shart va shundagina tarmoqning samaradonligini qayd etish mumkin. Eng asosiysi tarmoqga ulangan foydalanuvchilar kerakli axborotni qiynalmasdan olishi, printer, skaner, modem va boshqa bir qator apparat vositalaridan osongina foydalana olishi mumkin bo‘ladi. Bu imkoniyat tarmoq foydalanuvchilarning qimmatbaxo vositalarsiz kerakli vazifaga yechim topishi qulayligani yaratib beradi. Albatta buning uchun tarmoqda shu apparat vositalarning mavjudligi talab etadi.

Aytish mumkinki, kompyuter tarmoqlari mutaxasisi uchun eng qiyin ishlardan biri bu ular boshqaradigan infratuzilmada yuzaga kelishi mumkin bo‘lgan muammolarni hal qilishdir. Muammoni hal qilish tahlil va yechimni o‘z ichiga olgan muammoni hal qilish jarayoni sifatida tavsiflanadi. Muammoni aniqlagan yoki muammoni hal qilish bilan shug‘ullanayotgan shaxs bo‘lsa, javob faol bo‘lishi mumkin yoki agar u muammoli chipta sifatida kelgan bo‘lsa yoki foydalanuvchi yoki guruh tomonidan bildirilgan bo‘lsa, reaktiv bo‘lishi mumkin. Muammo yuzaga kelganda qilish kerak bo‘lgan birinchi qadam, administrator muammo yuzaga kelgan vaqt davomida kiritilgan o‘zgarishlar va hokazolar haqida iloji boricha ko‘proq ma'lumot to‘plashdir, shunda siz ildiz sababini aniqroq aniqlashingiz mumkin. Tegishli barcha ma'lumotlarni tanlash va olib tashlash vaqtni yo‘qotish yoki hatto mumkin bo‘lgan chalkashliklarni oldini olmaydi. Muammoning asosiy sababi hal qilish uchun eng yaxshi yondashuvni izlash va vaziyatga qarab tezkor harakat (masalan, RJ45 ulagichini tuzatish) yoki biroz vaqt talab qilishi (masalan, Ethernet kartasini almashtirish) bo‘lishi mumkinligi ma'lum. muammoni bir zumda hal qila olmaysiz, keyingi qadam mijozga ta'sir qiladimi yoki yo‘qligini so‘rashdir, agar shunday bo‘lsa, asosiy sabab hal qilinganda mijoz uchun ulanishni hal qilishga harakat qilish kerak (masalan, men portni o‘zgartirish). u mijozga ulangan).Biz tarmoq muammosini eng yaxshi hal qilish uchun qo‘llanilishi kerak bo‘lgan usullar, protseduralar va asosiy

vositalarni taqdim etamiz, chunki agar tizimli jarayonda muammolarni bartaraf etish rejasi bajarilmasa, bu allaqachon bajarilgan narsani eslay olmasligi yoki shunchaki kimdir yordamga kelishi va qila olmasligi mumkin. qanday bosqichlar va qanday tartibda bajarilganligini aniq tushuntiring.Ammo shunday bo‘lishi mumkinki, sizda mavjud muammo tanish va uni qanday hal qilishni allaqachon biladi. Bu usul odatda kalçadan otishni o‘rganish deb ataladi. Keyinchalik keng tarqalgan bo‘lib foydalaniladigan bir nechta muammolarni bartaraf etish usullari:Yuqoridan pastga usuli: OSI modelining yuqori qatlamlarida muammoni qidirishni boshlashga asoslanib, agar ma'lum bir qatlam u erda ishlayotgan bo‘lsa, shunday bo‘ladi deb taxmin qilish.Pastdan yuqoriga usuli: Bu yuqoridagi usulning teskari holati. Bu juda samarali, lekin katta tarmoqlarda sekin bo‘lishi mumkin.Bo‘l va zabt etish usuli: Bu usulda birinchi navbatda OSI modelining oraliq qatlamlarini tekshirish kerak, agar birinchisiga tegishli qism ikkinchi qismga e'tibor qaratish to‘g‘ri deb hisoblansa, sinov muvaffaqiyatli bo‘ladi. Aks holda, muammo birinchi yarmida qidiriladi.Trafik monitoringi usuli: Kelib chiqish va maqsadli trafik o‘rtasidagi qurilmalarni tahlil qilish asosida.

SHaxsiy kompyuterning konfiguratsiyalarni solishtirish usuli: Bu, ayniqsa, tarmoqqa o‘zgartirish kiritilgandan so‘ng muammolar yuzaga kelgan hollarda foydalidir. Bu shunchaki joriy konfiguratsiyani oxirgi ma'lum bo‘lgan yaxshilik bilan solishtirishga asoslangan. Qismlarni almashtirish usuli: Bu tarmoq segmentini tashkil etuvchi qismlarni jismonan almashtirishdan iborat bo‘lgan muammolar mavjud. Muammolarni bartaraf qilishda va OSI modelining 1-darajadagi xatolik tekshirilganda, masalan, xostda Internetga ulanmagan holda, avval tarmoq kartasini, kabelni, ulagich port routerini va hokazolarni jismonan tekshiring.

Muammolarni bartaraf etish usullari. Yaxshi tuzilgan nosozliklarni bartaraf etish jarayoni korxonadagi resurslardan samaraliroq foydalanishga yordam beradi va agar ma'mur boshqasining ishini davom ettirishi kerak bo‘lsa, qabul qilish osonroq bo‘ladi. Yuqoridagi bosqichlarning kombinatsiyasi orqali quyidagi jarayon tuzilgan: Muammo haqida hisobot. Odatda bu tarmoq resurslaridan foydalanadigan odamga beradi va ko‘pincha bu ma'lumot noto‘g‘ri va ba'zan noto‘g‘ri bo‘ladi. Muammolar haqida xabar beradigan kimdir, birinchi navbatda, tarmoqning bir qismi ta'sirlanganligini, buzilish uchun qaysi qurilmalar yoki guruh javobgarligini aniqlashga xizmat qiladi. Ma'lumotlaringizni to‘plang. Xato haqida xabar berilgandan va tarmoqning muammoga ega bo‘lgan qismi aniqlangandan so‘ng, ta'sirlangan qurilmalardanimkon qadar ko‘proq ma'lumot to‘plashingiz kerak, masalan, jurnallar, tarixiy o‘zgarishlar va hokazo. Agar tarmoq qurilmalari mavjud bo‘lmasa kirish uchun ushbu ma'lumot uchun tegishli guruhlarga murojaat qilish kerak bo‘ladi. Yig‘ilgan ma'lumotlarni ko‘rib chiqing. Barcha kerakli ma'lumotlarni to‘plaganingizdan so‘ng, har doim xabardor bo‘lgan holda uni chuqur tahlil qilish kerak: Muammoning asosiy sabablarini aniqlang. Keraksiz ma'lumotlarni olib tashlang.Administratorning tajriba darajasiga qarab, ko‘proq yoki kamroq tez javob berish uchun ba'zi savollarga javob berish kerak, siz u to‘plagan

barcha ma'lumotlarni tahlil qilishingiz yoki shunchaki tarmoq protokollarining xatti-harakatlarini kuzatishingiz kerak va hokazo. Bu savollar quyidagilar bo‘lishi mumkin:Tarmoqda nima sodir bo‘lmoqda?Qanday ishlashim kerak?Men nima bo‘lishim kerak?Potentsial sabablarni yo‘q qiladi. Ko‘rib chiqilgan ma'lumotlardan so‘ng, muammoga tegishli bo‘lmagan sabablar va to‘plangan gipotezada bo‘lmagan ma'lumotlarga asoslanib tasavvur qilmaslik yoki qilishni xohlamaslik juda muhim bo‘lgan ma'lumotlardan voz kechish kerak. Sabab uchun gipoteza yarating. Potentsial sabablarni bartaraf etgandan so‘ng, siz faqat yakuniy deb hisoblangan sababga e'tibor qaratishingiz kerak. Agar siz qurilmaga kirish imkoniga ega bo‘lsangiz, muammoni hal qilishga urinish davom etadi. Qurilmaga kirish imkoni bo‘lmasa, tegishli tarmoq ma'muri orqali muqobil yechim izlash kerak. Gipotezani tasdiqlang. Buning sababini bilganimizdan so‘ng, uni hal qilishga harakat qilishimiz mumkin. Qanday harakat qilish haqida o‘ylash kerak, chunki yechimni darhol amalga oshirish tarmoqdagi uzilishlarga olib kelishi mumkin, keyin kechasi yoki hozir ta'sir minimal bo‘lganda yaxshiroq aralashuvni yaxshiroq rejalashtirish. Bu vaziyatda qo‘llaniladigan barcha o‘zgarishlarni hujjatlashtirish juda muhim, mo‘ljallangan yechim muammoni hal qilmaydi, orqaga chekinish va boshqa yechim haqida o‘ylash mumkin. Muammoni hal qilish. Muammo hal qilingandan so‘ng, u qanday hal qilinganidekaniq hujjatlashtirilishi kerak va barcha tomonlar nima bo‘lganligi va qanday hal qilinganligi haqida tushuntirish olishlari kerak.Texnik xizmat ko‘rsatish va nosozliklarni bartaraf etish uchun vositalarU, shuningdek, siz foydalanayotgan operatsion tizimbilan birga kelgan ulanish muammolarini bartaraf etishning muhim vositalarini ham biladi.Ushbu asosiy vositalardan ba'zilari:Ping: funktsiya ICMP echo (Internet Control Message Protocol) dan foydalanadi va xost ulanganligini aniqlash uchun eng past darajadagi testdir. Ping -bu masofaviy kompyuterning to‘g‘ri ishlashini va tarmoq ulanishlari buzilganligini tekshiradigan vositadir. Ping 3-qavatdagi muammolarni bartaraf etish uchun juda foydali bo‘lib, nafaqat ma'lum bir xost faol yoki yo‘qligini ko‘rsatadi, balki ko‘proq ma'lumot beruvchi qo‘shimcha parametrlar imkoniyatini ham taklif qiladi. Traceroute (Tracert aka): Paket o‘z manziliga yetguncha uning yo‘lini kuzatib boring. Bu paketning har bir sakrash orqali o‘z manziliga etib borishi uchun qancha vaqtketishini o‘lchaydi. Pathping: Ping va Tracert xususiyatlarini boshqa ma'lumotlar bilan birlashtirgan marshrutlash vositasi. IPconfig: Kompyuteringizning IP konfiguratsiyasini tekshiring va kompyuterning tarmoqqa to‘g‘ri ulanishini aniqlash uchun foydalaniladigan ma'lumotlarni chiqaradi. Telnet: masofaviy xost yoki serverdan ulanishni tekshirish uchun ishlatiladi. Netstat: Serveringizni tinglaydigan barcha TCP / UDP portlarini, shu jumladan serveringizga va serverdan barcha faol tarmoq ulanishlarini ro‘yxatlaydi. Tarmoq monitori: keyingi tahlil qilish uchun tarmoq paketlarini olish imkonini beradi. SNMP: Resursdan foydalanish, turli hisoblagichlardagi xatolar soni va hokazo kabi qurilma statistikasini to‘playdi. U NMS (Tarmoqni boshqarish stantsiyasi) vaqti-vaqti bilan statistik ma'lumotlarni so‘raydigan "pull" stansiyasini ishlatadi. Bu keng tarqalgan, aytish

mumkinki, deyarli har qanday tarmoq qurilmasi SNMP dan foydalanishi mumkin.Netflow: Trafik namunalarini to‘plang. Push deb nomlangan modeldan foydalanadi. Ya'ni, qurilma vaqti-vaqti bilan trafik namunasini kollektor deb ataladigan boshqa qurilmaga yuboradi. U faqat marshrutizatorlarda va yuqori sifatli kalitlarda mavjud.

Kompyuter tarmoqlarining imkoniyatlari, starukturalari va turlari xam xilma-xil bo’lishi mumkin. Bunday tuslanishlar kompyuter tarmoqlarining xar-xil soxalarda rivojlanib borayotganini bildiradi. Kompyuter tarmoqlari asosan quidagi vazifalarni bajarishi va tarmoqlardan foydalanuvchilar uchun quyidagi qulayliklarni yaratishi lozim: tarmoqdagi foydalanuvchilar uchun taqsimlangan resurslarga oddiy, qulay kirishni taminlash; tarmoqdagi barcha foydalanuvchilarga tarmoq resurslarni birdey taqsimlash; tarmoqdan foydalanuvchilarning jamoa bo’lib ishlashini taminlash; foydalanuvchilar orasida ma’lumot almashishini tez va qulay bo’lishini taminlash; tarmoqlardagi axborotlarni va axborot oqimlarini ishonchli ximoyalashni taminlash; tarmoqga ruxsat berilmagan kirishdan ximoya qilishni taminlash; tarmoqdagi saqlanadigan axborotlarni zaxiralash xamda axborotlarini yuqolishidan ishonchli ximoyalash (katta tarmoqlarda va savdo iqtisodiy soxalaga tegishli tarmoqlarda viruslardan ximoyalanish)ni taminlash; tarmoqlardagi texnik va dasturiy kamchiliklar va nosozliklarni tez va ishonchli bartaraf etishni taminlash. Bu qulayliklani yarata oladigan tarmoqlar kompyuter tarmoqlari degan nomga sazavor. Lekin shunday tarmoqlar mavjudki, bu tarmoqlar ba’zi bir qulayliklarni o’z ichiga jamlay olmaydi. Masalan lokal tarmoqlar bu tarmoqlar kichik doirani qamrab oladi va shuning uchun bazi bir qulayliklani yarata olmaydi. Shunday bo’lsada bu tarmoqlar tezlik jixitidan juda qulaydir. Lokal tarmoqlar eng ko‘p tarqalgan tarmoq bo’lib deyarli xamma o‘quv yurtlari va boshqa muasasalarda qo‘llaniladi.

Internet tarmog‘i esa aytib o‘tilgan qulayliklarga yana qo‘shimcha imkoniyatlarni taqdim emoqda. Internet imkoniyatlari ko’paygani sari undan foydalanuvchilar soni xam ko‘payib bormoqda. Xozirda Internet global tarmog‘i

butun dunyo foydalanuvchilarga xizmat ko‘rsatishga tayor. Tarmoqlar xaqida gapirar ekanmiz shu tarmoqlarning ishlashini ta’minlaydigan apparat vositalari xamda uzatish kanallari xaqida gapirib o’tish lozim. Kompyuter tarmoqlari quyidagi apparat vositalaridan tashkil topishi mumkin:

1.Uzatish kanallari.

2.Axborot almashishini taminlaydigan apparat vositalari.

Bu maxsus simlar yoki simlarsiz tashkil qilinadigan kanallar bo’lib ular maxsus yoki maxalliy tashkil qilingan bo‘lishi mumkin:

Maxsus – bu kompyuter tarmoqlarini tashkil qilishda maxsus kanallar, kabellar va simlar o’tkaziladi yoki radio aloqa kanallarida maxsus efirlar ishlatiladi.

Maxalliy – bu kanallar xam simlar va radio kanallardan tashkil topishi mumkin, lekin ular maxalliy foydalanuvchilar komunikatsiyalari orqali o‘tadi.

Uzatish kanallari albatta o‘z qobiliyatlariga ega:

Uzatish kanallarining o‘tkazish qobiliyati birlik vaqt oralig‘ida tizim bo‘yicha

uzatilishi mumkin bo‘lgan ma’lumotlar miqdoridir. Tizimning bu qobiliyati o‘tkazgichdagi va qabul qilgichdagi axborotni o‘zgartirish tezligi bilan va uzatish kanali bo‘yicha axborotning uzatishning kanal va signallarning fizik xossalari orqali

aniqlanadi.

Axborot uzatish kanallarning xaqqoniylik qobiliyati axborotni buzmasdan

uzatishdir. Bunda kanallarning materiali va sifati katta ro‘l o‘ynaydi, ya’ni yuqori

sifatli kanallarda uzatish uzluksiz xamda xalaqitlarning juda kam bo’lishiga aytiladi.

Uzatish kanallarining ishonchlilk kobiliyati tarmoq tizimlarining xamma vazifalarini to‘g‘ri bajarishi to‘g‘ri ulanish, to‘liq va ishonchli yetkazilishini ta‘minlash.

Endi uzatish kanallari qanday kanallardan tashkil topgan bo’lishi mumkinligi xaqida aytib o‘tsak. Uzatish kanallari tabiatiga ko‘ra:

Mexanik – axborotlarning moddiy tashuvchilari uzatish (Bu kanal kompyuter soxasida qo‘llanilmaydi)

Akustik – tovushli signal uzatish (Bu kanal xam amalda qo‘llanilmaydi)

Optik– yoruglik signali o‘tkazish

Elektr– elektr signali uzatishlarga bo‘linadi. Biz albatta xozirgi zamon talablariga mos uzatish kanallarini ko‘rib o‘tishimiz shart.

Elektr kanallar quyidagicha ko‘rinishda bo’lishi mumkin:

Simli – signallarni o‘tkazish uchun fizik o‘tkazgichlar elektr simlar, kabellar, svetovodlar qo‘llaniladi. Bugungi kunda bu usul keng tarqalgan.

Simsiz – signallarni uzatish uchun radio kanallar, infraqizil kanallar, spektorli

kanallar, yuldosh orqali va efir orqali uzatiladi. Bu kanallar ochilib kelayotgan

imkoniyat bo’lib ular kelajakda ishonchli va keng qo‘llanilishi kutilmoqda. Bu

kanallar orqali axborotlar quyidagi ko‘rinishda o‘tishi mumkin:

Analogli (uzluksiz) – axborot analog kanallari bo‘ylab uzluksiz shakilda tasvirlangan bo‘ladi.

Raqamli – axborotlar raqamli kanallar bo‘ylab diskret yoki impulsli tarzda signal

ko‘rinishida uzatiladi. Bunda uzatish uzluksiz tazda bo’lishi mumkin. Tarmoq texnologiyasining keng ko‘lamda qo‘llanishi natijasida umumiy resurslardan foydalanish imkonini beruvchi lokal tarmoqqa kompyuterlar birlashtirildi. Kliyent-server texnologiyasining tatbiq etilishi esa bu tarmoqni taqsimlangan hisoblash muhitiga aylantirdi.

Tarmoqning xavfsizligi undagi barcha kompyuterlarning va tarmoq qurilmalarining xavfsizligi bilan aniqlanadi. Buzg‘unchi tarmoqning biror-bir tashkil

etuvchisining ishini buzish orqali butun tarmoqni obro‘sizlantirishi mumkin.

Zamonaviy telekommunikatsiya texnologiyalari lokal tarmoqlarni global tarmoqqa – Internetga ulash imkonini berdi. Internetningrivojlanishi xavfsizlikni ta’minlashni dolzarb masalaga aylantirdi va Internetga ulangan tarmoq va tizimlarda, qanday ma’lumotlarga ishlov berilishidan qat’iy nazar, xavfsizlik vositalari bo‘lishini taqozo etadi. Chunki,

Internetning imkoniyatlaridan foydalanib, buzg‘unchi xavfsizlikni buzishni global masshtabda olib borishi mumkin. Internetga ulangan

kompyuter tajovuz obyekti bo‘lsa, hujumni amalga oshirayotgan shaxsga uning qayerda (qo‘shni xonada yoki boshqa kontentda) joylashgani katta ahamiyatga ega emas.

Hamma foydalanayotgan tarmoqdan kelib chiqayotgan tahdidlarni blokirovkalash uchun «tarmoqlararo ekran» (Firewall) deb nomlanuvchi dasturiy va apparat-dasturiy vositalardan foydalaniladi. Odatda, alohida ajratilgan va himoyalangan KT «tarmoqlararo ekran» orqali hamma foydalanadigan tarmoqqa ulanadi.

Tarmoqlararo ekran himoyalangan KTga kelib tushayotgan va undan chiqib ketayotgan axborotlarni nazorat qilish uchun qo‘llaniladi.

Tarmoqlararo ekran quyidagi to‘rtta funksiyani bajaradi:

– ma’lumotlarni filtrlash;

– ekranlovchi agentlardan foydalanish;

– manzillarni translatsiyalash;

– hodisalarni qayd qilish.

Tarmoqlararo ekranning asosiy vazifasi (kirayotgan yoki chiqayotgan) trafikni filtrlashdan iborat. Korporativ tarmoqning himoyalanganlik darajasiga qarab filtrlashning turli qoidalari o‘rnatilishi mumkin. Filtrlash qoidalari filtrlar ketma-ketligini tanlash orqali amalga oshiriladi. Ushbu filtrlar o‘zidan keyingi filtrga yoki protokol sathiga ma’lumotlarni uzatilishiga ruxsat beradi yoki taqiqlaydi.

Tarmoqlararo ekran filtrlashni kanallar, tarmoqlar, transport va amaliy sathlarda amalga oshiradi. Ekran qancha ko‘p sathni o‘z ichiga olsa, shuncha takomillashgan hisoblanadi.

Tarmoqlararo ekranda, dasturiy vositachi vazifani bajaruvchi va subyekt va obyekt orasida ulanishni ta’minlovchi, so‘ngra axborotni qaydqilish va nazoratini amalga oshirib jo‘natuvchi, ekranlovchi agentlardan (proxy-serverlar) foydalaniladi. Ekranlovchi agentlarning qo‘shimcha vazifasi foydalanishga ruxsat berilgan subyektdan haqiqiy obyektni yashirishdan iborat. Ekranlovchi agentlarning o‘zaro aloqaishtirokchilariga ta’siri yo‘q.

Tarmoqlararo ekranning manzillarni translatsiyalash funksiyasi haqiqiy ichki manzillarni tashqi abonentlardan yashirish uchun mo‘ljallangan. Bu tarmoq topologiyasini yashirish va agar himoyalangan tarmoq uchun yetarli miqdorda manzillar ajratilmagan bo‘lsa, yanada ko‘proq sondagi manzillardan foydalanishga imkon yaratadi.

Tarmoqlararo ekran maxsus jurnallarda hodisalarni qayd qilib boradi.Biror aniq talab bo‘yicha ekranni sozlash orqali jurnallarni yuritish imkoniyati nazarda tutilgan. Yozuvlar tahlili o‘rnatilgan qoidalarni buzishga bo‘lgan buzg‘unchilarning urinishlarini qayd qilish va ularni aniqlash imkonini beradi.

Tarmoqlararo ekranlarga quyidagi zamonaviy talablar qo‘yiladi:

1. Asosiy talablar – bu ichki tarmoqning xavfsizlikni ta’minlash va tashqaridan ulanishlar va aloqa seanslarini to‘liq nazorat qilish.

2. Ekranlovchi tizim tashkilotning xavfsizlik siyosatini oddiy va to‘liq yuritish uchun quvvatli va moslanuvchan boshqarish vositalariga ega bo‘lmog‘i darkor.

3. Tarmoqlararo ekran lokal tarmoq foydalanuvchilariga sezdirmasdan ishlashi va ular tomonidan ruxsat etilgan amallarni bajarishlariga xalaqit bermasligi lozim.

4. Tarmoqlararo ekran ko‘p miqdordagi murojaatlar bilan blokirovka qilib qo‘yishni va ishdan chiqishining oldini olish uchun, uning protsessori tez ishlay olish, pik rejimlarida kiruvchi va chiquvchi oqimlarni yetarli darajada samarali qayta ishlay olishga ulgurishi lozim.

5. Xavfsizlikni ta’minlash tizimi har qanday tashqi noqonuniy ta’sirlardan himoyalangan bo‘lishi lozim, chunki bu ta’sirlar tashkilotning konfedensial ma’lumotlarini ochish kaliti bo‘lishi mumkin.

6. Ekranni boshqaruv tizimi olisdagi filiallar uchun ham yagona xavfsizlik siyosatini yuritishni markazlashgan holda ta’minlash imkoniyatiga ega bo‘lmog‘i lozim.

7. Tarmoqlararo ekran foydalanuvchilarning tashqi ulanishlari orqali foydalanishga ruxsat berishning mualliflashtirish vositalariga ega bo‘lmog‘i kerak. Bu tashkilot xodimlarini xizmat safarida ham tarmoqdan foydalanishlariga imkon yaratadi.

Kompyuter tarmog‘I - bu siz uchun yaratib bo‘lmaydigan yoki ishlamaydigan murakkab tizim. Tarmoq ma'muri ularning rivojlanishini sozlash, kuzatish va to‘g‘ri rejalashtirish imkoniyatiga ega bo‘lishi kerak. Bundan tashqari, Tarmoq menejeri tarmoq muammolari va lotin foydalanuvchilarini tezda hal qilishi kutilmoqda. Muammoning sababini va uni qanday hal qilishni mantiqiy aniqlash uchun resurslar va ko‘nikmalarga ega bo‘lish juda muhimdir. Ushbu hujjatda keltirilgan nosozliklarni bartaraf etish usullari va tartiblarini qo‘llash orqali administrator endi muammolarni tizimli va mantiqiy tarzda aniqlash va aniqlash uchun metodologiyani shakllantirishi va shu bilan tarmoq kompyuteringizdagi muammolarni eng yaxshi yechimiga erishishi mumkin

FOYDALANILGAN ADABIYOTLAR:

1. https://2ndsun.uz/index.php/yt/article/view/21/29

2. https://hozir.org/1--mavzu-kompyuter-kommunikasiyalari-kommunikasion-kanal-va-al.html

3. https://e-library.namdu.uz/telekommunikatsiya_uzatish_tizimlari.pdf

4. https://butunolam.nethouse.ru/static/doc/0000/0000/0344/344360.5yf0wk4bzs.pdf

5. https://arm.sies.uz/wp-content/uploads/2020/11/21-Axborot-tizimlari-2013-oquv-qollanma-R.X.Alimov-va-bosh.pdf

XAVFSIZLIK SOHASIDA NEYRON TARMOQLARDAN FOYDALANISH

S.M.To’xtasinova
Farg’ona ICHSHUI kasb-hunar maktabi
Maxsus fan o’qituvchisi

Annotatsiya: *Inson faoliyatining barcha sohalari va sohalarida innovatsion texnologiyalarni rivojlantirishning zamonaviy sharoitida yangi ilmiy yo'nalishlar paydo bo'ldi. Hozirgi zamon informatikasining istiqbolli yo’nalishlaridan biri neyroinformatikadir.*

Maqolada xavfsizlik sohasida neyron tarmoqlardan foydalanish xususiyatlari ko'rib chiqiladi.

Shuningdek, maqolada axborot xavfsizligiga eng dolzarb tahdidlar va shunga mos ravishda axborot xavfsizligini ta'minlash muammolarini hal qilishda sun'iy neyron tarmoqlardan foydalanishning asosiy yo'nalishlari haqida umumiy ma'lumot berilgan. Xavfsizlik sohasida neyron tarmoqlardan foydalanish sohada berilgan qo’shimcha imkoniyatlar to’g’risida ma’lumotlar keltirib o’tilgan.

Kalit so’zlar: *axborot xavfsizligi, neyron tarmoqlar, kriptografik usullar, Innovatsion texnologiyalar, sun'iy neyron tarmoqlar, xavfsizlik, xavfsizlik tizimlari, ob'ekt, neyron tarmoq, aniqlash, tasniflash, qo'riqlash signalizatsiya tizimi.*

Kompyuter tizimlari va tarmoqlarida axborotni muhofaza qilishi deganda, uzatilayotgan, saqlanayotgan va qayta ishlanilayotgan axborotni ishonchliligini tizimli tarzda ta’minlash maqsadida turli vosita va usullarni qo‘llash, choralarni ko‘rish va tadbirlarni amalga oshirishni tushunish qabul qilingan.

Davlatning axborot xavfsizligini ta’minlash muammosi milliy xavfsizlikni ta’minlashning asosiy va ajralmas qismi bo‘lib, axborotni muhofaza qilish esa davlatning birlamchi masalalariga, davlat siyosati darajasiga aylanmoqda.

Zamonaviy axborot texnologiyalarining taraqqiyoti sanoat shpionaji,kompyuter jinoyatchiligi, konfedensial ma’lumotlarga ruxsatsiz kirish,o‘zgartirish, yo‘qotish kabi salbiy hodisalar bilan birgalikda kuzatilmoqda.

Shuning uchun axborotni muhofaza qilish har qanday mamlakatda muhim davlat vazifasi hisoblanadi. O‘zbekistonda axborotni muhofaza qilishning zaruriyati axborotni muhofaza qilishning davlat tizimi yaratilishida va axborot xavfsizligining huquqiy bazasini rivojlantirishda o‘z ifodasini topmoqda. «Axborotlashtirish to‘g‘risida», «Davlat sirlarini saqlash to‘g‘risida», «Elektron hisoblash mashinalari dasturlari va ma’lumotlar bazalarini huquqiy himoya qilish to‘g‘risida» va boshqa qonunlar hamda bir qator Hukumat qarorlari qabul qilindi va amalga tatbiq etildi.

Axborot xavfsizligi deganda tabiiy yoki sun’iy xarakterdagi tasodifiy yoki