KOMPYUTER TARMOQLARIDA KIBERXAVFSIZLIK MUAMMOLARI

IBRAGIMOV SH.M.[1], BOQIJONOVA M.A.[2]

[1]*FarDU dotsenti, shavkat19702008@gmail.com*

[2]*FarDU talabasi, vahhobjonova05@gmail.com*

Annotatsiya: Ushbu maqolada zamonaviy kompyuter tarmoqlarida yuzaga kelayotgan kiberxavfsizlik muammolari, ularning kelib chiqish sabablari hamda ularni bartaraf etish usullari tahlil qilingan. Tarmoq arxitekturalari, SDN texnologiyalari va virtual tarmoqlar misolida xavfsizlikka ta'sir etuvchi omillar ko'rib chiqilgan. Shuningdek, zamonaviy himoya mexanizmlari zero-trust modeli, microsegmentation va shifrlash texnologiyalarining ahamiyati yoritilgan.

Kalit so'zlar: Kiberxavfsizlik, kompyuter tarmoqlari, SDN, zero-trust, microsegmentation, DDoS, tarmoq hujumlari, autentifikatsiya, shifrlash

KIRISH. Hozirgi kunda axborot-kommunikatsiya texnologiyalarining jadal rivojlanishi natijasida kompyuter tarmoqlari jamiyatning barcha sohalarida muhim o'rin egallab bormoqda. Internet tarmoqlarining kengayishi, raqamli iqtisodiyotning shakllanishi va axborot almashinuvining ortishi natijasida turli tizimlar o'zaro bog'langan holda faoliyat yuritmoqda. Shu sababli kompyuter tarmoqlarining ishonchliligi va xavfsizligini ta'minlash dolzarb masalalardan biriga aylandi.

Kompyuter tarmoqlari orqali uzatilayotgan ma'lumotlar hajmi kundan-kunga ortib bormoqda. Ushbu ma'lumotlar tarkibiga shaxsiy ma'lumotlar, moliyaviy operatsiyalar, tijorat sirlariga oid axborotlar va davlat ahamiyatiga ega ma'lumotlar kiradi. Mazkur ma'lumotlarning himoyasizligi yoki yetarli darajada muhofaza qilinmasligi turli xil kiberhujumlar va noqonuniy harakatlarga olib kelishi mumkin. Zamonaviy kompyuter tarmoqlari murakkab tuzilishga ega bo'lib, ular serverlar, marshrutizatorlar, kommutatorlar va boshqa tarmoq qurilmalaridan tashkil topgan. Bundan tashqari, bulutli texnologiyalar, virtual tarmoqlar va dasturiy boshqariladigan tarmoqlar kabi yangi texnologiyalar keng qo'llanilmoqda. Bu esa tarmoqlarning

samaradorligini oshirgan bo‘lsa-da, xavfsizlik nuqtai nazaridan yangi muammolarni ham yuzaga keltirmoqda.

Kiberxavfsizlik bugungi kunda nafaqat texnik, balki iqtisodiy va ijtimoiy ahamiyatga ega bo‘lgan global muammo hisoblanadi. Turli xil kiberhujumlar, jumladan, DDoS hujumlar, zararli dasturlar, fishing hujumlari va ruxsatsiz kirish holatlari soni ortib bormoqda. Ushbu tahdidlar nafaqat alohida foydalanuvchilarga, balki yirik tashkilotlar va davlat infratuzilmalariga ham katta zarar yetkazishi mumkin.

Bundan tashqari, inson omili ham kiberxavfsizlikka sezilarli darajada ta’sir ko‘rsatadi. Ko‘plab xavfsizlik muammolari foydalanuvchilarning ehtiyotsizligi, kuchsiz parollardan foydalanish yoki noto‘g‘ri sozlamalar natijasida yuzaga keladi. Shu sababli zamonaviy kiberxavfsizlik tizimlari nafaqat texnik himoya vositalarini, balki foydalanuvchilarni o‘qitish va xavfsizlik madaniyatini shakllantirishni ham o‘z ichiga oladi.

Shu nuqtai nazardan, kompyuter tarmoqlarida kiberxavfsizlik muammolarini o‘rganish, ularni tahlil qilish va samarali yechimlar ishlab chiqish muhim ilmiy va amaliy ahamiyatga ega. Ushbu ishning asosiy maqsadi kompyuter tarmoqlarida uchraydigan kiberxavfsizlik muammolarini o‘rganish va ularni bartaraf etish yo‘llarini tahlil qilishdan iborat.

Kompyuter tarmoqlarida kiberxavfsizlik tahdidlari

Kompyuter tarmoqlarida kiberxavfsizlik muammolari asosan turli xil tahdidlar va hujumlar natijasida yuzaga keladi. Ushbu tahdidlar tarmoq orqali uzatilayotgan ma’lumotlarning maxfiyligi, yaxlitligi va mavjudligiga zarar yetkazishi mumkin.

Eng keng tarqalgan tahdidlardan biri DDoS (Distributed Denial of Service) hujumlaridir. Bunda hujumchi tarmoqqa juda katta hajmda so‘rovlar yuborib, server yoki tizimni ishdan chiqarishga harakat qiladi. Natijada xizmatlardan foydalanish vaqtincha yoki to‘liq to‘xtab qoladi.

Yana bir muhim tahdid zararli dasturlar (malware) hisoblanadi. Ular viruslar, troyanlar, qurtlar (worms) va ransomware ko‘rinishida bo‘lishi mumkin. Bunday dasturlar tizimga kirib, ma’lumotlarni o‘g‘irlash, buzish yoki bloklab qo‘yish orqali

katta zarar yetkazadi. Ayniqsa ransomware hujumlarida foydalanuvchi ma’lumotlari shifrlanib, ularni tiklash uchun to‘lov talab qilinadi. Fishing (phishing) hujumlari ham keng tarqalgan bo‘lib, bunda foydalanuvchilar aldov yo‘li bilan maxfiy ma’lumotlarini (login, parol, karta ma’lumotlari) oshkor qilib qo‘yishadi. Bu hujumlar ko‘pincha soxta saytlar yoki elektron pochta orqali amalga oshiriladi.

Ruxsatsiz kirish (unauthorized access) ham jiddiy muammolardan biridir. Bu holatda hujumchi tizimga noqonuniy ravishda kirib, ma’lumotlarni o‘zgartirishi, o‘chirishi yoki o‘g‘irlashi mumkin. Bunga ko‘pincha zaif parollar, noto‘g‘ri sozlangan tizimlar yoki xavfsizlikdagi kamchiliklar sabab bo‘ladi.

Bundan tashqari, ichki tahdidlar (insider threats) ham mavjud bo‘lib, ular tashkilot ichidagi xodimlar tomonidan yuzaga keladi. Ba’zan xodimlar ataylab yoki bilmasdan xavfsizlik qoidalarini buzib, muhim ma’lumotlarning sizib chiqishiga sabab bo‘lishadi.

Yuqoridagi tahdidlarning ko‘pligi va murakkablashuvi kompyuter tarmoqlarida kiberxavfsizlikni ta’minlashni yanada dolzarb va murakkab vazifaga aylantirmoqda.

Tarmoq arxitekturasi va xavfsizlik muammolari

Kompyuter tarmoqlarining arxitekturasi ularning ishlash samaradorligi bilan bir qatorda xavfsizlik darajasiga ham bevosita ta’sir ko‘rsatadi. Noto‘g‘ri tanlangan yoki yetarli darajada himoyalanmagan tarmoq arxitekturasi turli xil kiberhujumlar uchun qulay sharoit yaratadi.

An’anaviy 3-qatlamli (core, distribution, access) arxitektura uzoq vaqt davomida keng qo‘llanilgan bo‘lib, u boshqaruvni soddalashtiradi va kichik hamda o‘rta tarmoqlar uchun samarali hisoblanadi. Biroq katta hajmdagi zamonaviy tarmoqlarda bu arxitektura ayrim kamchiliklarga ega. Masalan, trafik markazlashgan nuqtalardan o‘tishi sababli ortiqcha yuklanish yuzaga keladi va bu esa hujumlar uchun qulay imkoniyat yaratadi. Bundan tashqari, ayrim qurilmalar ishdan chiqsa, butun tarmoq faoliyati izdan chiqishi mumkin.

Zamonaviy tarmoqlarda qo‘llanilayotgan spine-leaf arxitekturasi esa yuqori tezlik va barqarorlikni ta’minlaydi. Bu arxitekturada barcha qurilmalar o‘zaro bog‘langan bo‘lib, trafik bir nechta yo‘llar orqali uzatiladi. Bu esa tarmoqning uzluksiz

ishlashiga yordam beradi. Lekin noto‘g‘ri sozlash yoki xavfsizlik siyosatining yetarli darajada yo‘lga qo‘yilmaganligi ushbu tizimda ham zaifliklarga olib kelishi mumkin.

Virtual tarmoqlar (VLAN, VXLAN) va bulutli infratuzilmalar keng qo‘llanilishi natijasida tarmoq chegaralari aniq bo‘lmay qolmoqda. Bu esa hujumchilar uchun yashirin ravishda tarmoq ichida harakatlanish (lateral movement) imkoniyatini oshiradi. Agar tarmoq to‘g‘ri segmentlarga ajratilmagan bo‘lsa, bitta zaif nuqta orqali butun tizim xavf ostida qolishi mumkin.

Shuningdek, zamonaviy tarmoqlarda dasturiy boshqaruv (SDN) texnologiyalarining joriy etilishi boshqaruvni yengillashtiradi, lekin markazlashgan boshqaruv nuqtasi mavjudligi sababli xavfsizlikka yangi tahdidlarni keltirib chiqaradi. Agar markaziy boshqaruv tizimi buzilsa, butun tarmoq ustidan nazorat yo‘qolishi mumkin.

Shu sababli tarmoq arxitekturasini loyihalashda xavfsizlik masalalarini birinchi o‘ringa qo‘yish zarur. Har bir qatlamda himoya mexanizmlarini joriy etish, tarmoqni segmentlarga ajratish va doimiy monitoring olib borish orqali kiberxavfsizlik darajasini oshirish mumkin.

SDN va zamonaviy texnologiyalarda xavfsizlik

Zamonaviy kompyuter tarmoqlarida dasturiy boshqariladigan tarmoqlar (SDN Software-Defined Networking) keng qo‘llanilmoqda. Ushbu texnologiya tarmoqni markazlashgan holda boshqarish imkonini berib, konfiguratsiya va nazorat jarayonlarini ancha soddalashtiradi. SDN da boshqaruv tekisligi (control plane) va ma’lumot uzatish tekisligi (data plane) ajratilgan bo‘lib, bu tarmoqni moslashuvchan va avtomatlashtirilgan tarzda boshqarish imkonini yaratadi.

SDN texnologiyasining asosiy afzalliklaridan biri xavfsizlik siyosatlarini markazlashgan holda boshqarish imkoniyatidir. Administratorlar butun tarmoq bo‘yicha yagona siyosat o‘rnatishi, trafikni kuzatishi va tezkor choralar ko‘rishi mumkin. Bu esa hujumlarni erta aniqlash va ularning oldini olishda muhim rol o‘ynaydi.

Biroq SDN texnologiyasi bilan bog‘liq ayrim xavfsizlik muammolari ham mavjud. Eng asosiy muammo markaziy boshqaruv qurilmasi (SDN controller) hisoblanadi. Agar ushbu qurilma hujumga uchrasa yoki ishdan chiqsa, butun tarmoq faoliyati izdan chiqishi mumkin. Shu sababli SDN tizimlarida yuqori darajadagi himoya va zaxira mexanizmlarini joriy etish talab etiladi.

Bulutli texnologiyalar (cloud computing) ham zamonaviy tarmoqlarning ajralmas qismiga aylangan. Bulutli muhitda ma’lumotlar masofaviy serverlarda saqlanadi va internet orqali boshqariladi. Bu esa qulaylik yaratishi bilan birga, ma’lumotlar xavfsizligiga tahdidlarni ham oshiradi. Ma’lumotlarning uchinchi tomon serverlarida saqlanishi ularning maxfiyligi va yaxlitligiga bo‘lgan xavfni kuchaytiradi.

Internet of Things (IoT) qurilmalarining keng tarqalishi ham kiberxavfsizlikka yangi muammolarni olib keldi. Ko‘plab IoT qurilmalari oddiy himoya mexanizmlariga ega bo‘lib, ular orqali hujumchilar tarmoqqa kirib olishlari mumkin. Bunday qurilmalar sonining ko‘pligi ularni nazorat qilishni qiyinlashtiradi.

Shuningdek, sun’iy intellekt va avtomatlashtirish texnologiyalarining rivojlanishi kiberhujumlarning yanada murakkablashishiga olib kelmoqda. Hujumchilar ham AI texnologiyalaridan foydalanib, aniq va samarali hujumlarni amalga oshirishlari mumkin. Shu sababli himoya tizimlari ham zamonaviy texnologiyalar asosida takomillashtirilishi zarur.

Umuman olganda, SDN, bulutli texnologiyalar va IoT tizimlari kompyuter tarmoqlarining imkoniyatlarini kengaytiradi, lekin ular bilan birga yangi xavfsizlik muammolarini ham yuzaga keltiradi. Shu bois ushbu texnologiyalarni joriy etishda xavfsizlik choralariga alohida e’tibor qaratish muhim hisoblanadi.

Zamonaviy himoya usullari

Kompyuter tarmoqlarida kiberxavfsizlikni ta’minlash uchun turli zamonaviy himoya usullari va texnologiyalar qo‘llaniladi. Ushbu usullar tarmoqdagi ma’lumotlarni himoyalash, hujumlarning oldini olish va tizim barqarorligini ta’minlashga xizmat qiladi.

Eng samarali usullardan biri tarmoqni segmentlarga ajratish (microsegmentation) hisoblanadi. Bu usulda tarmoq kichik, mustaqil qismlarga bo‘linadi va har bir segment alohida nazorat qilinadi. Natijada, agar bir segmentda xavfsizlik buzilishi yuz bersa, u boshqa qismlarga tarqalib ketmaydi. Bu usul ayniqsa yirik korporativ tarmoqlarda muhim ahamiyatga ega.

Zero-Trust xavfsizlik modeli ham zamonaviy yondashuvlardan biri bo‘lib, “ishonma, har doim tekshir” tamoyiliga asoslanadi. Ushbu modelda har bir foydalanuvchi va qurilma, hatto ular ichki tarmoqda bo‘lsa ham, doimiy ravishda autentifikatsiya va avtorizatsiyadan o‘tkaziladi. Bu esa ruxsatsiz kirish ehtimolini sezilarli darajada kamaytiradi.

Shifrlash (encryption) texnologiyalari ham muhim himoya vositasi hisoblanadi. Ma’lumotlar tarmoq orqali uzatilayotganda maxsus algoritmlar yordamida shifrlanadi, bu esa ularni uchinchi shaxslar tomonidan o‘qib olishni deyarli imkonsiz qiladi. Ayniqsa, HTTPS, VPN va boshqa xavfsiz protokollardan foydalanish ma’lumotlar xavfsizligini oshiradi.

Tarmoq xavfsizligini ta’minlashda xavfsizlik devorlari (firewall) va hujumlarni aniqlash tizimlari (IDS/IPS) ham muhim rol o‘ynaydi. Firewall tarmoqqa kiruvchi va chiquvchi trafikni nazorat qiladi, IDS/IPS tizimlari esa shubhali faoliyatni aniqlab, hujumlarning oldini olishga yordam beradi.

Bundan tashqari, muntazam monitoring va audit ishlari ham xavfsizlikni ta’minlashda muhim ahamiyatga ega. Tarmoq faoliyatini doimiy kuzatib borish orqali ehtimoliy tahdidlarni oldindan aniqlash va tezkor choralar ko‘rish mumkin bo‘ladi.

Foydalanuvchilarni o‘qitish va xavfsizlik madaniyatini shakllantirish ham muhim omil hisoblanadi. Chunki ko‘plab kiberhujumlar aynan inson omili sababli yuzaga keladi. Kuchli parollardan foydalanish, shubhali havolalarga kirmaslik va xavfsizlik qoidalariga rioya qilish orqali ko‘plab muammolarning oldini olish mumkin. Umuman olganda, zamonaviy himoya usullari kompleks tarzda qo‘llanilgandagina samarali natija beradi. Ya’ni, texnik vositalar, dasturiy yechimlar va inson omilini hisobga olgan holda integratsiyalashgan xavfsizlik tizimini yaratish zarur.

XULOSA

Kompyuter tarmoqlarida kiberxavfsizlikni ta’minlash bugungi kunda eng dolzarb masalalardan biri hisoblanadi. Axborot texnologiyalarining jadal rivojlanishi, internet tarmoqlarining kengayishi va ma’lumotlar hajmining ortib borishi natijasida turli xil kiberxavfsizlik tahdidlari ham ko‘payib bormoqda. Shu sababli tarmoqlarda xavfsizlikni ta’minlash kompleks yondashuvni talab qiladi.

Tahlillar shuni ko‘rsatadiki, kompyuter tarmoqlarida yuzaga keladigan asosiy muammolar DDoS hujumlar, zararli dasturlar, fishing hujumlari, ruxsatsiz kirish va ichki tahdidlar bilan bog‘liq. Bundan tashqari, zamonaviy texnologiyalar SDN, bulutli hisoblash va IoT tizimlarining joriy etilishi tarmoq imkoniyatlarini kengaytirgani holda, xavfsizlik nuqtai nazaridan yangi muammolarni ham yuzaga keltirmoqda.

Tarmoq arxitekturasi ham kiberxavfsizlik darajasiga sezilarli ta’sir ko‘rsatadi. Noto‘g‘ri loyihalangan yoki yetarli darajada himoyalanmagan tarmoqlar hujumlar uchun zaif bo‘ladi. Shu sababli tarmoqni loyihalash jarayonida xavfsizlik talablarini inobatga olish muhim hisoblanadi.

Zamonaviy himoya usullari microsegmentation, zero-trust modeli, shifrlash texnologiyalari, firewall va IDS/IPS tizimlari kiberxavfsizlikni ta’minlashda samarali vositalar hisoblanadi. Shu bilan birga, foydalanuvchilarni o‘qitish va xavfsizlik madaniyatini oshirish ham muhim ahamiyatga ega, chunki ko‘plab muammolar aynan inson omili bilan bog‘liq.

Xulosa qilib aytganda, kompyuter tarmoqlarida kiberxavfsizlikni ta’minlash uchun texnik, dasturiy va tashkiliy choralarni birgalikda qo‘llash zarur. Kelajakda esa sun’iy intellekt asosidagi himoya tizimlari, avtomatlashtirilgan monitoring va yangi avlod shifrlash texnologiyalari kiberxavfsizlikni yanada mustahkamlashda muhim rol o‘ynaydi.

FOYDALANILGAN ADABIYOTLAR

1. Stallings W. Network Security Essentials: Applications and Standards. – Pearson Education, 2017.

2. Kurose J., Ross K. Computer Networking: A Top-Down Approach. – Pearson, 2021.

3. Tanenbaum A., Wetherall D. Computer Networks. – Pearson, 2019.

Cisco Systems. Data Center Network Design Guide. – Cisco Press, 2021.

4. McKeown N. va boshqalar. OpenFlow: Enabling Innovation in Campus Networks. – ACM SIGCOMM, 2008.

5. Greenberg A. va boshqalar. The Cost of a Cloud: Research Problems in Data Center Networks. – ACM SIGCOMM, 2009.

6. Scarfone K., Mell P. Guide to Intrusion Detection and Prevention Systems (IDS/IPS). – NIST, 2007.

7. Behl A., Behl K. Cybersecurity and Cyberwar: What Everyone Needs to Know. – Oxford University Press, 2016.

8. Whitman M., Mattord H. Principles of Information Security. – Cengage Learning, 2018.