KOMPYUTER TARMOQLARI XAVFSIZLIGI: TAHDIDLAR, HIMOYA MEXANIZMLAR

Berdimurodov Mansur Alisherovich

O‘zXIA *Zamonaviy axborot-kommunikatsiya texnologiyalari kafedrasi katta o‘qituvchisi*

m.berdimurodov@iiau.uz

Xudoyqulov Kamoljon Toshpo‘latovich

Denov tadbirkorlik va pedagogika instituti “Axborot texnologiyalari” kafedrasi o‘qituvchisi

kamoljontoshpulatovich@gmail.com

Annotatsiya. Mazkur maqolada kompyuter tarmoqlari xavfsizligining nazariy va amaliy jihatlari tahlil qilinadi. Zamonaviy axborot tizimlarida tarmoq infratuzilmasi asosiy rol o‘ynashi sababli, unga qaratilgan tahdidlar va hujumlar ko‘lami tobora kengayib bormoqda. Maqolada tarmoq xavfsizligining asosiy tushunchalari, keng tarqalgan hujum turlari hamda ularni oldini olishda qo‘llaniladigan texnik va tashkiliy himoya mexanizmlari ko‘rib chiqiladi. Shuningdek, tarmoq xavfsizligini ta’minlashda zamonaviy yondashuvlar va ularning samaradorligi yoritiladi.

Kalit so‘zlar: kompyuter tarmoqlari, tarmoq xavfsizligi, kiberhujumlar, firewall, IDS/IPS, axborot xavfsizligi.

Kirish. Raqamli texnologiyalarning jadal rivojlanishi natijasida kompyuter tarmoqlari jamiyat hayotining barcha sohalariga chuqur kirib bordi. Internet, korporativ tarmoqlar va bulutli infratuzilmalar orqali katta hajmdagi ma’lumotlar uzatilishi axborot xavfsizligiga bo‘lgan talabni keskin oshirdi. Ayniqsa, tarmoqlar orqali amalga oshiriladigan kiberhujumlar nafaqat texnik, balki iqtisodiy va ijtimoiy xavflarni ham keltirib chiqarmoqda[1-5].

Shu sababli kompyuter tarmoqlari xavfsizligini ta’minlash bugungi kunda dolzarb ilmiy va amaliy masalalardan biri hisoblanadi. Ushbu maqolaning asosiy maqsadi tarmoq xavfsizligining fundamental tushunchalarini ochib berish, mavjud tahdidlarni tahlil qilish hamda samarali himoya usullarini ilmiy nuqtayi nazardan ko‘rib chiqishdan iborat[6,7].

Adabiyotlarni o‘rganish

Kompyuter tarmoqlari xavfsizligi masalalari bo‘yicha dastlabki ilmiy tadqiqotlar Internetning ommalashuvi bilan bog‘liq holda XX asr oxirlarida shakllandi. William Stallings, Andrew Tanenbaum, Ross Anderson kabi olimlar o‘z asarlarida tarmoq protokollari va ularning xavfsizlik muammolarini tizimli ravishda tahlil qilganlar. So‘nggi yillarda olib borilgan tadqiqotlarda DDoS hujumlari, tarmoq darajasidagi zaifliklar, shuningdek, IDS/IPS va firewall texnologiyalarining samaradorligi keng yoritilmoqda. Ilmiy adabiyotlar tarmoq xavfsizligini faqat texnik vositalar bilan emas, balki kompleks yondashuv — siyosat, monitoring va foydalanuvchi xabardorligini oshirish orqali ta’minlash zarurligini ko‘rsatadi.

Asosiy qism

Tarmoq xavfsizligiga tahdidlar turli shakllarda namoyon bo‘lishi mumkin. Eng keng tarqalgan hujumlarga quyidagilar kiradi:

DDoS (Distributed Denial of Service) hujumlari kompyuter tarmoqlari xavfsizligiga qaratilgan eng keng tarqalgan va xavfli tahdidlardan biri bo‘lib, ularning asosiy maqsadi tarmoq yoki server resurslarini haddan tashqari band qilish orqali qonuniy foydalanuvchilar uchun xizmatni vaqtincha yoki butunlay mavjud bo‘lmas holga keltirishdan iborat. Bunday hujumlar ko‘pincha botnet deb ataluvchi, zararli dasturlar bilan zararlangan minglab yoki millionlab qurilmalar yordamida amalga oshiriladi. DDoS hujumlari tarmoqning mavjudlik (availability) tamoyiliga bevosita tahdid soladi va ularning oqibatlari moliyaviy zarar, xizmatlarning uzilishi hamda tashkilot obro‘siga putur yetkazish bilan bog‘liq bo‘lishi mumkin[8].

Man-in-the-Middle (MITM) hujumlari aloqa qilayotgan ikki tomon — masalan, foydalanuvchi va server — o‘rtasiga hujumchining yashirincha joylashishi orqali amalga oshiriladi. Ushbu turdagi hujumlarda hujumchi uzatilayotgan ma’lumotlarni tinglash, nusxalash, o‘zgartirish yoki soxtalashtirish imkoniyatiga ega bo‘ladi. MITM hujumlari ayniqsa shifrlanmagan yoki zaif autentifikatsiya mexanizmlariga ega tarmoqlarda samarali bo‘lib, login-parollar, moliyaviy ma’lumotlar va shaxsiy axborotlarning oshkor bo‘lishiga olib kelishi mumkin. Natijada ma’lumotlarning maxfiyligi va yaxlitligi jiddiy xavf ostida qoladi.

ARP spoofing va DNS poisoning hujumlari tarmoq protokollarining ishonchga asoslangan ishlash mexanizmlaridan foydalanib amalga oshiriladigan soxtalashtirish hujumlari hisoblanadi. ARP spoofing jarayonida hujumchi o‘zini tarmoqdagi boshqa qurilma sifatida ko‘rsatib, trafikni o‘z nazorati ostiga oladi, bu esa MITM hujumlarini amalga oshirishga sharoit yaratadi. DNS poisoning esa domen nomlarini noto‘g‘ri IP manzillar bilan bog‘lash orqali foydalanuvchilarni soxta yoki zararli serverlarga yo‘naltiradi. Ushbu hujumlar foydalanuvchilarning ishonchini suiiste’mol qilishi va tarmoq infratuzilmasining yaxlitligiga jiddiy zarar yetkazishi bilan xavflidir[9,10].

Zararli dasturlar (malware) kompyuter tarmoqlari orqali tarqaluvchi va tizimlarning normal ishlashiga putur yetkazuvchi dasturiy tahdidlar majmuasini tashkil etadi. Ular viruslar, troyanlar, qurtlar (worms) va botnet komponentlari ko‘rinishida bo‘lib, foydalanuvchi xabarisiz tizimga kirib oladi. Zararli dasturlar tarmoq resurslaridan ruxsatsiz foydalanishi, maxfiy ma’lumotlarni o‘g‘irlashi, shuningdek, qurilmalarni DDoS hujumlari uchun botnet tarkibiga qo‘shishi mumkin. Bunday tahdidlar nafaqat alohida qurilmalar, balki butun tarmoq xavfsizligiga jiddiy xavf tug‘diradi.

Ushbu hujumlar tarmoqning mavjudligi, yaxlitligi va maxfiyligiga jiddiy xavf tug‘diradi.

Tarmoq xavfsizligini ta’minlash metodologiyasi. Tarmoq xavfsizligini ta’minlashda quyidagi asosiy himoya mexanizmlari qo‘llaniladi:

Firewall (tarmoqlararo himoya devori) tarmoq xavfsizligini ta’minlashning asosiy vositalaridan biri bo‘lib, u tarmoqlar o‘rtasida uzatilayotgan trafikni oldindan belgilangan xavfsizlik qoidalari asosida filtrlash vazifasini bajaradi. Firewall kiruvchi va chiquvchi paketlarni IP manzil, port raqami, protokol turi va sessiya holatiga qarab tahlil qilib, ruxsat etilgan trafikni o‘tkazadi va potentsial xavfli aloqalarni bloklaydi. Zamonaviy firewall tizimlari paket darajasida filtrlash bilan bir qatorda, ilova darajasida (application layer) tahlil qilish imkoniyatiga ega bo‘lib, tarmoqning tashqi hujumlardan himoyalanishida muhim rol o‘ynaydi[11].

IDS/IPS tizimlari (Intrusion Detection/Prevention Systems) tarmoqdagi shubhali faoliyat va hujumlarni aniqlash hamda ularning oldini olishga mo‘ljallangan maxsus xavfsizlik mexanizmlaridir. IDS tizimlari tarmoq trafikini doimiy monitoring qilib, ma’lum hujum signaturalari yoki anomaliyalar asosida xavfsizlik hodisalarini aniqlaydi va administratorni xabardor qiladi. IPS tizimlari esa aniqlangan hujumlarga faol tarzda javob berib, zararli trafikni avtomatik ravishda bloklaydi. Ushbu tizimlar tarmoq xavfsizligini kuchaytirishda firewall’ni to‘ldiruvchi muhim komponent hisoblanadi.

VPN (Virtual Private Network) texnologiyalari ochiq yoki ishonchsiz tarmoqlar orqali xavfsiz aloqa kanallarini yaratish imkonini beradi. VPN yordamida foydalanuvchi va tarmoq o‘rtasidagi ma’lumotlar maxsus shifrlangan tunnel orqali uzatiladi, bu esa ma’lumotlarni ruxsatsiz tinglash va o‘zgartirishdan himoya qiladi. VPN texnologiyalari masofaviy ishlash, filiallararo aloqa va mobil foydalanuvchilar xavfsizligini ta’minlashda keng qo‘llaniladi hamda tarmoq xavfsizligining muhim elementlaridan biri hisoblanadi.

Kriptografik protokollar (TLS va IPsec) tarmoq orqali uzatilayotgan ma’lumotlarning maxfiyligi, yaxlitligi va autentifikatsiyasini ta’minlashga

qaratilgan. TLS protokoli asosan veb-ilovalar va mijoz-server aloqalarida qo‘llanilib, ma’lumotlarni uzatish jarayonida shifrlash va tomonlarning haqiqiyligini tekshirishni amalga oshiradi. IPsec esa tarmoq darajasida ishlovchi protokol bo‘lib, IP paketlarini to‘liq yoki qisman shifrlash orqali himoyalaydi. Ushbu protokollar tarmoq xavfsizligini kriptografik asosda mustahkamlashda muhim rol o‘ynaydi[12].

Ushbu vositalar birgalikda qo‘llanilganda ko‘p qatlamli himoya tizimini hosil qiladi.

Natijalar va tahlil

Tahlillar shuni ko‘rsatadiki, faqat bitta himoya mexanizmi tarmoq xavfsizligini to‘liq ta’minlab bera olmaydi. Masalan, firewall trafikni cheklashi mumkin, biroq ichki tarmoqdagi hujumlarni aniqlashda IDS/IPS tizimlari muhim rol o‘ynaydi. Kompleks yondashuv asosida qurilgan tarmoq xavfsizlik arxitekturasi kiberhujumlar xavfini sezilarli darajada kamaytiradi.

Hujum turi	Hujum tavsifi (qisqacha)	Asosiy himoya texnologiyalari
DDoS (Distributed Denial of Service)	Server yoki tarmoq resurslarini haddan tashqari yuklash orqali xizmatni ishdan chiqarish	Firewall (rate limiting), IDS/IPS, Anti-DDoS tizimlari, Load Balancer
Man-in-the-Middle (MITM)	Aloqa jarayonida uchinchi tomon aralashuvi va ma’lumotlarni o‘g‘irlash	TLS/SSL, VPN, IPsec, sertifikatlar asosida autentifikatsiya
ARP spoofing	ARP jadvalini soxtalashtirib trafikni hujumchi tomon yo‘naltirish	Dynamic ARP Inspection (DAI), IDS/IPS, statik ARP yozuvlari
DNS poisoning	Soxta DNS yozuvlari orqali foydalanuvchini noto‘g‘ri serverga yo‘naltirish	DNSSEC, IDS/IPS, ishonchli DNS serverlar

Zararli dasturlar (Malware, Botnet)	Tarmoq orqali zararli kodlar tarqatish va boshqarish	IDS/IPS, Antivirus, Firewall, Network Monitoring
Brute-force hujumlari	Parol va autentifikatsiya mexanizmlarini kuch bilan buzish	Firewall, IDS/IPS, Multi-Factor Authentication (MFA)
Port scanning	Ochiq port va xizmatlarni aniqlash	Firewall, IDS/IPS, portlarni cheklash
Sniffing (Traffic listening)	Tarmoq trafikini yashirin tinglash	VPN, TLS, IPsec, shifrlangan protokollar
Insider attacks	Ichki foydalanuvchilar tomonidan amalga oshiriladigan hujumlar	Network Access Control (NAC), Monitoring, audit va loglar

Jadvaldan ko‘rinib turibdiki, tarmoq hujumlariga qarshi samarali himoya bitta texnologiya bilan emas, balki bir nechta himoya mexanizmlarini birgalikda qo‘llash orqali ta’minlanadi. Ayniqsa, firewall, IDS/IPS va kriptografik protokollar kombinatsiyasi tarmoq xavfsizligini sezilarli darajada oshiradi.

Xulosa

Kompyuter tarmoqlari xavfsizligi zamonaviy axborot jamiyatida strategik ahamiyatga ega bo‘lgan masala hisoblanadi. Ushbu maqolada tarmoq xavfsizligiga tahdid soluvchi asosiy hujumlar va ularni bartaraf etish usullari ilmiy jihatdan tahlil qilindi. O‘rganishlar shuni ko‘rsatadiki, tarmoq xavfsizligini ta’minlash texnik vositalar, kriptografik mexanizmlar va tashkiliy choralarni o‘z ichiga olgan kompleks yondashuvni talab etadi. Kelgusida sun’iy intellekt va avtomatlashtirilgan monitoring tizimlaridan foydalanish tarmoq xavfsizligini yanada yuqori bosqichga olib chiqishi mumkin.

Adabiyotlar ro‘yxati

1. Stallings W. *Network Security Essentials: Applications and Standards*. Pearson, 2020.

2. Tanenbaum A. S., Wetherall D. *Computer Networks*. Pearson, 2019.

3. Anderson R. *Security Engineering*. Wiley, 2020.

4. Scarfone K., Mell P. *Guide to Intrusion Detection and Prevention Systems*. NIST, 2018.

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

6. Urunbaev, E., Baizhumanov, A., and Berdimurodov, M., “Implementation of the algorithm for constructing a corrector of multivalued logic functions,” *Proceedings of the 2022 International Conference on Information Science and Communications Technologies (ICISCT)*, IEEE, 2022, pp. 1–5.

7. Berdimurodov, M., and Baizhumanov, A., “Algorithms for minimizing functions of the algebra of logic in the class of disjunctive normal forms and estimating their complexity,” *Proceedings of the 2022 International Conference on Information Science and Communications Technologies (ICISCT)*, IEEE, 2022, pp. 1–5.

8. Rakhimberdiev, K., Bozorov, A., and Berdimurodov, M., “Round Key Generation Algorithm Used in Symmetric Block Encryption Algorithms to Ensure the Security of Economic Systems,” *Proceedings of the 7th International Conference on Future Networks and Distributed Systems*, 2023, pp. 548–554.

9. Kabulov, A., Baizhumanov, A., Saymanov, I., and Berdimurodov, M., “Effective methods for solving systems of nonlinear equations of the algebra of logic based on disjunctions of complex conjunctions,” *Proceedings of the 2022 International Conference of Science and Information Technology in Smart Administration (ICSINTESA)*, IEEE, 2022, pp. 95–99.

10. Kabulov, A., Baizhumanov, A., Saymanov, I., and Berdimurodov, M., "Algorithms for minimizing disjunctions of complex conjunctions based on first-order neighborhood information for solving systems of Boolean equations," *Proceedings of the 2022 International Conference of Science and Information Technology in Smart Administration (ICSINTESA)*, IEEE, 2022, pp. 100–104.

11. Kabulov, A., Urunbaev, E., and Berdimurodov, M., "A logical method for finding maximum compatible subsystems of systems of Boolean equations," *Scientific Journal of Samarkand University*, vol. 2020, no. 3, pp. 27–37, 2020.

12. Kabulov, A. V., Berdimurodov, M. A., and Saymanov, I. M., "Logical Boolean function representation of cryptographic algorithm micro-operations (AES, ElGamal)," *Scientific Journal*, no. 3 (127/1), vol. 127, pp. 5–16, 2023