IQRO JURNALI , IQRO JOURNAL, ИКРО ЖУРНАЛИ
ISSN:2181-4341| wordlyknowledge.uz/index.php/iqro
Volume 20 Issue 01 April 2026

TARMOQ XAVFSIZLIGI MUAMMOLARI. XAVFSIZLIK USULLARI

Musayeva Muyassarxon O'rmonjanovna
Namangan viloyati Namangan shahar 1-sonli IMI
Informatika va axborot texnologiyalari fani o'qituvchisi
e-mail: muyassarmusayeva1985@gmail.com
+998930530685

Annotatsiya: Mazkur ilmiy maqolada tarmoq xavfsizligi sohasidagi asosiy muammolar, ularning kelib chiqish sabablari va zamonaviy axborot-kommunikatsiya tizimlarida yuzaga kelayotgan tahdidlar ilmiy manbalar asosida tahlil qilinadi. Shuningdek, kriptografik himoya usullari, autentifikatsiya mexanizmlari, tarmoqlararo ekranlar, IDS/IPS tizimlari hamda xavfsizlik siyosatlari kabi himoya vositalari o‘rganiladi. Maqolada tarmoq xavfsizligini ta’minlashda kompleks yondashuv zarurligi asoslab berilgan.

Kalit so‘zlar: tarmoq xavfsizligi, kiberxavfsizlik, kriptografiya, autentifikatsiya, IDS/IPS, xavfsizlik siyosati, zararli dasturlar, DDoS hujumlari.

Аннотация: В данной научной статье на основе научных источников анализируются основные проблемы в области сетевой безопасности, причины их возникновения, а также угрозы, возникающие в современных информационно-коммуникационных системах. Также рассматриваются методы криптографической защиты, механизмы аутентификации, межсетевые экраны, системы обнаружения и предотвращения вторжений (IDS/IPS), а также политики безопасности. В статье обосновывается необходимость комплексного подхода к обеспечению сетевой безопасности.

Ключевые слова: сетевая безопасность, кибербезопасность, криптография, аутентификация, IDS/IPS, политика безопасности, вредоносные программы, DDoS-атаки.

Annotation: This scientific article analyzes the main problems in the field of network security, their causes, and the threats emerging in modern information and communication systems based on scientific sources. It also examines cryptographic protection methods, authentication mechanisms, firewalls, intrusion detection and prevention systems (IDS/IPS), and security policies. The article substantiates the necessity of a comprehensive approach to ensuring network security.

Keywords: network security, cybersecurity, cryptography, authentication, IDS/IPS, security policy, malware, DDoS attacks.

Kirish

Axborot texnologiyalarining jadal rivojlanishi natijasida global tarmoqlar, ayniqsa Internet infratuzilmasi inson faoliyatining barcha sohalariga chuqur kirib bordi. Shu bilan birga, tarmoq xavfsizligi masalalari dolzarb muammolardan biriga aylandi. Statistik ma’lumotlarga ko‘ra, 2023-yilda dunyo bo‘yicha kiberhujumlar soni 38% ga oshgan [1, 12-bet]. Bu esa tarmoqlarda uzatilayotgan ma’lumotlarning maxfiyligi, yaxlitligi va mavjudligini ta’minlash zaruratini kuchaytirmoqda.

Tarmoq xavfsizligi — bu axborot resurslarini ruxsatsiz kirish, o‘zgartirish yoki yo‘q qilishdan himoya qilishga qaratilgan texnologiyalar, siyosatlar va amaliyotlar majmuasidir [2, 45-bet]. Zamonaviy tarmoqlar murakkab tuzilishga ega bo‘lib, ular turli xil tahdidlarga duch kelmoqda.

Metodologiya

Mazkur tadqiqotda ilmiy tahlil, solishtirma tahlil va tizimli yondashuv metodlaridan foydalanildi. Tarmoq xavfsizligi sohasidagi xalqaro ilmiy maqolalar, standartlar (ISO/IEC 27001), hamda amaliy tajribalar o‘rganildi. Shuningdek, turli xavfsizlik vositalarining samaradorligi ularning qo‘llanilish darajasi va real tahdidlar asosida baholandi.

Natijalar

Tadqiqot natijalari shuni ko‘rsatadiki, tarmoq xavfsizligidagi asosiy muammolar quyidagilardan iborat:

Birinchidan, zararli dasturlar (malware) keng tarqalgan bo‘lib, ular tizimlarga yashirin ravishda kirib, ma’lumotlarni o‘g‘irlash yoki tizimni ishdan chiqarishga xizmat qiladi. 2022-yilda ransomware hujumlari 13 soniyada bir marta sodir bo‘lgan [3, 78-bet].

Ikkinchidan, DDoS (Distributed Denial of Service) hujumlari serverlarni ortiqcha yuklab, xizmat ko‘rsatishni to‘xtatadi. 2023-yilda eng yirik DDoS hujumining hajmi 71 million so‘rov/sekundga yetgan [4, 21-bet].

Uchinchidan, inson omili — eng zaif bo‘g‘in sifatida qayd etiladi. Tadqiqotlarga ko‘ra, xavfsizlik buzilishlarining 82% i inson xatolari bilan bog‘liq [5, 34-bet].

Shuningdek, autentifikatsiya va parol siyosatining yetarli darajada kuchli emasligi ham tizimlarga noqonuniy kirishni osonlashtiradi.

Tahlil va muhokama

Tarmoq xavfsizligini ta’minlash bugungi kunda nafaqat texnik masala, balki strategik boshqaruv, iqtisodiy barqarorlik va milliy xavfsizlik bilan chambarchas bog‘liq kompleks muammoga aylangan. Zamonaviy tarmoqlar murakkablashib borayotgan sari ularga nisbatan tahdidlar ham ko‘payib, yanada takomillashgan shaklga ega bo‘lmoqda. Shu sababli, tarmoq xavfsizligini faqat bitta vosita yoki texnologiya orqali ta’minlash yetarli emas, balki ko‘p qatlamli (multi-layered) yondashuv talab etiladi.

Birinchi navbatda, kriptografik himoya tarmoq xavfsizligining asosiy tayanchlaridan biri hisoblanadi. Kriptografiya ma’lumotlarning maxfiyligini saqlash, ularning yaxlitligini ta’minlash va uzatish jarayonida uchinchi shaxslar tomonidan o‘zgartirilishining oldini olishga xizmat qiladi. Amaliyotda simmetrik va assimetrik shifrlash usullari keng qo‘llaniladi. Simmetrik algoritmlar tezkorligi bilan ajralib turadi, ammo kalitlarni xavfsiz uzatish muammosi mavjud. Assimetrik algoritmlar esa ochiq va yopiq kalitlardan foydalanib, yuqori darajadagi xavfsizlikni ta’minlaydi. AES algoritmining keng qo‘llanilishi uning yuqori darajadagi himoya imkoniyatlari va hisoblash samaradorligi bilan izohlanadi [6, 90-bet]. Shu bilan birga, RSA va ECC algoritmlari ham autentifikatsiya va kalit almashinuvida muhim rol o‘ynaydi.

Kriptografiyaning samaradorligi kalitlarni boshqarish tizimiga ham bog‘liq. Agar kalitlar noto‘g‘ri saqlansa yoki boshqarilsa, hatto eng kuchli shifrlash algoritmi ham samarasiz bo‘lishi mumkin. Shu sababli, kalitlarni boshqarish (Key Management System) alohida e’tibor talab etadi. Zamonaviy tizimlarda kalitlarni avtomatlashtirilgan tarzda yangilash va himoyalash mexanizmlari joriy etilmoqda.

Ikkinchi muhim yo‘nalish — autentifikatsiya va avtorizatsiya mexanizmlaridir. Oddiy parollar asosidagi tizimlar bugungi kunda yetarli darajada xavfsiz emasligi isbotlangan. Kuchli parol siyosati, biometrik autentifikatsiya va ko‘p faktorli autentifikatsiya tizimlari keng qo‘llanilmoqda. Ko‘p faktorli autentifikatsiya foydalanuvchining shaxsini tasdiqlashda bir nechta omildan foydalanadi: bilish (parol), egalik (telefon yoki token), va biometrik belgi (barmoq izi yoki yuz tanish). Tadqiqotlar shuni ko‘rsatadiki, MFA qo‘llanilishi hisoblarni buzish xavfini keskin kamaytiradi [7, 15-bet].

Shu bilan birga, autentifikatsiya tizimlarida Single Sign-On (SSO) texnologiyalari ham keng tarqalgan. Bu foydalanuvchilarga bir marta tizimga kirib, bir nechta xizmatlardan foydalanish imkonini beradi. Biroq, SSO tizimining buzilishi butun tizim xavfsizligiga tahdid solishi mumkin, shuning uchun uni qo‘shimcha himoya qatlamlari bilan mustahkamlash zarur.

Tarmoqlararo ekranlar (firewall) tarmoq xavfsizligining asosiy komponentlaridan biri hisoblanadi. Firewalllar tarmoq trafigini filtrlash orqali ruxsatsiz kirishni oldini oladi. Dastlabki firewalllar oddiy paket filtrlash asosida ishlagan bo‘lsa, zamonaviy firewalllar (Next Generation

Firewall — NGFW) ilovalar darajasida tahlil qilish, foydalanuvchi identifikatsiyasi va hatto zararli kodlarni aniqlash imkoniyatiga ega [8, 52-bet].

Firewall tizimlari to‘g‘ri sozlanmasa, ular samaradorligini yo‘qotadi. Masalan, noto‘g‘ri konfiguratsiya qilingan firewalllar ruxsatsiz trafikni o‘tkazib yuborishi yoki aksincha, foydali trafikni bloklashi mumkin. Shu sababli, firewall siyosatini muntazam ravishda yangilab borish va audit qilish zarur.

Intrusion Detection System (IDS) va Intrusion Prevention System (IPS) tizimlari tarmoqda sodir bo‘layotgan hodisalarni monitoring qilish orqali xavfli faoliyatni aniqlaydi. IDS tizimi faqat aniqlash bilan cheklansa, IPS tizimi aniqlangan tahdidlarni avtomatik tarzda bloklaydi. Zamonaviy IDS/IPS tizimlari signatura asosida ishlashdan tashqari, xulq-atvor (behavioral analysis) asosida ham tahdidlarni aniqlash imkoniyatiga ega [9, 66-bet].

Sun’iy intellekt va mashinaviy o‘rganish texnologiyalarining rivojlanishi IDS/IPS tizimlarining samaradorligini sezilarli darajada oshirdi. Ushbu tizimlar katta hajmdagi ma’lumotlarni tahlil qilib, oldindan noma’lum bo‘lgan tahdidlarni ham aniqlay oladi. Shu bilan birga, noto‘g‘ri pozitiv natijalar (false positives) muammosi ham mavjud bo‘lib, bu tizimlarning aniqligini oshirishni talab qiladi.

Tarmoq xavfsizligida inson omili alohida ahamiyatga ega. Statistik ma’lumotlarga ko‘ra, aksariyat xavfsizlik buzilishlari inson xatolari bilan bog‘liq [5, 34-bet]. Foydalanuvchilar tomonidan zaif parollardan foydalanish, phishing hujumlariga uchrash va xavfsizlik qoidalariga rioya qilmaslik keng tarqalgan muammolardandir. Shu sababli, tashkilotlarda xavfsizlik bo‘yicha muntazam treninglar o‘tkazish zarur [10, 101-bet].

Phishing hujumlari ayniqsa keng tarqalgan bo‘lib, foydalanuvchilarning shaxsiy ma’lumotlarini qo‘lga kiritishga qaratilgan. Zamonaviy phishing hujumlari juda murakkab bo‘lib, hatto tajribali foydalanuvchilarni ham chalg‘itishi mumkin. Shu sababli, texnik vositalar bilan bir qatorda foydalanuvchilarning xabardorligini oshirish ham muhim hisoblanadi.

Bulutli texnologiyalarning keng tarqalishi yangi xavfsizlik muammolarini yuzaga keltirdi. Bulutli muhitda ma’lumotlar markazlashgan serverlarda saqlanadi va internet orqali kirish imkoniyati mavjud bo‘ladi. Bu esa ma’lumotlarning xavfsizligini ta’minlashni murakkablashtiradi. Bulutli xizmat ko‘rsatuvchi provayderlar xavfsizlikni ta’minlash uchun turli mexanizmlarni joriy etgan bo‘lsa-da, foydalanuvchilar ham o‘z ma’lumotlari xavfsizligi uchun javobgardir.

Zero Trust modeli aynan shu muammolarni hal etishga qaratilgan. Ushbu modelga ko‘ra, tarmoq ichidagi hech bir foydalanuvchi yoki qurilmaga avtomatik ishonch berilmaydi. Har bir kirish so‘rovi alohida tekshiriladi va tasdiqlanadi [11, 39-bet]. Bu yondashuv ayniqsa masofaviy ishlash sharoitida samarali hisoblanadi.

Tarmoq xavfsizligida segmentatsiya ham muhim rol o‘ynaydi. Tarmoqni kichik segmentlarga bo‘lish orqali tahdidlar tarqalishini cheklash mumkin. Masalan, agar bitta segment buzilsa, qolgan segmentlar xavfsiz holatda qoladi. Bu usul ayniqsa korporativ tarmoqlarda keng qo‘llaniladi.

Shuningdek, tarmoq xavfsizligini ta’minlashda loglarni monitoring qilish va tahlil qilish muhim ahamiyatga ega. SIEM (Security Information and Event Management) tizimlari turli manbalardan kelayotgan loglarni yig‘ib, ularni tahlil qiladi va tahdidlarni aniqlaydi. Bu tizimlar real vaqt rejimida ishlaydi va tezkor choralar ko‘rish imkonini beradi.

Zamonaviy tahdidlar orasida Advanced Persistent Threat (APT) hujumlari alohida o‘rin tutadi. Bu hujumlar uzoq muddat davomida yashirin faoliyat olib borib, ma’lumotlarni sekin-asta o‘g‘irlashga qaratilgan. APT hujumlariga qarshi kurashish uchun kompleks himoya tizimlari va doimiy monitoring talab etiladi.

Shu bilan birga, IoT (Internet of Things) qurilmalarining ko‘payishi ham tarmoq xavfsizligiga yangi tahdidlarni keltirib chiqarmoqda. Ko‘plab IoT qurilmalari xavfsizlik

standartlariga to‘liq javob bermaydi, bu esa ularni kiberhujumlar uchun oson nishonga aylantiradi. Shu sababli, IoT qurilmalarini xavfsiz sozlash va yangilab borish muhim hisoblanadi.

Umuman olganda, tarmoq xavfsizligi ko‘p qirrali va doimiy rivojlanib borayotgan soha hisoblanadi. Har bir yangi texnologiya bilan birga yangi tahdidlar ham yuzaga keladi. Shu sababli, xavfsizlik strategiyasi ham doimiy ravishda yangilanib borilishi zarur. Kompleks yondashuv, zamonaviy texnologiyalar va foydalanuvchilar xabardorligini oshirish orqali tarmoq xavfsizligini yuqori darajada ta’minlash mumkin.

Xulosa

Tarmoq xavfsizligi zamonaviy axborot jamiyatining ajralmas qismi hisoblanadi. Tadqiqot natijalari shuni ko‘rsatadiki, xavfsizlik muammolari ko‘p qirrali bo‘lib, ularni hal etish kompleks yondashuvni talab qiladi. Kriptografiya, autentifikatsiya, IDS/IPS tizimlari, firewall va xavfsizlik siyosatlarini birgalikda qo‘llash yuqori darajadagi himoyani ta’minlaydi. Shuningdek, inson omilini kamaytirish uchun muntazam treninglar o‘tkazish zarur. Kelajakda sun’iy intellekt asosidagi xavfsizlik tizimlari yanada keng rivojlanishi kutilmoqda.

Foydalanilgan adabiyotlar ro‘yxati

[1] IBM Security. Cost of a Data Breach Report, 2023, 12-bet.
[2] Stallings W. Network Security Essentials, Pearson, 2017, 45-bet.
[3] Cybersecurity Ventures. Cybercrime Report, 2022, 78-bet.
[4] Cloudflare Inc. DDoS Attack Trends Report, 2023, 21-bet.
[5] Verizon. Data Breach Investigations Report, 2023, 34-bet.
[6] NIST. Advanced Encryption Standard (AES), 2001, 90-bet.
[7] Microsoft Security. Identity Security Report, 2022, 15-bet.
[8] Cheswick W., Bellovin S. Firewalls and Internet Security, Addison-Wesley, 2003, 52-bet.
[9] Scarfone K., Mell P. Guide to Intrusion Detection Systems, NIST, 2007, 66-bet.
[10] SANS Institute. Security Awareness Report, 2021, 101-bet.
[11] Kindervag J. Zero Trust Model, Forrester Research, 2010, 39-bet.
[12] ISO/IEC 27001 Standard, 2013, 27-bet.