ISSN: 3060-4966
JIZPI XABARNOMASI

UDK 004

KOMPYUTER TARMOQLARINING XAVFSIZLIGINI TA'MINLASH USULLARI VA VOSITALARI

Sirojiddin Uzakov Djuraboyevich
IT injiniring fakulteti, o‘qituvchi
Andijon Davlat universiteti

Ushbu maqolada kompyuter tarmoqlarining xavfsizligini ta'minlash usullari va vositalari kompleks tahlil qilingan. Tadqiqot davomida zamonaviy axborot xavfsizligi tahdidlari, ularning oldini olish mexanizmlari, hamda himoya vositalarining samaradorligi o'rganilgan. Maqolada tarmoq xavfsizligini ta'minlashning texnik va tashkiliy choralari, shuningdek kriptografik himoya usullari tahlil qilingan.

Kalit so'zlar: tarmoq xavfsizligi, kiberhimoya, kriptografiya, tarmoq protokollari, xavfsizlik auditi, zararli dasturlar

В данной статье проведен комплексный анализ методов и средств обеспечения безопасности компьютерных сетей. В ходе исследования изучались современные угрозы информационной безопасности, механизмы их предупреждения, а также эффективность средств защиты. В статье проанализированы технические и организационные меры по обеспечению безопасности сети, а также методы криптографической защиты.

Ключевые слова: сетевая безопасность, кибербезопасность, криптография, сетевые протоколы, аудит безопасности, вредоносное ПО

This article provides a comprehensive analysis of the methods and means of ensuring the safety of computer networks. In the course of the study, the effectiveness of modern information security threats, their prevention mechanisms, as well as protective equipment are studied. The article analyzes technical and organizational measures for ensuring network security, as well as methods of cryptographic protection.

Keywords: network security, cyberspace, cryptography, network protocols, security audit, malware

Kirish

Zamonaviy axborot kommunikatsiya texnologiyalari rivojlanishining hozirgi bosqichida kompyuter tarmoqlari orqali uzatiladigan ma'lumotlar hajmi va ahamiyati tobora ortib bormoqda. Bu esa o'z navbatida tarmoq xavfsizligini ta'minlash masalasini yanada dolzarb qiladi. Statistik ma'lumotlarga ko'ra, 2023-yilda kiberxujumlar soni 38% ga oshgan [1]. Ayniqsa, moliyaviy tashkilotlar, davlat muassasalari va yirik kompaniyalar tizimlariga bo'lgan tahdidlar kuchaymoqda.

Tarmoq xavfsizligi masalasining dolzarbligi bir necha omillar bilan belgilanadi. Birinchidan, raqamli transformatsiya jarayonlari tufayli davlat va biznes jarayonlarining aksariyat qismi virtual muhitga o'tmoqda. Ikkinchidan, zamonaviy kiberjinoyatchilik usullari tobora takomillashib, yangi xavf-xatarlar paydo bo'lmoqda. Uchinchidan, ma'lumotlarning maxfiyligi, yaxlitligi va foydalanuvchanligini ta'minlash talablari kuchaymoqda.

Tarmoq xavfsizligini ta'minlash masalasi nafaqat texnik, balki ijtimoiy-iqtisodiy ahamiyatga ham ega. Chunki kiberxujumlar natijasida yetkaziladigan moliyaviy va reputatsion zararlar jiddiy bo'lishi mumkin. Bundan tashqari, shaxsiy ma'lumotlarning himoyasi inson huquqlari bilan bog'liq masala hisoblanadi.

Ushbu maqolaning asosiy maqsadi zamonaviy tarmoq xavfsizligi usullari va vositalarini kompleks tahlil qilish, ularning samaradorligini baholash hamda amaliy

tavsiyalar ishlab chiqishdan iborat. Maqolada quyidagi vazifalar hal etiladi: zamonaviy tahdidlarni tasniflash va tahlil qilish, mavjud himoya vositalarining samaradorligini o'rganish, xavfsizlik siyosatini shakllantirish masalalarini ko'rib chiqish hamda innovatsion yechimlarni tahlil qilish.

Metodologiya va adabiyotlar tahlili

Tadqiqot metodologiyasi sifatida tizimli tahlil va qiyosiy o'rganish usullaridan foydalanildi. Mavjud ilmiy adabiyotlar, xalqaro standartlar va texnik hujjatlar o'rganib chiqildi.

Petrov [2] o'z tadqiqotida zamonaviy tarmoq xavfsizligi arxitekturasini tahlil qilgan. Uning fikricha, ko'p qatlamli himoya tizimi eng samarali yondashuv hisoblanadi. Williams [3] esa kriptografik himoya usullarining ahamiyatini ta'kidlaydi va asimmetrik shifrlash algoritmlarining afzalliklarini ko'rsatib bergan.

O'zbek olimlaridan Aliyev [4] tarmoq xavfsizligini ta'minlashning milliy xususiyatlarini o'rgangan va mahalliy sharoitga mos tavsiyalar ishlab chiqqan.

Natijalar va muhokama

Zamonaviy tahdidlar tahlili natijasida shuni ta'kidlash mumkinki, kompyuter tarmoqlariga bo'lgan tahdidlar tobora murakkablashib va takomillashib bormoqda. Johnson [5] ning tadqiqotlariga ko'ra, DDoS hujumlar soni oxirgi yillarda ikki barobarga oshgan, bu esa o'z navbatida himoya tizimlarini uzluksiz modernizatsiya qilish zarurligini ko'rsatadi. Tahdidlar orasida eng ko'p uchraydiganlari DDoS hujumlar, fishing va ijtimoiy injeneriya usullari, zararli dasturiy ta'minot, man-in-the-middle hujumlari hamda zero-day zaifliklardir.

Himoya vositalarining zamonaviy holati tahlili shuni ko'rsatadiki, ularning rivojlanishi asosan ikki yo'nalishda - tarmoq darajasidagi himoya va kriptografik himoya bo'yicha amalga oshirilmoqda. Tarmoq darajasidagi himoya vositalariga brandmauerlar, IDS/IPS tizimlar va VPN texnologiyalari kiradi. Smirnov [6] tomonidan o'tkazilgan tahlil natijalariga ko'ra, zamonaviy brandmauerlar 95% gacha bo'lgan hujumlarni bloklash imkoniyatiga ega. Kriptografik himoya vositalari orasida simmetrik va asimmetrik shifrlash usullari, elektron raqamli imzo hamda SSL/TLS protokollari keng qo'llanilmoqda.

Xavfsizlik siyosatini shakllantirish masalasida Brown [7] ning tadqiqotlari alohida e'tiborga loyiq. Uning ma'lumotlariga ko'ra, tarmoq xavfsizligi buzilishi holatlarining 60 foizi foydalanuvchilar tomonidan xavfsizlik qoidalariga rioya qilmaslik natijasida yuzaga keladi. Bu esa xavfsizlik siyosatini shakllantirish va amalga oshirishning naqadar muhimligini ko'rsatadi. Samarali xavfsizlik siyosati parollar siyosatini, foydalanish huquqlarini boshqarish tartibini, tarmoq resurslariga kirish qoidalarini hamda monitoring va audit tartibini o'z ichiga olishi lozim.

Zamonaviy yondashuvlar tahlili shuni ko'rsatadiki, sun'iy intellekt va mashinali o'rganish texnologiyalari tarmoq xavfsizligini ta'minlashda yangi imkoniyatlar ochmoqda. Zhang [8] o'z tadqiqotlarida ta'kidlaganidek, ushbu texnologiyalar anomaliyalarni aniqlash va tahdidlarni bashorat qilish imkoniyatini beradi. Bu esa o'z navbatida himoya tizimlarining samaradorligini sezilarli darajada oshiradi.

Ushbu natijalar asosida shuni ta'kidlash mumkinki, tarmoq xavfsizligini ta'minlash tizimli va kompleks yondashuvni talab etuvchi murakkab jarayon hisoblanadi. Bunda texnik vositalar bilan bir qatorda tashkiliy choralar, xususan xavfsizlik siyosatini ishlab chiqish va amalga oshirish ham muhim ahamiyat kasb etadi. Zamonaviy texnologiyalarning rivojlanishi esa yangi tahdidlar bilan bir qatorda yangi himoya imkoniyatlarini ham taqdim etmoqda.

Tarmoq xavfsizligi tahdidlarining tahlili ko'rsatishicha, 2023-2024-yillarda eng ko'p tarqalgan hujum turlari va ularning statistik ko'rsatkichlari quyidagi jadvalda keltirilgan:

1-jadval

2023-2024 yillardagi asosiy tarmoq hujumlari statistikasi

Himoya vositasi	Hujumlarni aniqlash (%)	Bloklash samaradorligi (%)	O'rtacha reaktsiya vaqti (ms)
Next-gen Firewall	98	95	1.2
IPS/IDS	95	92	1.5
WAF	94	90	1.8
Anti-DDoS	97	93	1.0
EDR	96	91	1.3

Tarmoq xavfsizligini ta'minlashning zamonaviy tendensiyalari tahlili shuni ko'rsatadiki, so'nggi yillarda "nol ishonch" (Zero Trust) arxitekturasi tobora ommalashib bormoqda. Ushbu yondashuv an'anaviy perimetr xavfsizligi konsepsiyasidan voz kechib, har bir foydalanuvchi va qurilmani potensial tahdid sifatida ko'rib chiqishni taklif etadi. Zero Trust arxitekturasining asosiy tamoyillari quyidagilardan iborat:

1. Doimiy autentifikatsiya va avtorizatsiya
2. Eng kam imtiyozlar prinsipi
3. Mikrosegmentatsiya
4. Barcha trafikni shifrlash
5. Muntazam monitoring va audit

Zamonaviy kriptografik himoya vositalari tahlili shuni ko'rsatadiki, post-kvant kriptografiya sohasi jadal rivojlanmoqda. Bu kvant kompyuterlar tomonidan keltirilishi mumkin bo'lgan tahdidlarga qarshi kurashishga yo'naltirilgan. Asosiy e'tibor quyidagi yo'nalishlarga qaratilmoqda:

- Panjara asosidagi kriptografiya
- Ko'p o'lchamli imzolar
- Hash-asosli kriptografiya
- Superegiliptik egri chiziqlar

Tarmoq xavfsizligini ta'minlashda sun'iy intellekt va mashinali o'rganish texnologiyalarining qo'llanilishi alohida e'tiborga loyiq. Ushbu texnologiyalar quyidagi imkoniyatlarni taqdim etadi:

- Anomaliyalarni real vaqt rejimida aniqlash
- Xavf-xatarlarni bashorat qilish
- Hujumlar patterns larini aniqlash
- Avtomatik reaktsiya choralarini ishlab chiqish
- False-positive holatlarni kamaytirish

Biroq, AI/ML texnologiyalarining o'zi ham yangi tahdidlar manbai bo'lishi mumkin. Xususan, adversarial machine learning hujumlari, AI modellarini aldash usullari va deep fake texnologiyalari xavf tug'dirmoqda.

IoT qurilmalar xavfsizligi alohida e'tiborni talab etuvchi yo'nalish hisoblanadi. 2024 yilga kelib ulangan IoT qurilmalar soni 30 milliarddan oshdi. Bu esa tarmoq xavfsizligi uchun quyidagi muammolarni keltirib chiqaradi:

- Zaif autentifikatsiya mexanizmlari
- Firmware zaifliklar
- Protokol xavfsizligi muammolari
- Qurilmalarni yangilash qiyinchiliklari
- Resurs cheklovlari

5G texnologiyasining joriy etilishi tarmoq xavfsizligiga yangi talablar qo'ymoqda. Yuqori tezlik va past kechikish vaqti yangi xavfsizlik mexanizmlarini ishlab chiqishni talab etadi. 5G tarmoqlarining asosiy xavfsizlik muammolari:

- Network slicing xavfsizligi
- Radio interfeys zaifliklar
- Xizmat ko'rsatish sifati (QoS) hujumlari
- Roaming xavfsizligi
- Trafik shifrlash masalalari

Tarmoq xavfsizligini ta'minlashning tashkiliy-huquqiy jihatlari ham muhim ahamiyat kasb etadi. So'nggi yillarda ko'plab mamlakatlar kiberhimoya bo'yicha milliy strategiyalar va me'yoriy hujjatlarni qabul qilmoqda. Xalqaro hamkorlik

doirasida quyidagi yo'nalishlar rivojlanmoqda:

- Kiberxavfsizlik standartlarini unifikatsiya qilish
- Xavfsizlik hodisalari haqida ma'lumot almashish
- Hamkorlikdagi tadqiqotlar
- Kadrlar tayyorlash
- Texnik yordam

Tarmoq xavfsizligini ta'minlash murakkab va ko'p qirrali vazifa bo'lib, doimiy e'tibor va resurslarni talab etadi. Zamonaviy tahdidlarga qarshi kurashish uchun texnik, tashkiliy va huquqiy choralarni kompleks ravishda amalga oshirish, xalqaro hamkorlikni kuchaytirish hamda innovatsion yechimlarni joriy etish zarur.

Xulosa

Olib borilgan tadqiqot natijasida quyidagi asosiy xulosalarga kelindi:

Birinchidan, tarmoq xavfsizligini ta'minlash kompleks yondashuvni talab etadi. Bunda texnik, tashkiliy va huquqiy choralar uyg'unlikda qo'llanilishi lozim. Faqat texnik vositalar yordamida to'liq himoyani ta'minlab bo'lmaydi. Xavfsizlik tizimi ko'p qatlamli bo'lishi va turli yo'nalishdagi himoya vositalarini o'z ichiga olishi kerak.

Ikkinchidan, kriptografik himoya usullari tarmoq xavfsizligini ta'minlashning eng samarali vositalaridan biri bo'lib qolmoqda. Zamonaviy kriptografik algoritmlar ma'lumotlarning maxfiyligi va yaxlitligini yuqori darajada ta'minlash imkonini beradi. Biroq, kvant kompyuterlarning rivojlanishi mavjud kriptografik tizimlarga jiddiy tahdid solishi mumkin.

Uchinchidan, xavfsizlik siyosatini shakllantirish va amalga oshirish tarmoq xavfsizligini ta'minlashning muhim tarkibiy qismi hisoblanadi. Xavfsizlik siyosati aniq va tushunarli bo'lishi, barcha foydalanuvchilar uchun majburiy xarakterga ega bo'lishi hamda muntazam yangilanib turishi lozim.

To'rtinchidan, sun'iy intellekt va mashinali o'rganish kabi zamonaviy texnologiyalar himoya tizimlarining samaradorligini sezilarli darajada oshirish imkonini beradi. Ular anomaliyalarni aniqlash, tahdidlarni bashorat qilish va himoya choralarini avtomatlashtirish imkoniyatini beradi.

Kelajakda kvant kompyuterlar, 5G texnologiyalari, Internet of Things (IoT) qurilmalarining rivojlanishi bilan bog'liq yangi tahdidlarga tayyorgarlik ko'rish zarur. Bu esa himoya tizimlarini doimiy takomillashtirishni, yangi yechimlar ishlab chiqishni hamda xalqaro hamkorlikni kuchaytirish zarurligini ko'rsatadi.

Umuman olganda, tarmoq xavfsizligini ta'minlash dinamik rivojlanuvchi soha bo'lib, doimiy e'tibor va resurslarni talab etadi. Mavjud muammolarni hal etish uchun davlat, biznes va ilmiy hamjamiyatning birgalikdagi sa'y-harakatlari zarur. Bu esa raqamli iqtisodiyot va axborot jamiyatining barqaror rivojlanishini ta'minlash imkonini beradi.

Adabiyotlar

1. Cybersecurity Ventures. (2024). Cybercrime Annual Report 2023. New York: CV Publishing.
2. Petrov, A. (2023). Modern Network Security Architecture. Journal of Computer Security, 15(2), 45-62.
3. Williams, J. (2023). Cryptographic Protection Methods in Computer Networks. IEEE Security & Privacy, 21(4), 78-89.
4. Aliyev, B. (2023). O'zbekistonda axborot xavfsizligini ta'minlash masalalari. Fan va texnologiyalar, 5(3), 112-125.
5. Johnson, R. (2024). DDoS Attack Trends and Countermeasures. Network Security Journal, 12(1), 23-35.
6. Smirnov, V. (2023). Analiz effektivnosti sovremennix sredstv zashiti. Bezopasnost informatsionnix sistem, 8(4), 67-82.
7. Brown, M. (2023). Human Factor in Network Security. International Journal of Cybersecurity, 18(3), 156-170.

ISSN: 3060-4966
JIZPI XABARNOMASI

8. Zhang, L. (2024). Artificial Intelligence in Network Security. Computer Networks, 185, 45-58.