TARMOQLAR VA KIBERXAVFSIZLIK

Sobirjonova Marjona Latif qizi
Axborot texnologiyalari va menejment universiteti
Raqamli texnalogiyalar fakulteti

Anotatsiya. *Mazkur maqolada kompyuter tarmoqlari va ularning asosiy tuzilmalari, shuningdek, kiberxavfsizlik tushunchalari va usullari tahlil qilinadi. Maqolada tarmoqlarda ma’lumot almashishning asosiy protokollari, xavfsizlik choralarining samaradorligi va zamonaviy himoya texnologiyalari haqida ma’lumot beriladi. Kiberxavfsizlikning ahamiyati, tarmoq hujumlari turlari va ularga qarshi kurash usullari muhokama qilinib, bugungi kunning dolzarb muammolari va ularni hal etish yo‘llari ko‘rib chiqiladi. Ushbu ish axborot xavfsizligini ta’minlash va tizimli tarmoqlarni himoya qilish sohasidagi ilg‘or yondashuvlarni o‘rganishga qaratilgan.*

Kalit so‘zlar: *kompyuter tarmoqlari, kiberxavfsizlik, ma’lumotlarni shifrlash, firewall, autentifikatsiya, zararli dasturlar, tarmoq protokollari, axborot xavfsizligi, sun’iy intellekt, bulutli xavfsizlik*

Аннотация. *В данной статье анализируются компьютерные сети и их основные структуры, а также понятия и методы кибербезопасности. В статье рассматриваются основные протоколы обмена данными в сетях, эффективность мер безопасности и современные технологии защиты. Обсуждается важность кибербезопасности, виды сетевых атак и способы борьбы с ними, а также актуальные проблемы современности и пути их решения. Работа направлена на изучение передовых подходов в обеспечении информационной безопасности и защите системных сетей.*

Ключевые слова: *омпьютерные сети, кибербезопасность, шифрование данных, межсетевой экран (firewall), аутентификация, вредоносные программы, сетевые протоколы, информационная безопасность, искусственный интеллект, облачная безопасность.*

Abstract. *This article analyzes computer networks and their fundamental structures, as well as the concepts and methods of cybersecurity. It provides information on the main protocols for data exchange in networks, the effectiveness of security measures, and modern protection technologies. The importance of cybersecurity, types of network attacks, and countermeasures are discussed, along with current pressing issues and ways to address them. This work is aimed at exploring advanced approaches to ensuring information security and protecting systemic networks.*

Keywords: *computer networks, cybersecurity, data encryption, firewall, authentication, malware, network protocols, information security, artificial intelligence, cloud security.*

Kirish

Zamonaviy axborot jamiyatida kompyuter tarmoqlari va ularning xavfsizligi muhim o‘rin tutadi. Kompyuter tarmoqlari orqali butun dunyo bo‘ylab ma’lumotlar tez va samarali almashiladi, biznes jarayonlari avtomatlashtiriladi, davlat boshqaruvi va ijtimoiy hayot faoliyatlari qo‘llab-quvvatlanadi. Shu bilan birga, tarmoqlar orqali uzatiladigan axborotning sir saqlanishi, yaxlitligi va mavjudligi ta’minlanishi axborot xavfsizligi sohasining dolzarb masalalaridan biridir. Axborot tizimlari va tarmoqlarga qarshi kiber hujumlarning ko‘payishi xavfsizlik choralarining doimiy ravishda takomillashtirilishini talab qiladi. Kiberxavfsizlik — bu axborot resurslarini ruxsatsiz kirish, buzish, o‘g‘irlash yoki zarar yetkazilishidan himoya qilish tizimi bo‘lib, zamonaviy texnologiyalar rivojlangan sayin uning ahamiyati yanada oshib bormoqda. Kiberxavfsizlik nafaqat yirik korporatsiyalar, davlat organlari uchun, balki har bir foydalanuvchi uchun ham muhim ahamiyatga ega, chunki har qanday tizim va foydalanuvchi kiber tahdidlar ostida bo‘lishi mumkin.

Kompyuter tarmoqlari va ularning xavfsizligi bilan bog‘liq asosiy tushunchalar, himoya usullari va protokollarni chuqur o‘rganish zamonaviy axborot texnologiyalari sohasida mutaxassislikni shakllantirishda asosiy bosqichlardan biri hisoblanadi. Shuningdek, zamonaviy kiberxavfsizlik yechimlari — ma’lumotlarni shifrlash, firewall, autentifikatsiya, zararli dasturlarga qarshi kurash vositalari kabi texnologiyalar kiberxavfsizlik sohasida samarali himoyani ta’minlash imkonini beradi. Ushbu maqola kompyuter tarmoqlari va kiberxavfsizlikning nazariy va amaliy jihatlarini tahlil qilish, zamonaviy xavfsizlik texnologiyalari va ularning samaradorligini ko‘rsatishga qaratilgan bo‘lib, axborot xavfsizligini ta’minlashdagi yangi yondashuvlarni o‘rganishga xizmat qiladi.

Kompyuter tarmoqlari — bu ikki yoki undan ortiq kompyuterlar va boshqa qurilmalar o‘rtasida ma’lumot almashish imkonini beruvchi tizimlar bo‘lib, ular turli o‘lcham va shakllarda bo‘lishi mumkin. Tarmoqlar mahalliy (LAN), keng (WAN), metropolitan (MAN) va global (Internet) tarmoqlarga bo‘linadi. Har bir tarmoq turi o‘ziga xos arxitektura va ishlash tamoyillariga ega bo‘lib, ma’lumotlar almashinuvi uchun maxsus protokollar, masalan, TCP/IP, HTTP, FTP kabi standartlar qo‘llaniladi. Ushbu protokollar ma’lumotlarning tarmoqlar bo‘ylab to‘g‘ri va xavfsiz yetkazilishini ta’minlaydi.

Kiberxavfsizlik esa axborot tizimlari va tarmoqlarni turli tahdidlardan, jumladan, zararli dasturlar, xakerlik hujumlari, phishing, DDoS (Distributed Denial of Service) kabi tarmoq hujumlaridan himoya qilishga qaratilgan faoliyatdir. Kiberxavfsizlik sohasida quyidagi asosiy komponentlar mavjud:

1. **Ma’lumotlarni shifrlash** — ma’lumotlarni kodlash orqali ularni ruxsatsiz o‘qilishdan himoya qilish usuli. Simmetrik va assimmetrik shifrlash algoritmlari keng qo‘llaniladi, masalan, AES, RSA.
2. **Firewall** — tarmoqqa kiruvchi va chiquvchi trafikni nazorat qiluvchi tizim bo‘lib, zararli trafikni bloklaydi va ruxsat berilgan trafikni o‘tkazadi. Bu qurilmalar dasturiy yoki apparat asosida bo‘lishi mumkin.
3. **Autentifikatsiya va avtorizatsiya** — foydalanuvchini yoki qurilmani aniqlash va ularga ma’lumotlarga kirish huquqini berish jarayoni. Bu usullar parollar, biometrik ma’lumotlar, ikki faktorli autentifikatsiya orqali amalga oshiriladi.
4. **Zararlangan dasturlar (malware) bilan kurashish** — antivirus va anti-malware dasturlari tizimni viruslar, troyanlar, ransomware va boshqa zararli kodlardan himoya qiladi.
5. **Tarmoq monitoringi va tahdidlarni aniqlash** — tarmoqlarni doimiy kuzatish orqali g‘ayrioddiy faoliyatlarni aniqlash va unga qarshi tezkor choralar ko‘rish.

Bugungi kunda kiberxavfsizlik sohasida sun’iy intellekt va mashinani o‘rganish texnologiyalari keng qo‘llanilmoqda. AI yordamida tahdidlarni oldindan aniqlash, xavfsizlik tizimlarini avtomatik yangilash va murakkab hujumlarga qarshi samarali javob qaytarish imkoniyati paydo bo‘ldi.

Shuningdek, bulutli hisoblash texnologiyalarining keng tarqalishi bilan bulutli xavfsizlik muhim ahamiyat kasb etmoqda. Bulutda saqlanayotgan ma’lumotlarni himoya qilish uchun maxsus himoya choralari va standartlar ishlab chiqilgan. Blokcheyn texnologiyasi esa ma’lumotlarning yaxlitligi va xavfsiz tranzaksiyalarni amalga oshirishda muhim vosita hisoblanadi. Tarmoqlar va kiberxavfsizlik sohasidagi zamonaviy texnologiyalar va usullar har doim yangilanib, murakkablashib boradi. Shu sababli mutaxassislar doimiy ravishda o‘z bilimlarini yangilab borishlari va yangi tahdidlarga qarshi samarali choralarni ishlab chiqishlari zarur. Kiberxavfsizlikning jahon bozorida talab ortib borayotgani ham bu sohaning ahamiyatini yanada oshirmoqda. Zamonaviy kompyuter tarmoqlari nafaqat an’anaviy qurilmalarni, balki IoT (Internet of Things — narsalar interneti) qurilmalarini ham o‘z ichiga oladi. IoT tarmoqlari kundalik hayotda aqlli uy tizimlari, sog‘liqni saqlash, sanoat avtomatizatsiyasi kabi sohalarda keng qo‘llanilmoqda. Biroq, IoT qurilmalarining ko‘pligi va ular orasidagi xavfsizlik standartlarining pastligi kiberxavfsizlik uchun yangi tahdidlarni yuzaga keltiradi. Shu sababli IoT tarmoqlarini himoya qilish uchun maxsus xavfsizlik protokollari va autentifikatsiya mexanizmlari ishlab chiqilmoqda.

Kiberxavfsizlikda shuningdek, **ransomware** (so‘rovchi dasturlar) hujumlari bugungi kunning eng xavfli tahdidlaridan biri hisoblanadi. Bu turdagi zararli dasturlar tizimdagi ma’lumotlarni shifrlab qo‘yadi va uni qayta tiklash uchun pul talab qiladi. Ransomware hujumlariga qarshi kurashishda muntazam zahira nusxalarini yaratish va

tizimlarni yangilab borish muhim ahamiyatga ega. Yana bir muhim yo‘nalish — **insider tahdidlar**. Ko‘pincha kiberxavfsizlik buzilishlari tashkilot ichidan, xodimlar yoki ichki foydalanuvchilar tomonidan yuz beradi. Shu sababli, faqat tashqi tahdidlar emas, balki ichki xavflarga qarshi ham qattiq nazorat va monitoring o‘rnatish zarur. Shuningdek, **tarmoq segmentatsiyasi** xavfsizlikni oshirish uchun qo‘llaniladigan samarali usul hisoblanadi. Bu usul tarmoqni kichikroq bo‘laklarga ajratib, har bir segment uchun alohida xavfsizlik qoidalarini joriy etishni ta’minlaydi. Bu hujumlarning tarqalishini cheklashga yordam beradi. So‘nggi yillarda **sun’iy intellekt (AI)** va **mashinani o‘rganish (ML)** texnologiyalari kiberxavfsizlik tizimlarida keng qo‘llanmoqda. AI yordamida tahdidlarni aniqlash va oldini olish jarayoni avtomatlashtiriladi, bu esa tezkor va samarali javob qaytarish imkonini beradi. Bunga misol sifatida tahdidlarni aniqlash tizimlari (Intrusion Detection Systems — IDS) va tahdidlarni oldini olish tizimlari (Intrusion Prevention Systems — IPS) keltirilishi mumkin.

Kiberxavfsizlikda **blokcheyn** texnologiyasi ham yangi imkoniyatlar ochmoqda. Uning yordamida ma’lumotlarning yaxlitligi va ishonchliligi kafolatlanadi, tranzaksiyalarni monitoring qilish va ma’lumotlarni maxfiy saqlash tizimlari takomillashadi.

Shuningdek, zamonaviy kiberxavfsizlik yondashuvlarida **Zero Trust Architecture (ZTA)** kontseptsiyasi muhim ahamiyat kasb etmoqda. Zero Trust tamoyili “hech kimga ishonma, har doim tekshir” prinsipiga asoslanadi va har bir foydalanuvchi, qurilma va tarmoq aloqasi doimiy ravishda tekshiriladi, bu esa xavfsizlikni sezilarli darajada oshiradi. Bugungi kunda tarmoqlar va kiberxavfsizlik doimiy ravishda yangi tahdidlarga duch kelmoqda, shuning uchun mutaxassislar uchun doimiy o‘qish, texnologiyalarni kuzatib borish va yangi xavfsizlik protokollarini ishlab chiqish juda muhimdir.

Xulosa

Bugungi kunda kompyuter tarmoqlari jamiyatning barcha sohalarida muhim infratuzilma hisoblanadi. Tarmoqlarning rivojlanishi axborot almashinuvini tezlashtirgan bo‘lsa-da, shu bilan birga xavfsizlik muammolarini ham keltirib chiqarmoqda. Kiberxavfsizlik — bu tarmoqlar va ma’lumotlarni turli tahdidlardan himoya qilishning zamonaviy va samarali vositasi bo‘lib, har bir tashkilot va foydalanuvchi uchun ustuvor ahamiyatga ega. Ma’lumotlarni shifrlash, autentifikatsiya, firewall va zararli dasturlarga qarshi choralar kabi texnologiyalar tarmoqlarni himoya qilishda muhim rol o‘ynaydi. Shuningdek, IoT, bulutli hisoblash, sun’iy intellekt va blokcheyn kabi yangi texnologiyalar kiberxavfsizlik sohasida yangi imkoniyatlar va muammolarni yuzaga chiqaradi. Zero Trust modeli kabi ilg‘or yondashuvlar esa xavfsizlikni yanada mustahkamlashga xizmat qiladi. Kiberxavfsizlik doimo rivojlanib borayotgan soha bo‘lib, zamonaviy tahdidlarga qarshi samarali kurashish uchun doimiy monitoring, yangilanish va mutaxassislarning malakasini oshirib borish talab

etiladi. Natijada, kompyuter tarmoqlari va kiberxavfsizlikni chuqur o‘rganish, yangi texnologiyalarni qo‘llash va xavfsizlikni ta’minlash uchun kompleks yondashuvlarni ishlab chiqish bugungi kunning asosiy vazifalaridan biridir.

Adabiyotlar ro‘yxati

1. Stallings W. Computer Networking with Internet Protocols and Technology. Pearson, 2021.
2. Kurose J., Ross K. Computer Networking: A Top-Down Approach. Pearson, 2020.
3. Schneier B. Applied Cryptography: Protocols, Algorithms, and Source Code in C. Wiley, 2015.
4. Anderson R. Security Engineering: A Guide to Building Dependable Distributed Systems. Wiley, 2020.
5. Whitman M., Mattord H. Principles of Information Security. Cengage Learning, 2021.
6. Mitnick K., Simon W. The Art of Deception: Controlling the Human Element of Security. Wiley, 2017.
7. Rouse M. What is Cybersecurity? TechTarget, 2023. https://www.techtarget.com/searchsecurity/definition/cybersecurity
8. Goodchild M. Introduction to IoT Security. Springer, 2022.
9. Zissis D., Lekkas D. "Addressing Cloud Computing Security Issues." Future Generation Computer Systems, 2012.
10. NIST. Zero Trust Architecture. National Institute of Standards and Technology, Special Publication 800-207, 2020.