ZAMONAVIY IQTISODIYOT VA INTELLEKTUAL TEXNOLOGIYALAR
Ilmiy-uslubiy elektron jurnali — Sharq universiteti
ISSN: 3093-9062 Vol. 1 No. 1 (2026)

KOMPYUTER TARMOQLARI XAVFSIZLIGI: ASOSIY TAHDIDLAR VA ULARDAN HIMOYA USULLARI

Mardiyeva Mohinur Hikmatulla qizi,
JDPU Aniq fanlar fakulteti, Kompyuter injiniring yo'nalishi,
I bosqich 121-25-guruh talabasi
DOI: https://doi.org/10.66493/rwy0xz33

Annotatsiya: Ushbu maqolada zamonaviy kompyuter tarmoqlarida uchraydigan asosiy xavf-xatarlar, kiberhujumlarning keng tarqalgan turlari hamda ulardan himoyalanishning samarali usullari tahlil qilingan. Raqamli texnologiyalarning jadal rivojlanishi bilan birga tarmoq xavfsizligiga bo'lgan tahdidlar ham ortib bormoqda, bu esa nafaqat yirik tashkilotlarni, balki oddiy foydalanuvchilarni ham xavf ostiga qo'ymoqda. Maqolada DDoS, MITM, fishing, troyan dasturlar va ransomware kabi keng tarqalgan hujum turlarining mohiyati va ta'sir mexanizmlari yoritilgan. Shuningdek, tarmoqni himoya qilishning asosiy vositalari — shifrlash texnologiyalari (AES, RSA, ECC), ikki bosqichli autentifikatsiya, firewall va IDS/IPS tizimlari, zaxiralash mexanizmlari hamda xavfsizlik siyosati batafsil ko'rib chiqilgan. Tarmoq xavfsizligi bugungi raqamli davrda har bir tashkilot va foydalanuvchi uchun muhim ahamiyat kasb etishi sababli, maqolada bu masalalar sodda va tushunarli tilda bayon etilgan. Mazkur ish kompyuter injiniringi yo'nalishida tahsil olayotgan talabalar uchun ham nazariy, ham amaliy jihatdan foydali bo'lishi ko'zda tutilgan bo'lib, xavfsizlik sohasida chuqur bilim shakllantirishga xizmat qiladi.

Аннотация: В данной статье анализируются основные риски, характерные для современных компьютерных сетей, широко распространённые виды кибератак, а также эффективные методы защиты от них. Стремительное развитие цифровых технологий сопровождается ростом угроз сетевой безопасности, что подвергает риску не только крупные организации, но и обычных пользователей. В статье раскрыты сущность и механизмы воздействия таких распространённых атак, как

© Sharq universiteti, 2026

ISSN: 3093-9062 Vol. 1 No. 1 (2026)

DDoS, MITM, фишинг, троянские программы и программы-вымогатели (ransomware). Также подробно рассмотрены основные средства защиты сети — технологии шифрования (AES, RSA, ECC), двухфакторная аутентификация, системы firewall и IDS/IPS, механизмы резервного копирования и политика безопасности. Поскольку в современную цифровую эпоху сетевая безопасность имеет важное значение для каждой организации и пользователя, данные вопросы изложены простым и понятным языком. Настоящая работа предназначена для студентов направления компьютерной инженерии и может быть полезна как в теоретическом, так и в практическом плане, способствуя формированию глубоких знаний в области информационной безопасности.

Abstract: This article analyzes the main risks encountered in modern computer networks, widespread types of cyberattacks, and effective methods of protection against them. The rapid development of digital technologies has been accompanied by a growing number of threats to network security, putting not only large organizations but also ordinary users at risk. The article describes the nature and mechanisms of common attacks such as DDoS, MITM, phishing, Trojan programs, and ransomware. It also examines in detail the main protective tools, including encryption technologies (AES, RSA, ECC), two-factor authentication, firewall and IDS/IPS systems, backup mechanisms, and security policy. Since network security is of great importance for every organization and user in today's digital era, these issues are presented in simple and understandable language. This work is intended for students majoring in computer engineering and aims to be useful both theoretically and practically, contributing to a deeper understanding of information security.

Kalit so‘zlar: axborot xavfsizligi, kompyuter tarmoqlari, kiberhujum, autentifikatsiya, shifrlash, kriptografiya, MITM, DDoS, fishing, troyan dastur, ransomware, firewall, IDS/IPS, xavfsizlik siyosati, himoyalanish usullari.

Kirish

DOI: https://doi.org/10.66493/rwy0xz33
© Sharq universiteti, 2026

ISSN: 3093-9062 Vol. 1 No. 1 (2026)

Raqamli texnologiyalar keskin rivojlangan XXI asrda kompyuter tarmoqlari global kommunikatsiyaning asosi sifatida shakllandi. Tarmoqlarning keng miqyosda qo'llanilishi bilan birga, ularga tahdidlar ham jiddiy darajada ortdi. Bugungi kunda nafaqat yirik tashkilotlar, balki ta'lim muassasalari, kichik biznes subyektlari, hatto oddiy foydalanuvchilar ham kiberhujumlarning nishoniga aylanmoqda. Mutaxassislar fikriga ko'ra, dunyo bo'yicha har yili milliardlab dollarlik iqtisodiy zarar aynan tarmoq xavfsizligi buzilishi sababli yuzaga keladi. Shu sababli tarmoq xavfsizligini ta'minlash hozirgi zamon IT mutaxassisining eng muhim vazifalaridan biri hisoblanadi. Axborot xavfsizligining asosiy tamoyillari bo'lmish maxfiylik, yaxlitlik va mavjudlik (CIA modeli) tarmoq muhitida eng ko'p tahdid ostida bo'ladi. Tahdidlar nafaqat tashqi dushmanlar tomonidan, balki ichki xodimlar, noto'g'ri konfiguratsiyalar, dasturiy ta'minotdagi zaifliklar va texnik xatoliklar oqibatida ham yuzaga kelishi mumkin. Shu bois bu mavzuning chuqur o'rganilishi kompyuter injiniringi yo'nalishidagi talabalarning kelajakdagi kasbiy faoliyati uchun katta ahamiyat kasb etadi. Ushbu maqolaning maqsadi — kompyuter tarmoqlarida uchraydigan asosiy xavf-xatarlarni tizimlashtirish, keng tarqalgan kiberhujum turlarini tahlil qilish hamda ulardan himoyalanishning amaliy usullarini ko'rib chiqishdan iborat.

Adabiyotlar tahlili

Kompyuter tarmoqlarida tahdidlarning tabiati. Tarmoq xavfsizligiga tahdidlar asosan uch guruhga bo'linadi: texnik tahdidlar, dasturiy tahdidlar va inson omili bilan bog'liq tahdidlar. Texnik tahdidlar qatoriga tarmoq qurilmalarining ishdan chiqishi, kanallar shikastlanishi yoki elektr uzilishi kabi holatlar kiradi. Dasturiy tahdidlar esa zararli dasturlar, viruslar, troyanlar, eksploitlar va boshqa dasturiy kodlar orqali amalga oshiriladi. Eng xavflisi — inson omili bilan bog'liq xatoliklar bo'lib, statistikaga ko'ra, axborot xavfsizligi buzilishlarining 60 foizdan ortig'i aynan insonning beparvoligi yoki xatoliklari sababli sodir bo'ladi. Stallings tarmoq xavfsizligining nazariy asoslarini, Pfleeger axborot xavfsizligini boshqarish tamoyillarini, Kurose va Ross esa tarmoq

DOI: https://doi.org/10.66493/rwy0xz33
© Sharq universiteti, 2026

ISSN: 3093-9062 Vol. 1 No. 1 (2026)

protokollari darajasidagi zaifliklarni tahlil qilgan bo'lsa, Schneier kriptografik himoya usullarining amaliy ahamiyatini ko'rsatib bergan. Ushbu manbalarning umumiy xulosasi shundan iboratki, tarmoq xavfsizligi murakkab, ko'p qatlamli yondashuvni talab qiladigan soha hisoblanadi.

Tadqiqot metodologiyasi

Ushbu tadqiqotda tahliliy va tavsiflovchi tadqiqot metodlaridan foydalanilgan. Tadqiqot mavzusi bo'yicha mahalliy va xorijiy ilmiy adabiyotlar, jumladan tarmoq xavfsizligiga oid monografiyalar, ilmiy maqolalar hamda xalqaro standartlar (jumladan, ISO/IEC 27001:2022) o'rganildi. Ma'lumotlar manbai sifatida nashr etilgan ilmiy adabiyotlar, sohaga oid statistik ma'lumotlar va amaliy tajriba natijalaridan foydalanildi. Tadqiqot jarayonida kiberhujumlarning asosiy turlari tasniflandi, ularning ishlash mexanizmlari qiyosiy tahlil qilindi hamda mavjud himoya vositalarining samaradorlik darajasi baholandi. Bu esa olingan xulosalarning ilmiy va amaliy jihatdan asoslanganligini ta'minlaydi.

Tahlil va natijalar

Keng tarqalgan kiberhujumlarga quyidagilarni kiritishimiz mumkin. Zamonaviy tarmoq infratuzilmasi turli xil kiberhujumlarni boshdan kechirmoqda. Eng ko'p uchraydiganlari quyidagilar: DDoS hujumi — hujumchi server yoki tarmoqni ortiqcha so'rovlar bilan band qilib, ularning ishlashiga to'sqinlik qiladi. Natijada xizmatlar vaqtincha ishlamay qoladi. MITM (Man-in-the-Middle) — ikki foydalanuvchi o'rtasidagi aloqaga yashirincha aralashish orqali ma'lumotlarni o'zgartirish yoki o'g'irlashga yo'naltirilgan hujum turidir. Fishing hujumi — soxta saytlar va e-mail xabarlari orqali foydalanuvchining shaxsiy ma'lumotlarini qo'lga kiritish usuli. Troyan dasturlar — foydalanuvchiga foydali dasturdek ko'rinadi, ammo fon rejimida zararli amallarni bajaradi. Ransomware — shifrlovchi zararli dastur bo'lib, foydalanuvchi fayllarini bloklab, ularni ochish uchun pul talab qiladi.

DOI: https://doi.org/10.66493/rwy0xz33
© Sharq universiteti, 2026

ISSN: 3093-9062 Vol. 1 No. 1 (2026)

Bu hujumlarning har biri o'ziga xos xavf tug'diradi va tarmoqqa jiddiy zarar yetkazishi mumkin. Tarmoqlarni himoyalashning asosiy usullari quyidagilar: tarmoq xavfsizligida texnik vositalar, dasturiy ta'minot va tashkiliy choralar birgalikda qo'llangandagina natija samarali bo'ladi. Shifrlash texnologiyalari — ma'lumotlarni uzatishda ularni shifrlash eng samarali himoya usullaridan biri sanaladi. Bugungi kunda AES, RSA, ECC kabi algoritmlar keng qo'llanadi. Mutaxassislar fikricha, to'g'ri tashkil etilgan kriptografik himoya MITM hujumlarining 90 foizini oldini oladi. Autentifikatsiya va avtorizatsiya — ikki bosqichli autentifikatsiya, biometrik tekshiruv, xavfsiz parollar siyosati tarmoqqa kirishni cheklashda muhim rol o'ynaydi. Firewall va IDS/IPS tizimlari — tarmoqqa kiruvchi va chiquvchi trafikni nazorat qilishning asosiy vositasi bo'lib, IDS (Intrusion Detection System) va IPS (Intrusion Prevention System) tizimlari hujumlarni aniqlash va oldini olish imkonini beradi. Zaxiralash va tiklash tizimlari — zaxira nusxalari bo'lmasa, ransomware kabi hujumlar katta talofatlar keltirib chiqaradi, shuning uchun barcha tashkilotlarda muntazam ravishda avtomatik zaxiralash yo'lga qo'yilishi shart. Xavfsizlik siyosati va xodimlarni o'qitish — inson omili asosiy risk bo'lgani uchun xodimlarni doimiy ravishda o'qitish, parol siyosatini nazorat qilish, ichki qoidalarni ishlab chiqish tarmoq xavfsizligining muhim qismidir.

Xulosa va takliflar

Kompyuter tarmoqlari xavfsizligini ta'minlash — texnik imkoniyatlar, ilmiy yondashuv va inson omilini uyg'un boshqarish orqali amalga oshiriladigan murakkab jarayondir. Tahdidlar yildan-yilga o'zgarib bormoqda, shu bilan birga himoya vositalari ham takomillashmoqda. Maqolada qayd etilganidek, tarmoq xavfsizligi faqat dasturiy vositalarni o'rnatish bilangina emas, balki kompleks yondashuvni talab qiladi. Shifrlash texnologiyalari, kuchli autentifikatsiya, tarmoq monitoringi, zaxira tizimi, xavfsizlik siyosati va xodimlarning bilimi — bularning barchasi xavfsiz infratuzilmaning ajralmas tarkibiy qismidir. Shu asosda quyidagi tavsiyalarni berish mumkin:

DOI: https://doi.org/10.66493/rwy0xz33
© Sharq universiteti, 2026

ISSN: 3093-9062 Vol. 1 No. 1 (2026)

tashkilotlarda kriptografik himoya vositalarini muntazam yangilab borish, xodimlar uchun xavfsizlik bo'yicha davriy trening dasturlarini joriy etish, zaxiralash tizimlarini avtomatlashtirish hamda IDS/IPS tizimlarini tarmoq monitoringining ajralmas qismiga aylantirish maqsadga muvofiqdir. Kompyuter injiniringi yo'nalishidagi talabalar ushbu bilimlarni chuqur o'zlashtirsa, zamonaviy axborot xavfsizligi bo'yicha yuqori malakali mutaxassis bo'lib yetishishlari shubhasiz.

Foydalanilgan adabiyotlar

[1] Stallings, W. Network Security Essentials. Pearson Education, 2020.

[2] Pfleeger, C., Shari L. Security in Computing. Prentice Hall, 2019.

[3] Kurose, J., Ross, K. Computer Networking: A Top-Down Approach. Addison-Wesley, 2017.

[4] Schneier, B. Applied Cryptography. Wiley Publishing, 2016.

[5] Simmons, R. "DDoS Attack Methods and Mitigation Techniques." Journal of Cyber Defense, 2022.

[6] Anderson, R. Security Engineering. Wiley, 2020.

[7] Katz, J., Lindell, Y. Introduction to Modern Cryptography. CRC Press, 2018.

[8] Scarfone, K., Mell, P. "Guide to Intrusion Detection and Prevention Systems." NIST Publications, 2021.

[9] ISO/IEC 27001:2022. Axborot xavfsizligi boshqaruvi standartlari.

DOI: https://doi.org/10.66493/rwy0xz33
© Sharq universiteti, 2026