KOMPYUTER TARMOQLARIDA AXBOROT XAVFSIZLIGI MUAMMOLARI VA ULARNI BARTARAF ETISHNING ZAMONAVIY USULLARI

Ibragimov Sh.M.[1], Komilova M.T.[2]

[1]FarDU dotsenti, shavkat19702008@gmail.com

[2]FarDU talabasi, komilovamohlaroy99@gmail.com

Annotatsiya: *Ushbu maqolada kompyuter tarmoqlarida axborot xavfsizligini ta'minlashning dolzarb muammolari tahlil qilinadi. Zamonaviy axborot texnologiyalarining jadal rivojlanishi natijasida tarmoqlarda turli xil tahdidlar va xavfsizlik muammolari yuzaga kelmoqda. Maqolada ushbu muammolarning asosiy sabablari, ularning oqibatlari hamda ularni bartaraf etishning samarali usullari ko'rib chiqilgan. Shuningdek, axborot xavfsizligini ta'minlashda zamonaviy himoya vositalari va texnologiyalarining ahamiyati yoritilgan.*

Kalit so'zlar: *kompyuter tarmoqlari, axborot xavfsizligi, kiberxavfsizlik, tarmoq tahdidlari, ma'lumotlarni himoyalash, shifrlash, autentifikatsiya, firewall, zararli dasturlar, tarmoq himoyasi.*

KIRISH

Hozirgi kunda axborot-kommunikatsiya texnologiyalarining jadal rivojlanishi kompyuter tarmoqlarining jamiyat hayotidagi ahamiyatini yanada oshirmoqda. Kompyuter tarmoqlari orqali katta hajmdagi ma'lumotlar tezkor almashinuvi ta'minlanib, turli sohalarda samaradorlikni oshirishga xizmat qilmoqda. Shu bilan birga, tarmoqlarning kengayishi va ulardan foydalanish ko'lamining ortishi axborot xavfsizligi bilan bog'liq muammolarni ham keltirib chiqarmoqda.

Zamonaviy kompyuter tarmoqlarida turli xil tahdidlar, jumladan, zararli dasturlar, ruxsatsiz kirish, ma'lumotlarni o'g'irlash va buzish kabi holatlar tobora ko'payib bormoqda. Bu esa axborot resurslarini himoya qilish, ularning maxfiyligi, yaxlitligi va mavjudligini ta'minlashni muhim vazifa sifatida belgilaydi. Axborot

xavfsizligini ta’minlash nafaqat texnik, balki tashkiliy va huquqiy choralarni ham talab etadi.

Mazkur maqolaning maqsadi kompyuter tarmoqlarida axborot xavfsizligi bilan bog‘liq muammolarni tahlil qilish hamda ularni bartaraf etishning zamonaviy usullarini o‘rganishdan iborat. Shu asosda axborot xavfsizligini ta’minlash bo‘yicha samarali yechimlar ishlab chiqish va amaliy tavsiyalar berish ko‘zda tutiladi.

ADABIYOTLAR TAHLILI VA USULLAR

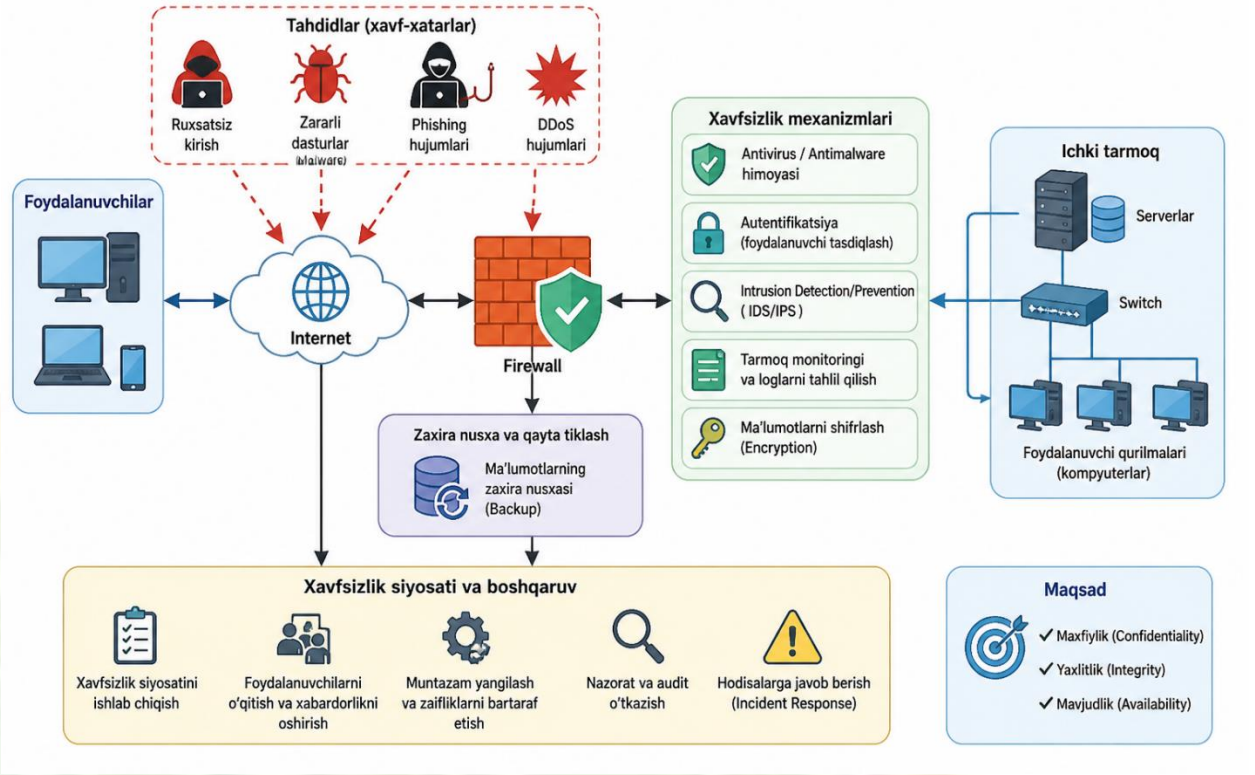
Kompyuter tarmoqlarida axborot xavfsizligini ta’minlash masalalari so‘nggi yillarda ilmiy tadqiqotlarning muhim yo‘nalishlaridan biriga aylangan. Ilmiy manbalarda qayd etilishicha, tarmoq xavfsizligi asosan ma’lumotlarning maxfiyligi, yaxlitligi va mavjudligini ta’minlashga qaratilgan kompleks choralar tizimi sifatida qaraladi. Tadqiqotlarda tarmoqlarda yuzaga keladigan asosiy tahdidlar sifatida zararli dasturlar (malware), xizmat ko‘rsatishni rad etish (DDoS) hujumlari, fishing (phishing) va ruxsatsiz kirish holatlari keng tahlil qilingan [1].

Bir qator ilmiy ishlarda axborot xavfsizligini ta’minlashda kriptografik usullarning ahamiyati alohida ta’kidlanadi. Xususan, ma’lumotlarni shifrlash, foydalanuvchilarni autentifikatsiya qilish va kirishni nazorat qilish mexanizmlaridan foydalanish tarmoq xavfsizligini oshirishning samarali vositalaridan biri sifatida e’tirof etiladi. Shuningdek, zamonaviy tadqiqotlarda tarmoqni himoyalashda firewall, antivirus dasturlari va kirishni aniqlash tizimlari (IDS/IPS) muhim rol o‘ynashi ko‘rsatib o‘tilgan [2].

Mazkur maqolada axborot xavfsizligi muammolarini o‘rganishda tahliliy, taqqoslash va umumlashtirish usullaridan foydalanildi. Mavzuga oid mavjud ilmiy adabiyotlar chuqur o‘rganilib, ulardagi nazariy qarashlar tahlil qilindi. Shuningdek, kompyuter tarmoqlarida uchraydigan asosiy xavfsizlik muammolari tizimli ravishda ajratib olinib, ularni bartaraf etishning zamonaviy usullari o‘zaro taqqoslash asosida baholandi.

MUHOKAMA

Kompyuter tarmoqlarida axborot xavfsizligini ta’minlash ko‘p darajali tizimni talab etadi. Ushbu tizimning asosiy elementlari va o‘zaro bog‘liqligi 1-rasmda keltirilgan.



1-rasm. Kompyuter tarmoqlarida axborot xavfsizligi tizimi

Kompyuter tarmoqlarida axborot xavfsizligini ta’minlash bugungi kunda dolzarb va murakkab masalalardan biri hisoblanadi. Tarmoqlarning kengayishi va ulardan foydalanish hajmining ortishi bilan xavfsizlikka tahdid soluvchi omillar ham murakkablashib bormoqda. Xususan, zararli dasturlar, DDoS hujumlari, phishing va ijtimoiy muhandislik kabi tahdidlar tarmoq infratuzilmasining zaif nuqtalaridan foydalanib, jiddiy zarar yetkazishi mumkin.

Tahlillar shuni ko‘rsatadiki, zamonaviy tashkilotlarda eng ko‘p uchraydigan muammolardan biri — xavfsizlikka kompleks yondashuvning yetishmasligidir. Masalan, ayrim hollarda foydalanuvchilar oddiy va oson topiladigan parollardan foydalanishi yoki shubhali elektron pochta xabarlariga e’tiborsiz munosabatda bo‘lishi natijasida tarmoqqa ruxsatsiz kirish holatlari yuzaga keladi. Phishing hujumlari orqali foydalanuvchilarning shaxsiy ma’lumotlari qo‘lga kiritilishi esa axborot xavfsizligiga jiddiy tahdid tug‘diradi.

Bundan tashqari, DDoS hujumlari server resurslarini ortiqcha yuklash orqali xizmatlarning vaqtincha yoki to‘liq to‘xtab qolishiga olib keladi. Bu esa, ayniqsa, yirik korporativ tarmoqlar va onlayn xizmat ko‘rsatuvchi tizimlar uchun katta iqtisodiy zarar keltirib chiqarishi mumkin. Shu jihatdan qaraganda, tarmoq xavfsizligini ta’minlashda faqat bitta himoya vositasiga tayanish yetarli emas.

Shuningdek, xavfsizlikni ta’minlashda inson omili muhim rol o‘ynaydi. Amaliy kuzatuvlar shuni ko‘rsatadiki, ko‘plab xavfsizlik buzilishlari foydalanuvchilarning yetarli bilimga ega emasligi yoki xavfsizlik qoidalariga amal qilmasligi natijasida yuzaga keladi. Shu sababli, xodimlarni muntazam o‘qitish, xavfsizlik siyosatini ishlab chiqish va nazorat mexanizmlarini joriy etish zarur hisoblanadi.

Yuqoridagi tahlillarga asoslanib, kompyuter tarmoqlarida axborot xavfsizligini ta’minlash uchun ko‘p darajali himoya tizimini joriy etish maqsadga muvofiqdir. Bunda shifrlash, autentifikatsiya, tarmoq monitoringi va foydalanuvchi xabardorligini oshirish kabi choralarni birgalikda qo‘llash yuqori samaradorlikni ta’minlaydi.

NATIJALAR

Olib borilgan tahlillar natijasida kompyuter tarmoqlarida axborot xavfsizligiga tahdid soluvchi asosiy omillar sifatida zararli dasturlar, DDoS hujumlari, phishing va ruxsatsiz kirish holatlari aniqlandi. Tadqiqotlar shuni ko‘rsatdiki, ko‘plab hollarda xavfsizlik muammolari kompleks himoya choralarining yetarli darajada qo‘llanilmasligi bilan bog‘liq.

Shuningdek, axborot xavfsizligini ta’minlashda faqat texnik vositalardan foydalanish yetarli emasligi, inson omilining ham muhim ahamiyatga ega ekanligi aniqlandi. Tahlil natijalariga ko‘ra, ko‘p darajali himoya tizimini joriy etish, jumladan, shifrlash, autentifikatsiya, tarmoq monitoringi va foydalanuvchilarni o‘qitish kabi choralarni birgalikda qo‘llash samarali natija berishi asoslandi.

XULOSA

Ushbu maqolada kompyuter tarmoqlarida axborot xavfsizligini ta’minlash bilan bog‘liq dolzarb muammolar ko‘rib chiqildi. Olib borilgan tahlillar natijasida

zamonaviy tarmoqlarda uchraydigan asosiy tahdidlar, jumladan, zararli dasturlar, DDoS hujumlari, phishing va ruxsatsiz kirish holatlarining axborot xavfsizligiga jiddiy ta’sir ko‘rsatishi aniqlandi.

Tadqiqotlar shuni ko‘rsatdiki, axborot xavfsizligini ta’minlashda faqat alohida himoya vositalaridan foydalanish yetarli emas. Shu bois, ko‘p darajali va kompleks himoya tizimini joriy etish muhim ahamiyatga ega. Xususan, shifrlash, autentifikatsiya, tarmoq monitoringi hamda foydalanuvchilarning axborot xavfsizligi bo‘yicha bilim va ko‘nikmalarini oshirish zarur.

Yuqoridagilardan kelib chiqib, kompyuter tarmoqlarida axborot xavfsizligini ta’minlashda texnik, tashkiliy va inson omillarini o‘zaro uyg‘un holda qo‘llash tavsiya etiladi. Bu esa axborot resurslarini ishonchli himoya qilish va xavfsizlik darajasini oshirishga xizmat qiladi.

ADABIYOTLAR RO‘YXATI

1. Stallings W. Network Security Essentials: Applications and Standards. – Pearson Education, 2017.
2. Kurose J.F., Ross K.W. Computer Networking: A Top-Down Approach. – Pearson, 2021.
3. Forouzan B.A. Data Communications and Networking. – McGraw-Hill, 2013.
4. Tanenbaum A.S., Wetherall D.J. Computer Networks. – Pearson, 2019.
5. Schneier B. Applied Cryptography: Protocols, Algorithms, and Source Code in C. – Wiley, 2015.
6. Bishop M. Computer Security: Art and Science. – Addison-Wesley, 2018.
7. Whitman M.E., Mattord H.J. Principles of Information Security. – Cengage Learning, 2021.
8. Ciampa M. Security+ Guide to Network Security Fundamentals. – Cengage Learning, 2022.
9. Stallings W., Brown L. Computer Security: Principles and Practice. – Pearson, 2018.
10. Easttom C. Network Defense and Countermeasures. – Pearson IT Certification, 2014.

11. Kaufman C., Perlman R., Speciner M. Network Security: Private Communication in a Public World. – Prentice Hall, 2016.