KOMPYUTER TARMOQLARI UCHUN XAVFSIZ PROTOKOLLAR ISHLAB CHIQISH

Ne'matjonova Sarvinoz Ikromjon qizi
Qo'qon universiteti andijon filiali Kompyuter injiniringi 1-bosqich talabasi

Annotatsiya: *Ushbu maqolada kompyuter tarmoqlarining xavfsizligini ta'minlashda muhim rol o'ynaydigan tarmoq protokollari, ularning zaif jihatlari hamda zamonaviy xavfsizlik mexanizmlari tahlil qilinadi. Tarmoqda ma'lumot almashinuvi jarayonida shifrlash, autentifikatsiya va ma'lumotlarning yaxlitligini saqlash usullari asosida xavfsiz protokollarni ishlab chiqish tamoyillari yoritiladi. Shuningdek, TLS, IPsec, SSH kabi amalda qo'llanilayotgan protokollarning afzalliklari va kamchiliklari o'rganilib, yangi yondashuvlar asosida takomillashtirish yo'llari taklif etiladi.*

Kalit so'zlar: *kompyuter tarmoqlari, xavfsizlik, protokollar, shifrlash, autentifikatsiya, TLS, IPsec, SSH, kriptografiya.*

KIRISH

So'nggi yillarda dunyo miqyosida raqamli texnologiyalar va kompyuter tarmoqlari rivoji inson faoliyatining deyarli barcha sohalarini qamrab oldi. Davlat boshqaruvi, ta'lim, sog'liqni saqlash, moliya va bank tizimi, sanoat hamda harbiy sohalarda axborot tizimlari va global tarmoqlar asosiy infratuzilma sifatida shakllandi. Shu bilan birga, tarmoqlar orqali amalga oshirilayotgan ma'lumot almashinuvi hajmi ortgani sari, ularni himoya qilish zarurati ham kuchayib bormoqda. Xavfsizlik masalalariga e'tibor qaratmaslik iqtisodiy, siyosiy va ijtimoiy sohalarda jiddiy talafotlarga olib kelishi mumkin.

O'zbekiston Respublikasi Prezidenti tomonidan qabul qilingan bir qator hujjatlar mamlakatda raqamli infratuzilmani rivojlantirish va axborot xavfsizligini mustahkamlashning huquqiy asosini yaratdi. Jumladan, "Raqamli O'zbekiston – 2030" strategiyasi to'g'risida"gi Prezident qarorida raqamli iqtisodiyot, davlat xizmatlarini elektron shaklga o'tkazish, kiberxavfsizlikni kuchaytirish va axborot tizimlarida xavfsiz ma'lumot almashinuvi mexanizmlarini joriy etish ustuvor yo'nalish sifatida belgilangan [1]. Shu bilan bir qatorda, 2022-yil 15-avgustdagi PQ–344-sonli Prezident qarori bilan tasdiqlangan "Axborot xavfsizligi sohasini yanada rivojlantirish chora-tadbirlari" dasturida milliy tarmoqlarda qo'llanilayotgan protokollarni yangilash, ularni xalqaro xavfsizlik standartlariga moslashtirish hamda kriptografik himoya tizimlarini takomillashtirish vazifalari belgilab berilgan [2].

Kompyuter tarmoqlarida ma'lumot almashinuvi protokollar orqali amalga oshiriladi. Shu sababli, bu protokollarning xavfsizligi butun tarmoq infratuzilmasining ishonchliligini belgilaydi. Amaldagi protokollar – HTTP, FTP, SMTP, DNS kabi tizimlar ochiq ma'lumot almashinuvi asosida ishlaydi va ularni kiberhujumlardan himoya qilish uchun TLS, IPsec, SSH singari xavfsizlik protokollari qo'llaniladi. Biroq, mavjud xavfsizlik protokollari ham to'liq himoya kafolatini bermaydi, chunki yangi turdagi kiberxavflar, masalan, "man-in-the-middle", "phishing", "spoofing" hujumlari, kriptografik zaifliklardan foydalanish holatlari muntazam ravishda ortib bormoqda.

Shu sababli, zamonaviy tarmoqlarda xavfsiz protokollarni ishlab chiqish, ularni kriptografik algoritmlar bilan takomillashtirish hamda milliy standartlarga moslashtirish dolzarb ilmiy-amaliy muammolardan biri hisoblanadi. Bu yo‘nalishda amalga oshiriladigan tadqiqotlar nafaqat texnik jihatdan, balki yuridik va tashkiliy jihatdan ham muhim ahamiyat kasb etadi. Zero, har bir davlatning axborot suvereniteti bevosita uning tarmoq xavfsizligi darajasiga bog‘liqdir.

5.6 Tadqiqot metodologiyasi

Mazkur tadqiqotning metodologiyasi kompyuter tarmoqlarida ma’lumot uzatish jarayonida xavfsizlikni ta’minlashga qaratilgan zamonaviy yondashuvlarni tahlil qilish, mavjud protokollarning zaif jihatlarini aniqlash va ularni takomillashtirishga asoslangan. Tadqiqotning markazida axborot almashinuvi protokollarini ilmiy-nazariy hamda amaliy jihatdan o‘rganish, shuningdek, xavfsiz tarmoq muhitini yaratish uchun samarali texnologik echimlarni ishlab chiqish masalasi turadi.

ASOSIY QISM: TAHLIL VA NATIJALAR

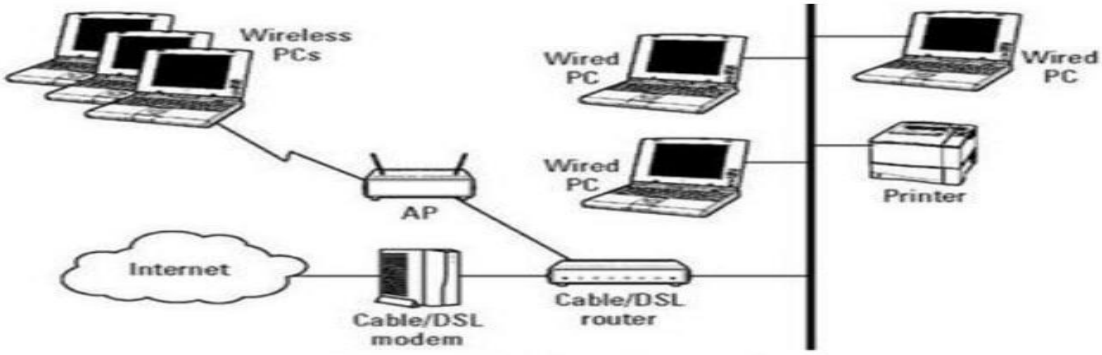
Hozirgi davrda tashkilotlar samarali va produktiv muloqot qilish uchun asosan kompyuter tarmoqlariga suyanadilar. Har bir xodimning maxsus ish stantsiyasi bor deb taxmin qilsak, yirik kompaniyalarda ularning soni bir necha mingga etishi mumkin, shuningdek, tarmoqda ko’plab serverlar ham mavjud bo’lishi mumkin.

Ehtimol, ushbu ish stantsiyalarini markazdan boshqarish mumkin emas va ularning atrof-muhiti xavfsizligi ta’minlanmagan. Foydalanuvchilar orasida turli xil sir tutilishi darajalariga ega bo’lgan xabarlarni, turli xil operatsion tizimlarga, qo’shimcha qurilmalarga, dasturlarga va protokollarga ega bo’lishi mumkin bo’lgan o’rtalikda almashish holatlari juda ko’p. Endi tasavvur qiling, kompaniya tarmog’idagi ushbu minglab ish stantsiyalari to’g’ridan - to’g’ri Internetga ulangan. Ko’plab zaifliklarga ega qimmatbaho ma’lumotlarni o’z ichiga olgan ushbu xavfli tarmoq bir nechta xakerlar hujumi uchun oson nishonga aylanadi.[3]

Fizik tarmoq Tarmoq deganda - resurslarni samarali almashish uchun bir-biriga ulangan ikki yoki undan ortiq hisoblash qurilmalari tushuniladi. Ikki yoki undan ortiq tarmoqlarni bir-biriga ulash esa o’zaro bog’langan tarmoqlar deb ataladi. Shunday qilib, Internet shunchaki o’zaro bog’langan tarmoq yoki o’zaro bog’langan tarmoqlarning to’plamidir. Tashkilot o’zining ichki tarmog’ini sozlash uchun turli xil variantlardan foydalanadi. U ish stantsiyalarini ulash uchun simli yoki simsiz tarmoqdan foydalanishi mumkin. Hozirgi kunda tashkilotlar asosan simli va simsiz tarmoqlarning kombinatsiyasidan foydalanadilar.

Simli va simsiz tarmoqlar

Simli tarmoqda qurilmalar bir-biriga kabellar yordamida ulanadi. Odatda simli tarmoqlar Ethernet protokoliga asoslanadi, bu yerda qurilmalar himoya qobig’i bilan qoplangan juft (UTP- Unshielded Twisted Pair) kabellar yordamida turli xil komutatorlarga ulanadi. Ushbu komutatorlar qo’shimcha ravishda Internetga kirish uchun tarmoq marshrutizatoriga ulangan bo’ladi.



1-Rasm Aralash yoki gibrid kompyuter tarmog'i[4]

Simsiz tarmoqda qurilma radio signallar yordamida kirish nuqtasiga ulanadi. Kirish nuqtalari qo'shimcha ravishda tashqi tarmoqqa kirish uchun kommutatorga/marshrutizatorga kabellar orqali ulanadi.

Simsiz tarmoqlar mobilligi tufayli keng qo'llanilishiga erishdi. Mobil qurilmalar kabelga bog'lanmagan va simsiz signallar diapazonlarida erkin harakatlanishi mumkin. Bu esa qulay aloqani ta'minlaydi va ish samaradorligini oshiradi.

Tarmoq - bu ma'lumotlarni uzatish va qayta ishlash qurilmalari tomonidan hosil qilingan ob'ektlar to'plami. Xalqaro standartlashtirish tashkiloti kompyuter tarmog'ini bir-biriga ulangan mustaqil qurilmalar o'rtasida bit-yo'naltirilgan ketma-ket ma'lumotlarni uzatish deb ta'riflagan.

Tarmoqlar odatda foydalanuvchilar tomonidan xususiy ravishda boshqariladi va ba'zi hududlarni egallaydi va hududiy jihatdan quyidagilarga bo'linadi:

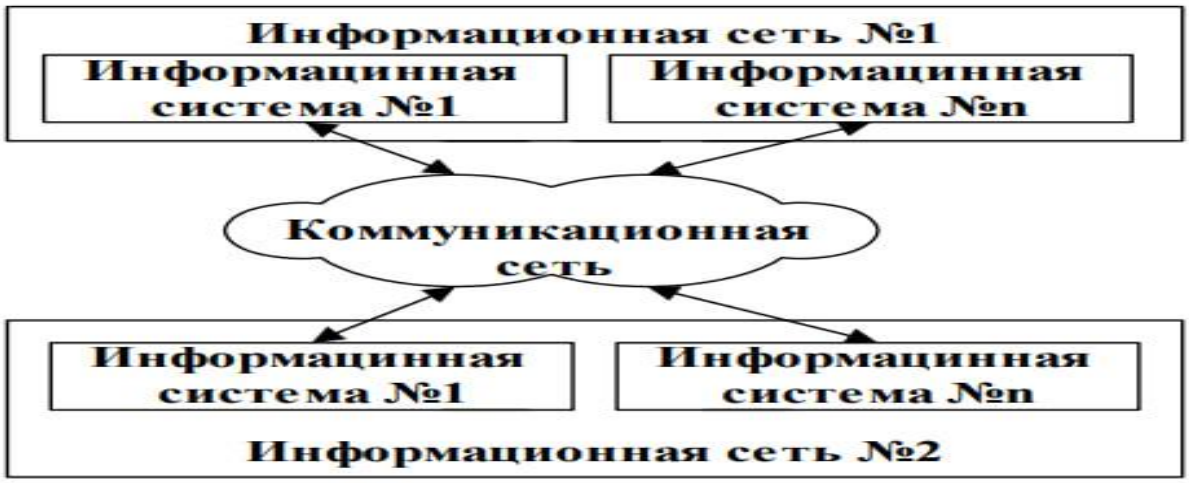
- LAN (Local Area Network) - bir yoki bir nechta yaqin joylashgan binolarda joylashgan lokal (mahalliy) tarmoqlar yoki LANlar odatda tashkilot (korporatsiya, muassasa) ichida joylashgan, shuning uchun ular korporativ deb ham nomlanadi.
- WAN (Wide Area Network) - hududiy, aralash, global, binolarda, shaharlarda va mamlakatlarda joylashgan yoki taqsimlangan kompyuter tarmoqlari. Shunga qarab global tarmoqlar to'rt asosiy turga bo'linadi: shahar, mintaqaviy, milliy va transmilliy.

Juda katta miqyosda tarqatilgan tarmoqlarga quyidagilar kiradi:

Internet, EUNET (European UNIX Network), Relcom, FIDO (Fast IDentity Online). Tarmoq odatda quyidagi elementlarni o'z ichiga oladi:

- tarmoq kompyuterlari (tarmoq adapteri bilan jihozlangan);
- aloqa kanallari (kabel, sun'iy yo'ldosh, telefon, raqamli, optik tolali, radiokanallar va boshqalar);
- har xil turdagi signal o'zgartirgichlari;
- tarmoq qurilmalari.

Tarmoqning ikkita tushunchasi mavjud: aloqa tarmog'i va axborot tarmog'i (2-rasm). Aloqa tarmog'i ma'lumotlarni uzatish uchun mo'ljallangan bo'lib, u shuningdek ma'lumotlarni o'zgartirish bilan bog'liq vazifalarni bajaradi. Aloqa tarmoqlari ishlatiladigan fizik ulanish vositalariga ko'ra farqlanadi.



2-Rasm

Axborot tarmog'i axborotni saqlash uchun mo'ljallangan va axborot tizimlaridan iborat. Aloqa tarmog'i asosida axborot tarmoqlari guruhini qurish mumkin:

Axborot tizimini axborotni etkazib beruvchi yoki iste'molchisi bo'lgan tizim deb tushunish kerak.[5]

Kompyuter tarmog'i axborot tizimlari va aloqa kanallaridan iborat.

Axborot tizimini axborotni saqlash, qayta ishlash yoki uzatish qobiliyatiga ega bo'lgan ob'ekt deb tushunish kerak. Axborot tizimiga quyidagilar kiradi: kompyuterlar, dasturlar, foydalanuvchilar, ma'lumotlarni qayta ishlash va uzatish jarayoniga mo'ljallangan boshqa komponentlar. Kelajakda foydalanuvchi vazifalarini hal qilishga mo'ljallangan axborot tizimi -workstation (mijoz) deb nomlanadi. Tarmoqdagi ish stantsiyasi odatdagi shaxsiy kompyuterdan (kompyuter) tarmoq kartasi (tarmoq adapteri), ma'lumotlar uzatish kanali va tarmoq dasturining mavjudligi bilan farq qiladi.

5.7 Xulosa

Bugungi kunda raqamli texnologiyalar jadal rivojlanayotgani sharoitida kompyuter tarmoqlari xavfsizligini ta'minlash global miqyosdagi eng muhim masalalardan biri sifatida dolzarb ahamiyat kasb etmoqda. Axborot oqimlari hajmining ortib borishi, foydalanuvchilar sonining ko'payishi va tarmoqlar o'rtasidagi o'zaro bog'liqlikning kuchayishi natijasida yangi turdagi kiberxavf va hujumlar paydo bo'lmoqda. Shu bois, mavjud protokollarni qayta ko'rib chiqish, ularni zamonaviy kriptografik mexanizmlar asosida takomillashtirish zarurati kuchaymoqda.

FOYDALANILGAN ADABIYOTLAR:

[1] O'zbekiston Respublikasi Prezidentining "Raqamli O'zbekiston – 2030" strategiyasini tasdiqlash to'g'risidagi PQ–6079-son qarori. — 2020-yil 5-oktabr.
[2] O'zbekiston Respublikasi Prezidentining "Axborot xavfsizligi sohasini yanada rivojlantirish chora-tadbirlari to'g'risida"gi PQ–344-son qarori. — 2022-yil 15-avgust.
[3] Stallings, W. Network Security Essentials: Applications and Standards. — Pearson Education, 2021.

[4] RFC 8446. The Transport Layer Security (TLS) Protocol Version 1.3. — IETF, 2018.
[5] Alabady, S. A. "Design and Implementation of Secure Network Protocols." International Journal of Computer Applications, Vol. 183, No. 45, 2022.