

## MULTISERVISLI ALOQA TARMOQLARIDA AXBOROTLARGA TAHDID TURLARI

**S.G'. Toxirova**

Muhammad Al-Xorazmiy nomidagi  
TATU Farg'ona filiali "Axborot texnologiyalari" kafedراسi assistenti.

**A.G'. Muhammadjonov**

Muhammad Al-Xorazmiy nomidagi  
TATU Farg'ona filiali "Dasturiy ingineriing" kafedراسi assistenti.

**M.Y. Siddiqov**

Muhammad Al-Xorazmiy nomidagi  
TATU Farg'ona filiali "Axborot xavfsizligi" talabasi

### ANNOTATSIYA

Zamonaviy multiservis tarmoqlarini loyihalash va ishlatishning o'ziga xos xususiyatidan biri ularning axborot xavfsizligini ta'minlash hisoblanadi. Bu tegishli xavfsizlik siyosatini ishlab chiqishni talab qiladi, uni ishlab chiqish va amalga oshirish uchun OSI modelining tarmoq darajalarida asosiy zaifliklar va tahdidlarni tahlil qilish kerak.

**Kalit so'zlar.** Axborotga tahdid turlari, tarmoq, axborot xavfsizlik, multiservisli tarmoqlar, zaifliklar.

Zamonaviy telekommunikatsiyalarda ochiq tizimlarning o'zaro ta'siri uchun OSI mos yozuvlar modeli keng qo'llanilladi. U ma'lumotlarni uzatish jarayonini yetti darajaga bo'linadi: jismoniy, kanal, tarmoq, transport, seans, taqdimot va amaliy. Ushbu model asosida tizim elementlarining tasnifi o'zaro ta'sirlar va mantiqiy konstruktsiyalar masalasini ko'rib chiqishni soddalashtirish mumkin.

Xavfsizlik siyosatini ishlab chiqishda ushbu modeldan foydalanish samarali yechim hisoblanadi, chunki u butun tarmoq uchun potentsial tahdidlarni va mavjud zaifliklarni to'liq tahlil qilish imkonini beradi. Modelning quyi darajalarini (jismoniy, kanal, tarmoq) tahlil qilishga alohida e'tibor beriladi, chunki ular multiservis tarmog'ining apparat ta'minotini amalga oshirish uchun javobgardir.

Jismoniy qatlam jismoniy nazoratni amalga oshiradi. U signalni yetkazib berish muhitini belgilaydi va bit oqimi darajasida jismoniy ulanishni o'rnatish, saqlash va tugatish uchun jismoniy, elektr, funktsional va protsessual xususiyatlar bilan

shugʻullanadi. 1-jadvalda ushbu darajadagi zaifliklar va potentsial tahdidlar tahlili keltirilgan.

Bogʻlanish qatlami jismoniy havola orqali maʼlumotlar ramkalarini yoʻnaltirishni anglatadi va havolalarni boshqarish uchun javobgardir. Bunday holda, uzatiladigan bloklarning bosh va quyruq ramkasini belgilaydigan va ushbu bloklarni almashtirish protokolini belgilaydigan jismoniy aloqani boshqarish protsedurasi talab qilinadi. Ushbu darajada xato xabarlar, tarmoq topologiyasi va paketlar oqimini boshqarish buyruqlari, shuningdek, ushbu jismoniy havola darajasida lokalizatsiya qilingan jismoniy ulanish port manzillarining Media Access Control (MAC) boshqaruvi mavjud. 2-jadvalda ushbu darajadagi zaifliklar va potentsial tahdidlar tahlili keltirilgan.

1-jadval.

Zaifliklar	Tahdidlar
Jismoniy himoyaning yetarli emasligi (qurilmalar va uzatish vositalari); Uzatish vositasi orqali shifrlanmagan maʼlumotlarni uzatish;	Faol va passiv qabul qilish usullaridan foydalangan holda aloqa liniyalari orqali uzatiladigan trafikni ushlab turish, tahlil qilish va buzish.

2-jadval.

Zaifliklar	Tahdidlar
Turli terminallardan foydalanish hisobiga foydalanuvchi MAC manzillari oshkor boʻlishi; Multiservisli tarmoq trafiginini ochiq holda uzatish; Autentifikatsiya mexanizmi yoki xabarlarining raqamli imzosi yoʻqligi.	Trafik oʻzgarishi: qonuniy joy sifatida niqoblangan xabarni qabul qilish qobiliyati; Joʻnatuvchi sifatida maskarad qilish va xabarlarini joʻnatish qobiliyati.

Tarmoq qatlami virtual yoki mantiqiy sxemaga ishora qiladi. Bu zanjir jismonan mavjud emas, lekin u tufayli yuqori darajalar bir-biri bilan oʻzaro taʼsir qilishi mumkin, chunki u mavjud. Ushbu darajadagi maʼlumotlar tarmoqlarida IP-paketlardan foydalaniladi, barcha tarmoq tugunlarining mantiqiy adreslanishi amalga oshiriladi va koʻp servisli trafik marshrutlari aniqlanadi. 3-jadvalda ushbu darajadagi zaifliklar va tahdidlar tahlili keltirilgan.

3-jadval.

Zaifliklar	Tahdidlar
Kommutatsiya qurilmalari va transport marshrutini masofadan boshqarish imkoniyati; Tarmoq qurilmalariga jismoniy kirish;	Yolg'on marshrut qo'yish orqali soxta ob'ektni kiritish; Kommutatsiya va marshrutlash qurilmalarining yopilishi va ishdan chiqishi;

Shunday qilib, OSI modelining quyi darajalarida multiservis tarmog'ining mavjud zaif tomonlari va potentsial tahdidlari tahlili o'tkazildi, bu tarmoq ichidagi axborot jarayonlari xavfsizligiga xavflarni baholash va tegishli choralarni ishlab chiqish imkonini beradi.

#### **FOYDALANILGAN ADABIYOTLAR RO'YXATI: (REFERENCES)**

1. Mozhaev O. et al. Multiservice network security metric //2017 2nd International Conference on Advanced Information and Communication Technologies (AICT). – IEEE, 2017. – C. 133-136.
2. Muhammadjonov A., Toxirova S. YARIMO'TKAZGICHLARNING TURLARI. ICHKI VA TASHQI YARIMO'TKAZGICHLAR //Research and implementation. – 2023.
3. Shin D. H. Determinants of customer acceptance of multi-service network: An implication for IP-based technologies //Information & Management. – 2009. – T. 46. – №. 1. – C. 16-22.