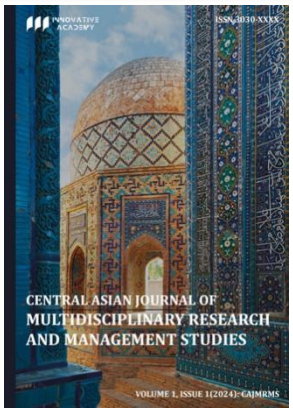


MULTIMEDIALI ALOQA TARMOQLARIGA BO‘LADIGAN HUJUMLARNI ANIQLASH USULLARI.

Shaydullayev Jahongir Qudrat o‘g‘li
Muhammad al-Xorazmiy nomidagi Toshkent axborot texnologiyalari universiteti
Shaydullayevjahongir579@gmail.com
https://doi.org/10.5281/zenodo.14992969

ARTICLE INFO

Received:27th February 2025
Accepted:28th February 2025
Published: 8th March 2025

KEYWORDS

Xizmat ko‘rsatishni rad etish (DoS) hujumlari, Man-in-the-Middle (MitM) hujumlari, Zararli dasturiy ta'minot hujumlari, Spoofing hujumi, Fishing hujumlari, Ma'lumotlarni kiritish hujumi.

ABSTRACT

ushbu maqolada multimediali aloqa tarmoqlariga bo‘ladigan hujumlarni aniqlash haqida fikr yuritilgan.

Korporativ kompyuter tarmoqlarida axborot xavfsizligini ta'minlash muammolari mahalliy ish stantsiyalari, mahalliy tarmoqlar xavfsizligiga tahdidlar va umumiy ma'lumotlar tarmoqlariga kirish imkoniga ega bo‘lgan korporativ tarmoqlarga hujumlar bilan bog'liq. Tarmoq hujumlari ular maqsad qilgan tizimlar kabi xilma-xildir. Ba'zi hujumlar juda murakkab, boshqalari oddiy operator tomonidan amalga oshirilishi mumkin, hatto uning faoliyati qanday oqibatlarga olib kelishini taxmin qilmaydi. Hujumni amalga oshirayotgan jinoyatchining maqsadlari:

- uzatilayotgan axborotning maxfiyligini buzish;
- uzatilayotgan axborotning yaxlitligi va ishonchliligini buzish;
- butun tizim yoki uning alohida qismlarining noto‘g'ri ishlashi.

Taqsimlangan tizimlar, birinchi navbatda, masofaviy hujumlarga sezgir, chunki taqsimlangan tizimlarning tarkibiy qismlari odatda ochiq ma'lumotlarni uzatish kanallaridan foydalanadi va buzg'unchi nafaqat uzatilgan ma'lumotni passiv tinglashi, balki uzatiladigan trafikni ham o‘zgartirishi mumkin (faol ta'sir). Va agar trafikka faol ta'sirni qayd etish mumkin bo‘lsa, unda passiv ta'sir amalda aniqlanmaydi. Ammo taqsimlangan tizimlarning ishlashi jarayonida tizim komponentlari o‘rtasida xizmat ma'lumotlari almashinuvi ochiq ma'lumotlarni uzatish kanallari orqali ham amalga oshirilganligi sababli, xizmat ma'lumotlari foydalanuvchi ma'lumotlari bilan bir xil hujum ob'ektiga aylanadi.

Masofaviy hujum faktini aniqlashning qiyinligi ushbu turdagi noqonuniy xatti-harakatlarni xavflilik darajasi bo‘yicha birinchi o‘ringa olib chiqadi va amalga oshirilgan tahdidga o‘z vaqtida javob berishga to‘sqinlik qiladi, buning natijasida huquqbuzarning muvaffaqiyatli bo‘lish imkoniyatini oshiradi. Mahalliy tarmoq xavfsizligi Internet tarmog'i xavfsizligidan farq qiladi, chunki ro‘yxatdan o‘tgan foydalanuvchilarning qoidabuzarliklari birinchi o‘ringa chiqadi, chunki bu holda mahalliy tarmoqning ma'lumotlar uzatish kanallari boshqariladigan hududda joylashgan va ruxsatsiz ulanishdan himoyalanish ma'muriy usullar bilan amalga oshiriladi.

Amalda, IP tarmoqlari aloqa jarayoniga ruxsatsiz kirishning ko‘plab usullariga nisbatan zaifdir. Kompyuter va tarmoq texnologiyalarining rivojlanishi bilan (masalan, mobil Java ilovalari va

ActiveX boshqaruvlarining paydo bo‘lishi bilan) IP tarmoqlariga tarmoq hujumlarining mumkin bo‘lgan turlari ro‘yxati doimiy ravishda kengayib bormoqda.

Multimedia aloqa tarmoqlari zamonaviy hayotimizning muhim qismi bo‘lib, bizga turli yo‘llar bilan ma'lumot almashish va boshqalar bilan muloqot qilish imkonini beradi. Biroq, bu tarmoqlar o‘zlarining zaif tomonlarini o‘z maqsadlari uchun ishlatishga intilayotgan yomon niyatli shaxslarning hujumlariga ham zaifdir. Ushbu bobda biz multimediya aloqa tarmoqlariga eng ko‘p uchraydigan hujumlar va ularni oldini olish uchun ishlatilishi mumkin bo‘lgan qarshi choralarni ko‘rib chiqamiz.

Multimedia aloqa tarmoqlariga bo‘ladigan hujumlar turlari:

Xizmat ko‘rsatishni rad etish (DoS) hujumlari: DoS hujumlari hujumlar turi bo‘lib, bu hujumchilar multimedia aloqa tarmoqlarini trafik bilan to‘ldirib, tarmoqning ishdan chiqishiga yoki javob bermasligiga olib keladi. DoS hujumlari tarmoqni trafik bilan to‘ldirish, tarmoq dasturiy ta'minotidagi zaifliklardan foydalanish yoki tarmoqni so‘rovlar bilan ortiqcha yuklash kabi turli usullar yordamida amalga oshirilishi mumkin.

Qarshi choralar: DoS hujumlarining oldini olishning eng yaxshi usullaridan biri shubhali trafikni aniqlash va blokirovka qilish mumkin bo‘lgan trafik filtrlash vositalaridan foydalanishdir. Bundan tashqari, tarmoq ma'murlari muntazam ravishda tarmoq trafigini kuzatib borishlari va DoS hujumlarini aniqlash va oldini olish uchun hujumlarni aniqlash tizimlarini o‘rnatishlari kerak.

Man-in-the-Middle (MitM) hujumlari: MitM hujumlari - bu hujumchi ikki tomon o‘rtasidagi aloqani to‘xtatib, suhbatga o‘zini qo‘shadigan hujum turi. Keyin tajovuzkor aloqani tinglashi yoki hatto uni o‘zgartirishi mumkin.

Zararli dasturiy ta'minot hujumlari: Zararli dasturiy ta'minot hujumlari multimedia aloqa tarmoqlarini zararlash uchun viruslar, qurtlar va troyanlar kabi zararli dasturlardan foydalanishni o‘z ichiga oladi. Zararli dastur maxfiy ma'lumotlarni o‘g'irlash, tarmoq operatsiyalarini buzish yoki qurilmalarga zarar etkazish uchun ishlatilishi mumkin.

Qarshi chora-tadbirlar: Zararli dastur hujumlarining oldini olish uchun multimedia aloqa tarmoqlari zararli dasturlarni aniqlash va o‘chirish uchun antivirus dasturidan foydalanishi kerak. Bundan tashqari, tarmoq ma'murlari tajovuzkorlar tomonidan ma'lum zaifliklardan foydalanishning oldini olish uchun dasturiy ta'minot va xavfsizlik yamoqlarini muntazam yangilashlari kerak.

Spoofing hujumi - bu tajovuzkor tarmoqqa kirish uchun qonuniy foydalanuvchi yoki qurilma nomini olgan hujum. Multimedia aloqa tarmoqlarida maxfiy ma'lumotlarni o‘g'irlash yoki aloqani buzish uchun firibgarlik hujumlaridan foydalanish mumkin. Misol tariqasida IP-spoofing, MAC-spoofing yoki ARP-spoofing kabi, DHCP-serverni aldash hujumlarini keltirish mumkin. DHCP bilan autentifikatsiyani amalga oshirish mumkin emasligi sababli, u firibgarlik hujumlariga juda zaifdir.

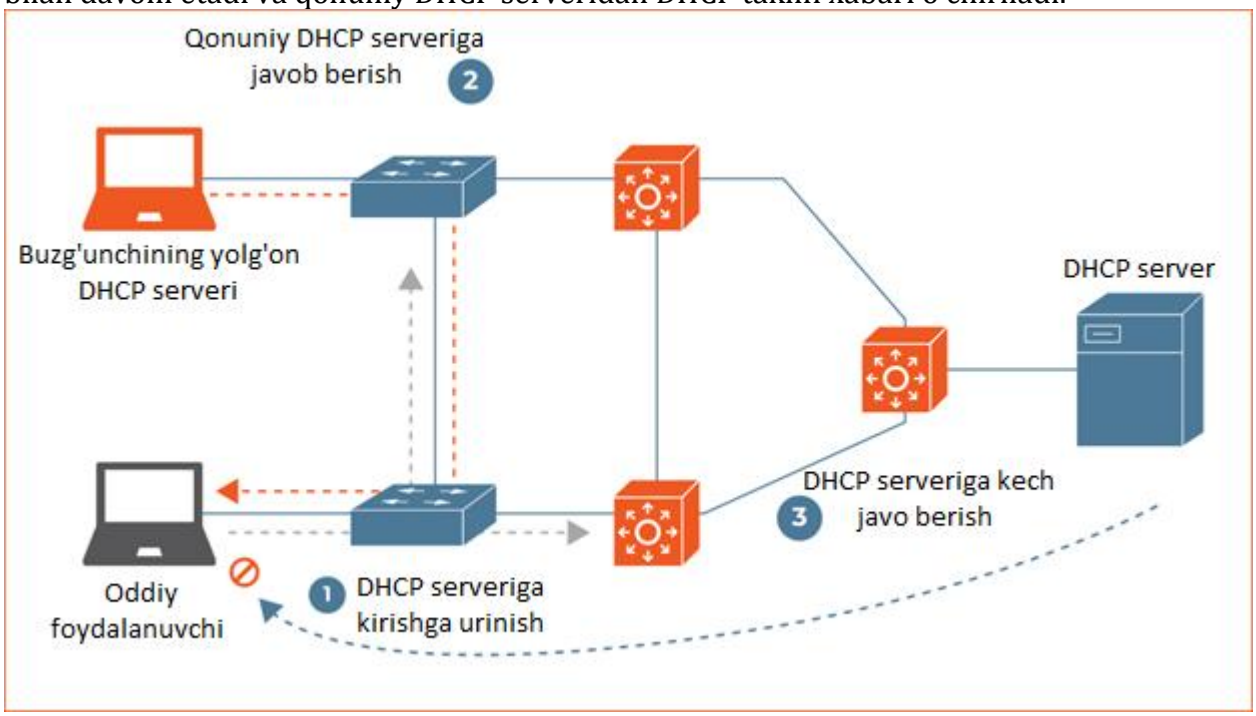
Buzg'unchi noto‘g'ri DHCP serverini ishlatganda, foydalanuvchi tarmoqdagi qonuniy DHCP server o‘rniga tajovuzkor bilan DHCP aloqasini ko‘r-ko‘rona boshlashi mumkin. Bu noto‘g'ri DHCP serveri DHCP mijoziga yaqinroq bo‘lganda va qonuniy DHCP serveridan oldin javob berganda osonlik bilan sodir bo‘lishi mumkin.

Natijada, tajovuzkor o‘zini DHCP mijozlariga qaytariladigan DHCP javoblarida standart shlyuz yoki DNS server sifatida belgilash orqali o‘rtadagi odam hujumini amalga oshirishi mumkin. Bu tajovuzkorga konfiguratsiya qilingan mijozlar va tarmoqning qolgan qismi o‘rtasidagi IP-muloqotni to‘xtatish imkonini beradi.

1-rasmda tarmoqda noto‘g'ri DHCP server mavjud bo‘lganda bajariladigan qadamlar ko‘rsatilgan. Birinchidan, foydalanuvchi IP ma'lumotlarini olish uchun DHCP serveriga kirishga harakat qiladi. Ikkinchidan, bu xabar translyatsiya ramkasi bo‘lganligi sababli, kalit barcha interfeyslarda xabarni to‘ldiradi, ya'ni bir nusxasi qonuniy DHCP serveriga, ikkinchisi esa yolg'on DHCP serveriga yuboriladi.

Nihoyat, agar tajovuzkor qurilmasi avval javob qaytarsa, butun DHCP aloqasi faqat shu server

bilan davom etadi va qonuniy DHCP serveridan DHCP taklifi xabari o‘chiriladi.



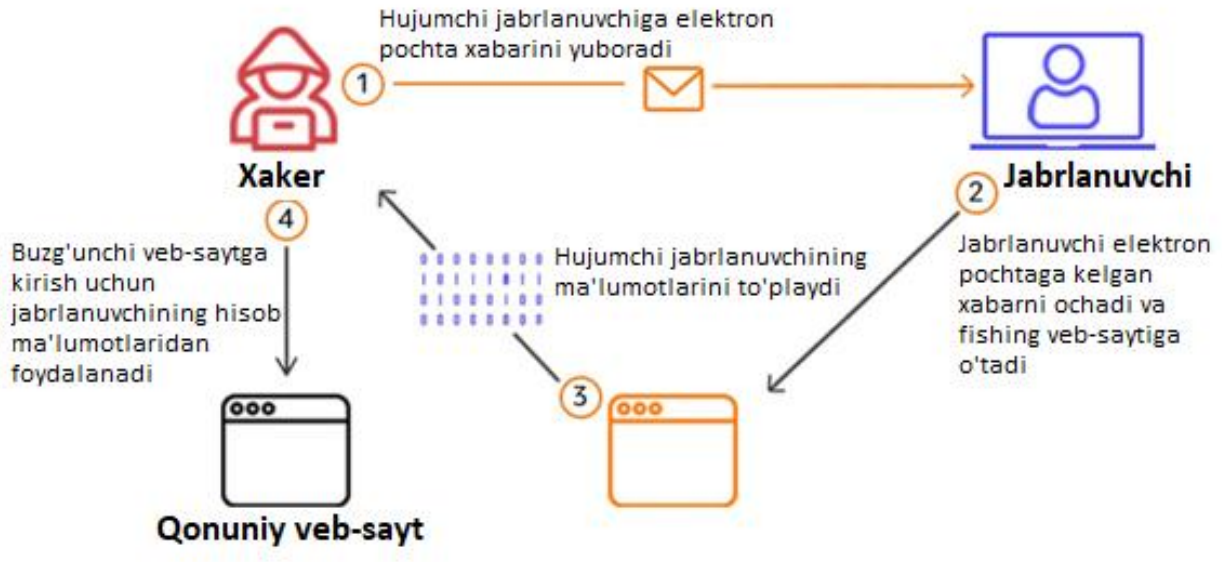
1-rasm. **DHCP serveriga spoofing hujumi**

Spoofing hujumlariga qarshi turish uchun tarmoq ma'murlari kengaytiriladigan autentifikatsiya protokoli (EAP) yoki Secure Shell (SSH) kabi autentifikatsiya protokollaridan foydalanishi mumkin.

Qarshi choralar: Spoofing hujumlarining oldini olish uchun multimedia aloqa tarmoqlari tarmoqqa kirishga ruxsat berishdan oldin foydalanuvchilar va qurilmalarning shaxsini tekshirish uchun autentifikatsiya mexanizmlaridan foydalanishi kerak. Bundan tashqari, tarmoq ma'murlari shubhali manbalardan keladigan trafikni blokirovka qilish uchun xavfsizlik devorlaridan foydalanishlari va firibgarlik hujumlarini aniqlash va oldini olish uchun kirishni aniqlash tizimlarini o‘rnatishlari kerak.

DHCP spoofing hujumidan himoya qilish uchun ikkita yechim mavjud. Birinchi yechim tarmoqdagi barcha so‘nggi nuqtalarda IP ma'lumotlarini qo‘lda sozlashdir, bu katta muhitda deyarli imkonsiz bo‘ladi. Ikkinchi yechim kalitlarda DHCP snooping xususiyatini amalga oshirishdir.

Fishing hujumlari - tajovuzkorni ijtimoiy muhandislik usullaridan foydalangan holda foydalanuvchilarni aldash uchun kirishni hisobga olish ma'lumotlari yoki kredit karta raqamlari kabi maxfiy ma'lumotlarni ochishni o‘z ichiga oladi, bu multimedia aloqa tarmoqlarini buzish uchun ishlatilishi mumkin
(2-rasm).



2-rasm. **Fishing hujumi**

Qarshi chora-tadbirlar: Fishing hujumlarining oldini olish uchun multimedia aloqa tarmoqlari foydalanuvchilarni fishing xatarlari haqida o‘rgatishi va ularga fishing firibgarliklarini aniqlash va oldini olish bo‘yicha treninglar o‘tkazishi kerak. Bundan tashqari, tarmoq ma'murlari fishing elektron pochta xabarlarini bloklash uchun spam filtrlaridan foydalanishi va fishing hujumlarini aniqlash va oldini olish uchun hujumlarni aniqlash tizimlarini o‘rnatishi kerak.

Ma'lumotlarni kiritish hujumi - bu hujumchining aloqa oqimiga zararli ma'lumotlarni kiritadigan hujumidir. Multimediyali aloqa tarmoqlarida ma'lumotlarni kiritish hujumlari aloqani buzish yoki nozik ma'lumotlarni o‘g'irlash uchun ishlatilishi mumkin. Ma'lumotlarni kiritish hujumlariga qarshi turish uchun tarmoq ma'murlari kirishni tekshirish va ma'lumotlarni tozalash kabi ma'lumotlarni tekshirish usullaridan foydalanishi mumkin.

Ushbu hujumlardan tashqari, multimediali aloqa tarmoqlariga qarshi ishlatilishi mumkin bo‘lgan boshqa ko‘plab hujumlar mavjud. Ushbu tarmoqlarni himoya qilish uchun tarmoq ma'murlari xavfsizlik devorlari, IDS, yuk balanslagichlari, shifrlash protokollari, autentifikatsiya protokollari va ma'lumotlarni tekshirish usullarini o‘z ichiga olgan bir qator xavfsizlik choralarini qo‘llashlari kerak. Shuningdek, ular o‘z tarmoqlarini so‘nggi xavfsizlik yamoqlari va yangilanishlari bilan yangilab turishlari va noodatiy faoliyat belgilari uchun o‘z tarmoqlarini muntazam ravishda kuzatib borishlari kerak. Ushbu qadamlarni bajarish orqali tarmoq ma'murlari o‘zlarining multimedia aloqa tarmoqlari orqali uzatiladigan ma'lumotlarning xavfsizligi va maxfiyligini ta'minlashga yordam berishi mumkin.

Yuqorida ko‘rib o‘tilgan multimediyali aloqa tarmoqlariga bo‘ladigan hujumlarni va qarshi qo‘llanilishi mumkin bo‘lgan turli usullar va choralarni tahlil qildik va taqqoslash osonroq bo‘lishi uchun ularni jadval shaklida taqdim etamiz
(1-jadval).

1-jadval

Hujum usuli	Tavsif	Qarshi chora
Xizmatni rad etish (DoS)	Tarmoqni trafik bilan to‘ldirish, uni yaroqsiz holga keltirish	Shubhali trafikni aniqlash va blokirovka qilish uchun trafikni filtrlash vositalari va kirishni aniqlash tizimlaridan foydalaning
Spoofing	Tarmoqqa ruxsatsiz kirish uchun o‘zini qonuniy foydalanuvchi sifatida ko‘rsatish	Foydalanuvchilar va qurilmalarning identifikatorini tekshirish va shubhali

		manbalardan kelayotgan trafikni bloklash uchun autentifikatsiya mexanizmlari, xavfsizlik devorlari va hujumlarni aniqlash tizimlaridan foydalaning.
Zararli dastur	Tarmoqni zararli dasturlar bilan zararlash, multimedia kontentining yaxlitligi va mavjudligini buzish	Antivirus dasturidan foydalaning va zararli dasturlarni aniqlash va o‘chirish uchun dasturiy ta'minot va xavfsizlik tuzatishlarini muntazam yangilang
Fishing	Foydalanuvchilarni kirish ma'lumotlari yoki kredit karta raqamlari kabi nozik ma'lumotlarni oshkor qilishda aldash uchun ijtimoiy muhandislik usullaridan foydalanish	Foydalanuvchilarga fishing xatarlari haqida ma’lumot bering, fishing firibgarliklarini aniqlash va oldini olish, spam-filtrlardan foydalanish va fishing hujumlarini aniqlash va oldini olish uchun hujumlarni aniqlash tizimlarini o‘rnatish bo‘yicha treninglar o‘tkazing.
IP-spoofing va MAC manzilini buzish	Xavfsizlik choralarini chetlab o‘tish uchun soxta IP-manzildan foydalanadigan IP-spoofing	Autentifikatsiya mexanizmlari Firewallar
Spam xatlar va Ijtimoiy muhandislik	Qonuniy manbadan kelgan va tizimga kirish ma'lumotlari yoki boshqa shaxsiy ma'lumotlarni so‘ragan elektron xatlar	Spam filtrlari va Foydalanuvchilarni o‘qitish va o‘rgatish

Jadvalda ko‘rinib turibdiki, multimedia aloqa tarmoqlariga hujum qilishning turli usullari mavjud va ularning har biri uning ta'sirini oldini olish yoki yumshatish uchun muayyan qarshi choralarni talab qiladi. Masalan, shubhali trafikni aniqlash va blokirovka qilish uchun trafik filtrlash vositalari va hujumlarni aniqlash tizimlari yordamida DoS hujumlarini oldini olish mumkin, tinglash hujumlarini esa kuchli shifrlash algoritmlari va multimedia kontentini ruxsatsiz kirishdan himoya qilish uchun virtual xususiy tarmoqlar (VPN) yordamida oldini olish mumkin.

Boshqa tomondan, foydalanuvchilar va qurilmalarning identifikatorini tekshirish va shubhali manbalardan trafikni blokirovka qilish uchun autentifikatsiya mexanizmlari, xavfsizlik devorlari va tajovuzni aniqlash tizimlaridan foydalanish orqali soxta hujumlarning oldini olish mumkin. Zararli dasturiy ta'minot hujumlarining oldini olish uchun antivirus dasturidan foydalanish va zararli dasturlarni aniqlash va o‘chirish uchun dasturiy ta'minot va xavfsizlik patchlarini muntazam yangilab turish, fishing hujumlarini esa foydalanuvchilarni fishing xatarlari haqida o‘rgatish, fishing firibgarliklarini aniqlash va oldini olish bo‘yicha treninglar o‘tkazish orqali oldini olish mumkin. spam filtrlari va fishing hujumlarini aniqlash va oldini olish uchun hujumlarni aniqlash tizimlarini o‘rnatish.

Multimedia kontentini ruxsatsiz kirishdan himoya qilish uchun kuchli shifrlash algoritmlaridan foydalanish va foydalanuvchilar va tarmoq o‘rtasida xavfsiz aloqa kanalini

yaratish uchun virtual xususiy tarmoqlar (VPN) yordamida tinglash hujumlarining oldini olish mumkin.

Tarmoqqa kirishga ruxsat berishdan oldin foydalanuvchilar va qurilmalarning identifikatorini tekshirish uchun autentifikatsiya mexanizmlaridan foydalanish, shubhali manbalardan kelayotgan trafikni blokirovka qilish uchun xavfsizlik devorlaridan foydalanish va soxtalashtirish hujumlarini aniqlash va oldini olish uchun tajovuzni aniqlash tizimlarini qo‘llash orqali soxta hujumlarning oldini olish mumkin.

Zararli dasturiy ta'minotni aniqlash va o‘chirish uchun antivirus dasturidan foydalanish hamda ma'lum zaifliklardan tajovuzkorlar tomonidan foydalanishni oldini olish uchun dasturiy ta'minot va xavfsizlik yamoqlarini muntazam yangilab turish orqali zararli dastur hujumlarining oldini olish mumkin.

Foydalanuvchilarni fishing xatarlari haqida o‘rgatish va ularga fishing firibgarliklarini aniqlash va oldini olish bo‘yicha treninglar o‘tkazish, fishing elektron pochta xabarlarini bloklash uchun spam-filtrlardan foydalanish hamda fishing hujumlarini aniqlash va oldini olish uchun hujumlarni aniqlash tizimlarini qo‘llash orqali fishing hujumlarining oldini olish mumkin.

Parollar, ikki faktorli autentifikatsiya va biometrik identifikatsiyalash kabi autentifikatsiya mexanizmlari yordamida foydalanuvchilar va qurilmalarning tarmoqqa kirishiga ruxsat berishdan oldin ularning identifikatorini tekshirish orqali firibgarlik hujumlarini yumshatish mumkin. Xavfsizlik devorlari shubhali manbalardan trafikni blokirovka qilish uchun ham ishlatilishi mumkin va buzg'unchilikni aniqlash tizimlari firibgarlik hujumlarini aniqlashi va oldini olishi mumkin.

FOYDALANILGAN ADABIYOTLAR RO‘YXATI:

1. B. Furht, "Multimedia Systems: An Overview", IEEE Multimedia, Vol.1, No.1, Spring 1994, pp.47-59.

2. R.I.Isayev, R.Atametov, R.Radjapovalarning “Telekommunikatsiya uzatish tizimlari”, Toshkent axborot texnologiyalari universiteti, Toshkent, 2011.

3. R.I.Isayev, D.X.Ibatova. “Multimediyali aloqa tarmoqlari”. Toshkent axborot texnologiyalari universiteti, Toshkent, 2019.

4. S. R. Ahuja and J. R. Ensor, "Coordination and Control of Multimedia Conferencing". IEEE Communications Magazine, Vol. 30, No.5, May 1992, pp. 38-43.

5. S.K.Ganiyev, A.A.Ganiyev, Z.T.Xudoyqulov. Kiberxavfsizlik asoslari: o‘quv qo‘llanma. – T.: «Aloqachi», 2020, 303 bet.