KONFERENSIYALAR.COM

ANJUMANLAR PLATFORMASI

IX RESPUBLIKA ILMIY-AMALIY KONFERENSIYASI

YANGI DAVR ILM-FANI: INSON UCHUN INNOVATSION G‘OYA VA YECHIMLAR

OKTYABR, 2025

ELEKTRON NASHR:
https://konferensiyalar.com

KONFERENSIYALAR.COM
ANJUMANLAR PLATFORMASI

YANGI DAVR ILM-FANI: INSON UCHUN INNOVATSION G‘OYA VA YECHIMLAR

IX RESPUBLIKA ILMIY-AMALIY KONFERENSIYASI MATERIALLARI

2025-yil, oktyabr

TOSHKENT-2025

Yangi davr ilm-fani: inson uchun innovatsion g‘oya va yechimlar. IX Respublika ilmiy-amaliy konferensiyasi materiallari to‘plami. 1-jild, 9-son (oktyabr, 2025-yil). – 71 bet.

Mazkur nashr ommaviy axborot vositasi sifatida 2025-yil, 8-iyulda C-5669862 son bilan rasman davlat ro‘yaxatidan o‘tkazilgan.

Elektron nashr: https://konferensiyalar.com

Konferensiya tashkilotchisi: “Scienceproblems Team” MChJ

Konferensiya o‘tkazilgan sana: 2025-yil, 23-oktyabr

Mas’ul muharrir:
Isanova Feruza Tulqinovna

Annotatsiya
Mazkur to‘plamda “Yangi davr ilm-fani: inson uchun innovatsion g‘oya va yechimlar” mavzusidagi IX Respublika ilmiy-amaliy konferensiyasi materiallari jamlangan. Nashrda respublikaning turli oliy ta’lim muassasalari, ilmiy markazlari va amaliyotchi mutaxassislari tomonidan tayyorlangan maqolalar o‘rin olgan bo‘lib, ular ijtimoiy-gumanitar, tabiiy, texnik va yuridik fanlarning dolzarb muammolari va ularning innovatsion yechimlariga bag‘ishlangan.
Ushbu nashr ilmiy izlanuvchilar, oliy ta’lim o‘qituvchilari, doktorantlar va soha mutaxassislari uchun foydali qo‘llanma bo‘lib xizmat qiladi.

Kalit so‘zlar: ilmiy-amaliy konferensiya, innovatsion yondashuv, zamonaviy fan, fanlararo integratsiya, ilmiy-tadqiqot, nazariya va amaliyot, ilmiy hamkorlik.

MUNDARIJA

MULTIMEDIALI ALOQA TARMOQLARIDA HUJUMLARNI ANIQLASHNING ILG‘OR TEXNOLOGIYALARI

Mirjalolova Nargiza Asqar qizi
Muhammad al-Xorazmiy nomidagi
Toshkent axborot texnologiyalari universiteti
Email: imirjalolov@gmail.com

Annotatsiya. Ushbu maqolada multimediali aloqa tarmoqlarida kiberhujumlarni aniqlashning ilg‘or texnologiyalari tahlil qilinadi. Tadqiqotda multimedia oqimlari – audio, video va ma’lumotlar uzatish jarayonida yuzaga keladigan tahdidlarni erta aniqlash uchun zamonaviy intellektual yondashuvlar, jumladan, mashinaviy o‘rganish va sun’iy intellekt usullari qo‘llaniladi. Taklif etilgan texnologiyalar tarmoq xavfsizligini oshirish, uzatish sifatini barqaror saqlash hamda tizim ishonchliligini ta’minlashga qaratilgan.

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.

ADVANCED TECHNOLOGIES FOR DETECTION OF ATTACKS IN MULTIMEDIA COMMUNICATION NETWORKS

Mirjalolova Nargiza Askar kizi
Tashkent University of Information Technologies named after Muhammad al-Khwarizmi

Annotatsiya. This article analyzes advanced technologies for detecting cyberattacks in multimedia communication networks. The study uses modern intelligent approaches, including machine learning and artificial intelligence methods, for early detection of threats that arise during the transmission of multimedia streams - audio, video and data. The proposed technologies are aimed at increasing network security, maintaining stable transmission quality and ensuring system reliability.

Keywords: Denial of Service (DoS) attacks, Man-in-the-Middle (MitM) attacks, Malware attacks, Spoofing attacks, Phishing attacks, Data injection attacks.

DOI: https://doi.org/10.47390/ydif-y2025v1i9/n03

Korporativ kompyuter tarmoqlarida axborot xavfsizligini ta’minlash masalalari asosan mahalliy ish stantsiyalari, lokal tarmoqlar xavfsizligi hamda korporativ tarmoqlarning umumiy axborot tizimlariga kirish imkoniyatiga ega bo‘lgan hujumlar bilan bog‘liq. Tarmoq hujumlari ularning maqsadlariga va qamroviga qarab turlicha namoyon bo‘ladi: ba’zilari murakkab texnik usullarni talab etsa, boshqalari oddiy operatorda ham amalga oshirilishi mumkin, hatto hujumchi uning oqibatlarini to‘liq anglamasligi ham ehtimoldir. Jinoyatchilarning asosiy maqsadlari quyidagilardan iborat bo‘lishi mumkin: uzatilayotgan axborotning maxfiyligini buzish; ma’lumotlarning yaxlitligi va ishonchliligini izdan chiqarish; butun tizim yoki uning ayrim qismlarining noto‘g‘ri ishlashiga sabab bo‘lish.

Taqsimlangan tizimlar ayniqsa masofaviy hujumlarga moyildir, chunki ularning komponentlari ko‘pincha ochiq kanal orqali ma’lumot uzatadi — bu esa hujumchiga nafaqat ma’lumotni passiv ravishda tinglash, balki uzatilayotgan trafikni faol ravishda o‘zgartirish imkonini beradi. Trafikka faol aralashuvni aniqlash mumkin bo‘lsa-da, passiv tinglash amalda ko‘pincha aniqlanmay qoladi. Bundan tashqari, taqsimlangan tizimlarda xizmatlararo axborot

almashinuvi ham foydalanuvchi ma’lumotlari kabi ochiq kanallar orqali o‘tishi sababli, xizmat ma’lumotlari ham hujum ob’ekti bo‘lib qoladi.

Masofaviy hujumlarni aniqlashning qiyinligi bunday noqonuniy xatti-harakatlarni xavf darajasi jihatidan birinchi o‘ringa chiqaradi va tahdidga tezkor javob berishni murakkablashtiradi, bu esa huquqbuzarning muvaffaqiyatga erishish ehtimolini oshiradi. Mahalliy tarmoqlar xavfsizligi Internet tarmog‘idan farq qiladi: mahalliy tarmoqlarda ruxsatsiz xatti-harakatlar ko‘pincha ro‘yxatdan o‘tgan foydalanuvchilar tomonidan sodir etilishi mumkin, chunki mahalliy kanallar nazorat ostidagi hududda joylashgan va ruxsatsiz ulanishlardan himoya asosan ma’muriy chora-tadbirlar orqali amalga oshiriladi.

Amalda IP tarmoqlari aloqa jarayoniga ruxsatsiz kirishning turli usullariga nisbatan zaif. Kompyuter va tarmoq texnologiyalarining (masalan, mobil Java ilovalari yoki ActiveX-kontrollar) rivojlanishi bilan birga IP tarmoqlariga qarshi mumkin bo‘lgan hujum turlari ham doimiy ravishda ko‘payib bormoqda.

Multimedia aloqa tarmoqlari bugungi hayotda muhim o‘rin tutadi: ular turli formatlardagi ma’lumotlarni uzatish va insonlar orasida muloqotni ta’minlaydi. Biroq, aynan shu funksiyalar tufayli multimediya tarmoqlari yomon niyatli sub’ektlar hujumlariga nisbatan sezgir. Ushbu maqolada biz multimediya aloqa tarmoqlariga qarshi eng ko‘p uchraydigan hujum turlarini va ularni oldini olish uchun qo‘llanishi mumkin bo‘lgan asosiy himoya choralarini tahlil qilamiz.

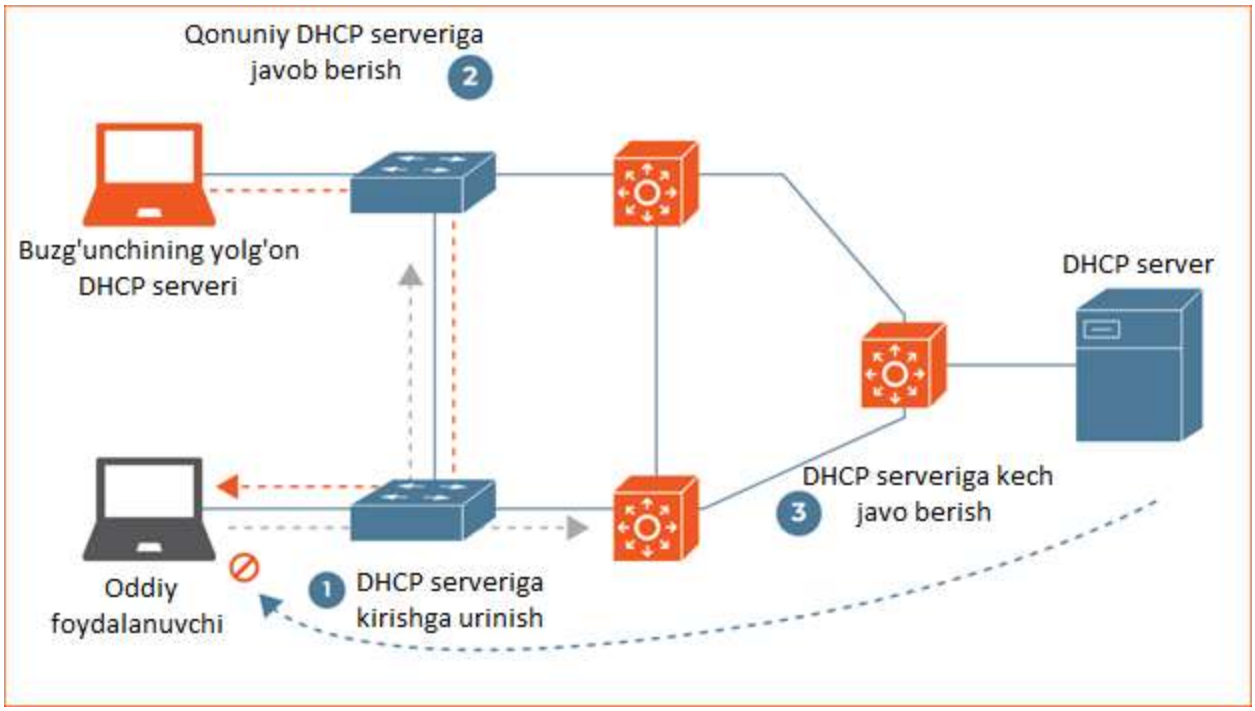
Korporativ va multimedia tarmoqlarida axborot xavfsizligi asosan mahalliy ish stantsiyalari, lokal tarmoqlar va korporativ tarmoqlarning markaziy resurslariga kirish imkonini beruvchi hujumlar bilan bog‘liq. Tarmoq hujumlari turlicha xususiyatga ega: ba’zilari yuqori texnik murakkablik talab etsa, boshqalari oddiy vositalar orqali ham amalga oshiriladi. Hujumchilarning asosiy maqsadlari — uzatilayotgan multimedia kontentining maxfiyligini buzish, ma’lumotlarning yaxlitligi va ishonchliligini buzish hamda butun xizmat yoki uning alohida qismlarini ishlashdan to‘xtatishdir.

Xizmat ko‘rsatishni rad etish (DoS) hujumlari multimedia tizimlarida ayniqsa xavflidir: hujumchi real-time audio va video oqimlarini yoki signalling kanalini trafik bilan to‘ldirib, xizmat sifatini pasaytiradi yoki butunlay uzilishlarga sabab bo‘ladi. Bunday hujumlarni aniqlash va bartaraf etish uchun ilg‘or usullar — trafikni profilga solish, anomal trafikni aniqlovchi va bloklovchi filtrlar, shuningdek, sun’iy intellekt asosidagi trafikka nazorat va avtomatik mitigatsiya platformalaridan foydalanishdir.

Man-in-the-Middle (MitM) hujumlarida tajovuzkor ikki tomon o‘rtasidagi real-vaqtli multimedia almashinuvini ushlab, tinglashi yoki mazmunni o‘zgartirishi mumkin. Bu turdagi hujumlarni aniqlash uchun sessiya va kriptografik kalitlar butunligi tekshiruvi, TLS/DTLS inspeksiyasi, o‘rnatilgan signallarning o‘zaro mosligini tekshirish va anomaliyalarni aniqlovchi monitoring tizimlari (masalan, behaviour-based IDS) samarali hisoblanadi.

Zararli dasturiy ta’minot (malware) esa ko‘pincha qurilmalarga yoki serverlarga zarar yetkazish, sessiya ma’lumotlarini o‘g‘irlash yoki videostream’ni buzish uchun qo‘llaniladi. Ularni aniqlash uchun an’anaviy antiviruslardan tashqari, tarmoq qatlami va ilova qatlami telemetriyalarini tahlil qiluvchi uddaburon (advanced) malware detection tizimlari, xatti-harakatlardan kelib chiqib tahdidlarni aniqlaydigan mashinaviy o‘rganish yechimlari kerak bo‘ladi. Muhim chora — dasturiy ta’minotni va xavfsizlik yamoqlarini doimiy yangilab borishdir.

Spoofing (IP/MAC/ARP soxtalashtirish) hujumlari esa multimedia kanallarida xabarlarning noto‘g‘ri manbadan kelganday ko‘rinishiga olib keladi va xususan DHCP-ga asoslangan aldovlar orqali tarmoq konfiguratsiyasini egallashga sabab bo‘ladi. Masalan, soxta DHCP server mijozlarga noto‘g‘ri shlyuz yoki DNS ma’lumotlarini o‘tkazib, trafikni yo‘naltirib MitM holatini yaratishi mumkin. Bunday hujumlarni oldini olish uchun DHCP snooping, dinamik ARP-inspektsiyasi, port-security va 802.1X kabi tarmoq qatlamidagi autentifikatsiya va filtratsiya mexanizmlari, shuningdek konfi guratsiyalarni qattiq nazorat qilish va tarmoq bo‘ylab tafovutlarni real-vaqt kuzatish tavsiya etiladi. Umuman olganda, multimediya tarmoqlariga qarshi hujumlarni aniqlash va ularga qarshi kurashish uchun ilg‘or texnologiyalar quyidagilarni o‘z ichiga oladi: signatura-asosli va anomaliya-asosli IDS/IPS tizimlari, sun’iy intellekt va mashinaviy o‘rganish asosida trafikni tahlil qilish, real-vaqtli telemetriya yig‘ish, kriptografik himoya (TLS/DTLS) va tarmoq qatlamida kuchli autentifikatsiya (802.1X, DHCP snooping). Bunday kombinatsiya real-time multimedia xizmatlarining sifatini saqlagan holda tarmoqlardagi tahdidlarni erta aniqlash va tezkor mitigatsiyalash imkonini beradi.



1-rasm. DHCP serveriga spoofing hujumi

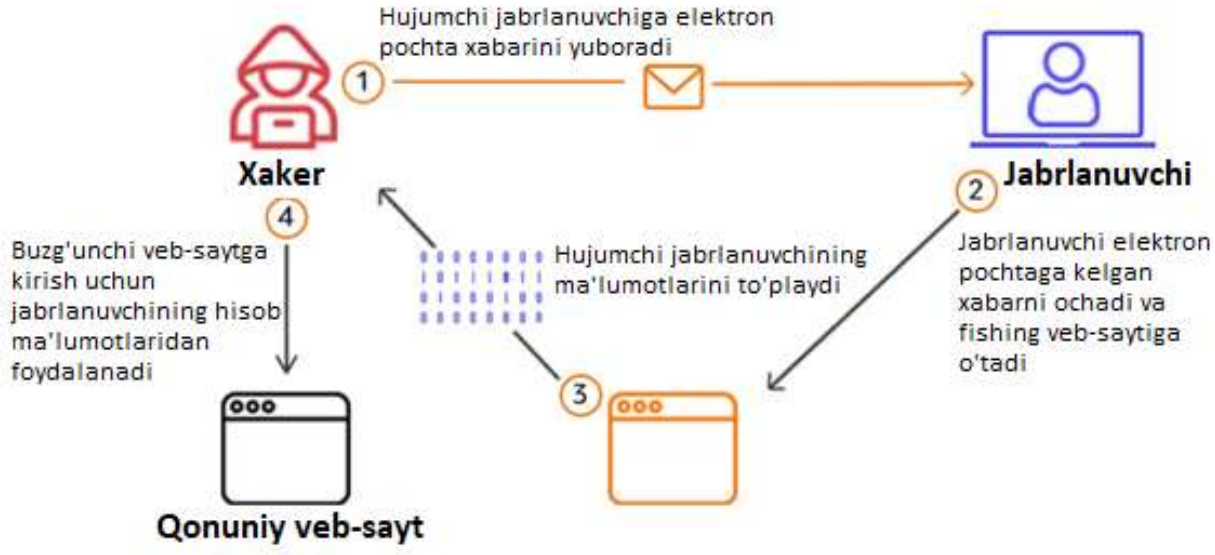
Spoofing hujumlariga qarshi turish uchun tarmoq ma'murlari kengaytiriladigan autentifikatsiya protokoli (EAP) yoki Secure Shell (SSH) kabi autentifikatsiya protokollaridan foydalanishi mumkin.

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.

Adabiyotlar/Литература/References:

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.

KONFERENSIYALAR COM
ANJUMANLAR PLATFORMASI

YANGI DAVR ILM-FANI: INSON UCHUN INNOVATSION G‘OYA VA YECHIMLAR

IX RESPUBLIKA ILMIY-AMALIY KONFERENSIYASI MATERIALLARI

2025-yil, oktyabr

Mas’ul muharrir: *F.T.Isanova*
Texnik muharrir: *N.Bahodirova*
Diszayner: *I.Abdihakimov*

Yangi davr ilm-fani: inson uchun innovatsion g‘oya va yechimlar.
IX Respublika ilmiy-amaliy konferensiyasi materiallari to‘plami.
1-jild, 9-son (oktyabr, 2025-yil). – 71 bet.

Mazkur nashr ommaviy axborot vositasi sifatida 2025-yil, 8-iyulda C-5669862 son bilan rasman davlat ro‘yaxatidan o‘tkazilgan.

Elektron nashr: https://konferensiyalar.com

Konferensiya tashkilotchisi: “Scienceproblems Team” MChJ

Konferensiya o‘tkazilgan sana: 2025-yil, 23-oktyabr