TOSHKENT AXBOROT TEXNOLOGIYALARI UNIVERSITETI HUZURIDAGI ILMIY DARAJALAR BERUVCHI DSc.09/2025.27.12. T.01.01.M RAQAMLI ILMIY KENGASH

MIRZO ULUG‘BEK NOMIDAGI O‘ZBEKISTON MILLIY UNIVERSITETINING JIZZAX FILIALI

JO‘RAYEV MA’RUF TO‘RAQUL O‘G‘LI

KOMPYUTER TARMOQLARINING MA’LUMOTLAR OQIMINI MONITORING QILISHNING ALGORITMLARI VA DASTURIY TA’MINOTI

05.01.04 - Hisoblash mashinalari, majmualari va kompyuter tarmoqlarining matematik va dasturiy ta’minoti

TEXNIKA FANLARI BO‘YICHA FALSAFA DOKTORI (PhD) DISSERTATSIYASI AVTOREFERATI

Toshkent – 2026

UDK: 004.042

**Texnika fanlari bo‘yicha falsafa doktori (PhD)
dissertatsiyasi avtoreferati mundarijasi**

**Оглавление автореферата диссертации
доктора философии (PhD) по техническим наукам**

**Contents of dissertation abstract of doctor of philosophy (PhD)
on technical sciences**

TOSHKENT AXBOROT TEXNOLOGIYALARI UNIVERSITETI HUZURIDAGI ILMIY DARAJALAR BERUVCHI DSc.09/2025.27.12. T.01.01.M RAQAMLI ILMIY KENGASH

MIRZO ULUG‘BEK NOMIDAGI O‘ZBEKISTON MILLIY UNIVERSITETINING JIZZAX FILIALI

JO‘RAYEV MA’RUF TO‘RAQUL O‘G‘LI

KOMPYUTER TARMOQLARINING MA’LUMOTLAR OQIMINI MONITORING QILISHNING ALGORITMLARI VA DASTURIY TA’MINOTI

05.01.04 - Hisoblash mashinalari, majmualari va kompyuter tarmoqlarining matematik va dasturiy ta’minoti

TEXNIKA FANLARI BO‘YICHA FALSAFA DOKTORI (PhD) DISSERTATSIYASI AVTOREFERATI

Toshkent – 2026

Texnika fanlari bo‘yicha falsafa doktori (PhD) dissertatsiyasi mavzusi O‘zbekiston Respublikasi Oliy ta’lim, fan va innovatsiyalar vazirligi huzuridagi Oliy attestatsiya komissiyasida B2025.3.PhD/T5882 raqam bilan ro‘yxatga olingan.

Dissertatsiya Mirzo Ulug‘bek nomidagi O‘zbekiston Milliy universitetining Jizzax filialida bajarilgan. Dissertatsiya avtoreferati uch tilda (o‘zbek, rus, ingliz (rezyume)) Ilmiy kengash veb-sahifasi (www.tuit.uz) va «Ziyonet» axborot-ta’lim portalida (www.ziyonet.uz) joylashtirilgan.

Ilmiy rahbar:	**Kabulov Anvar Vasilovich** texnika fanlari doktori, professor
Rasmiy opponentlar:	**Djumanov Jamoljon Xudaykulovich** texnika fanlari doktori, professor
	Muxamediyeva Dilnoz Tulkunovna texnika fanlari doktori, professor
Yetakchi tashkilot:	**Sharof Rashidov nomidagi Samarqand davlat universiteti**

Dissertatsiya himoyasi Toshkent axborot texnologiyalari universiteti huzuridagi DSc.09/2025.27.12. T.01.01.M raqamli Ilmiy kengashning 2026 yil «12» fevral da soat 14^{00} dagi majlisida bo‘lib o‘tadi. (Manzil: 100202, Toshkent shahri, Amir Temur ko‘chasi, 108-uy. Tel.: (99871) 238-64-43; faks: (99871) 238-65-52; e-mail: tuit@tuit.uz).

Dissertatsiya bilan Toshkent axborot texnologiyalari universitetining Axborot-resurs markazida tanishish mumkin (406 raqam bilan ro‘yxatga olingan). Manzil: 100202, Toshkent shahri, Amir Temur ko‘chasi, 108-uy. Tel.: (99871) 238-64-43).

Dissertatsiya avtoreferati 2026 yil «2» fevral kuni tarqatildi.
(2026 yil «2» fevral dagi 3 raqamli reestr bayonnomasi).

M.M.Musayev
Ilmiy darajalar beruvchi ilmiy kengash raisi,
texnika fanlar doktori, professor

E.Sh.Nazirova
Ilmiy darajalar beruvchi ilmiy kengash
ilmiy kotibi, texnika fanlar doktori, professor

Dj.B.Sultanov
Ilmiy darajalar beruvchi ilmiy kengash qoshidagi
ilmiy seminar raisi, texnika fanlar doktori, dotsent

KIRISH (falsafa doktori (PhD) dissertatsiyasi annotatsiyasi)

Dissertatsiya mavzusining dolzarbligi va zarurati. Jahon tajribasi shuni ko‘rsatadiki, kompyuter tarmoqlarida ma’lumotlar oqimi va ularni tashkil etuvchi paketlarni monitoring qilish usullari axborot tizimlarini samarali boshqarish hamda ularning ishonchliligini ta’minlash muammosi alohida ahamiyat ega. Tarmoq oqimini kuzatish jarayonida tizimli tahlil va statistik qayta ishlash metodlari qo‘llanilishi tarmoq samaradorligini oshirish bilan birga, uzatilayotgan ma’lumotlarning yaxlitligi va ishonchliligini ta’minlash imkonini beradi. Shuningdek, tarmoq paketlarini chuqur tahlil qilishga asoslangan ilg‘or algoritmlar va dasturiy ta’minot majmualari yordamida axborot tizimlarida yuzaga kelishi mumkin bo‘lgan xatoliklar va nosozliklar erta bosqichda aniqlanishi va ularni bartaraf etish imkoniyatini kengaytiradi. Bunday tizimlarda paketlarni qayta ishlash va qoidalarga asoslangan tarmoq monitoringi dolzarb masalalardan biri bo‘lib hisoblanadi.

Jahon tajribasiga asosan kompyuter tarmoqlarining ma’lumotlar oqimini monitoring qilish natijalarini o‘rganish shuni ko‘rsatadiki, tarmoq oqimlarini tahlil qilish, qayta ishlash, algoritmlar va dasturiy vositalarni ishlab chiqishga qaratilgan vazifalar dolzarbdir. Tarmoq oqimlarini monitoring qilish algoritmlari real vaqt rejimida tarmoqlardagi kiruvchi va chiquvchi oqimlarni kuzatib, tarmoq holatini tahlil qilish imkonini beradi. Axborot tizimlarida tarmoq oqimlarini samarali boshqarish va nazorat qilish bo‘yicha keng qamrovli chora-tadbirlar amalga oshirilmoqda. Jumladan, monitoring dasturlari, tarmoq barqarorligini ta’minlash vositalari va zamonaviy axborot texnologiyalarining so‘nggi yutuqlari asosida turli ilmiy va amaliy tadqiqotlar olib borilmoqda. Xususan tarmoq oqimlarini tashkil etuvchi paketlarni tahlili qilishda asosiy yondashuvlar paketlarni yuzaki tahlili, paketlarni o‘rta darajadagi tahlili va paketlarni chuqur tahlili hisoblanadi. Paketlarni tahlil qilishda asosan qayta ishlanmagan paketlar ustida tahlil amalga oshiriladi. Bu esa tarmoq holatini aniqlashda samaradorlikni pasaytiradi va natijada tarmoq oqimlari monitoringiga salbiy ta’sir ko‘rsatadi. Shu sababli paketlarni qayta ishlash algoritmlarini va tarmoq oqimlarini monitoring qilish qoidalarini ishlab chiqish dolzarb hisoblanadi.

Respublikamizda so‘nggi yillarda raqamli axborot hajmi jadal sur’atlar bilan ortib bormoqda. Kompyuter tarmoqlarida ma’lumotlar oqimini monitoring qilish talablari va xususiyatlarini hisobga olgan holda tarmoq oqimlarini monitoring qilish algoritmlari va qoidalari hozirgi vaqtda yetarli darajada o‘rganilmagan. Ushbu ish tarmoq oqimlarini monitoring qilish algoritmlari va dasturlarini ishlab chiqishning ilmiy-texnik muammolarini hal qilishga qaratilgan.

Respublikamizda davlat dasturlari va strategiyalarini amalga oshirish asosida kompyuter tarmoqlarining ishonchliligini ta’minlash hamda mahalliy dasturiy vositalar bozorini rivojlantirish bo‘yicha chora-tadbirlar amalga oshirilmoqda. O‘zbekiston Respublikasi Prezidentining 2025-yil 16-sentabrdagi PQ-286-son “Respublikaning hudud, soha va tarmoqlarida raqamli texnologiyalar joriy etilishini yanada jadallashtirish chora-tadbirlari to‘g‘risida”, 2018-yil 21-noyabrdagi PQ-4024-son “Axborot texnologiyalari va kommunikatsiyalarining joriy etilishini

nazorat qilish, ularni himoya qilish tizimini takomillashtirish chora-tadbirlari to‘g‘risida” va 2022-yil 28-yanvardagi PF-60-son “2022 — 2026-yillarga mo‘ljallangan Yangi O‘zbekistonning taraqqiyot strategiyasi to‘g‘risida”gi farmon va qarorlari hamda mazkur faoliyatga tegishli boshqa me’yoriy-huquqiy hujjatlarda belgilangan vazifalarni amalga oshirishda ushbu tadqiqot ishi ham ilmiy va amaliy jihatdan muayyan darajada xizmat qiladi.

Tadqiqotning respublika fan va texnologiyalari rivojlanishi-ning ustuvor yo‘nalishlariga mosligi. Mazkur tadqiqot respublika fan va texnologiyalar rivojlanishining IV. “Axborotlashtirish va axborot-kommunikatsiya texnologiyalarini rivojlantirish” ustuvor yo‘nalishi doirasida bajarilgan.

Muammoning o‘rganilganlik darajasi. Dunyoning rivojlangan davlatlarida, xususan, AQSh, Xitoy, Rossiya, Yaponiya, Janubiy Koreya, Germaniya va boshqa davlatlarda axborot tizimlarida tarmoq ma’lumotlar oqimini monitoring qilish va paket ma’lumotlarini tahlil qilish bo‘yicha ilmiy izlanishlar olib borilmoqda. Xususan, R.I.Pasechnikov, D.V.Kostin, K.Zhou, O.I.Sheluxin, R.A.Sudarikov, H.Kim, K.C.Claffy, M.Fomenkov, G.Jain, D.Barman, N.Medhi, M.Faloutsos, M.Tahboush, V.Pallavi va boshqalarning ilmiy ishlarida ham ushbu masalalar tadqiq qilingan.

Respublikamizda esa bu muammolarni hal qilishda yetakchi olimlaridan Sh.X.Fozilov, T.F.Bekmuratov, M.M.Musayev, X.N.Zaynidinov, U.R.Xamdamov, K.A.Tashev, Sh.R.G‘ulomov, J.X.Djumanov va boshqa olimlar o‘zlarining katta hissasini qo‘shgan.

Adabiyotlarni tahlil qilish natijalariga ko‘ra, kompyuter tarmoqlarida ma’lumotlar oqimini monitoring qilish, sinflarga ajratish algoritmlari va kutilmagan holatlarni aniqlash talablarini hisobga olgan holda, kompyuter tarmoqlarida ma’lumotlar oqimlarni monitoring qilish masalasi yetarli darajada o‘rganilmagan.

Dissertatsiya tadqiqotining dissertatsiya bajarilgan oliy ta’lim muassasasining ilmiy–tadqiqot ishlari rejalari bilan bog‘liqligi. Ushbu dissertatsiya ishi Mirzo Ulug‘bek nomidagi O‘zbekiston Milliy universitetida olib borilgan № F-OT-2021-248 “Funksional jadvallar asosida axborotni himoya qilishni ta’minlashda tahdidlarni aniqlash, identifikasiya qilish va zararsizlantirishning intellektual usullari va texnologiyalarini ishlab chiqish” (2022-2024) ilmiy-tadqiqot ishi doirasida amalga oshirilgan.

Tadqiqotning maqsadi. Kompyuter tarmoqlarida ma’lumotlar oqimini monitoring qilishning produksion qoidalarga asoslangan algoritmlari va dasturiy vositasini ishlab chiqish hisoblanadi.

Tadqiqotning vazifalari:

tarmoq oqimidan informativ belgilarni ajratib olish, oqim atributlarini hisoblash, paketlarni sinflarga ajratishda tasniflash va ustuvorlik algoritmlarini ishlab chiqish;

tarmoq oqimidagi kutilmagan holatlarni aniqlash uchun statistik ko‘rsatkichlarni uyg‘unlashtirgan holda uchta holatdan iborat Markov zanjirini taklif etish;

Petri tarmoqlari yordamida TCP protokolining ishonchliligini modellashtirish, dekompozitsiya algoritmi asosida matematik ta’minotini ishlab chiqish;

produksion qoidalar asosida tarmoq oqimlarini monitoring qilish va qaror qabul qilishni qo‘llab-quvvatlash uchun bilimlar bazasi va dasturiy vositani yaratish.

Tadqiqotning obyekti sifatida axborot tizimlaridagi kompyuter tarmoqlarining ma’lumotlar oqimi va tarmoq oqimini monitoringini olib boruvchi dasturiy vositalari tanlangan.

Tadqiqotning predmeti tarmoq oqimini real vaqt rejimida tahlil qilish, tasniflash, nazorat qilish va boshqarishda qo‘llaniladigan matematik usullar, algoritmlar va dasturiy vositalar hisoblanadi.

Tadqiqotning usullari. Tadqiqotlar jarayonida tarmoq oqimi ma’lumotlarini qayta ishlash, qiyosiy tahlil, tizimli tahlil, sinflashtirish usullari va statistik tahlil usullari hamda dasturlash texnologiyalaridan foydalanilgan.

Tadqiqotning ilmiy yangiligi quyidagilardan iborat:

tarmoq oqimidan informativ belgilarni ajratib olish hamda oqim atributlarini hisoblash asosida paketlarni sinflarga ajratishning tasniflash va ustuvorlik algoritmlari ishlab chiqilgan;

tarmoq oqimidagi kutilmagan holatlarni aniqlash uchun statistik ko‘rsatkichlarni uyg‘unlashtirgan holda uchta holatdan iborat Markov zanjiri taklif etilgan;

Petri tarmog‘i asosida tarmoqdagi kutilmagan uzilishlarni aniqlashning matematik ta’minoti ishlab chiqilgan;

produksion qoidalar asosida tarmoq oqimlarini monitoring qilish va qaror qabul qilishni qo‘llab-quvvatlash uchun bilimlar bazasi va dasturiy vosita yaratilgan.

Tadqiqotning amaliy natijalari quyidagilardan iborat:

ma’lumotlar oqimini monitoring qilish va qayta ishlash algoritmlari ishlab chiqilgan;

mavjud va ishlab chiqilgan algoritmlar asosida tarmoq oqimlaridagi kutilmagan holatlarni aniqlash va tasniflashni amalga oshiruvchi dasturiy ta’minot yaratilgan;

tarmoq oqimlarini produksion qoidalar asosida tahlil qilishda qoidalar ishlab chiqilgan bo‘lib, bu tarmoq holatini baholash imkonini beradi.

Tadqiqot natijalarining ishonchliligi. Tadqiqot natijalarining ishonchliligi tarmoq oqimini tahlil qilishda ishlab chiqilgan algoritmlarning to‘g‘riligi, o‘rganilayotgan tarmoq oqimi tahlil natijalarining umumqabul qilingan mezonlar asosida qiyosiy tahlili, shuningdek, ishlab chiqilgan dasturiy vosita yordamida olingan tajriba natijalari bilan tasdiqlangan.

Tadqiqot natijalarining ilmiy va amaliy ahamiyati. Tadqiqot natijalarining ilmiy ahamiyati, tarmoq oqimini real vaqt rejimida tahlil qilish bo‘yicha kompleks yondashuv, algoritmlari va dasturiy vosita ishlab chiqilganligi bilan izohlanadi.

Tadqiqot natijalarining amaliy ahamiyati yaratilgan dasturiy vosita yordamida axborot tizimlarida ma’lumotlar oqimlarini real vaqt rejimida kuzatish, tarmoq faoliyatidagi nosozliklarni erta aniqlash va tizim barqarorligini oshirish bilan izohlanadi.

Tadqiqot natijalarining joriy qilinishi. Tadqiqotda ishlab chiqilgan tarmoq oqimi ma’lumotlarini monitoring qilish algoritmlari va dasturiy ta’minoti asosida amalga oshirilgan joriy etish natijalari:

kompyuter tizimlarida ma’lumotlar oqimini monitoring qilishning produksion qoidalarga asoslangan algoritmlari asosidagi dasturiy vositasi Raqamli texnologiyalar vazirligi Surxondaryo viloyat hududiy sho‘basida tarmoq oqimini monitoring qilishda hamda paketlarni tasniflash orqali tarmoqqa kirib keluvchi ma’lumotlarni tahlil qilib erta qaror qabul qilishni qo‘llab-quvvatlash vaqtini qisqartirish maqsadida joriy etilgan (Surxondaryo viloyati hokimligining 2025-yil 26-sentabrdagi 07-07/8583-sonli ma’lumotnomasi). Natijada dasturiy vositaga yuz mingdan ortiq tarmoq oqimi paketlari yuborilib, monitoring jarayonida ishlab chiqilgan algoritm o‘rtacha 7% ga erta qaror qabul qilish imkoniyatini bergan;

tadqiqot ishida tarmoqdagi kutilmagan holatlarni aniqlashda ishlab chiqilgan produksion qoidalar asosidagi algoritmi Surxondaryo viloyati statistika boshqarmasining Raqamlashtirish va statistik registrlarni yuritish bo‘limida joriy etilgan (Surxondaryo viloyati hokimligining 2025-yil 26-sentabrdagi 07-07/8583-sonli ma’lumotnomasi). Natijada ishlab chiqilgan algoritm ma’lumotlarni uzatishdagi kutilmagan holatlarni aniqlashda 7% ga yaxshiroq natija ko‘rsatgan;

shuningdek tarmoq oqimini monitoring qilishda hamda paketlarni tasniflash orqali tarmoqqa kirib keluvchi ma’lumotlarni tahlil qilib erta qaror qabul qilishni qo‘llab-quvvatlash vaqtini qisqartirish maqsadida Surxondaryo viloyatigi IT park Termiz filialida joriy etilgan (Surxondaryo viloyati hokimligining 2025-yil 26-sentabrdagi 07-07/8583-sonli ma’lumotnomasi). Dasturiy vositaga bir milliontadan ortiq tarmoq oqimi paketlari yuborildi, monitoring jarayonida ishlab chiqilgan algoritm o‘rtacha 8% ga erta qaror qabul qilish imkoniyatini bergan.

Tadqiqot natijalarining aprobatsiyasi. Tadqiqotlar natijalari 5 ta xalqaro, 9 ta respublika ilmiy-amaliy konferensiyalar hamda ilmiy seminarlarda muhokama qilingan.

Tadqiqot natijalarining e’lon qilinganligi. Tadqiqot mavzusi bo‘yicha jami 29 ta ilmiy ish nashr qilingan, shulardan 8 ta maqola O‘zbekiston Respublikasi Oliy attestatsiya komissiyasining dissertatsiyalar asosiy ilmiy natijalarini chop etish tavsiya etilgan ilmiy nashrlarda, shu jumladan 3 ta xorijiy va 5 ta respublika miqyosidagi ilmiy jurnallarda chop etilgan hamda 7 ta EHM uchun dasturiy ta’minotlarga guvohnoma olingan.

Dissertatsiyaning tuzilishi va hajmi. Dissertatsiya kirish, to‘rtta bob, xulosa, foydalanilgan adabiyotlar ro‘yxati va ilovalardan iborat. Dissertatsiyaning hajmi 120 betni tashkil etadi.

DISSERTATSIYANING ASOSIY MAZMUNI

Kirish qismida dissertatsiya mavzusining dolzarbligi va zaruriyati asoslangan, tadqiqotning O‘zbekiston Respublikasi fan va texnologiyalar taraqqiyotining ustuvor yo‘nalishlariga mosligi ko‘rsatilgan, tadqiqotning maqsad va vazifalari belgilab olingan hamda tadqiqot obyekti va predmeti aniqlangan, olingan natijalarning ishonchliligi asoslab berilgan, ularning nazariy va amaliy ahamiyati,

tadqiqot natijalarini amalda joriy qilish holati, nashr etilgan ishlar va dissertatsiya tuzilishi bo‘yicha ma’lumotlar keltirilgan.

Dissertatsiyaning “**Tarmoq oqimi ma’lumotlariga va Pcap fayllariga qayta ishlov berish usullari hamda dasturiy vositalari analitik tahlili”** deb nomlangan birinchi bobi uchta paragrafdan iborat bo‘lib, unda tarmoq oqimi ma’lumotlariga ishlov berishning tahlil usullari, oqim ma’lumotlarini qayta ishlashda dasturiy vositalar tahlili, oqim ma’lumotlari asosi bo‘lgan paket xususiyatlarni ajratishda pcap fayl tahlili va tarmoq oqimini real vaqtda tahlil qilish usullari tahlili keltirilgan. O‘rganish natijalari asosida solishtirma tahlil qilindi.

Paketlarni yozib olishda dasturiy vositalar quyidagi algoritmdan foydalanadi:

1. Paket oqimini aniqlashda tarmoqdan kelayotgan barcha paketlarni ketma-ketlik sifatida belgilanadi: $P_{pcap} = \{p_{pcap_1}, p_{pcap_2}, p_{pcap_3}, \dots, p_{pcap_n}\}$ bu yerda p_{pcap_i} i-paketning butun baytlar ketma-ketligini bildiradi.

2. Vaqt tamg‘asi qo‘yish har bir paket kelgan vaqtini belgilashdir. $V = \{v_1, v_2, v_3, \dots, v_n\}$ bu yerda v_i — paket p_{pcap_i} kelgan aniq vaqt (sekund va mikrosekundlarda) yozib qo‘yadi.

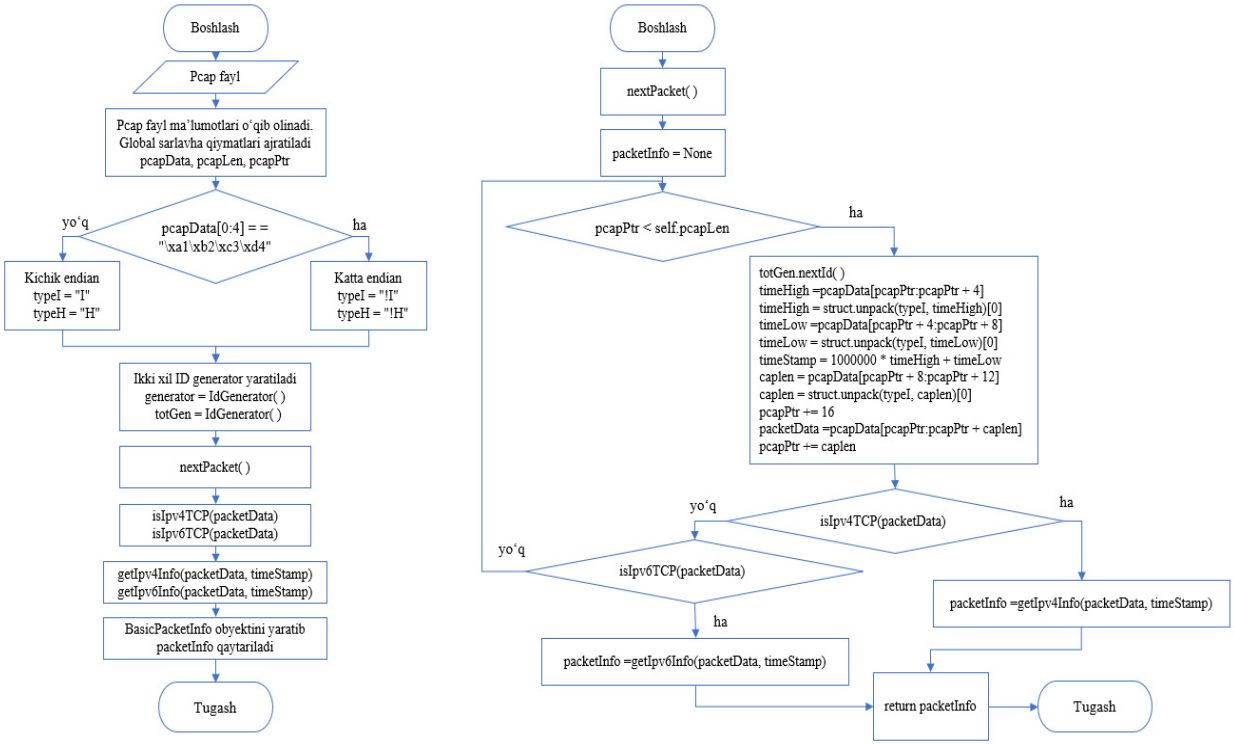
3. Pcap fayl tuzilmasi Global header qismi quyidagicha aniqlanadi. $H_g = (magic\_number, version\_major, version\_minor, thiszone, sigfigs, snaplen, network)$. Har bir paket $R_i = (ts\_\text{sec}_i, ts\_usec_i, incl\_len_i, orig\_len_i, p_{pcap_i})$ bu yerda $ts\_\text{sec}_i - v_i$ ning sekund qismi, $ts\_usec_i - v_i$ ning mikrosekund qismi, $incl\_len_i$ yozilgan paket uzunligi (baytlarda), $orig\_len_i$ asl paket uzunligi, p_{pcap_i} paketning xom bayt ma’lumotlari.

4. Saqlash algoritmi $PCAP = H_g \parallel \parallel_{i=1}^{n} R_i$ bu yerda $\parallel$ — ketma-ket qo‘shish amali hisoblanadi.

5. Algoritm bosqichlari tarmoq interfeysini promiscuous/monitor rejimga o‘tkazish $mode \leftarrow promiscuous$, global header yozish $write(H_g)$, har bir kelgan paket uchun vaqtni o‘lchash $v_i \leftarrow timestamp(p_{pcap_i})$, uzunliklarni hisoblash $incl\_len_i, orig\_len_i$, yozuv hosil qilish: $R_i \leftarrow (ts_{\text{sec}_i}, ts_{useci}, incl_{len_i}, orig\_len_i, p_{pcap_i})$, faylga qo‘shish $append(R_i)$, faylni yopish $close(PCAP)$.

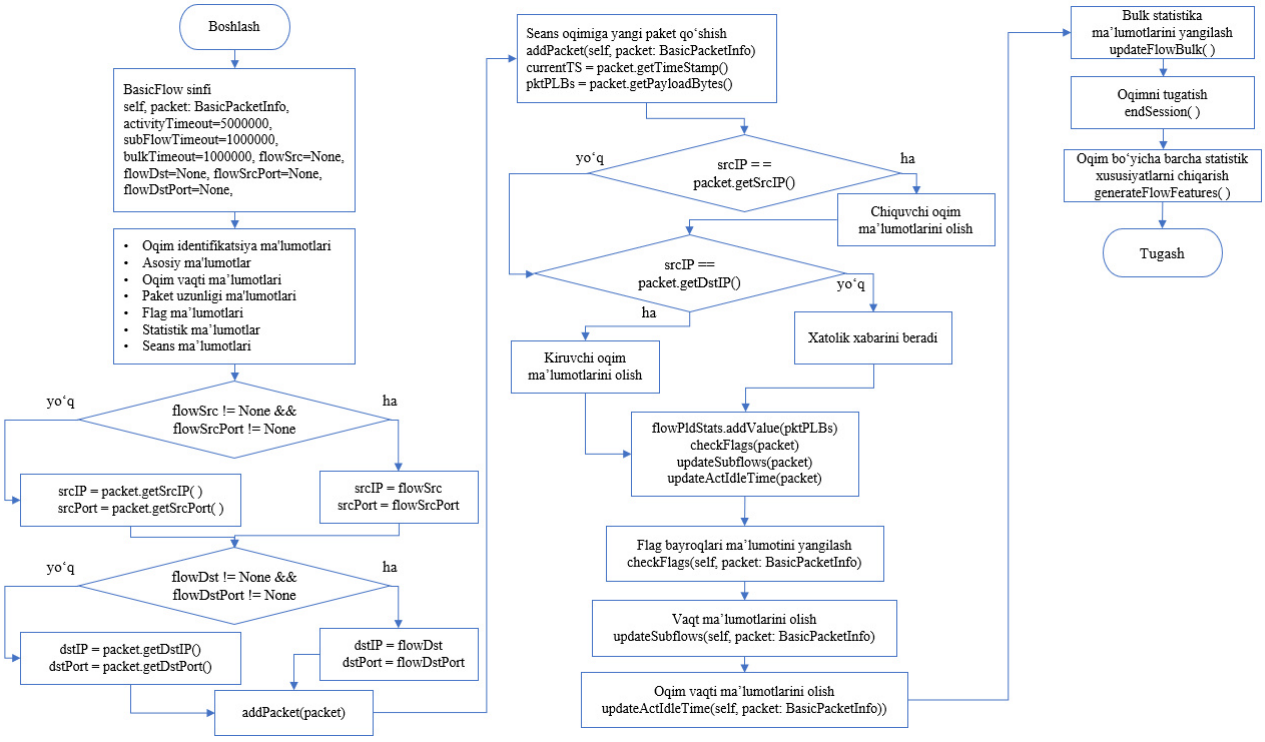
Barcha dasturiy vositalar deyarli shu taxlit ishlaydi. Faqat ma’lumotlarni saqlash formati, interfeys ko‘rinishi bilan farq qiladi. Tarmoq oqimini tahlil qilish tarmoq paketlarini real vaqt rejimida ularning mazmuniga qarab yig‘ish, qayta ishlash, tasniflash, nazorat qilish va o‘zgartirish imkonini beruvchi texnologiyalar hisoblanadi. Tarmoq oqimini tahlil qilish vositalarini rivojlanishiga ko‘ra tahlil algoritmlari va yondashuvlarining rivojlanishiga ajratiladi. Tahlil qilish vazifani samarali hal qilish uchun dasturiy-apparat vositalarining rivojlanishi muhimdir.

Dissertatsiyaning **“Tarmoq oqimidagi informativ belgilarni tanlash va sinflashtirish algoritmlarini ishlab chiqish”** nomli ikkinchi bobida tarmoq oqimidagi informativ belgilar to‘plamini aniqlash uchun paket xususiyatlarini tahlil qilishda, tarmoq oqimi orqali o‘tuvchi paket xususiyatlari tahlil qilinib oqim sifatida shakllantirish algoritmlari ishlab chiqildi. Algoritmda paket ma’lumotlari olinadi va statistik xususiyatlari hisoblanadi. SummaryStatistics sinfi statistik ko‘rsatkichlarni hisoblash uchun quyidagi metodlardan foydalanildi.



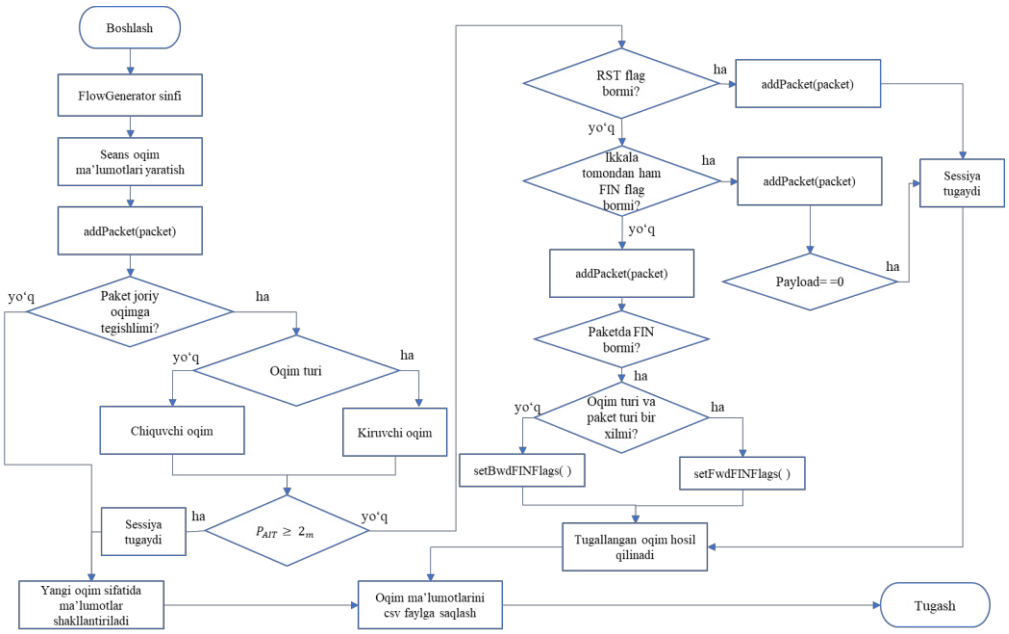
1-rasm. Pcap faylni o‘qish va paket xususiyatlarni ajratish algoritmi.

1-rasmdagi algoritmga ko‘ra pcap fayl strukturasi bo‘yicha global sarlavha, paket sarlavhasi va paket ma’lumotlari o‘qib olinadi. TCP flaglari $flags = \sum_{i=0}^{7} bit_i 2^i$ bilan hisoblanadi. Berilgan algoritm asosida global sarlavha ma’lumoti asosida pcap fayl turi aniqlanadi va nextPacket( ) metodi orqali har bir paket ma’lumotlari olinadi.



2-rasm. Tarmoq oqimini hosil qilish algoritmi.

Tarmoq oqimini hosil qilish 2-rasmda keltirilgan algoritm bo‘yicha amalga oshadi. Bunda, tahlil qilinayotgan paketlar oqim identifikatori bo‘yicha qaysi oqimga tegishli bo‘lsa, shu oqim ma’lumotlari yangilanib boradi.

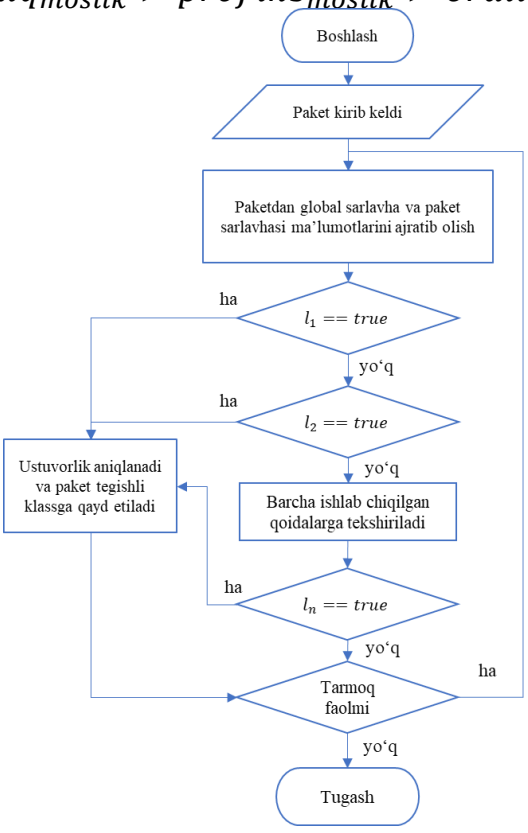


3-rasm. Oqimni hosil qilish va csv faylga yozish algoritmi.

Paketlardan sessiya oqimlarini yig‘ish, tugallangan oqimlarni saqlash va ularning xususiyatlarini csv faylga yozish uchun 3-rasm keltirilgan algoritmdan foydalaniladi. Oqim tugallangan bo‘lsa csv faylga yozib boriladi, agar tugallanmagan bo‘lsa yangi paket oqimga qo‘shiladi. Jarayon pcap fayldan o‘qilgan paket ma’lumotlari tugamaguncha davom etadi.

Paketlar asosida klassikatsiya qilishda bitta paket bir vaqtning o‘zida bir nechta klassifikatsiya tushushi mumkin. Shuning uchun qoidalar ishlaganda ularga ustuvorlik berildi.

$$Aniq_{moslik} > prefiks_{moslik} > oraliq_{moslik} \quad (1)$$



4-rasm. Paketlarni tasniflash algoritmi.

Paket hajmlari bo‘yicha klassifikatsiya juda muhim ma’lumotlarni beradi. 4-rasmda paketlarni tasniflash algoritmi berilgan. Agar paketni 2-formuladagi kabi tartiblangan bo‘lsa paket hajm katta bo‘lsa, keyingi paket hajmlar esa tezlik jihatidan kamayib boradi. Agar bu jarayon sodir bo‘lmasa demak tarmoqda ehtimoliy hujum sodir bo‘lishi mumkin deb faraz qilishga sabab bo‘ladi.

$$L_{to‘plami} = \{l_1, l_2, \dots, l_n\} \quad (2)$$

Tarmoq oqimi ma’lumotlarini yig‘ib olish va tahlil qilishda birinchidan kirib kelayotgan tarmoq oqimi ma’lumotlarini ishlab chiqilgan dasturiy vosita yordamida yozib olindi. Yozib olingan ma’lumot pcap fayl formatida saqlanadi. Ikkinchidan pcap faylda saqlangan ma’lumotlar ishlab chiqilgan algoritm asosida o‘qib olinadi, o‘qilgan ma’lumotdan 89 xil xususiyatlar ajratib olinib csv fayl formatida qayta saqlanadi.

Csv fayldagi ma’lumotlar statistik tahlil algoritmlari orqali qayta ishlanadi va tekshiriladi. Statistik tahlil natijalari orqali markov zanjiri shakllantiriladi. Markov zanjiri holatlar to‘plamini belgilashda statistik tahlil natijalari muhim hisoblanadi.

Tasodifiy o‘zgaruvchilar ketma-ketligi $X_0, X_1, X_2, \dots$ ning qiymatlari $\{1,2, \dots n\}$ holat maydonida olinadi va ixtiyoriy $n \geq 0$ uchun $P_m = \left(p_{m_{ij}}\right)$, nxn matritsa mavjud bo‘lsa Markov zanjiri deyiladi. $X_0, X_1, X_2, \dots$ bu holatlar to‘plamini bildiradi.

$$P_m(X_{n+1} = j | X_n = i, X_{n-1} = i_{n-1}, \dots, X_0 = i_0) = P_m(X_{n+1} = j | X_n = i) = p_{m_{ij}}$$

P_m matritsa zanjirining o‘tish matritsasi deyiladi va $P_{m_{ij}}$ i dan j gacha o‘tish ehtimoli hisoblanadi. $p_{m_{ij}} = P_m(X_{n+1} = j | X_n = i)$ o‘tish ehtimoli $p_{m_{ij}}$ larni matritsa shaklida yozib olinadi va u quyidagicha:

$$P_m = \begin{bmatrix} p_{m_{11}} & p_{m_{12}} & \cdot & \cdot & \cdot & p_{m_{1n}} \\ p_{m_{21}} & p_{m_{22}} & \cdot & \cdot & \cdot & p_{m_{2n}} \\ \cdot & \cdot & \cdot & \cdot & \cdot & \cdot \\ \cdot & \cdot & \cdot & \cdot & \cdot & \cdot \\ p_{m_{n1}} & p_{m_{n2}} & \cdot & \cdot & \cdot & p_{m_{nn}} \end{bmatrix} \quad (3)$$

har bir qatordagi $p_{m_{11}}, p_{m_{12}}, \dots, p_{m_{1n}}$ o‘tish ehtimollari yig‘indisi $p_{m_{11}} + p_{m_{12}} + \dots + p_{m_{1n}} = 1$ ga teng bo‘lishi shart.

$$\sum_{j=1}^{n} p_{m_{ij}} = \sum_{j=1}^{n} P_m(X_{n+1} = j | X_n = i) = 1 \quad (4)$$

bu yerda qatordagi barcha imkoniyatlar birgalikda 100% ni tashkil etadi. Demak $X_0, X_1, X_2, \dots$ Markov zanjiri tashkil etsa bundan nxn P_m matritsaning t qadamdagi o‘tish ehtimoli $P_m(X_t = j | X_0 = i) = (P_m^t)_{ij}$ teng bo‘ladi. $X_0, X_1, X_2, \dots$ Markov zanjiri tashkil etsa bundan nxn P_m matritsaning X_0 ehtimollik taqsimoti 1 ga n o‘lchamdagi qator vektor π^T uchun ehtimollik taqsimoti $\pi^T P_m^t$ shaklida ifodalanadi.

$$X_0 = \pi^T \Rightarrow X_t = \pi^T P_m^t \quad (5)$$

Stasionar ehtimollik

$$\pi P_m = \pi \quad (6)$$

tashkil etadi. $\sum \pi_i = 1$ shart ham bajarilishi lozim, bunda jarayon qaysi holatda qancha vaqt qolish ehtimolini ko‘rsatadi.

Tarmoq oqimida kutilmagan holatlarni aniqlash uchun statistik xususiyatlardan foydalaniladi. Tahlil qilishda tarmoq oqimi uchun quyidagi statistik xususiyatlarni hisoblash amalga oshiriladi:

- namunaviy o‘rtacha:

$$m_i = \frac{1}{n}\sum_{j=i}^{i+n} S_j \tag{7}$$

bu yerda m_i o‘rtacha namunaviy qiymat, n tanlangan vaqt oralig‘idagi paketlar soni, $S_i - j$ vaqtdagi harakat intensivligining namunaviy qiymati, $j = i$ dan $i + n$ gacha bo‘lgan qiymatlar yig‘indisi olinadi.

- dispersiya:

$$D = \frac{1}{n-1}\sum_{j=i}^{i+n}\left(S_j - m_j\right)^2 \tag{8}$$

bu yerda D dispersiya, n — o‘rganilayotgan oyna uzunligi (nechta qiymat olingan), $S_i - j$ vaqtdagi intensivlik (paket soni, trafik hajmi), m_j o‘rtacha qiymati.

- assimetriya koeffitsienti:

$$K_a = \frac{\frac{1}{n}\sum_{j=i}^{i+n}\left(S_j - m_j\right)^3}{D^3} \tag{9}$$

bu yerda $S_i - j$ vaqtdagi qiymat (masalan, paket soni), m_i o‘rtacha qiymat, D dispersiya, n qiymatlar soni. Assimmetriya koeffitsienti statistik taqsimotning og‘irlik markazining siljishini ifodalaydi.

- kurtoz koeffitsienti:

$$K_k = \frac{\frac{1}{n}\sum_{j=i}^{i+n}\left(S_j - m_j\right)^4}{D^4} - 3 \tag{10}$$

bu yerda: $S_i - j$ vaqtdagi qiymat, m_i o‘rtacha qiymat, D dispersiya, n qiymatlar soni. Kurtoz yoki keskinlik koeffitsienti statistik taqsimotning cho‘qqisining balandligi yoki tepasining o‘tkirligini o‘lchaydi. Boshqacha aytganda, taqsimotdagi qiymatlar o‘rtachadan qanchalik uzoqlashmagan yoki shu atrofida to‘planganligini bildiradi.

- qarama-qarshilik koeffitsenti:

$$K_{oc} = \frac{1}{\sqrt{\eta}} \tag{11}$$

η ortiqcha parametr, quyidagicha aniqlanadi:

$$\eta = K_k = \frac{\mu_4}{\sigma^4} \tag{12}$$

bu yerda σ - standart og‘ish (ya’ni dispersiyaning kvadrat ildizi), μ_4- to‘rtinchi markaziy moment (ya’ni barcha qiymatlarning o‘rtachadan 4-darajali og‘ishini o‘rtachasi). K_{oc} parametri 0 dan (Koshi taqsimoti bo‘yicha) 1 gacha (diskret ikki qiymatli taqsimot) o‘zgaradi. Oddiy taqsimot uchun $K_{oc} = \frac{1}{\sqrt{3}} \approx 0.577$.

Tarqatish shaklini tavsiflovchi yana bir parametr entropiya koeffitsienti hisoblanadi.

- entropiya koeffitsienti:

$$K_{en} = \frac{\Delta_\alpha}{\sigma} \tag{13}$$

bu yerda Δ_α - xatoning entropiya qiymati ya'ni taqsimotning noaniqlik darajasi, σ standart og'ish ya'ni o'rtacha qiymatdan chetlanish darajasini bildiradi.

$$\Delta_\alpha = \frac{1}{2} e^{H_h\left(\frac{a_h}{a_{h_n}}\right)} \tag{14}$$

bu yerda $H_h(\frac{a_h}{a_{h_n}})$ - a_h tasodifiy o'zgaruvchini o'lchash orqali kiritilgan entropiya (noaniqlik) o'zgarishi, e matematik doimiysi. Entropik xato shuni ko'rsatadiki, qanchalik taqsimotda noaniqlik kuchli bo'lsa, entropik xato ham shunchalik katta bo'ladi.

$$H_h(\frac{a_h}{a_{h_n}}) = \int_{-\infty}^{+\infty} p_h(X)\, ln\big(p_h(X)\big) dX \tag{15}$$

sifatida aniqlanadi, bu yerda $p_h(X)$ tasodifiy o'zgaruvchining ehtimollik zichligi.

Tekshirish uchun yozib olingan ma'lumotlari har xil vaqtda yozilgan. csv formatdagi fayllar birlashtirilgan. Bu ma'lumotlar asosida statistik tahlillash amalga oshiriladi. Olingan natijalar 1-jadvalda keltirildi.

1-jadval.

Tarmoq oqimida kutilmagan holat natijalarining statistik tahlili.

№	Statistik tahlil usuli	Statistik tahlil natijasi
1	Namunaviy o'rtacha	$m_i = 1646.5714$
2	Dispersiya	$D = 9474632.51^2$
3	Asimmetriya koeffitsienti	$K_a = 2.463632$
4	Kurtoz koeffitsienti	$K_k = 8.352490$
5	Qarama-qarshilik koeffitsienti	$K_{oc} = 0.3516$
6	Etropiya koeffitsienti	$K_{en} = 1.6231$

Olingan statistik natijalar bo'yicha markov zanjiri baholanadi. Statistik tahlil natijasi bo'yicha markov zanjiri asosida baholashda birinchi X_0, X_1, X_2 holatlar to'plamini qurib olinadi. Uchta holat Markov zanjirining holatlari deb olindi va statistik tahlildan olingan ma'lumot asosida o'tish ehtimoli hisoblandi va 3-formula bo'yicha o'tish matritsasi qurildi.

$$P_m = \begin{bmatrix} 0.4 & 0.4 & 0.2 \\ 0.2 & 0.4 & 0.4 \\ 0.1 & 0.2 & 0.7 \end{bmatrix}$$

Stasionar ehtimollik 6-formula yordamida hisoblandi. Stasionar ehtimollik $\pi = [0.1852 \quad 0.2963 \quad 0.5185]$ ga teng bo'ldi.

Dissertatsiyaning **"Tarmoq oqimilarini bilimlar bazasidan foydalangan holda tahlil qilish va matematik ta'minotini shakllantirish"** deb nomlangan uchinchi bobi Petri tarmoqlari yordamida tarmoq oqimida TCP protokolining ishonchliligini tekshirishni, ma'lumotlar oqimini monitoring tizimining produksion modeli orqali oqimni tahlil qilishda bilimlar bazasini mantiqiy xulosalash samaradorligini oshirishga qaratilgan. Petri modeli asosida TCP protokolining umumiy tuzilishi 5-rasmda berilgan. Modelni ikkita asosiy qismga ajratish mumkin.

A qism va B qismga, shundan A qism TCP standart protokoli holat diagrammasiga mos ravishda yaratildi. B qism ham holat diagrammasini mos lekin belgilashda x prefiksida foydalanildi. Holat diagrammasini yoylarini esa Petri tarmog‘ining o‘tishlari bilan ifodalandi. Bunda positonlar $\{P_{p_i}\}, i = \overline{0,n}$ transitionlar $\{T_{t_i}\}, i = \overline{0,n}$ ko‘rinishida belgilab chiqildi. 2, 3-jadvallarda transition va position ta’riflari berilgan. Position sifatida TCP flaglari va qo‘shimcha sifatida yordamchi belgilashlar kiritilgan. Chunki qo‘yilgan masalada RFC 793 Petri modelini to‘liq qamrab olmaydi. Qolgan positionlar sifatida standart protokol holat diagrammasi belgilashlari olingan. Transition sifatida protokol qoidasidan kelib chiqib shartlar kiritilgan. Qo‘yilgan masala yechimiga kelish uchun ham qo‘shimcha shartlar keltirildi.

2-jadval.

Transition elementlaning tavsifi.

№	Transition	№	Transition	Ta’rifi
1	T_{t_0}	13	xT_{t_0}	Faol ulanish ochiq
2	T_{t_1}	14	xT_{t_1}	Passiv ulanish ochiq
3	T_{t_2}	15	xT_{t_2}	Ulanish so‘rovini yuborish
4	T_{t_3}	16	xT_{t_3}	Ulanish muvaffaqiyatli
5	T_{t_4}	17	xT_{t_4}	O‘rnatilgan ulanishda kutilmagan uzilish
6	T_{t_5}	18	xT_{t_5}	Dastlabki holatga qaytish
7	T_{t_6}	19	xT_{t_6}	O‘chirish so‘rovini yuborish
8	T_{t_7}	20	xT_{t_7}	Qonuniy uzilishni boshlash
9	T_{t_8}	21	xT_{t_8}	Qonuniy uzilish yuz berdi
10	T_{t_9}	22	xT_{t_9}	Yopiq
11	$T_{t_{10}}$	23	$xT_{t_{10}}$	Dastlabki holatga qaytish
12	$T_{t_{11}}$	24	$xT_{t_{11}}$	Tugash

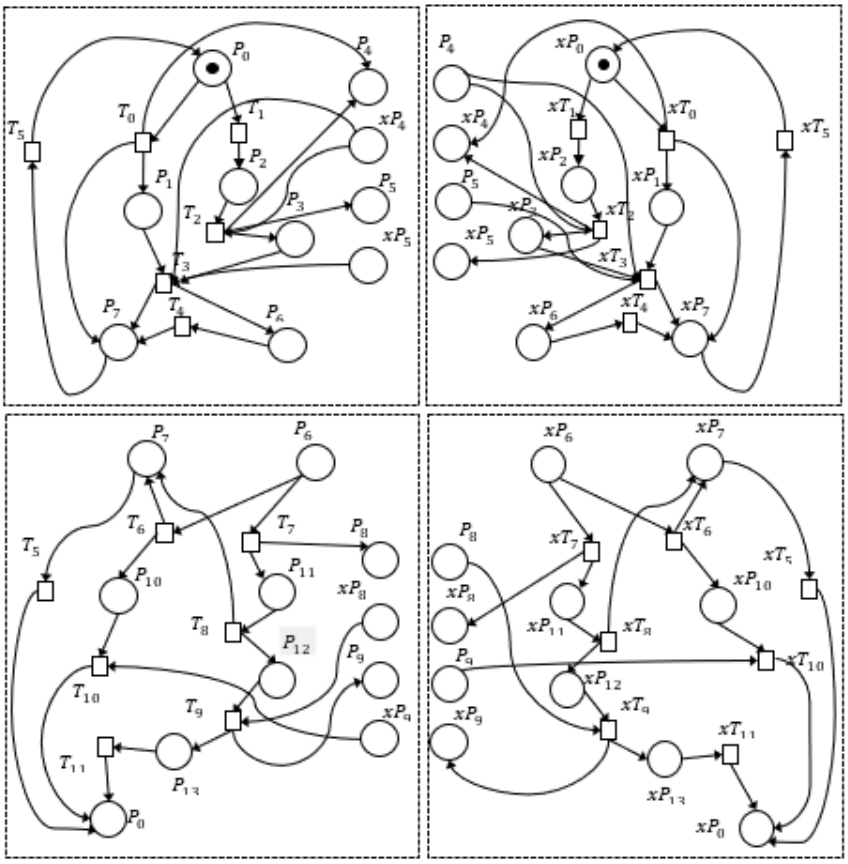
3-jadval.

Position elementlarining tavsifi.

№	Position	Nomi	№	Position	Nomi
1	P_{p_0}	CLOSED	15	xP_{p_0}	xCLOSED
2	P_{p_1}	SYNSENT	16	xP_{p_1}	xSYNSENT
3	P_{p_2}	LISTEN	17	xP_{p_2}	xLISTEN
4	P_{p_3}	SYNRVD	18	xP_{p_3}	xSYNRVD
5	P_{p_4}	SYN	19	xP_{p_4}	xSYN
6	P_{p_5}	SYNACK	20	xP_{p_5}	xSYNACK
7	P_{p_6}	ESTABLD	21	xP_{p_6}	xESTABLD
8	P_{p_7}	RST	22	xP_{p_7}	xRST
9	P_{p_8}	FIN	23	xP_{p_8}	xFIN
10	P_{p_9}	FINACK	24	xP_{p_9}	xFINACK
11	$P_{p_{10}}$	LASTACK	25	$xP_{p_{10}}$	xLASTACK

12	$P_{p_{11}}$	FINWAIT1	26	$xP_{p_{11}}$	xFINWAIT1
13	$P_{p_{12}}$	FINWAIT2	27	$xP_{p_{12}}$	xFINWAIT2
14	$P_{p_{13}}$	TIMEWAIT	28	$xP_{p_{13}}$	xTIMEWAIT

TCP protokoli Petri modelini dekompozitsiya algoritmiga muvofiq funksional kichik tarmoqlarga bo‘lish dekompozitsiya algoritmini TCP protokoli modeliga tadbiq etish natijasida to‘rtta minimal funksional tarmoqdan iborat bo‘ldi. $Z^{1,1}, Z^{1,2}, Z^{2,1}, Z^{2,2}$ kabi belgilandi. Shuni ta’kidlash kerakki, tizimlar o‘zaro ta’sirining simmetriyasi tufayli quyi tarmoqlar juftliklari $Z^{1,1}$, $Z^{1,2}$ va $Z^{2,1}, Z^{2,2}$ izomorf hisoblanadi. Shuning uchun ham ushbu to‘rtta quyi tarmoqdan faqat ikkitasining xususiyatlarini o‘rganish yetarli hisoblanadi. Minimal funksional quyi tarmoqlarni yaratishning turli usullari modelni chap va o‘ng o‘zaro ta’sir qiluvchi Z^1 va Z^2 tizimlariga dekompozitsiyalandi, shuningdek ulanishni o‘rnatuvchi bilan kutilmagan uzilish va kutilmagan uzilish bilan odatiy uzilishni amalga oshiradigan tarmoqlarga Z'^1 va Z'^2 ga ajratish imkonini beradi. Bu yerda quyidagi bog‘liqliklar mavjud: $Z^1 = Z^{1,1} + Z^{1,2}, Z^2 = Z^{2,1} + Z^{2,2}, Z'^1 = Z^{1,1} + Z^{2,1}, Z'^2 = Z^{1,2} + Z^{2,2}$. Bu dekompozitsiya TCP protokoli modelining o‘zaro ta’sir qiluvchi tizimlari jarayonlarini alohida o‘rganish imkonini beradi.



5-rasm. TCP protokolini Petri modeli bo‘yicha dekompozitsiyalash.

4-jadval.

$Z^{1,1}$ va $Z^{1,2}$ kichik tarmoqlarning asosiy invariantlari.

$Z^{1,1}$ quyi tarmoq invarianti	$Z^{1,2}$ quyi tarmoq invarianti
1. $P_{p_0} \rightarrow P_{p_1} \rightarrow P_{p_6} \rightarrow P_{p_7}$ 2. $P_{p_0} \rightarrow P_{p_2} \rightarrow P_{p_3} \rightarrow P_{p_6} \rightarrow P_{p_7}$	1. $P_{p_0} \rightarrow P_{p_6} \rightarrow P_{p_7}$ 2. $P_{p_0} \rightarrow P_{p_6} \rightarrow P_{p_{10}}$

3. $P_{p_0} \to P_{p_6} \to P_{p_7} \to xP_{p_4}$	3. $P_{p_6} \to P_{p_8}$
4. $P_{p_0} \to P_{p_3} \to P_{p_6} \to P_{p_7} \to xP_{p_4}$	4. $P_{p_0} \to P_{p_6} \to P_{p_7} \to P_{p_{11}}$
5. $P_{p_0} \to P_{p_6} \to P_{p_7} \to xP_{p_5}$	5. $P_{p_6} \to P_{p_9} \to P_{p_{11}} \to P_{p_{12}}$
6. $P_{p_0} \to P_{p_7} \to xP_{p_5}$	6. $P_{p_0} \to P_{p_6} \to P_{p_{11}} \to P_{p_{12}} \to P_{p_{13}}$
7. $P_{p_0} \to P_{p_1} \to P_{p_7}$	7. $P_{p_9} \to xP_{p_8}$
8. $P_{p_4} \to xP_{p_4}$	8. $P_{p_0} \to P_{p_{13}} \to xP_{p_8}$
9. $P_{p_0} \to P_{p_3} \to P_{p_7} \to xP_{p_4}$	9. $P_{p_0} \to xP_{p_9}$

4-jadvalda keltirilgan positionlarning raqamlanishidan invariantlarni vektorlarga nisbatan matritsa shaklida ifodalanadi.

$$(x_1, x_2, x_3, x_4, x_5, x_6, x_7, x_8, x_{19}, x_{20}) = (z_1^1, z_2^1, z_3^1, z_4^1, z_5^1, z_6^1, z_7^1, z_8^1, z_9^1) * G^{1,1},$$
$$(x_1, x_7, x_8, x_9, x_{10}, x_{11}, x_{12}, x_{13}, x_{14}, x_{23}, x_{24}) =$$
$$= (z_1^2, z_2^2, z_3^2, z_4^2, z_5^2, z_6^2, z_7^2, z_8^2, z_9^2) * G^{1,2} \quad (16)$$

endi $G^{1,1}$ va $G^{1,2}$ matritsa ko‘rinishiga keltiriladi.

$\overline{x}$ vektorining $Z^{1,1}$ va $Z^{1,2}$ quyi tarmoqlariga mos keladigan komponentlari yozilgan va ulardan tuzilgan matritsalar ustunlarini indekslashni belgilaydi. Qator indekslari vektor komponentlariga mos keladi.

$$G^{1,1} = \begin{vmatrix} 1 & 1 & 0 & 0 & 0 & 0 & 1 & 1 & 0 & 0 \\ 1 & 0 & 1 & 1 & 0 & 0 & 1 & 1 & 0 & 0 \\ 1 & 0 & 0 & 0 & 0 & 0 & 1 & 1 & 1 & 0 \\ 1 & 0 & 0 & 1 & 0 & 0 & 1 & 1 & 1 & 0 \\ 1 & 0 & 0 & 0 & 0 & 0 & 1 & 1 & 0 & 1 \\ 1 & 0 & 0 & 0 & 0 & 0 & 0 & 1 & 0 & 1 \\ 1 & 1 & 0 & 0 & 0 & 0 & 0 & 1 & 0 & 0 \\ 0 & 0 & 0 & 0 & 1 & 0 & 0 & 0 & 1 & 0 \\ 1 & 0 & 0 & 1 & 0 & 0 & 0 & 1 & 1 & 0 \end{vmatrix}$$

$$G^{1,2} = \begin{vmatrix} 1 & 1 & 1 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\ 1 & 1 & 0 & 0 & 0 & 1 & 0 & 0 & 0 & 0 & 0 \\ 0 & 1 & 0 & 1 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\ 1 & 1 & 1 & 0 & 0 & 0 & 1 & 0 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 & 1 & 0 & 1 & 1 & 0 & 0 & 0 \\ 1 & 1 & 0 & 0 & 0 & 0 & 1 & 1 & 1 & 0 & 0 \\ 0 & 0 & 0 & 0 & 1 & 0 & 0 & 0 & 0 & 1 & 0 \\ 1 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 1 & 1 & 0 \\ 1 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 1 \end{vmatrix}$$

$\overline{z}^1 = (z_1^1, z_2^1, z_3^1, z_4^1, z_5^1, z_6^1, z_7^1, z_8^1, z_9^1)$ va $\overline{z}^2 = (z_1^2, z_2^2, z_3^2, z_4^2, z_5^2, z_6^2, z_7^2, z_8^2, z_9^2)$. Taqdim etilgan yechimlar 16 ta chunki 2-qator 3-qator va 6-qator yig‘indisi, 3-qator 6-qator va 7-qatorlar yig‘indisidi. Demak, TCP protokoli Petri modelida p_{p_i}-invariantdir, 1, 5 va 9 bazis invariantlarining yig‘indisi bo‘lgan invariant

$x = (8 \quad 5 \quad 1 \quad 3 \quad 3 \quad 1 \quad 5 \quad 9 \quad 2 \quad 1 \quad 2 \quad 2 \quad 1 \quad 2 \quad 5 \quad 1 \quad 1 \quad 1)$

barcha tabiiy komponentlarni o‘z ichiga oladi. Shuning uchun protokol modeli konservativ va cheklangan tarmoqni ifodalaydi. Vaqt murakkabligi 2^q tartibli bo‘lsin, bu yerda q – tarmoq cho‘qqilari soni.

$$\frac{2^{14}}{2^{10} + 2^{11}} = \frac{2^{14}}{2^{10} * (1 + 2)} = \frac{2^4}{3} \approx 5$$

TCP ulanishini o‘rnatish va tugatish bosqichlarida kutilmagan nosozliklarni aniqlash va tekshirish uchun Petri net modelini ishlab chiqish va tekshirish amalga oshirildi. TCP protokolining tarmoqdagi roli va uning ishonchlilik xususiyatlari tahlil qilindi. TCP modelining to‘g‘riligi va ishonchliligi Petri tarmog‘ining invariantlarini hisoblash yo‘li bilan tekshirildi. Modelning real tarmoq sharoitida TCP protokolining ishlashiga ta’siri baholandi.

Mazkur tadqiqot doirasida tarmoq oqimini monitoring qilish va tahlil qilish asosida muammolarni aniqlash va ularni samarali bartaraf etish jarayonini avtomatlashtirish imkonini beruvchi tizim konsepsiyasi ishlab chiqildi. Tizimning asosiy maqsadi tarmoq administratorining qaror qabul qilish jarayonini yengillashtirish, xatoliklarni aniqlashda aniqlik va tezlikni oshirish, foydalanuvchi va administrator o‘rtasida uzviy hamkorlikni ta’minlashdan iboratdir. Tadqiqotda ishlab chiqilgan tizim produksiyaviy bilimlar modeli asosida tuzildi. Tizimda 38 ta aniq va mantiqiy bog‘langan produksion qoidalar shakllantirildi. Har bir qoida tarmoq holatidagi muayyan vaziyatni ifodalaydi va unga tegishli qaror yoki tavsiyani o‘z ichiga oladi.

Paket xususiyatlarini belgilashda 89 ta xususiyatlar ro‘yxatini B to‘plam sifatida belgilash kiritib olindi.

$$B = \{b_1, b_2, \dots, b_{89}\} \quad (17)$$

Tarmoq oqimidan yozib olingan ma’lumotlarni paket xususiyatalariga ajratib olingandan so‘ng tarmoq holatini tekshirish uchun yaratilgan produksion qoidalar asosida tekshiriladi. Yaratilgan produksion qoidalarni P' to‘plam sifatida belgilash kiritib olindi.

$$P' = \{p'_1, p'_2, \dots, p'_{110}\} \quad (18)$$

Demak $P': B' \to A'$ to‘plam shaklida ifodalandi. Qoidalar esa 19-formula orqali hosil qilinadi. B' to‘plam paket xususiyatlariga berilgan shartlar bajarilganda hosil bo‘ladi. Bu yerda, $b'_j \in B'$, $j = \overline{1,89}$ bo‘lgan paket xususiyatlarini bildiradi. Qachonki b'_j bajariladi, b_j tegishli shartlar bajarilganda. 19-formulada berilgan $b'_j \; va \; b'_k$ bir vaqtda bir-biriga teng bo‘lmaydi.

$$p'_i: \left(b'_j \wedge \dots \wedge b'_k\right) \to a'_i \quad (19)$$

$p'_1: b'_{34} \wedge b'_{35} \wedge b'_{45} \wedge b'_{55} \wedge b'_{58} \wedge b'_{68} \to a'_1 \mid b_{34} > 5000, b_{35} > 10, b_{45} < 1, b_{55} > 100, b_{58} < 10, b_{68} > 50$

$p'_2: b'_{36} \wedge b'_{45} \wedge b'_{55} \wedge b'_{58} \wedge b'_{68} \to a'_2 \mid b_{36} > 1000, b_{45} < 1, b_{55} > 100, b_{58} < 5, b_{68} > 30$

...

$p'_{109}: b'_8 \wedge b'_{19} \wedge b'_{40} \to a'_{109} \mid b_8 > 1000, b_{19} = 0, b_{40} > 20$

$p'_{110}: b'_8 \wedge b'_{33} \wedge b'_{36} \to a'_{110} \mid b_8 < 500, b_{33} > 100000, b_{36} < 1$

Tarmoq oqimini tahlil qilish nuqtai nazaridan eng muhim, tez-tez uchraydigan va aniqlash muhim bo‘lgan holatlar sifatida 110 ta produksion qoidalardan 25 tasi tanlab olindi. 110 ta tarmoq holati 7 ta guruhga ajratib olingan.

$$P' = \begin{Bmatrix} p'_1, p'_2, p'_3, p'_5, p'_6, p'_{19}, p'_{22}, p'_{25}, p'_{26}, p'_{42}, p'_{43}, p'_{58}, p'_{60}, \\ p'_{64}, p'_{65}, p'_{67}, p'_{69}, p'_{72}, p'_{80}, p'_{81}, p'_{84}, p'_{85}, p'_{86}, p'_{90}, p'_{103} \end{Bmatrix}$$

Tanlab olingan produksion qoidalar ichida faqat normal va foydali oqimlar guruhiga kiruvchi bironta tarmoq holati yo‘q. Sababi birinchidan tanlab olingan produksiyalar tizimning samarali ishlashiga va tizim faoliyatining buzilmasligiga qaratilgan. Ikkinchidan bu guruhga kiruvchi holatlar ko‘pincha normal oqimlar hisoblanib, tarmoq faoliyatida ruxsat etilgan oqimlari turiga kiradi.

Dissertatsiyaning **“Dasturiy vositani ishlash jarayoni va amaliyotga tadbiqi”** nomli to‘rtinchi bobida ochiq va yopiq portlarni tekshirish algoritmi, dasturiy vositadan foydalangan holda tarmoq faoliyatini baholash va doimiy monitoring olib borish amaliy tadqiqi va monitoring natijalarini shakllantirish uchun dasturlash vositasining umumiy arxitekturasi ishlab chiqilgan.

Tarmoq monitoringi tarmoq boshqaruvchisi ishining muhim qismi bo‘lgan qiyin va mashaqqatli vazifadir. Tarmoq ma’murlari doimiy ravishda o‘z tarmoqlarining uzluksiz ishlashini ta’minlashga intilishadi. Tarmoq nosozliklari yuzaga kelganda, monitoring dasturlari tarmoqdagi nosozliklarni aniqlashi, ajratishi va tuzatishi va ehtimol nosozlikni tiklashi kerak. Paketlarni klassifikatsiya qilishda 12 ta klassifikatsiya guruhini tuzib olingandi. 12 ta klassifikatsiya guruhining har biri uchun 5 tadan qoidalar yaratildi. Bu qoidalar qayta ishlanmagan paket ma’lumotlarini klassifikatsiya qilishda ular orqali aniqlash mumkin qo‘lgan atributlardan foydalanildi. W to‘plami qoidalarni bildiradi, ularni soni 60 tani tashkil etdi.

$$W = \{w_1, w_2, \dots, w_{60}\} \tag{20}$$

Ustuvorlik bo‘yicha yaratilgan qoidalar belgilab olinadi. U_A aniq ustuvorlik, U_P prefiks bo‘yicha ustuvorlik va U_O oraliq ustuvorlikni bildiradi.

$$U_A = \left\{ \begin{matrix} w_2, w_3, w_6, w_7, w_{13}, w_{14}, w_{15}, w_{34}, w_{38}, \\ w_{39}, w_{46}, w_{47}, w_{48}, w_{51}, w_{52}, w_{53}, w_{54}, w_{55} \end{matrix} \right\}$$

$$U_P = \{w_8, w_9, w_{10}, w_{28}, w_{41}, w_{42}, w_{43}, w_{44}, w_{45}, w_{49}, w_{50}\}$$

$$U_O = \left\{ \begin{matrix} w_1, w_4, w_5, w_{11}, w_{12}, w_{16}, w_{17}, w_{18}, w_{19}, w_{20}, w_{21}, \\ w_{22}, w_{23}, w_{24}, w_{25}, w_{26}, w_{27}, w_{29}, w_{30}, w_{31}, w_{32}, \\ w_{33}, w_{35}, w_{36}, w_{37}, w_{40}, w_{56}, w_{57}, w_{58}, w_{59}, w_{60} \end{matrix} \right\}$$

Tarmoq monitoringi jarayonida ma’lumotlarni qayta ishlash va produksion qoidalar asosida tadqiq etish dasturiy majmuasi uzluksiz ravishda tarmoq trafikini va tarmoq uskunalarining ish holatini baholab boradi. Tajriba tadqiqotlari tarmoq oqimidan informativ belgilarni ajratib oluvchi algoritmlar, paketlarni sinflarga ajratishda klassifikatsiya va ustuvorlik algoritmlari va produksion qoidalarga asoslangan tarmoq oqimlarini monitoring qilish asosida dasturiy vositasi tarmoq oqimidagi ma’lumotlarni tahlil qilishda taqmoq oqimi jarayonlarida foydalanildi. Dasturiy vositaga bir milliontadan ortiq tarmoq oqimi paketlari yuborildi, monitoring jarayonida ishlab chiqilgan algoritm o‘rtacha 8% tezroq erta qaror qabul qilish imkoniyatini berdi. Tarmoqdagi kutilmagan holatlarni aniqlashda ishlab chiqilgan produksion qoidalar asosidagi algoritmi tajriba sinovda mavjud intuitiv va formallashgan usullarga qaraganda 7% ga yaxshiroq natija ko‘rsatdi. Ishlab chiqilgan dasturiy vositaga yuz mingdan dan ortiq tarmoq oqimi paketlari yuborildi, monitoring jarayonida ishlab chiqilgan algoritm o‘rtacha 7% tezroq erta qaror qabul qilish imkoniyatini berdi.

XULOSA

“Kompyuter tarmoqlarining ma’lumotlar oqimini monitoring qilishning algoritmlari va dasturiy ta’minoti” mavzusidagi falsafa doktori (PhD) dissertatsiyasi bo‘yicha olib borilgan tadqiqotlar natijasida quyidagi xulosalar taqdim etiladi:

1. Pcap fayllaridan paketlarni oqim sifatida qayta ishlash va ular asosida atributlarni aniqlash bo‘yicha ishlab chiqilgan yondashuv monitoring samaradorligini sezilarli darajada oshirdi. Ajratilgan 89 ta oqim xususiyatlari paketlarning statistik, vaqtli va bayroq parametrlarini chuqur tavsiflab, tarmoq trafigining dinamikasini keng qamrovda tahlil qilish imkonini berdi. Ushbu yondashuv real vaqt rejimida tahdidlarni aniqlash, ishonchlilikni ta’minlash va tarmoq oqimini kuzatish tizimlarining aniqlik darajasini oshirishda muhim amaliy ahamiyat kasb etdi.
2. Kutilmagan holatlarni aniqlashda namunaviy o‘rtacha, dispersiya, assimetriya va kurtoz koeffitsientlari, qarama-qarshilik koeffitsienti hamda entropiya qo‘llanilishi monitoringning analitik imkoniyatlarini kengaytirdi. Shu bilan birga, Markov zanjiri asosida qurilgan model tarmoq oqimdagi hodisalar ketma-ketligini bashorat qilishda samarali natijalar berdi. Bu esa tarmoq oqimining ichki qonuniyatlarini ochib berib, xavfsizlik tizimlari uchun muhim nazariy asos yaratdi.
3. TCP protokolining barqarorligini Petri tarmoqlari asosida formal tekshirish natijasida ulanish jarayonlari, uzilishlar va tiklanish mexanizmlari aniq modellashtirildi. Bu yondashuv hisoblash murakkabligini kamaytirish, invariantlarni aniqlash samaradorligini oshirish hamda boshqa murakkab protokollarni ham formal verifikatsiya qilish imkonini berdi.
4. Ishlab chiqilgan produksion qoidalar asosida tarmoq oqimlarini avtomatik monitoring qilish imkonini berdi. Bu tizim foydalanuvchi bilan interaktiv ishlaydi, ogohlantirishlar beradi va real vaqt rejimida administrator qarorlarini qo‘llab-quvvatlaydi. Ushbu yondashuv tahdidlarni erta aniqlash, xavfsizlikni ta’minlash va mantiqiy xulosalash samaradorligini sezilarli darajada oshirdi.
5. Yaratilgan 9 bo‘limli kompleks dastur real vaqt rejimida tarmoq holatini chuqur va tizimli tarzda kuzatish imkonini berdi. Ma’lumotlar tahlili natijalari esa kelgusidagi tahdidlarni prognozlash uchun ilmiy-amaliy asos bo‘lib xizmat qildi.
6. Dissertatsiya doirasida olib borilgan tadqiqotlar natijasida ishlab chiqilgan algoritmlar va yaratilgan dasturiy ta’minot Surxondaryo viloyati IT Park Termiz filialida, Surxondaryo viloyati statistika boshqarmasida hamda O‘zbekiston Respublikasi Raqamli texnologiyalar vazirligi Surxondaryo viloyat hududiy sho‘basida joriy qilingan. Natijada tarmoq oqimini monitoring qilish hamda paketlarni tasniflash orqali tarmoqqa kirib keluvchi ma’lumotlarni tahlil qilib erta qaror qabul qilishni qo‘llab-quvvatlash vaqtini qisqartirish va tarmoqdagi kutilmagan holatlarni aniqlash mavjud intuitiv va formallashgan usullarga qaraganda 7% ga yaxshiroq natija ko‘rsatdi.

НАУЧНЫЙ СОВЕТ DSc.09/2025.27.12. T.01.01.M
ПО ПРИСУЖДЕНИЮ УЧЕНЫХ СТЕПЕНЕЙ ПРИ ТАШКЕНТСКОМ УНИВЕРСИТЕТЕ ИНФОРМАЦИОННЫХ ТЕХНОЛОГИЙ

ДЖИЗАССКИЙ ФИЛИАЛ НАЦИОНАЛЬНОГО УНИВЕРСИТЕТА УЗБЕКИСТАНА ИМЕНИ МИРЗО УЛУГБЕКА

ЖУРАЕВ МАЪРУФ ТУРАКУЛ УГЛИ

АЛГОРИТМЫ И ПРОГРАММНОЕ ОБЕСПЕЧЕНИЕ ДЛЯ МОНИТОРИНГА ПОТОКА ДАННЫХ В КОМПЬЮТЕРНЫХ СЕТЯХ

05.01.04 – Математическое и программное обеспечение вычислительных машин, комплексов и компьютерных сетей

АВТОРЕФЕРАТ ДИССЕРТАЦИИ
ДОКТОРА ФИЛОСОФИИ (PhD) ПО ТЕХНИЧЕСКИМ НАУКАМ

Ташкент – 2026

Тема диссертации доктора философии (PhD) по техническим наукам зарегистрирована в Высшей аттестационной комиссии при Министерстве высшего образования, науки и инноваций Республики Узбекистан за B2025.3.PhD/T5882.

Диссертация выполнена в Джизаский филиал Национального университета Узбекистана имени Мирзо Улугбека.

Автореферат диссертации на трех языках (узбекский, русский, английский (резюме)) размещен на веб странице (www.tuit.uz) и информационно-образовательном портале «Ziyonet» (www.ziyonet.uz).

Научный руководитель:	**Кабулов Анвар Василевич** доктор технических наук, профессор
Официальные оппоненты:	**Джуманов Жамолжон Худайкулович** доктор технических наук, профессор
	Мухамедиева Дилноз Тулкуновна доктор технических наук, профессор
Ведущая организация:	**Самаркандский государственный университет имени Шарофа Рашидова**

Защита состоится «12» февраля 2026 г. в 14⁰⁰ часов, на заседании Научного совета DSc.09/2025.27.12. T.01.01.M при Ташкентском университете информационных технологий. (Адрес: 100202, г. Ташкент, ул. Амира Темура, 108. Тел: (99871) 238-64-43; факс: (99871) 238-65-52; э-mail: tuit@tuit.uz).

С диссертацией можно ознакомиться в Информационно-ресурсном центре Ташкентского университета информационных технологий (Регистрационный № 406). (Адрес: 100202, г.Ташкент, ул. Амира Темура, 108. Тел: (99871) 238-64-43).

Автореферат диссертации разослан «2» февраля 2026 г.
(протокол рассылки № 3 от «2» февраля 2026 г.).

М.М.Мусаев
Председатель научного совета по присуждению учёных степеней, д.т.н., профессор

Э.Ш.Назирова
Ученый секретарь научного совета по присуждению учёных степеней, д.т.н., профессор

Дж.Б.Султанов
Председатель научного семинара при научном совете по присуждению учёных степеней, д.т.н., доцент

ВВЕДЕНИЕ (аннотация диссертации доктора философии (PhD))

Актуальность и необходимость темы диссертации. Мировой опыт показывает, что методы мониторинга потоков данных и составляющих их пакетов в компьютерных сетях имеют особое значение для эффективного управления информационными системами и обеспечения их надежности. Использование методов системного анализа и статистической обработки при мониторинге сетевых потоков позволяет не только повысить эффективность работы сетей, но и обеспечить целостность и надежность передаваемых данных. Кроме того, современные алгоритмы и программные комплексы, основанные на глубоком анализе сетевых пакетов, повышают возможности раннего обнаружения и устранения ошибок и сбоев, которые могут возникнуть в информационных системах. В таких системах обработка пакетов и сетевой мониторинг на основе правил являются одной из актуальных задач.

Изучение результатов мониторинга потоков данных компьютерных сетей, основанное на мировом опыте, показывает, что задачи, направленные на анализ, обработку, разработку алгоритмов и программных средств анализа сетевых потоков, являются актуальными. Алгоритмы мониторинга сетевых потоков позволяют контролировать входящие и исходящие потоки в сетях в режиме реального времени и анализировать состояние сети. Для эффективного управления и контроля сетевых потоков в информационных системах реализуется широкий спектр мер. В частности, проводятся различные научные и практические исследования, основанные на программах мониторинга, средствах обеспечения устойчивости сетей и новейших достижениях современных информационных технологий. В частности, основными подходами к анализу пакетов, составляющих сетевые потоки, являются поверхностный анализ пакетов, среднеуровневый анализ пакетов и глубокий анализ пакетов. При анализе пакетов анализу подвергаются преимущественно необработанные пакеты. Это снижает эффективность определения состояния сети и, как следствие, негативно сказывается на мониторинге сетевых потоков. Поэтому актуальна разработка алгоритмов обработки пакетов и правил мониторинга сетевых потоков.

В последние годы объём цифровой информации в нашей республике стремительно растёт. Алгоритмы и правила мониторинга сетевых потоков, учитывающие требования и особенности мониторинга потоков данных в компьютерных сетях, изучены недостаточно. Данная работа направлена на решение научно-технических задач по разработке алгоритмов и программ мониторинга сетевых потоков.

В нашей республике принимаются меры по обеспечению надежности компьютерных сетей и развитию локального рынка программного обеспечения на основе реализации государственных программ и стратегий. Данная научно-исследовательская работа также в определенной мере служит научно и практически выполнению задач, обозначенных в указах и постановлениях Президента Республики Узбекистан №ПП-286 от 16 сентября 2025 года «О мерах по дальнейшему ускорению внедрения цифровых

технологий на территориях, в отраслях и отраслях республики», №ПП-4024 от 21 ноября 2018 года «О мерах по совершенствованию системы контроля за внедрением информационно-коммуникационных технологий, их защитой» и №ПФ-60 от 28 января 2022 года «О Стратегии развития нового Узбекистана на 2022-2026 годы» и других нормативно-правовых документах, связанных с этой деятельностью.

Соответствие исследования приоритетным направлениям развития науки и технологий республики. Настоящая работа выполнена в соответствии с приоритетным направлением развития науки и технологий Республики Узбекистан IV. «Информатизация и развитие информационно-коммуникационных технологий».

Степень изученности проблемы. В развитых странах мира, в частности, в США, Китае, России, Японии, Южной Корее, Германии и других, ведутся научные исследования по мониторингу сетевых потоков данных и анализу пакетных данных в информационных системах. Эти вопросы, в частности, исследованы в научных трудах Р.И.Пасечникова, Д.В.Костина, K.Zhou, О.И.Шелухина, Р.А.Сударикова, H.Kim, K.C.Claffy, М.Фоменкова, G.Jain, D.Barman, N.Medhi, M.Faloutsos, M.Tahboush, V.Pallavi и других.

В нашей республике большой вклад в решение этих проблем внесли ведущие учёные Ш.Х.Фозилов, Т.Ф.Бекмуратов, М.М.Мусаев, Х.Н.Зайнидинов, У.Р.Хамдамов, К.А.Ташев, Ш.Р.Гуломов, Ж.Х.Джуманов и другие.

По результатам анализа литературы, вопрос мониторинга потоков данных в компьютерных сетях изучен недостаточно, учитывая требования к мониторингу потоков данных в компьютерных сетях, алгоритмам классификации и обнаружения непредвиденных ситуаций.

Связь диссертационного исследования с научно-исследовательской работой высшего учебного заведения, в котором выполняется диссертация. Диссертационная работа выполнена в рамках научно-исследовательского проекта № Ф-ОТ-2021-248 «Разработка интеллектуальных методов и технологий обнаружения, идентификации и нейтрализации угроз для обеспечения защиты информации на основе функциональных таблиц» (2022-2024 гг.), проводимого в Национальном университете Узбекистана имени Мирзо Улугбека.

Целью исследования. Разработка алгоритмов и программного обеспечения на основе продукционных правил для мониторинга потоков данных в компьютерных сетях.

Задачи исследования:

извлечение информативных символов из сетевого трафика, вычисление атрибутов трафика, разработка алгоритмов классификации и приоритетности для разделения пакетов на классы;

предложить трехступенчатую цепь Маркова, объединяющую статистические показатели для обнаружения непредвиденных событий в сетевом потоке;

моделирование надежности протокола TCP с использованием сетей Петри, разработка математического обеспечения на основе алгоритма декомпозиции;

создание базы знаний и программного инструмента для мониторинга сетевого трафика и поддержки принятия решений на основе продукционных правил.

Объектом исследования выступили программные средства, осуществляющие мониторинг потоков данных и сетевого трафика в компьютерных сетях информационных систем.

Предметом исследования являются математические методы, алгоритмы и программные средства, используемые для анализа, классификации, мониторинга и управления сетевым трафиком в реальном времени.

Методы исследования. В исследовании использовались обработка данных сетевых потоков, сравнительный анализ, систематический анализ, методы классификации, методы статистического анализа и технологии программирования.

Научная новизна исследования заключается в следующем:

разработаны алгоритмы классификации и приоритизации разбиения пакетов на классы, основанные на извлечении информативных признаков сетевого потока и вычислении атрибутов потока;

предлагается использовать трехступенчатую цепь Маркова, объединяющую статистические показатели, для обнаружения непредвиденных ситуаций в сетевом потоке;

разработано математическое обеспечение для обнаружения непредвиденных сбоев в работе сети на основе сетей Петри;

созданы база знаний и программный инструмент для мониторинга сетевых потоков и поддержки принятия решений на основе продукционных правил.

Практические результаты исследования:

Разработаны алгоритмы мониторинга и обработки потоков данных;

Создано программное обеспечение на основе существующих и разработанных алгоритмов для выявления и классификации непредвиденных ситуаций в сетевых потоках;

Разработаны правила анализа сетевых потоков на основе продукционных правил, позволяющие оценивать состояние сети.

Достоверность результатов исследования. Достоверность результатов исследования подтверждается корректностью разработанных алгоритмов анализа сетевых потоков, сравнительным анализом результатов анализа исследуемых сетевых потоков на основе общепринятых критериев, а также экспериментальными результатами, полученными с помощью разработанного программного средства.

Научная и практическая значимость результатов исследования. Научная значимость результатов исследования обусловлена разработкой

комплексного подхода, алгоритмов и программного средства для анализа сетевых потоков в режиме реального времени.

Практическая значимость результатов исследования обусловлена мониторингом потоков данных в информационных системах в режиме реального времени с помощью созданного программного средства, ранним выявлением сбоев в работе сети и повышением устойчивости системы.

Внедрение результатов исследования. Результаты внедрения на основе разработанных в ходе исследования алгоритмов мониторинга сетевых потоков данных и программного обеспечения:

Программное средство, основанное на алгоритмах продукционных правил для мониторинга потоков данных в компьютерных системах, было внедрено в Сурхандарьинском областном филиале Министерства цифровых технологий с целью сокращения времени мониторинга сетевых потоков и поддержки раннего принятия решений путем анализа входящих данных посредством классификации пакетов (справка Сурхандарьинского областного хокимията № 07-07/8583 от 26 сентября 2025 г.). В результате на программное средство было отправлено более ста тысяч пакетов сетевых потоков, а разработанный в процессе мониторинга алгоритм позволил обеспечить раннее принятие решений в среднем на 7%;

Алгоритм, основанный на продукционных правилах, разработанных в ходе научно-исследовательской работы для выявления непредвиденных ситуаций в сети, был внедрен в Отделе цифровизации и ведения статистических регистров Сурхандарьинского областного управления статистики (справка №07-07/8583 Сурхандарьинского областного хокимията от 26 сентября 2025 года). В результате разработанный алгоритм показал на 7% лучший результат выявления непредвиденных ситуаций при передаче данных;

Также алгоритм был внедрен в Термезском филиале IT-парка Сурхандарьинской области для сокращения времени мониторинга сетевого трафика и анализа входящих данных за счет классификации пакетов и поддержки раннего принятия решений (справка №07-07/8583 Сурхандарьинского областного хокимията от 26 сентября 2025 года). На программный инструмент было отправлено более миллиона пакетов сетевого трафика, а разработанный в процессе мониторинга алгоритм позволил обеспечить в среднем 8% раннего принятия решений.

Апробация результатов исследования. Результаты исследования обсуждались на 5 международных и 9 республиканских научно-практических конференциях и научных семинарах.

Публикация результатов исследования. По теме исследования опубликовано 29 научных работ, из них 8 статей опубликованы в научных изданиях, рекомендованных ВАК Республики Узбекистан для публикации основных научных результатов диссертаций, в том числе в 3 зарубежных и 5 республиканских научных журналах, а также получены авторские свидетельства на 7 программ для ЭВМ.

Структура и объем диссертации. Диссертация состоит из введения, четырех глав, заключения, списка использованной литературы и приложений. Объем диссертации составляет 120 страниц.

ОСНОВНОЕ СОДЕРЖАНИЕ ДИССЕРТАЦИИ.

Во введении обосновывается актуальность и необходимость темы диссертации, указывается на соответствие исследования приоритетным направлениям развития науки и техники в Республике Узбекистан, определяются цели и задачи исследования, определяются объект и предмет исследования, обосновывается достоверность полученных результатов, приводятся сведения об их теоретической и практической значимости, состоянии внедрения результатов исследования в практику, опубликованных работах, а также структура диссертации.

Первая глава диссертации, озаглавленная **«Аналитический анализ методов и программных средств обработки данных сетевых потоков и Pcap-файлов»**, состоит из трёх параграфов, в которых представлены методы анализа обработки данных сетевых потоков, анализ программных средств обработки данных потоков, анализ pcap-файлов для извлечения характеристик пакетов на основе данных потоков и анализ методов анализа сетевых потоков в реальном времени. По результатам исследования проведён сравнительный анализ.

При записи пакетов программные средства используют следующий алгоритм:

1. При определении потока пакетов все пакеты, поступающие из сети, определяются как последовательность: $P_{pcap} = \{p_{pcap_1}, p_{pcap_2}, p_{pcap_3}, \dots, p_{pcap_n}\}$ где p_{pcap_i} обозначает всю последовательность байтов i-пакета.

2. Присвоение метки времени — это процесс присвоения времени прибытия каждого пакета. $V = \{v_1, v_2, v_3, \dots, v_n\}$ где v_i — записывает точное время (в секундах и микросекундах) прибытия пакета p_{pcap_i}.

3. Структура файла pcap раздел глобального заголовка определяется следующим образом. $H_g = (magic\_number, version\_major, version\_minor, thiszone, sigfigs, snaplen, network)$. Каждый пакет — это $R_i = (ts\_\text{sec}_i, ts\_usec_i, incl\_len_i, orig\_len_i, p_{pcap_i})$ где $ts\_\text{sec}_i - v_i$ секундная часть, $ts\_usec_i - v_i$ микросекундная часть, $incl\_len_i$ записанная длина пакета (в байтах), $orig\_len_i$ исходная длина пакета, p_{pcap_i} необработанные байтовые данные пакета.

4. Алгоритм хранения $PCAP = H_g \,\|\|_{i=1}^{n}\, R_i$ где $\|$ — операция последовательного сложения.

5. Шаги алгоритма включают в себя переключение сетевого интерфейса в режим promiscuous/monitor $mode \leftarrow promiscuous$, запись глобального заголовка $write(H_g)$, измерение времени для каждого входящего пакета $v_i \leftarrow timestamp(p_{pcap_i})$, вычисление длин $incl\_len_i, orig\_len_i$, создание записи:

$R_i \leftarrow (ts_{\mathrm{sec}_i}, ts_{useci}, incl_{len_i}, orig\_len_i, p_{pcap_i})$, добавление в файл $append(R_i)$, закрытие файла $close(PCAP)$.

Все программные инструменты работают практически одинаково. Различия заключаются лишь в формате хранения данных и внешнем виде интерфейса. Анализ сетевых потоков — это технология, позволяющая собирать, обрабатывать, классифицировать, отслеживать и модифицировать сетевые пакеты в режиме реального времени на основе их содержимого. Разработка инструментов анализа сетевых потоков подразделяется на разработку алгоритмов и подходов анализа. Разработка программных и аппаратных средств важна для эффективного решения задачи анализа.

Во второй главе диссертации, озаглавленной **«Разработка алгоритмов выделения и классификации информативных символов в сетевом потоке»**, разработаны алгоритмы анализа характеристик пакетов, проходящих через сетевой поток, и формирования их в поток с целью определения набора информативных символов в сетевом потоке. Алгоритм извлекает данные из пакетов и вычисляет их статистические свойства. Для вычисления статистических показателей класса SummaryStatistics использованы следующие методы.

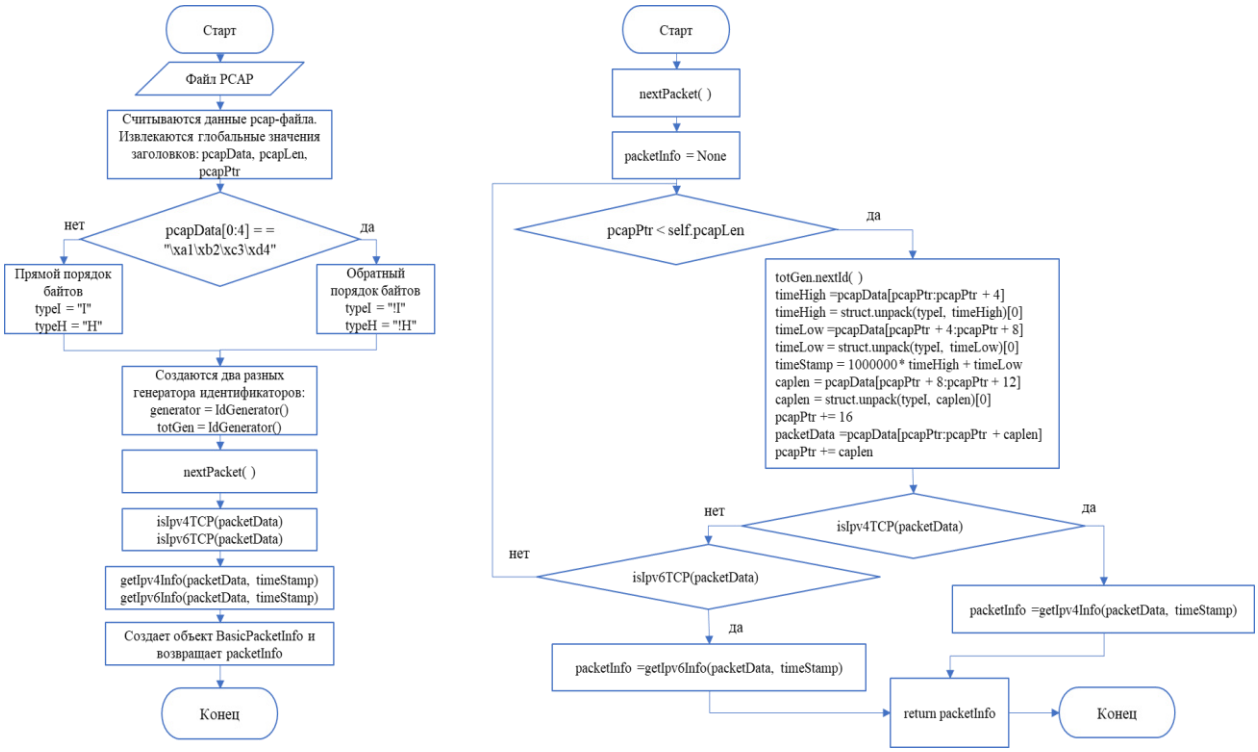


Рисунок 1. Алгоритм чтения pcap-файла и извлечения характеристик пакета.

Согласно алгоритму на рисунке 1, глобальный заголовок, заголовок пакета и данные пакета считываются из структуры файла pcap. Флаги TCP вычисляются по формуле $flags = \sum_{i=0}^{7} bit_i 2^i$. На основе данного алгоритма тип файла Pcap определяется на основе информации глобального заголовка, а данные каждого пакета извлекаются с помощью метода nextPacket( ).

Генерация сетевого потока выполняется согласно алгоритму, представленному на рисунке 2. В этом случае информация о потоке

обновляется на основе идентификатора потока, к которому принадлежат анализируемые пакеты.

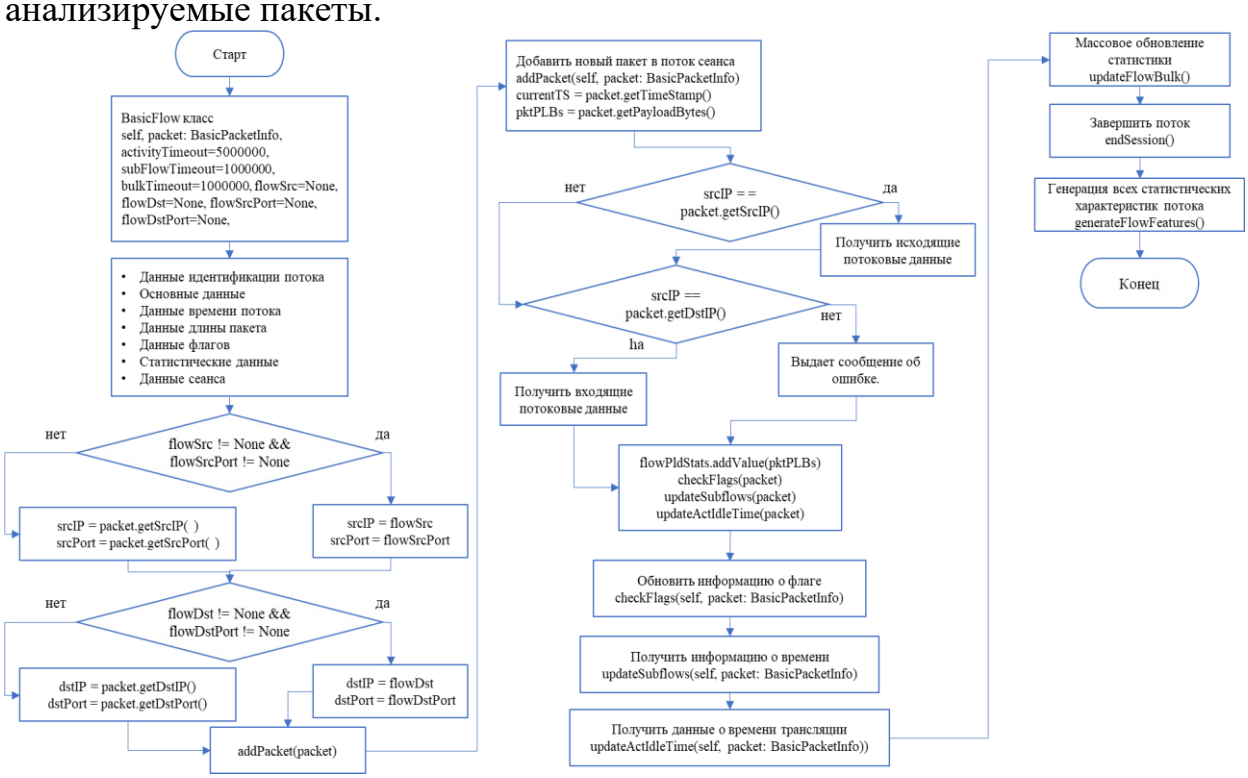


Рисунок 2. Алгоритм генерации сетевого потока.

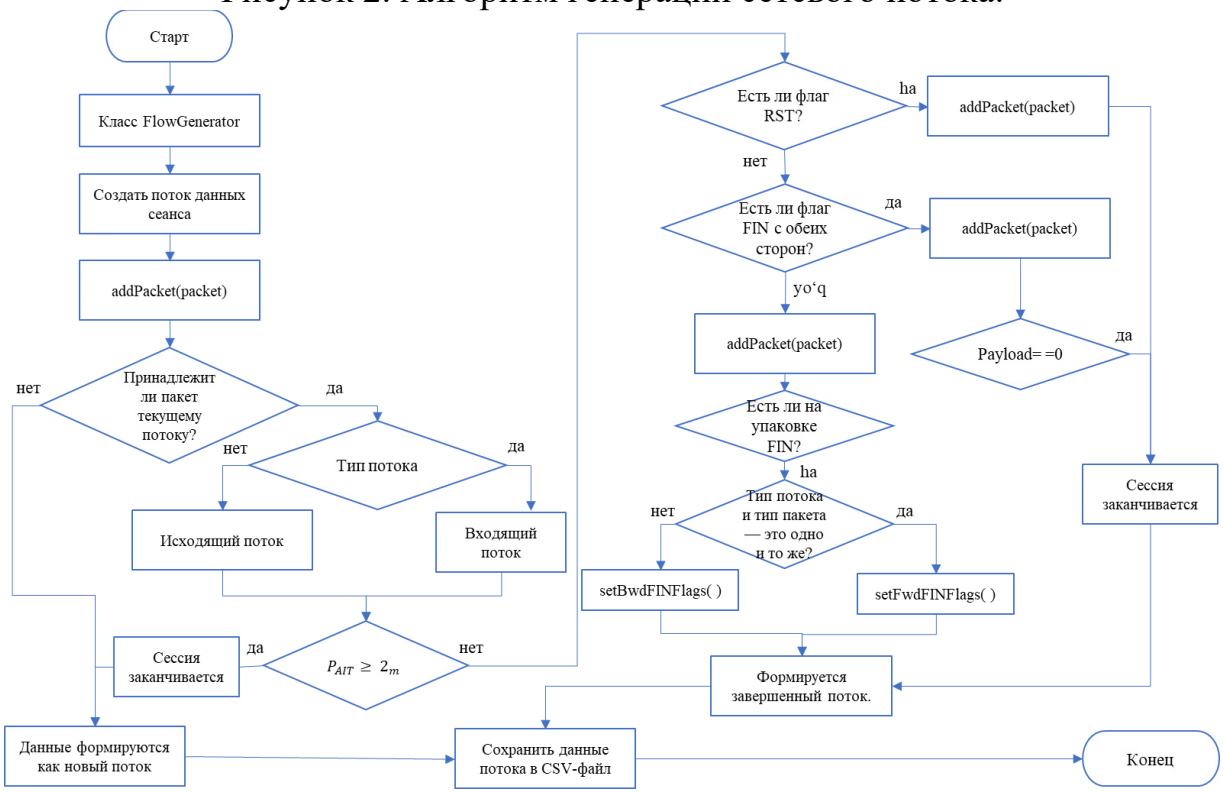


Рисунок 3. Алгоритм формирования потока и записи CSV-файла.

Алгоритм, показанный на рисунке 3, используется для сбора сеансовых потоков из пакетов, хранения завершённых потоков и записи их свойств в CSV-файл. Если поток завершён, он записывается в CSV-файл, а если нет, к потоку добавляется новый пакет. Процесс продолжается до тех пор, пока не будут исчерпаны данные пакета, считанные из PCAP-файла.

При классификации на основе пакетов один пакет может одновременно подпадать под несколько классификаций. Поэтому им отдаётся приоритет при применении правил.

$$\text{Точное}_{\text{соответствие}} > \text{префиксное}_{\text{соответствие}} > \text{промежуточное}_{\text{соответствие}} \quad (1)$$

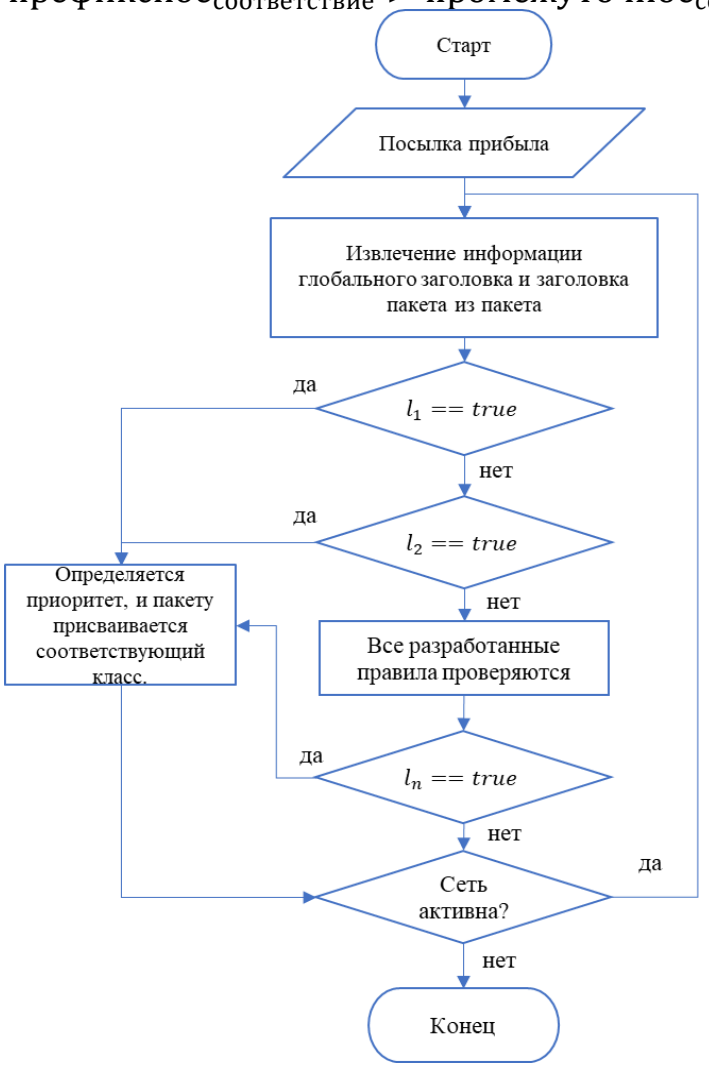


Рисунок 4. Алгоритм классификации пакетов.

Классификация по размеру пакета даёт очень важную информацию. На рисунке 4 показан алгоритм классификации пакетов. Если пакеты отсортированы по формуле 2, то чем больше размер пакета, тем меньше размер пакета и тем меньше размер пакета. Если этот процесс не происходит, можно предположить, что в сети произошла возможная атака.

$$L_{\text{коллекция}} = \{l_1, l_2, \dots, l_n\} \quad (2)$$

В процессе сбора и анализа данных о сетевых потоках, во-первых, входящие данные о сетевых потоках регистрируются с помощью разработанного программного инструмента. Записанные данные сохраняются в файле формата pacp. Во-вторых, данные, хранящиеся в pcap-файле, считываются на основе разработанного алгоритма. Из считанных данных извлекаются 89 различных признаков, которые затем сохраняются в файле формата csv.

Данные в csv-файле обрабатываются и проверяются с помощью алгоритмов статистического анализа. По результатам статистического анализа

формируется цепь Маркова. Результаты статистического анализа важны для определения множества состояний цепи Маркова.

Последовательность случайных величин $X_0, X_1, X_2, \ldots$ называется цепью Маркова, если значения $\{1,2, \ldots n\}$ берутся в пространстве состояний и матрица $P_m = \left(p_{m_{ij}}\right)$, nxn существует для любого $n \geq 0$. $X_0, X_1, X_2, \ldots$ обозначает множество состояний.

$P_m(X_{n+1} = j|X_n = i, X_{n-1} = i_{n-1}, \ldots, X_0 = i_0) = P_m(X_{n+1} = j|X_n = i) = p_{m_{ij}}$ P_m называется матрицей перехода цепочки матриц, а $P_{m_{ij}}$ вероятностью перехода от i к j. gacha Вероятность перехода $p_{m_{ij}} = P_m(X_{n+1} = j|X_n = i)$ записывается в виде матрицы $p_{m_{ij}}$ и выглядит следующим образом:

$$P_m = \begin{bmatrix} p_{m_{11}} & p_{m_{12}} & \cdot & \cdot & \cdot & p_{m_{1n}} \\ p_{m_{21}} & p_{m_{22}} & \cdot & \cdot & \cdot & p_{m_{2n}} \\ \cdot & \cdot & \cdot & \cdot & \cdot & \cdot \\ \cdot & \cdot & \cdot & \cdot & \cdot & \cdot \\ p_{m_{n1}} & p_{m_{n2}} & \cdot & \cdot & \cdot & p_{m_{nn}} \end{bmatrix} \quad (3)$$

сумма вероятностей перехода $p_{m_{11}}, p_{m_{12}}, \ldots, p_{m_{1n}}$ в каждой строке должна быть равна $p_{m_{11}} + p_{m_{12}} + \cdots + p_{m_{1n}} = 1$.

$$\sum_{j=1}^{n} p_{m_{ij}} = \sum_{j=1}^{n} P_m(X_{n+1} = j|X_n = i) = 1 \quad (4)$$

где, все возможные значения в последовательности вместе дают 100%. Таким образом, если $X_0, X_1, X_2, \ldots$ образует цепь Маркова, то вероятность перехода матрицы nxn P_m на шаге t равна $P_m(X_t = j|X_0 = i) = (P_m^t)_{ij}$. Если $X_0, X_1, X_2, \ldots$ образует цепь Маркова, то распределение вероятностей матрицы nxn P_m X_0 выражается как распределение вероятностей для вектора последовательности π^T размером от 1 до n, как $\pi^T P_m^t$.

$$X_0 = \pi^T \Rightarrow X_t = \pi^T P_m^t \quad (5)$$

Стационарная вероятность

$$\pi P_m = \pi \quad (6)$$

составляет. Также должно выполняться условие $\sum \pi_i = 1$, которое указывает вероятность того, что процесс останется в заданном состоянии в течение определённого времени. Статистические характеристики используются для выявления непредвиденных ситуаций в сетевом потоке. В ходе анализа для сетевого потока рассчитываются следующие статистические характеристики:

- выборочное среднее:

$$m_i = \frac{1}{n} \sum_{j=i}^{i+n} S_j \quad (7)$$

где, m_i среднее значение выборки, n количество пакетов в выбранном интервале времени, $S_i - j$ выборочное значение интенсивности трафика в момент времени, а берется сумма значений от $j = i$ до $i + n$.

- дисперсия:

$$D = \frac{1}{n-1}\sum_{j=i}^{i+n}\left(S_j - m_j\right)^2 \quad (8)$$

где, D дисперсия, n — длина исследуемого окна (сколько значений было получено), $S_i - j$ интенсивность в момент времени (количество пакетов, объем трафика), m_j среднее значение.

- коэффициент асимметрии:

$$K_a = \frac{\frac{1}{n}\sum_{j=i}^{i+n}\left(S_j - m_j\right)^3}{D^3} \quad (9)$$

где, $S_i - j$ значение в момент времени (например, количество пакетов), m_i среднее значение, D дисперсия, а n — количество значений. Коэффициент асимметрии представляет собой смещение центра тяжести статистического распределения.

- коэффициент эксцесса:

$$K_k = \frac{\frac{1}{n}\sum_{j=i}^{i+n}\left(S_j - m_j\right)^4}{D^4} - 3 \quad (10)$$

где, $S_i - j$ значение в момент времени, m_i среднее значение, D дисперсия, n количество значений. Коэффициент эксцесса или асимметрии измеряет высоту или остроту пика статистического распределения. Другими словами, он показывает, насколько близки значения в распределении к среднему значению, или насколько они кластеризованы.

- коэффициент сопротивления:

$$K_{oc} = \frac{1}{\sqrt{\eta}} \quad (11)$$

η избыточный параметр, определяемый следующим образом:

$$\eta = K_k = \frac{\mu_4}{\sigma^4} \quad (12)$$

где, σ - стандартное отклонение (т.е. квадратный корень из дисперсии), μ_4-четвёртый центральный момент (т.е. среднее арифметическое четвёртых стандартных отклонений всех значений от среднего). Параметр K_{oc} варьируется от 0 (согласно распределению Коши) до 1 (дискретное биномиальное распределение). Для нормального распределения $K_{oc} = \frac{1}{\sqrt{3}} \approx 0.577$.

Другим параметром, характеризующим форму распределения, является коэффициент энтропии.

- коэффициент энтропии:

$$K_{en} = \frac{\Delta_\alpha}{\sigma} \quad (13)$$

где, Δ_α - значение энтропии ошибки, т. е. степень неопределенности распределения, а σ стандартное отклонение, т. е. степень отклонения от среднего значения.

$$\Delta_\alpha = \frac{1}{2} e^{H_h\left(\frac{a_h}{a_{h_n}}\right)} \quad (14)$$

где, $H_h(\frac{a_h}{a_{h_n}})$ - изменение энтропии (неопределённости), внесённое измерением случайной величины a_h а e математическая константа. Энтропийная ошибка показывает, что чем больше неопределённость в распределении, тем больше энтропийная ошибка.

$$H_h(\frac{a_h}{a_{h_n}}) = \int_{-\infty}^{+\infty} p_h(X)\, ln\big(p_h(X)\big) dX \quad (15)$$

определяется как, где $p_h(X)$ плотность вероятности случайной величины.

Для проверки полученные данные были записаны в разное время. Файлы в формате CSV были объединены. На основе этих данных был проведён статистический анализ. Полученные результаты представлены в таблице 1.

Таблица 1.

Статистический анализ неожиданных состояний потока в сети.

№	Метод статистического анализа	Результат статистического анализа
1	Выборочное среднее	$m_i = 1646.5714$
2	Дисперсия	$D = 9474632.51^2$
3	Коэффициент асимметрии	$K_a = 2.463632$
4	Коэффициент эксцесса	$K_k = 8.352490$
5	Коэффициент сопротивления	$K_{oc} = 0.3516$
6	Коэффициент этропии	$K_{en} = 1.6231$

На основе полученных статистических результатов оценивается цепь Маркова. При оценке цепи Маркова на основе результатов статистического анализа строится первый набор состояний X_0, X_1, X_2 В качестве состояний цепи Маркова были взяты три состояния, и на основе информации, полученной в результате статистического анализа, была рассчитана вероятность перехода и построена матрица перехода по формуле 3.

$$P_m = \begin{bmatrix} 0.4 & 0.4 & 0.2 \\ 0.2 & 0.4 & 0.4 \\ 0.1 & 0.2 & 0.7 \end{bmatrix}$$

Стационарная вероятность была рассчитана с использованием Формулы 6. Стационарная вероятность была равна $\pi = [0.1852 \quad 0.2963 \quad 0.5185]$.

Третья глава диссертации под названием **«Анализ сетевых потоков с использованием базы знаний и формирование математического обеспечения»** направлена на проверку надежности протокола TCP в сетевом потоке с использованием сетей Петри и повышение эффективности логического вывода базы знаний при анализе потоков на основе продукционной модели системы мониторинга потоков данных.

Общая структура протокола TCP, основанного на модели Петри, показана на рисунке 5. Модель можно разделить на две основные части: часть A и часть B, из которых часть A создается в соответствии с диаграммой состояний стандартного протокола TCP. Часть B также создается в соответствии с

диаграммой состояний, но для ее обозначения используется префикс x. Дуги диаграммы состояний были представлены переходами сети Петри. В данном случае позиции были определены как $\{P_{p_i}\}, i = \overline{0,n}$ а переходы — как $\{T_{t_i}\}, i = \overline{0,n}$. Таблицы 2 и 3 содержат определения перехода и позиции. Флаги TCP были включены в качестве позиций, а вспомогательные определения в качестве дополнений. Поскольку RFC 793 не полностью охватывает модель Петри в задаче, оставшиеся позиции были взяты в качестве стандартных определений диаграммы состояний протокола. Условия, основанные на правилах протокола, были включены в качестве переходов. Для решения задачи также были введены дополнительные условия.

Таблица 2.

Описание переходных элементов.

№	Переход	№	Переход	Определение
1	T_{t_0}	13	xT_{t_0}	Активное соединение открыто
2	T_{t_1}	14	xT_{t_1}	Пассивное соединение открыто
3	T_{t_2}	15	xT_{t_2}	Отправить запрос на подключение
4	T_{t_3}	16	xT_{t_3}	Подключение успешно установлено
5	T_{t_4}	17	xT_{t_4}	Неожиданное отключение установленного соединения
6	T_{t_5}	18	xT_{t_5}	Возврат в исходное состояние
7	T_{t_6}	19	xT_{t_6}	Подать запрос на удаление
8	T_{t_7}	20	xT_{t_7}	Начинаем легальный перерыв
9	T_{t_8}	21	xT_{t_8}	Произошло юридическое прерывание
10	T_{t_9}	22	xT_{t_9}	Закрыто
11	$T_{t_{10}}$	23	$xT_{t_{10}}$	Возврат в исходное состояние
12	$T_{t_{11}}$	24	$xT_{t_{11}}$	Конец

Таблица 3.

Описание элементов позиции.

№	Позиция	Имя	№	Позиция	Имя
1	P_{p_0}	CLOSED	15	xP_{p_0}	xCLOSED
2	P_{p_1}	SYNSENT	16	xP_{p_1}	xSYNSENT
3	P_{p_2}	LISTEN	17	xP_{p_2}	xLISTEN
4	P_{p_3}	SYNRVD	18	xP_{p_3}	xSYNRVD
5	P_{p_4}	SYN	19	xP_{p_4}	xSYN
6	P_{p_5}	SYNACK	20	xP_{p_5}	xSYNACK
7	P_{p_6}	ESTABLD	21	xP_{p_6}	xESTABLD
8	P_{p_7}	RST	22	xP_{p_7}	xRST
9	P_{p_8}	FIN	23	xP_{p_8}	xFIN
10	P_{p_9}	FINACK	24	xP_{p_9}	xFINACK

11	$P_{p_{10}}$	LASTACK	25	$xP_{p_{10}}$	xLASTACK
12	$P_{p_{11}}$	FINWAIT1	26	$xP_{p_{11}}$	xFINWAIT1
13	$P_{p_{12}}$	FINWAIT2	27	$xP_{p_{12}}$	xFINWAIT2
14	$P_{p_{13}}$	TIMEWAIT	28	$xP_{p_{13}}$	xTIMEWAIT

Модель протокола TCP разбивается на функциональные подсети согласно алгоритму декомпозиции модели Петри. В результате применения алгоритма декомпозиции к модели протокола TCP получены четыре минимальные функциональные подсети, обозначенные как $Z^{1,1}, Z^{1,2}, Z^{2,1}, Z^{2,2}$. Следует отметить, что в силу симметрии взаимодействия систем пары подсетей $Z^{1,1}$, $Z^{1,2}$ и $Z^{2,1}, Z^{2,2}$ изоморфны. Следовательно, достаточно изучить свойства только двух из этих четырёх подсетей. Различные методы создания минимальных функциональных подсетей позволяют декомпозировать модель на лево- и правовзаимодействующие системы Z^1 и Z^2, а также разделить сеть на сети Z^1 и Z^2, реализующие неожиданное отключение с устанавливающим соединение и обычное отключение с неожиданным отключением. Здесь имеются следующие зависимости: $Z^1 = Z^{1,1} + Z^{1,2}, Z^2 = Z^{2,1} + Z^{2,2}, Z'^1 = Z^{1,1} + Z^{2,1}, Z'^2 = Z^{1,2} + Z^{2,2}$. Такое разложение позволяет нам изучать взаимодействующие системные процессы модели протокола TCP по отдельности.

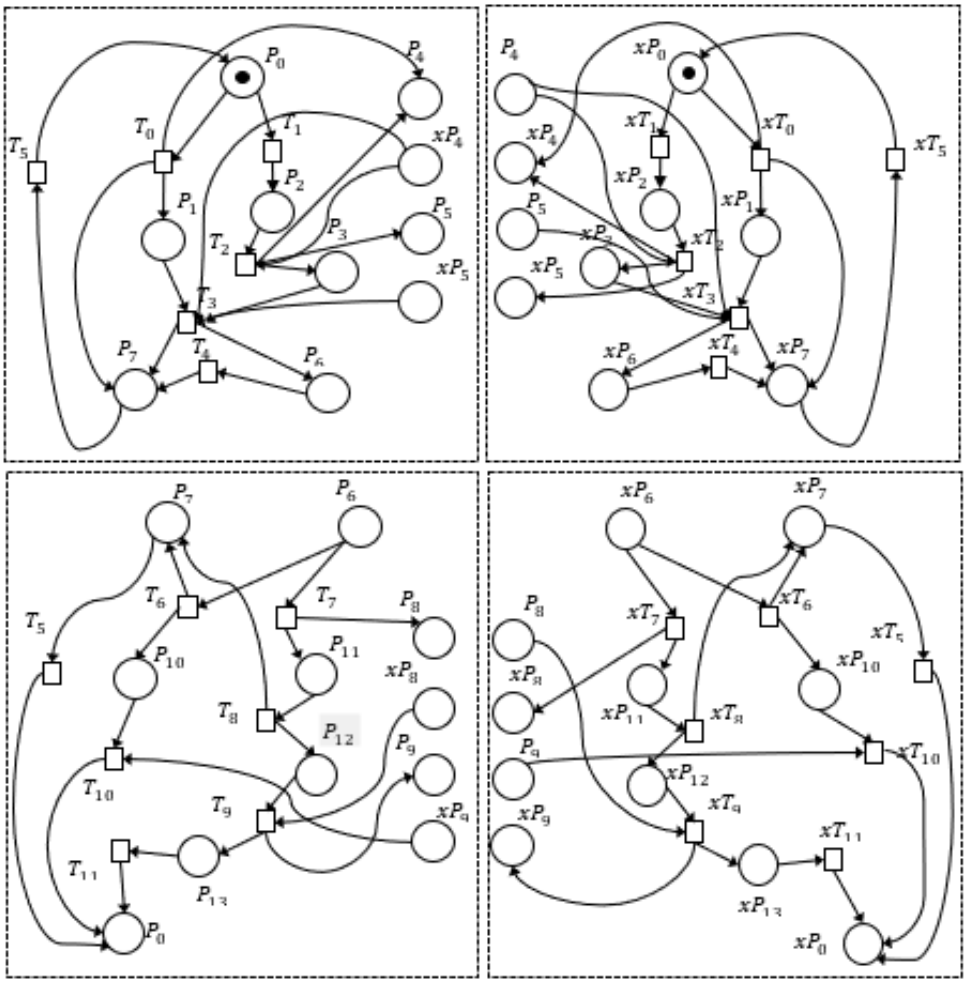


Рисунок 5. Разложение протокола TCP с использованием модели Петри.

Таблица 4.

$Z^{1,1}$ и $Z^{1,2}$ являются основными инвариантами подсетей.

Инвариант подсети $Z^{1,1}$	Инвариант подсети $Z^{1,2}$
10.$P_{p_0} \rightarrow P_{p_1} \rightarrow P_{p_6} \rightarrow P_{p_7}$	10.$P_{p_0} \rightarrow P_{p_6} \rightarrow P_{p_7}$
11.$P_{p_0} \rightarrow P_{p_2} \rightarrow P_{p_3} \rightarrow P_{p_6} \rightarrow P_{p_7}$	11.$P_{p_0} \rightarrow P_{p_6} \rightarrow P_{p_{10}}$
12.$P_{p_0} \rightarrow P_{p_6} \rightarrow P_{p_7} \rightarrow xP_{p_4}$	12.$P_{p_6} \rightarrow P_{p_8}$
13.$P_{p_0} \rightarrow P_{p_3} \rightarrow P_{p_6} \rightarrow P_{p_7} \rightarrow xP_{p_4}$	13.$P_{p_0} \rightarrow P_{p_6} \rightarrow P_{p_7} \rightarrow P_{p_{11}}$
14.$P_{p_0} \rightarrow P_{p_6} \rightarrow P_{p_7} \rightarrow xP_{p_5}$	14.$P_{p_6} \rightarrow P_{p_9} \rightarrow P_{p_{11}} \rightarrow P_{p_{12}}$
15.$P_{p_0} \rightarrow P_{p_7} \rightarrow xP_{p_5}$	15.$P_{p_0} \rightarrow P_{p_6} \rightarrow P_{p_{11}} \rightarrow P_{p_{12}} \rightarrow P_{p_{13}}$
16.$P_{p_0} \rightarrow P_{p_1} \rightarrow P_{p_7}$	16.$P_{p_9} \rightarrow xP_{p_8}$
17.$P_{p_4} \rightarrow xP_{p_4}$	17.$P_{p_0} \rightarrow P_{p_{13}} \rightarrow xP_{p_8}$
18.$P_{p_0} \rightarrow P_{p_3} \rightarrow P_{p_7} \rightarrow xP_{p_4}$	18.$P_{p_0} \rightarrow xP_{p_9}$

Инварианты из нумерации позиций, приведенной в таблице 4, выражены в матричной форме относительно векторов.

$$(x_1, x_2, x_3, x_4, x_5, x_6, x_7, x_8, x_{19}, x_{20}) = (z_1^1, z_2^1, z_3^1, z_4^1, z_5^1, z_6^1, z_7^1, z_8^1, z_9^1) * G^{1,1},$$
$$(x_1, x_7, x_8, x_9, x_{10}, x_{11}, x_{12}, x_{13}, x_{14}, x_{23}, x_{24}) =$$
$$= (z_1^2, z_2^2, z_3^2, z_4^2, z_5^2, z_6^2, z_7^2, z_8^2, z_9^2) * G^{1,2} \quad (17)$$

теперь $G^{1,1}$ и $G^{1,2}$ преобразуются в матричную форму.

Компоненты вектора $\overline{x}$, соответствующие подсеткам $Z^{1,1}$ и $Z^{1,2}$, записываются и определяют индексацию столбцов построенных на их основе матриц. Индексы строк соответствуют компонентам вектора.

$$G^{1,1} = \begin{vmatrix} 1 & 1 & 0 & 0 & 0 & 0 & 1 & 1 & 0 & 0 \\ 1 & 0 & 1 & 1 & 0 & 0 & 1 & 1 & 0 & 0 \\ 1 & 0 & 0 & 0 & 0 & 0 & 1 & 1 & 1 & 0 \\ 1 & 0 & 0 & 1 & 0 & 0 & 1 & 1 & 1 & 0 \\ 1 & 0 & 0 & 0 & 0 & 0 & 1 & 1 & 0 & 1 \\ 1 & 0 & 0 & 0 & 0 & 0 & 0 & 1 & 0 & 1 \\ 1 & 1 & 0 & 0 & 0 & 0 & 0 & 1 & 0 & 0 \\ 0 & 0 & 0 & 0 & 1 & 0 & 0 & 0 & 1 & 0 \\ 1 & 0 & 0 & 1 & 0 & 0 & 0 & 1 & 1 & 0 \end{vmatrix}$$

$$G^{1,2} = \begin{vmatrix} 1 & 1 & 1 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\ 1 & 1 & 0 & 0 & 0 & 1 & 0 & 0 & 0 & 0 & 0 \\ 0 & 1 & 0 & 1 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\ 1 & 1 & 1 & 0 & 0 & 0 & 1 & 0 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 & 1 & 0 & 1 & 1 & 0 & 0 & 0 \\ 1 & 1 & 0 & 0 & 0 & 0 & 1 & 1 & 1 & 0 & 0 \\ 0 & 0 & 0 & 0 & 1 & 0 & 0 & 0 & 0 & 1 & 0 \\ 1 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 1 & 1 & 0 \\ 1 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 1 \end{vmatrix}$$

$\overline{z}^1 = (z_1^1, z_2^1, z_3^1, z_4^1, z_5^1, z_6^1, z_7^1, z_8^1, z_9^1)$ va $\overline{z}^2 = (z_1^2, z_2^2, z_3^2, z_4^2, z_5^2, z_6^2, z_7^2, z_8^2, z_9^2)$. Представленных решений 16, поскольку строка 2 представляет собой сумму строк 3 и 6, а строка 3 – сумму строк 6 и 7. Следовательно, протокол TCP является p_{p_i}-инвариантным в модели Петри, причем инвариант представляет собой сумму базисных инвариантов 1, 5 и 9

$$x = (8 \quad 5 \quad 1 \quad 3 \quad 3 \quad 1 \quad 5 \quad 9 \quad 2 \quad 1 \quad 2 \quad 2 \quad 1 \quad 2 \quad 5 \quad 1 \quad 1 \quad 1)$$

включает все естественные компоненты. Следовательно, модель протокола представляет собой консервативную сеть с ограничениями. Пусть временная сложность имеет порядок 2^q, где q – количество вершин сети.

$$\frac{2^{14}}{2^{10} + 2^{11}} = \frac{2^{14}}{2^{10} * (1 + 2)} = \frac{2^4}{3} \approx 5$$

Была разработана и протестирована модель сети Петри для обнаружения и исследования непредвиденных сбоев на этапах установления и завершения TCP-соединения. Проанализирована роль протокола TCP в сети и его характеристики надежности. Корректность и надежность модели TCP были проверены путём расчёта инвариантов сети Петри. Оценено влияние модели на работу протокола TCP в реальных сетевых условиях.

В рамках данного исследования была разработана концепция системы, позволяющая автоматизировать процесс выявления проблем и их эффективного устранения на основе мониторинга и анализа сетевого трафика. Основной целью системы является упрощение процесса принятия решений администратором сети, повышение точности и скорости обнаружения ошибок, а также обеспечение бесперебойного взаимодействия пользователя и администратора. Разработанная в исследовании система основана на модели производственных знаний. Система сформировала 38 понятных и логически связанных продукционных правил. Каждое правило отображает конкретную ситуацию в состоянии сети и содержит соответствующее решение или рекомендацию.

При определении свойств пакета был включен список из 89 свойств, определяющих их как пакет B.

$$B = \{b_1, b_2, \dots, b_{89}\} \tag{17}$$

После извлечения данных из сетевого потока в свойства пакета они проверяются на соответствие продукционным правилам, созданным для проверки состояния сети. Введено обозначение созданных продукционных правил как множества P'.

$$P' = \{p'_1, p'_2, \dots, p'_{110}\} \tag{18}$$

Итак, $P' : B' \to A'$ выражается как набор. Правила генерируются по формуле 19. Набор B' генерируется при выполнении условий, заданных для свойств пакета. Здесь, $b'_j \in B'$, $j = \overline{1,89}$ обозначает свойства пакета. При выполнении b'_j b_j удовлетворяет соответствующим условиям. В формуле 19 b'_j и b'_k не могут быть равны друг другу одновременно.

$$p'_i : \left(b'_j \wedge \dots \wedge b'_k\right) \to a'_i \tag{19}$$

$p'_1 : b'_{34} \wedge b'_{35} \wedge b'_{45} \wedge b'_{55} \wedge b'_{58} \wedge b'_{68} \to a'_1 \mid b_{34} > 5000, b_{35} > 10, b_{45} < 1, b_{55} > 100, b_{58} < 10, b_{68} > 50$

$p'_2 : b'_{36} \wedge b'_{45} \wedge b'_{55} \wedge b'_{58} \wedge b'_{68} \to a'_2 \mid b_{36} > 1000, b_{45} < 1, b_{55} > 100, b_{58} < 5, b_{68} > 30$

...

$p'_{109} : b'_8 \wedge b'_{19} \wedge b'_{40} \to a'_{109} \mid b_8 > 1000, b_{19} = 0, b_{40} > 20$

$p'_{110}: b'_8 \wedge b'_{33} \wedge b'_{36} \rightarrow a'_{110} \mid b_8 < 500, b_{33} > 100000, b_{36} < 1$

С точки зрения анализа сетевого потока, 25 из 110 продукционных правил были выбраны как наиболее важные, часто встречающиеся и важные для идентификации. 110 состояний сети были разделены на 7 групп.

$$P' = \begin{Bmatrix} p'_1, p'_2, p'_3, p'_5, p'_6, p'_{19}, p'_{22}, p'_{25}, p'_{26}, p'_{42}, p'_{43}, p'_{58}, p'_{60}, \\ p'_{64}, p'_{65}, p'_{67}, p'_{69}, p'_{72}, p'_{80}, p'_{81}, p'_{84}, p'_{85}, p'_{86}, p'_{90}, p'_{103} \end{Bmatrix}$$

В выбранных правилах продукций нет ни одного состояния сети, которое попадало бы исключительно в группу нормальных и полезных потоков. Это объясняется тем, что, во-первых, выбранные правила продукций направлены на эффективную и неразрушающую работу системы. Во-вторых, состояния, попадающие в эту группу, часто считаются нормальными потоками и представляют собой тип потоков, разрешенных при работе сети.

В четвертой главе диссертации под названием **«Процесс работы с программным средством и его применение на практике»** разработан алгоритм проверки открытых и закрытых портов, практическое исследование оценки сетевой активности и проведения непрерывного мониторинга с помощью программного средства, а также общая архитектура программного средства формирования результатов мониторинга.

Мониторинг сети — сложная и ответственная задача, являющаяся важной частью работы сетевого администратора. Сетевые администраторы постоянно стремятся обеспечить бесперебойную работу своих сетей. При возникновении сетевых сбоев программы мониторинга должны обнаруживать, изолировать и устранять сбои, а также, по возможности, восстанавливать сеть после сбоя. Для классификации пакетов было создано 12 групп классификации. Для каждой из 12 групп классификации было создано 5 правил. Эти правила использовались для классификации необработанных данных пакетов с использованием атрибутов, которые можно было идентифицировать с их помощью. Набор W представляет собой 60 правил.

$$W = \{w_1, w_2, \dots, w_{60}\} \tag{20}$$

Создаваемые правила определяются приоритетом. U_A обозначает абсолютный приоритет, U_P обозначает префиксный приоритет, а U_O обозначает промежуточный приоритет.

$$U_A = \begin{Bmatrix} w_2, w_3, w_6, w_7, w_{13}, w_{14}, w_{15}, w_{34}, w_{38}, \\ w_{39}, w_{46}, w_{47}, w_{48}, w_{51}, w_{52}, w_{53}, w_{54}, w_{55} \end{Bmatrix}$$

$$U_P = \{w_8, w_9, w_{10}, w_{28}, w_{41}, w_{42}, w_{43}, w_{44}, w_{45}, w_{49}, w_{50}\}$$

$$U_O = \begin{Bmatrix} w_1, w_4, w_5, w_{11}, w_{12}, w_{16}, w_{17}, w_{18}, w_{19}, w_{20}, w_{21}, \\ w_{22}, w_{23}, w_{24}, w_{25}, w_{26}, w_{27}, w_{29}, w_{30}, w_{31}, w_{32}, \\ w_{33}, w_{35}, w_{36}, w_{37}, w_{40}, w_{56}, w_{57}, w_{58}, w_{59}, w_{60} \end{Bmatrix}$$

В процессе мониторинга сети программный комплекс обработки данных и анализа на основе продукционных правил непрерывно оценивает сетевой трафик и рабочее состояние сетевого оборудования. В экспериментальных исследованиях использовались алгоритмы извлечения информативных признаков из сетевого трафика, алгоритмы классификации и приоритетности для разделения пакетов на классы, а также программное средство мониторинга сетевого трафика на основе продукционных правил для анализа данных в

сетевом трафике. На программное средство было отправлено более миллиона пакетов сетевого трафика, и разработанный в процессе мониторинга алгоритм позволил принять раннее решение в среднем на 8%. Разработанный на основе продукционных правил алгоритм обнаружения непредвиденных ситуаций в сети показал результат на 7% лучше существующих интуитивно-формализованных методов в ходе экспериментальной проверки. На разработанное программное средство было отправлено более ста тысяч пакетов сетевого трафика, и разработанный в процессе мониторинга алгоритм позволил принять раннее решение в среднем на 7%.

ЗАКЛЮЧЕНИЕ

В результате исследования, проведенного по диссертации на соискание ученой степени доктора философии (PhD) на тему «Алгоритмы и программное обеспечение для мониторинга потоков данных в компьютерных сетях», представлены следующие выводы:

1. Разработанный подход к обработке пакетов из Pcap-файлов как потока и определению на их основе атрибутов существенно повысил эффективность мониторинга.89 выявленных признаков потока обеспечили детальное описание статистических, временных и флаговых параметров пакетов, что позволило провести комплексный анализ динамики сетевого трафика. Данный подход приобрел важное практическое значение для выявления угроз в режиме реального времени, обеспечения надежности и повышения точности систем мониторинга сетевых потоков.

2. Использование выборочного среднего, коэффициентов дисперсии, асимметрии и эксцесса, отношения шансов и энтропии для выявления непредвиденных ситуаций расширило аналитические возможности мониторинга. При этом модель, построенная на основе цепи Маркова, дала эффективные результаты в прогнозировании последовательности событий в сетевом потоке. Это позволило раскрыть внутренние закономерности сетевого потока и создать важную теоретическую базу для систем безопасности.

3. В результате формальной проверки устойчивости протокола TCP на основе сетей Петри были достоверно смоделированы процессы установления соединений, прерывания связи и механизмы восстановления. Данный подход позволил снизить вычислительную сложность, повысить эффективность обнаружения инвариантов, а также провести формальную верификацию других сложных протоколов.

4. Разработанная система позволила осуществлять автоматический мониторинг сетевых потоков на основе правил. Эта система взаимодействует с пользователем, предоставляет оповещения и поддерживает решения администратора в режиме реального времени. Такой подход значительно повысил эффективность раннего обнаружения угроз, обеспечения безопасности и логического вывода.

5. Созданная 9-секционная комплексная программа позволила осуществлять углубленный и систематический мониторинг состояния сети в режиме реального времени. Результаты анализа данных послужили научно-практической основой для прогнозирования будущих угроз.

6. Разработанные в результате исследований, проведенных в рамках диссертации, алгоритмы и программное обеспечение были внедрены в Термезском филиале Сурхандарьинского областного IT-парка, Сурхандарьинском региональном управлении статистики и Сурхандарьинском областном территориальном отделении Министерства цифровых технологий Республики Узбекистан. В результате мониторинг сетевого потока и анализ классификации пакетов входящих в сеть данных показали на 7% лучшие результаты в сокращении времени, необходимого для принятия решений на ранних этапах и выявления непредвиденных ситуаций в сети, по сравнению с существующими интуитивными и формализованными методами.

SCIENTIFIC COUNCIL AWARDING SCIENTIFIC DEGREES DSc.09/2025.27.12. T.01.01.M AT TASHKENT UNIVERSITY OF INFORMATION TECHNOLOGIES

JIZZAKH BRANCH OF NATIONAL UNIVERSITY OF UZBEKISTAN NAMED AFTER MIRZO ULUGBEK

JURAEV MARUF TURAQUL UGLI

ALGORITHMS AND SOFTWARE FOR MONITORING DATA FLOW IN COMPUTER NETWORKS

05.01.04 – Mathematical and software support of computers, complexes and computer networks

DISSERTATION ABSTRACT OF THE DOCTOR OF PHILOSOPHY (PhD) ON TECHNICAL SCIENCES

Tashkent – 2026

The theme of doctor of philosophy (PhD) on technical sciences was registered at the Supreme Attestation Commission at the Cabinet of Ministery of Higher education, science and innovations of the Republic of Uzbekistan under number B2025.3.PhD/T5882.

The dissertation has been prepared at Jizzakh branch of National university of Uzbekistan named after Mirzo Ulugbek.

The abstract of the dissertation is posted in three languages (Uzbek, Russian, English (resume)) on the website (www.tuit.uz) and on the website of "Ziyonet" Information and educational portal (www.ziyonet.uz.)

Scientific adviser:	**Kabulov Anvar Vasilevich** Doctor of Technical Sciences, professor
Official opponents:	**Djumanov Jamoljon Xudaykulovich** Doctor of Technical Sciences, professor
	Mukhamedieva Dilnoz Tulkunovna Doctor of Technical Sciences, professor
Leading organization:	**Samarkand State University named after Sharof Rashidov**

The defense of dissertation will take place "12" February 2026 at 14^{00} at the meeting of Scientific Council No. DSc.09/2025.27.12. T.01.01.M at Tashkent University of Information Technologies (Address: 100202, Tashkent city, Amir Temur street, 108. Ph.: (+99871) 238-64-43, e-mail: tuit@tuit.uz).

The dissertation can be reviewed at the Information Resourse Centre of Tashkent University of Information Technologies (is registered under No. 406). (Address: 100202, Tashkent city, Amir Temur street, 108. Ph.: (+99871) 238-64-43).

Abstract of the dissertation sent out on "2" February 2026 y.
(mailing report No. 3 on "2" February 2026 y.)

M.M. Musaev
Chairman of the scientific council awarding scientific degrees, Doctor of Technical Sciences, professor

E.Sh. Nazirova
Scientific secretary of scientific council awarding scientific degrees, Doctor of Technical Sciences, professor

Dj.B. Sultanov
Chairman of the academic seminar under the scientific council awarding scientific degrees, Doctor of Technical Sciences, Docent

INTRODUCTION (abstract of PhD thesis)

The aim of the research work. The development of algorithms and software based on production rules for monitoring data flow in computer networks.

The research objective. Software tools for monitoring data flow and network traffic in computer networks in information systems were selected.

Scientific novelty of research work is as follows:

classification and prioritization algorithms have been developed for dividing packets into classes based on extracting informative symbols from network traffic and calculating traffic attributes.

a Markov chain consisting of three states, combining statistical indicators, has been proposed to detect unexpected situations in network flows;

a mathematical support for detecting unexpected network outages based on Petri nets has been developed;

a knowledge base and software tool have been created to monitor network flows and support decision-making based on production rules.

Implementation of the research results. Results of implementation based on the network flow data monitoring algorithms and software developed in the study:

A software tool based on production rule-based algorithms for monitoring data flow in computer systems was implemented in the Surkhandarya regional branch of the Ministry of Digital Technologies in order to reduce the time for monitoring network flow and supporting early decision-making by analyzing incoming data through packet classification (Reference of the Surkhandarya Regional Administration No. 07-07/8583 dated September 26, 2025). As a result, more than one hundred thousand network flow packets were sent to the software tool, and the algorithm developed during the monitoring process allowed for early decision-making by an average of 7%;

The algorithm based on production rules developed in the research work for detecting unexpected situations in the network was implemented in the Department of Digitization and Maintaining Statistical Registers of the Surkhandarya Regional Statistics Department (Reference No. 07-07/8583 of the Surkhandarya Regional Administration dated September 26, 2025). As a result, the developed algorithm showed a 7% better result in detecting unexpected situations in data transmission;

It was also implemented in the Termez branch of the IT park in Surkhandarya region in order to reduce the time for monitoring network traffic and analyzing incoming data by classifying packets and supporting early decision-making (Reference No. 07-07/8583 of the Surkhandarya Regional Administration dated September 26, 2025). More than one million network traffic packets were sent to the software tool, and the algorithm developed during the monitoring process allowed for an average of 8% early decision-making.

The structure and volume of the thesis. The dissertation consists of an introduction, four chapters, a conclusion, a list of references, and appendices. The volume of the dissertation is 120 pages.

E’LON QILINGAN ISHLAR RO‘YXATI
СПИСОК ОПУБЛИКОВАННЫХ РАБОТ
LIST OF PUBLISHED WORKS

I bo‘lim (I часть; I part)

1. Juraev M., Yarashov I., Kudaybergenov A., Babadzhanov A., & Mamatova Z. Research on Network Flow Based on Statistical Analysis Methods. International Journal of Advanced Computer Science & Applications. Vol. 16, №6, 2025. -P. 169-176. doi: 10.14569/IJACSA.2025.0160618. (05.00.00; №1, Web of Science)
2. Babadzhanov A., Yarashov I., Juraev M., Otakhonov A., Kudaybergenov A., & Utemuratov R. Mathematical Representation of Netflow Analysis Decision Making Based on Production Logic. International Journal of Advanced Computer Science & Applications. Vol. 16, №9, 2025. -P. 154-166. doi: 10.14569/IJACSA.2025.0160916. (05.00.00; №1, Web of Science)
3. Yarashov I., Kuvonchbek R., Juraev M., & Rahmonov F. Processing and Analysis of Network Flow Data Using Intelligent Technologies. Lecture Notes in Computer Science. Vol. 15555 LNCS, 2026. doi: 10.1007/978-3-031-95296-8_4. (05.00.00; №3, Scopus)
4. Кабулов А. & Жўраев М. Продукционной модели для анализа сетевых потоков в информационных системах. “Development of science” ilmiy jurnali. 2025/6, Volume 4. -P. 470-483. (05.00.00; OAK Rayosatining 2025 – yil 12-fevraldagi 376–son qarori)
5. Kabulov A. & Juraev M. A new approach to intelligent network traffic flow analysis. Development of science ilmiy jurnali, 2025/6, Volume 2. -P. 363-372. (05.00.00; OAK Rayosatining 2025 – yil 12-fevraldagi 376–son qarori)
6. Ma’ruf Jo‘rayev. Tarmoq oqimini monitoring qilish dasturiy tizimi. Al-Farg‘oniy avlodlari ilmiy elektron jurnali. Vol. 1, №3, 2024. -B. 73–77. https://doi.org/10.5281/zenodo.13954907. (05.00.00; OAK Rayosatining 2023 – yil 30-sentabrdagi 343–son qarori)
7. Кабулов А.В., Жураев М.Т., Ярашов И.К., Сайманов И.М., Анализ и оценка записанного сетевого потока на основе разделения признаков, Axborot xavfsizligi muammolari ilmiy jurnali, №2 (3), 2025. -C. 50-63. (05.00.00; OAK Rayosatining 2024 – yil 30-noyabrdagi 1099–son qarori)
8. А.В. Кабулов, И.М. Сайманов, И.К. Ярашов, М.Т. Жураев. “Исследование и оценка статистических параметров сетевого потока на основе индексов Херста”, Muhammad al-Xorazmiy avlodlari ilmiy-amaliy va axborot-tahliliy jurnali. № 3 (33), 2025. -C. 71-75. (05.00.00; №10)

II bo‘lim (II часть; II part)

9. Yarashov I., Juraev M., Ismatillayev A., & Rakhimberdiev K. Behavior Modeling in Computerized Production Systems. Proceedings of the 8th International Conference on Future Networks and Distributed Systems Marakech, Morocco-2024. -P. 873-880. doi: 10.1145/3726122.3726249
10. Yarashov I.K., Jo‘rayev M.T., Otaxonov A.A. “Mantiqiy funksiyadan foydalangan holda axborot himoya tizimlarining ishonchlilik holatini tadqiq qilish”

QarDU xabarlari ilmiy-nazariy, uslubiy jurnali. №4/1(59), 2023. -B. 23-30. (01.00.00; OAK Rayosatining 2021 – yil 31-martdagi 295/6–son qarori)

11. Ma’ruf Jo‘rayev, Analytical analysis of mathematical methods for processing computer network flow data, “Zamonaviy innovatsion tadqiqotlarning dolzarb muammolari va rivojlanish tendensiyalari: yechimlar va istiqbollar” mavzusidagi Respublika ilmiy-texnik anjuman materiallari to‘plami. Jizzax -2025. -P. 138-141

12. Ma’ruf Jo‘rayev, TCP flaglarni Markov zanjiri asosida tahlil qilish, “Axborot xavfsizligi sohasida raqamlashtirish muammolari va istiqbollari” Respublika ilmiy-amaliy anjumani materiallari to‘plami. Toshkent-2025. -B. 73-76

13. Normatov I, Juraev M, Development of a decision-making model based on network data flow analysis, Abstracts of the IX International Scientific Conference “Actual problems of applied mathematics and information technologies Al-Khwarizmi 2024”. Tashkent, Uzbekiston-2024. -P. 258-259

14. Ma’ruf Jo‘rayev, Tarmoq trafigini monitoring qilish va tarmoq paketlari tahlili, “Zamonaviy innovatsion tadqiqotlarning dolzarb muammolari va rivojlanish tendensiyalari: yechimlar va istiqbollar” mavzusidagi Respublika ilmiy-texnik anjumani. Jizzax-2024. -B. 190-192

15. Alisher Otakhonov, Maruf Juraev, Detecting the origin of cyberattacks using machine learning and network traffic analysis, International Conference on “Advancing Interdisciplinary Research in Art and Humanities”. Utrecht, Netherlands-2025. -P. 18-25

16. Normatov Ibrokhimali, Dadazhanov Ruzmat, Juraev Maruf, Otakhonov Alisher, Atajonov Muzaffar, Modeling Of Free Space In Porous Media By Hydrodynamic Methods, Abstracts of Second International Conference on “Information Technologies and Their Applications”. Part III. Baku, Azerbaijan-2024, -P. 1–10

17. Jo‘rayev Ma’ruf, Fayziyev Voxid, Pythonda tarmoq skaneri va socket vazifasi, “Zamonaviy innovatsion tadqiqotlarning dolzarb muammolari va rivojlanish tendensiyalari: yechimlar va istiqbollar” mavzusidagi Respublika ilmiy-texnik anjumani. Jizzax-2023. -B. 239-242

18. Kabulov Anvar, Jo’rayev Ma'ruf, Yarashov Inomjon, Analysis of a phishing attack on information system based on production logic, Abstracts of VIII International Scientific Conference “Actual problems of applied mathematics and information technologies Al-Khwarizmi 2023”. Samarkand, Uzbekistan-2023. -P. 244

19. Inomjon Yarashov, Ma’ruf Jo‘rayev, Furqat Rahmonov, The study of cyberattacks occurring on the internet (on the example of a DDoS cyberattack), Conference of Proceedings of “Prospects of Development of Science and Education”. №39. Farg‘ona-2023. -P. 30-33

20. Inomjon Yarashov, Ma’ruf Jo‘rayev, Furqat Rahmonov, Studying the problem of DDoS attacks, Conference of Proceedings of “Prospects of Development of Science and Education”. №39. Farg‘ona-2023. -P. 26-29

21. Inomjon Yarashov, Ma’ruf Jo‘rayev, Fishing hujumlari va ularni oldini olish yechimlari, “Iqtidorli talabalar, magistrantlar, doktorantlar va mustaqil izlanuvchilar” mavzusidagi ilmiy-amaliy anjumanining to‘plami. Farg‘ona-2023. -B. 434-437

22. Ma’ruf Jo‘rayev, Cisco packet tracer yordamida tarmoqni monitoring qilishda netflow yechimlari, “Zamonaviy innovatsion tadqiqotlarning dolzarb muammolari va rivojlanish tendensiyalari: yechimlar va istiqbollar” mavzusidagi Respublika ilmiy-texnik anjumani. Jizzax-2023. -B. 242-246

23. Tangriberdiyev O.B., Normatov I.X., Otaxonov A.A., Jo‘rayev M.T., Yarashov I.K., Qaror qabul qilishni qo‘llab-quvvatlashning intellektual tizimlari himoyasi dasturiy ta’minoti, O‘zbekiston Respublikasi Adliya vazirligi. Elektron hisoblash mashinalari uchun yaratilgan dasturning rasmiy ro‘yxatdan o‘tkazilganligi to‘g‘risidagi guvohnoma № DGU 45143. Toshkent, 05.12.2024

24. Kabulov A.V., Yarashov I.K., Otaxonov A.A., Jo‘rayev M.T., Amonov S.X., Axborot himoyasi uchun ma’lumotlar oqimini monitoring qilish dasturi, O‘zbekiston Respublikasi Adliya vazirligi. Elektron hisoblash mashinalari uchun yaratilgan dasturning rasmiy ro‘yxatdan o‘tkazilganligi to‘g‘risidagi guvohnoma № DGU 23375. Toshkent, 31.03.2023

25. Kabulov A.V., Jo‘rayev M.T., Yarashov I.K., Babadjanov A.F., Funksional jadvallar asosida axborotni himoya qilishni ta’minlashda tahdidlarni aniqlash va zararsizlantirishning intellektual usullari va texnologiyalari dasturiy ta’minoti, O‘zbekiston Respublikasi Adliya vazirligi. Elektron hisoblash mashinalari uchun yaratilgan dasturning rasmiy ro‘yxatdan o‘tkazilganligi to‘g‘risidagi guvohnoma № DGU 38256. Toshkent, 18.05.2024

26. Kabulov A.V., Jo‘rayev M.T., Yarashov I.K., Raxmonov F.D., DDOS hujumlarni aniqlash uchun tizim monitoringi dasturi, O‘zbekiston Respublikasi Adliya vazirligi. Elektron hisoblash mashinalari uchun yaratilgan dasturning rasmiy ro‘yxatdan o‘tkazilganligi to‘g‘risidagi guvohnoma № DGU 37529. Toshkent, 08.05.2024.

27. Kabulov A.V., Jo‘rayev M.T., Yarashov I.K., Funksional jadval (FT 1.0.0) asosida axborot himoya qilishning immitatsion modeli uchun dasturiy ta’minoti, O‘zbekiston Respublikasi Adliya vazirligi. Elektron hisoblash mashinalari uchun yaratilgan dasturning rasmiy ro‘yxatdan o‘tkazilganligi to‘g‘risidagi guvohnoma № DGU 38255. Toshkent, 18.05.2024

28. Amonov S.X., Jo‘rayev M.T., Axborot tizimida buyruqlar orqali Firewallni boshqarish dasturiy ta’minoti, O‘zbekiston Respublikasi Adliya vazirligi. Elektron hisoblash mashinalari uchun yaratilgan dasturning rasmiy ro‘yxatdan o‘tkazilganligi to‘g‘risidagi guvohnoma № DGU 32576. Toshkent, 16.01.2024

29. Kabulov A.V., Jo‘rayev M.T., Yarashov I.K., Ergashev B.A., Taqsimlangan tizimlarda qoidalarga asoslangan kirishni boshqarishni dasturiy ta’minoti, O‘zbekiston Respublikasi Adliya vazirligi. Elektron hisoblash mashinalari uchun yaratilgan dasturning rasmiy ro‘yxatdan o‘tkazilganligi to‘g‘risidagi guvohnoma № DGU 27038. Toshkent, 26.08.2023

Avtoreferat “Muhammad al-Xorazmiy avlodlari” ilmiy jurnali tahririyatida tahrirdan o‘tkazildi hamda o‘zbek, rus va ingliz tillaridagi matnlarini mosligi tekshirildi.

Bichimi 60x84$^{1}/_{16}$. Raqamli bosma usulida chop etildi. Times New Roman garniturasi. Shartli bosma tabog‘i: 3. Adadi 100. Buyurtma № 15. «O‘zR Fanlar Akademiyasi Asosiy kutubxonasi» bosmaxonasida chop etilgan. Bosmaxona manzili: 100170, Toshkent sh., Ziyolilar ko‘chasi 13-uy.