ՀԱՅԱՍՏԱՆԻ ԱԶԳԱՅԻՆ ՊՈԼԻՏԵԽՆԻԿԱԿԱՆ ՀԱՄԱԼՍԱՐԱՆ

**ՀՈՎՀԱՆՆԻՍՅԱՆ ԾԱՂԻԿ ՍՏԵՓԱՆԻ**

# ԿՈՐՊՈՐԱՏԻՎ ՀԵՌԱՀԱՂՈՐԴԱԿՑԱԿԱՆ ՑԱՆՑԵՐԻ ՕՊԵՐԱՏԻՎ ԿԱՌԱՎԱՐՄԱՆ ՄԻՋՈՑՆԵՐԻ ՄՇԱԿՈՒՄԸ

ԱՏԵՆԱԽՈՍՈՒԹՅՈՒՆ

Ե.12.03 - «Հեռահաղորդակցական ցանցեր, սարքավորումներ և համակարգեր» մասնագիտությամբ տեխնիկական գիտությունների թեկնածուի գիտական աստիճանի համար

Գիտական ղեկավար՝ տ.գ.դ., Գ.Տ. Կիրակոսյան

Երևան 2017

## Բովանդակություն

# Ներածություն

**<u>Թեմայի արդիականությունը</u>:** Կորպորատիվ հեռահաղորդակցական ցանցերը շարունակ բարդանում են մի շարք պատճառներով. դրանցից են՝ նոր տեխնոլոգիաների, արձանագրությունների ստեղծումը, հեռահաղորդակցական ցանցի թողունակության, հասանելիության և անվտանգության մակարդակի ավելացումը: Կան բազմաթիվ այլ պատճառներ, որոնցից են հեռահաղորդակցական ցանցի օգտատերերի քանակի ավելացումը, հաղորդվող տվյալների արժեքի և թողունակության մեծացումը:

Նման պայմաններում կտրուկ մեծանում է կորպորատիվ հեռահաղորդակցական ցանցով անցնող տրաֆիկը: Ցանցի օպերատորների համար դժվարանում է յուրաքանչյուր հաղորդվող փաթեթի հսկումը, որին զուգընթաց կորպորատիվ հեռահաղորդակցական ցանցերի վրա գրոհները շատանում են, և դրանց իրականացման եղանակները հետզհետե բարդանում են:

Հեռահաղորդակցական ցանցերի վրա հարձակումները և չարտոնված մուտքի փորձերը մեծ վնասներ են հասցնում այդ ցանցերի միջոցով բազմապիսի ծառայություններ մատուցող կազմակերպություններին [64]: Նման դեպքերում ավելանում է ցանցի ծանրաբեռնվածությունը, ինչը շատ հաճախ հանգեցնում է մատուցվող ծառայությունների որակի վատացմանը: Ծառայության որակի համաձայնագրի (SLA, Service Layer Agreement) առկայության դեպքում հեռահաղորդակցական ծառայություններ մատուցող ընկերությունները պարտավոր են հատուցել հաճախորդներին հասցված վնասները: Հետազոտությունները ցույց են տալիս, որ նման խնդիրների պատճառով ոլորտի ընկերությունները կրում են տասնյակ միլիարդավոր դոլարի վնասներ:

Հաղորդակցական մեքենայությունների հսկման ասոցիացիայի (Communications Fraud Control Association, CFCA) կատարած հետազոտությունները ցույց են տալիս, որ հեռահաղորդակցական մեքենայությունների պատճառով տարբեր կազմակերպությունների և անհատների հասցվել է 38.1 միլիարդ ԱՄՆ դոլարի վնաս:

Նման դեպքերից խուսափելու համար անհրաժեշտ է մշակել մեխանիզմներ, որոնք թույլ կտան հայտնաբերել կորպորատիվ հեռահաղորդակցական ցանցերում տեղի ունեցող անոմալիաները և ձեռնարկել կանխարգելիչ կամ վերականգնողական գործողություններ: Վերջին ժամանակներս հեռահաղորդակցական ցանցերում անոմալիաների հայտնաբերումը լայնորեն քննարկվում է գիտական և կոմերցիալ շրջանակներում: Անոմալիաների հայտնաբերումը կիրառվում է անվտանգության, հասանելիության, ծառայության որակի, վիրուսային ծրագրերի հայտնաբերման համար:

Կորպորատիվ հեռահաղորդակցական ցանցերի բնականոն աշխատանքի և ծառայության որակի անհրաժեշտ մակարդակի ապահովման համար անհրաժեշտ է ոչ միայն ունենալ ցանցի ներկա վիճակի մասին տեղեկատվություն, այլև կարողանալ այն կանխատեսել: Արդիական է դիտարկել այնպիսի համակարգի մշակումը, որը թույլ կտա ավտոմատ կերպով հայտնաբերել հեռահաղորդակցական ցանցերում անոմալիաների առաջացումը և հնարավորության դեպքում ձեռնարկել կանխարգելիչ միջոցառումներ: Անոմալիաների հայտնաբերման համար մեքենայական ուսուցման համակարգի ներդրումը հնարավորություն կտա ոչ միայն հայտնաբերել հայտնի պատճառներով առաջացող անոմալիաներ, այլ նաև այնպիսիք, որոնց առաջացման պատճառը նախկինում չի եղել:

**<u>Հետազոտման օբյեկտը</u>**: Ատենախոսության հետազոտման օբյեկտը ԿՀՑ-ներն են և դրանց արդյունավետ օպերատիվ կառավարման կազմակերպումը և իրականացումը:

**<u>Աշխատանքի նպատակը և խնդիրները</u>**: Ատենախոսության նպատակն է՝ հետազոտել կորպորատիվ հեռահաղորդակցական ցանցերի բնականոն աշխատանքին խանգարող խնդիրները և, դիտարկելով ու վերլուծելով ցանցերի մշտադիտարկման արդյունքները, մշակել կորպորատիվ հեռահաղորդակցական ցանցերի օպերատիվ կառավարման միջոցները:

Նշված նպատակներին հասնելու համար ձևակերպվել և լուծվել են հետևյալ խնդիրները.

1. ԿՀՑ-ների կազմակերպման ժամանակակից եղանակների ուսումնասիրումը,

համեմատումը և գնահատումը:

2. ԿՀՑ-ների կառավարման գործիքամիջոցների հետազոտումը, համեմատական վերլուծությունը և ընտրումը:
3. ԿՀՑ-ներում մասնագիտացված սարքերի և սարքավորումների միջոցով ցանցի ստորին շերտերում տրաֆիկը վերահսկելու համար անվտանգության օպերատիվ ղեկավարման համակարգի մշակումը:
4. ԿՀՑ-ների աշխատունակության վրա ազդող անոմալիաների հայտնաբերման մեթոդի և ալգորիթմի մշակումը:
5. ԿՀՑ-ների օպերատիվ կառավարման միջոցների համար նախատեսված ավտոմատացված համակարգի մշակումը:

**<u>Հետազոտման մեթոդները:</u>** Ատենախոսությունում օգտագործվել են կորպորատիվ հեռահաղորդակցական ցանցերի կառուցման տեսական և գործնական եղանակներն ու միջոցները, դիտարկվել են մշտադիտարկման մաթեմատիկական մոդելները և իրականացման համակարգերը, ինչպես նաև արհեստական բանականության եղանակները:

**<u>Գիտական նորույթը</u>:** Հետազոտություններից ստացվել են հետևյալ գիտական արդյունքները.

1. Հիմնավորվել է ԿՀՑ-ների օպերատիվ կառավարման միջոցների իրականացումը մեքենայական ուսուցման համակարգով, ինչը բարձրացնում է ցանցերի հուսալիությունը, աշխատունակությունը և շահագործման արդյունավետությունը:
2. ԿՀՑ-ների օպերատիվ կառավարման գործընթացում խնդիրների լուծման արդյունավետությունը բարձրացնելու համար մշակվել է մեթոդ, որի օգտագործման դեպքում յուրաքանչյուր խնդրի համար փնտրվում է արդեն գոյություն ունեցող լուծումներից այն միակը, որն արդեն հաջողությամբ կիրառվել և փորձարկվել է:
3. Մշակվել է ԿՀՑ-ների օպերատիվ կառավարման համար ինքնուսուցվող համակարգի միջոցով անոմալիաների հայտնաբերման ալգորիթմը:
4. Մշակվել է ԿՀՑ-ների օպերատիվ կառավարման միջոցների համար ցանցերում

անոմալիաների արագ հայտնաբերման և մշակման ավտոմատացված բաց երկխոսային համակարգ, որի կիրառումը բարձրացնում է ցանցի հուսալիությունը, աշխատունակությունը և շահագործման արդյունավետությունը, ինչպես նաև նվազեցնում է ծանրաբեռնվածությունը:

**<u>Պաշպանության են ներկայացված հետևյալ դրույթները</u>.**

1. Կորպորատիվ հեռահաղորդակցական ցանցերի օպերատիվ կառավարման համար արհեստական բանականության եղանակի ընտրության հիմնավորումը:
2. Կորպորատիվ հեռահաղորդակցական ցանցերի աշխատունակության վրա ազդող մեքենայական ուսուցման միջոցով անոմալիաների հայտնաբերման մաթեմատիկական մոդելը, մեթոդը և համակարգի ճարտարապետությունը:
3. Կորպորատիվ հեռահաղորդակցական ցանցերի օպերատիվ կառավարման համար ինքնուսուցման և անոմալիաների հայտնաբերման բաց երկխոսային ավտոմատացված համակարգը:

**<u>Գիտական հիմնադրույթների հավաստիությունը</u>** հիմնավորվել է կատարված հետազոտությունների մեթոդաբանությամբ, կիրառված մաթեմատիկական մոդելներով, մշակված մեթոդների և իրական պրոցեսներին միջոցների (ծրագրային ապահովման) համապատասխանությամբ և աշխատանքի արդյունքների ներդրմամբ:

**<u>Աշխատանքի փորձահավանությունը</u>:** Ատենախոսության հիմնական գիտական և կիրառական դրույթները զեկուցվել ու քննարկվել են ՀԱՊՀ տարեկան գիտաժողովներում՝ (2012-2016թթ.), ՀԱՊՀ ՔՀ և Ց ամբիոնի գիտական սեմինարներում (2011-2016թթ.):

Ատենախոսական աշխատանքն իրականացվել է ՀԱՊՀ-ի ՔՀ և Ց ամբիոնում տարվող գիտահետազոտական և ուսումնամեթոդական աշխատանքների շրջանակներում:

**<u>Աշխատանքի գործնական արժեքը և ներդրումը:</u>** Ատենախոսության արդյունքները կարող են կիրառվել փոքր և մեծ կորպորատիվ հեռահաղորդակցական ցանցերի աշխատունակության բարձրացման և արդյունավետ շահագործումն ապահովելու համար:

Աշխատանքի արդյունքները օգտագործվել և ներդրվել են՝

- Հայկական «Օնլայնաճուրդ» ՍՊԸ-ում, որը մատուցում է աճուրդի կազմակերպման ծառայություն՝ բացառապես օնլայն հարթակում: «Օնլայնաճուրդ» ՍՊԸ-ի կողմից CTNOCAS ավտոմատացված համակարգն օգտագործվում է հեռահաղորդակցական ցանցում խնդիրների հայտնաբերման և ցանցի օպերատիվ կառավարման նպատակով:
- Ռուսական ОМС կազմակերպությունում, որի գլխամասը գտնվում է Մոսկվայում և ունի 35 մասնաճյուղ այլ քաղաքներում: Տվյալ կորպորատիվ հեռահաղորդակցական ցանցի համար.
  - մոդելավորվել է DDoS հարձակում, որի նպատակն է եղել խափանել անվտանգության համակարգերի սպասարկումն ապահովող հեռահաղորդակցական ցանցի աշխատանքը: DDoS հարձակման արդյունքում կտրուկ ավելացել է ցանցի ծանրաբեռնվածությունը, ինչը վաղաժամ հայտնաբերվել է CTNOCAS ավտոմատացված համակարգի կողմից և ադմինիստրատորի կողմից ձեռնարկված համապատասխան միջոցառումներից հետո ցանցի բնականոն աշխատանքը վերականգնվել է:
  - մոդելավորվել է իրավիճակ, երբ կորպորատիվ հեռահաղորդակցական ցանցում վնասակար ծրագրի հայտնվելու հետևանքով մեծացել է ցանցի ծանրաբեռնվածությունը: Տվյալ դեպքում CTNOCAS-ի կողմից վնասակար ծրագրի աշխատանքը հայտնաբերվել է: Այն պայմանավորված է եղել այն հանգամանքով, որ տվյալ ցանցի համար ուսուցման գործընթացում բնականոն և ոչ բնականոն աշխատանքների ծանրաբեռնվածությունների միջակայքը մեծ է եղել:
- «Հայաստանի ազգային պոլիտեխնիկական համալսարանի» (ՀԱՊՀ) «Քոմփյութերային համակարգերի և ցանցեր» (ՔՀ և Ց) ամբիոնում դասավանդվող «Քոմփյութերային ցանցերի կազմակերպում-2» առարկայի լաբորատոր աշխատանքների իրականացման գործընթացում՝ «D-Link սարքավորումներով ցանցերի կազմակերպում» լաբորատոր աշխատանքների մեթոդական ցուցումներ:

**<u>Հրապարակումները</u>:** Ատենախոսության հիմնական դրույթները տպագրվել են 9 գիտական հոդվածում:

**<u>Ատենախոսության կառուցվածքը և ծավալը:</u>** Ատենախոսությունը բաղկացած է ներածությունից, 4 գլխից, եզրակացությունից, 110 անուն օգտագործված գրականության ցանկից և հավելվածից: Աշխատանքը ներառում է 41 նկար և 7 աղյուսակ: Աշխատանքի ընդհանուր ծավալը 131 էջ է: Աշխատանքը գրված է հայերեն լեզվով:

# ԳԼՈՒԽ 1. ԿՈՐՊՈՐԱՏԻՎ ՀԵՌԱՀԱՂՈՐԴԱԿՑԱԿԱՆ ՑԱՆՑԵՐԻ ԶԱՐԳԱՑՄԱՆ ՄԻՏՈՒՄՆԵՐԸ ԵՎ ԿԱՌԱՎԱՐՄԱՆ ՀԻՄՆԱԽՆԴԻՐՆԵՐԸ

Կորպորատիվ հեռահաղորդակցական ցանցը ծրագրային և ապարատային կոմպոնոնտների համակարգ է, որոնք փոխկապակցված են: Ցանկացած ցանց բնութագրվում է տոպոլոգիաներով, արձանագրություններով, ինտերֆեյսներով, ցանցային տեխնիկական և ծրագրային միջոցներով: Ժամանակակից տեղեկատվական տեխնոլոգիաների, առաջավոր հեռահաղորդակցության և կապի միջոցների ներդրումը հրամայական դարձրին տեղեկատվության պաշտպանության վարչական, իրավական և կազմակերպական համալիր միջոցառումների մշակումը՝ տեղեկատվության անվտան-գությունն ապահովելու համար [10, 11]: Հեռահաղորդակցական ոլորտում առկա է մեծ մրցակցություն և առավել մրցունակ է այն կազմակերպությունը, որը տրամադրում է մեծ քանակությամբ ծառայություններ և միաժամանակ ապահովում դրանց բարձր որակը: Սակայն իրական ժամանակում նորանոր ծառայությունների մատուցման անհրաժեշտությունը հանգեցնում է դրանց շահագործման և կառավարման հետ կապված մի շարք խնդիրների: Ներկայումս նշված խնդիրները հաշվի են առնվում ժամանակակից հեռահողորդակցական ցանցերի նախագծման փուլից սկսած, ինչը պարզեցնում է նման ցանցերի կառավարումը, սակայն կան բազմաթիվ շահագործվող հեռահաղորդակցական ցանցեր, որոնցում նշված խնդիրները առկա են և պահանջում են արդյունավետ լուծում:

## 1.1. Կորպորատիվ հեռահաղորդակցական ցանցերի ընթացիկ վիճակը և զարգացման միտումները

Կապիտալ և գործառնական ծախսերի կրճատումը, բիզնես գործընթացների ավտոմատացման և օպտիմալացման շնորհիվ ներդրված գումարների վերադարձի ցուցանիշի բարձրացումը, մատուցվող ծառայությունների որակի բարձրացման արդյունքում հաճախորդների բավարարվածության և լոկալության ցուցանիշի

բարձրացումը, մեծ դեր է խաղում հեռահաղորդակցական ծառայություններ մատուցող կազմակերպությունների մրցակցության մեջ: Այս խնդիրների լուծման համար կարևոր դեր է խաղում նշված ցանցերի կառավարման արդյունավետությունը:

Հեռահաղորդակցական ցանցերի սպասարկումը ենթադրում է ցանցերի մոնիտորինգ և կառավարում, խնդիրների հայտնաբերում և լուծում, ցանցի արտադրողականության կառավարում, ենթակառուցվածքների արդյունավետ բաշխում, մատուցվող ծառայությունների առաջնահերթության որոշում և նմանատիպ այլ խնդիրների լուծում [34,41,47]: Սակայն նշված խնդիրներից շատերի լուծումները համապիտանի են մեկ հեռահաղորդակցական ցանցի շրջանակներում: Հաճախ առաջացած խնդիրը լուծելու համար նոր լուծում որոնելու անհրաժեշտություն չկա, այլ բավարար է կիրառել արդեն իսկ գտած լուծումը:

Ժամանակակից կորպորատիվ հեռահաղորդակցական ցանցային տեխնոլոգիաների զարգացման միտումները կարելի է որակավորել որպես շարժում դեպի կատարելագործումը:

Հեռահաղորդակցական ցանցերում տվյալների և ձայնային տրաֆիկները ունեն այնքան տարբեր հատկություններ, որ դրանք բավականին դժվար է կիրառել նույն ցանցում: Առաջինն ունի ոչ կանխատեսելի բնույթ, այն զբաղեցնում է առկա ցանցային բոլոր ռեսուրսները ժամանակի պատահական հատվածներում, այն դեպքում, երբ երկրորդը ունի կանխատեսվող բնույթ և պահանջում է հասարակ փոխանցում ծայրակետերի միջև սպասման քիչ ժամանակով:

Հեռահաղորդակցական ցանցի [19] առաջին սերունդը դասական հեռախոսային կապն էր (POTS), որն իր մեջ ներառնում էր տեխնոլոգիաների և ցանցային կառուցվածքների ամբողջական լուծումներ, որոնք ի հայտ եկան Integrated Service Digital Network – ISDN ծառայությունների ինտեգրացմամբ թվային ծառայության մեջ:

1980թ.-ից զարգացավ ISDN-ի ցանցային հայեցակարգը ինտեգրացված ցանցերում կարող էր տրամադրել կապի տարբեր ծառայություններ մեկ ինտեգրացված միջավայրում, որի հիմքը, սակայն, մնաց հեռախոսը: ISDN ցանցերը նախատեսում էին հաղորդման թվային համակարգի կիրառումը կոմուտացիայի թվային հանգույցներում:

Ի սկզբանե, ինֆորմացիայի տարբեր տեսակների փոխանցման համար կառուցվել են առանձին կապի կորպորատիվ (գերատեսչական) ցանցեր՝ հեռախոսային ցանցեր, հեռագրային ցանց, տվյալների փոխանցման և այլ ցանցեր: 20-րդ դարի երկրորդ կեսին առաջացավ բոլոր կորպորատիվ կապի ցանցերը մեկի մեջ միավորելու մտահղացումը: Այսպիսով ստեղծվել է ISDN ցանցի հայեցակարգը: ISDN-ցանցի միավորող ցանցը Ընդհանուր օգտագործման հեռախոսային ցանցն է:

1990-ականներին Ինտերնետի հայտնվելուց հետո ինտերնետի հիմնական օգտագործողները դարձան ֆիզիկական անձինք՝ մարդիկ, ովքեր զուգահեռաբար օգտագործում են և՛ հեռախոսային, և՛ ինտերնետային կապը, որը շահագործման և տնտեսական առումներով շահավետ չէր: Դա հանգեցրեց նոր տեխնոլոգիական լուծումների մշակմանը՝ տարբեր տիպի տեղեկատվության կապի տարբեր ծառայությունների միավորմանը մեկ ցանցային ընդհանուր կառուցվածքում: Այս լուծման հիմքում ընկած է փաթեթների կոմուտացիայի միասնական մեթոդը, որի ձևավորումը հանգեցրեց ցանցի 3-րդ սերնդի NGN ցանցերի կիրառմանը [77]: NGN ցանցերի գաղափարով ցանցում առկա կամայական տիպի տեղեկատվությունը պետք է ներկայացվի միասնական IP-փաթեթի տեսքով: Իսկ ավանդական և ժամանակակից ցանցերը պետք է ճանաչեն IP-փաթեթի ֆորմատը և աջակցեն IP-փաթեթի թրաֆիկի փոխանակմանը: NGN-ը մի հայեցակարգ է, որը միտված է այնպիսի հեռահաղորդակցական կորպորատիվ համացանցի կառուցմանը, որի միջոցով հնարավորություն կստեղծվի մի ցանցի սահմաններում տրամադրել տարբեր տիպի ծառայություններ, օրինակ, ինտերնետ հասանելիություն, թվային հեռուստատեսություն, և այլն:

**NGN(Next Generation Network)**

Ինչպես հայտնի է, NGN-ը ցանցերի մշակման և սահմանման հայեցակարգ է. ցանցերի, որը հնարավորություն է տալիս ծառայություններ մատուցողներին և ISP օպերատորներին ծառայությունների ապակենտրոնացված ղեկավարմամբ ստեղծել մուլտիսերվիսային կապի ցանց, որի հիմքն է կազմում առկա համացանցը և կորպորատիվ ցանցերի միասնականությունը, որը ներառում է ինչպես

տրանսպորտային մակարդակի, այնպես էլ կոմուտացիաների և փոխանցումների ղեկավարման մակարդակի գործառույթները [15, 40, 44]: Համաձայն հասարակ սահմանման՝ NGN ցանցը բաց, ստանդարտ փաթեթային ենթակառուցվածք է, որը ընդունակ է արդյունավետորեն աջակցել գոյություն ունեցող հավելվածների ու ծառայությունների ողջ գամմային՝ ապահովելով անհրաժեշտ մասշտաբայնությունը և ճկունությունը՝ թույլ տալով արձագանքել նոր պահանջներին ֆունկցիոնալությամբ և թողունակությամբ:

Այս ցանցերը հիմնվում են ինտերնետ տեխնոլոգիաների վրա՝ ներառելով IP արձանագրություն և MPLS տեխնոլոգիա [22-23,43,106]: Ներկա դրությամբ նախագծված է մի քանի մոտեցում՝ ITU-T և IETF, H.323, SIP և MGCP, IP-տելեֆոնիայի ցանցերի կառուցման համար, որոնք առաջարկված են կազմակերպությունների կողմից:

Այժմ կապուղիների կոմուտացիայով ավանդական ցանցից փաթեթների կոմուտացիայով ցանցերին (NGN) անցման խնդիրը կապի օպերատորների համար ամենաարդիականներից մեկն է: Հեռանկարային նախագծումները IP-կոմուտացիայի միջավայրում կապված են համալիր լուծումների ստեղծման հետ, որոնք NGN ցանցերի զարգացման ժամանակ հնարավորություն են տալիս պահպանել գոյություն ունեցող միացումները և ապահովել անխափան աշխատանք հեռախոսային, գալարազույգ, օպտոթելք մալուխներով, անլար (WiMAX, WiFi) կապով (ETTH, PLC և այլն) ցանցերում: Համաձայն հայեցակարգի NGN-ին անցումը պետք է հնարավորություն տա փոխելով առանձին սեգմենտներ անցնել նոր տեխնոլոգիայի առանց ամբողջ ցանցի կառուցվածքի արմատական փոփոխության [99]: Սակայն NGN-ին անցման համար պետք է բավարարվեն հետևյալ պահանջները.

- գոյություն ունեցող օպերատորի ցանցի աջակցում, նոր տրանսպորտային տեխնոլոգիայի և սովորական կառավարման մոդելի ինտեգրում,
- աշխարհագրական, բաշխված մոդուլային ճարտարապետության հնարավորություններ,
- համակարգում սերվերների ավելացումով արտադրողականության ծավալների մեծացում,

- ծառայությունների նոր հնարավորությունների ներդրում նվազագույն ժամկետներում,
- համապատասխանեցում գոյություն ունեցող ցանցի ճարտարապետությանը և օրենսդրության պահանջներին:

## Անլար ցանցային տեխնոլոգիաների զարգացման միտումները և տարատեսակների համեմատական վերլուծությունը

### WiFi ցանցեր

Wi-Fi (Wireless Fidelity) գրանցվել է 1999 թվականին: Այն անլար ցանցի ստանդարտ է, որն իր մեջ միավորում է մի քանի արձանագրություններ և ունի պաշտոնական անվանում IEEE 802.11 [86]: Սարքավորումները, որոնք նախատեսված են աշխատել IEEE802.11x ստանդարտով հիմնականում բաժանվում են 2 խմբի՝ կլիենտ և Access Point: Կլիենտի դերում կարող են լինել անհատական համակարգիչներ, նոութբուքերը, մոբայլ սարքավորումները և այլն: Access Point-ը նախատեսված է անլար ցանցի կլիենտներին սպասարկելու համար:

Կիրառվում է հիմնականում IEEE 802.11b արձանագրությունը, որտեղ տվյալների հաղորդման համար կիրառվում է 2,4 մինչև 2.4835 ԳՀց հաճախականությունների միջակայքը և ապահովում է առավելագույն 11 մբիթ/վ արագություն մինչև 100 մետր հեռավորության վրա (բաց տարածությունում մինչև 300-400մետր):

### WiMAX տեխնոլոգիա

Անլար ցանցի հաջորդ սերունդ է Wi-Max (Worldwide Interoperability for Microwave Access) ստանդարտը, որը մեծ տարածությունների վրա տարատեսակ սարքավորումների համար համընդհանուր անլար կապի տրամադրման նպատակով նախատեսված հեռահաղորդակցման տեխնոլոգիա է, հիմնված է IEEE 802.16 ստանդարտի վրա, որը նաև կոչվում է Wireless MAN [85]:

Աղյուսակ 1-ում ներկայացված են անլար տեխնոլոգիաներն իրենց ստանդարտներով և հնարավորություններով:

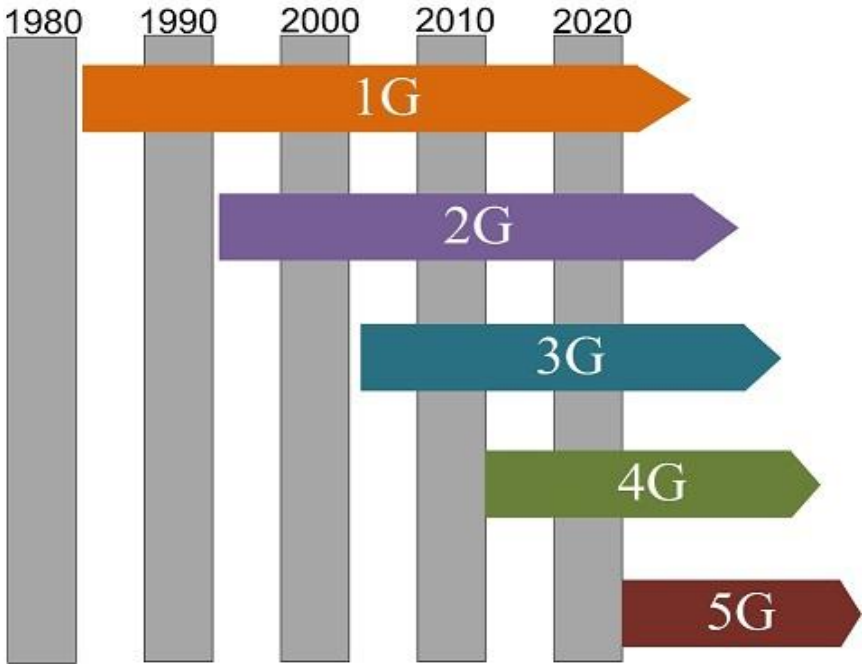
Աղյուսակ 1. Անլար կապի ստանդարտների համեմատական աղյուսակ

| Տեխնո-լոգիա | Ստան-դարտ | Կիրա-ռում | Թողունակություն | Ազդեցության շառավիղ | Հաճախականություն |
|---|---|---|---|---|---|
| Wi-Fi | 802.11a | WLAN | մինչև 54 մբիթ/վրկ | մինչև 300 մետր | 5,0 ԳՀց |
| Wi-Fi | 802.11b | WLAN | մինչև 11 մբիթ/վրկ | մինչև 300 մետր | 2,4 ԳՀց |
| Wi-Fi | 802.11g | WLAN | մինչև 54 մբիթ/վրկ | մինչև 300 մետր | 2,4 ԳՀց |
| Wi-Fi | 802.11n | WLAN | մինչև 300 մբիթ/վրկ | մինչև 300 մետր | 2,4 —2,5կամ 5,0 ԳՀց |
| WiMax | 802.16d | WMAN | մինչև 75 մբիթ/վրկ | 25-80 կմ | 1,5-11 ԳՀց |
| WiMax | 802.16e | Mobile WMAN | մինչև 40 մբիթ/վրկ | 1-5կմ | 2.3-13.6 ԳՀց |
| WiMax | 802.16m | WMAN, Mobile WMAN | մինչև 1 գբիթ/վրկ (WMAN), մինչև 100 մբիթ/վրկ (Mobile WMAN) | Մշակման փուլում է | Մշակման փուլում է |

## Շարժական կապի կառուցվածքը և սերունդները

Ներկայումս, երբ խոսում ենք շարժական կապի մասին, ընդունված է այն բաժանել 4 սերունդների՝ 1-ին սերնդին են (1G) պատկանում 1980-ականների կեսերին ստեղծված շարժական կապի անալոգային կամ կիսաանալոգային (անալոգային ռադիոտրակտ, թվային կոմուտացիա) ցանցեր: Այս ցանցերի բաժանորդներին տրամադրվող հիմնական ծառայությունների մեջ շեշտը դրվում էր ձայնի փոխանցման որակի վրա: Պայմանավորված շարժական կապի առաջարկի մեծացմամբ՝ անհրաժեշտություն առաջացավ ստեղծելու համընդհանուր շարժական կապի համակարգ, որով և զբաղվեցին միջազգային ստանդարտացման օրգանները [25,31]:

Նրանք սկսեցին մշակել երկրորդ սերնդի (2G) շարժական կապի հիմնական բնութագրերը:: Երկրորդ սերնդի (2G) ցանցում ավելացվեց տրամադրվող ծառայությունների ցանկը: Ստանդարտացման տարածաշրջանային մոտեցումը թույլ տվեց լիարժեք իրագործել գլոբալ շարժական կապի հայեցակարգն և արդյունքում շուկայում հայտնվեցին 2G համակարգի մի քանի տարբերակներ: Դրանց շարքում, կոմերցիոն շահավետության տեսակետից, կարելի է առանձնացնել գլոբալ շարժական կապի համակարգը (GSM) և նրա տարատեսակները [35, 45]:




Նկ. 1. Շարժական կապի սերունդերը

Շարժական կապի գլոբալացման ընթացքը պետք է ավարտվեր երրորդ սերնդի (3G) համակարգերով: Բայց և այստեղ առաջացան բարդություններ՝ պայմանավորված ազգային և տարածաշրջանային հետաքրքրությունների հետ: Այսպես թե այնպես, ընդհանուր միտումն այնպիսին էր, որ 3G համակարգերը հիմնականում պետք է հենվեին GSM տեխնիկական լուծումների վրա՝ ելնելով հետևյալ երկու պատճառից. շուկայում գերակշռում էր GSM տեխնոլոգիան և նրանում ներդրված ահռելի գումարները պետք է փոխծածկվեին:

Չորրորդ սերնդի շարժական համակարգերի (4G) հիմնական անհրաժեշտությունը առաջանում է տեխնոլոգիական հնարավորությունների ընդլայնման արդյունքում և երրորդ սերնդի շարժական ցանցի (3G) ծառայությունների համակարգերի խնդիրները լուծելու նպատակով, որոնք, սարքավորումներ արտադրող առաջադեմ

ընկերությունների կարծիքների, անկարող են բավարարել մուլտիմեդիոն ծառայությունների պահանջարկին:

Աղյուսակ 2. Շարժական կապի սերունդների համեմատական աղյուսակ

| Սերունդ | 1G | 2G | 3G | 3.5G | 4G | 5 G |
|---|---|---|---|---|---|---|
| Մշակման սկիզբը | 1970 | 1980 | 1990 | <2000 | 2000 | |
| Իրագործում | 1984 | 1991 | 2002 | 2006—2007 | 2008—2010 | 2020 |
| Հաղորդման արագություն | 1,9 կբիթ/վ | 9,6-14,4 կբիթ/վ | 2 մբիթ/վ | 3-14 մբիթ/վ | 1 գբիթ/վ | - |
| Ստանդարտ | AMPS, TACS, NMT | TDMA, CDMA, GSM, PDC | WCDMA, CDMA 2000, UMTS | HSDPA | Միասնական ստանդարտ | - |
| Ցանց | PSTN | PSTN | տվյալների փաթեթային հաղորդման ցանց | տվյալների փաթեթայի ն հաղորդման ցանց | Ինտերնետ | Ինտերնետ |

4G բջջային տեխնոլոգիաների նախագիծը բարձր արդյունավետությամբ համընդհանուր գլոբալ ռադիոհասանելիության ցանցի կոնցեպտուալ կառուցվածք է, ուր առկա են մալուխային ցանցին ինտեգրվելու բոլոր հնարավորությունները [21]:

Ենթադրելով, որ բջջային կապի օպերատորի ցանցի զարգացման քաղաքականությունը կարող է հնարավորություն չտալ լիարժեք ծածկույթ ստանալ տվյալ պետության ամբողջ երկայնքով, ապա ուսումնասիրելով այլ բջջային կամ գծային օպերատորների ցանցային խտության ռեսուրսները, նպատակահարմար է ստեղծել միասնական վիրտուալ հիմնահարթակ: Այն իր մեջ կներառի երկրի բոլոր

բջջային և գծային օպերատորների ցանցային ռեսուրսները [2,18]: Հիմնահարթակը թույլ կտա զարգացող պետություններում կիրառելով առկա ցանցային միջոցները՝ խուսափել նոր ֆիանսական ներդրումներից գերատեսչական, մասնագիտացված և կորպորատիվ ցանցեր կազմակերպելու համար [26,30,32]:

Տրաֆիկի կառավարումը չափազանց կարևով հատկություն է արագ փոփոխման դինամիկա ունեցող բջջային ցանցերի կապուղիների համար: Այսպիսով դա հիմնահարթակին հնարավորության կտա չծանրաբեռնել մեկ օպերատերի մագիստրալային ռեսուրսները, այլ օգտագործել տվյալ պահի ավելի ազատ գտվող գիծը: Այսպիսով MPLS երթուղավորման տեխնոլոգիայով իրականացաված հիմնահարթակը ստանում է բարձր ճկունություն:

## 1.2. Կորպորատիվ հեռահաղորդակցական ցանցերի կազմակերպման արդի վիճակը, առանձնահատկությունները և դժվարությունները

Այսօր տեղի են ունենում կորպորատիվ հեռահաղորդակցական ցանցերում փոխանցվող ինֆորմացիայի կառուցվածքի և բնույթի լրջագույն փոփոխություններ: Փոփոխվում են ցանցի կառուցման մոտեցումները, իսկ առաջին պլան են դուրս գալիս նոր սերնդի ցանցերը, այսպես կոչված բազմասերվիսային ցանցերը [16]:

Բազմասերվիսային ցանցը միացյալ ցանց է, որը ունակ է փոխանցել ձայնը, տեսապատկերները և տվյալները: Բազմասերվիսային ցանցերի ի հայտ գալը կարող է ունենալ վճռական ազդեցություն հեռահաղորդակցման և տվյալների փոխանցման բնագավառի զարգացման վրա: Այդպիսի ցանցերի հիմնական բնութագիրը նույն որակով տարբեր տիպի թրաֆիկի փոխանցումն է, կապի թողունակությունը, փաթեթների կոմուտացիան և ղեկավարելիությունը:

Բազմասերվիսային ցանցի կառուցումը կապված է տվյալների թրաֆիկի աճի տեմպերի հետ, ինչն անհամեմատելի է ձայնային թրաֆիկի հետ: Այստեղ ներկայացված է կապուղային կոմուտացիայով TDM-ցանցերի աստիճանաբար անցումը փաթեթային ցանցերի:

Ժամանակակից հեռահաղորդակցական ցանցային տեխնոլոգիաների զարգացման միտումները կարելի է որակավորել որպես շարժում դեպի դրանց կատարելագործումը [38,49,101]:

Տվյալների և ձայնային տրաֆիկը ունեն այնքան տարբեր հատկություններ, որ դրանք բավականին դժվար է կիրառել նույն ցանցում: Առաջինն ունի ոչ կանխատեսելի բնույթ, այն զբաղեցնում է առկա ցանացային բոլոր ռեսուրսները ժամանակի պատահական հատվածներում, այն դեպքում, երբ երկրորդն ունի կանխատեսվող բնույթ և պահանջում է հասարակ փոխանցում ծայրակատերի միջև սպասման քիչ ժամանակով:

Բազմասերվիսայնությունն ընդգրկում է մի քանի ասպեկտներ, որոնք վերաբերում են ցանցի կազմակերպման տարբեր կողմերին.

– ցանցի բեռնման զուգամիտություն՝ միացում, որը որոշում է տարբեր տեսակի տրաֆիկի փոխանցումը տվյալների ներկայացման միացյալ ֆորմատի շրջանակներում: Օրինակ, ներկայումս աուդիո և վիդեո տրաֆիկի փոխանցումը կատարվում է կանալային կոմուտացիայիով աշխատող ցանցերի միջոցով, իսկ տվյալների փոխանցումը՝ փաթեթային կոմուտացիայով ցանցերով: Ցանցի բեռնման զուգամիտությունը (կոնվերգենցիա) որոշում է փաթեթների կոմուտացիայով ցանցերի աուդիո և վիդեո փաթեթների փոխանցման օգտագործման միտումը:

– արձանագրությունների զուգամիտությունը, որը որոշում է գոյություն ունեցող բազմաքանակ ցանցային արձանագրություններից մեկ ընդհանուրին (որպես կանոն IP) անցումը: Այն դեպքում, երբ գոյություն ունեցող ցանցերը նախատեսված են բազմաթիվ արձանագրությունների՝ ղեկավարման համար, ինչպիսին են IP, IPX, AppleTalk, նույն տիպի թրաֆիկը, մինչդեռ բազմասերվիսային ցանցերը հիմնվում են մեկ արձանագրությունների և տարբեր սերվիսների վրա, որոնք անհրաժեշտ են տարատեսակ թրաֆիկի ապահովման համար,

– ֆիզիկական զուգամիտություն, որը որոշում է տարբեր տեսակի տրաֆիկների փոխանցումը մեկ միասնական ցանցային ենթակառուցվածքի շրջանակներում: Ե՛վ մուլտիմեդիային տրաֆիկը, և՛ ձայնայինը կարող են փոխանցվել միևնույն սարքավորումների կիրառմամբ՝ հաշվի առնելով թողունակության և հապաղման

պահանջները: Ռեսուրսների պահուստավորման արձանագրությունները, հերթերի առաջնայնության ձևավորումը և սպասարկման որակը (QoS) թույլ են տալիս տարբերակել ծառայությունները տրաֆիկի տարբեր տեսակների համար,

– սարքավորումների զուգամիտությունը, որը որոշում է այն ցանցային սարքավորումների կառուցման ճարտարապետության միտումը, որոնք ունակ են մեկ ընդհանուր համակարգի շրջանակներում ապահովել տարատեսակ տրաֆիկ: Այսպիսով, կոմուտատորը Ethernet-փաթեթների կոմուտացիան է, IP-երթուղավորումը ATM միացումները: Ցանցի սարքավորումներիը կարող են մշակել տվյալներ, որոնք փոխանցվում են՝ համաձայն ցանցի ընդհանուր արձանագրության (օրինակ IP) և ունեն սերվիսային տարբեր պահանջներ (օրինակ հապաղման ժամանակը): Բացի այդ, սարքավորումները կարող են ապահովել ինչպես Web-կողմնորոշված հավելվածներ, այնպես էլ փաթեթային հեռախոսակապ,

– հավելվածների զուգամիտությունը, որը որոշում է տարբեր ֆունկցիաների միավորումը մեկ միացյալ ծրագրային միջոցի շրջանակներում: Օրինակ Web-բրաուզերը թույլ է տալիս մեկ էջի շրջանակներում միավորել այնպիսի տվյալներ ինչպիսիք են ձայնը, տեսաազդանշանը և բարձր թողունակությամբ գրաֆիկներ;

– տեխնոլոգիաների զուգամիտությունը ցույց է տալիս կապի ցանցերի համար մեկ ընդհանուր տեխնիկական բազա ստեղծելու ձգտումը, որոնք ունակ են բավարարելու ինչպես տարածաշրջանային, այնպես էլ տեղային հաշվողական ցանցերի պահանջները: Այդպիսի բազա արդեն գոյություն ունի. օրինակ փոխանցման ասինխրոն համակարգը (ATM) կարող է օգտագործվել բավարարելու ինչպես ռեգիոնալ այնպես էլ լոկալ հաշվողական ցանցերին,

– կազմակերպչական զուգամիտությունը առաջարկում է ցանցային, հեռահաղորդակցական, ինֆորմացիոն ծառայությունների կենտրոնացումը, որոնք ղեկավարվում են բարձր օղակի մենեջերի, օրինակ՝ փոխտնօրենի կողմից: Դա ապահովվում է անհրաժետ կազմակերպչական նախադրյալներ ձայնի, տեսաազդանշանի և տվյալների ինտեգրում մեկ ընդհանուր ցանցում:

Թվարկած բոլոր ասպեկտներով որոշվում են այն բազմասերվիսային ցանցի կառուցման տարբեր կողմերը, որոնք ունակ են փոխանցել տարբեր տեսակի տրաֆիկը ցանցի ծայրամասում, այնպես էլ նրա միջուկում:

Բազմասերվիսային ցանցերի հիմնական խնդիրը տարբեր կոմուտացիոն ենթահամակարգերի համագործակցության ապահովումն է, որպեսզի ձայնի, վիդեոի և այլ տվյալների փոխանցման համար օգտագործվի միացյալ ենթակառուցվածք:

Լինուքս օպերացիոն համակարգի (ՕՀ) տարբեր դիստրիբյուտիվներ ունեցող տարասերվեր կորպորատիվ հեռահաղորդակցական ցանցերում թրաֆիկի կառավարման երթուղավորման գործընթացի արդյունավետության բարձրացման համար առաջարկվում է երթուղավորման ստատիկ, արտահանվող-տարանցիկ երթուղիների առանձնահատկությունների համար կիրառել նոր ծրագրային մեթոդներ՝ դեմոններ, տարբեր HP-UX, FreeBSD, RedHat ՕՀ-երի համար [59]:

Առաջին անգամ ինքնանման տրաֆիկի մասին խոսվել է 1993 թ.-ին ամերիկացի մի խումբ գիտնականների կողմից, ովքեր հետազոտելով Ethrnet-տրաֆիկը Bellcore կորպորացիայի ցանցում հայտնաբերեցին, որ մեծ մասշտաբներում այն ունի ինքնանման բնույթ, այսինքն՝ որակապես նույնն է ցանկացած (բավական մեծ) ժամանակային տիրությում: Պարզվեց, որ ցանցի տրաֆիկն ունի ինքնանման հատկություն, հիշողություն, ինչպես նաև ունի բարձր հաճախություն: Այդ իսկ պատճառով ինֆորմացիայի բաշխման համակարգի հաշվարկը դասական բանաձևերի միջոցով տալիս է ոչ ճիշտ, չարդարացված ադյունքներ:

**Ինքնանման** տրաֆիկի պայմաններում քոմփյութերային ցանցի հաշվարկման մեթոդները (կապուղու թողունակություն, բուֆերի տարողություն և այլն) հիմնված են մարկովյան մոդելների և Էրլանգի բանաձևի վրա (որոնք մեծ հաջողությամբ օգտագործվում են հեռախոսային ցանցերի նախագծման ժամանակ), սակայն տալիս են չարդարացված լավատեսական լուծումներ և բերում են ծանրաբեռնվածության թերագնահատմանը:

Այս աշխատանքներում ապացուցվում է, որ իր բնույթով ցանցային տրաֆիկը ինքնանման **(** self-similar) է կամ ֆրակտալ (fractal), այսինքն նրանում առկա են

տվյալների այսպես կոչված թռիչքներ (burst), որոնք երևում են ժամանակի տարբեր միջակայքերում (միլիվայրկիաններից մինչև րոպեներ և ժամեր) [92]:

Ոչ ֆորմալ ինքնանման պրոցեսը դա պատահական պրոցես է, որի ստատիկ բնութագրերը ցուցաբերում են մասշտաբային հատկություն:

Ի տարբերություն պուասոնյան պրոցեսների, ինքնանման պրոցեսները բնութագրվում են հետևանքի առկայությամբ. հաջորդ (հերթական) իրադարձության ի հայտ գալու հավանականությունը կախված է ոչ միայն ժամանակից, այլև նախորդ իրադարձությունից (նախապատմություն): Սա նշանակում է, որ ժամանակի առանձին պահերին ընթացիկ իրադարձությունների թիվը կախված է մինչ այդ եղած իրադարձությունների թվից:

Անընդհատ ստոխաստիկ $X(t)$ պրոցեսը համարվում է ստատիկ ինքնանման $H$ $(0.5 \leq H \leq 1)$ գործակցով, եթե ցանկացած դրական a թվի համար $X(t)$ և $\alpha^{-H}H(\alpha t)$ պրոցեսները կունենան նույն բաշխվածությունը, այսինքն՝ կունենան նույն ստատիկ հատկությունները բոլոր դրական ամբողջ n թվերի համար:

$$\{X(t_1),X(t_2),\dots X(t_n)\}^D \sim \{\alpha^{-H}X(\alpha t_1),\alpha^{-H}X(\alpha t_2),\dots,\alpha^{-H}X(\alpha t_n)\} \quad (1)$$

Պրակտիկորեն ստատիկ ինքնանմանությունը ենթադրում է, որ կատարվում են հետևյալ պայմանները [11,12,13].

- միջին $E[X(t)] = \frac{E[X(\alpha t)]}{\alpha^H}$ (2)
- դիսպերսիա $V_{\alpha r}[X(t)] = \frac{V_{\alpha r}[X(\alpha t)]}{\alpha^{2H}}$ (3)
- -ավտոկոռելացիայի ֆունկցիա $R(t,\tau) = \frac{R(\alpha t,\alpha \tau)}{\alpha^H}$ (4)

որտեղ $H$-ն Հարսթի (Hurst) գործակիցն է,

$\alpha$-ն դրական թիվ:

Հարսթի գործակիցը ցույց է տալիս ինքնանմանության "աստիճանը": $H$-ի 0,5 արժեքի դեպքում նշանակում է ինքնանմանության բացակայություն, իսկ $H$-ի մեծ արժեքը (մոտ 1-ի) ցույց է տալիս պրոցեսում ինքնանմանության բարձր աստիճանը կամ երկար-կախվածությունը (long-range dependent, LRD): Սա նշանակում է, որ եթե անցյալում LRD պրոցեսն ուներ մեծացման (կամ փոքրացման) միտում, ապա մեծ

հավանականությամբ այն կունենա մեծացման (կամ փոքրացման) միտում նաև ապագայում:

### 1.3. Կորպորատիվ հեռահաղորդակցական ցանցերի օպերատիվ կառավարման մեթոդների վերլուծությունը

Ցանցի մոնիտորինգ ասելով հասկանում ենք այն աշխատանքը, որը կատարվում է ցանցի աշխատանքին անընդհատ հետևելու և որևէ սխալի դեպքում ցանցի ադմինիստրատորին հաղորդելու համար [12, 27]: Օպերացիոն համակարգերում գոյություն ունեն հատուկ ծրագրեր, որոնցով կարելի է իրականացնել ցանցի մոնիթորինգը: Կորպորատիվ հեռահաղորդակցական ցանցերի աշխատանքի ղեկավարումը բաժանվում է երկու փուլի.

- մոնիտորինգ,
- անալիզ:

Մոնիտորինգի փուլում կատարվում է պարզ գործողություն՝ ցանցի աշխատանքի մասին առաջնային տվյալների հավաքագրում. կատարվում է վիճակագրություն ցանցում գործող բոլոր կադրերի և տարբեր արձանագրությունների փաթեթների, հաբերի, բնիկների, կոմուտատորների և երթուղավորիչների վիճակի մասին:

Այնուհետև իրականացվում է վերլուծություն, որը բարդ և ինտելեկտուալ գործողություն է, մոնիտորինգի փուլում հավաքված ինֆորմացիայի իմաստավորում, համեմատվում է նախկինում ստացված տվյալների և արդյունքների հետ, որի հիման վրա կատարվում է ցանցում տեղի ունեցող դանդաղումների, աշխատանքային գործընթացների խափանումների հնարավոր պատճառների մասին եզրահանգումների մշակում: Մոնիտորինգի խնդիրները որոշվում են ծրագրային և ապարատային չափիչներով, տեստերով, ցանցային անալիզատորներով, ինչպես նաև ղեկավարման համակարգի գործակալով:

Անալիզի խնդիրը պահանջում է մարդու ակտիվ մասնակցություն և այնպիսի բարդ միջոցների օգտագործում, ինչպիսիք են մասնագիտացված համակարգերը, ցանցային մասնագետների գործնական փորձը [28-29]:

**Մոնիտորինգի և անալիզի միջոցների դասակարգումը**

Բոլոր տարատեսակ միջոցները,որոնք կիրառվում են անալիզի և հեռահաղորդակցական ցանցերի ախտորոշման համար,կարելի է բաժանել մի քանի խոշոր դասերի.

- **Ղեկավարման համակարգի գործակալները** սատարում են ստանդարտ MIB –ի ֆունկցիաներից մեկը և տեղադրում են ինֆորմացիա SNMP կամ CMIP արձանագրության միջոցով: Գործակալներից տվյալներ ստանալու համար պահանջվում են կառավարման համակարգեր, որոնք հավաքում են տվյալներ ավտոմատ ռեժիմում:
- **Համակարգում և կառավարում** (Embedded systems): Այդ համակարգը իրականացվում է ծրագրաապարատային մոդուլի տեսքով, որոնք տեղադրում են կոմունիկացիոն սարքավորումներ, ինչպես նաև ծրագրային մոդուլի տեսքով [51]: Այն իրականացնում է արատորոշման ֆունկցիա և ղեկավարում միայն մեկ միջոցով: Այդ դասի օրինակ է Ethernet բազմասեգմենտային ղեկավարման մոդուլը, որը սխալի հայտնաբերման դեպքում իրականացնում է բնիկների սեգմենտացիա:
- Ա**րձանագրությունների անալիզատորները** ծրագրային կամ ապարատա-ծրագրային համակարգեր են, որոնք ղեկավարման համակարգից տարբերվում են ցանցում մոնիտորինգի և վերլուծության տրաֆիկի գործառույթներով: Արձանագրությունների անալիզատորները առանձին փաթեթների նվաճման համար թույլատրում են տեղադրել մի քանի տրամաբանական պայմաններ:
- **Մալուխային համակարգի արատորոշման և սերտիֆիկացիայ**ի համար սարքերը պայմանականորեն կարելի է բաժանել չորս հիմնական խմբի՝

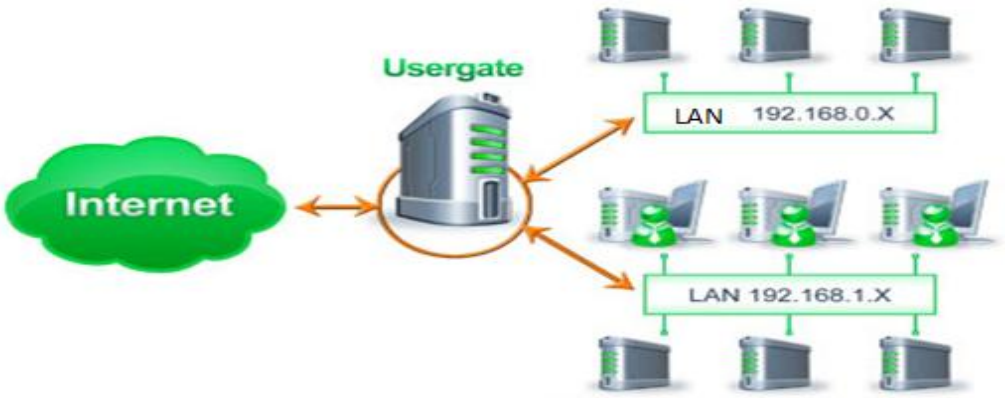
1. ցանցային մոնիտորներ,
2. մալուխային համակարգի սերտիֆիկացիայի համար նախատեսված նյութեր,
3. մալուխային սկաներներ,
4. տեստերներ:

- **Ցանցային մոնիտորներ** (կոչվում են նաև ցանցային անալիզատորներ) օգտագործում են մալուխային տարբեր մակրդակների թեստավորման համար: Այս սարքերը ավելի ինտելեկտուալ են, քան տվյալ դասի չորս խմբերը, քանի որ ֆիզիկական մակարդակից բացի աշխատում են կապուղային, երբեմն էլ ցանցային մակարդակում:

- **Մալուխային համակարգի սերտիֆիկացիայի** համար նախատեսված սարքավորումներն իրականացնում են սերտիֆիկացիա մալուխային համակարգի միջազգային ստանդարտներից մեկի պահանջների հետ համատեղ:
- **Մալուխային սկաները** օգտագործում են մալուխային համակարգի արատորոշման համար:

### 1.3.1. Հեռահաղորդակցական ցանցերի տրաֆիկի ղեկավարման ծրագրեր

UserGate–ը, որը պրոքսի սերվեր (Proxy Server) է, ապահովում է լոկալ ցանցի օգտագործողների մուտքը ինտերնետ: UserGate -ն ապահովում է ինտերնետ կապերի կենտրոնացված կառավարում [9]:




Նկ. 2. UserGate ծրագրի իրականացումը

UserGate–ի առանձնահատկություններից է.

- յուրաքանչյուր օգտագործողի սահմանափակումների ճկուն ղեկավարում,
- ցանցի բոլոր պրոցեսների մոնիտորինգ,
- օգտագործողի ընթացիկ հաշվեկշիռի որոշում,
- ինտերնետ մուտքի սահմանափակում,
- ինտերնետ երթուղու սահմանափակում:

Այս առանձնահատկությունները ծրագիրը դարձնում են անփոխարինելի լոկալ ցանցում ծառայությունների մատուցման, օգտագործողների ղեկավարման և ինտերնետի ծախսերի օպտիմացման համար:

Հաշվի առնելով ուսումնասիրությունները՝ կարելի է համեմատական գնահատել ցանցային տրաֆիկի ծրագրային փաթեթները.

Աղյուսակ 3. Ցանցային տրաֆիկի ծրագրային փաթեթների համեմատում

| | Traffic Inspector | UserGate | Kerio |
|---|---|---|---|
| Ամբողջ ցանցի ղեկավարում | այո | այո | այո |
| Տրաֆիկի մոնիտորինգ | Ռեալ ժամանակում | Ռեալ ժամանակում | Ռեալ ժամանակում |
| User-ի արագության ղեկավարում | Անհատական և խմբակային | Անհատական և խմբակային | Անհատական և խմբակային |
| Տվյալների քեշավորում | այո | այո | այո |
| Տրաֆիկի ֆիլտրացում | Ներքին/արտաքին | Ներքին/արտաքին | Ներքին/արտաքին |
| Տրաֆիկի հաշվարկ | Տրաֆիկին հմպ | Տրաֆիկին հմպ | Տրաֆիկին հմպ |
| Հակավիրուսային անվտանգություն | այո | այո | այո |
| Ցանցի տիպը | Լոկալ/Կորպորատիվ | Լոկալ/Կորպորատիվ | Լոկալ/Կորպորատիվ |
| ՕՀ | Microsoft Windows | Microsoft Windows | Microsoft Windows, Linux |
| Գինը | 150$ | 100$ | 150-500$ Microsoft Windows, 600$ for Linux |

Այս ծրագրային միջոցները նախատեսված են լոկալ կամ կորպորատիվ ցանցերում տրաֆիկի ղեկավարման համար: Ծրագրի ընտրությունը կախված է ղեկավարվող ցանցի կառուցվածքից և ադմինիստրատորի ընտրությունից:

### 1.3.2. Անվճար և բաց կոդով մոնիտորինգի ծրագրերի վերլուծություն

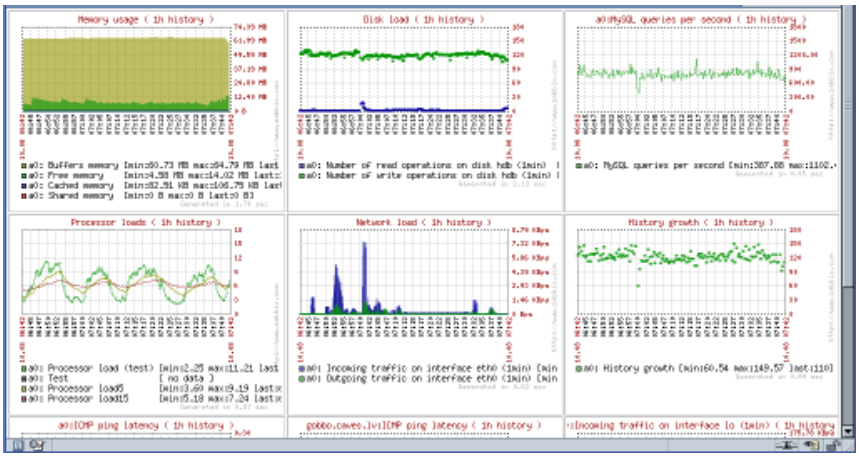
**Zabbix**

Zabbix-ը ցանցի, ցանցային ծառայությունների, սերվերների և մոնիտորինգի համար նախատեսված բաց կոդով ծրագիր է: Zabbix-ը բաղկացած է սերվերից, proxy-ից, ագենտից և վեբ ինտերֆեյսից: Սերվերը, proxy-ին և ագենտը գրված են C լեզվով, վեբ ինտերֆեյսը՝ PHP-ով և Javascript-ով, և նրա աշխատանքի համար պահանջվում է վեբ սերվեր: Zabbix-ը ունի մոնիտորինգի մի քանի տեսակ.

- Simple checks – ստուգում է հոստի հասանելիությունը և ստանդարտ ծառայությունների (օրինակ HTTP և SMTP) արագ արձագանքը տեղադրել առանց լրացուցիչ ծրագրային ապահովման,
- ZABBIX agent – տեղադրվում է UNIX-անման կամ Windows համակարգերի վրա, պրոցեսորի ծանրաբեռնվածության, օգտագործվող ցանցի, սկավառակային տարածության և այլ ինֆորմացիաների ստացման համար:
- External check – ZABBIX մոնիտորինգը կարող է իրականացնել SNMP, TCP և ICMP-ի:

Zabbix -ի առանձնահատկություններն են.

- բարձր արտադրողականություն և թողունակություն: 1000-ից ավել հոստեր ղեկավարելու հնարավորություն,
- սերվերների և ցանցային սարքավորումների ավտոմատ հայտնաբերում, լոգ ֆայլերի կենտրոնացված մոնիտորինգ միջոցով, ինչպես նաև IPMI, JMX, SSH, telnet-ի միջոցով,
- բաշխված մոնիտորինգ կենտրոնացված վեբ կառավարմամբ,
- օգտագործողների անվտանգ աուդենտիֆիկացիա,



Նկ. 3. ZABBIX մոնիտորինգի ծրագրային փաթեթ

- աուդիտ մատյան,
- ցանցային քարտեզի ստեղծման հնարավորություն,
- ինֆորմացիայի պահպանման համար MySQL, PostgreSQL, SQLite և Oracle տվյալների բազաների օգտագործում,

- Zabbix սերվերը հասանելի է Linux, Solaris, HP-UX, AIX, FreeBSD, NetBSD, OpenBSD, Mac OS/X օպերացիոն համակարգերի վրա,
- Zabbix ագենտը հասանելի է Linux, Solaris, HP-UX, AIX, FreeBSD, OpenBSD, OS X, Tru64/OSF1, Windows 2000, Windows Server 2003, Windows XP, Windows Vista, Windows Server 2008, Windows 7 օպերացիոն համակարգերի վրա
- JMX և SNMP v1, 2, 3 աջակցում
- հիշեցումներ/զգուշացումներ էլ. փոստի, SMS հաղորդագրության և ձայնային ազդանշանների միջոցով,
- վիճակագրության գրաֆիկական պատկերում:

**Nagios**

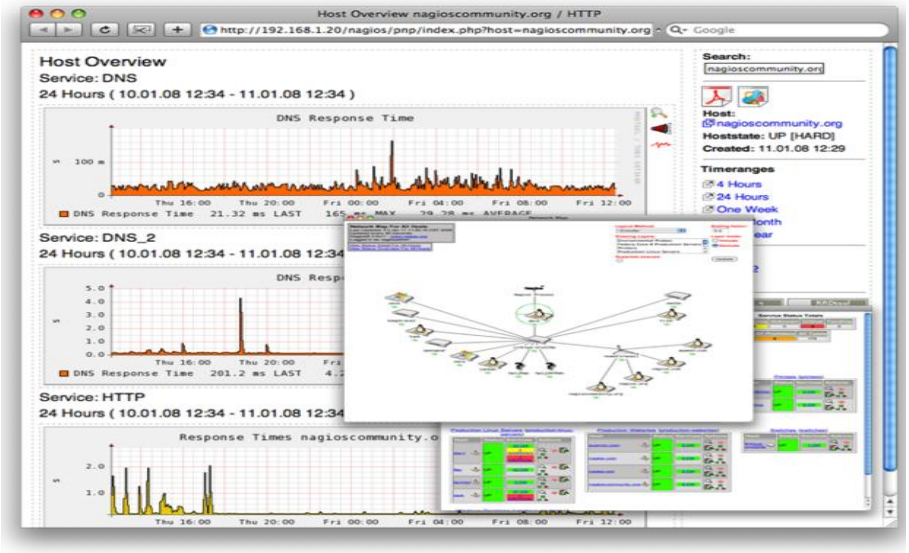
Nagios-ը համակարգչային համակարգերի և ցանցերի մոնիտորինգի համար նախատեսված բաց կոդով ծրագիր է: Սկզբնական շրջանում Նագիոսը նախատեսված էր Լինուքս օպերացիոն համակարգի համար, բայց այն նույնպես շատ լավ աշխատում է մի շարք օպերացիոն համակարգերի՝ Sun Solaris, FreeBSD, AIX և HP-UX-ի հետ:


Նկ. 4. Nagios մոնիտորինգի ծրագրային փաթեթ

Nagios -ի առանձնահատկություններն են՝

- ✓ ցանցային ծառայությունների մոնիտորինգ (SMTP, POP3, HTTP, NNTP, ICMP, SNMP),
- ✓ հոստերի վիճակի մոնիտորինգ (պրոցեսորի բեռնում, սկավառակի օգտագործում, համակարգի տեղեկամատյան) մեծ քանակությամբ ցանցային օպերացիոն համակարգերում,
- ✓ հեռացված մոնիտորինգի օգնությամբ ծածկագրված թունելային ssh կամ SSL,

- ✓ լայն տարածում գտած պարզ ճարտարապետական մոդուլները հնարավորություն են տալիս, օգտագործելով ցանկացած ծրագրավորման լեզու՝ ըստ ցանկության (Shell, C++, Perl, Python, PHP, C# և այլն) հեշտությամբ իրագործվում է իր սեփական ստուգման ծառայությունների մեթոդով,




Նկ. 5. Nagios –ի աշխատանքը

- ✓ զուգահեռաբար իրագործվող ծառայությունների ստուգում,
- ✓ հնարավորություն է տալիս սահմանել «Ծնողական» հոստի օգնությամբ՝ հիերարխիայի ցանցային հոստ, որը թույլ է տալիս հայտնաբերել և տարբերակել հոստերը, որոնք համակարգից դուրս են եկել և որոնք անհասանելի են,
- ✓ հիշեցման ուղարկում, ծառայություններում կամ հոստերում խնդրի առաջացման ժամանակ (փոստի, էջագրիչի, SMS-ի կամ որևէ այլ միջոցով, ինչ-որ կարգով օգտվողի մոդուլի օգնությամբ),
- ✓ հնարավորություն է տալիս սահմանել առաջացած վերամշակման միջոցառումները ծառայությունների կամ հոստերի տվյալ խնդրին նախաձեռնողական լուծում տալու համար,
- ✓ «Մուտք-ֆայլեր»-ի ավտոմատ կերպով ռոտացիայի կատարում,
- ✓ հնարավորություն է տալիս համագործակցելու կազմակերպություններին մի շարք մոնիտորինգի համակարգերի բարելավման գործում,

- ✓ ներառում է «Նագիոսթաթս»-ի ուտիլիտներ, որոնք ցուցադրում են բոլոր հոստերի համար ընդհանուր ամփոփում, որի միջոցով կատարվում է մոնիտորինգ:

**Cacti**

Cacti-ն բաց կոդով, վեբ հիմքով ցանցի թրաֆիկի մոնիտորինգի, պրոցեսորի բեռնվածության, ցանցի թողունակության որոշման համար նախատեսված ծրագիր է, որը RRDtool-ի միջոցով պահպանում է ինֆորմացիա և կառուցում է գրաֆիկաներ: Ծրագիրը գրված է PHP լեզվով, իսկ ինֆորմացիան պահպանվում է MySQL տվյալների բազայում: Cacti -ի առանձնահատկություններն են.

- գրաֆների էլեմենտների անսահմանափակ քանակություն,
- SNMP աջակցում,
- գրաֆիկաների, հոստերի և տվյալների աղբյուրների շաբլոններ/նմուշներ,
- ոչ ստանդարտ ժամանակային կտրվածքով տվյալների հավաքում և մշակում,


Նկ. 6. Cacti ցանցի տրաֆիկի մոնիտորինգի ծրագրային փաթեթ

- գրաֆների տվյալների ծառային և ցուցակային դիտում մոնիտորինգի ծրագրային փաթեթ
- կարող է աշխատել մի քանի օգտագործողի հետ, որոնցից յուրաքանչյուր ունի իր սեփական գրաֆների հավաքածուն
- լրացուցիչ սկրիպների միջոցով կարող է իրականացնել մոնիտորինգ ցանկացած տեսակի տվյալների համար:

Աղյուսակ 4. Մոնիտորինգի ծրագրային փաթեթների համեմատում

| Համակարգի մոնիտորինգի համեմատումը ցանցում | Անվանումը | Nagios | ZABBIX | Ganglia |
|---|---|---|---|---|
| | 1 | 2 | 3 | 4 |
| | Դիագրամներ | + | + | + |
| | SLA հաշվետվություն | Պլագինի միջոցով | + | Անհայտ |
| | Տրամաբանական խմբավորում | + | + | Անհայտ |
| | Trending (զարգացում) | + | + | Անհայտ |
| | Trend Prediction (զարգացման գուշակում) | - | + | Անհայտ |
| | Ավտոմատ հայտնաբերում | Պլագինի միջոցով | + | Անհայտ |
| | Գործակալ | + | Աջակցվում է | + |
| | SNMP | Պլագինի միջոցով | + | Անհայտ |
| | Syslog | Պլագինի միջոցով | + | Անհայտ |
| | Արտաքին սկրիպտներ | + | + | Անհայտ |
| | Պլագիններ | + | + | Անհայտ |
| | | | | |
| | Պլագինի ստեղծման դժվարություն | Հեշտ | Հեշտ | Անհայտ |
| | Տրիգերներ | + | + | Անհայտ |
| | Մուտք Web-ի միջոցով | Դիտում, հաշվետվություն, կառավարում | Լրիվ մուտք | + |
| | Բաշխված մոնիտորինգ | + | + | Անհայտ |
| | Տվյալների պահպանման մեթոդ | Նեղ տվյալների բազա,SQL | SQLite,MySQL,PostgreSQL,Oracle | Անհայտ |
| | Լիցենզիա | GNU GPL | GNU GPL | Լիցենզիա BSD |
| | Քարտեր | Դինամիկ և կառուցող | + | Անհայտ |
| | Լեզու | C | C — ագենտ, սերվեր, պրոքսի; PHP — frontend | C, Perl, PHP, Python |

Հետազոտելով անվճար և բաց կոդերով մոնիտորինգի ծրագրային փաթեթները՝ մեր աշխատանքի համար ընտրել ենք Zabbix –ը, քանի որ նրա ինտերֆեյսը ունի բազմալեզու տարբերակներ և աշխատում է բոլոր օպերացիոն համակարգերի հետ [8, 65,1]:

**Հեռահաղորդակցական ցանցերում SNMP արձանագրություն**

Ինչքան էլ որ լավ լինի կառուցված ցանցը, ցանցային սարքավորումների և համակարգիչների ծրագրային ապահովումները լավ տեղակայված լինեն, ցանցի ղեկավարումը միայն ադմինիստրատորի կողմից չի կարող հսկվել:
Հեռահաղորդակցական ցանցերի օպերատիվ կառավարման առաջարկվող մոտեցման դեպքում անհրաժեշտ է.

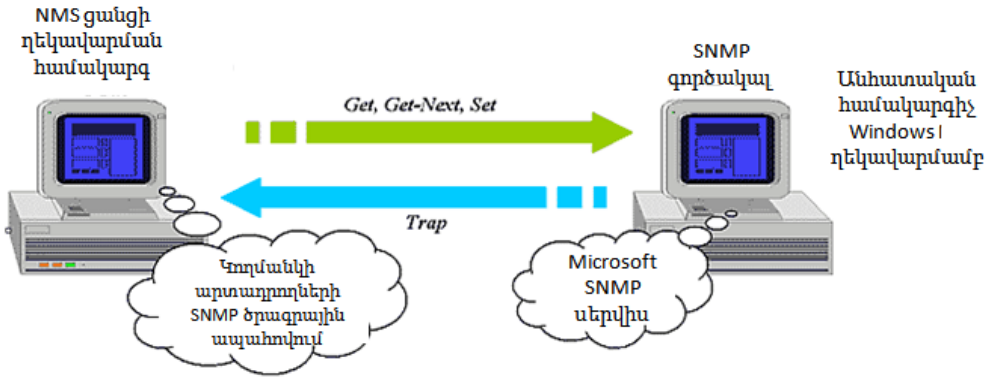
- կատարել հեռահաղորդակցական ցանցի մշտադիտարկում,
- հայտնաբերել հեռահաղորդակցական ցանցերում առաջացած պատահարները,
- հիշել պատահարների լուծման և ծառայությունների մատուցման համար անհրաժեշտ քայլերը,
- անհրաժեշտության դեպքում կիրառել որոշակի խնդիրների համար անհրաժեշտ լուծումները:

Հեռահաղորդակցական ցանցերում թույլ կամ անաշխատունակ հանգույցների հայտնաբերման համար անհրաժեշտ է կատարել մշտադիտարկում և շեղումներ հայտանբերելու դեպքում այդ մասին տեղյակ պահել ադմինիստրատորներին, ովքեր կկարողանան շտկել խափանումը և վերականգնել ցանցի աշխատունակությունը [17,39,48]: Հեռահաղորդակցական ցանցերում անաշխատունակ հանգույցները կարող են զգալի նյութական վնասներ հասցնել այն կազմակերպությանը, որին պատկանում է ցանցը, ուստի կարևոր է, որ ադմինիստրատորները խափանման մասին տեղեկացվեն որքան հնարավոր է շուտ և ունենան բավարար նախնական տեղեկատվություն, որպեսզի կարողանան հնարավորինս արագ վերականգնել ցանցի աշխատունակությունը: Ադմնիստրատորին արագ տեղեկացնելու նպատակով կիրառվում են էլեկտրոնային փոստի, կարճ հաղորդագրության և որոշ դեպքերում՝ հեռախոսային զանգի միջոցով ծանուցման ավտոմատ համակարգեր:

Հեռահաղորդակցական ցանցերում մշտադիտարկումն իրականացնում են այդ նպատակով ստեղծված հատուկ ապարատածրագրային համակարգեր: Նման համակարգերի գործառույթներն են՝ հայտնաբերել ցանցում առկա խափանումները, անոմալիաները, անսարքությունները, ինչպես նաև կատարել դիագնոստիկ և պրոֆիլակտիկ աշխատանքներ: Մշտադիտարկման համակարգերը հսկում են հանգույցների նախապես նշված բնութագրերը, օրինակ CPU-ի ծանրաբեռնվածությունը, հիշողության վիճակը և այլն: Մշտադիտարկման համար կա երկու մոտեցում՝ պասիվ և ակտիվ: Պասիվ մեթոդները հիմնված են ցանցային թրաֆիկի լսելու և վերլուծության վրա, որոնք մեծ տարածում չեն գտել: Ի տարբերություն պասիվ մեթոդի, ակտիվ մեթոդի դեպքում իրականացվում է նպատակային ցանցային փոխազդեցություն համակարգի հետ: Նման մոտեցումներից է ոչ ստանդարտ վերնագրով TCP փաթեթների փոխանակումը:

Որպես կանոն մշտադիտարկումն իրականացվում է լայն տարածում ստացած ICMP (Internet Control Message Protocol) և SNMP (Simple Network Management Protocol) արձանագրությունների միջոցով [27]:

SNMP - նախատեսված TCP/IP փաթեթի համար, և այլ փաթեթների իրականացմանը օրինակ, IPX/SPX (նկ. 7): SNMP արձանագրությունը և նրա հետ սերտորեն կապված SNMP MIB արձանագրությունը մշակվել է երթուղիչ-ինտերնետ համակարգի համար՝ որպես ժամանակավոր լուծում:




Նկ. 7. SNMP-ի աշխատանքի սկզբունքը

SNMP –ն դա «հարց -պատասխան» տիպի արձանագրություն է, այսինքն՝ մենեջերի յուրաքանչյուր դիմումին գործակալը պետք է ուղարկի պատասխան: Արձանագրության առանձնահատկությունը իր ծայրահեղ պարզությունն է, այն ներառում է ընդամենը մի քանի հրահանգ:

*Get-request* –ը հրահանգն օգտագործում է մենեջերը՝ գործակալից իր անունով ցանկացած օբյեկտի արժեքները ձեռք բերելու համար:

GetNext—*request* - հրահանգը օգտագործում է մենեջերը հաջորդ օբյեկտի արժեքը ստանալու համար (առանց ժամկետի երկարաձգման) օբյեկտների աղյուսակի հաջորդական տեսածրման դեպքում:

*Get-response*- Այս հրահանգի օգնությամբ SNMP գործակալը ուղարկում է մենեջերին GetNext—*request կամ Get-request* հրահանգին պատասխան:

Set - հրահանգի օգնությամբ տեղի է ունենում սարքի ինքնավերահսկումը- անջատել պորտը, պորտը միացնել մի կոնկրետ VLAN-ին եւ այլն:

*Trap*- հրահանգն օգտագործում է գործակալը մենեջերին արտառոց դեպքերի զեկույցի համար:

Արձանագրության գլխավոր փոխազդող անձինք գործակալներն են և կառավարման համակարգերը: Եթե դիտենք այդ երկու հասկացությունները լեզվում «հաճախորդ - սերվեր», ապա սերվերի դերը կատարում են գործակալները, այսինքն՝ այդ նույն սարքերը, որի համար էլ հենց մշակվել է արձանագրությունը:

Բոլոր տեղեկությունները համակարգի գործակալի օբյեկտների մասին պահվում է այսպես կոչված Managment Information Base-ում (MIB) - կառավարման տեղեկատվական բազայում, այլ կերպ ասած, MIB-ը օբյեկտների համախումբ է, որոնք հասանելի են յուրաքանչյուր հաճախորդին կարդալ-գրելու գործողությունները՝ կախված կառուցվածքից և հաճախորդի նպատակներից: Կա չորս MIB-ի բազա.

1) Internet MIB - օբյեկտների բազայի տվյալներ: Ներառում է 171 օբյեկտ (այդ թվում MIB I օբյեկտները):

2) LAN manager MIB- բազան 90 օբյեկտից կազմված իր մեջ ներառում է գաղտնաբառեր, սպառողներ, ընդհանուր ռեսուրսներ:

3) WINS MIB – տվյալների բազա օբյեկտների համար, որոնք անհրաժեշտ են WINS սերվերի օգտագործման համար (WINSMIB.DLL):

4) DHCP MIB - տվյալների բազա օբյեկտների համար, որոնք անհրաժեշտ են DHCP սերվերի (DHCPMIB.DLL) օգտագործման համար:

Կառավարման համակարգերում, որոնք հիմնված են SNMP արձանագրության վրա, ստանդարտացվում են հետևյալ տարրերը:

- գործակալների եւ մենեջերների համագործակցության արձանագրություն:
- MIB մոդելների լեզվի և SNMP - ի ուղերձների նկարագրությունը լեզուն, վերացական շարահյուսական նշումների լեզու է՝ ASN.1 (ISO ստանդարտ 8824: առաջարկություններ ITU-T X.208):

Բոլոր MIB-ի անուններն ունեն հիերարխիկ կառուցվածք: Կան տասն արմատային դոմեն:

1) System - այս MIB-ի խումբը պարունակում է յոթ օբյեկտ, որոնցից յուրաքանչյուրը նախատեսված է համակարգի մասին տեղեկություններ պահպանման համար: (ՕՀ տարբերակ,աշխատանքի ժամանակը և այլն),

2) Interfaces - պարունակում է 23 օբյեկտ, որոնք անհրաժեշտ են գործակալների ցանցային ինտերֆեյսի ներածման համար (ինտերֆեյսի քանակը, MTU-ի չափը, ֆիզիկական հասցեներ և այլն),

3) AT- (3 օբյեկտներ) պատասխանատու են հասցեի տեղեկության համար: Այլևս չի օգտագործվում: Ընդգրկվել է MIB I-ում,

4) IP (42 օբյեկտներ) - IP փաթեթների մասին տվյալները (հարցումների և պատասխանների քանակ,

5)ICMP (26 օբյեկտներ)–տեղեկություններ վերահսկողական հաղորդագրությունների մասին (մուտքային / ելքային հաղորդագրություններ և այլն),

6) TCP (19) –այն ամենը, ինչը վերաբերում են նույնանուն տրանսպորտային արձանագրությանը (ալգորիթմներ, հաստատուններ, կապեր և այլն).

7) UDP (6) – նույնը, միայն UDP արձանագրության համար (մուտքային / ելքային դեյթագրամներ),

8) EGP (20) – տվյալներ Exterior Gateway Protocol տրաֆիկի մասին (օգտագործվում է երթուղագծիչների կողմից, օբյեկտները պահում են ստացված / ուղարկած /կադրերի մասին տեղեկատվությունը,

9) Transmission – վերապահված է MIB-ի համար,

10) SNMP (29) – SNMP-ի մասին վիճակագրություն - մուտքային / ելքային փաթեթներ, փաթեթ չափի սահմանափակում, սխալներ և այլն:

### 1.4. Աշխատանքի նպատակը և հետազոտության խնդիրները

Հեռահաղորդակցական ոլորտում առկա է մեծ մրցակցություն, և առավել մրցունակ է այն կազմակերպությունը, որը տրամադրում է մեծ քանակությամբ ծառայություններ և միաժամանակ ապահովում՝ դրանց բարձր որակը: Սակայն իրական ժամանակում նորանոր ծառայությունների մատուցման անհրաժեշտությունը հանգեցնում է դրանց շահագործման և կառավարման հետ կապված մի շարք խնդիրների [1, 2]: Ներկայումս նշված խնդիրները հաշվի են առնվում ժամանակակից կորպորատիվ հեռահաղորդակցական ցանցերի նախագծման փուլից սկսած, ինչը պարզեցնում է նման ցանցերի կառավարումը, սակայն կան բազմաթիվ շահագործվող հեռահաղորդակցական ցանցեր, որոնցում նշված խնդիրները առկա են, դրանց համար պահանջվում են արդյունավետ լուծումներ:

Կապիտալ և գործառնական ծախսերի կրճատումը, բիզնես գործընթացների ավտոմատացման և օպտիմալացման շնորհիվ ներդրված գումարների վերադարձի ցուցանիշի բարձրացումը, մատուցվող ծառայությունների որակի բարձրացման արդյունքում հաճախորդների բավարարվածության և լոկալության ցուցանիշի բարձրացումը մեծ դեր են խաղում հեռահաղորդակցական ծառայություններ մատուցող կազմակերպությունների մրցակցության մեջ: Այս խնդիրների լուծման համար կարևոր դեր է խաղում նշված ցանցերի կառավարման արդյունավետությունը [2, 3]:

Կորպորատիվ հեռահաղորդակցական ցանցերի սպասարկումը ենթադրում է ցանցերի մոնիտորինգ և կառավարում, խնդիրների հայտնաբերում և լուծում, ցանցի արտադրողականության կառավարում, ենթակառուցվածքների արդյունավետ բաշխում, մատուցվող ծառայությունների առաջնահերթության որոշում և նման այլ

խնդիրների լուծում: Սակայն նշված խնդիրներից շատերի լուծումները համապիտանի են մեկ հեռահաղորդակցական ցանցի շրջանակներում: Հաճախ առաջացած խնդիրը լուծելու համար անհրաժեշտ չէ որոնել նոր լուծում, այլ բավարար է կիրառել արդեն իսկ գտած լուծումը:

Արդիական է դիտարկել այնպիսի մեթոդի մշակումը, որով հնարավոր կլինի դասակարգել կառավարման և շահագործման առաջացած խնդիրը, հիշել դրանց լուծումները և անհրաժեշտության դեպքում կիրառել արդեն իսկ հայտնի լուծումը: Այդպիսի մոտեցումը թույլ կտա նվազեցնել հեռահաղորդակցական ցանցերում առաջացող խնդիրների լուծման համար պահանջվող ժամանակն այն դեպքերի համար, երբ արդեն հայտնի է տվյալ խնդրի լուծումը: Դա իր հերթին կհանգեցնի կորպորատիվ հեռահաղորդակցական ցանցի աշխատունակության բարձրացմանը, որը կնպաստի վերջինիս եկամտաբերության ավելացումը: Մեկ այլ խնդիր է որոշակի ծառայությունների մատուցման համար ռեսուրսների պահեստավորումն ու արդյունավետ բաշխումը: Դրա համար պահանջվում է որոշակի կրնկնվող գործողությունների կատարում, որոնք նույնպես կարող են հիշվել և հետագայում կիրառվել՝ զգալիորեն կրճատելով ծառայության մատուցման նախապատրաստման համար պահանջվող ժամանակը:

Ատենախոսության նպատակն է՝ կորպորատիվ հեռահաղորդակցական ցանցերի օպերատիվ կառավարման ժամանակ խնդիրների լուծման արդյունավետությունը բարձրացնելու համար առաջարկել այնպիսի մեթոդ, որի կիրառման դեպքում յուրաքանչյուր խնդրի համար որոնվում են հնարավոր լուծումներ, ինչպես նաև նախագծել կորպորատիվ հեռաղորդակցական ցանցերում մեքենայական ուսուցման միջոցով անոմալիաների հայտնաբերման համակարգ, որի կիրառմամբ ավելի անխափան կլինի ցանցի աշխատանքը:

Նշված նպատակին հասնելու համար ձևակերպվել և լուծվել են հետևյալ խնդիրները.

- կորպորատիվ հեռահաղորդակցական ցանցերի կառուցման ժամանակակից տեխնոլոգիաների հետազոտումը և վերլուծությունը,

- կորպորատիվ հեռաղորդակցական ցանցերի ղեկավարման խնդիրները լուծելու համար հեռահաղորդակցական ցանցերի անվտանգության հետազոտում և ղեկավարման համակարգի առաջադրում,
- ցանցերում անոմալիաների հայտնաբերման արհեստական բանականության եղանակների հետազոտում և վերլուծություն,
- կորպորատիվ հեռաղորդակցական ցանցերում մեքենայական ուսուցման միջոցով անոմալիաների հայտնաբերման համակարգի նախագծում,
- կորպորատիվ հեռահաղորդակցական ցանցերի օպերատիվ կառավարան երկխոսային CTNOCAS ավտոմատացված համակարգի մշակում:

## Գլուխ 1-ի վերաբերյալ եզրակացություններ

Տվյալ գլխում կատարված հետազոտությունների հիման վրա կարելի է հանգել հետևյալ եզրակացությունների.

1. Կորպորատիվ հեռաղորդակցական ցանցերը կառուցվածքային տեսանկյունից կարող են հիմնված լինել տարատիպ տեխնոլոգիաների վրա:
2. Հեռահաղորդակցական ոլորտում առկա է մեծ մրցակցություն, և առավել մրցունակ է այն կազմակերպությունը, որը տրամադրում է մեծ քանակությամբ ծառայություններ:
3. Կորպորատիվ հեռահաղորդակցական ցանցերի սպասարկումը ենթադրում է ցանցերի ճիշտ մոնիտորինգ և կառավարում, որը ցանցերը գրեթե միշտ կպահեն աշխատունակ վիճակում:
4. Իր բնույթով ցանցային տրաֆիկը ինքնանման է (self-similar) կամ ֆրակտալ (fractal), նրանում տվյալները թռիչքներ են, որոնք արտացոլվում են ժամանակի տարբեր պահերին (միլիվայրկյան, վայրկյան, րոպե, ժամ):
5. Վերլուծելով կորպորատիվ հեռահաղորդակցական ցանցերում հիմնականում օգտագործվող մոնիտորիգի ծրագրերը՝ ընտրել ենք Zabbix-ը, քանի որ այն բաց կոդով է և աշխատում է բոլոր օպերացիոն համակարգերի հետ:

# ԳԼՈՒԽ 2. ԿՈՐՊՈՐԱՏԻՎ ՀԵՌԱՀԱՂՈՐԴԱԿՑԱԿԱՆ ՑԱՆՑԵՐԻ ՕՊԵՐԱՏԻՎ ԿԱՌԱՎԱՐՄԱՆ ՄԵԹՈԴՆԵՐԻ ԵՎ ԱԼԳՈՐԻԹՄՆԵՐԻ ՄՇԱԿՈՒՄ

Ժամանակակից կորպորատիվ հեռահաղորդակցական ցանցերին բնորոշ են այնպիսի զարգացումներ, ինչպիսին տվյալների բազաներում (ՏԲ) SS ռեսուրսների կենտրոնացումն է: Կոնսոլիդացիայի գաղափարը, վիրտուալացումը [24], ամպային տեխնոլոգիաները, Web-ծառայությունները, մոբայլ սարքերի թվի և տեսակների աճը, հեռահար աշխատանքը, փոխանցվող և պահվող տվյալների ծավալի մեծացումը, ծառայությունների կենտրոնացումը ստիպում են ավելի մեծ ուշադրություն դարձնել Կորպորատիվ հեռահաղորդակցական ցանցերի (ԿՀՑ) օպտիմալացմանը:

## 2.1. Կորպորատիվ հեռահաղորդակցական ցանցերում անվտանգության դինամիկ կազմակերպումը

Կորպորատիվ հեռահաղորդակցական ցանցերի անվտանգությունը էապես կախված է հոսթերի և տվյալների բազայի անվտագությունից [14,20,33]: Կորպորատիվ Հեռահաղորդակցական ցանցերի անվտանգության համար առաջարկվում է TNSCS (Telekommunication Network Security Control System)՝ Հեռահաղորդակցության ցանցերի անվտանգության ղեկավարման համակարգ, որն ապահովում է հեռահաղորդակցության ցանցերի հուսալի շահագործումը: TNSCS-ն օգտագործում է ծրագրավորվող կոմուտատորներ, որոնք նախատեսված են տրաֆիկը ցանցի ստորին շերտերում վերահսկելու: Նկարագրված է TNSCS - ի կառուցվածքը, ցույց է տրված, թե ինչպես կարող է այն հաղթահարել առկա խնդիրները և ապահովել անվտանգության նոր գործառույթներ:

TNSCS-երը նախատեսված են հեռահաղորդակցական ցանցերում անվտանգության ապահովման համար: Նրանք օգտագործում են ծրագրավորվող կոմուտատորներ տրաֆիկի ղեկավարման նպատակով և կիրառում միջոցներ՝ բարձր մակարդակի անվտանգության քաղաքականության իրականացման համար (օրինակ,

տրաֆիկի ուղղության փոփոխություն):

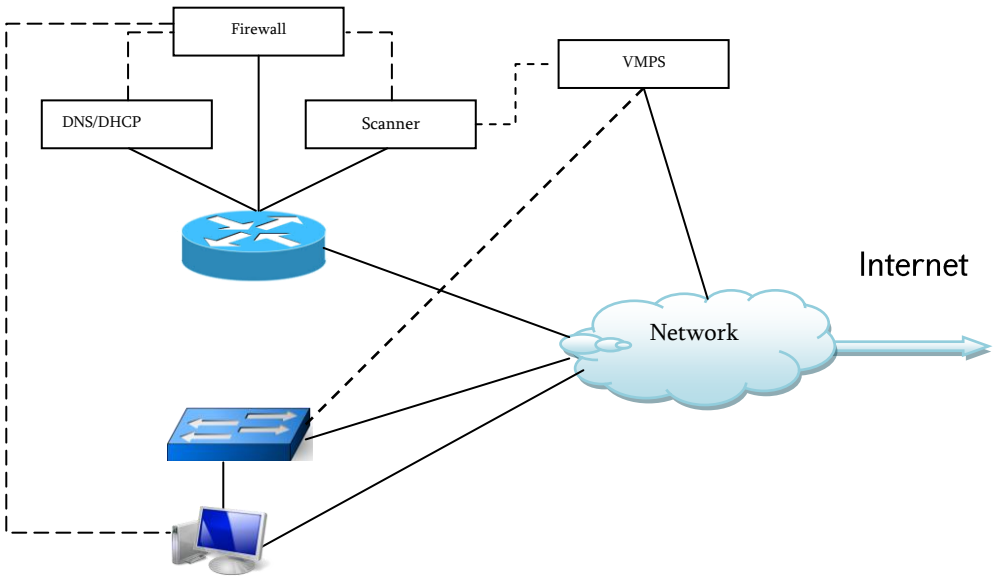
***Կորպորատիվ հեռահաղորդակցական ցանցերի ղեկավարման խնդիրներ***. Սովորաբար հեռահաղորդակցական ցանցերը մեծ են և դժվար ղեկավարելի: Որպես կանոն, դրանք կառուցվում են VLAN տեխնոլոգիաների հիման վրա և ղեկավարվում են VMPS (VLAN Management Policy Server) -ի միջոցով: Այդպիսի ցանցերն ունեն հետևյալ հատկությունները.

*Գրանցում*. Վեբ-ինտերֆեյսն օգնում է օգտատերերին գրանցման գործընթացի ժամանակ: DNS սերվերը վերադարձնում է գրանցման սերվերի IP-հասցեները բոլոր DNS հարցումների համար՝ դոմենների այն ցուցակի համար, որոնք պետք է ուղղվեն (օրինակ, windowsupdate.com): Համակարգում աշխատում է 2 DHCP-սերվեր. մեկը չգրանցված VLAN-ների համար, մյուսը գրանցված VLAN-ների համար: Յուրաքանչյուրն ունի կարգաբերումների իր սեփական ֆայլերը, որոնք ստեղծվում են ավտոմատ կերպով տվյալների բազաներում առկա ինֆորմացիայի հիման վրա:

*Սկանավորում*. Գրանցման ընթացքում համակարգերը ստուգվում են հայտնի խոցելիությունների առկայության բացահայտման համար: Եթե սկանավորումը ի հայտ է բերում խոցելի տեղեր, օգտատերը տեղեկացվում է այդ մասին, և նրան տրվում է համակարգը թարմացնելու հնարավորություն: Միջցանցային էկրանը թույլատրում է տրաֆիկը համապատասխանեցնել թարմացման սերվերներ:

*Միջցանցային էկրան*. VLAN գրամցման ժամանակ օգտագործվում է միջցանցային էկրան՝ չգրանցված հոսթերի ցանցային տրաֆիկի արգելափակման համար: Միջցանցային էկրանը թույլ է տալիս փոխանցել վեբ-տրաֆիկը (այսինքն 80 և 443 բնիկ) այնպես, որ հոսթերը կարող են հասնել սայթերի թարմացմանը: Տարբեր երթուղավորիչներ և կոմուտատորներ [2,66,93] ստեղծում են անհրաժեշտ VLAN ցանցեր: Լոկալ կոմուտատորները որոշում են VLAN-ներ ցանցին միացված յուրաքանչյուր մեքենայի համար: Կոմուտատորը պարբերաբար ներբեռնում է VLAN քարտեր VMPS-ից:

Նշված ձևով կառուցված հեռահաղորդակցական ցանցերի ճարտարապետության օրինակը, որը կառուցված է նման ձևով, ցույց է տրված նկար 8-ում:




Նկ.8. VLAN տեխնոլոգիայով հեռահաղորդակցական ցանցերի ճարտարապետություն

Շատ թերություններ այն բանի արդյունքն են, որ անվտանգության գործառույթները ավելացված են ցանցի առկա ենթակառուցվածքի վերին մասում: Սակայն կոմուտատորներ արտադրողները սկսեցին առաջարկել ստանդարտ ինտերֆեյս - Open-Flow [74,95], որի արդյունքում արտաքին կոնտրոլերը կարող է ազդել ուղղորդված տրաֆիկի կոմուտատորի վրա:

OpenFlow ապահովմամբ կոմուտատորն առաջարկում է ծախսերի աղյուսակի ծրագրավորման համար բաց արձանագրություն և քայլեր է ձեռնարկում, որոնք հիմնված են այդ աղյուսակներում կատարված գրառումների վրա: Ներկայումս OpenFlow կոմուտատորներն աջակցում են երեք գործողության. 1) փաթեթների հոսքի ուղղորդում դեպի որոշակի բնիկ կամ բնիկներ: Այս ֆունկցիան ապահովում է փաթեթն ուղարկումը, 2) փաթեթի հոսքի ինկապսուլացիա և ուղարկում դեպի կոնտրոլեր: Այս դեպքում փաթեթն ուղարկվում է պաշտպանված կապուղուն, որն ինկապսուլյացիայի է ենթարկում փաթեթը և փոխանցում կոնտրոլորին; 3) փաթեթի հոսքի դեն նետում:

Նմանատիպ խնդիրների լուծման համար առաջարկվում է օգտագործել TNSCS: TNSCS տարֆիկի ղեկավարումը կատարվում է քաղաքականությունների միջոցով,

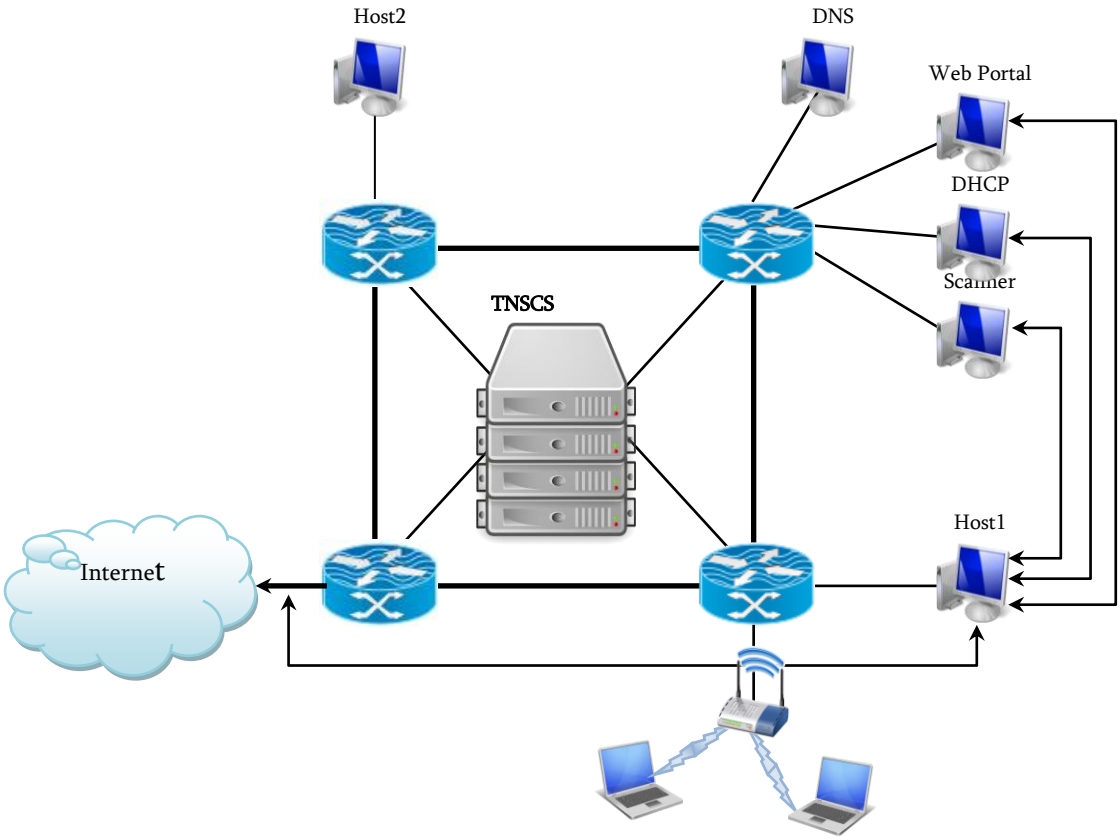
որոնք հաստատվում են ծրագարվորվող կոմուտատորում: Ստեղծվում է մատչման հսկման դինամիկ համակարգ կոնտրոլերի և մոնիտորինգի ենթահամակարգերի ինտեգրացման միջոցով: Այդպիսի ինտեգրացումը թույլ է տալիս օպերատորին որոշել, թե ինչպես ցանցը պետք է ղեկավարի տրաֆիկը և ինչպես է կատարվում ցանցի վիճակի փոփոխությունը: Օրինակ, TNSCS կարող է ավտոմատ կերպով տեղափոխել օգտատերերին կարանտին, եթե ի հայտ են եկել վտանգներ կամ անվտանգության օրենքների այլ խախտումներ:

***TNSCS ինտեգրացումը կորպորատիվ հեռահաղորդակցական ցանցերին***

Նախնական նախագծի պարզեցման համար ենթադրվում է, որ բոլոր հանգույցները գտնվում են միևնույն անվտանգության դասում, և դրանց վիճակը փոխվում է միայն ինքնության ստուգման արդյուքում:

Նկար 9-ում ցույց է տրված TNSCS-ում իրականացված ցանցի աշխատանքը: Սարքը տալիս է DHCP հայտնաբերում հաղորդագրությունը: DHCP սերվերն ուղարկում է հետ արտաքին IP-հասցեն մեքենայի համար: Ինտերնետի հասանելիություն ստանալու համար մեքենան պետք է իդենտիֆիակացնի իրեն վեբ-ծառայության միջոցով: OpenFlow ապահովմամբ կոմուտատորները լռելյայն կարող են ուղղորդել բոլոր HTTP- հարցումները դեպի վեբ-էջի սկիզբ:

Այն բանից հետո, երբ օգտագտերը ինդենտիֆիկացնում է մեքենան, վեբ-ծառայությունը պահում է MAC հասցեն և թարմացնում է այն, որպեսզի ապահովի մատչում դեպի սահմանափակ ուղղություններ (Օրինակ, Microsoft Update): Այդ պահին սկաները անալիզի է ենթարկում սարքավորումը [87]: Եթե մեքենան անցնում է ստուգումը, TCTB վեբ-սերվիսը ուղարկում է հարցում դեպի կոնտրոլեր, որպեսզի թույլատրի տրաֆիկի փոխանցումը այդ մեքենայից, որը կուղարկվի ցանկացած կետ: Ցանցը կատարում է հոսթերի անընդհատ սկանավորում՝ անհարաժեշտության դեպքում օգտագործելով կարանտին մտցնելու տրամաբանական բաշխված մեթոդներ:

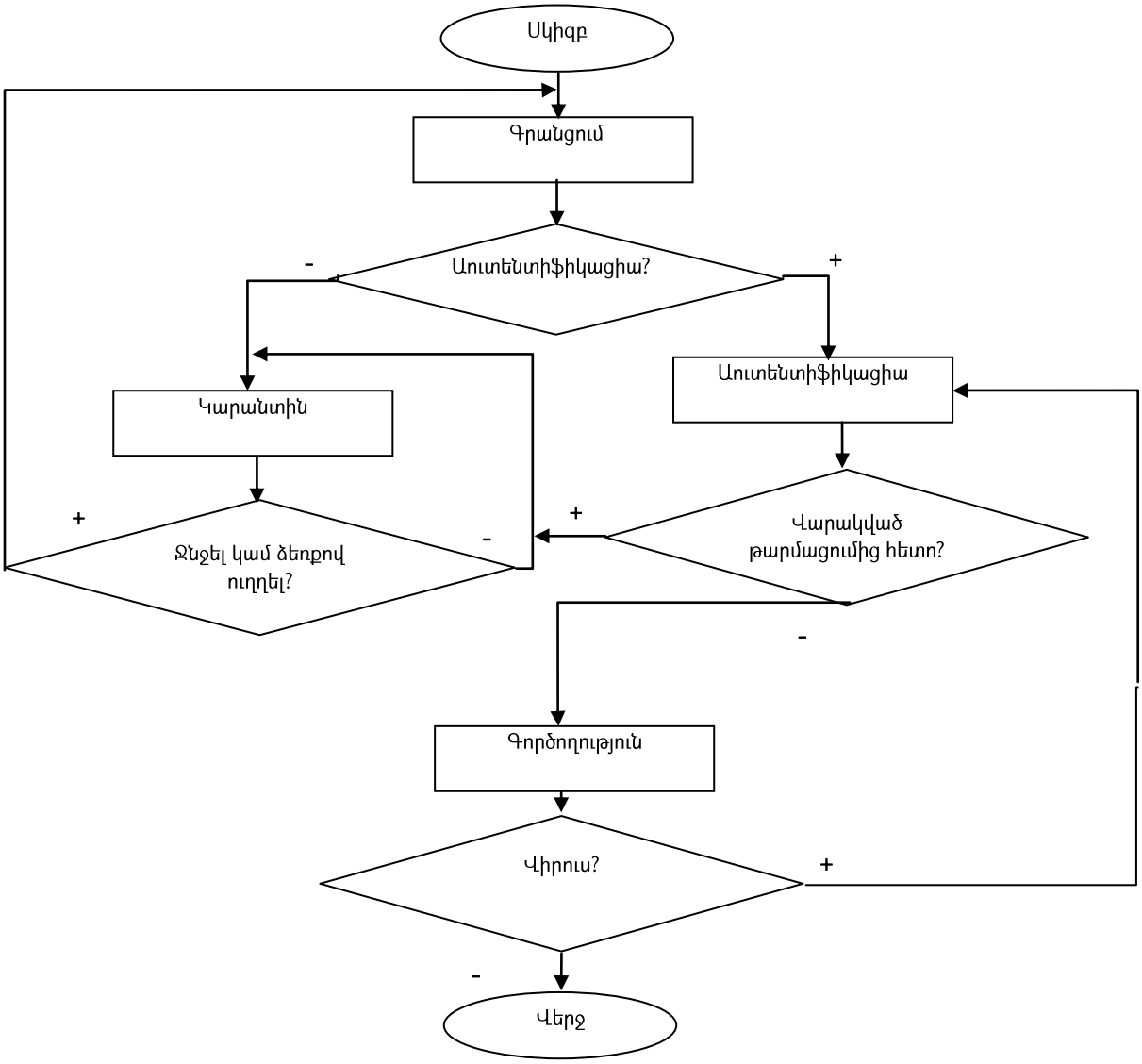



Նկ. 9. TNSCS կիրառումը ՏՏՏԲ-ում

Կոնտրոլերը հետևում է յուրաքանչյուր հանգույցի վիճակին և թարմացնում է արրտաքին աղբյուրների ելքերի ընթացիկ վիճակը: Եթե կլիենտը աուտենտիֆիկացվում է, ուղարկվում է հաղորդագրություն կոնտրոլերին, որպեսզի այն բերի հանգույցը աուտետիկ վիճակի ("հաջողված աուտենդիֆիկացում"): Հետո կոմուտատորը կատարում է հոսթերի սկանավորում (նկար 10): Եթե կլիենտը անցնում է ստուգումը, սկաները տեղեկացնում է կոնտրոլերին, որպեսզի այն տեղափոխի կլիենտին աշխատանքային վիճակ ("մաքուր է սկանավորումից հետո"):

Հակառակ դեպքում կլիենտը տեղափոխվում է "կարանտին" վիճակ: Երկու դեպքում էլ կոնտրոլերը համապատախանաբար թարմացնում է հոսքերի աղյուսակը:

Այսպիսով, ցանցի մատչման ղեկավարումը պետք է լինի ավելի դինամիկ և ներառի ավելի շատ ինֆորմացիա հոսթի վիճակի մասին: Առկա հեռահաղորդակցական ցանցերը պահանջում են ցանցային մոնիտորինգի և մատչման հսկման ավելի բարձր մակարդակ (օրինակ, DHCP, հավելվածների մակարդակում հարձակումների բացահայտում և այլն):




Նկ. 10. Հոսթերի սկանավորման բլոկ-սխեման

Այդպիսի անսարքությունների վերացման համար առաջարկվում է TNSCS կոմպլեքսը անվտանգության քաղաքականության կիրառման համար: TNSCS համակարգը նախատեսված է ցանցի ղեկավարման քաղաքականության դինամիկ որոշման համար և իրականացված է OpenFlow ճարտարապետության մեջ:

## 2.2. Կորպորատիվ հեռահաղորդակցական ցանցերում ապարատածրագրային միջոցների առաջադրումը ծանրաբեռնվածության լավարկման համար

1980-ական թվականների վերջում ինտերնետը բնութագրվում էր տրաֆիկի ցածր ծավալի օգտագործմամբ և ցանցային հավելվածների փոքր թվով: Սպասարկման տեսակի բիթի ToS (Type of Service) կիրառումը կարելի էր անտեսել, ինչը և արվում էր

IP արձանագրության գրեթե բոլոր իրականացումների ժամանակ: IP-ծառայությունները չէին տեղադրում այդ բիթի արժեքը, իսկ երթուղավորիչները անտեսում էին այն IP-փաթեթի երթուղու ընտրման ժամանակ:

QoS (Quality of Service)-ի մեխանիզմների ներդրման կարևորությունը մեծացավ շնորհիվ Ցանցի արդիականության կտրուկ աճի և ըստ նրա կոմերցիոն բնույթի: Ինտերնետը, գործառական տեսակետից ինֆորմացիայի չերաշխավորված փոխանցում է, ինչի համար օգտագործվում է երկու արձանագրություն՝ փոխանցման ղեկավարման արձանագրություն՝ TCP (Transmission Control Protocol) և ինտերնետ արձանագրություն՝ IP (Internet Protocol), որոնք հայտնի են որպես TCP/IP ստեկ: Անկախ նրանից, թե որ կապի հաստատման բացակայությունն է դարձնում Ինտերնետը ավելի ճկուն և կայուն խափանումների նկատմամբ, փոխանցվող տվյալների հոսքի դինամիկան դարձնում են այն ծանրաբեռնելի, ինչը հաճախ ի հայտ է գալիս իրարից զգալիորեն տարբերվող թողունակությամբ երկու ցանցերի հատման մասում:

Հետևաբար, IP արձանագրությունների հիման վրա ստեղծված փաթեթների կոմուտացիայով ցանցերը չեն ապահովում ֆիքսված թողունակություն, քանի որ չեն երաշխավորում փաթեթի առաքումը:

Այն ծառայություններում, որտեղ կարևոր չէ փաթեթների ընդունման հերթականությունը և ընդունման միջակայքը, առանձին փաթեթների միջև հապաղման ժամանակը չունի որոշիչ նշանակություն: Օրինակ, IP հեռախոսակապի համար կարևոր է փաթեթների ստացման հերթականությունը և ազդանշանի փոխանցման դինամիկան, որն ապահովվում է ժամանակակից կոդավորման և ինֆորմացիայի փոխանցման մեթոդներով: TCP/IP ստեկի տրանսպորտային արձանագրությունները, որոնք իրականացվում են IP արձանագրության վրայով, չեն ապահովում տրաֆիկի սպասարկման բարձր որակ: TCP արձանագրությունը, թեև ապահովում է ինֆորմացիայի ճշգրիտ փոխանցում, սակայն փոխանցում է այն անկանխատեսելի հապաղումներով: UDP արձանագրությունը, որը որպես կանոն օգտագործվում է իրական ժամանակում ինֆորմացիայի փոխանցման համար, ապահովում է TCP

արձանագրության համեմատ ավելի փոքր հապաղման ժամանակ, սակայն, ինչպես և IP արձանագրությունը չունի սպասարկման որակի ապահովման ոչ մի մեխանիզմ:

Սպասարկման որակը հիմականում օգտագործվում է՝ որոշելու համար սերվիսի ծառայությունների հավաքածուն: IP ցանցերում QoS-ը կարող է ներկայացվել, օրինակ, որպես IP փաթեթների փոխանցման արդյունավետություն մեկ կամ ավելի ցանցերով անցնելիս:

Բացի արտադրողականության մեծացման և ցանցերի անվտանգության խնդիրներից, ցանցային սերվիսներ տրամադրողները ձգտում են տրամադրել օգտագործողներին երաշխավորված որակ տարբեր տեսակի տվյալների փոխանցման համար (վիդեո, ձայն):

Անհրաժեշտ սպասարկումը բնութագրվում է տարբեր ցուցանիշներով, որոնք բնութագրում են հենց սպասարկման որակը.

– Տրամադրվող սերվիսի պատրաստվածությունը (service availability) որոշում է կապի ապահովությունը օգտագործողի և սերվիս-պրովայդերի միջև:

– հապաղումը (delay) բնութագրում է փաթեթների ընդունման և փոխանցման միջև եղած միջակայքը:

– հապաղման վարիացիա կամ ֆլուկտուացիան (jitter) ցուցանիշ է, որը նկարագրում է փաթեթների փոխանցման ժամանակ հապաղման ժամանակից հնարավոր շեղումները:

– արտադրողականություն կամ թողունակություն (throughput) - ցանցում փաթեթների փոխանցման արագություն; տարբերում են միջին (avarage rate) և գագաթնակետային (peak rate) արագություն:

– թողունակության գիծը (bandwidth) նկարագրում է ինֆորմացիայի փոխանցման միջավայրի անվանական թողունակությունը, որոշում է կապուղու լայնությունը և չափվում բիթ/վ, կբիթ/վ, Մբիթ/վ-ներով:

– փաթեթների կորստի արագություն (packet loss rate) - առավելագույն արագությունն է, որի ընթացքում փաթեթները կարող են մերժվել ցանցով փոխանցվելիս: Փաթեթի կորուստ տեղի է ունենում հիմնականում ցանցի գերբեռնվածության ժամանակ (congestion)

Այժմ մեծացել է IP հեռախոսակապի ծառայության պահանջը: Այդ պահանջների բավարարման համար կապի օպերատորները կատարում են արդեն եղած ցանցերի լավարկում և նոր ցանցերի ստեղծում՝ ապահովելով աստիճանաբար անցում դեպի բազմասերվիսային ցանցեր: Բազմասերվիսային ցանցը (ԲՑ) կապի ցանց է, կառուցված NGN (Next Generation Network) հայեցակարգային համապատասխան և ապահովում է անսահմանափակ ծառայությունների տրամադրում:

Բազմասերվիսային ցանցերին բնորոշ են ինֆորմացիայի փաթեթային փոխանցման տեխնոլոգիաները: Որպես օրինակ կարող է լինել այնպիսի ծառայությունների տարածումը, ինչպիսին է IP հեռախոսակապը, վիդեոկոնֆերենցները, ըստ հարցման վիդեո և աուդիո ծառայությունները (VAoD - Video and Audio Demand) և այլն:

Հետևաբար, ապագա բազմասերվիսային ցանցերի կարևոր մասը պետք է կազմի սպասարկման որակի ապահովման մեխանիզմը: Խնդիրն այն է, որ ամբողջ ցանցի երկայնքով, անկախ նրա մասշտաբից և փոխանցվող արձանագրություններից, պետք է ապահովել տվյալների երաշխավորված փոխանցում՝ կիրառելով համապատասխան չափանիշներ: Այդպիսի չափանիշներ են տրամադրվող սերվիսի պատրաստավծությունը, հապաղումը, հապաղման վարիացիան, թողունակությունը և փաթեթների կորստի արագությունը:

Ինչպես ցույց է տալիս ինտերնետի ներկա վիճակը, ամբողջ տրաֆիկի հավասար մշակումը կարող է բերել լուրջ խնդիրների, հատկապես սահմանափակ թողունակության դեպքում: Այսպիսով, կարևոր տվյալների փոխանցումը կարող է ժամանակավորապես արգելափակվել մեծ ծավալով ֆայլի փոխանցման պատճառով: Համակցված ֆունկցիաներով ցանցերի ստեղծման ժամանակ պետք է ապահովել ծառայության անհրաժեշտ մակարդակ սերվիսի յուրաքանչյուր հավելվածի համար: Հակառակ դեպքում օգտագործողները ստիպված կլինեն հրաժարվել բազմասերվիսային ցանցերից:

Ցանցի ֆունկցիաները կարող են փոփոխվել, ի հայտ գալ նորերը: Փոխվում են նաև ծառայությունները՝ իրենց հետ բերելով նոր պահանջներ ցանցի նկատմամբ: Կիրառական աշխատանքային կայանները այժմ տրամադրում են

հաղորդագրությունների, տեսաինֆորմացիայի, հեռախոսակապի մշակման ծառայություններ:

Նշված պարագայում ստեղծվում է արձագանքման ժամանակի, թողունակության և ցանցի այլ պարամետրերի ապահովագրության անհրաժեշտություն:

**Թողունակության գիծ:** Թողունակության գծի եզրույթը (bandwidth) օգտագործվում է ինֆորմացիայի փոխանցման միջավայրի անվանական թողունակությունը նկարագրելու համար: Այս եզրույթը բավական էֆեկտիվ որոշում է "կապուղու լայնությունը", որը անհրաժեշտ է ծառայությանը ցանցում փոխհամագործակցության համար: Որպես կանոն յուրաքանչյուր կապ ունի երաշխավորված թողունակության անհրաժեշտություն և պահանջում է ցանցից նվազագույն թողունակության գծի տրամադրում:

**Հապաղում փաթեթի փոխնացման ժամանակ:** Հապաղումը փաթեթի փոխանցման ժամանակ (packet delay) կամ լատենտությունը (latency) յուրաքանչյուր անցման համար բազկացած է սերիալիզացման հապաղումից, տարածման հապաղումից և կոմուտացիայի հապաղումից:

Հապաղումների տեսակների դասակարգումը.

– Սերիալիզացիայի հապաղումը (serialization delay) այն ժամանակն է, որն անհրաժեշտ է սարքին փաթեթի փոխանցման համար թողունակության նշված գծով: Այս հապաղումը կախված է ինչպես փոխանցվող ինֆորմացիայի թողունակության գծի լայնությունից, այնպես էլ փոխանցվող փաթեթի չափերից: Օրինակ, 64 բայթանոց փաթեթի փոխանցումը 3Մբիթ/վ թողունակությամբ կապուղով կկազմի ընդամենը 171նվ: Սերիալիզացիայի հապաղումը մեծապես կախված է թողունակության գծից. այդ նույն փաթեթի ուղարկումը 19,2կբիթ/վ թողունակությամբ գծով կկազմի արդեն 26մվ: Հաճախ սերիալիզացիայի հապաղումն անվանում են նաև փոխանցման հապաղում (transmission delay):

– տարածման հապաղումը (propagation delay) այն ժամանակն է, որն անհրաժեշտ է փոխանցվող ինֆորմացիայի բիթին, որ այն հասնի կապուղու մյուս ծայրում ընդունող սարքին: Տարածման հապաղումը կախված է տարածությունից և ինֆորմացիայի

փոխանցման միջավայրից, և ոչ թե թողունակության գծից: Գլոբալ ցանցերի համար տարածման հապաղումը չափվում է միլիվայրկյաններով:

– կոմուտացիայի հապաղումները (switching delay) այն ժամանակն է, որն անհրաժեշտ է փաթեթը ընդունած սարքին՝ այն հաջորդ սարք փոխանցել սկսելու համար: Որպես կանոն այդ արժեքը փոքր է 10 նվ-ից:

Սովորաբար յուրաքանչյուր փաթեթ, որը պատկանում է նույն տրաֆիկի հոսքին, փոխանցվում է հապաղման տարբեր արժեքներով: Փաթեթի փոխանցման ժամանակ հապաղումը փոխվում է՝ կախված միջանկյալ ցաների վիճակից:

Այն դեպքում երբ ցանցը չունի գերբեռնում, փաթեթները չեն դրվում հերթի երթուղավորիչներում, իսկ փաթեթի փոխանցման հապաղման ընդհանուր ժամանակը կազմվում է յուրաքանչյուր միջանկյալ անցման սերիալիզացիայի և տարածման հապաղումների գումարից: Այս դեպքում կարելի է խոսել տրված ցանցով փաթեթի փոխանցման նվազագույն հապաղման մասին: Պետք է նշել, որ սերիալիզացիայի հապաղումը դառնում է աննշան տարածման հապաղման նկատմամբ, երբ կապուղու թողունակությունը մեծ է:

Եթե ցանցը գերբեռնված է, երթուղավորիչներիում հերթերի ձևավորման հապաղումները սկսում են ազդել փաթեթների փոխանցման ընդհանուր հապաղման վրա: Ունի մեծ նշանակություն, քանի որ հենց դա է որոշում վերջնակետում փաթեթի ստացման առավելագույն հապաղումը:

**Փաթեթների կորուստ**: Փաթեթների կորստի մակարդակը որոշվում է փաթեթների քանակով, որոնք դուրս են մղվում փոխանցման ժամանկ: Փաթեթների կորստի հիմանական պատճառը ցանցի գերբեռնումն է և կապի գծով փոխանցման ժամանակ փաթեթների վնասումը: Սովորաբար փաթեթի դեն նետումը կատարվում է գերբեռնման կետերում, որտեղ եկող փաթեթների թիվը մի քանի անգամ գերազանցում է հերթի շեմային սահմանը:

Փաթեթների կորստի մակարդակը նկարագրվում է որոշակի ժամանակի ընթացքում դուրս թողնված փաթեթների թվով: Որոշ հավելվածներ ունակ չեն նորմալ աշխատել կամ աշխատում են ոչ արդյունավետ, երբ տեղի է ունենում փաթեթի կորուստ: Այդ հավելվածները պահանջում են ցանցի երաշխավորված փոխանցումների

ապահովում: Լավ նախագծված ցանցը բնութագրվում է փաթեթների կորստի փոքր թվով: Ինչ վերաբերում է օպտիկամանրաթելքային կապի գծերին, որտեղ սխալ բիթերի ի հայտ գալու հաճախությունը ( Bit Eror Rate -BER) $10^{-9}$E է, ապա փաթեթի կորուստներ հնարավոր է միայն դրանց դուրս մղման տեսքով ցանցի գերբեռնված հատվածներում: Փաթեթի դեն նետումը անխուսափելի երևույթ է տրաֆիկի չերաշխավորված փոխանցումների ժամանակ, սակայն այս դեպքում ևս դա բացատրվում է ծայրահեղ անհրաժեշտությամբ:

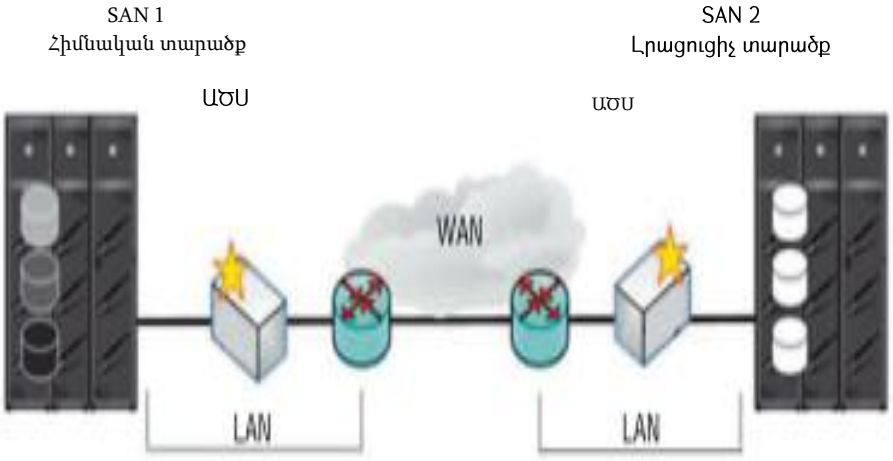
Կորպորատիվ հեռահաղորդակցական ցանցերում՝ ԿՀՑ, կանալների ծանրաբեռնվածության մեծացմամբ փաթեթների կորուստը տեղի է ունենում ավելի հաճախ, որն իր հերթին հանգեցնում է աշխատանքի որակի վատացմանը և ծառայության արձագանքման ժամանակի մեծացմանը [4]: Կանալի (սեփական կամ վարձակալած) թողունակության ավելացումը հաճախ թանկ է նստում, քանի որ ցանցում հապաղումների թիվը մնում է բավականին բարձր: Երբեմն խնդիրը (մասամբ կամ ամբողջապես) հնարավոր է լինում լուծել սպասարկման առաջնայնության (QoS- ***Q****uality* ***o****f* ***S****ervice*) կանոնների կիրառմամբ, ծառայության կարգաբերումների փոփոխմամբ կամ լուծումների վերանայմամբ:

ԿՀՑ-ի աշխատանքի բարելավման նպատակով՝ որպես ամենագործուն և խնայողական լուծում, կիրառվում են ցանցի ապարատածրագրային սարքերը (ԱԾՍ): ԱԾՍ-երը ներդրվում են արագ և հեշտ, ընդ որում՝ միշտ չէ, որ պահանջվում են ցանցի ճարտարապետության փոփոխություններ: ԱԾՍ-ի աշխատանքի սկզբունքն է՝ ծառայությունների միջոցով տվյալների ծավալի կրճատում, կապուղու թողունակության արդյունավետության մեծացում և բաշխում ծառայությունների միջև, ինչի շնորհիվ էլ ցանցային ծառայությունների աշխատանքի արագությունը ԿՑ կապուղով մոտենում է լոկալ ցանցերում դրանց աշխատանքի արագությանը:

ԱԾՍ-երը միացվում են գլոբալ ցանցի երթուղավորիչներին լոկալ ցանցի միջոցով, ինչպես ներկայացրել ենք նկար 11-ում, բացի այդ, ԿՀՑ օպտիմալացումը կարող է լինել ամպային ծառայությունների տեսքով:

Փորձագետների գնահատմամբ ԿՀՑ օպտիմարարները կարող են մեծացնել ծառայությունների աշխատունակությունը 50 անգամ: Ցանցի թողունակությանն

ուղղված պահանջները փոքրանում են 65…95%-ով, տվյալների փոխանցման վրա կատարվող ծախսերը՝ 10%-ով, իսկ ծառայության արձագանքման ժամանակը (կախված տվյալների տեսակից)՝ 60…90%-ով:




Նկ. 11. ԱԾՍ սարքավորումների միացման եղանակը

ԱԾՍ-ների հաջող ներդրումը հնարավորություն է տալիս փոքրացնել լոկալ ծառայությունների և սերվիսների թիվը, ավելի ակտիվ օգտագործել ամպային տեխնոլոգիաները [108]: Բացի այդ, ԱԾՍ-ները արագացնում են պահուստային պատճենահանման/վերականգնման, ՏԲ-ների ռեպլիկացիայի և սինխրոնացման գործընթացը: Որոշ կազմակերպություններում, որտեղ պահուստային պատճենահանման գործընթացը տևում է 1 օրից ավելի, այժմ իրականացվում է 2…3 ժամում: Շնորհիվ արագացված (մինչև 45 անգամ) ռեպլիկացիայի, կարելի է հաճախ կատարել տվյալների պատճենում և բավականին կրճատել վերականգնման ժամանակը:

Սովորաբար ԱԾՍ-երն օգտագործում են LZ հոսքային սեղմման ալգորիթմները, որոնց արդյունավետությունը կախված է տրաֆիկի տեսակից: HTML էջի տվյալները սեղմվում են բավականին լավ, մինչդեռ կոդավորված տվյալների դեպքում դա գրեթե անհնար է: Ապադուբլիկացիան թույլ է տալիս կրճատել ցանցով փոխանցվող ինֆորմացիայի ծավալը 65…95%-ով:

Ֆայլերի և այլ ռեսուրսների օգտագործման դեպքում տվյալների քեշավորումը միավորվում է ապարատային սեղմման մեթոդների հետ: Քեշավորման ժամանակ, երբ

մասնաճյուղի աշխատողը բեռնում է ֆայլը կենտրոնական սերվերից, ԱԾՍ-ն պահպանում է լոկալ պատճենը և փոփոխում դա՝ սինխրոնացնելով դրա հետ սերվերում գտնվող ֆայլը: Սարքերը կարող են քեշավորել արդեն փոփոխված ֆայլերը և հետագայում փոխանցել միայն հղումներն այդ ֆայլերին:

Տարբեր եղանակների համակցումը, տարատեսակ տրաֆիկի դեպքում, ապահովում է փոխանցվող տվյալների ծավալի նվազեցումը 100 և ավելի անգամ, իսկ աշխատանքային կայաններում կատարվում է ընդհանուր տրաֆիկի կրճատում 5...6 անգամ: ԿՀՑ օպտիմալացման սարքավորումների ներդրումը թույլ է տալիս բարձրացնել ցանցի թողունակության օգտագործման արդյունավետությունը, ինչը ակնհայտորեն հանգեցնում է բիզնես-գործընթացների: ԱԾՍ-ն սովորաբար տեղադրվում է կապի սկզբնական և վերջնական կետերում [4]:

Այժմ արտադրողներն առաջարկում են կորպորատիվ հեռահաղորդակցական ցանցի օպտիմալացման կոմպլեքս մեթոդներ [36]: Նրանք ձգտում են հաշվի առնել առավելագույն թվով պահանջներ և իրագործել որքան հնարավոր է շատ եղանակներ՝ մասնաճյուղերում աշխատակիցների արդյունավետ աշխատանքի, բիզնես-գործընթացների արագացման և միացյալ աշխատանքի լավարկման համար: Բացի այդ, օպտիմալացման միջոցները ներառված են երթուղավորիչների ֆունկցիաներում, բայց, որպես կանոն, դրանք ԱԾՍ-երի, այսպես կոչված, «թեթևացված» տարբերակներն են՝ առանց լավարկված ապադուբլիկացիայի և վերին մակարդակի արձանագրությունների արագացմամբ [55,62,68,105,]: Այս ճանապարհն են ընտրել, մասնավորապես, Cisco և Juniper ընկերությունները:

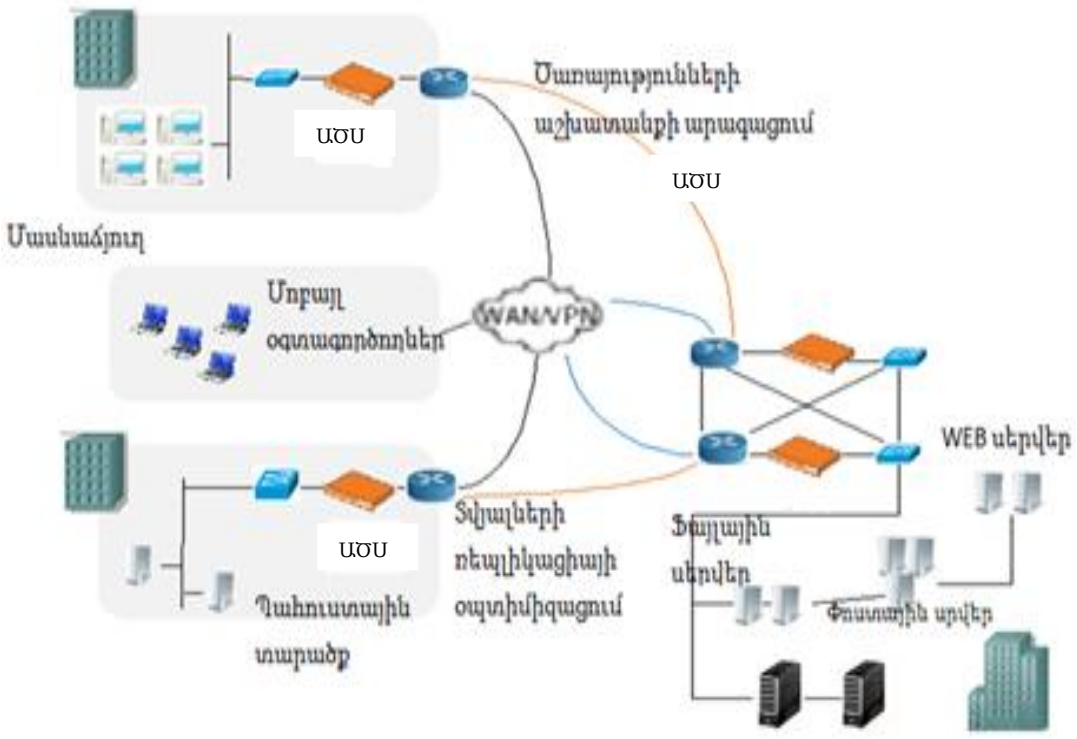
Cisco ընկերությունն առաջարկում է ԱԾՍ սարքավորումներ [69,73,80,88], որոնցից ներկայացված է նկար 12-ում և ISR երթուղավորիչների համար օպտիմալացման ծրագրային ապահովում [4]:


Նկ. 12. Cisco ընկերության սարքավորումները

HTTP և HTTPS տրաֆիկի օպտիմալացման համար մասնագետները խորհուրդ են տալիս Riverbed SteelHead, իսկ որպես այլընտրանք, կարելի է դիտարկել Silver Peak VX: Սովորաբար արտադրողականությունը մեծանում է 140...166%-ով:

Ինչ վերաբերում է VoIP տրաֆիկին [56,83,100], ապա այն արդեն օպտիմալացված է կոդեկով, սակայն ԱԾՍ-երի կիրառումը տալիս է որոշակի արդյունավետություն: Օրինակ, համաձայն թեստավորման տվյալների, Silver Peak VX սարքավորումների կիրառման ժամանակ այն կազմում է 9%, Riverbed SteelHead դեպքում՝ 7%, իսկ միջին ցուցանիշների դեպքում՝ 3%: Սակայն դրա հետ մեկտեղ ԿՀՑ օպտիմարարների տեղադրումը կարող է հանգեցնել հապաղման տատանումների, ինչն էլ առաջացնում է կապի որակի վատացում: Այսպես, Silver Peak VX և Riverbed SteelHead կիրառման դեպքում թեստային կոնֆիգուրացիաներում տատանումները մեծանում են գրեթե 10%-ով, այն դեպքում, երբ Citrix CloudBridge-ը կրճատում էր դրանք 16%-ով [58,67,82[:

Օպտիմարարների ներդրման պրակտիկ փորձը ցույց է տալիս, որ ապահովվում է բարձր արդյունավետություն: Նման սարքավորումների կիրառումը նպատակահարմար է ԿՀՑ կանալներով տվյալների փոխանցման ցանցերում՝ տեղակայված հեռահար մասնաճյուղերի, օֆիսների և ՏԲ-ների միջև (նկ.13):




Նկ. 13. ԱԾՍ սարքավորումների աշխատանքի կազմակերպումը

Այս դեպքում փոխանցվող տրաֆիկի ծավալը փոքրանում է 3...5 անգամ, իսկ տվյալների փոխանցման պիկային արագությունը մեծանում՝ 100 և ավելի անգամ:

ԱԾՍ-երի օգտագործման դեպքում փոխանցվող տրաֆիկի ծավալը փոքրանում է 3...5 անգամ, իսկ տվյալների փոխանցման պիկային արագությունը մեծանում՝ մոտ 100 անգամ [4]:

Նոր տեխնոլոգիաներն ուղղված են ամպային սերվիսների օպտիմալացման, հեռավար և մոբայլ օգտագործողների՝ աշխատանքի ավելի հարմար պայմանների ստեղծման համար: Դրանք համապատասխանում են մասշտաբայնության և հուսալիության աճող պահանջներին և կարող են կիրառվել իբրև վիրտուալ սարքավորումներ վիրտուալացված ՏԲ-ներում: Ծառայությունների՝ ամպային տեխնոլոգիաների տեղափոխմամբ ԿՀՑ-երի օպտիմարարների պահանջարկն ավելանում է [76,108], քանի որ ցանցի արտադրողականությունը դառնում է առավել մեծ արդյունավետության անհրաժեշտ գործոն, իսկ օպտիմիարարների վիրտուալ տարբերակը՝ արտադրողականության և հուսալիության շահավետ լուծում:

## 2.3. Կորպորատիվ հեռահաղորդակցական ցանցերի մշտադիտարկման մաթեմատիկական մոդելը և ալգորիթմը

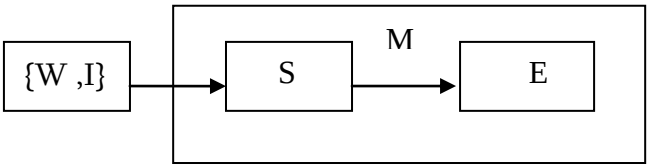
Մոնիտորինգ ասելով հասկանում ենք օբյեկտի բնութագրերի գործունեությանը կանոնավոր ռեժիմից շեղման իդենտիֆիկացիան, կամ բնութագրերի փոփոխության միտումների ի հայտ բերելը՝ հիմնվելով օբյեկտի մասին ինֆորմացիայի ստատիկ հավաքագրման և անալիզի վրա [37]: Մոնիտորինգի խնդիրը բնորոշ է գործունեության այն տեսակներին, որտեղ դիտարկվող օբյեկտը ներկայանում է իբրև բազմակոմպոնենտ համակարգ, որի վիճակի մասին կարելի է դատել համակարգի հատկությունների ամբողջական կամ նրա որոշ մասերի փոփոխմամբ: Որպես գործունեության տեսակի օրինակ, որոնց անբաժան մասն է կազմում մոնիտորինգի խնդիրը, կարելի է բերել էպիդեմիոլոգիական հսկումը, լայնամասշտաբ տեխնիկական օբյեկտների և արտադրության ղեկավարումը, հանրային անվտանգությունը:

Տվյալների հավաքագրումը մոնիտորինգի անբաժան մասն է, դրա համար տվյալների հավաքագրման խնդիրներին նվիրված շատ աշխատանքներ կան, որոնք

դիտարկում են տվյալ խնդրի լուծման ինչպես տեխնոլոգիական, այնպես էլ տեսական հիմքերը: Պարզ դեպքերում, որոնց համար բավական է լուծել միայն տվյալների հավաքագրման խնդիրը, տվիչի ազդանաշանը միաժամանակ նաև համակարգի կանոնավոր ռեժիմից շեղման ազդանաշանն է: Հրդեհի ազդանաշանը բացահայտ օրինակ է, երբ մեկ տվիչի միացումը նաև կանոնավոր ռեժիմից շեղման զգուշացում է: Տվյալների հավաքագրման համակարգերի հնարավորությունները բավարար չեն այն համակարգերի մոնիտորինգի համար, որոնց կանոնավոր ռեժիմը բնութագրվում է տվիչների «ֆոնային» ազդանաշանների առկայությամբ: Ֆոնի առկայությունը բնորոշ է էկոնոմիկայի, բժշկության, տեխնիկական բարդ համակարգերի մեծամասնության համար: Լավ օրինակ է հիվանդությունների մոնիտորինգը, որտեղ կանոնավոր ռեժիմից դուրս գալու ազդանշանը հիվանդության շեմի գերազանցումն է:

**Բազմակոմպոնենտ համակարգի մաթեմատիկական մոդելը**

Ընդհանուր առմամբ հետազոտվող համակարգը կազմված է բազմաթիվ օբյեկտներից, որոնք փոխհամագործակցում են միմյանց հետ, և շատ տվիչներից, որոնք չափում են օբյեկտի բնութագրերը և փոխանցում դրանք տվյալների մշակման կենտրոն (նկ.14):




Նկ. 14. Հետազոտվող համակարգի ընդհանուր սխեմա

Սխեմայի վրա կատարվել են հետևյալ նշանակումները.

$\{W, I\}$ – բազմակոմպոնենտ համակարգ,

$M = \{S, E\}$ - մոնիտորինգի համակարգ:

Բազմակոմպոնենտ համակարգը՝ $\{W, I\}$ -ն ներկայացված է $W = \{w_{1,\dots} w_{|W|}\}$ մոնիտորինգի օբյեկտների բազմությամբ և $I$ օբյեկտների վիճակների փոփոխման մոդելով:

Մոնիտորինգի համակարգը $M = \{S, E\}$ կազմված է $S = \{s_1, \dots, s_{|s|}\}$ համակարգի բազմաթիվ տվիչներից և տվյալների մշակման E կենտրոնից: Ինդեքսում ուղիղ փակագծերը նշանակում են համապատասխան բազմությունների

չափողականությունը: $w \in W$ օբյեկտները նկարագրվում են բնութագրիչ վեկտրով՝ $D = (d_1,\ldots,d_{|D|})$, նրա $|D|$ չափողականությունը կախված է լուծվող խնդրից, $D$ վեկտորի $\in$ , $= 1\ldots$ տարրերը նկարագրում են օբյեկտի ներքին վիճակը:

Բարդ համակարգերի մոդելավորման [13] ժամանակակից մոտեցումների բնութագրիչ գիծը գիտավարկածի ձևակերպումն է, որը նկարագրում է գործընթացի դինամիկան միկրոմակարդակում [6]. $I$ մոդելը նկարագրում է ժամանակի ընթացքում առանձին $w \in W$ օբյեկտների վիճակի փոփոխության դինամիկան $(D)$, և կարող է ներկայանալ հետևյալ ձևով. $W$ օբյեկտի վիճակը նկարագրվում է $D$ վեկտրով, և փոփոխվում է որոշակի դիսկրետ պահերին համաձայն հետևյալ արտահայտության.

$$d_{1,new} = a_{i1}d_1 + a_{i2}d_2 + \cdots + a_{i|D|}d_D + f_i \qquad (5)$$

որտեղ $a_i$ –ն համապատասխան չափողականությունների վեկտորի գործակիցն է, իսկ $f_i$ –ը $W$ օբյեկտի արտաքին ազդեցության $f$ վեկտորի տարրը: Նշանակենք $\ldots < T_0 < T_1 < \ldots < T_n < \ldots W$ օբյեկտի վիճակի փոփոխության պահերը: Այդ դեպքում $W$ օբյեկտի վիճակի փոփոխությունը $d_i(t)$ կարող է նկարագրվել հավասարմամբ, որտեղ ենթադրվում է $d_i(t)$ ֆունկցիայի անընդհատությունը յուրաքանչյուր $T_n < t \leq T_{n+1}$ միջակայքում: Հավասարումը նկարագրում է օբյեկտի վիճակի փոփոխությունը, որը պայմանված է իր գործունեության ներքին կանոններով և արտաքին $f$ ազդեցությամբ: $w \in W$ օբյեկտների միջև փոխազդեցության առկայության դեպքում $w_i$ օբյեկտի $D_i$ վիճակի հավասարումը կունենա հետևյալ տեսքը.

$$D_i(T_{n+1}) = a_{ij}D_i(T_n) + \sum_{j=1,i\neq j}^{|W|} a_{ij}\ D_j(T_n) + f_i(T_n) \qquad (6)$$

որտեղ $a_{ij}D_i(T_n)$ -ը բնութագրում է օբյեկտի վիճակի փոփոխության ներքին օրենքները, $\sum_{j=1,i\neq j}^{|W|} a_{ij}\ D_j(T_n)$-ն օբյեկտների փոխազդեցությունը, իսկ $f_i(T_n)$ -ն՝ նկարագրում է արտաքին միջավայրի ազդեցությունը $\omega_i$ օբյեկտի վրա: Որոշ դեպքերում կարող է կիրառվել համապատասխան բանաձևերի գրառումը դիսկրետ տեսքով [7]: Ամփոփելով կարելի է ասել, որ $I$ օբյեկտի վիճակի փոփոխության մոդելը կազմված է հետևյալ էլեմենտներից.

$$I = \{A, F\}, \qquad (7)$$

որտեղ $A$ –ն մատրից է, որը կազմված է հիմնականում $a_{ij}$ վեկտորից, $F$ –ը $\omega$ համակարգի օբյեկտների վրա արտաքին ազդեցությունների մատրիցն է: Ընդհանուր առմամբ, տարբեր $T$ օբյեկտների վիճակների փոփոխման պահերը չեն համընկնում, այսինքն՝ համակարգը ասինխրոն է: Հավասարումները գրված մատրիցային տեսքով կարող են հետազոտվել ասինխրոն համակարգերի մեթոդներով: Հետազոտությունների համար կարող են կիրառվել հավանականային և այլ մեթոդներ: Համակարգերի և պրոցեսների մոնիտորինգի տեսակետից հետաքրքիր են համակարգի ընդհանրացված բնութագրերը:

Ընդհանրացված ցուցանիշները, օրինակ, հիվադությունների, հանցագործությունների և այլի մակարդակը, հաճախ արտացոլում են $W$ օբյեկտի բազմության ենթաբազմությունների քանակի կախվածությունը ժամանակից: Ենթաբազմությունները ներկայացվում են օբյեկտի վիճակի $D$ վեկտորի և ենթաբազմության կենտրոնական վեկտորի հարևանության սկզբունքով:

$$\omega \in C \Longleftrightarrow \rho_C (D, D_C) < \varepsilon_C, \tag{8}$$

որտեղ $\omega$ –ն օբյեկտ է $W$ օբյեկտների բազմությունից, $C \subset W$ –ն $W$ օբյեկտի բազմության ենթաբազմություն է, $\rho_C$ –ն օբյեկտների վիճակների միջև հեռավորությունն է, $D$ –ն $\omega$ օբյեկտի վիճակի վեկտորն է, $D_C$ –ն $C$ ենթաբազմության կենտրոնական վեկտորն է, $\varepsilon_C$ –ն՝ $C$ ենթաբազմության շառավիղը: Այսպիսով, $C$ ենթաբազմությունը տրվում է հետևյալ հավաքածուի միջոցով.

$$C = \{\rho_C, D_C, \varepsilon_C\} \tag{9}$$

Յուրաքանչյուր $\omega$ օբյեկտին կարող է համապատասխանել մեկ կամ ավելի ենթաբազմություն, այս դեպքում կասենք, որ օբյեկտը պատկանում է մեկ կամ շատ դասերի:

$$C(\omega) = C(D) = \{C_{\omega 1}, \ldots\}, \tag{10}$$

որտեղ $D$ –ն $\omega$ օբյեկտի վիճակի վեկտորն է, քանի որ $D = D(t)$, ուստի օբյեկտի դասերի հավաքածուն նույնպես փոխվում է ժամանակի ընթացքում, այսինքն՝ $C(\omega) = C(t)$: Այս դեպքում $C$ դասի $|C|$ մեծությունը որոշվում է որպես $w$ օբյեկտների քանակ, որոնք պատկանում են $C$ դասին: $|C| = \sum_{\omega \in W} \omega \in C$, որտեղ $\omega \in C$

արտահայտությունը ընդունում է 1 արժեք, եթե $w$ օբյեկտը պատկանում է $C$ դասին և 0 արժեք՝ հակառակ դեպքում: Օբյեկտների և դասերի տերմինաբանության մեջ ընդհանրացված ցուցանիշները, որոնք բնութագրում են պրոցեսների դինամիկան մակրոմակարդակում, ընդունում են հետևյալ տեսքը.

$$F(t) = F(|C_1(t)|, |C_2(t)| \dots \dots |C_n(t)|, t), \quad (11)$$

որտեղ $F(t)$ –ն համակարգի վիճակի ընդհանրացված ցուցանիշն է, $C_1, \dots, C_n$ – ն օբյեկտի դասերը, $t$–ն՝ ժամանակը: Տվյալ արտահայտության մեջ $F$-ի ֆունկցիոնալ կախվածությունը $|C|$ դասերի մեծությունից նշանակվում է ինչպես կախվածություն $|C(t)|$ ֆունկցիայից, այնպես էլ նրա ածանցյալ, ինտեգրալ և այլ հնարավոր բնութագրերից:

### *Բազմակոմպոնենտ համակարգերի մոնիտորինգ*

Նշված համակարգերի մոնիտորինգի համար անհրաժեշտ են ինֆորմացիայի մշակման ավելի հստակ մեթոդներ, որոնք աշխատում են ֆոնի առկայության պայմաններում: Արհեստական բանականության շրջանակներում հետազոտվող տվյալների ինտելեկտուալ անալիզի մեթոդների կիրառումը գործնականում հաճախ սահմանափակ է՝ կապված ինտելեկտուալ կառուցվածքների իրականացման և ուսուցման հետ [42]: Պարզագույն մեթոդների և տվյալների ինտելեկտուալ անալիզի միջև տարբերությունը հանգեցնում է մեծ քանակությամբ նեղ մասնագիտական կիրառական համակարգերի ի հայտ գալուն, որոնց թիվը միևնույն առարկայական ուղղվածության մեջ բավական մեծ է: Մասնավորապես, ըստ գնահատականների, որոնք բերված էն Դ. Բրավատի աշխատությունում, միայն էպիդեմիոլոգիական ուղղվածության մեջ հաշվարկվում է 115-ից ոչ պակաս մոնիտորինգի համակարգ, որոնց մասին հրատարակված է ավելի քան տասնյոթ հազար գիտական աշխատանք:

**Բազմակոմպոնենտ համակարգերի մոնիտորինգի մաթեմատիկական մոդելը**

Ձևակերպենք $W_B$ համակարգի վիճակի մոնիտորինգի խնդիրները մաթեմատիկական մոդելի տերմիններում: Կդիտարկենք երկու խնդիր. համակարգի

բնութագրերի կանոնավոր ռեժիմից շեղման խնդիրը և շեղման բնույթի հիփոթեզի ստուգման խնդիրը:

Համակարգի բնութագրերի կանոնավոր ռեժիմից շեղման խնդիրը կայանում է այնպիսի $C_1,\dots,C_n$ դասերի հավաքածուների, նրա որոշման $F(t)$ ֆունկցիաների մեթոդների և $F_0(t)$ կանոնավոր ռեժիմից $\varepsilon_F$ շեղման շեմի ընտրությունն է, որոնց դեպքում $|F(t) - F_0(t)| > \varepsilon_F$ շեղումը կհամապատասխանի $I$ օբյեկտների վիճակների փոփոխության մոդելի էական կոռեկցիայի մոդելին: Էական շեղման գաղափարը կախված է մոդելի կիրառման հստակ բնագավառից և կարող է ձևակերպվել, օրինակ, $W$ ասինխրոն համակարգի հուսալիության դեպքում:

Կանոնավոր ռեժիմից համակարգի բնութագրերի շեղման բնույթի ստուգման խնդիրը լուծում է համակարգի բնութագրերի շեղման ինդենտիֆիկացիայի խնդիրը: Բացի շեղման իդենտիֆիկացիայից $|F(t) - F_0(t)| > \varepsilon_H$ անհրաժեշտ է ընտրել գիտափորձի $H = \{H_1,\dots,H_N\}$ հիփոթեզների բազմությունից առավել հավանական $H_{prob}(t)$, այնպես, որ

$$|F(t) - H_{prof}(t)| = \min_{H_i \in H}(|F(t) - H_i(t)|) \qquad (12)$$

Շահումը պրոցեսի զարգացման հիփոթեզի ստուգումից $\varepsilon_H < \varepsilon_F$ արժեքի ընտրումն է: Պրակտիկայում որպես նորմ, որը կիրառվում է համակարգի բնութագրերի շեղման որոնման համար, նպատակահարմար է օգտագործել $|\int \Delta t\,(F(t) - F_0(t))|$ ինտեգրալ բնութագիր $\Delta t$ ժամանակի միջակայքում $F(t)$ աճի ճնշման(զսպման) համար:

## 2.4. Հեռահաղորդակցական ցանցերում մերժման և սպասման համակարգերում մաթեմատիկական մոդելները և ծանրաբեռնվածության հաշվարկը

Տրաֆիկի մաթեմատիկական մոդելում.

- հայցի հոսքը բնութագրվում է Պուասոնի բաշխման օրենքով,
- հայցի տևողությունը բնութագրվում է էքսպոնենցիալ բաշխման օրենքով:

Տարբեր մոդելներ իրարից տարբերվում են նրանով, թե ինչ «ճակատագիր» է բաժին ընկնում հայցին այն դեպքում, երբ համակարգի բոլոր կապուղիները զբաղված են լինում: Այդ զանգերը կարող են չիրականացվել կամ մնալ հերթում և սպասել

այնքան ժամանակ, մինչև որևէ կապուղի կազատվի, որից հետո անհրաժեշտ ժամանակի ընթացքում կսպասարկվի [7, 58]: Հնարավոր են նաև միջանկյալ դեպքեր, օրինակ, սահմանափակ ժամանակի տևողությամբ սպասման համակարգի մոդելը:

**Մերժման համակարգով մոդելը կոչվում է Էռլանգի B մոդել** [109, 110]: Այս մոդելում արգելման հավանականությունը հայցի արգելափակումը, երբ բոլոր ուղիները զբաղված են, որոշվում է հետևյալ արտահայտությամբ՝

$$P_B = \frac{A^N / N!}{\sum_{n=0}^{N} \left( A^n / n! \right)}, \tag{13}$$

որտեղ՝ $N$-ը կապուղիների թիվն է, $A$-ն՝ $A = \langle \lambda \rangle \cdot \langle T \rangle$ տրաֆիկն է:

Այս մոդելում հավանականությունը, որ բոլոր կապուղիները ազատ են, որոշվում է հետևյալ կերպ՝

$$P_{0B} = \frac{1}{\left[ \sum_{n=0}^{N} \left( \frac{A^n}{n!} \right) \right]}, \tag{14}$$

$k$ թվով կապուղիների զբաղված լինելու հավանականությունը որոշվում է՝

$$P_{kB} = P_{0B} \left[ A^k / (k!) \right], \tag{15}$$

Զբաղված կապուղիների միջին թիվը՝

$$\langle k \rangle = P_{0B} \sum_{n=1}^{N} \left[ A^n / (n-1)! \right] : \tag{16}$$

**Սպասման համակարգով մոդելը կոչվում է Էռլանգի C մոդել** [110]**:** Այս մոդելում հապաղման ժամանակը (այսինքն հավանականությունն այն բանի, որ մուտք եկած հայցը անմիջապես չի սպասարկվի, այլ «հերթում» կսպասի) որոշվում է հետևյալ արտահայտությամբ՝

$$P_C = P_{0C} \cdot \left[ A^N \cdot N / (N - A) \cdot N! \right], \tag{17}$$

որտեղ $P_{0C}$-ն այն հավանականությունն է, որ բոլոր կապուղիները ազատ են՝

$$P_{0C} = \frac{1}{\left\{\left[\sum_{n=0}^{N-1}\left(A^n/n!\right)\right] + \left[A^N \cdot N/(N-A)N!\right]\right\}} : \qquad (18)$$

**Սահմանափակ ժամանակի տևողությամբ սպասումով համակարգի մոդելը կոչվում է Էռլանգի A կամ Պուասոնի մոդել** [109]**:**

Այս դեպքում, երբ համակարգում բոլոր կապուղիները զբաղված են լինում, մուտքին եկած հայցը «հերթում»սպասում է, բայց սպասման ժամանակը չի գերազանցում սպասարկման միջին տևողությանը: Եթե այդ ժամանակահատվածում անգամ մեկ կապուղի ազատվում է, ապա միջին սպասարկման ժամանակի ազատված մասում հայցն այն զբաղեցնում է: Այս համակարգում հայցի մերժման հավանականությունը որոշվում է՝

$$P_A = \sum_{n-N}^{\infty}\left[A \cdot e^{-A} \big/ n!\right] : \qquad (19)$$

Սովորաբար, եթե խոսում ենք բջջային շարժական կապի համակարգի մասին, ապա թողունակությունը հաշվարկելիս օգտագործում են Էռլանգի B մոդելը: Դա պայմանավորված է նրանով, որ արգելման հավանականության փոքր արժեքների դեպքում Էռլանգի B և C մոդելները բավականին մոտ արդյունքներ են ցուցաբերում: Երբ արգելման հավանականությունը՝ $P_B > 0{,}1$, տրաֆիկի համեմատաբար ոչ մեծ աճը ($A > 40$) հանգեցնում է հայցի արգելման հավանականության կտրուկ աճին, այսինքն՝ սպասարկման որակի կտրուկ վատացմանը: Այդ պատճառով բջջային շարժական կապի համակարգի թողունակությունը հաշվարկելը կատարվում է հայցի արգելման հավանականության 0,01...0,05 սահմաններում:

Սովորաբար պրակտիկայում (13) արտահայտությունը ներկայացվում է աղյուսակի տեսքով (աղյուսակ 5) [30, 106] :

Աղյուսակ 5

| Կապուղիների թիվը | Կանչի մերժման հավանականությունը $P_B = \psi(A, N)$ | | | | |
|---|---|---|---|---|---|
| | 0.002 | 0.01 | 0.02 | 0.05 | 0.10 |
| | $A$-տրաֆիկ (Էռլանգ) | | | | |
| 1 | 0.002 | 0.01 | 0.02 | 0.05 | 0.11 |
| 2 | 0.07 | 0.15 | 0.22 | 0.38 | 0.60 |
| 5 | 0.90 | 1.36 | 1.66 | 2.22 | 2.88 |
| 10 | 3.4 | 4.5 | 5.1 | 6.2 | 7.5 |
| 20 | 10.1 | 12.0 | 13.2 | 15.2 | 17.6 |
| 30 | 17.6 | 20.3 | 21.9 | 24.8 | 28.11 |
| 40 | 25.6 | 29.0 | 31.0 | 34.6 | 38.8 |
| 50 | 33.9 | 37.9 | 40.3 | 44.5 | 49.6 |
| 100 | 77.5 | 84.1 | 88.0 | 95.2 | 104.1 |
| 150 | 122.9 | 131.6 | 136.8 | 146.7 | 159.1 |
| 200 | 169.2 | 179.7 | 186.2 | 198.5 | 214.3 |

Կապուղիների թիվը մեծացնելիս տրաֆիկն ավելի արագ է աճում, քան կապուղիների թիվը: Այդ պատճառով ռացիոնալ նախագծված ցանցի յուրաքանչյուր բջջում կապուղիների թիվը պետք է լինի 30-ից ոչ պակաս:

### 2.4.1. Կորպորատիվ հեռահաղորդակցական ցանցի ծանրաբեռնվածության հաշվարկ

Կորպորատիվ հեռահաղորդակցական ցանցի ծանրաբեռնվածությունը տվյալների ծավալ է, որն իրապես փոխանցվում է ցանցով միավոր ժամանակում: Ցանցի ծանրաբեռնվածության հաշվարկը կատարվում է հետևյալ բանաձևով.

$$V = nv_i \qquad (20)$$

որտեղ $n$-ը ցանցում քոմփյութերների թիվն է,

$v_i$ – ն՝ ցանցում մեկ քոմփյութերի ծանրաբեռնվածությունը:

Ցանցում մեկ քոմփյութերի ծանրաբեռնվածությունն հաշվվում է հետևյալ բանաձևով.

$$V_i = D/t \ , \qquad (21)$$

որտեղ $D$ –ն փոխանցվող տվյալների քանակն է,

$t$- ն՝ ժամանակը, որի ընթացքում փոխանցվում են տվյալները:

Եթե D=3Մբ, t=60 վայրկյան, ապա v=3/60=0.05Մբ/վ: Եթե ընդունենք. որ ցանցում կա 50 քոմփյութեր, ապա ցանցի ծանրաբեռնվածությունը կկազմի V=50*0.05=2.5Մբ/վ:

**Ցանցի թողունակություն**

Թողունակությունը տվյալ ցանցի համար տվյալների փոխանցման առավելագույն թույլատրելի արագությունն է, որը որոշվում է բիթային արագությամբ և մի քանի այլ սահմանափակող ֆակտորներով (փոխանցվող տվյալների բլոկների միջև ինտերվալների տևողություն, ցանցով փոխանցվող ծառայողական ինֆորմացիայի ծավալ և այլն): Թողունակության արժեքը ցանցային տեխնոլոգիաների համար հայտնի են և տրվում են ըստ ստանդարտի: Շատ դեպքերում թողունակությունը կարելի է համարել հավասար բիթային արագությանը: Թողունակությունը 100BASE-TX ստանդարտի համար կազմում է 100Մբիթ/վրկ=12.5Մբ/վրկ:

**Ցանցի օգտագործման գործակից**

Ցանցի օգտագործման գործակիցը հավասար է ցանցի ծանրաբեռնվածության և թողունակության հարաբերությանը

$$ՑՕԳ = V/vmax: \qquad (22)$$

Անկախ նրանից, որ որոշակի տեխնոլոգիայով ցանցում տվյալների փոխանցման արագությունը միշտ նույնն է, ցանցի արտադրողականությունը փոքրանում է տվյալների փոխանցման ծավալին զուգընթաց: Առաջինը՝ փոխանցվող տվյալների ծավալը (տրաֆիկ) բաժանվում է ցանցի բոլոր քոմփյութերների միջև: Երկրորդ՝ նույնիսկ բաժանվող սեգմենտի թողունակության այն մասը, որը պետք է բաժին ընկնի մեկ հանգույցին, հաճախ նրան չի հասնում՝ տվյալների փոխանցման ընդհանուր միջավայրի հասանելիության աշխատանքի մեխանիզմի առանձնահատկություններից

ելնելով: Ցանցի օգտագործման գործակցի մեծացման որոշակի չափը բերում է տվյալների փոխանցման իրական արագության կտրուկ փոքրացմանը: Ժամանակի կորուստները, որոնք կապված են բաժանվող միջավայրի հասանելիության աշխատանքի մեխանիզմի հետ, կախված են քոմփյութերների ցանցին դիմելու բնույթից և չեն կարող հստակ հաշվարկվել, հետևաբար բավարար արտադրողականություն ապահովելու համար տրվում է ցանցի օգտագործման սահմանային արժեք, որի դեպքում ցանցն արագ կարձագանքի օգտատերերի հարցումներին:

## 2.5. Կորպորատիվ հեռահաղորդակցական ցանցերի աշխատունակության վրա ազդող մեքենայական ուսուցման միջոցով անոմալիաների հայտնաբերման մեթոդը և ալգորիթմը

Օրեցօր ավելանում են կորպորատիվ հեռահաղորդակցական ցանցերին անօրինական մատչում ստանալու փորձերը: Նման փորձերը հաջողվելու դեպքում միլիոնավոր դոլարների վնասներ են հասցվում հեռահաղորդակցական ծառայություններ մատուցող կազմակերպություններին: Վնաս հասցնող մեկ այլ պատճառ է ցանցում անսարքությունների առաջացումը: Խնդիր է առաջանում ունենալ ինտելեկտուալ համակարգեր, որոնք կկարողանան ժամանակին հայտնաբերել ցանցում տեղի ունեցող անոմալիաները և միջոցներ կձեռնարկեն՝ դրանց հետևանքները վերացնելու համար:

Ցանցի աշխատունակությունը բնութագրող տվյալները պարունակում են որակական բնութագրեր, որոնք հայտնի են որպես աշխատունակության առանցքային ցուցիչ կամ ԱԱՑ: Այդ տվյալները բնութագրում են հեռահաղորդակցական ցանցի վարքը և օգտագործվում են անոմալիաների հայտնաբերման համար: Երբ այդ բնութագրերի արժեքները դուրս են գալիս բնական վիճակում գտնվող հեռահաղորդակցական ցանցի բնութագրերի արժեքների միջակայքից, դա նշանակում է, որ համակարգում առաջացել է անոմալիա: Անոմալիաների առաջացման պատճառները բազմապիսի են: Ամեն մի խնդիր կարող է առաջանալ բազմաթիվ գործոնների պատճառով և դրանցից յուրաքանչյուրի դեպքում կարող է պահանջվել

առանձին մոտեցում: Բացի այդ կորպորատիվ հեռահաղորդակցական ցանցում առաջացող անոմալիաները հնարավոր չէ հայտնաբերել մեկ ԱԱՑ-ի միջոցով: Ցանցի բնութագրերից յուրաքանչյուրը ներկայացվում է մի քանի ԱԱՑ-ների միջոցով և անհրաժեշտ է հսկել դրանցից յուրաքանչյուրի արժեքը: ԱԱՑ-ների արժեքների հսկումն իրականացվում է մշտադիտարկման համակարգերի միջոցով:

Անոմալիաների հայտնաբերման համար կա 2 տարածված մոտեցում, որոնք հիմնված են դետերմինացված և վիճակագրական համակարգերի կիրառման վրա:

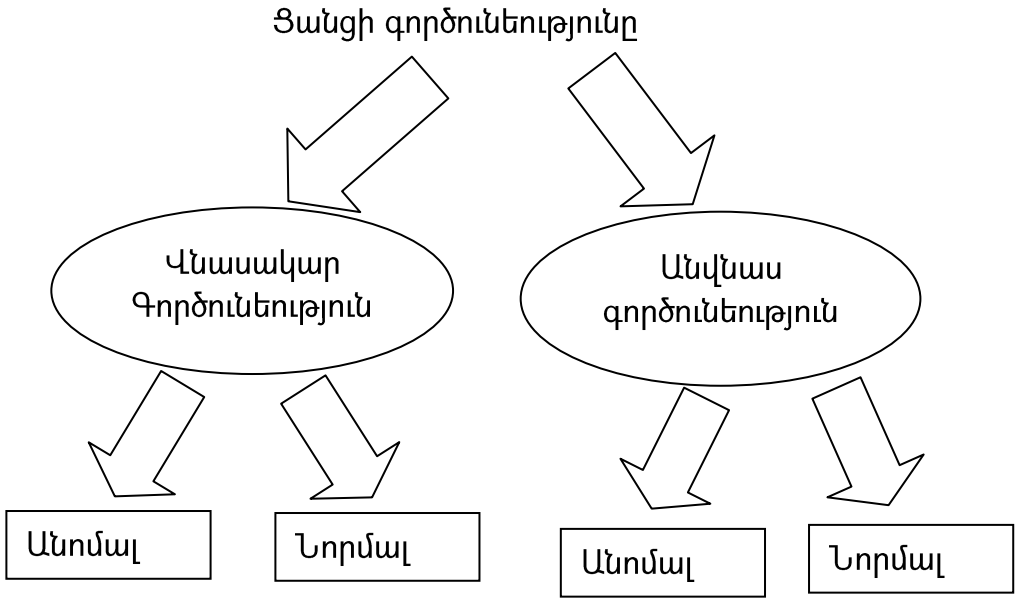
Դետերմինացված համակարգերն ԱԱՑ-ները համեմատում են իրենց մոտ պահվող արժեքների հետ: Նման համակարգերը պետք է ժամանակ առ ժամանակ թարմացնեն ԱԱՑ-ների իրենց տվյալները, իսկ նոր անոմալիաների առաջացման դեպքում նրանք անկարող են հայտնաբերել դրանք, քանի որ չունեն անհրաժեշտ տվյալներ, ինչը նման համակարգերի հիմնական թերությունն է:

Վիճակագրական համակարգերը, ի տարբերություն դետերմինացվածի, հավաքում են բնականոն վիճակում գտնվող համակարգի ԱԱՑ-ները և հայտնաբերումը կատարում են այդ տվյալների հիման վրա: Նման մոտեցումը թույլ է տալիս հայտնաբերել անհայտ անոմալիաները, ինչը այս մոտեցման առավելությունն է:

Վնասող գործունեություններից են ցանցի խափանումը, աշխատունակության կորուստը կամ ցանցի վրա ծանրաբեռնվածություն առաջացնող երթուղավորման ճանահապարհները: Բացի նշվածից, կա գործունեության ևս մեկ տեսակ, որը կարող է դիտարկվել որպես անոմալիա, սակայն դրանք անվնաս են: Դրանք ցանցային ադմինիստրատորի համար կարևորություն չեն ներկայացնում: Նման գործունեության օրինակ է ցանցային միջավայրում աշխատող նոր ծրագրի ավելացումը: Այդպիսի ծրագրերը կարող են զգալիորեն փոփոխել հեռահաղորդակցական ցանցի թրաֆիկը, հետևաբար նաև՝ ԱԱՑ-ները, սակայն դա պետք է դառնա ցանցի բնականոն աշխատանքի նոր վիճակ: Գործունեությունները բերված են նկ. 15-ում:

Անոմալիաների հայտնաբերման հետ մեկտեղ, դրանց հայտնաբերման համակարգերը պետք է ազդանշանների միջոցով այդ մասին տեղեկացնեն ադմինիստրատորին, ով պետք է ձեռնարկի համապատասխան միջոցառումներ: Ազդանշաններն իրենց մեջ պետք է պարունակեն հայտնաբերված անոմալիային

վերաբերող մետա-տվյալներ, ինչպիսիք են՝ հայտնաբերման ժամանակը, ասոցացվող IP հասցեն, ԱԱՑ արժեքը և այլն: Ցանցային ադմինիստրատորն այդ տեղեկատվությունն օգտագործում է անոմալիայի հայտնաբերման ազդանշանի առաջացման պատճառը հասկանալու համար: Առանց ավտոմատացման ազդանշանի առաջացման պատճառի հայտնաբերումը ժամանակատար գործընթաց է և կարող է տևել մինչև 1 ժամ:



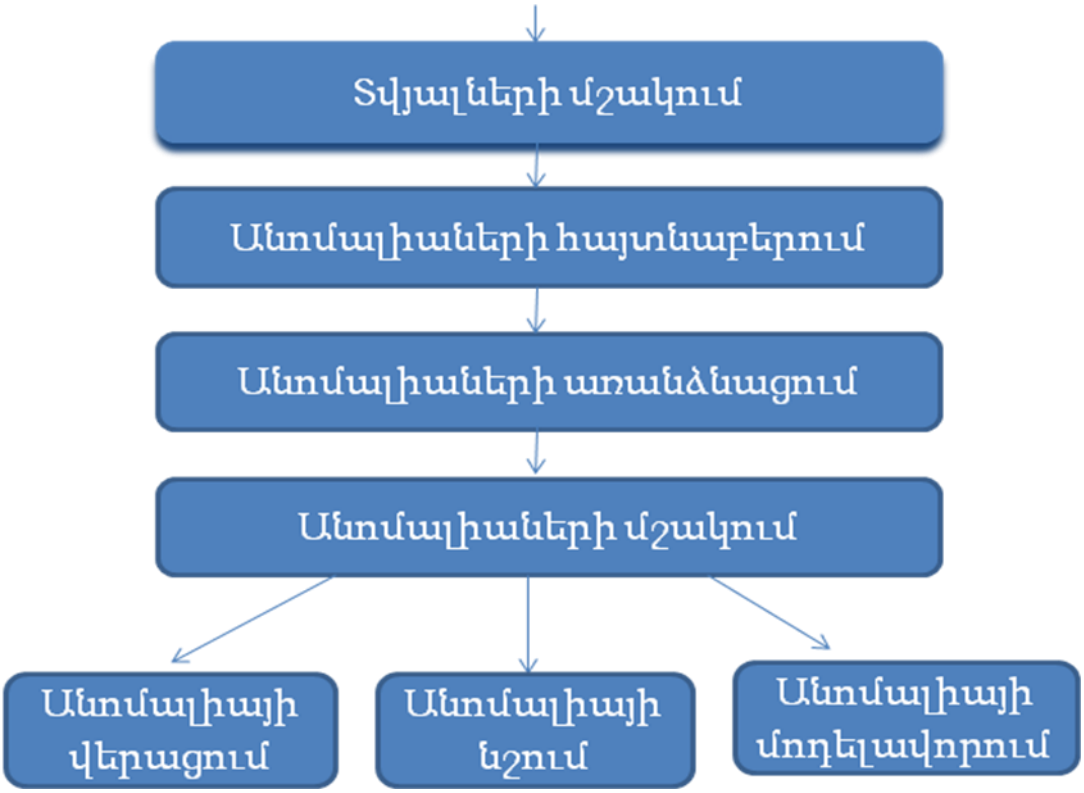

Նկ. 15. Անոմալիայի հայտնաբերման գործընթացը

Կորպորատիվ հեռահաղորդակցական ցանցերում անոմալիաների հայտնաբերումը և մշակումը (նկ. 16) կատարվում է մի քանի փուլով: Դրանք են.

- տվյալների մշակում,
- անոմալիաների հայտնաբերում,
- անոմալիայի առանձնացում,
- անոմալիայի մշակում,

Տվյալների մշակման փուլում անհրաժեշտ է եկած տեղեկատվության հոսքից առանձնացնել բոլոր այն տվյալները, որոնց վերլուծության արդյունքում հնարավոր է որոշել անոմալիայի առկայությունը:

Տվյալների առանձնացումից հետո կատարվում է մշակում, որի հիման վրա պետք է որոշվի՝ արդյոք հեռահաղորդակցական ցանցում դիտվու՞մ է անոմալիա, թե այն աշխատում է բնականոն վիճակում:




Նկ. 16. ԿՀՑ-ում անոմալիաների հայտնաբերումը և մշակման քայլային հաջորդականությունը

Եթե հեռահաղորդակցական ցանցում առաջացել է անոմալիա, ապա անհրաժեշտ է այն առանձնացել, առանձնացնել նրան այն չափանիշները, որոնց վերլուծության շնորհիվ հայտնաբերվել է անոմալիան, և ձեռնարկել անհրաժեշտ գործողություններ:

Անոմալիաների հայտնաբերման գործընթացը բաղկացած է երկու փուլից: Առաջինը տվյալների դասակարգումն է: Դրա միջոցով առանձնացվում է տվյալների խումբը, որոնք ունեն նորմալ արժեք և չեն կարող առաջացնել անոմալիա: Երկրորդ փուլով մնացած տվյալների համար կատարվում է համեմատում նորմալ վիճակի հետ և որոշվում դրանց շեղված կամ չշեղված լինելը:

**Անոմալիաների հայտնաբերումը մեքենայական ուսուցման միջոցով**

Կորպորատիվ հեռահաղորդակցական ցանցերի թրաֆիկի հոսքի դասակարգման անհրաժեշտությունը հետզհետե աճում է: Դասակարգումն օգտագործվում է այնպիսի նպատակներով, ինչպիսիք են միտումների վերլուծությունը, թրաֆիկի ադապտիվ, ցանցի վրա հիմնված QoS նշումը, մատչման դինամիկ հսկումը և այլն: Դասակարգում ասելով հասկանում ենք ծրագրերի կամ ծրագրերի խմբի առանձնացում, որոնք պատասխանատու են թրաֆիկի հոսքի համար:

Պորտերի վրա հիմնված դասակարգումը լայն տարածում ունի՝ չնայած այդ եղանակով կատարվող դասակարգման ճշտությունը մեծ չէ: Ճշտությունը հետզհետե էլ ավելի է նվազում, քանի որ ցանցային միջավայրում աշխատող ծրագերի քանակը գնալով աճում է, լայնորեն կիրառվում են NAT (Network Address Translation), պորտերի դինամիկ հատկացում, հեռահաղորդակցական ցանցից օգտվողների կողմից կիրառվող պորտերի փոփոխություն և այլն:

Ծրագրերի արձանագրությունների թրաֆիկի հոսքերի դասակարգման համար մեքենայական ուսուցման (ՄՈւ) տեխնոլոգիաների կիրառումը խոստումնալից այլընտրանք է [90,107]: Յուրաքանչյուր թրաֆիկի հոսք բնութագրվում է գործառույթների միևնույն խմբով, սակայն՝ դրանց տարբեր արժեքներով: ՄՈւ-ի վրա հիմված դասակարգումը կատարվում է ծրագրերի կողմից ստեղծվող թրաֆիկի հայտնի հոսքի վրա կատարվող ուսուցման հիման վրա:

Տվյալ խնդրի լուծման համար գոյություն ունեն ՄՈւ բազմաթիվ եղանակներ, և դրանցից յուրաքանչյուրի կիրառելիության մասին կատարվել են բազմաթիվ հետազոտություններ: Հնարավոր եղանակներից յուրաքանչյուրի կիրառման դեպքում ստացվում են տարբեր ճշտություններ: Հետազոտությունները ցույց են տալիս, որ առավել մեծ ճշտություն հնարավոր է ստանալ, եթե կիրառվեն ՄՈւ նեյրոնային ցանցերի կամ հենասյունային վեկտորների մեթոդները:

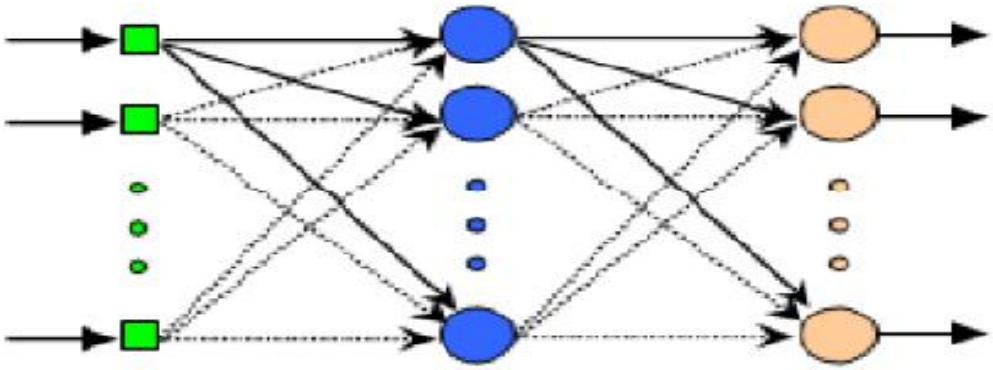
Այս եղանակները կիրառելի են ոչ միայն թրաֆիկի դասակարգման, այլև հետագայում դրանց վերլուծության հիման վրա հնարավոր է հայտնաբերել հեռահաղորդակցական ցանցերում առաջացող անոմալիաները:

### *Անոմալիաների հայտնաբերումը նեյրոնային ցանցերի միջոցով*

Նեյրոնային ցանցերը մեծ կիրառություն ունեն տարբեր տեսակի ծրագրերում, օրինակ պատկերների և ձայնի ճանաչման ծրագրերը արդյունքների մշակման և այլ բնագավառներում: Հաճախ այս բնագավառներում նեյրոնային ցանցերով աշխատող ծրագրերն անհամեմատ ավելի լավ արդյունք են տալիս, քան ուսուցման այլ համակարգեր: Նեյրոնային ցանցերն ունակ են կատարել մեծ ճշտությամբ

մոտարկումներ, ինչը նշանակում է, որ դրանք կարող են օգտագործվել դասակարգման խնդիրների լուծման համար:

Երբ նեյրոնային ցանցը (նկար 17) օգտագործվում է շաբլոնների դասակարգման համար, ապագա վեկտորի ամեն տարրի համար կա մեկ մուտքային հանգույց: Որպես կանոն ամեն հնարավորության համար, որը կարող է օգտագործվել, կա մեկ ելքային հանգույց: Թաքցված հանգույցները թույլ են տալիս ուսուցման ընթացքում նեյրոնային ցանցի կողմից մշակվել տվյալի ներքին ներկայացումը:



Նկ. 17. Պարզ նեյրոնային ցանցի սխեման

Նեյրոնային ցանցերի ուսուցման եղանակներից մեկը կոչվում է հետադարձ տարածման օրենք: Սա գրադիենտային նվազման եղանակ է և հիմնված է սխալի ֆունկցիայի վրա, որը ներկայացնում է ցանցի հաշվարկված և ցանկալի ելքերի տարբերությունը: Ներկայացված սխալի ֆունկցիան որոշվում է միջին քառակուսային սխալի (ՄՔՍ) հիման վրա: $I$ շաբլոնի սխալը ներկայացվում է հետևյալ բանաձևով.

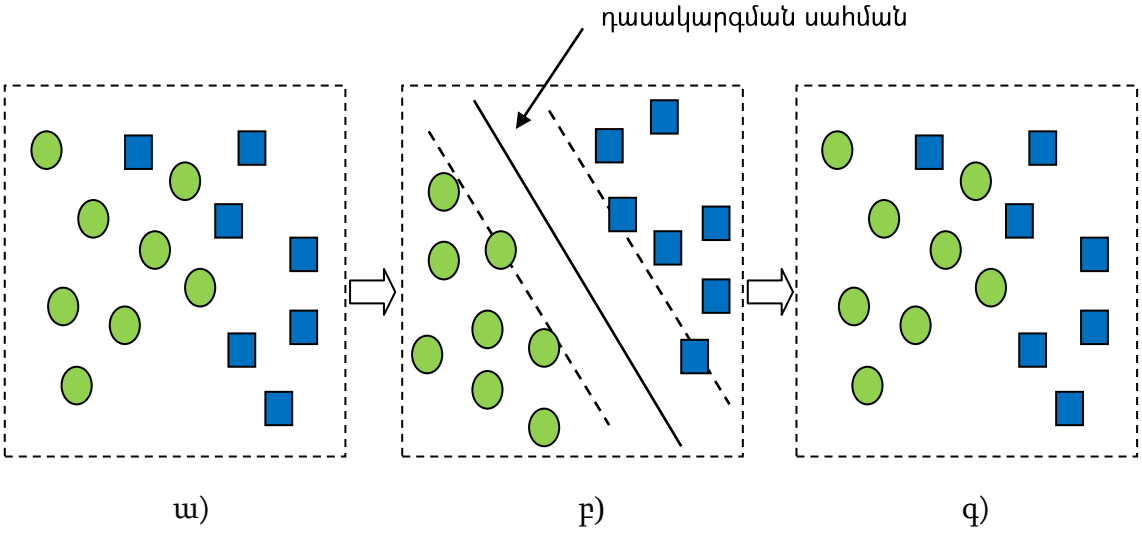
$$E^i = \frac{1}{2}\sum_{p=1}^{k}(y_p^i - O_p^i)^2, \qquad (23)$$

որտեղ $y_p^i$-ն $p$-րդ ելքային հանգույցի իրական ելքային տվյալն է, երբ $i$-րդ տարբերակի վեկտորը տրվում է ցանցին, և $k$ -ն ցույց է տալիս տվյալ ելքային շերտի նեյրոնների քանակը: Նման կերպ $O_p^i$-ն $p$-րդ ելքային հանգույցի ցանկալի ելքային տվյալն է: Դրա հետևանքով ՄՔՍ-ն կարող է հաշվարկվել ուսուցանող ամբողջ մուտքային տվյալների համար:

Որպեսզի նեյրոնային ցանցերի վրա հիմնած համակարգը հաջողությամբ սովորի, ցանցի իրական ելքը պետք է մոտենա ցանկալի ելքին՝ շարունակաբար նվազեցնելով այս սխալը: Հետադարձ տարածման օրենքը որոշակի մուտքի համար հաշվում է սխալը և այն մեկ մակարդակից հաղորդում նախորդին: Հանգույցների միջև եղած միացումների կշիռների հետ տարածված սխալի հիման վրա ճշգրտվում են այնպես, որ սխալը նվազեցվում է և համակարգը սովորում է:

**Արհեստական բանականության հենասյունային վեկտորների մեթոդը**

Հենասյունային վեկտորային մեթոդը (ՀՎՄ) մուտքային տվյալներն արտապատկերում է մեծ չափանի տարածության վրա, օգտագործելով համապատասխան միջուկային ֆունկցիան և կառուցում է որոշումների ֆունկցիան, որով լավագույն կերպով կարողանում է մի դասի տվյալները բաժանել մեկ այլ դասի տվյալներից: Նկար 18-ում բերված է ՀՎՄ-ի երկրաչափական ներկայացումը:




Նկ. 18- ՀՎՄ-ով ոչ գծային բաժանում. ա) մուտքային տվյալներ, բ) արտապատկերում մեծ տարածության վրա, գ) հետադարձ արտապատկերում

Ենթադրենք տրված է առանց դասակարգնան մասին տեղեկատվության $X_i \in R^n$, $i = 1,2,\dots l$, ուսուցող տվյալների խումբը, որտեղ $i$ -ն ուսուցման հավաքածուում առկա կետերի քանակն է, $R^n$ -ն՝ մուտքային տարածությունը և $n$ –ը՝ մուտքային տարածության չափը: $\Phi(x)$-ը արտապատկերող ֆունկցիա է, որը մուտքային

տարածության $x$ -ը ձևափոխում է ապագայի F տարածության: $f(x)$ որոշման ֆունկցիան կունենա հետևյալ տեսքը.

$$f(x) = w^T \Phi(x) - \rho:$$

(24)

Այն սկզբնական տվյալները բաժանում է բոլոր հնարավոր $\Phi(x)$, $i = 1,2,\dots.,l$ վեկտորների: $w$ -ն հիպերտարածության նորմավորված ուղղահայացն է, իսկ $\rho$ -ն՝ հիպերտարածության շեղումը: $w$ -ն և $\rho$ -ն գտնելու համար անհրաժեշտ է լուծել հետևյալ օպտիմիզացման խնդիրը:

Նպատակային ֆունկցիա

$$min \frac{1}{2} w^T w + \frac{1}{vl} \sum_{i=1}^{l} \xi_i - \rho, \quad (25)$$

սահմանափակումներ

$$w^T \Phi(x) \geq -\rho - \xi_i, \xi_i \geq 0, i = 1,2 \dots, l \quad (26)$$

Որտեղ $\xi_i$ -ն փոփոխական է, որը ճշտություն է մտցնում նպատակային ֆունկցիայում, իսկ $V \in (0,1)$-ն կառավարում է կոմպրոմիսը՝ առավելագույնի հասցնելով հիպերտարածության և սկզբնակետի հեռավորությունը և դրանում եղած կետերի քանակը : Նպատակային ֆունկցիան լուծելու համար անեն $xi$ -ի համար ներմուծենք $\alpha_i$ Լագրանժի արտադրիչը: Խնդրի լուծումը բերում է.

$$W = \sum_{i=1}^{l} \alpha_i \ \Phi(X_i), \quad (27)$$

որտեղ $0 \leq \alpha_i \leq \frac{1}{vl}$ : $f(x)$ ֆունկցիան դառնում է հետևյալ ոչ գծային ֆունկցիան.

$$f(x) = \sum_{i=1}^{l} \alpha_i K(x_i, x) - \rho \quad (28)$$

որտեղ $K(x_i, x) = \Phi(x_i)^T \Phi(x)$, որը մուտքային տարածության միջուկային ֆունկցիան է:

Հետազոտությունները ցույց են տալիս [5, 6], որ անոմալիաների հայտնաբերման համար ՀՎՄ-ները տալիս են ավելի բարձր արդյունք, սակայն եթե համեմատվում է, հայտնաբերման ճշտությունը, ապա արհեստական նեյրոնային ցանցերն ունեն ավելի մեծ ճշտություն: Տվյալ աշխատանքում կիրառվել է ՀՎՄ-ն:

Հեռահաղորդակցական ցանցերի բնութագրերի արդյունավետ և մատչելի չափումները շատ կարևոր են հատկապես այն ժամանակ, երբ ցանցը շահագործվում է ինտերնետին միացված վիճակում: Հեռահաղորդակցական ցանցերի բնութագրերում օգտագործվում են ինտերնետի վրա հիմնված համակարգերի կողմից՝ օգտագործողներին ավելի որակով ծառայություններ տրամադրելու նպատակով:

Մատուցվող ծառայությունների որակն անմիջականորեն կախված է այն հեռահաղորդակցական ցանցի բնութագրերից, որոնցով այդ ծառայությունները մատուցվելու են: Վեբ սերվերը հնարավոր չէ օգտագործել, եթե դրան միացված երթուղավորիչը սարքին չէ, կամ VoIP ծառայության հնարավորությունները խիստ սահմանափակ են քիչ թողունակությամբ ցանցերի համար:

Ցանցային բնութագրերի կարևորությունն ու արդիականությունը մեծապես կախված են այն ծրագրերից, որոնք օգտվելու են տվյալ ցանցից: Պարունակության բաշխման ցանցերը (content distribution network) կարող են հետաքրքրված լինել հաճախորդի և ծրագրային սրեվերի միջև եղած հապաղումներով, իսկ ծանրաբեռնվածության բաշխման ծրագրերի համար առկա թողունակությունն ավելի կարևոր չափանիշ է: Այլ բնութագրեր, ինչպիսիք են հերթերի երկարությունը, ցանցի ձախողումները և այլն, նույնպես շատ կարևոր են և կիրառվում են բազմաթիվ ծրագրային համակարգերի կողմից: Սակայն կա չորս հիմնական բնութագիր, որոնցով կազմվում է ցանցերի չափման հիմնական պարադիգման և կարող են կիրառվել այլ բնութագրերի հաշվման համար: Դրանք են.

- հապաղումը,
- փաթեթների կորուստը,
- ճանապարհի որոշումը,
- թողունակությունը:

Հապաղումը ցույց է տալիս այն ժամանակը, որը պահանջվում է հաղորդագրությունից, որպեսզի այն ուղարկող հանգույցից հասնի ստացող հանգույց: Սովորաբար այն չափվում է միլիվայրկյաններով (մվ): Բազնաթիվ ծրագրեր հապաղումն օգտագործում են սերվերների հասանելիությունը ստուգելու համար կամ

հապաղման տեսանկյունից մոտակա սերվերների որոշման համար [46]: Համեմատելով նույն հագույցների միջև եղած տարբեր ճանապարհներով տվյալների հաղորդման հապաղումները՝ հանարվոր է գտնել առավել արդյուանվետ ճանահապարհը:

Փաթեթների կորուստը չափվում է հաղորդված և ստացված փաթեթների քանակով: Եթե դրանք տարբեր են, ուրեմն տեղի է ունեցել կորուստ: Ճանապարհի կորստի գործակիցը տոկոսների տեսքով ցույց է տալիս, թե փաթեթների քանի տոկոսն է կորել, երբ հաղորդվել են տվյալ ճանապարհով: Կորած փաթեթներն ազդում են ծրագրերի արդյունավետության վրա, քանի որ հաճախ կորած փաթեթներն անհրաժեշտ է նորից հաղորդել: Ուստի միշտ գերադասելի է ընտրել այնպիսի ճանապարհ, ուր կորստի գործակիցը ցածր է:

Ճանապարհի որոշումը կիրառվում է, երբ հաղորդագրությունը մի հանգույցից պետք է հասնի մեկ այլ հանգույց: Այդ հանգույցների միջև կարող են լինել բազմաթիվ երթուղավորիչներ, որոնք պետք է վերահաղորդեն հաղորդագրությունը: Ճանապարհի որոշումը գործընթաց է, որով որոշվում է հաղորդագրության անցնելու այն իրական ճանապարհը, երբ մի հանգույցից ուղարկվում է մեկ այլ հանգույց:

Թողունակությունը ցույց է տալիս, թե ճանապարհը միավոր ժամանակում ինչ տարողություն ունի: Այն չավում է բիթ վայրկյանով (bps, bits per second): Թողունակությունը մեծ կարևորություն և ազդեցություն ունի հատկապես մուլտիմեդիա ծրագրերի համար: Նման ծրագրերն ունեն թողունակության մեծ պահանջ: Թողունակություն տերմինը կարող է ցույց տալ արագությունների երկու տարբեր տեսակ: Վերբեռնման արագությունը ցույց է տալիս տվյալները նպատակակետ հասցնելու գործակիցը, իսկ ներբեռնման արագությունը ցույց է տալիս այն գործակիցը, որով տվյալները ստացվում են: Թողունակության չափման համար կիրառելի է երկու եզրույթ՝ տարողություն և հասանելի թողունակություն:

Տարողությունը ցույց է տալիս, թե հանգույցը առավելագույնը ինչքան տվյալ կարող է հաղորդել: Այն չափվում է միավոր ժամանակում հաղորդված տվյալների միավորների քանակով: Հանգույցի տարողությունը տվյալների մակարդակի համար

որպես կանոն հաստատուն է: Օրինակ, գիգաբիթ Ethernet-ի համար այն 1 գիգաբիթ վայրկյան է:IP ցանցերում IP փաթեթները ներկառուցված են տվյալների մակարդակի փաթեթների մեջ, ուստի տարողունակությունը պետք է հաշվի առնի նաև տվյալները ֆրեմերով ուղարկելու պատճառով առաջացող լրացուցիչ բեռնվածքը:

Ճանապարհի իրական թողունակությունը կարող է ներկայացվել հետևյալ կերպ.

$$C = C_L \frac{L}{O+L}, \tag{29}$$

որտեղ $C$-ն իրական տարողությունն է, $C_L$ –ը՝ տվյալների մակարդակի տարողությունը, $O$-ն IP փաթեթի ինկապսուլիացիայի վրադիր ծախսն է, իսկ $L$ –ը՝ Ethernet ֆրեյմի երկարությունը:

Առկա թողունակությունը հանգույցի չօգտագործված թողունակութոյնն է: Ժամանակի ցանկացած պահի հանգույցը կամ ամբողջ արագությամբ տվյալ է հաղորդում, կամ ազատ է, ուստի հանգույցի օգտագործումը $(\mu)$ ներկայացվում է որպես ժամանակային միջակայքերի հաջորդականության միջին: Միջին թողունակությունը հավասար է գումարային թողունակությունից հանած միջին օգտագործումը, որտեղ օգտագործումը ներկայացվում է որպես ընդհանուր թողունակության չափամաս $A = C(1 - \mu)$:

Ճանապարհի առկա թողունակությունը կարող է հաշվվել՝ միավոր ժամանակում հաղորդված տվյալների քանակը չափելով: Հապաղումը չափելու համար կարելի է կիրառել Նմուշների Ճեղքվածքի Մոդելը (ՆՃՄ), որը կարող է ներկայացվել հետևյալ կերպ. ուղարկվում է երկու նմուշ, որոնք բաժանված են $t_1$ ժամանակային միջակայքով: Երկու նմուշները տեղ են հասնում $t_2$ ինտերվալով: Եթե $t_2 > t_1$, ուրեմն տեղի է ունեցել հապաղում: Եթե կա հապաղման մեկ պատճառ, ուստի $t_2$-$t_1$-ը հապաղումն է: Եթե հապաղման պատճառի տարողությունը $C$ է, ապա այդ հատվածում օգտագործումը կլինի

$$\mu = C\left(\frac{t_2 - t_1}{t_1}\right) \tag{30}$$

Քանի որ տվյալ մոդելը ենթադրում է հապաղման մեկ պատճառ, ուրեմն ճանապարհի օգտագործումը հավասար է հապաղման առաջացման պատճառի (bottleneck) օգտագործմանը: Առկա թողունակությունը կլինի.

$$A = C\ (1 - \frac{t_2 - t_1}{t_1}) \tag{31}$$

Դիցուք ունենք $W = W_1, W_2, \dots, W_T$ ժամանակի շարք, որը կազմված է ժամանակի իրար հավասար $T$ մասերից՝ $t = 1,2, \dots, T$:

Ժամանակի շարքի ընդհանուր մոդելը կարելի է ներկայացնել հետևյալ կերպ.

$$w_t = g(t) + Y_t\ , \tag{32}$$

որտեղ $g(t)$-ն ժամանակի դետերմինացված ֆունկցիա է, իսկ $Y_t$-ն՝ ներկայացնում է աղմուկը կամ սխալը:

Մեքենայական ուսուցման եղանակով ժամանակի տվյալ պահին արժեքի կանխատեսումը կարող ենք ներկայացնել հետևյալ ձևով.

$$y = f(x) + n\ , \tag{33}$$

որտեղ $f(x)$-ը դետերմինացված ֆունկցիա է, $n$-ը աղմուկն է կամ սխալը:

Որպես մուտքային տվյալ ունենք $\{(x_i y_i) : i = 1, \dots, N\}$ ուսուցողական տվյալները, որտեղ $x_i = (x_{i1}, \dots, x_{in})$, իսկ $y_i$-ն գեներացվում է նախորդ տվյալների հիման վրա:

Մեքենայական ուսուցման նպատակն է՝ գտնել այնպիսի $f'(x)$ ֆունկցիա, որը հնարավորինս լավ կկանխատեսի $f(x)$ ֆունկցիան:

ՀՎՄ-ի կիրառման դեպքում ժամանակի $t$ պահին ստացված արժեքի համար պետք է որոշվի, թե արդյոք այն գտնվու՞մ է անոմալիայի գոտում:

Ենթադրենք ժամանակի անոմալիայի գոտում գտնվող արեժքները ստացվում են հետևյալ ֆունկցիայով.

$$y_{an} = f_{an}(t), \tag{34}$$

իսկ անոմալիայի գոտուց դուրս գտնվողները հետևյալով.

$$y_n = f_n(t)\ : \tag{35}$$

Այդ դեպքում ժամանակի $t$ պահին ստացված արժեքը որ գոտուն որ մոտ կգտնվի, այդ գոտուն էլ կհամապատասխանի դրա արժեքը, ուստի անհրաժեշտ է գտնել հետևյալ արտահայտության նվազագույն արժեքը և ըստ դրա որոշել, թե որ գոտուն է պատկանում մուտքային արժեքը.

$$z = \min\left(y - y_{an}, y - y_n\right) \tag{36}$$

Հեռահաղորդակցական ցանցերի բնութագրերի արդյունավետ և մատչելի չափումները շատ կարևոր են հատկապես, երբ ցանցը շահագործվում է ինտերնետին միացված վիճակում: Հեռահաղորդակցական ցանցերի բնութագրերն օգտագործվում են ինտերնետի վրա հիմնված բաշխված համակարգերի կողմից, որպեսզի օգտագործողներին տրամադրեն ավելի լավ որակի ծառայություններ:

## Գլուխ 2-ի վերաբերյալ եզրակացություններ

Տվյալ գլխում կատարված հետազոտությունների հիման վրա կարելի է գալ հետևյալ եզրակացությունների.

1. Կորպորատիվ հեռաղորդակցական ցանցերի ղեկավարման խնդիրները լուծելու համար առաջարկվում է օգտագործել հեռահաղորդակցական ցանցերի անվտանգության ղեկավարման համակարգ, որն ապահովում է հեռահաղորդակցական ցանցերի աշխատանքի հուսալիություն և կատարում է հոսթերի սկանավորում:
2. Կորպորատիվ հեռահաղորդակցական ցանցերի ապարատածրագրային սարքերի՝ տվյալ դեպքում օպտիմարարների, ներդրման պրակտիկ փորձը ցույց է տալիս, որ տեղադրման ժամանակ փոխանցվող տրաֆիկի ծավալը փոքրանում է 3…5 անգամ, իսկ տվյալների փոխանցման գագաթնակետային արագությունը մեծանում է մոտ 100 անգամ:
3. Կորպորատիվ հեռահաղորդակցական ցանցերում անոմալիաների հայտնաբերման արհեստական բանականության մեթոդներից պետք է դիտարկել հենասյունային վեկտորային մեթոդը, որը տալիս է ցանցի համար անոմալիայի հայտնաբերման ավելի բարձր արդյունք:

# ԳԼՈՒԽ 3. ԿՈՐՊՈՐԱՏԻՎ ՀԵՌԱՀԱՂՈՐԴԱԿՑԱԿԱՆ ՑԱՆՑԵՐԻ ՕՊԵՐԱՏԻՎ ԿԱՌԱՎԱՐՄԱՆ ԱՎՏՈՄԱՏԱՑՎԱԾ ՀԱՄԱԿԱՐԳԻ ՄՇԱԿՈՒՄԸ

Հեռահաղորդակցական ոլորտում առկա է մեծ մրցակցություն, և առավել մրցունակ է այն կազմակերպությունը, որը տրամադրում է մեծ քանակությամբ ծառայություններ և միաժամանակ ապահովում՝ դրանց բարձր որակը: Սակայն իրական ժամանակում նորանոր ծառայությունների մատուցման անհրաժեշտությունը հանգեցնում է դրանց շահագործման և կառավարման հետ կապված մի շարք խնդիրների: Ներկայումս նշված խնդիրները հաշվի են առնվում ժամանակակից հեռահաղորդակցական ցանցերի նախագծման փուլից սկսած, ինչը պարզեցնում է նման ցանցերի կառավարումը, սակայն կան բազմաթիվ շահագործվող հեռահաղորդակցական ցանցեր, որոնցում նշված խնդիրները առկա են և դրանց համար պահանջվում են արդյունավետ լուծումներ:

## 3.1. Կորպորատիվ հեռահաղորդակցական ցանցերի օպերատիվ կառավարման համար առաջարկվող մեթոդը

Կապիտալ և գործառնական ծախսերի կրճատումը, բիզնես գործընթացների ավտոմատացման և օպտիմալացման շնորհիվ ներդրված գումարների վերադարձի ցուցանիշի բարձրացումը, մատուցվող ծառայությունների որակի բարձրացման արդյունքում հաճախորդների բավարարվածության և լոկալության ցուցանիշի բարձրացումը մեծ դեր են խաղում հեռահաղորդակցական ծառայություններ մատուցող կազմակերպությունների մրցակցության մեջ: Այս խնդիրների լուծման համար կարևոր դեր է խաղում նշված ցանցերի կառավարման արդյունավետությունը:

Կորպորատիվ հեռահաղորդակցական ցանցերի սպասարկումը ենթադրում է.

1. ցանցերի մոնիտորինգ և կառավարում,
2. խնդիրների հայտնաբերում և լուծում,
3. ցանցի արտադրողականության կառավարում,
4. ենթակառուցվածքների արդյունավետ բաշխում,

5. մատուցվող ծառայությունների առաջնահերթության որոշում,
6. նմանատիպ այլ խնդիրների լուծում:

Սակայն նշված խնդիրներից շատերի լուծումները համապիտանի են մեկ հեռահաղորդակցական ցանցի շրջանակներում: Հաճախ առաջացած խնդիրը լուծելու համար անհրաժեշտ չէ որոնել նոր լուծում, այլ բավարար է կիրառել արդեն իսկ գտած լուծումը:

Կորպորատիվ հեռահաղորդակցական ցանցերի աշխատունակությունն ապահովելու համար անհրաժեշտ է կատարել դրա ճիշտ կառավարում: Գրագետ կառավարում իրականացնելու համար անհրաժեշտ է օգտվել հեռահաղորդակցական ցանցերի կառավարման համակարգերից (ՀՑԿՀ): ՀՑԿՀ-ն ապարատային և ծրագրային լուծումների հավաքածու է, որը հնարավորություն է տալիս ադմինիստրատորներին հեռահաղորդակցական ցանցում կատարել առանձին բաղադրիչների հսկում և կառավարում:

Նման համակարգերը հնարավորություն են տալիս կատարել հետևյալ գործառույթները.

- Ցանցային սարքավորումների հայտնաբերում – հայտնաբերել, թե տվյալ պահին ինչ սարքեր են միացված համակարգին,
- Ցանցային սարքավորումների մշտադիտարկում – մշտադիտարկել ցանցում առկա սարքավորումները, որպեսզի պարզ լինի, թե ինչ վիճակում են գտնվում ցանցի առանձին բաղադրիչները և ինչ աստիճանի է դրանց կատարողականությունը համապատասխանում նախապես տրված արժեքներին,
- Ցանցի կատարողականության գնահատում – կատարվում է ցանցի այնպիսի բնութագրերի հսկմամբ, ինչպիսիք են թողունակությունը, փաթեթների կորուստը, հապաղումը, հասանելիությունը,
- Ինտելեկտուալ ծանուցումներ – կարգավորվող ազդանշաններ, որոնք կարձագանքեն որոշակի ցանցային իրավիճակներին՝ ցանցային ադմինիստրատորին տեղյակ պահելով sms հաղորդագրության, էլ փոստի կամ այլ եղանակներով:

Արդիական է դիտարկել այնպիսի մեթոդի մշակումը, որով հնարավոր կլինի դասակարգել կառավարման և շահագործման առաջացած խնդիրը, հիշել դրանց

լուծումները և անհրաժեշտության դեպքում կիրառել արդեն իսկ հայտնի լուծումը: Այդպիսի մոտեցմամբ հնարավոր է նվազեցնել հեռահաղորդակցական ցանցերում առաջացող խնդիրների լուծման համար պահանջվող ժամանակն այն դեպքերի համար, երբ արդեն հայտնի է տվյալ խնդրի լուծումը: Դա իր հերթին կհանգեցնի հեռահաղորդակցական ցանցի աշխատունակության բարձրացման և, որպես հետևանք, կմեծանա վերջինիս եկամտաբերությունը: Մեկ այլ խնդիր է որոշակի ծառայությունների մատուցման համար ռեսուրսների պահեստավորումն ու արդյունավետ բաշխումը: Դրա համար պահանջվում է որոշակի կրնկնվող գործողությունների կատարում, որոնք նույնպես կարող են հիշվել և հետագայում կիրառվել՝ զգալիորեն կրճատելով ծառայության մատուցման նախապատրաստման համար պահանջվող ժամանակը:

Հեռահաղորդակցական ցանցերի օպերատիվ կառավարման առաջարկվող մեթոդի դեպքում անհրաժեշտ է.

- կատարել հեռահաղորդակցական ցանցի մշտադիտարկում,
- հայտնաբերել հեռահաղորդակցական ցանցերում առաջացած պատահարները,
- հիշել պատահարների լուծման և ծառայությունների մատուցման համար անհրաժեշտ քայլերը,
- անհրաժեշտության դեպքում կիրառել որոշակի խնդիրների համար անհրաժեշտ լուծումները:

### Կորպորատիվ հեռահաղորդակցական ցանցերի մշտադիտարկում

Կորպորատիվ հեռահաղորդակցական ցանցերում թույլ կամ անաշխատունակ հանգույցների հայտնաբերման համար անհրաժեշտ է կատարել մշտադիտարկում և շեղումներ հայտանբերելու դեպքում այդ մասին տեղյակ պահել ադմինիստրատորներին, ովքեր կկարողանան շտկել խափանումը և վերականգնել ցանցի աշխատունակությունը: Կորպորատիվ հեռահաղորդակցական ցանցերում անաշխատունակ հանգույցները կարող են զգալի նյութական վնասներ հասցնել այն կազմակերպությանը, որին պատկանում է ցանցը, ուստի կարևոր է, որ ադմինիստրատորները խափանման մասին տեղեկացվեն որքան հնարավոր է շուտ և

ունենան բավարար նախնական տեղեկատվություն, որ կարողանան հնարավորինս արագ վերականգնել ցանցի աշխատունակությունը: Ադմնիստրատորին արագ տեղեկացնելու նպատակով կիրառվում են էլեկտրոնային փոստի, կարճ հաղորդագրության և որոշ դեպքերում՝ հեռախոսային զանգի միջոցով ծանուցման ավտոմատ համակարգեր:

Կորպորատիվ հեռահաղորդակցական ցանցերում մշտադիտարկումն իրականացնում են այդ նպատակով ստեղծված հատուկ ապարատածրագրային համակարգերը: Նման համակարգերի գործառույթներն են՝ հայտնաբերել ցանցում առկա խափանումները, անոմալիաները, անսարքությունները, ինչպես նաև կատարել դիագնոստիկ և պրոֆիլակտիկ աշխատանքներ: Մշտադիտարկման համակարգերը հսկում են հանգույցների նախապես նշված բնութագրերը՝ CPU-ի ծանրաբեռնվածությունը, հիշողության վիճակը և այլն:

Մշտադիտարկման համար կա երկու մոտեցում՝ պասիվ և ակտիվ:

Պասիվ մեթոդները հիմնված են ցանցային թրաֆիկի լսելու և վերլուծության վրա, որոնք մեծ տարածում չեն գտել:

Ի տարբերություն պասիվ մեթոդի, ակտիվ մեթոդի դեպքում իրականացվում է նպատակային ցանցային փոխազդեցություն նպատակային համակարգի հետ: Նման մոտեցումներից է ոչ ստանդարտ վերնագրով TCP փաթեթների փոխանակումը:

Որպես կանոն, մշտադիտարկումն իրականացվում է լայն տարածում ստացած ICMP (Internet Control Message Protocol) և SNMP (Simple Network Management Protocol) արձանագրությունների միջոցով: Գոյություն ունեն մշտադիտարկման բազմաթիվ անվճար և այնպես էլ վճարովի համակարգեր: Աշխատանքում ներկայացված համակարգի համար նպատակահարմար է կիրառել անվճար և բաց կոդով տարածվող համակարգեր, որոնցից առավել տարածվածներն են openNMS, Zenoss Core, Nagios, Zabbix, icinga, cacti:

Բացի նշված համակարգերից, կան նաև հարթակներ, որոնք հնարավորություն են տալիս ստեղծել որոշակի խնդիրների լուծմանն ուղղված մասնագիտացված համակարգեր: Դրանցից կարելի է առանձնացնել PayLes հարթակը, որը նախատեսված է SDN-ի (Software-defined networking) համար:

## 3.2. Կորպորատիվ հեռահաղորդակցական ցանցերի օպերատիվ կառավարման ավտոմատացված եղանակի մշակումը

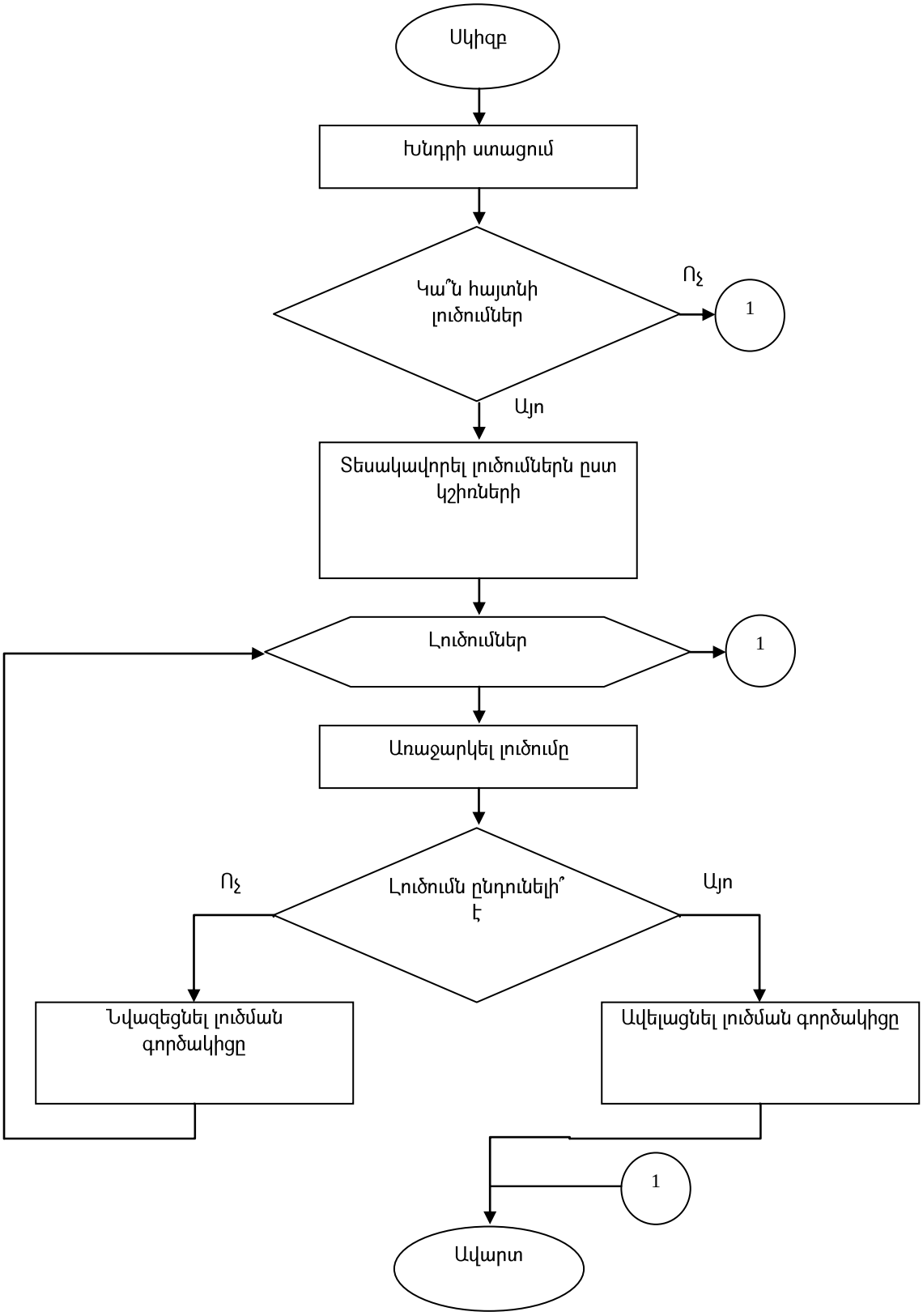
Ինչպես արդեն նշվեց, կորպորատիվ հեռահաղորդակցական ցանցերի օպերատիվ կառավարման խնդիրները հաճախ կրկնվում են և պահանջում են միևնույն լուծումը: Սակայն լինում են դեպքեր, երբ առաջարկվող լուծումն ընդունելի չի լինում, և անհրաժեշտություն է առաջանում կիրառել մեկ այլ լուծում: Այս դեպքում պետք է ինչ-որ ձևով գնահատել լուծումները: Դա կարելի է անել՝ յուրաքանչյուր լուծմանը տալով որոշակի գործակից և ադմինիստրատորի կողմից տվյալ լուծումը կիրառելու կամ չկիրառելու դեպքում համապատասխան ավելացնել կամ նվազեցնել գործակցի արժեքը: Նկարագրված մոտեցման բլոկ-սխեման բերված է նկ. 19-ում:

Դիտարկենք ներկայացված ալգորիթմի աշխատանքը:

Այն բաղկացած է հետևյալ փուլերից.

- խնդրի ստացում,
- լուծումների որոնում,
- կշիռների վերահաշվարկ:

Դիտարկենք փուլերից յուրաքանչյուրը: Առաջին փուլում մշտադիտարկման համակարգի կողմից հայտնաբերվում է որևէ խնդիր և այն ուղարկվում է մշակման: Մշակման փուլում ստուգվում է, թե արդյոք նման խնդրի համար կա արդեն իսկ կիրառված լուծում կամ լուծումներ, թե՝ ոչ: Եթե տվյալ խնդրի համար լուծում չի գտնվում, ապա ալգորիթմի աշխատանքն ավարտվում է: Եթե կա մեկ կամ մի քանի լուծում, ապա դրանք տեսակավորվում են ըստ կշիռների և առաջարկվում ադմինիստրատորին: Ադմինիստրատորը հաջորդաբար ստանալով լուծումները՝ հերթով դիտարկում է դրանք [5]:




Նկ. 19. Խնդիրների լուծումների կշիռների որոշման առաջարկվող մոտեցման բլոկ-սխեման

Եթե հերթական լուծումը նրան բավարարում է, ապա դրա կշիռը մեծացվում է և մյուս լուծումները չեն դիտարկվում, ու ալգորիթմի աշխատանքն ավարտվում է: Եթե

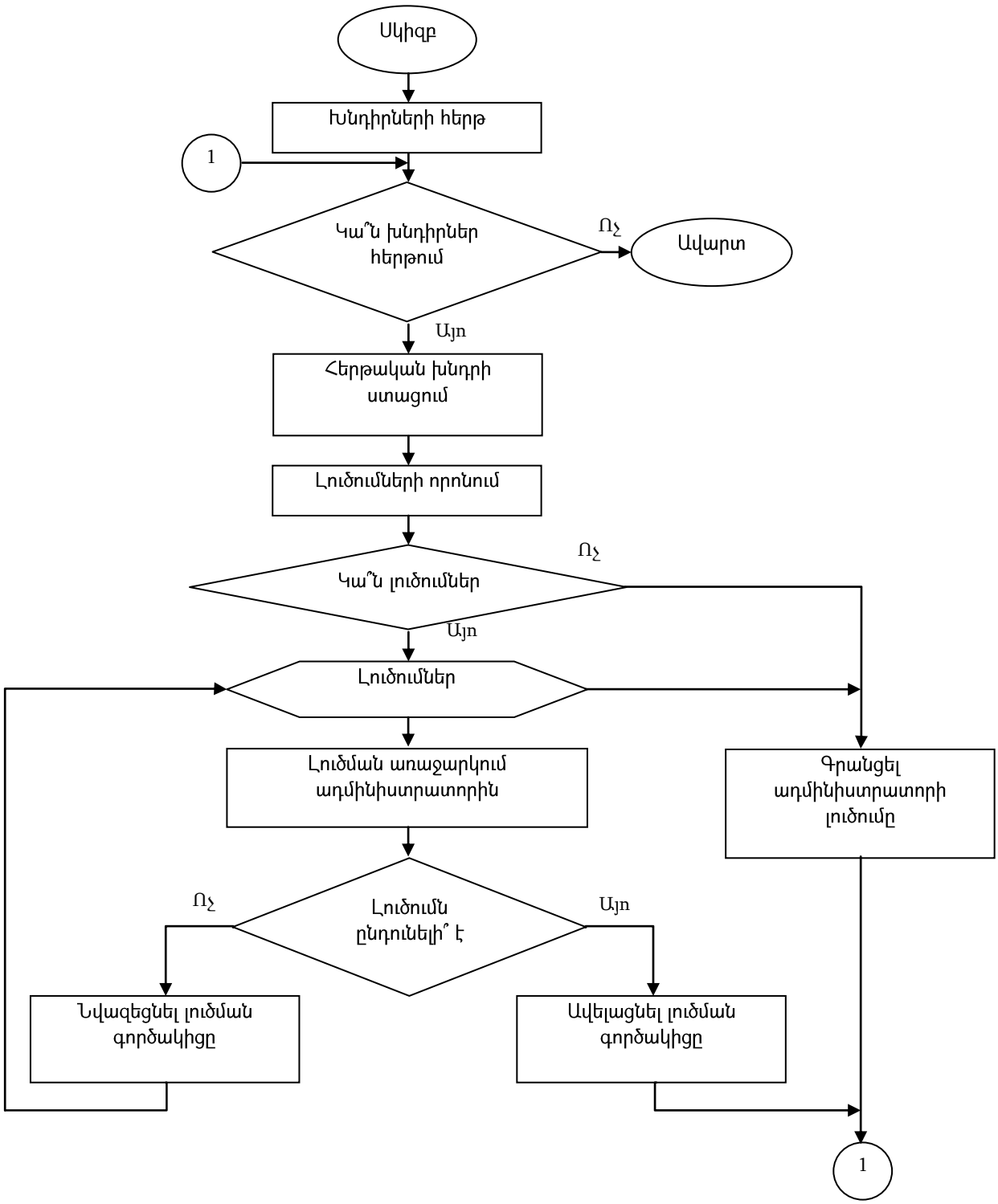
հերթական լուծումը չի ընդունվում ադմինիստրատորի կողմից, ապա դրա կշիռը նվազեցվում է և առկայության դեպքում առաջարկվում է հաջորդ լուծումը: Եթե լուծումներ այլևս չկան, ալգորիթմի աշխատանքն ավարտվում է: Կորպորատիվ հեռահաղորդակցական ցանցերի օպերատիվ կառավարման ժամանակ առաջացած խնդիրները կարելի է բաժանել երկու ընդհանրացված խմբի. պատահարներ և պլանավորված գործողություններ:

Առաջին խմբի պատահարների մեջ մտնում են մշտադիտարկման համակարգերի և կորպորատիվ հեռահաղորդակցական ցանցի օգտվողների կողմից հայտնաբերված անսարքություններն ու թերությունները, օրինակ, հանգույցների ծանրաբեռնվածությունը, սարքերի խափանումը, թողունակության անկումը և այլն:

Երկրորդ խմբի խնդիրներից են տեսակոնֆերանսների կազմակերպումը, թողունակության պահուստավորումը և այլ աշխատանքներ, որոնք հանդիսանում են կորպորատիվ հեռահաղորդակցական ցանցերի բնականոն աշխատանքի բաղացուցիչ մաս և իրենց բնույթով պատահարներ չեն:

Առաջարկվում է կորպորատիվ հեռահաղորդակցական ցանցերի օպերատիվ կառավարման ժամանակ առաջացած խնդիրների լուծման արդյունավետության բարձրացման համար կիրառել այն մեթոդը, որի բլոկ-սխեման բերված է նկ. 20-ում:

Ներկայացված եմեթոդը առաջացած յուրաքանչյուր խնդրի համար փնտրում է հնարավոր լուծումներ: Եթե լուծումներ գտնվում են, դրանք առաջարկվում են ադմինիստրատորին, հակառակ դեպքում՝ ադնինիստրատորի կողմից առաջարկվում է խնդրի նոր լուծում:




Նկ. 20. Հեռահաղորդակցական ցանցերի օպերատիվ կառավարման առաջարկվող մեթոդի բլոկ-սխեման

Եթե ադմինիստրատորին առաջարկված լուծումները կիրառելի չեն լինում տվյալ խնդրի լուծման համար, ներմուծվում է նոր լուծում, որը հետագայում կառաջարկվի նմանատիպ խնդիրների լուծման համար:

Առաջարկվող մեթոդի հիման վրա կարելի է մշակել գործիքամիջոց, որը ադմինիստրատորների կողմից կարող է օգտագործվել կորպորատիվ հեռահաղորդակցական ցանցերի օպերատիվ կառավարման համար՝ զգալիորեն մեծացնելով կառավարման արդյունավետությունը:

### 3.3. Կորպորատիվ հեռահաղորդակցական ցանցերում անոմալիաների հայտնաբերման ավտոմատացված համակարգի նախագծումը

Վերջին ժամանակներում կորպորատիվ հեռահաղորդակցական ցանցերում անոմալիաների հայտնաբերումը լայնորեն քննարկվում է գիտական և առևտրային շրջանակներում: Թույլատրելի-ընդունելի սահմաններից դուրս վիճակը կոչվում է անոմալիա: Անոմալիաների հայտնաբերումը կիրառվում է անվտանգության, հասանելիության, ծառայության որակի, վիրուսային ծրագրերի հայտնաբերման համար:

Կորպորատիվ հեռահաղորդակցական ցանցերում անոմալիան կարելի է ներկայացնել որպես իրադարձություն, որն առանձնացվում է ցանցի բնականոն աշխատանքից:

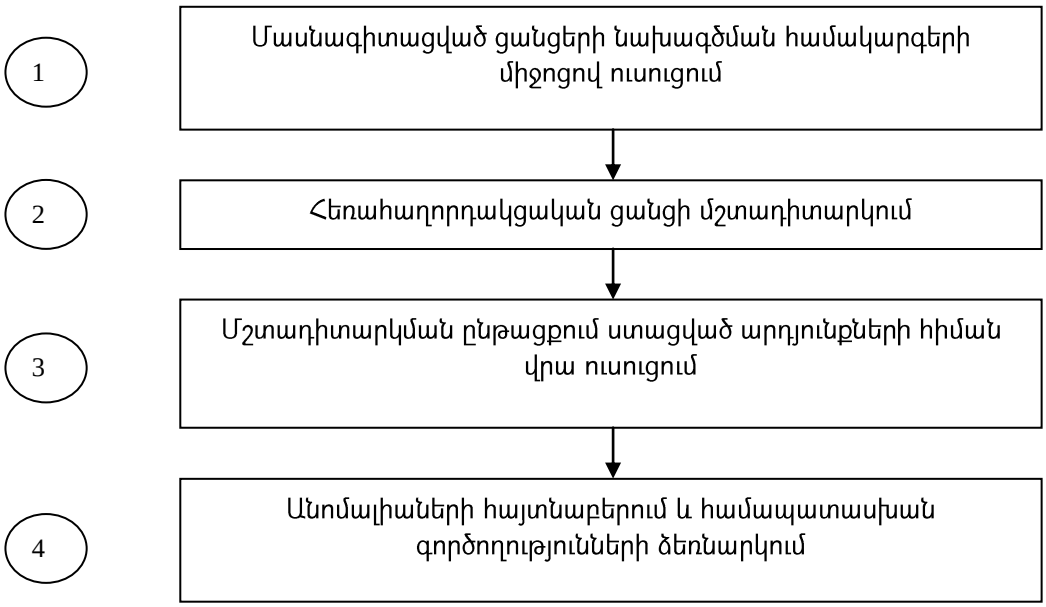
Կորպորատիվ հեռահաղորդակցական ցանցերում անոմալիաների հայտնաբերման համար անհրաժեշտ է այդ ցանցերում կատարել մշտադիտարկում: Մշտադիրատկման արդյունքում ստացված արդյունքների վերլուծության հիման վրա կարելի է հայտնաբերել խափանումներ, ծանրաբեռնված հանգույցներ և այլն: Սակայն մինչ անոմալիաների հայնտաբերումը պետք է հեռահաղորդակցական ցանցի համար որոշվի մշտադիտարկվող պարամետրերի արժեքները ցանցի աշխատանքի նորմալ ռեժիմի համար: Անոմալիայի հայտնաբերման դեպքում անհրաժեշտ է հեռահաղորդակցական ցանցում կատարել անհրաժեշտ միջամտություններ: Անոմալիաների հայտնաբերման ժամանակ հեռահաղորդակցական ցանցի օպերատիվ կառավարման համար կարելի է կիրառել մշակված մեթոդը:Այս համակարգում մեքենայական ուսուցման մասն ունի կարևոր նշանակություն, քանի որ դրա ճշտությունից է կախված ողջ համակարգի աշխատանքի արդյունավետությունը:

Համակարգի ուսուցման համար կարելի է կիրառել երկու եղանակ.

1. ուսուցում ցանցի աշխատանքի ընթացքում,
2. նախնական ուսուցում մոդելավորման համակարգերի կիրառմամբ:

Եթե նախագծվող համաակարգում կիրառվի միայն 1-ին եղանակը, ապա հեռահաղորդակցական ցանցի աշխատանքի ընթացքում անոմալիաների հայտնաբերման գործընթացը բավականին երկար կտևի և կլինի ոչ արդյունավետ: Ուստի պետք է կիրառվի նաև 2-րդ մոտեցումը: Տվյալ դեպքում մասնագիտացված ցանցերի նախագծման գործիքամիջոցներով, ինչպիսին է օրինակ [8]-ը, կառուցվում է հեռահաղորդակցական ցանցի մոդելը, մոդելի վրա կատարվում է տարբեր իրավիճակների սիմուլիացիա և ստացված արդյունքները տրվում են մեքենայական ուսուցման համակարգին որպես մուտք: Դա զգալի արագացնում է ուսուցման ընթացքը և համակարգին թույլ է տալիս արագորեն հայտնաբերել անոմալիաները: Կորպորատիվ հեռահաղորդակցական ցանցի շահագործման ընթացքում կիրառվում է նաև 1-ին մոտեցումը, ինչը մեծացնում է ճշտությունը և թույլ տալիս հայտնաբերել դեպքեր, որոնք չէին ուսուցանվել մոդելավորման համակարգերի միջոցով [6]:

Ելնելով վերը շարադրվածից, կատարվող քայլերի հերթականությունը կարելի է ներկայացնել նկ.21-ով:




Նկ. 21 - Անոմալիաների հայտնաբերման քայլերի հաջորդականություն

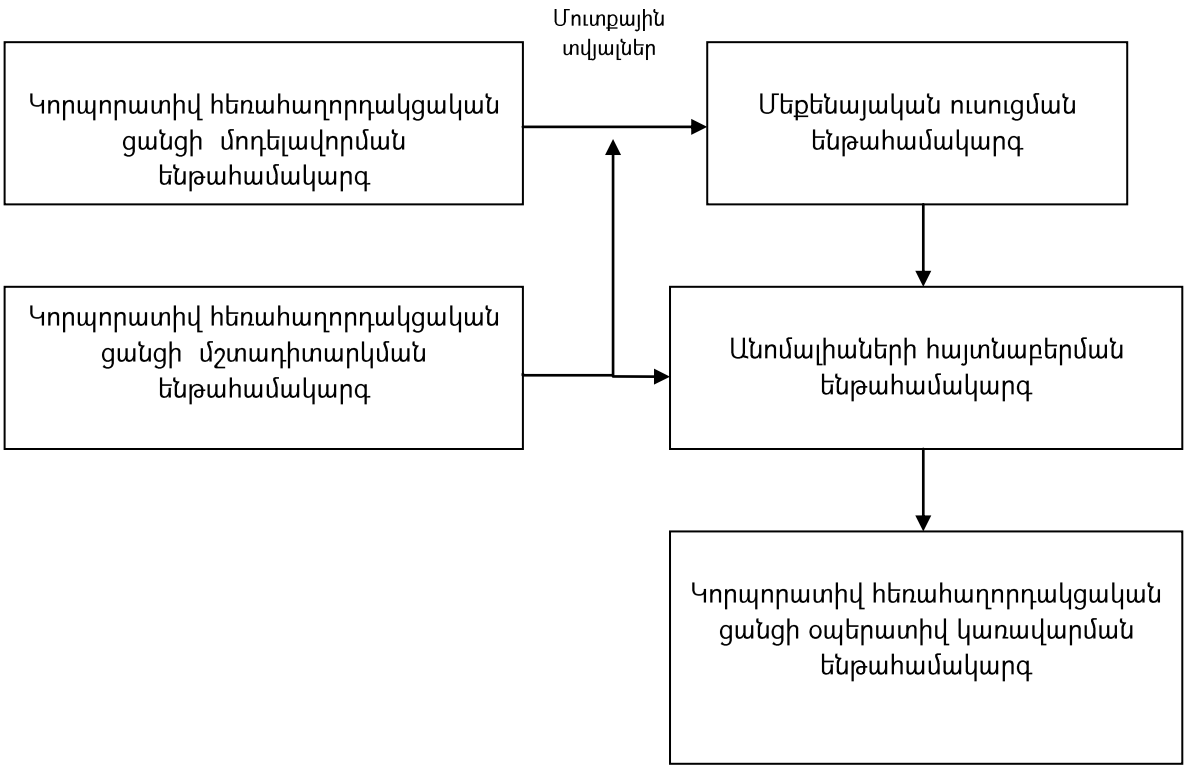
Կորպորատիվ հեռահաղորդակցական ցանցերում մեքենայական ուսուցման միջոցով անոմալիաների հայտնաբերման նախագծվող համակարգի ընդհանրացված ճարտարապետությունը բերված է նկ. 22-ում:

Համակարգը բաղկացած է հետևյալ 5 ենթահամակարգից.

1) Կորպորատիվ հեռահաղորդակցական ցանցի մոդելավորման ենթահամակարգ,
2) Կորպորատիվ հեռահաղորդակցական ցանցի մշտադիտարկման ենթահամակարգ,
3) մեքենայական ուսուցման ենթահամակարգ,
4) անոմալիաների հայտնաբերման ենթահամակարգ,
5) Կորպորատիվ հեռահաղորդակցական ցանցի օպերատիվ կառավարման ենթահամակարգ:

Ենթահամակարգերի գործառույթները հետևյալն են մոդելավորման ենթահամակարգը թույլ է տալիս մասնագիտացված գործիքամիջոցների կիրառմամբ ստեղծել հեռահաղորդակցական ցանցի մոդելը և այդ մոդելի վրա իրականացնել տարբեր իրավիճակների սիմուլյացիա ու արդյունքների հավաքագրում: Ստացված արդյունքների վերլուծության հիման վրա ստացվում են դիտարկվող պարամետրերի մոդելավորվող իրավիճակին համապատասխան արդյունքները:

Մշտադիտարկման ենթահամակարգը նախատեսված է շահագործման հանձնված կորպորատիվ հեռահաղորդակցական ցանցի դիտարկվող պարամետրերի ստացման համար: Այս և մոդալավորման ենթահամակարգերից ստացված արդյունքները փոխանցվում են անոմալիաների հայտնաբերման ենթահամակարգին, որը մշակելով ստացված արդյուքները, ՀՎՄ-ի միջոցով հայտնաբերում է անոմալիաներ և այդ մասին տեղեկացնում օպերատիվ կառավարման ենթահամակարգին: Օպերատիվ կառավարման ենթահամակարգի միջոցով կատարվում են տվյալ իրավիճակին համապատասխանող քայլեր և վերականգնվում է հեռահաղորդակցական ցանցի բնականոն աշխատանքը:




Նկ. 22. Կորպորատիվ հեռահաղորդակցական ցանցերում մեքենայական ուսուցման միջոցով անոմալիաների հայտնաբերման համակարգի ճարտարապետությունը

Արհեստական բանականության վրա հիմնված ինքնուսուցվող համակարգերով կորպորատիվ հեռահաղորդակցական ցանցերում անոմալիաների հայտնաբերման համար անհրաժեշտ է կատարել հետևյալ քայլերը.

- արհեստական բանականության համակարգի ընտրություն,
- ընտրված ինքնուսուցվող համակարգով անոմալիաների հայտնաբերման ավտոմատացված համակարգի մշակում,
- մշակված համակարգով անոմալիաների հայտնաբերման արդյունավետության գնահատում:

## 3.4. Կորպորատիվ հեռահաղորդակցական ցանցերի ինքնուսուցման և անոմալիաների հայտնաբերման կառավարման համակարգի իրականացումը

Ինքնուսուցման համակարգերը բաժանվում են երեք դասի.

1. ուսուցչով ուսուցվող համակարգեր,

2. առանց ուսուցչի ուսուցվող համակարգեր,
3. արտաքին օժանդակությամբ ուսուցվող համակարգեր:

Վերջին տարիներին կատարված բազմաթիվ հետազոտություններ ցույց են տվել, որ անոմալիաների հայտնաբերման համար առավել արդյունավետ են ուսուցիչով ուսուցվող համակարգերը: Կորպորատիվ հեռահաղորդակցական ցանցերում անոմալիաների հայտնաբերման խնդիրը նման համակարգերից առավել արդյունավետ են լուծում արհեստական նեյրոնային ցանցերը և հենասյունային վեկտորային մեթոդը (ՀՎՄ): Բազմաթիվ հետազոտություններ ցույց են տվել, որ ատենախոսությունում դիտարկված խնդրի համար առավել արդյունավետ է ՀՎՄ-ի կիրառումը, քանի որ տալիս է ավելի մեծ ճշտություն:

Ինչպես արդեն նշվել է, հեռահաղորդակցական ցանցերի օպերատիվ կառավարումն արդյունավետ իրականացնելու համար անհրաժեշտ է կատարել հետևյալ հիմնական գործողությունները.

- հեռահաղորդակցական ցանցի մշտադիտարկում,
- հեռահաղորդակցական ցանցում անոմալիաների հայտնաբերում,
- հեռահաղորդակցական ցանցերում հայտնաբերված անոմալիաների մշակում:

Հեռահաղորդակցական ցանցերում անոմալիաների հայտնաբերման համար մեքենայական ուսուցման համակարգերի կիրառման արդյունավետությունն արդեն հիմնավորվել է նախորդ բաժիններում: Մեքենայական ուսուցման կիրառման համար անհրաժեշտ է ստեղծել գիտելիքների որոշակի բազա, որի հիման վրա էլ կկատարվի ուսուցումը: Ուսուցման արդյունավետությունը մեծապես կախված է մուտքային տեղեկատվության քանակից և որակից: Կորպորատիվ հեռահաղորդակցական ցանցերում անոմալիաների հայտնաբերման գործընթացի ուսուցման համար կիրառելի են հետևյալ մոտեցումները.

- ուսուցում ցանցի շահագործման ընթացքում ստացված տվյալների հիման վրա,
- ուսուցում մոդելավորման միջոցներից ստացված տվյալների հիման վրա,
- նախորդ եղանակների համադրում:

Կորպորատիվ հեռահաղորդակցական ցանցի շահագործման ընթացքում ստացված տվյալների հիման վրա ուսուցման գործընթացը կազմակերպելն ունի մեկ թերություն: Քանի որ ուսուցումը պետք է կատարվի ոչ միայն դրա աշխատանքի բնականոն, այլ նաև ոչ բնականոն շահագործման պայմաններում, ուսուցումը կարող է տևել շատ երկար: Բացի այդ, բոլոր հնարավոր տարբերակների ուսուցման համար անհրաժեշտ է կորպորատիվ հեռահաղորդակցական ցանցում ստանալ այդ վիճակները, ինչը բարդ գործընթաց է:

Կորպորատիվ հեռահաղորդակցական ցանցերը, լինելով բարդ հիերարխիկ համակարգեր, պետք է ունենան արդյունավետ կառուցման, զարգացման և կառավարման գործիքամիջոցներ: Կորպորատիվ հեռահաղորդակցական ցանցերն արդյունավետ կառուցելու և շահագործելու համար հարկավոր է, մինչ ցանցը ֆիզիկապես նախագծելը, կիրառել նրա կառուցվածքի մոդելավորումը [63]: Գոյություն ունեն համապատասխան ծրագրային համակարգեր՝ հեռահաղորդակցական ցանցերի, այդ թվում նաև՝ կորպորատիվ հեռահաղորդակցական ն ցանցերի մոդելավորման համար: Այդպիսի ծրագրային համակարգերը ստեղծում են հեռահաղորդակցական ցանցային վիրտուալ մոդելը՝ հիմնվելով նախնական տվյալների, ցանցի տոպոլոգիայի, օգտագործվող արձանագրությունների, ցանցում ներառված հաղորդակցական սարքերի և սարքավորումների վրա [84,91,94,104]:

Կորպորատիվ հեռահաղորդակցական ցանցերի գնահատման համար, մինչ ցանցի ֆիզիկական կառուցվածքը ներկայացնելը, արդյունավետ է օգտվել հայտնի մոդելավորման գործիքամիջոցներից՝ ցանցային սիմուլյատորներից, OpenWNS-ը, OPNET Modeler-ը, NetSim-ը, GNS3-ը, OMNeT++-ը և NS3-ը:

Կորպորատիվ հեռահաղորդակցական ցանցային մոդելավորման գործիքային միջոցների՝ սիմուլյատորների ուսումնասիրությունները, վերլուծությունները և գնահատումները հանգեցնում են նրան, որ մասնագիտացված ցանցերի, այդ թվում նաև կորպորատիվ հեռահաղորդակցական ցանցերի կառուցման գործընթացում նպատակահարմար է կիրառել OMNeT++-ը (Objective Modular Network Testbed in C++) ցանցային մոդելավորման գործիքային միջոցը [52, 61, 79]:

OMNeT++ ծրագրային փաթեթը նախատեսված է տարատեսակ ցանցերի՝ լարային և անլար կառուցվածքների մոդելավորման համար, նրա ճարտարապետությունը կառուցված է մոդուլային սկզբունքով՝ ունի սիմուլյացիայի C++ գրադարան և հարթակ այն բաց տիպի ծրագրային ապահովում է և ընդլայնվելու հնարավորություն ունի: Քանի որ OMNeT++ մոդելավորման գործիքամիջոցն ունի ցանցի էմուլյացիայի ընդլայնումներ և իրական ժամանակի սիմուլյացիայի հնարավորություններ, ուստի այն կարող է օգտագործվել հեռահաղորդակցական ցանցերի մոդելավորման համար [78,81,89,98]: Ցանցային սիմուլյատոր OMNeT++-ը իրականացնում է ընդհանրացված բաղադրիչային կառուցվածք, և ստացված բաղադրիչները կարող են միավորվել ու կառուցել մեկ մեծ բաղադրյալ մոդել:

Այն օգտագործվում է բաղադրիչների միջև հաղորդակցման համար: Ազդանշաններն առաջանում են մոդուլներում և կապուղիներում, այնուհետև հիերարխիայով բարձրանում են վերև: Բնական է, որ մոդուլները, որոնք գրանցվել են որևէ ազդանշան լսելու համար, կտեղեկացվեն դրանց մասին այն դեպքում, երբ այդ ազդանշաններն ուղարկվեն հիերարխիայում իրենցից ներքև գտնվող մոդուլներից: Քանի որ մոդուլները կարող են դիմել ցանկացած այլ մոդուլի, ուստի դրանք կարող են տեղեկացված լինել ցանկացած իրադարձության, որոնք տեղի են ունենում սիմուլյացիայի ընթացքում: Սիմուլյացիայի ընթացքում ազդանշանը կարող է օգտագործվել մի շարք նպատակներով [53,57,60,75]: Դրանցից են .

- Մոդուլների միջև հրապարակել-բաժանորդագրվել տարբեր տեսակի հաղորդակցության համար: Կիրառելի է այն դեպքերում, երբ ազդանշան հրապարակողը և այն սպասողը միմյանցից տեղյակ չեն:
- Երբ մոդուլները պետք է տեղյակ լինեն մոդելի վիճակի փոփոխության մասին: Նման փոփոխություն կարող է լինել մոդուլի ստեղծումը, կապի հաստատումը, փաթեթի կորուստը և այլն:
- Փոփոխականներին՝ որպես սիմուլյացիայի արդյունք գրանցելու համար: Նման փոփոխականներ են, օրինակ, հերթի երկարությունը, հապաղումը և այլն: Սրա իրականացման համար սիմուլյատորի կողմից ստեղծվում են ունկնդիրներ, որոնք էլ իրականացնում են փոփոխականների արժեքների հավաքագրումը:

- Անիմացիայի իրականացում: Անիմացիա իրականացնող մոդուլները պետք է գրաֆիկորեն պատկերեն տեղի ունեցող փոփոխությունները, ուստի դրանք լսում են այն ազդանշանները, որոնց միջոցով ստացված տեղեկատվությունը կարող է ազդեցություն ունենալ գրաֆիկորեն ցուցադրվող պատկերների վրա:

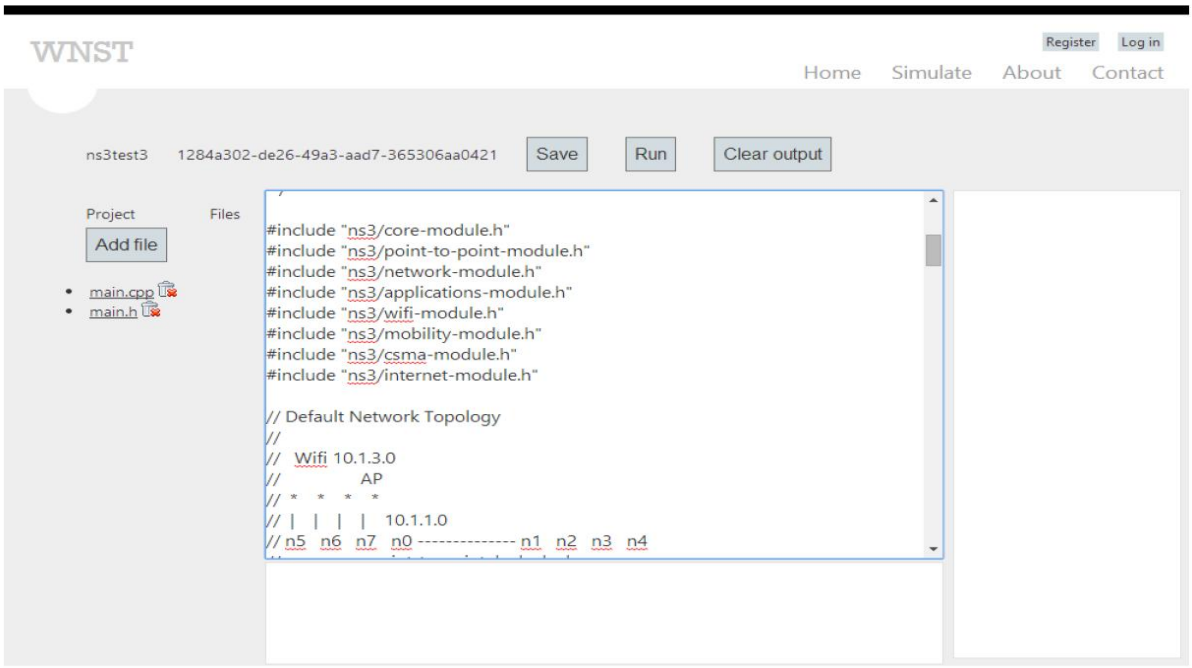
Մոդելավորման միջոցների կիրառումը լուծում է նշված բոլոր խնդիրները: Այսօր գոյություն ունեն կորպորատիվ հեռահաղորդակցական ցանցերի մոդելավորման բազմաթիվ գործիքամիջոցներ, որոնք թույլ են տալիս արդյունավետ կերպով իրականացնել ցանկացած բարդությամբ ցանցի աշխատանքի մոդելավորում ամենատարբեր պայմանների և մուտքային տվյալների համար [98, 102, 103]: Մոդելավորման նման տարածված գործիքամիջոցներ են OMNeT++ և ns3 սիմուլյացիոն գործիքամիջոցները:

Միայն մոդելավորման գործիքամիջոցների կիրառման դեպքում կարող է առաջանալ մեկ խնդիր: Կազմակերպություններում աշխատանքի բնույթի կամ աշխատողների քանակի փոփոխման դեպքում հեռահաղորդակցական ցանցի բնութագրերը փոխվում են, ինչը բնականոն աշխատանքային վիճակ է հեռահաղորդակցական ցանցի համար, սակայն նախորդ բաժիններում դիտարկված անոմալիաների հայտնաբերման համար դրանք նորմալ պարամետրեր չեն:

Հաշվի առնելով այս հանգամանքը առավել արդյունավետ է կիրառել դիտարկված երկու տարբերակների համադրումը: Կորպորատիվ հեռահաղորդակցական ցանցերի մոդելավորման գործիքամիջոցներով պետք է կատարվի նախնական ուսուցում, իսկ ցանցի շահագործուման ընթացքում հավաքված տվյալները պետք է նորից փոխանցվեն ուսուցման համակարգին, որպեսզի գիտելիքների բազան միշտ պարունակի վերիջին տվյալները:

WNST ավտոմատացված համակարգի վեբ ինտերֆեյսը բերված է նկար 23-ում: WNST-ն նախագծված է կլիենտ-սերվեր ճարտարպետությամբ: Ունի տվյալների բազա, որտեղ պահվում են ցանցերի տարբեր կառուցվածքների մոդելավորման ընթացքում ստացված տվյալները [7]: WNST ավտոմատացված համակարգը բաց է, ինչը թույլ է

տալիս այն հեշտությամբ ինտեգրել տարբեր այլ համակարգերին, օրինակ, CTNOCAS- ին:



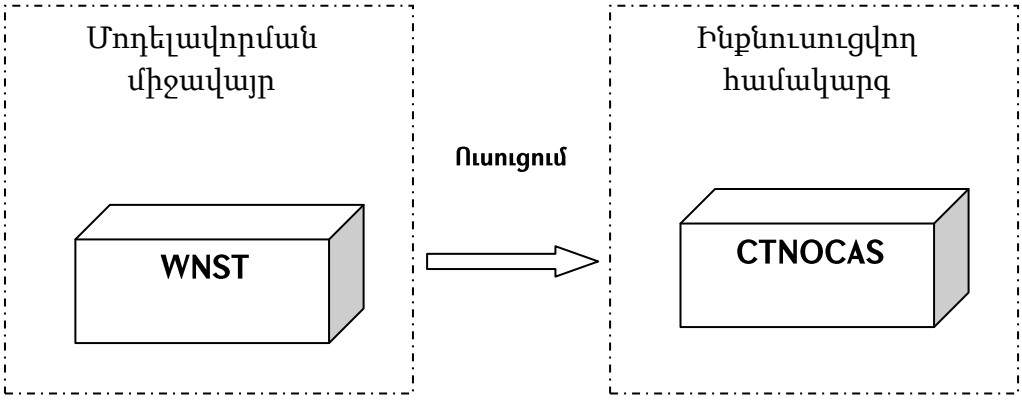

Նկ. 23 - WNST ավտոմատացված համակարգի վեբ ինտերֆեյսը

WNST ավտոմատացված համակարգն բաղկացած է երկու մակարդակից՝ օգտագործողի մակարդակ և սերվերային մակարդակ [7]:

Օգտագործողի մակարդակում կիրառվում է վեբ-ստանդարտների հիման վրա մշակված ծրագիրը, որը հնարավոր է օգտագործել պլանշետների, սմարթֆոնների, նոութբուքերի և այլ սարքավորումների վրա: Ծրագիրը թույլ է տալիս օգտագործողին ստեղծել սիմուլյացիա, տալ անհրաժեշտ կարգավորումները և հրամանները: Համացանցի միջոցով այն կապ է հաստատում սերվերային մակարդակի հետ:

Սերվերային մակարդակն ամպային տեխնոլոգիաների վրա հիմված համակարգ է: Այն ապահովում է օգտագործողի և սիմուլյատորի միջև երկխոսությունը: Սերվերային մակարդակը բաղկացած է մի քանի հիմնական մասերից, որոնք ապահովում են առանձին հանգույցների՝ տվյալների պահոցի, սիմուլյացիոն մոդուլի, ցանցի կառուցվածքի բարելավման մոդուլի և այլ մասերի զուգահեռ աշխատանքը [7]:

CTNOCAS-ի և WNST-ի միջոցով հեռահաղորդակցական ցանցերի տարբեր ռեժիմներում աշխատանքի ուսուցման կառուցվածքը բերված է նկարում:




Նկ. 24 - CTNOCAS-ի և WNST-ի միջոցով հեռահաղորդակցական ցանցերի տարբեր ռեժիմներում աշխատանքի ուսուցման կառուցվածքը

Ատենախոսության շրջանակներում մշակվել է կորպորատիվ հեռահաղորդակցական ցանցերի օպերատիվ կառավարան երկխոսային CTNOCAS (**C**orporative **T**elecommunication **N**etworks **O**perative **C**ontrol **A**utomated **S**ystem) ավտոմատացված համակարգը: CTNOCAS ավտոմատացված համակարգն աշխատում է ցանցերի նախագծման WNST ավտոմատացված համակարգի հետ: WNST ավտոմատացված համակարգ է, որը թույլ է տալիս արդյունավետ կերպով նախագծել կորպորատիվ հեռահաղորդակցական ցանցեր և կիրառելով ցանցերի մոդելավորման տարբեր գործիքամիջոցներ ստուգել նախագծվող ցանցի աշխատանքը շահագործման տարբեր պայմաններում: WNST-ն կիրառվում է CTNOCAS-ի ուսուցման ենթահամակարգում: Այն թույլ է տալիս վեբ ինտերֆեյսի միջոցով նախագծել հեռահաղորդակցական ցանցը և մոդելավորել վերջինիս աշխատանքը ոչ միայն շահագործման բնականոն պայմաններում, այլ նաև կատարել աշխատանքի մոդելավորում այնպիսի իրավիճակներում, ինչպիսին DDoS հարձակումներն են, հեռահաղորդակցական ցանցի սարքավորումների խափանումները, ծանրաբեռնվածության ավելացումը և այլն:

## Գլուխ 3-ի վերաբերյալ եզրակացություններ

Տվյալ գլխում կատարված մշակումների և ստացված արդյունքների հիման վրա կարելի է ներկայացնել.

1. Կորպորատիվ հեռաղորդակցական ցանցերի օպերատիվ կառավարման համար առաջարկվում է կիրառել մոտեցում, որի դեպքում հնարավոր կլինի դասակարգել կառավարման և շահագործման խնդիրները, հիշել դրանց լուծումները և անհրաժեշտության դեպքում կիրառել արդեն հայտնի լուծումները:
2. Կորպորատիվ հեռաղորդակցական ցանցերի օպերատիվ կառավարման համար ավելի նպատակահարմար է գնահատել խնդիրների լուծումները, որի դեպքում յուրաքանչյուր խնդրի լուծմանը տալով որոշակի գործակից, ավելացնել կամ նվազեցնել գործակցի արժեքը՝ հաշվի առնելով՝ թե նախորդ լուծումները արդյոք ադմինիստրատորի կողմից նախորդ լուծումների կիրառումը:
3. Կորպորատիվ հեռաղորդակցական ցանցերի օպերատիվ կառավարման ժամանակ խնդիրների լուծման արդյունավետությունը բարձրացնելու համար առաջարկում ենք եղանակ, որի կիրառման դեպքում յուրաքանչյուր խնդրի համար որոնվում են հնարավոր լուծումներ, և դրանք գտնելում դեպքում առաջարկվում են ադմինիստրատորին, եթե ոչ՝ ադմինիստրատորի կողմից առաջարկվում է նոր լուծում, որը հետագայում կառաջարկվի նմանատիպ խնդիրների լուծման համար:
4. Նախագծվել է կորպորատիվ հեռաղորդակցական ցանցերում մեքենայական ուսուցման միջոցով անոմալիաների հայտնաբերման համակարգի ճարտարապետությունը:
5. Մշակվել է կորպորատիվ հեռահաղորդակցական ցանցերի օպերատիվ կառավարան երկխոսային CTNOCAS (**T**elecommunication **N**etworks **O**perative **C**ontrol **A**utomated **S**ystem) ավտոմատացված համակարգը, որն աշխատում է ցանցերի նախագծման WNST ավտոմատացված համակարգի հետ:

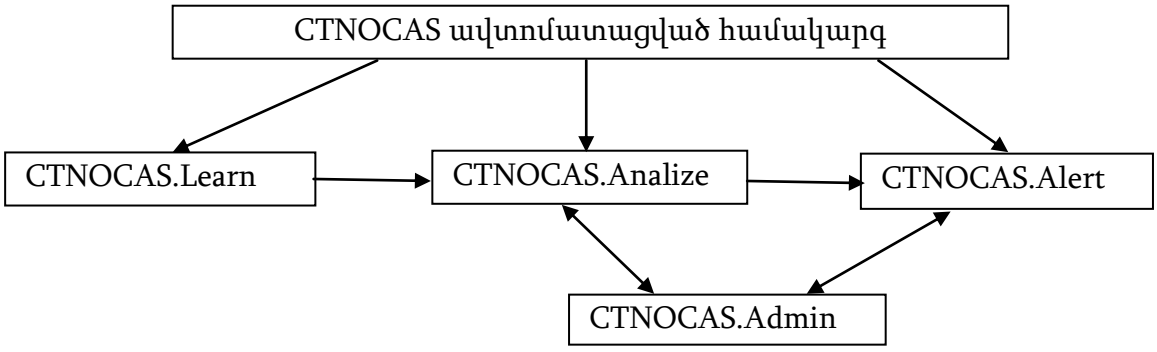
# ԳԼՈՒԽ 4. ԿՈՐՊՈՐԱՏԻՎ ՀԵՌԱՀԱՂՈՐԴԱԿՑԱԿԱՆ ՑԱՆՑԵՐԻ ՕՊԵՐԱՏԻՎ ԿԱՌԱՎԱՐՄԱՆ ՀԱՄԱՐ ՄՇԱԿՎԱԾ ԱՎՏՈՄԱՏԱՑՎԱԾ ՀԱՄԱԿԱՐԳԻ ՀՆԱՐԱՎՈՐՈՒԹՅՈՒՆՆԵՐԻ ՀԵՏԱԶՈՏՈՒՄԸ ԵՎ ԿԻՐԱՌՈՒՄԸ

Ատենախոսության նախորդ գլուխներում դիտարկվել են կորպորատիվ հեռահաղորդակցական ցանցերի օպերատիվ կառավարման առանձնահատկությունները և դրա իրականացման հնարավոր եղանակները: Կատարված հետազոտությունների հիման վրա մշակվել է CTNOCAS ավտոմատացված համակարգը, որի միջոցով կատարվում է հեռահաղորդակցական ցանցերի օպերատիվ կառավարումը: CTNOCAS ավտոմատացված համակարգի մշակման փուլում դրվել են մի շարք պահանջներ, որոնց համակարգը պետք է բավարարի: Դրանք են.

- ունենալ բաց ճարտարապետություն,
- մշակված լինի բաց կոդով,
- հնարավոր լինի կիրառել տարբեր օպերացիոն համակարգերի վրա,
- ունենա պարզ կիրառական ինտերֆեյս:

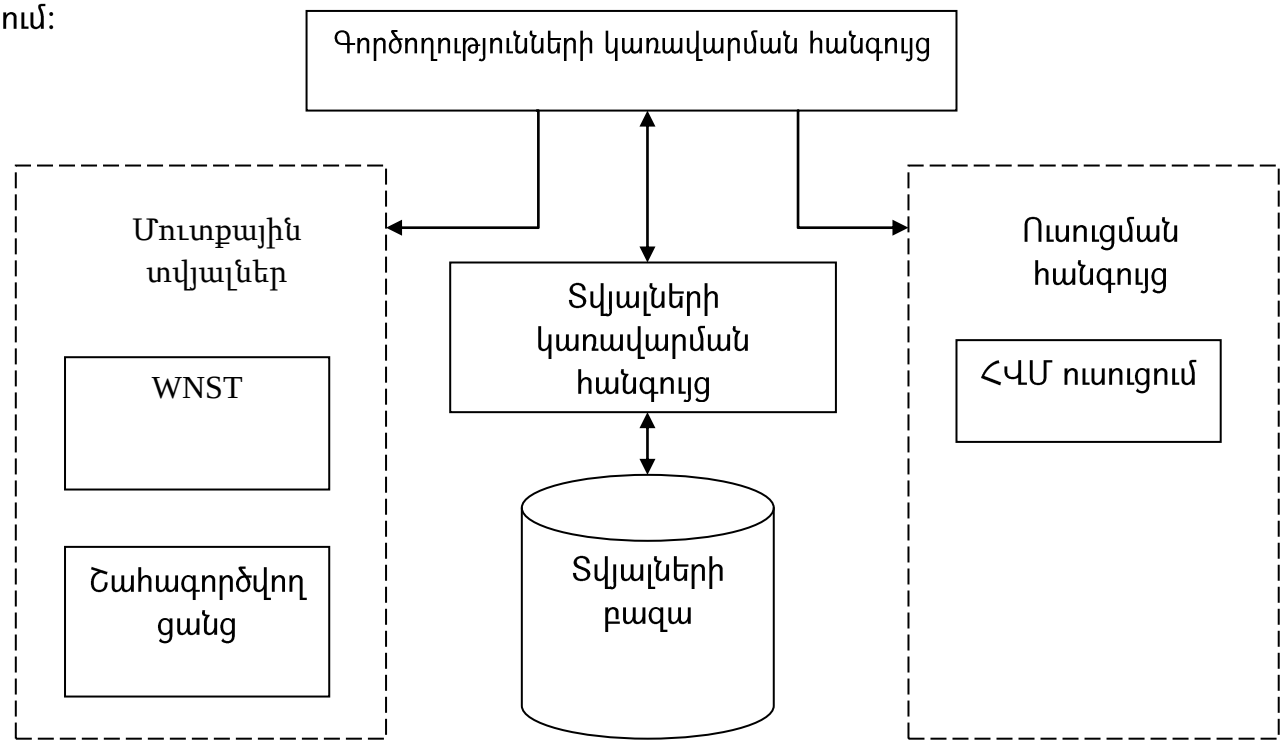
## 4.1. Կորպորատիվ հեռահաղորդակցական ցանցերի օպերատիվ կառավարման համար մշակված CTNOCAS համակարգի նկարագրումը

Կորպորատիվ հեռահաղորդակցական ցանցերի օպերատիվ կառավարման CTNOCAS ավտոմատացված համակարգը բաղկացած է հետևյալ ենթահամակարգերից նկ.25. CTNOCAS.Learn, CTNOCAS.Analize, CTNOCAS.Alert, CTNOCAS.Admin:




Նկ. 25- CTNOCAS ավտոմատացված համակարգը

CTNOCAS.Learn ենթահամակարգը պատասխանատու է մուտքային տարբեր աղբյուրներից ստացված տվյալների հիմնա վրա ուսուցման գործընթացը կազմակերպելու համար: Ուսուցման գործընթացը բացված տեսքով բերված է նկ. 26-ում:



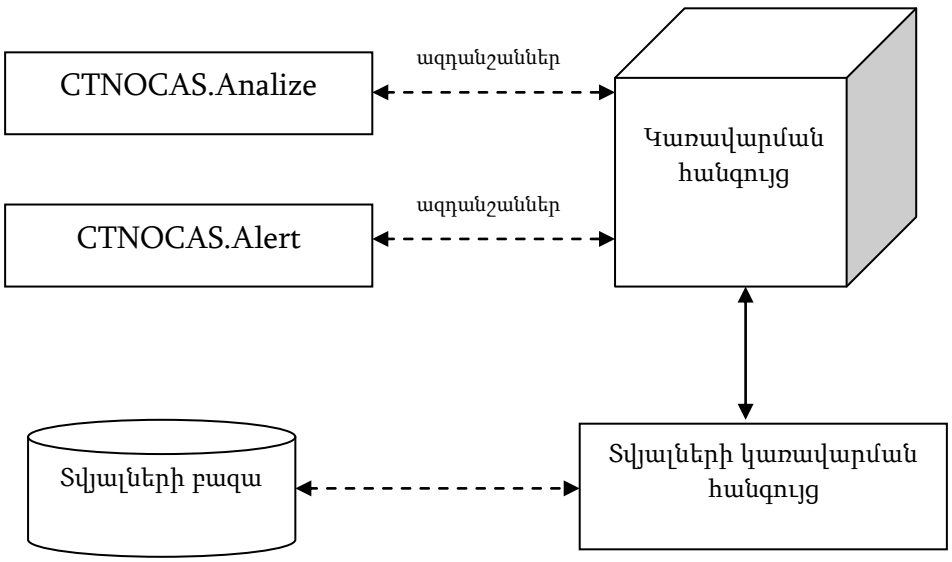

Նկ. 26 - CTNOCAS.Learn ուսուցման գործընթացը

CTNOCAS ավտոմատացված համակարգում ուսցումը կատարվում է գործողությունների կառավարման հանգույցի կողմից եկող ազդանշանների հիման վրա: Տվյալ հանգույցը մշտական կապի մեջ է մոդելավորման գործիքների և շահագործվող ցանցում ներդրված մշտադիտարկման համակարգերի հետ: Ստանալով նոր տվյալներ՝ գործողությունների կառավարման հանգույցը դրանք գրանցում է տվյալների բազայում: Բազայում տվյալների գրանցումը և ընթերցումը կատարվում է Տվյալների կառավարման հանգույցի միջոցով: Գործողությունների կառավարման հանգույցի տվյալների բազային անմիջական հասանելիություն չունենալը որոշակի ճկունություն է հաղորդում CTNOCAS ավտոմատացված համակարգին: Շնորհիվ այն բանի, որ տվյալների հետ աշխտանքը կատարվում է առանձին ենթահանգույցի միջոցով, հնարավոր է դառնում հեշտությամբ փոփոխել տվյաների բազան կամ դրա կառուցվածքը՝ չազդելով ընդհանուր համակարգի աշխատանքի վրա: Տվյալների

բազայում տեխնոլոգիական կամ կառուցվածքային փոփոխությունների դեպքում փոխվում է միայն Տվյալների կառավարման հանգույցը, սակայն Գործողությունների կառավարման հանգույցի հետ աշխատանքի ինտերֆեյսը փոփոխության չի ենթարկվում: Համակարգի նման ճարտարապետությունը թույլ է տալիս որպես տվյալների պահպանման միջավայր օգտագործել այնպիսի ծրագրային համակարգեր, ինչպիսիք են. MSSQL, MySQL, MogoDB, Postgre SQL և այլ [96-97]:

CTNOCAS.Analize ենթահամակարգը պատասխանատու է ուսուցման համակարգից եկած տվյալների վերլուծություն կատարելու և անոմալիաների հայնտաբերման դեպքում CTNOCAS.Alert ենթահամակարգի միջոցով այդ մասին ադմինիստրատորին տեղեկացնելու համար: CTNOCAS.Alert ենթահամակարգը ադմինիստրատորին կարող է ազդանշաններ ուղարկել տեքստային հաղորդագրությունների, էլ փոստի կամ հեռախոսազանգի միջոցով:

CTNOCAS.Admin ենթահամակարգը նախատեսված է Կորպորատիվ հեռահաղորդակցական ցանցը սպասարկող ադմինիստրատորների կողմից համակարգի կառավարման և դրանով եկող ազդանշանների մշակման համար: Հենց այս ենթահամակարգի միջոցով է կատարվում ցանցի օպերատիվ կառավարումը: CTNOCAS.Admin ենթահամակարգի կառուցվածքը բերված է նկար 27-ում:




Նկ. 27 - CTNOCAS.Admin ենթահամակարգի կառուցվածքը

CTNOCAS.Admin ենթահամակարգը մշտական կապի մեջ է գտնվում CTNOCAS.Analize և CTNOCAS.Alert ենթահամակարգերի հետ, որոնց հետ անընդհատ կատարում է կառավարման ազդանշանների փոխանակում: Տվյալների կառավարման հանգույցը պատասխանատու է բազայում տվյալների գրանցման և անհրաժեշտության դեպքում հարցումների միջոցով դրանց ընթերցման ու Կառավարման հանգույցին փոխանցելու համար: Ինչպես CTNOCAS.Learn-ի դեպքում, այստեղ ևս տվյալների կառավարման առանձին ենթահամակարգը թույլ է տալիս տվյալները պահպանել ցանկացած հարմար միջավայրում և անհրաժեշտության դեպքում հեշտությամբ փոխարինել այն մեկ այլ միջավայրով:

Տվյալների բազայում են պահվում տարբեր խնդիրների համար ադմինիստրատորի կողմից կիրառված լուծումները և դրանցից յուրաքանչյուրի արդյունավետության կշիռը, որը փոփոխության է ենթարկվում նմանատիպ խնդիրների ի հայտ գալու դեպքում, ինչպես դա ներկայացված է գլուխ 3.2-ում:

Հեռահաղորդակցական ցանցի օպերատիվ կառավարումն իրականացնող ադմինիստրատորի և CTNOCAS.Admin ենթահամակարգի աշխատանքը կազմակերպված է վեբ ինտերֆեյսի միջոցով, ինչը թույլ է տալիս համակարգը կիրառել համացանցին հասանելիություն ունեցող ցանկացած սարքավորումից, օրինակ անհատական օգտագործման հանակարգիչները, նոութբուքերը, պլանշետները և սմարթֆոնները:

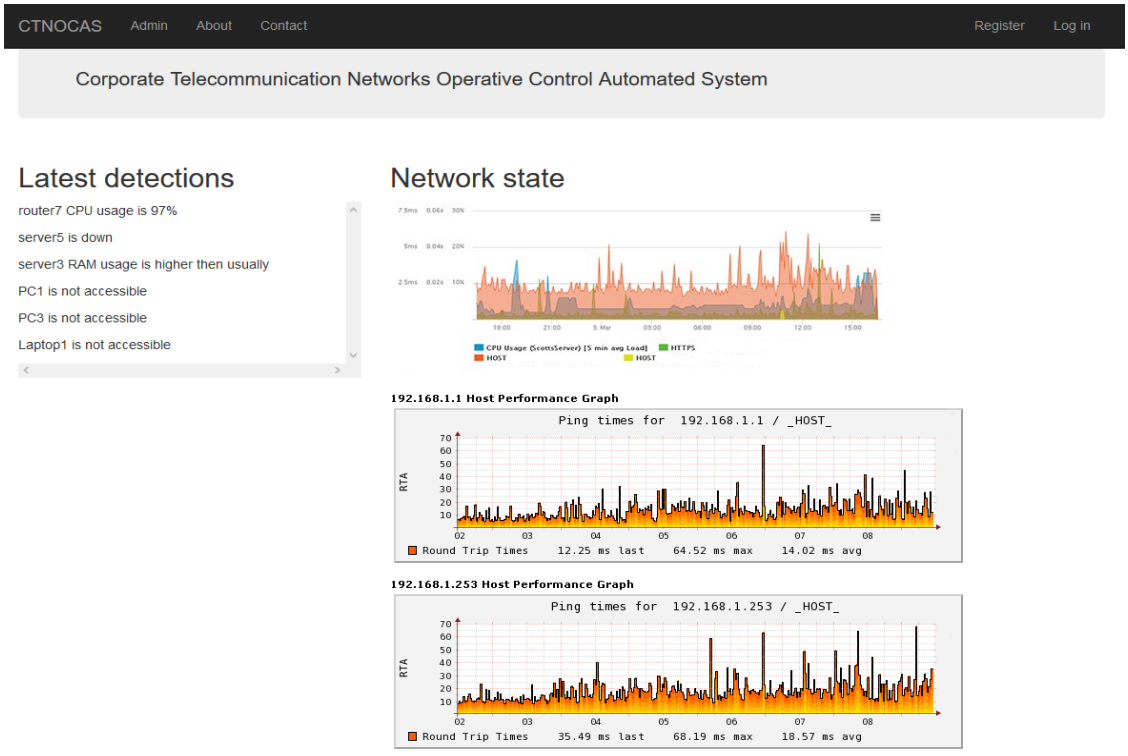
### 4.2. CTNOCAS ավտոմատացված համակարգի իրականացումը

CTNOCAS ավտոմատացված համակարգն ամբողջությամբ բավարում է վերը նշված բոլոր պահանջները: Այն ունի բաց ճարտարապետություն, ինչի շնորհիվ թույլ է տալիս որը թույլ է տալիս ավելացնել ոչ միայն համատեղելի սիմուլյատորների քանակը, այլ նաև փոխարինել արդեն գոյություն ունեցող սիմուլյատորները CTNOCAS-ի հետ համատեղելի այլ սիմուլյատորներով:

CTNOCAS ավտոմատացված համակարգն ունի կլիենտ-սերվեր ճարտարապետություն: Կլիենտ մասն իրականացված է վեբ համակարգի տեսքով: CTNOCAS-ի մշակման ընթացքում կիրառվել է Microsoft ընկերության .NET

Core տեխնոլոգիան, իսկ վեբ համակարգի համար՝ ASP.Net Core տեխնոլոգիան: Տվյալների պահոցն իրականացվել է MSSQL Server տեխնոլոգիայով: Նշված բոլոր համակարգերը կիրառելի են ինչպես Microsoft Windows օպերացիոն համակարգի համար, այնպես էլ Linux ընտանիքի Red Hat Enterprise և Ubuntu օպերացիոն համակարգերի համար: Դա թույլ է տալիս համակարգը կիրառել Windows և Linux օպերացիոն համակարգերի վրա [1,50]:

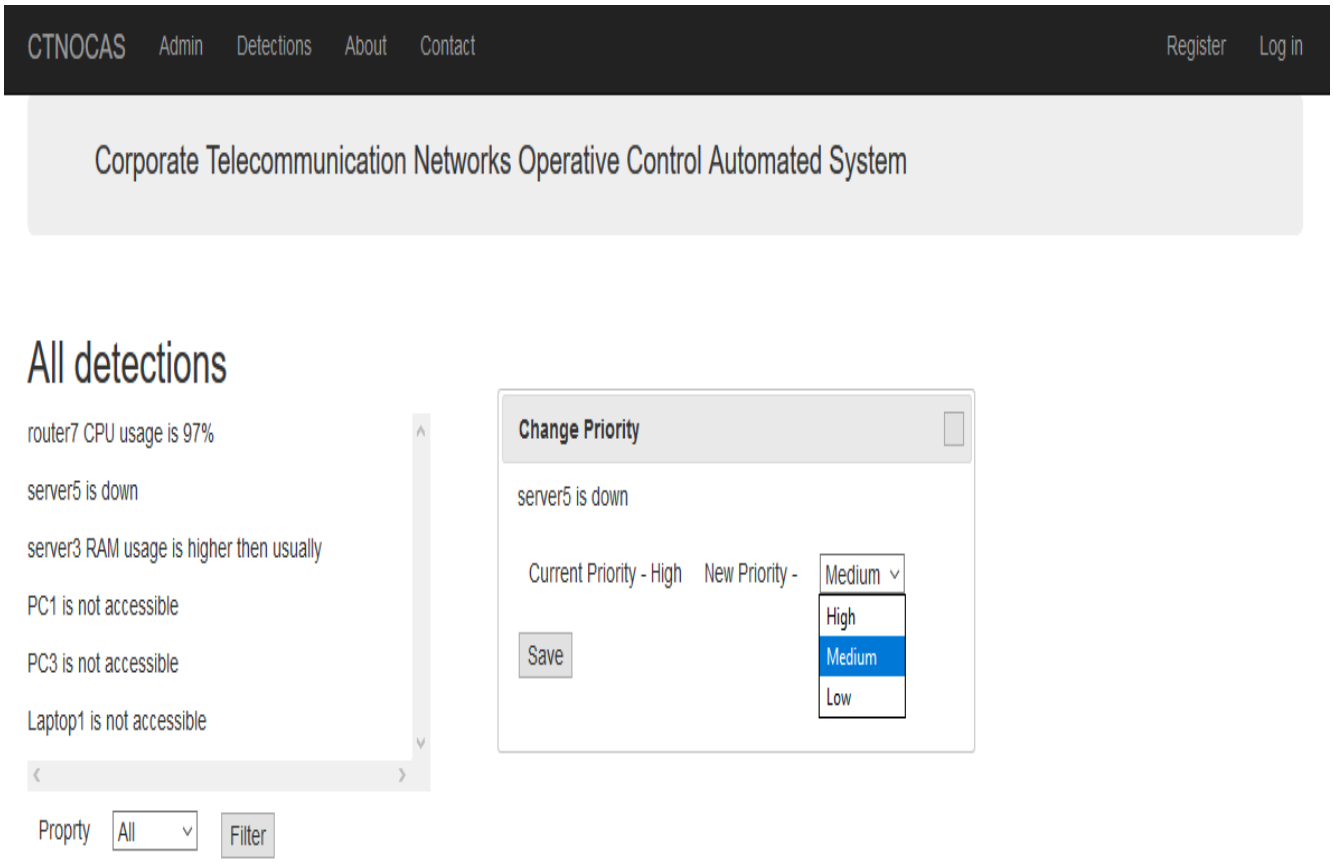
Ինչպես արդեն նշվել է, CTNOCAS ավտոմատացված ենթահամակարգի կլիենտ մասն իրականացվել է ASP.Net Core տեխնոլոգիայով [54, 70-72]: Դա թույլ է տվել համակարգը կիրառել ցանկացած սարքավորման վրա, որը թույլ է տալիս դիտարկիչի միջոցով աշխատել վեբ կայքերի հետ: ASP.Net Core տեխնոլոգիայի Linux ընտանիքի օպերացիոն համակարգերի հետ համատեղելի լինելու շնորհիվ CTNOCAS համակարգը կարելի է տեղադրել Linux սերվերների վրա և ինտեգրել հեռահաղորդակցական ցանցերում ներդրված մշտադիտարկման համակարգերի հետ: Նկար 28-ում բերված է CTNOCAS.Admin ենթահամակարգի գրաֆիկական տեսքը:



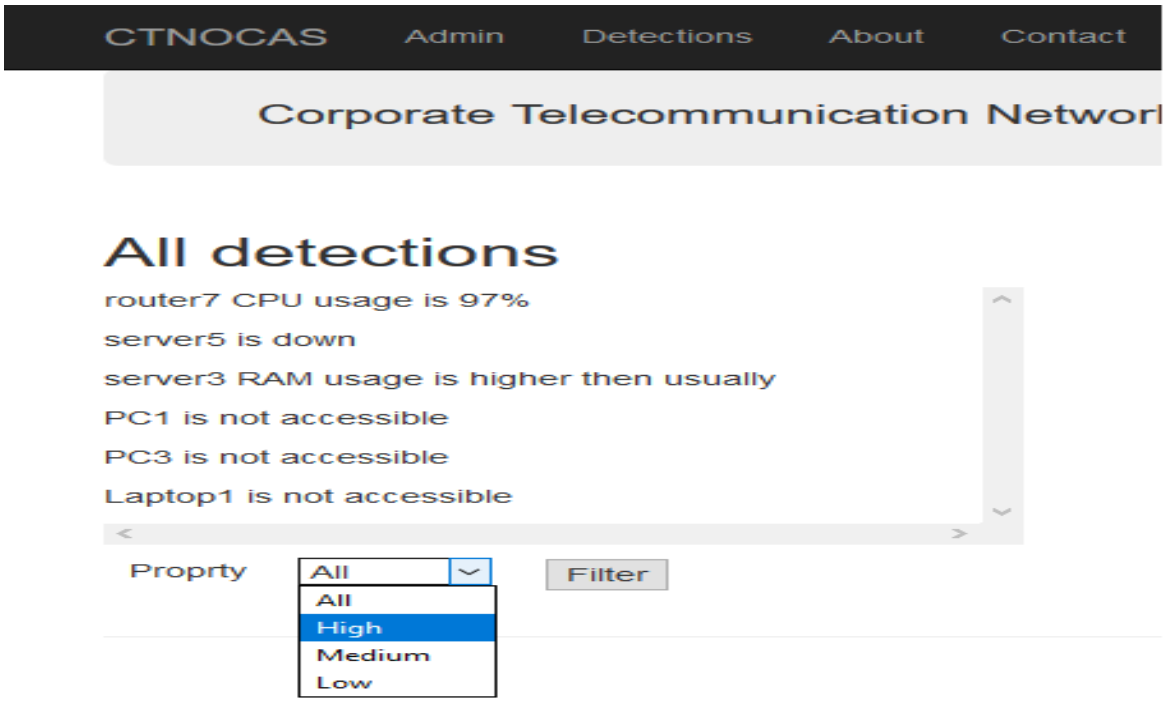

Նկ. 28. CTNOCAS.Admin ենթահամակարգի գրաֆիկական տեսքը

Գրաֆիկական մասում ներկայացվում է հեռահաղորդակցական ցանցի ընթացիկ վիճակը և վերջերս գտնված անոմալիաների ցուցակը: Ադմինիստրատորը կարող է ընտրել դրանցից յուրաքանչյուրը և տեսնել, թե ինչ գործողություններ են կատարվել տվյալ խնդրի լուծման համար: Առանձին դաշտով ներկայացվում են այն խնդիրները, որոնք դեռևս չեն մշակվել ադմինիստրատորի կողմից: Նոր խնդրի ի հայտ գալու դեպքում այն ավելացվում է ցուցակի վերին մասում: Յուրաքանչյուր խնդրի համար տրվում է դրա հայտնաբերման ժամանակը: Ընտրելով համապատասխան խնդիրը ադմինիստրատորը սկսում է դրա մշակումը: Յուրաքանչյուր խնդիր կարող է ունենալ կարևորության 3 աստիճան՝ բարձր, միջին և ցածր:

Բոլոր նոր առաջացած խնդիրների համար տրվում է կարևորության բարձր աստիճան: Ադմինիստրատորի կողմից հնարավոր է կատարել կարևորության աստիճանի փոփոխում (նկ.29): Գրաֆիկական մասում հնարավոր է խնդիրները ֆիլտրել ըստ կարևորության աստիճանի (նկ.30):

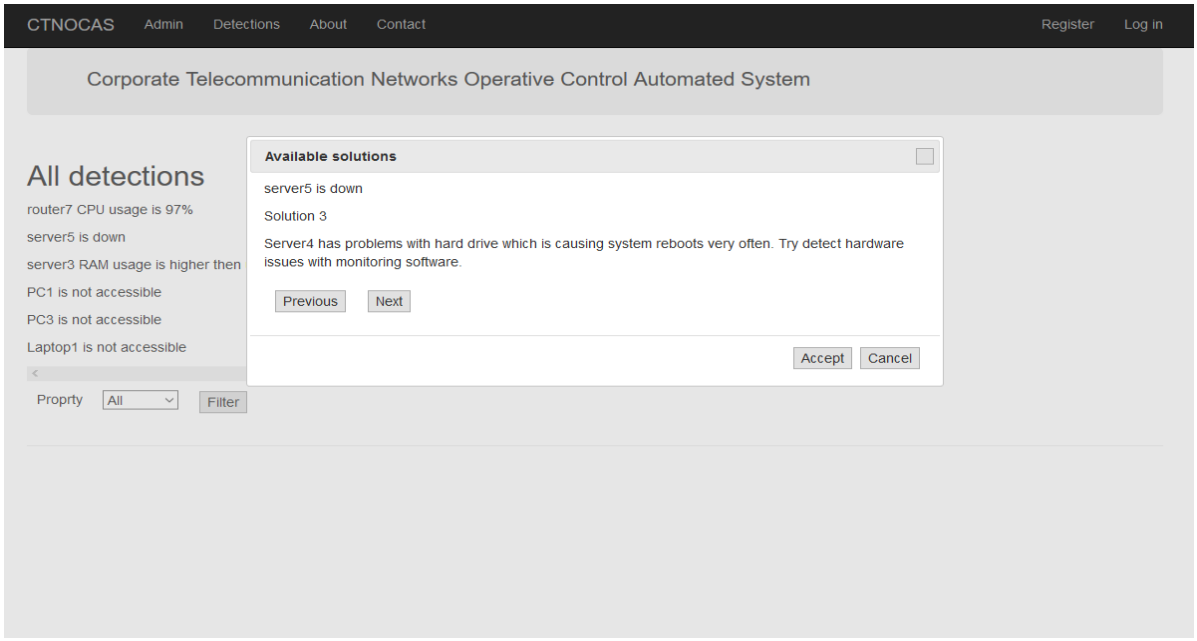



Նկ.29- CTNOCAS.Admin ենթահամակարգում խնդիրների կարևորության աստիճանի փոփոխումը



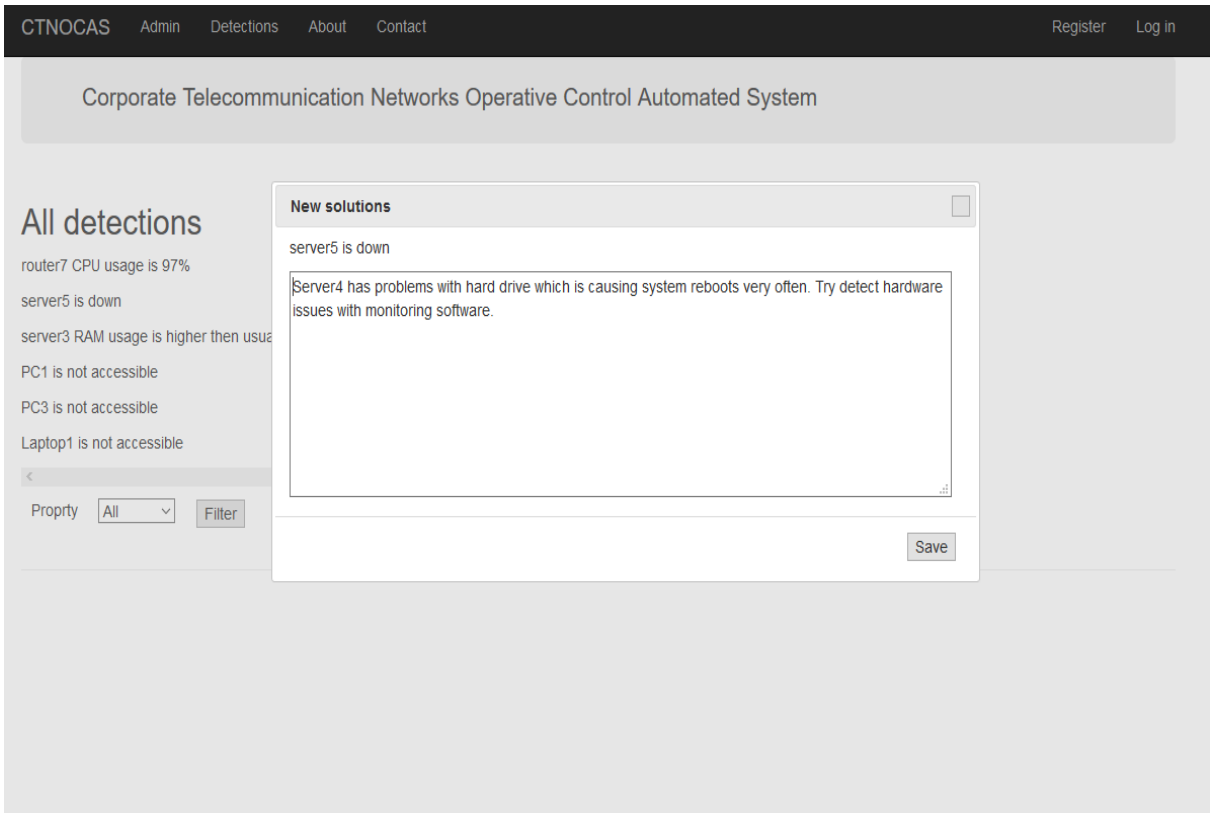

Նկ.30. CTNOCAS.Admin ենթահամակարգում խնդիրների ֆիլտրումն ըստ կարևորության

Համակարգում խնդիրների մշակման պատուհանն ունի նկ.31-ում բերված տեսքը: Խնդիրն ընտրելուց հետո համակարգը, հնարավորության դեպքում, առաջարկում է այն լուծումների բազմությունը, որոնք նախկինում կիրառված են եղել տվյալ դասի խնդիրների լուծման համար:




Նկ.31. CTNOCAS.Admin ենթահամակարգում խնդիրների մշակման գրաֆիկական տեսքը

Եթե եղած լուծումներն ադմինիստրատորին չեն բավարարում, կամ տվյալ դասի խնդրի համար դեռևս չկա լուծում, հնարավորություն կա ադմինիստրատորի կողմից մուտքագրել լուծում (նկ.32): Հետագայում այն կառաջարկվի նման դասի խնդիրների լուծման համար:




Նկ.32. CTNOCAS.Admin ենթահամակարգում խնդիրների նոր լուծման գրանցումը

## 4.3. CTNOCAS ավտոմատացված համակարգի գործնական արդյունքները և վերլուծությունը

Կորպորատիվ հեռահաղորդակցական ցանցերի օպերատիվ կառավարման CTNOCAS ավտոմատացված համակարգը ներդրվել է հայկական «Օնլայնաճուրդ» ՍՊԸ-ում և ռուսական OMC կազմակերպությունում: «Օնլայնաճուրդ» ՍՊԸ-ն մատուցում է աճուրդի կազմակերպման ծառայություն՝ բացառապես օնլայն հարթակում: OMC-ն բազմաբնույթ ծառայություններ է մատուցում այլ կազմակերպություններին, մասնավորապես իրականացնում է շինությունների ենթակառուցվածքների սպասարկում, ինժեներական սարքավորումների սպասարկում, անվտանգության և այլ ծառայություններ:

«Օնլայնաճուրդ» ՍՊԸ-ի կողմից CTNOCAS ավտոմատացված համակարգն օգտագործվում է հեռահաղորդակցական ցանցում խնդիրների հայտնաբերման և ցանցի օպերատիվ կառավարման նպատակով: Հաշվի առնելով այն հանգամանքը, որ կազմակերպությունը զբաղվում է առցանց աճուրդներով, կարևոր է, որ հեռահաղորդակցական ցանցը մշտապես գտնվի աշխատունակ վիճակում, իսկ խնդիրների ի հայտ գալու դեպքում դրանք շտկվեն նվազագույն ժամանակահատվածում:

Այդ պատճառով CTNOCAS ավտոմատացված համակարգի միջոցով ստեղծվել է «Օնլայնաճուրդ» ՍՊԸ-ի հեռահաղորդակցական ցանցի մոդելը և այդ մոդելի վրա կատարվել է տարբեր տիպի անսարքությունների մոդելավորում:

«Օնլայնաճուրդ» ՍՊԸ-ի հեռահաղորդակցական ցանցի համար որոշվել են ցանցի ծանրաբեռնվածության արժեքները աշխատանքի բնականոն և ծանրաբեռնված ռեժիմների համար ըստ օրվա ժամերի: Չափումները բերված են աղյուսակ 6-ում:

Աշխատանքային օրերին ցանցը առավելապես ծանրաբեռնված է լինում առավոտյան և երեկոյան ժամերին, ինչը կարելի է տեսնել նկար 33-ում:

Ոչ աշխատանքային օրերին ցանցը առավել ծանրաբեռնված է ցերեկային և երեկոյան ժամերին, ինչպես ցույց է տրված նկ. 34-ում:

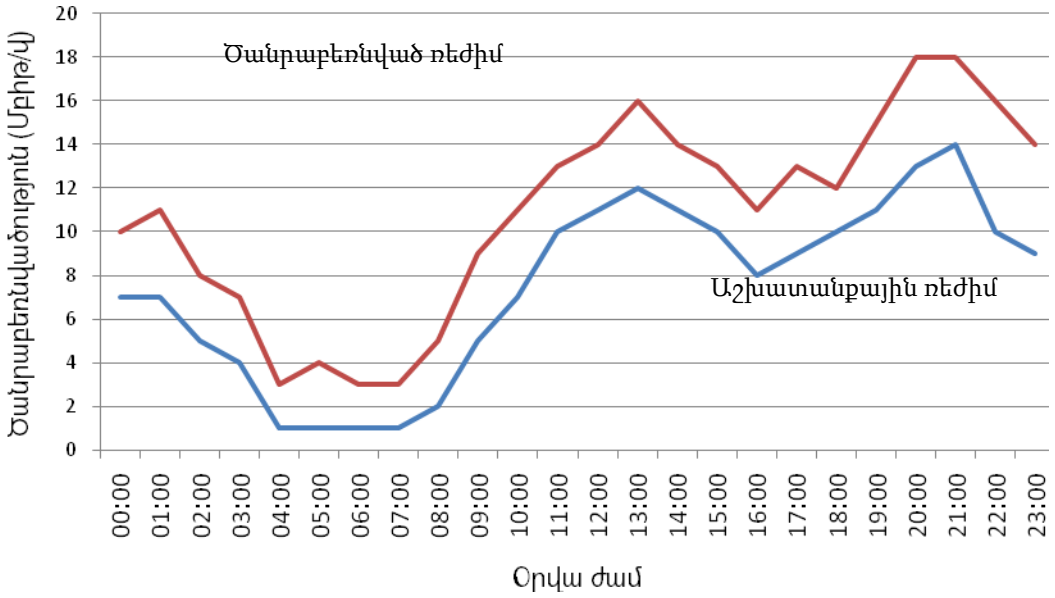
Աղյուսակ 6

«Օնլայնաճուրդ» ՍՊԸ-ի հեռահաղորդակցական ցանցի ծանրաբեռնավածությունն ըստ օրվա ժամերի

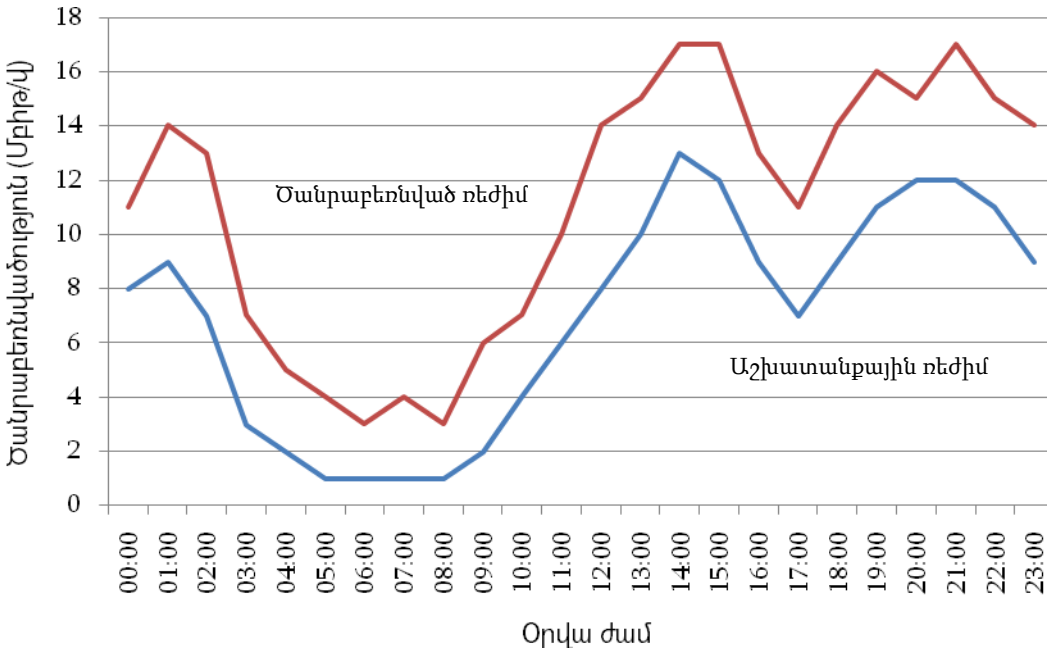
| **Ժամ** | **Աշխատանքային օր (Մբիթ/վ)** | | **Ոչ աշխատանքային օր (Մբիթ/վ)** | |
|---|---|---|---|---|
| | **Չծանրաբեռնված** | **Ծանրաբեռնված** | **Չծանրաբեռբված** | **Ծանրաբեռնված** |
| **1** | **2** | **3** | **4** | **5** |
| 00:00 | 7 | 10 | 8 | 11 |
| 01:00 | 7 | 11 | 9 | 14 |
| 02:00 | 5 | 8 | 7 | 13 |
| 03:00 | 4 | 7 | 3 | 7 |
| 04:00 | 1 | 3 | 2 | 5 |

Աղյուսակ 6-ի շարունակություն

| 1 | 2 | 3 | 4 | 5 |
|---|---|---|---|---|
| 05:00 | 1 | 4 | 1 | 4 |
| 06:00 | 1 | 3 | 1 | 3 |
| 07:00 | 1 | 3 | 1 | 4 |
| 08:00 | 2 | 5 | 1 | 3 |
| 09:00 | 5 | 9 | 2 | 6 |
| 10:00 | 7 | 11 | 4 | 7 |
| 11:00 | 10 | 13 | 6 | 10 |
| 12:00 | 11 | 14 | 8 | 14 |
| 13:00 | 12 | 16 | 10 | 15 |
| 14:00 | 11 | 14 | 13 | 17 |
| 15:00 | 10 | 13 | 12 | 17 |
| 16:00 | 8 | 11 | 9 | 13 |
| 17:00 | 9 | 13 | 7 | 11 |
| 18:00 | 10 | 12 | 9 | 14 |
| 19:00 | 11 | 15 | 11 | 16 |
| 20:00 | 13 | 18 | 12 | 15 |
| 21:00 | 14 | 18 | 12 | 17 |
| 22:00 | 10 | 16 | 11 | 15 |
| 23:00 | 9 | 14 | 9 | 14 |



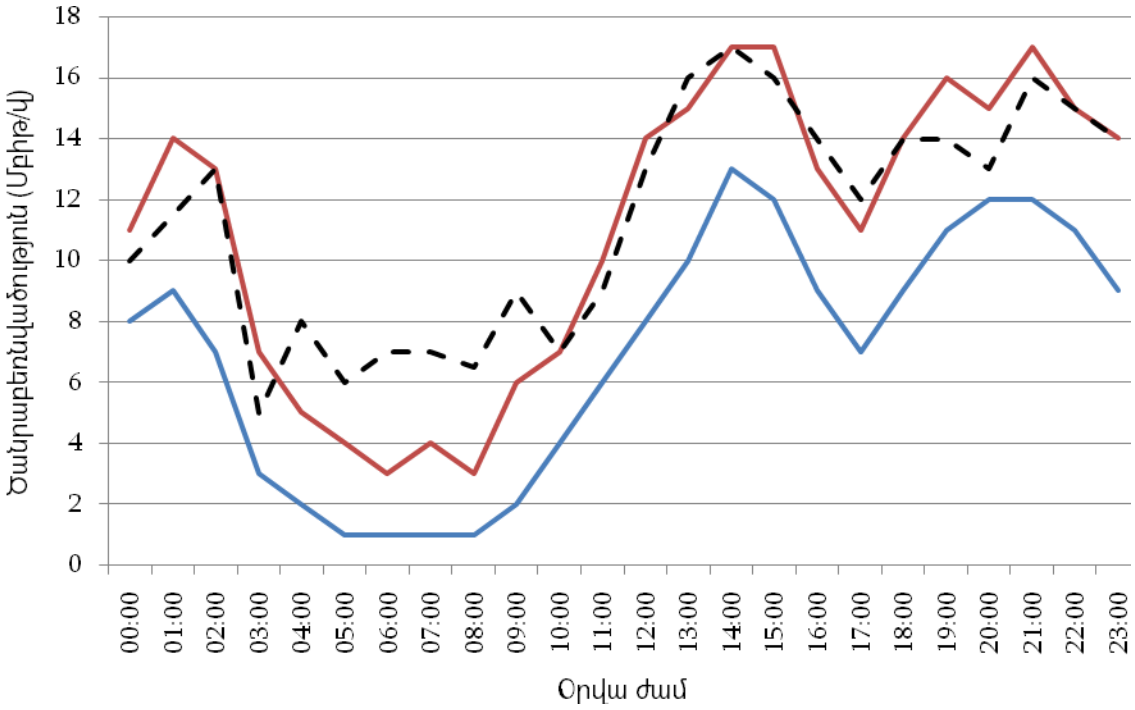

Նկ.34. «Օնլայնաճուրդ» ՍՊԸ-ի հեռահաղորդակցական ցանցի ծանրաբեռնավածությունն ըստ աշխատանքային օրվա ժամերի




Նկ.35. «Օնլայնաճուրդ» ՍՊԸ-ի հեռահաղորդակցական ցանցի ծանրաբեռնավածությունն ըստ ոչ աշխատանքային օրվա ժամերի

«Օնլայնաճուրդ» ՍՊԸ-ի հեռահաղորդակցական ցանցի համար մոդելավորվել են ցանցի ոչ բնականոն աշխատանքի բազմաթիվ դեպքեր, որոնցից մեկը եղել է ցանցի

ծանրաբեռնվածության աճ՝ պայմանավորված այցելուների մեծ ակտիվությամբ, ինչը բնորոշ չի եղել օրվա տվյալ ժամի համար: Նկար 36-ում բերված է ոչ աշխատանքային օրվա համար ցանցի ծանրաբեռնվածության փոփոխությունը՝ պայմանավորված այցելուների քանակի փոփոխությամբ:

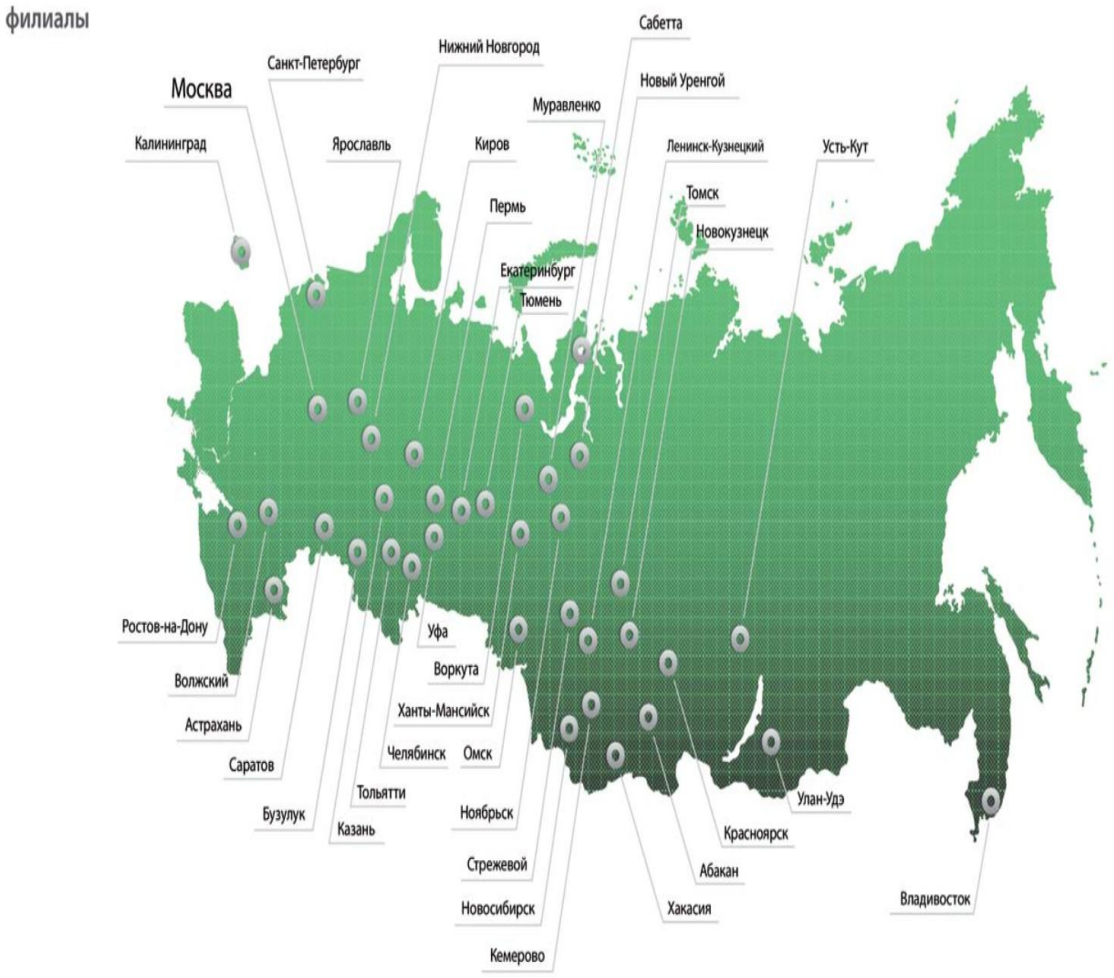



Նկ.36. «Օնլայնաճուրդ» ՍՊԸ-ի հեռահաղորդակցական ցանցի ծանրաբեռնավածությունն ըստ ոչ աշխատանքային օրվա ժամերի, այցելուների քանակի փոփոխության դեպքում

Նկար 36-ում նոր ծանրաբեռնվածությունը ներկայացված է կետագծերով: Հեռահաղորդակցական ցանցերի օպերատիվ կառավարման CTNOCAS ավտոմատացված համակարգի միջոցով հնարավոր է եղել հայտնաբերել ցանցի ծանրաբեռնվածության աճի դեպքերի 97%-ը: Ադմինիստրատորի կողմից ձեռնարկված համապատասխան միջոցները գրանցվել են համակարգում, որից հետո նմանատիպ այլ իրավիճակների մոդելավորման ժամանակ լուծումներն առաջարկվել են ադմինիստրատորին:

Ռուսաստանյան ՕՄՀ կազմակերպության գլխամասը գտնվում է Մոսկվա քաղաքում և այն ունի բազմաթիվ մասնաճյուղեր 35 քաղաքներում (նկ. 37): Կազմակերպությունն ունի մեծ կորպորատիվ հեռահաղորդակցական ցանց, որով

կատարվում է նրա մասնաճյուղերի սպասարկումը և տրամադրվում են բազմապիսի ծառայություններ, որոնցից օբյեկտների հեռակառավարումն է:




Նկ.37. ОМС կազմակերպության մասնաճյուղերը

Հեռահաղորդակցական ցանցերի օպերատիվ կառավարման CTNOCAS ավտոմատացված համակարգը ներդրվել է ОМС կազմակերպության հեռահաղորդակցական ցանցում և կիրառվում է դրա օպերատիվ կառավարման համար: Աղյուսակ 7-ում բերված են գլխամասի կողմից պատվիրատուներից մեկի շինության անվտանգության համակարգերի հեռավար կազմակերպման համակարգի սպասարկման համար կիրառվող հեռահաղորդակցական ցանցի աշխատանքային ծանրաբեռնվածությունները: Սպասարկվող կազմակերպությունում կան անվտանգության տեսահսկման համակարգեր, բազմապիսի տվիչներ, հակահրդեհային համակարգեր: Ծանրաբեռվնածության գրաֆիկներն աշխատանքային և ոչ աշխատանքային օրերի համար բերված են նկ. 38-ում և 39-ում:

Աղյուսակ 7

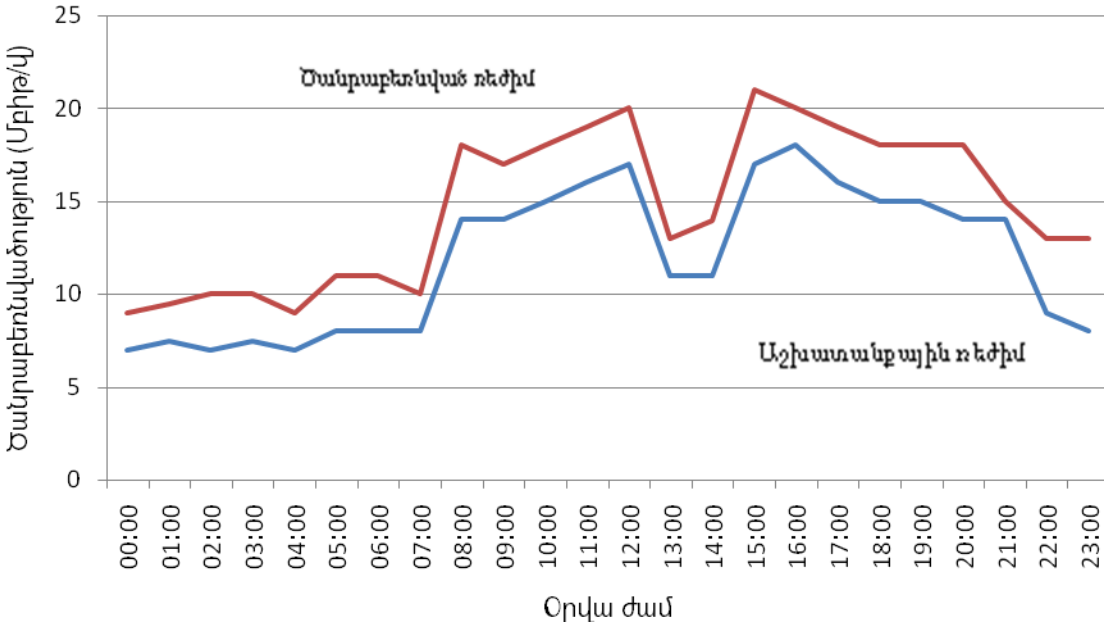
ՕՄՀ կազմապերպության գլխամասի հեռահաղորդակցական ցանցի ծանրաբեռնավածությունն ըստ օրվա ժամերի

| Ժամ | Աշխատանքային օր (Մբիթ/վ) | | Ոչ աշխատանքային օր (Մբիթ/վ) | |
|---|---|---|---|---|
| | Չծանրաբեռված | Ծանրաբեռնված | Չծանրաբեռբված | Ծանրաբեռնված |
| 00:00 | 7 | 9 | 5 | 9 |
| 01:00 | 7.5 | 9.5 | 5 | 8 |
| 02:00 | 7 | 10 | 3 | 7 |
| 03:00 | 7.5 | 10 | 3 | 7 |
| 04:00 | 7 | 9 | 3 | 8 |
| 05:00 | 8 | 11 | 3 | 7 |
| 06:00 | 8 | 11 | 5 | 9 |
| 07:00 | 8 | 10 | 6 | 10 |
| 08:00 | 14 | 18 | 7 | 10 |
| 09:00 | 14 | 17 | 7 | 11 |
| 10:00 | 15 | 18 | 8 | 11 |
| 11:00 | 16 | 19 | 7 | 12 |
| 12:00 | 17 | 20 | 8 | 13 |
| 13:00 | 11 | 13 | 6 | 11 |
| 14:00 | 11 | 14 | 6 | 11 |
| 15:00 | 17 | 21 | 8 | 12 |
| 16:00 | 18 | 20 | 7 | 13 |
| 17:00 | 16 | 19 | 7 | 11 |
| 18:00 | 15 | 18 | 8 | 13 |
| 19:00 | 15 | 18 | 8 | 13 |
| 20:00 | 14 | 18 | 7 | 13 |
| 21:00 | 14 | 15 | 7 | 10 |
| 22:00 | 9 | 13 | 5 | 9 |
| 23:00 | 8 | 13 | 5 | 8 |

Տվյալ հեռահաղորդակցական ցանցի համար մոդելավորվել է DDoS հարձակում, որի նպատակն է եղել խափանել անվտանգության համակարգերի սպասարկումն ապահովող հեռահաղորդակցական ցանցի աշխատանքը: DDoS հարձակման

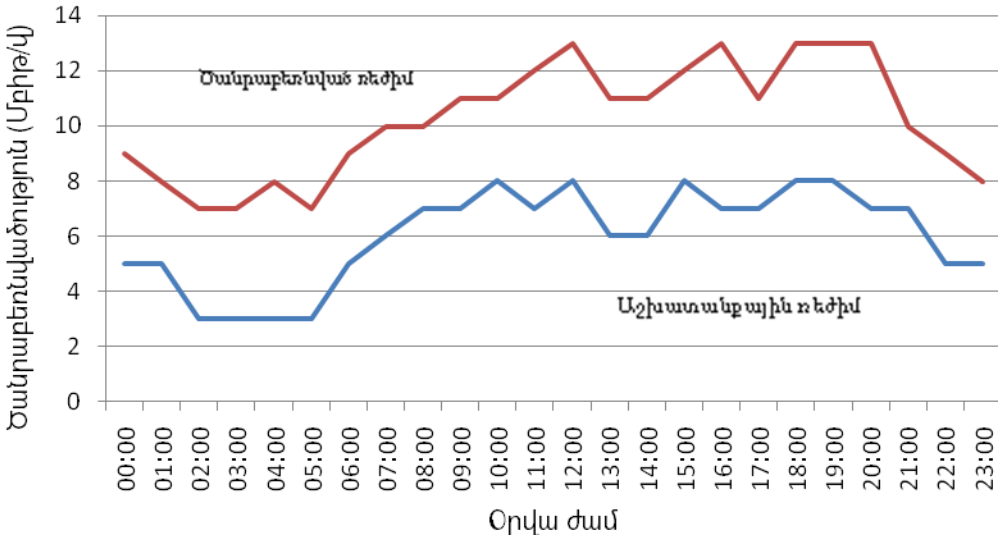
արդյունքում կտրուկ ավելացել է ցանցի ծանրաբեռնվածությունը, ինչը վաղաժամ հայտնաբերվել է CTNOCAS ավտոմատացված համակարգի կողմից և ադմինիստրատորի կողմից ձեռնարկված համապատասխան միջոցներից հետո ցանցի բնականոն աշխատանքը վերականգնվել է: Նման բնույթի խափանումները հեշտ հայտնաբերվում են, քանի որ դրանց դեպքում զգալի ավելանում է հեռահաղորդակցական ցանցի ծանրաբեռնվածությունը:

Տվյալ կազմակերպության համար մոդելավորվել է ևս մեկ իրավիճակ, երբ հեռահաղորդակցական ցանցում վնասակար ծրագրի հայտնվելու հեևանքով մեծացել է ցանցի ծանրաբեռնվածությունը:



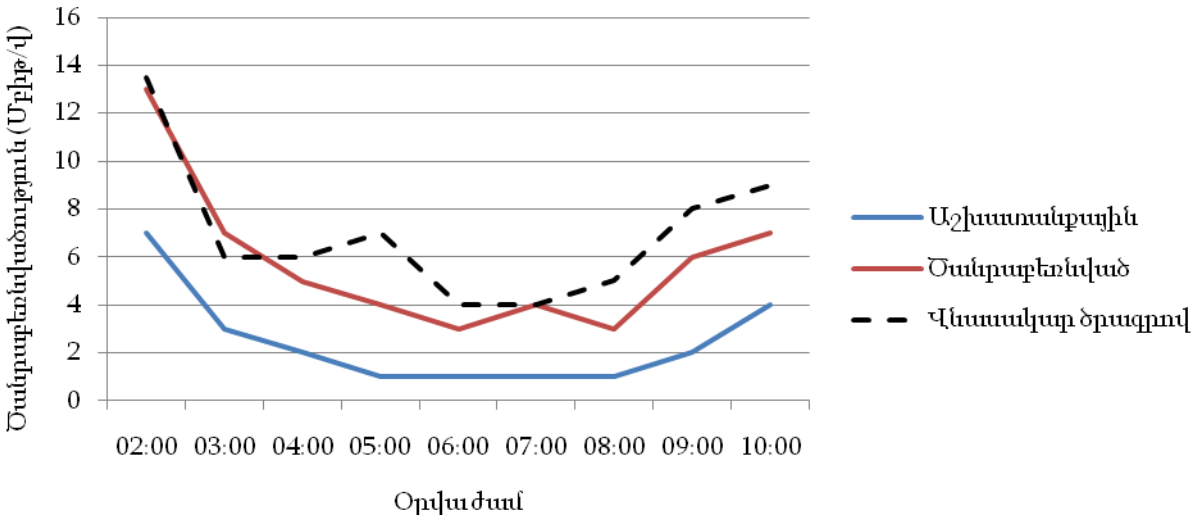

Նկ.38. ՕՄՀ կազմապերպության կորպորատիվ հեռահաղորդակցական ցանցի ծանրաբեռնավածությունն ըստ աշխատանքային օրվա ժամերի

Ի տարբերություն նախորդ դեպքի, ցանցի ծանրաբեռնվածությունը քիչ է ավելանում, քանի որ վնասակար ծրագիրը իր սերվեր է ուղարկում վարակված հանույցներում առկա ֆայլերը և չհայտնաբերվելու համար փոխանցումը կատարվում է փոքր արագությամբ: Հեռահաղորդակցական ցանցի աշխատանքը 02:00-ից 10:00-ի արանքում ընկած ժամանակահատվածի համար բերված է նկար 40-ում:

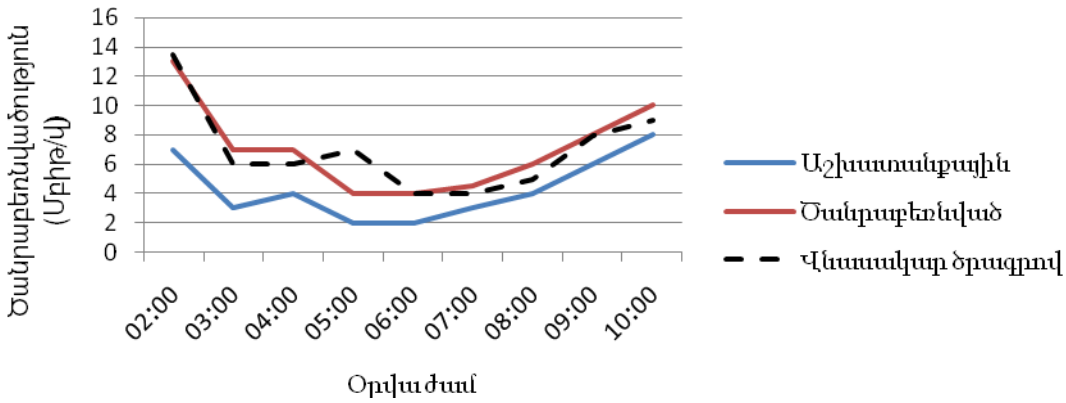



Նկ.39. ՕՄՀ կազմապերպության կորպորատիվ հեռահաղորդակցական ցանցի ծանրաբեռնավածությունն ըստ ոչ աշխատանքային օրվա ժամերի

Տվյալ դեպքում CTNOCAS-ի կողմից վնասակար ծրագրի աշխատանքը հայտնաբերվել է 65% ճշտությամբ: Դա պայմանավավորված է եղել այն հանգամանքով, որ տվյալ ցանցի համար ուսուցման գործընթացում բնականոն և ոչ բնականոն աշխատանքների ծանրաբեռնվածությունների միջակայքը բավականին մեծ էր:




Նկ.40. ՕՄՀ հեռահաղորդակցական ցանցի ծանրաբեռնավածությունը վնասակար ծրագրի առկայության դեպքում




Նկ.41. ՕՄՀ հեռահաղորդակցական ցանցի ծանրաբեռնավածությունը վնասակար ծրագրի առկայության դեպքում լրացուցիչ ուսուցումից հետո

Առաջացած խնդիրը լուծելու համար կատարվել է համակարգի լրացուցիչ ուսուցում, ինչից հետո վնասակար ծրագրի աշխատանքը հայտնաբերվել է 95 % ճշտությամբ (նկ. 41):

# Գլուխ 4-ի վերաբերյալ եզրակացություններ

Տվյալ գլխում մշակված մեթոների և ավտոմատացված համակարգի կիրառման օրինակների վերլուծությունների հիման վրա կարելի է գալ հետևյալ եզրակացությունների.

**1.** CTNOCAS ավտոմատացված համակարգն ունի բաց ճարտարապետություն, ինչի շնորհիվ թույլ է տալիս ավելացնել ոչ միայն համատեղելի սիմուլյատորների քանակը, այլ նաև փոխարինել արդեն գոյություն ունեցող սիմուլյատորները CTNOCAS-ի հետ համատեղելի այլ սիմուլյատորներով :

**2.** Մշակված CTNOCAS ավտոմատացված համակարգն ունի կլիենտ-սերվեր ճարտարապետություն: Կլիենտ մասն իրականացված է վեբ համակարգի տեսքով: CTNOCAS-ի մշակման ընթացքում կիրառվել է Microsoft ընկերության .NET Core տեխնոլոգիան, իսկ վեբ համակարգի համար՝ ASP.Net Core տեխնոլոգիան: Տվյալների պահոցն իրականացվել է MSSQL Server տեխնոլոգիայով: Նշված բոլոր համակարգերը կիրառելի են ինչպես Microsoft Windows օպերացիոն համակարգի համար, այնպես էլ Linux ընտանիքի Red Hat Enterprise և Ubuntu օպերացիոն համակարգերի համար:

**3.** «Օնլայնաճուրդ» ՍՊԸ-ի կողմից CTNOCAS ավտոմատացված համակարգն օգտագործվում է հեռահաղորդակցական ցանցում խնդիրների հայտնաբերման և ցանցի օպերատիվ կառավարման նպատակով: Հեռահաղորդակցական ցանցերի օպերատիվ կառավարման CTNOCAS ավտոմատացված համակարգի միջոցով հնարավոր է եղել հայտնաբերել ցանցի ծանրաբեռնվածության աճը: Ադմինիստրատորի կողմից ձեռնարկված համապատասխան միջոցառումները գրանցվել են համակարգում, որից հետո նմանատիպ այլ իրավիճակների մոդելավորման ժամանակ լուծումներն առաջարկվել են ադմինիստրատորին:

**4.** Հեռահաղորդակցական ցանցերի օպերատիվ կառավարման CTNOCAS ավտոմատացված համակարգը ներդրվել է ՕՄՀ կազմապերպության հեռահաղորդակցական ցանցում և կիրառվում է դրա օպերատիվ կառավարման համար: Տվյալ հեռահաղորդակցական ցանցի համար մոդելավորվել է DDoS հարձակում, որի նպատակն է եղել խափանել անվտանգության համակարգերի

սպասարկումն ապահովող հեռահաղորդակցական ցանցի աշխատանքը: DDoS հարձակման արդյունքում կտրուկ ավելացել է ցանցի ծանրաբեռնվածությունը, ինչը վաղաժամ հայտնաբերվել է CTNOCAS ավտոմատացված համակարգի կողմից և ադմինիստրատորի կողմից ձեռնարկված համապատասխան միջոցառումներից հետո ցանցի բնականոն աշխատանքը վերականգնվել է:

# ԵԶՐԱՀԱՆԳՈՒՄ

Ընդհանրացնելով ատենախոսական աշխատանքի չորս գլխում քննարկված, վերլուծված և ներկայացված նյութը՝ կարող ենք եզրահանգել.

1. Հիմնավորվել է կորպորատիվ հեռաղորդակցական ցանցերի օպերատիվ կառավարման խնդիրների լուծման համար առաջարկվող հեռահաղորդակցական ցանցերի անվտանգության ղեկավարման համակարգի օգտագործման անհրաժեշտությունը, որն ապահովում է հեռահաղորդակցական ցանցերի աշխատանքի հուսալիություն և կատարում է հոսթերի սկանավորում:

2. Կորպորատիվ հեռահաղորդակցական ցանցերում անոմալիաների հայտնաբերման արհեստական բանականության մեթոդներից պետք է կիրառել հենասյունային վեկտորային մեթոդը, քանի որ այն մյուս մեթոդների համեմատ տալիս է ցանցերի համար անոմալիայի հայտնաբերման ավելի բարձր արդյունք:

3. Նախագծվել է կորպորատիվ հեռաղորդակցական ցանցերում մեքենայական ուսուցման միջոցով անոմալիաների հայտնաբերման համակարգը:

4. Մշակվել է կորպորատիվ հեռահաղորդակցական ցանցերի օպերատիվ կառավարան երկխոսային CTNOCAS (**T**elecommunication **N**etworks **O**perative **C**ontrol **A**utomated **S**ystem) ավտոմատացված համակարգը, որն աշխատում է ցանցերի նախագծման WNST ավտոմատացված համակարգի հետ:

5. Մշակված CTNOCAS ավտոմատացված համակարգն ունի բաց ճարտարապետություն, ինչի շնորհիվ թույլ է տալիս ոչ միայն ավելացնել համակարգի հետ աշխատող նոր ենթահամակարգեր, այլև արդեն իսկ եղած ենթահամակարգերը փոխարինել CTNOCAS ավտոմատացված համակարգի հետ համատեղելի այլ ենթահամակարգերով:

# ՕԳՏԱԳՈՐԾՎԱԾ ԳՐԱԿԱՆՈՒԹՅԱՆ ՑԱՆԿ


1. Սարգսյան Գ.Հ., Հովհաննիսյան Ծ.Ս. Ցանցի կառավարման ծրագրային միջոցների վերլուծություն և ցանցային տրաֆիկի բաշխումը Լինուքս օպերացիոն համակարգում // ՀՊՃՀ Լրաբեր. Գիտական հոդվածների ժողովածու.- Երևան: Ճարտարագետ, 2011. - էջ 241-248:
2. Պետրոսյան Ա.Հ., Հովհաննիսյան Ծ.Ս., Մանուկյան Հ.Մ. Միասնական տրանսպորտային վիրտուալ ցանցի ստեղծման հնարավորությունը և նպատակահարմարությունը // ՀՊՃՀ Լրաբեր, Գիտական հոդվածների ժողովածու. -Երևան: Ճարտարագետ, 2013. -մաս1. - էջ 163-167:
3. Հովհաննիսյան Ծ.Ս. Հեռահաղորդակցական ցանցերում անվտանգության դինամիկ կազմակերպումը //ՀԱՊՀ Բանբեր. Տեղեկատվական տեխնոլոգիաներ, էլեկտրոնիկա, ռադիոտեխնիկա. -2015. -№1. -էջ 26-33:
4. Սարգսյան Գ.Հ., Հովհաննիսյան Ծ.Ս., Թորոսյան Լ.Յու. Հեռահաղորդակցության ցանցերում ապարատածրագրային սարքերի կիրառումը բեռնվածության բարելավման համար // ՀՀ ԳԱԱ և ՀԱՊՀ Տեղեկագիր. Տեխնիկական գիտությունների սերիա. -2015. -Հ.68, № 4. -էջ 429-435:
5. Հովհաննիսյան Ծ.Ս., Սիրադեղյան Ս.Ա., Կիրակոսյան Գ.Տ. Հեռահաղորդակցական ցանցերի օպերատիվ կառավարման եղանակի մշակում //Հայաստանի ճարտարագիտական ակադեմիա Լրաբեր. -2015.- Հատոր 12, № 4. -էջ 718-722:
6. Հովհաննիսյան Ծ.Ս., Սիրադեղյան Ս.Ա., Կիրակոսյան Ռ.Գ. Հեռահաղորդակցական ցանցերում մեքենայական ուսուցման միջոցով անոմալիաների հայտնաբերման համակարգի նախագծում // ՀՀ ԳԱԱ և ՀԱՊՀ Տեղեկագիր. Տեխնիկական գիտությունների սերիա. -2016.- Հատոր 69, № 4. -էջ 373-380:

7. Սիրադեղյան Ս.Ա. Կամայական թրաֆիկով ցանցերի կառուցվածքի օպտիմալ սինթեզի միջոցների մշակումը: Ե.13.03 - «Հաշվողական մեքենաներ, համալիրներ, համակարգեր, ցանցեր, դրանց տարրերը և սարքավորումները» մասնագիտությամբ տեխնիկական գիտությունների թեկնածուի գիտական աստիճանի հայցման ատենախոսության սեղմագիր. - Երևան, 2014. - 22 էջ:
8. Саргсян Г.О., Оганнисян Ц.С., Торосян Л.Ю. Анализ программ наблюдения трафика сети в режиме реальной работы // Materiały IX Międzynarodowej naukowi-praktycznej konferencji «Wschodnie partnerstwo - 2013». – Przemyśl: Nauka i studia, 2013.- Vol 35. Techniczne nauki. -C. 29-33.
9. Оганнисян Ц.С., Акопян А.А. Анализ программных методов управления трафика в корпоративной сети //Materiały IX Międzynarodowej naukowi-praktycznej konferencji «Wschodnie partnerstwo - 2013».- Przemyśl: Nauka i studia, 2013.- Vol 35. Techniczne nauki. -C. 45-49.
10. Абрагин Д. Телекоммуникационные сети нового поколения // Первая Миля. - 2009. - № 2. - С. 28-31.
11. Алиев Т.И. Сети ЭВМ и телекоммуникации. - СПб.: Изд-во СПбГУ ИТМО, 2011. - 400 с.
12. Апрышкина Г. Мониторинг в корпоративных сетях // Компьютер Пресс. - 2001.- № 7.- С. 72-78.
13. Арьков В.Ю. Нечеткие марковские модели систем управления // Управление в сложных системах, модели, методы и алгоритмы управления. - 1999. - С. 45-54.
14. Ачилов Р. Построение защищенных корпоративных сетей. - М.: ДМК Пресс, 2012. - 250 с.
15. Бакланов И.Г. NGN: принципы построения и организации. - М.: Эко-Трендз, 2008. - 400 с.

16. Балков М., Колпаков И., Колгатин С. Мультисервисные сети: стратегия планирования // Теле-Спутник. - 2002. - № 10 (84). - С. 41-46.
17. Бителева А. Сети Ethernet. Часть 4. Транспортные технологии // Теле-Спутник. - 2008. - № 12. - С. 98-101.
18. Бондаренко А.Д., Леохин Ю.Л. Проектирование интеллектуальных систем управления компьютерными сетями // Вестник Московского государственного университета. - 2007. - Вып. 2 (51). - С. 180-186.
19. Величко В.В., Субботин Е.А., Шувалов В.П., Ярославцев А.Ф. Телекоммуникационные системы и сети. Современные технологии. Том 3: Мультисервисные сети. - М.: Горячая линия, 2005. - 592 с.
20. Гоголев В.В. Использование системы автоматического проектирования работы корпоративных сетей для более эффективного заполнения предоставленной полосы канала // Математические машины и системы. - 2007. - Вып. № 3-4, том 1. - С. 85-94.
21. Голышко А.В. Сети связи будущего: консенсус в мультинумерации // Вестник связи. - 2002. - № 7. - С. 32-35.
22. Гольдштейн А.Б. Механизм эффективного туннелирования в сети MPLS // Вестник связи. - 2004. - № 2. - С. 48-54.
23. Гринфильд Д. Глобальная служба MPLS: опережая время // Журнал сетевых решений LAN. - 2002. - С. 32-38.
24. Дзегеленок И.И., Харитонов В.Ю., Орлов Д.А. Вычислительные аспекты построения распределенных систем виртуальной реальности // Вестник Московского энергетического института. - 2008. - № 5. - С. 27-32.
25. Иванов А.Ю., Кучерявый Л.Е., Гильченок Л.З. Пакетная сеть связи общего пользования. - М.: Наука и техника, 2004. - 272 с.

26. Кайлбах В., Бурдэн де Сен-Мартэн Т., Шпербер Р. На пути к конвергентному транспорту для магистральных IP-сетей // Технологии и средства связи. - 2006. - № 1. - С. 34-38.
27. Калимулина Э.Ю. Моделирование и анализ надёжности корпоративной сети // Стандарты и качество. - 2008. - № 8. - С. 96-101.
28. Коберси И.С., Белоглазов Д.А. Анализ недостатков методов классической теории управления // Сборник материалов докладов VII Всероссийской конференции молодых ученых, аспирантов и студентов "Информационные технологии, системный анализ и управление". - Таганрог, 2009. - С. 152-154.
29. Козерацкая Л.Н. Целочисленные задачи оптимизации: проблема устойчивости и параметрический анализ: Автореф. дис. д-ра физ.-мат. наук. - Украина, 1997. - 60 с.
30. Колгатин С.Ю., Колпаков И.А. Вопросы и проблемы построения оптических сетей // Кабельщик. - 2006. - №5. - С. 48-53.
31. Усикян Л.Д. Вероятностная модель пропускной способности каналов мобильной системы // Труды 9-й Международной научно-практической конференции “Современные информационные и электронные технологии”. – Одесса, Украина, 2008. – С. 244.
32. Колпаков И.А. Особенности реализации оптической транспортной среды при строительстве сетей с архитектурой FTTB/FTTH // Кабельщик. - 2007. - № 5. - С. 21-27.
33. Котенко И.В., Степашкин М.В. Анализ защищенности компьютерных сетей на этапах проектирования и эксплуатации // Изв. вузов. Приборостроение. - 2006. - № 5. - С. 3-8.
34. Крук Б.И., Попантонопуло В.Н., Шувалов В.П. Телекоммуникационные системы и сети. Современные технологии. Том 1. - М.: Телеком, 2003. - 648 с.

35. Кучерявый А.Е., Гильченок Л.З. Принципы модернизации телефонной сети общего пользования // Электросвязь. - 2002. - № 2. - С. 26-33.
36. Ларин Р.М., Плясунов А.В., Пяткин А.В. Методы оптимизации. Примеры и задачи. - М.: Изд-во НГУ, 2003. - 120 с.
37. Леохин Ю.Л. Анализ информационной структуры корпоративной сети // Известия высших учебных заведений. - 2008. - № 4. - С. 27-40.
38. Леохин Ю.Л. Многоуровневый подход к управлению мультисервисными корпоративными сетями // Телематика. - 2009. - Том 2. - С. 277-278.
39. Нетес В.А. Задание требований по надежности в соглашениях об уровне обслуживания // Электросвязь. - 2004. - № 4. - С. 46-51.
40. Николаев С. Пути преобразования телефонных сетей в NGN сети // Connect! Мир связи. - 2007. - № 5. - С. 9-16.
41. Райман Л.Д. Концепция развития рынка телекоммуникационных услуг // Электросвязь. - 2001. - № 1. - С. 8-16.
42. Рерле Р.Д., Гольдштейн Б.С., Ехриель И.М. Интеллектуальные сети. - М.: Радио и связь, 2003. - 504 с.
43. Сатовский Б.Л. MPLS - технология маршрутизации для нового поколения сетей общего пользования // Сети и системы связи. - 2001. - № 5. - С. 42-47.
44. Сети следующего поколения NGN / А.В. Росляков, М.Ю. Самсонов, И.В. Шибаева и др. - М.: Эко-Трендз, 2009. - 424 с.
45. Соколов Н.А. Выбор технологии коммутации для сетей следующего поколения // Мобильные системы. - 2004. - № 7. - С. 7-11.
46. Соколов Н.А. Семь аспектов развития сетей доступа // Технологии и средства связи. - 2005. - № 3. - С. 14-23.
47. Столлингс В. Современные компьютерные сети. -2-е издание. - СПб.: Питер, 2003. - 782 с.

48. Тюрин М.В. Экспертная оценка живучести телекоммуникационных систем и компьютерных сетей (ТСКС) в условиях неполноты информации // Автоматизация в промышленности. - 2008. - № 7. - С. 15-18.
49. Устинов С.А., Алексеев Е.Б. Технологии оптического доступа: тенденции развития // Технологии и средства связи. Отраслевой каталог. - 2005. - С. 91-97.
50. Hovhannisyan Ts. The traffic management in different Linux distributive servers in corporative networks for effective routing //Proceedings of engineering academy of Armenia (PEAA). –Vol.10, №4.- P.769-773.
51. Abraham A., Jain R., Thomas J. D-SCIDS:Distributed soft computing intrusion detection system //Journal of Network and Computer Applications.- 2007.- Vol. 30.-P. 81-98.
52. Ahmet Y. Şekercioğlu, Andras Varga, and Gregory K. Egan. Parallel Simulation made easy with OMNeT++ // Proceedings of European Simulation Symposium, Delft.- The Netherlands, 2003.- P. 493-499.
53. Altman E., Jiménez T. NS Simulator for Beginners.- Morgan & Claypool Publishers, 2012.- 184 p.
54. ASP.NET MVC 4 in Action / J. Palermo, J. Palermo, E. Hexter, et al.- Manning Publications, 2012.- 440 p.
55. Black N.U. IP Routing Protocols: RIP, OSPF, BGP, PNNI and Cisco Routing Protocols.- Prentice Hall, 2000.- 387 p.
56. Boghe M., Renwanz M. A realisitic VoIP traffic generation and evaluation tool for OMNeT++ // OMNeT++ 2008: Proceedings of the 1st International Workshop on OMNeT++.- 2008.
57. Burbank J., Kasch W., Ward J. An Introduction to Network Modeling and Simulation for the Practicing Engineer.- IEEE Press, 2011.- 216 p.
58. Buyya R., Broberg J., Goscinki A. Cloud Computing: Principles and Paradigms.- Wiley, 2011.- 664 p.
59. Cambron K.G. Global Networks: Engineering, Operations and Design.- Wiley, 2012.- 414 p.

60. Casilari E., González J.F., Sandoval F. Modeling of HTTP Traffic // IEEE communications letters.- 2001.- Vol. 5, № 6.- P. 272-274.
61. Chamberlain T. Learning OMNeT++.- Packt Publishing, 2013.- 102 p.
62. Day R. OSPF 140 Success Secrets: 140 Most Asked Questions On OSPF - What You Need To Know.- Emereo Publishing, 2014.- 102 p.
63. DiMarzio F.J. Network Architecture & Design "A Field Guide for IT Professionals."- Sams Publishing, 2001.- 384 p.
64. Donahue A.G. Network Warrior.- O'Reilly Media, 2011.- 788 p.
65. Dymora P., Mazurek M., Strzałka D. Computer network traffic analysis with the use of statistical self-similarity factor // Annales UMCS Informatica.- Lublin, 2014.- Vol. 13, issue 2.- P. 69–81.
66. Empson S. CCNA Routing and Switching Portable Command Guide. -3rd Edition.- Cisco Press, 2013.- 320 p.
67. Erl T., Puttini R., Mahmood Z. Cloud Computing: Concepts, Technology & Architecture.- Prentice Hall, 2013.- 523 p.
68. Fall R.K., Stevens R.W. TCP/IP Illustrated, Volume 1: The Protocols.- Addison-Wesley Professional, 2011.- 1056 p.
69. Fortz B., Rexford J., Thorup M. Traffic Engineering With Traditional IP Routing Protocols // IEEE Communications Magazine.- October, 2002.- P. 118-124.
70. Freeman A. Pro ASP.NET MVC 4.- Apress, 2013.- 756 p.
71. Galloway J., Haack P.,Wilson B., Allen S.K. Professional ASP.NET MVC 4.-Wrox, 2012.- 504 p.
72. Guizani M., Rayes A., Khan B., Al-Fuqaha A. Network Modeling and Simulation: A Practical Perspective.- Wiley-Interscience, 2010.- 304 p.
73. Hartpence B. Packet Guide to Core Network Protocols.- O'Reilly Media, 2011.- 264 p.
74. Heller D.M., Luckie C.D. Behavior Analysis of Network Flow Traffic.- Amazon Digital Services - Inc., 2012.- 73 p.
75. Issariyakul T., Hossain E. Introduction to Network Simulator NS2.- Springer, 2012.- 536 p.

76. Jamsa K.D. Cloud Computing: SaaS, PaaS, IaaS, Virtualization, Business Models, Mobile, Security and More.- Jones & Bartlett Learning, 2012.- 324 p.
77. Janevski T. NGN Architectures, Protocols and Services.- Wilay, 2014.- 366 p.
78. Jefferson D., Sowizral H. Fast concurrent simulation using Time-Warp mechanism // Distributed Simulation.- 1985.- P. 63-69.
79. Jónsson V.K. HttpTools: A Toolkit for Simulation of Web Hosts in OMNeT++ // OMNeT++ 2009: Proceedings of the 2nd International Workshop on OMNeT++.- 2009.
80. Karim A., Khan A.M. Behaviour of Routing Protocols for Medium to Large Scale Networks // Australian Journal of Basic and Applied Sciences.- 2011.- 5(6).- P. 1605-1613.
81. Kasch W.T., Ward J.R., and Andrusenko J. Wireless Network Modeling and Simulation Tools for Designers and Developers // IEEE Communications Magazine.- March 2009.- Vol. 47, № 3.- P. 120-127.
82. Kavis J.M. Architecting the Cloud: Design Decisions for Cloud Computing Service Models (SaaS, PaaS, and IaaS).- Wilay, 2014.- 199 p.
83. Kozierok M.C. The TCP/IP Guide: A Comprehensive, Illustrated Internet Protocols Reference.- No Starch Press, 2005.- 1616 p.
84. Kurose F.J., Ross W.K. Computer Networking: A Top-Down Approach. -6th Edition.- Pearson, 2012.- 864 p.
85. Lessmann J., Janacik P., Lachev L., Orfanus D. Comparative Study of Wireless Network Simulators // The Seventh International Conference on Networking. – 2008. – P. 517-523.
86. Maureira J., Dalle O., Dujovne D. Generation of Realistic 802.11 Interferences in the Omnet++ INET Framework Based on Real Traffic Measurements // OMNeT++2009: Proceedings of the 2nd International Workshop on OMNeT++.- 2009.

87. McCabe D.J. Network Analysis, Architecture, and Design. -Third Edition.- Morgan Kaufmann, 2007.- 496 p.
88. Michel T. Network Design Cookbook: Architecting Cisco Networks.- lulu.com, 2013.- 384 p.
89. Nowak M., Novak S. Parallel simulations with modified INET simulation package // Theoretical and Applied Informatics.-Warsaw, 2007.- Vol. 19, № 2.- P. 147-156.
90. Osareh A., Shadgar B. Intrusion Detection in Computer Networks based on Machine Learning Algorithms // IJCSNS International Journal of Computer Science and Network Security .-2008. -Vol.8 .- № 11.
91. Olifer N., Olifer V. Computer Networks: Principles, Technologies and Protocols for Network Design.- Wiley, 2005.- 1000 p.
92. Park K., Willinger W. Self-Similar Network Traffic and Performance Evaluation.- Wiley-Interscience, 2000.- 558 p.
93. Pepelnjak I. EIGRP Network Design Solutions: The Definitive Resource for EIGRP Design, Deployment, and Operation.- Cisco Systems, 2000.- 366 p.
94. Peterson L.L., Davie S.B. Computer Networks. -Fifth Edition: A Systems Approach.- Morgan Kaufmann, 2011.- 920 p.
95. Pioro M., Medhi D. Routing, Flow, and Capacity Design in Communication and Computer Networks.- Morgan Kaufmann, 2004.- 800 p.
96. Professional SQL Server 2008 Internals and Troubleshooting / C. Bolton, J. Langford, et al.- Ozar, Wrox, 2010.- 624 p.
97. Rankins R., Bertucci P., Gallelli C., Silverstein T.A. Microsoft SQL Server 2008 R2 Unleashed.- Sams Publishing, 2010.- 1704 p.
98. Reineck K.M., Jonas K., Uhde K. Evaluation and Comparison of Network Simulation Tools: Master Thesis.- Sankt Augustin, Germany, 2008.- 93 p.

99. Sayeed A., Morrow J.M. MPLS and Next-Generation Networks: Foundations for NGN and Enterprise Virtualization.- Cisco Press, 2006.- 422 p.
100. Siradeghyan S., Kirakossian R. Performance Evaluation of VoIP Traffic on Wired and Wireless Networks // Computer Science and Information Technologies.- Yerevan, Armenia, 2013.- P. 376-378.
101. Watson M., Lewis S., Cacioppi P., Jayaraman J. Supply Chain Network Design: Applying Optimization and Analytics to the Global Supply Chain.- Pearson FT Press, 2012.- 424 p.
102. Wehrle K., Gune M. Gross J. Modeling and Tools for Network Simulation.- Springer, 2010.- 545 p.
103. Weingarten E., Lehn H.V., Wehrle K. A performance comparison of recent network simulators // IEEE International Conference on Communications.- 2009.- P. 1-5.
104. White R., Donohue D. The Art of Network Architecture: Business-Driven Design.- Cisco Press, 2014.- 352 p.
105. Xu D., Trajković L. Performance Analysis of RIP, EIGRP, and OSPF using OPNET // International Journal of Computer Applications.- Washington DC, USA, 2011.- Vol. 48, № 18.- P. 6-11.
106. Xu Z. Designing and Implementing IP/MPLS-Based Ethernet Layer 2 VPN Services: An Advanced Guide for VPLS and VLL.- Wilay, 2009.- 984 p.
107. https://en.wikipedia.org/wiki/Machine_learning
108. https://aws.amazon.com/ru/ec2/
109. http://erlang.org/doc/pdf/otp-system-documentation.pdf
110. http://alexott.net/ru/erlang

# ՀԱՎԵԼՎԱԾՆԵՐ

## Ատենախոսության արդյունքների ներդրման երեք ակտը

**Հավելված 1**

«Օնլայնաճուրդ» ընկերությունում կորպորատիվ հեռահաղորդակցական ցանցում խնդիրների հայտնաբերման և ցանցի օպերատիվ կառավարման համար օգտագործվում է CTNOCAS ավտոմատացված համակարգը:

(ԱԿՏԸ (1 էջ) ԱՌԿԱ Է ԵՎ ՊԱՏՃԵՆԸ ԿԴՐՎԻ ԱՏԵՆԱԽՈՍՈՒԹՅԱՆ ՀԱՎԵԼՎԱԾՈՒՄ)

**Հավելված 2**

CTNOCAS ավտոմատացված համակարգը օգտագործվում է «ՕՄՀ» ընկերությունում: Մշակված CTNOCAS-ի կողմից կորպորատիվ հեռահաղորդակցական ցանցում հայտնաբերվում է վնասակար ծրագրերը, որոնց հայտնվելու հետևանքով մեծանում է ցանցի ծանրաբեռնվածություն, ինչն էլ իր հերթին խաթարում է կորպորատիվ հեռահաղորդակցական ցանցի բնականոն աշխատանքը:

(ԱԿՏԸ (1 էջ) ԱՌԿԱ Է ԵՎ ՊԱՏՃԵՆԸ ԿԴՐՎԻ ԱՏԵՆԱԽՈՍՈՒԹՅԱՆ ՀԱՎԵԼՎԱԾՈՒՄ)

**Հավելված 3**

«Հայաստանի ազգային պոլիտեխնիկական համալսարանի «Քոմփյութերային համակարգեր և ցանցեր» ամբիոնում դասավանդվող «Քոմփյութերային ցանցերի կազմակերպում-2» առարկայի լաբորատոր աշխատանքների իրականացման գործընթացում՝ «D-Link սարքավորումներով ցանցերի կազմակերպման» լաբորատոր աշխատանքների մեթոդական ցուցումների տեսքով:

(ԱԿՏԸ (1 էջ) ԱՌԿԱ Է ԵՎ ՊԱՏՃԵՆԸ ԿԴՐՎԻ ԱՏԵՆԱԽՈՍՈՒԹՅԱՆ ՀԱՎԵԼՎԱԾՈՒՄ)