ҚАЗАҚСТАН РЕСПУБЛИКАСЫ БІЛІМ ЖӘНЕ ҒЫЛЫМ МИНИСТРЛІГІ

Коммерциялық емес акционерлік қоғамы
АЛМАТЫ ЭНЕРГЕТИКА ЖӘНЕ БАЙЛАНЫС УНИВЕРСИТЕТІ

Инфокоммуникациялық технологиялар **кафедрасы**

«Қорғауға жіберілді»
Кафедра меңгерушісі
т.ғ.к., доцент Чежимбаева К.С.
(аты-жөні, ғылыми дәрежесі, атағы)

_____ «____» _____20___ж.
(қолы)

ДИПЛОМДЫҚ ЖОБА

Тақырыбы: VPN желісі үшін желілік ресурстарды тиімді ұлестірудің моделін таңдау

5В071900–Радиотехника,электроника және телекоммуникациялар **мамандығы бойынша**

Орындаған Бенжебаев Бауыржан СТкуп-13-1
(аты - жөні) (тобы)

Жетекші т.ғ.к., доцент Сапшимбаева Г.М
(аты-жөні, ғылыми дәрежесі, атағы, қолы)

Кеңесшілер:

Экономикалық бөлім бойынша:
т.ғ.к. профессор Бахшилов Кашен Барылович
(ғылыми дәрежесі, атағы, аты-жөні)
_____ «23» 05 20 16 ж.
(қолы)

Өмір тіршілігі қауіпсіздігі бойынша:
б.ғ.к. аға оқытушы Мустафин Нұрлат Габбасович
(ғылыми дәрежесі, атағы, аты-жөні)
_____ «30» 05 20 16 ж.
(қолы)

Есептеу техникасын қолдану бойынша:
т.ғ.к., доцент Чежимбаева К.С.
(ғылыми дәрежесі, атағы, аты-жөні)
_____ «3» 06 20 16 ж.
(қолы)

Мөлшер бақылаушы: т.ғ.к., доцент Чежимбаева К.С
(ғылыми дәрежесі, атағы, аты-жөні)
_____ «3» 06 20 16 ж.
(қолы)

Пікір жазушы: Серік Н.
(ғылыми дәрежесі, атағы, аты-жөні)
_____ «3» 06 20 16 ж.
(қолы)

Алматы 2016

ҚАЗАҚСТАН РЕСПУБЛИКАСЫ БІЛІМ ЖӘНЕ ҒЫЛЫМ МИНИСТРЛІГІ

Коммерциялық емес акционерлік қоғамы
АЛМАТЫ ЭНЕРГЕТИКА ЖӘНЕ БАЙЛАНЫС УНИВЕРСИТЕТІ

Радиотехника және байланыс факультеті
Радиотехника, электроника және телекоммуникациялар мамандығы
Инфокоммуникациялық технологиялар кафедрасы

жобаны орындауға берілген

ТАПСЫРМА

Студент Нежебаев Бухар
(аты - жөні)

Жоба тақырыбы VPN желісі үшін желілік ресурстарды тиімді үлестірудің моделін таңдау

ректордың «19» қазан № 148 бұйрығы бойынша бекітілген.

Аяқталған жұмысты тапсыру мерзімі: «_____» 05 20___ж.

Жобаға бастапқы деректер (талап етілетін жоба нәтижелерінің параметрлері және нысанның бастапқы деректері):

$M(\alpha) = 58,62$
$R(\alpha) = 1.38$
$S_n = 39.7\ м^2$
$S_0 = 6.3\ м^2$
$S_1 = 3,15$
$S_2 = 1,75$
$p = 1.125$

Диплом жобасындағы әзірленуі тиіс сұрақтар тізімі немесе диплом жобасының қысқаша мазмұны:

Кіріспе
Виртуалды жеке желілердің құру негіздері
Маршрутизаторлар базасындағы VPN
VPN құру сұлбалары
Қызметтік сапасын қамтамасыз ететін базалық тех-р
Виртуалды жеке желілердің моделін құру
Арналық модель базасында VPN үйлесімділігі әдістері
Арналық модель.
Өмір тіршілік қауіпсіздігі
Бизнес-жоспар
Қорытынды

Сызба материалдарының (міндетті түрде дайындалатын сызуларды көрсету) тізімі:

1.1 Ақпараттық өзара алмасу қауіпсіздігін қамтамасыз ету
2 Интернет негізінде виртуалды жеке желіні құру
3. Желі аралық экрандар базасындағы VPN жүзеге асыру
4 Маршрутизаторлар базасындағы VPN
5. Бағдарламалық қамтамасыздандыру базасындағы VPN
6 Маманданған аппараттық құралдар базасындағы VPN
7. VPN құратын провайдерлік сұлба
8. VPN жүйесінің интенсивтілігінің матрицасы
9. VPN арасында желінің жеке звеноларының өткізу қолдаған ұлестіруудің графигі
10. C++ алгоритмдік тілінің негізгі терезесі.
11 шаңдар орналасу сұрағы
12. БҚ өңдеудің сметалық құнының құрылымдық сұлбасы.

Негізгі ұсынылатын әдебиеттер

1. Росляков А.В. Оптимальное распределение сетевых ресурсов для реализации виртуальных частных сетей СПб., СПбГУТ - 2004 - с 65-74
2 Сериков И. Виртуальные частные сети http://www.pcmag.ru/archive/5/059932.asp · 20.10.2012.
3. Браун С. Виртуальные частные сети - М.: Лори, 2001. - 508 с.

Жоба бойынша бөлімшелерге қатысты белгіленген кеңесшілер

бөлімшелер	кеңесші	мерзімі	қолы
Экономика	Бабаев К.Б	14.4-28.05.16	
Тех. бөлім	Сагимбаева Ж.М	10.12.15-30.06.16	
ЕТБ	Чекембаева К.Е.	30.05-3.06.16	
Мәдениет бақылау	Чекембаева К.Е.	30.05-3.06.16	

диплом жобасын дайындау

КЕСТЕСІ

№ р/с	Тарау аттары, әзірленетін сұрақтардың тізімі	Жетекшіге ұсыну мерзімдері	Ескерту
1	Теориялық бөлім	26.12 – 28.12.15	орындалды
	Виртуалды жеке желілердің		
	анықтау		
	VPN құру сұлбалары		
	Қызметтік сапасын	21.01. – 30.01.16	орындалды
	қамтамасыз ететін		
	бағалық технологиялар		
2	Есептеу бөлімі	07.02. – 01.03.16	орындалды
	Арналық модель		
	арналық модельдің үйлесіндіру		
	жүйесімен		
	VPN желісінің өміршеңдігін	02.03. – 14.03.16	орындалды
	есептеу		
3	Өміртіршілік қауіпсіздігі	25.03 – 30.03.16	орындалды
4	Экономикалық бөлім	20.04 – 2.05.16	орындалды

Тапсырманың берілген уақыты «10» желтоқсан 2015ж.

Кафедра меңгерушісі _____ т.ғ.к., доцент Чежимбаева К.С.
(қолы) (аты-жөні, ғылыми дәрежесі, атағы)

Жоба жетекшісі _____ Сагимбаева Г.М. т.ғ.к. доцент
(қолы) (аты-жөні, ғылыми дәрежесі, атағы)

Орындалатын тапсырманы
кабылдаған студент _____ _____
(қолы) (аты -жөні)

Аннотация

В выпускной работе исследована модель оптимального распределения сетевых ресурсов для VPN сети.

Рассмотрены основы построения виртуальных частных сетей. Предоставлены услуги VPN и ее варианты технической реализации и схемы.

Предоставлены базовые технологии обеспечения качества услуг и информационной безопасности. Предоставлены особенности реализации оптических VPN.

В разделе безопасности жизнедеятельности рассмотрен анализ условия труда в помещении, производственное освещение и кондиционирование.

Разработаны технико-экономическое обоснование внедрения данного проекта и бизнес-план.

Annotation

The graduation paper the model of optimal allocation of network resources to VPN.

The basics of virtual private networks. Provided services VPN and its technical implementation options and schemes.

Provided the basic technology to ensure the quality of services and information security. Provided optical features of the implementation of VPN.

The life safety section describes the analysis of working conditions in the room, industrial lighting and air conditioning.

Developed feasibility study for implementation of the project and a business plan.

Аңдатпа

Бұл бітіру жұмысында VPN желісінде желілік ресурстарды тиімді үлестіру моделі зерттелген.

Виртуалды жеке желілерді құру негіздері қарастырылған. VPN қызметтері мен оны техникалық жүзеге асыру нұсқалары мен сұлбалары көрсетілген.

Сапалы қызмет көрсету мен ақпараттық қауіпсіздіктің базалық технологиялары қарастырылған. Оптикалық VPN жүзеге асыру ерекшеліктері көрсетілген.

Сонымен қатар өміртіршілік қауіпсіздігі бөлімінде бөлмедегі еңбек жағдайын талдау, жасанды жарықтандыру мен ауа баптау қарастырылған.

Осы жобаны енгізудің техника-экономикалық негіздемесі және бизнес-жоспар жасалынған.

Мазмұны

Кіріспе 8
1 Виртуалды жеке желілерді құру негіздері 9
1.1 Виртуалды жеке желілердің арналуы 9
1.2 VPN қызметтері 12
1.3 Техникалық жүзеге асыру нұсқалары 20
1.3.1 Желі аралық экрандар базасындағы VPN 20
1.3.2 Маршрутизаторлар базасындағы VPN 21
1.3.3 Бағдарламалық қамтамасыздандыру базасындағы VPN 21
1.3.4 Желілік операциялық жүйе базасындағы VPN 22
1.3.5 Арнаулы аппаратты құралдар базасындағы VPN 22
1.4 VPN құру сұлбалары 23
1.4.1 Бірлескен сұлба 23
1.4.2 Провайдерлік сұлба 25
1.4.3 Аралас сұлба 27
1.5 VPN жабдықтарын желіде орналастыру нұсқалары 28
2 Қызметтің сапасын қамтамасыз ететін базалық технологиялар 32
2.1 Базалық технологиялардың сипаттамалары 32
2.1.1 RSVP протоколының базасында сапаны қамтамасыз ету 32
2.1.2 Дифференциалды қызмет көрсету базасында сапаны қамтамасыз ету 34
2.1.3 MPLS технологиясының базасында сапаны қамтамасыз ету 35
2.2 Ақпараттық қауіпсіздіктің базалық технологиялары 37
2.2.1 IP базасында VPN қауіпсіздікті қамтамасыз ету жабдықтары. 38
2.2.2 Арналық деңгейде деректерді қорғау 44
2.2.3 Желілік деңгейде деректерді қорғау 46
3 Виртуалды жеке желілердің моделін құру 48
3.1 VPN жүзеге асыру үшін желілік ресурстарды тиімді үлестіру мәселелері 48
3.2 Арналық модель 52
3.2.1 Арналық модель түсінігі 52
3.2.2 Арналық модель базасында VPN үйлесімділеу мәселелері 53
3.2.3 Арналық модельді үйлесімділеу әдістемесі 54
3.3 VPN желісінің өміршеңдігін есептеу 63
4 Өміртіршілік қауіпсіздігі 66
4.1 Еңбек жағдайларын талдау 66
4.2 Бөлме жарықтандыруын есептеу 67
4.2.1 Бөлменің табиғи жарықтандыруын есептеу 67
4.2.2 Бөлменің жасанды жарықтандыруын есептеу 71
4.3 Бөлменің желдендіруін есептеу 74
5 Бизнес-жоспар 77
5.1 Презентация 77
5.2 Жобаның мақсаты 77

5.3 Ғылыми зерттеу жұмыстың жоспары 78
5.4Бағдарламалық құралдардың бағасын анықтаудың негізгі қағидалары 80
5.5 Бағдарламалық құралдардың сметалық құнын есептеу реті 80
5.6 Интелектуалды еңбек құнын анықтау 85
5.7 Қорытынды 85
Қорытынды 86
Қысқартылған сөздер тізімі 87
Әдебиеттер тізімі 88
А қосымшасы Алгоритм листінгі 90
Ә қосымшасы Құрылған моделдің блок сұлбасы
Б қосымшасы Желінің өміршеңдігінің блок сұлбасы
В қосымшасы Желінің өміршеңдігінің бағдарлама листінгі

Кіріспе

Соңғы жылдары дүние жүзінде телекоммуникацияда виртуалды жеке желілердің VPN (Virtual Private Network) қарқынды дамуы қызығарлықтай. Ол Интернет желісі арқылы қашықталған пайдаланушылар мен қашықталған кеңселердің арзан қосылуынан бірлескен желілерді үстау үшін кететін шығындарды төмендетуге негізделген. Бірақта, желілерді Интернет арқылы біріктіргенде деректерді таратудың қауіпсіздігі пайда болады. Сондықтан, таратылатын ақпараттың бүтіндігі мен құпиялығын қамтамасыз ететін механизмдерді жасау қажеттігі туды. Осындай механизмдер базасында құрылған желілерді VPN деп атады.

VPN желілерінің негізгі мәселесіне тұрақталған аутентификация стандарттары мен шифрленген ақпараттардың алмасуының жоқ болуы. Осы стандарттар әлі де өңделу процесінде жүргізіліп жатыр. Сондықтан, әртүрлі өндірушілердің өнімдері VPN-қосылуларды және кілттермен автоматты алмасуды орната алмайды. Көрсетілген мәселе VPN баяу таралуына әкеледі. Себебі, әртүрлі кәсіпорындарды бір өндіруші өнімдерімен қолдануды талап етуге болмайды.

Жоғарыдан көрінгендей VPN құрудың өнімдері желіде кішкентай орынды алуы мүмкін. Ол ақпараттың шифрленуі мен көптеген қосылуларды қолдау үшін осы қосылулармен таралатын қолданылатын құрылғылардың жоғарғы өнімділігі қажет етіледі. Осы мәселе VPN құрудың кемшілігіне жатады.

VPN тағы бір осал жеріне біртұтас сенімді басқару әдістерінің жоқ болуы жатады. Ол желілік әкімшіліктер үшін өте маңызды. Интернет желісінде сапалы сервисті қамтамасыз ететін механизмдердің жоқтығы VPN желісін құруды күрделендіреді. Кейбір қосымшалар үшін шектелген уақыт ішінде ақпараттың кепілденген жетуін талап етеді.

Берілген қызмет көрсету сапасын қолдау (QoS — Quality of Service) виртуалды жеке желілерді еңгізу бойынша басты мәселе болып саналады. Бірақта мұндай мәселені шешу қиынға соғады, әсіресе берілген қызмет көрсету сапасын Интернетта қамтамасыз ету керек болса. Виртуалды жеке желілерді жүзеге асыру кезінде сенімді қорғанысты қамтамасыз ету ең басты мәселе.

VPN желісінде желілік ресурстарды тиімді үлестіру зерттеледі. Ол арналық модель базасында жүргізіледі. VPN құрудың ең басты мәселесіне қолданылатын есептеу әдістерінің масштабтылығын қамтамасыз ету жатады.

Сонымен қатар, бұл бітіру жұмысында өміртіршілік қауіпсіздігі мәселелері қарастырылады. Бөлмедегі еңбек жағдайын талдау және жасанды жарықтандыру мен ауа баптауды қарастыру.

Осы жобаны енгізудің техника-экономикалық негіздемесі мен бизнес-жоспар жасалынады.

1 Виртуалды жеке желілерді құру негіздері

1.1 Виртуалды жеке желілердің арналуы

Соңғы жылдары байқалған, Интернеттің тез дамуы компьютердің кез-келген иесіне шектелмеген ақпарат қорларына рұқсат береді. Соған байланысты бірлескен желіге жеке және коллективті рұқсат мүмкіндігі кез-келген уақытта іскерлік өмірдің талабына айналады. Кәсіпорындар серіктестерімен және жабдықтаушыларымен қызметтестікті нығайту үшін оларға өз желілерінің бөлек сегменттерін ашады. Соған байланысты жаңа өнімді еңгізуге кететін уақыт үнемделеді және де клиенттерге қызмет көрсету жақсартылады.

Үлкен аймақты-бөлінген бірлескен желінің (мұндай желілерге мемлекеттік қажеттіліктерге арналған телекоммуникациялық желілер жатады) бір белгісі болып глобалды байланысты қолдану болып табылады. Кәсіпорындар филиалдарының бөлек локалды желілерін және де компьютерлердің алыстандырылған қызметкерлерінің орталық локалды желімен біріктіру.

Мекемелік немесе бірлескен желі құрудың дәстүрлі әдісі – қашықталған пайдаланушылар байланысы үшін, жалпы қолданылатын телефонды желілер және «желі-желі» байланыстарын ұйымдастыру үшін бөлінген арналар байланысын (көбінесе телекоммуникациялық операторлардан жалға алынған) қолдану. IP-желілердің қарқынды дамуы (ең бастысы Интернеттің) жаңа үрдісті туғызды – глобалды бірлескен байланысты құру үшін арзанырақ және рұқсат етілген дестелік желілерді тасымалдауды қолдану (бөлінген арналармен салыстырғанда).

Бірақта, мұндай қызығарлықтай және арзанырақ шешім – бұқаралық дестелік желі арқылы бірлескен деректерді тарату, мысалы Интернет арқылы – кез-келген кәсіпорын желісі қауіпсіздігі үшін қауіпті болады. Мемлекеттік билік пен басқару органдары үшін бұл тіпті қауіпті. Интернеттің көптеген пайдаланушылары үшін бірлескен желінің ішкі қорларына рұқсат болады және де құпиялы трафиктер қаскүнемдермен қаралу мүмкін. Одан басқа да кәсіпорындар кепілденген өткізгіштік қабілетпен бөлінген арналардан бас тартқаннан кейін Интернеттегі байланыс арналарының сипаттамаларымен, өнімділігі мен сенімділігіне байланысты міндетті түрде келісуі керек.

Бұл мәселелерді шешу үшін виртуалды жеке желілер VPN (Virtual Private Network) технологиясы қолданылуы мүмкін. Бұл технология жалпы қолданудың дестелік желілерінде қосылуды тоқтатып кепілденген өткізгіштік қабілетпен қорғалған арналарды пайдаланады. VPN дәстүрлі желілердегідей қосылуды ұйымдастыру бағасын сақтау кезінде қауіпсіздік пен жасырындықты қамтамасыз етеді. Сонымен қатар жалпы пайдаланатын желілерде. Осыдан, мұндай қызмет өзіне меншікті ресурстары жоқ кәсіпорындар мен мекемелерге, ең бастысы мемлекеттік билік органдарына және бюджетті мекемелерге үнемділігі мен рұқсаттылығына қажет болады.

VPN – бұл әдейіленген аппаратты немесе бағдарламалық құрылғылармен қашықталған локалды желілерді немесе жеке жұмыс орындарын біріктіру және де

транзитті трафиктің ақпараттық қауіпсіздігін қамтамасыз етуі және де оның ақпаратты дестелік таратумен бұқаралық желілердің үстінен туннелдеу.

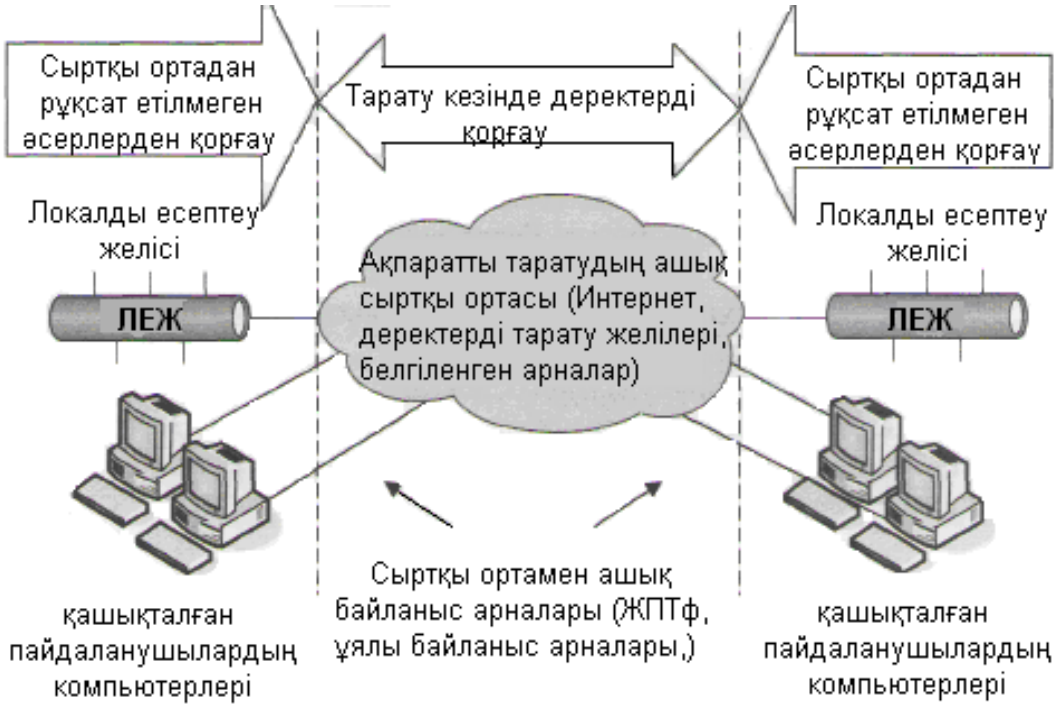
Локалды желілермен және жеке компьютерлердің арасында ақпараттың өзара әрекетесу қауіпсіздігі екі базалық есептеудің сапалық шешімін талап етеді 1.1 сурет көрсетілген. Мысалы, Интернет арқылы.

- локалды желілер мен жеке компьютерлердің бұқаралық байланыс арналарына қосылғандағы сыртқы орта жағынан рұқсат етілмеген әсерлерінен қорғану;
- ашық байланыс арналар бойымен таратылғанда ақпаратты қорғау.

Ақпараттармен алмасу кезінде қажет қауіпсіздік деңгейі кешенді ақпараттық-бағдарламалық, техникалық, ұйымдастыратын және криптографиялық қорғаныс тәсілдерін қолдану арқылы қамтамасыз етіледі және де ақпараттың қауіпсіздігін қамтамасыз етуі үшін қолданған әдістердің әсерін үздіксіз бақылауды жүзеге асыру. Қорғаныс тәсілдерінің кешені міндетті түрде қарастырылуы керек:

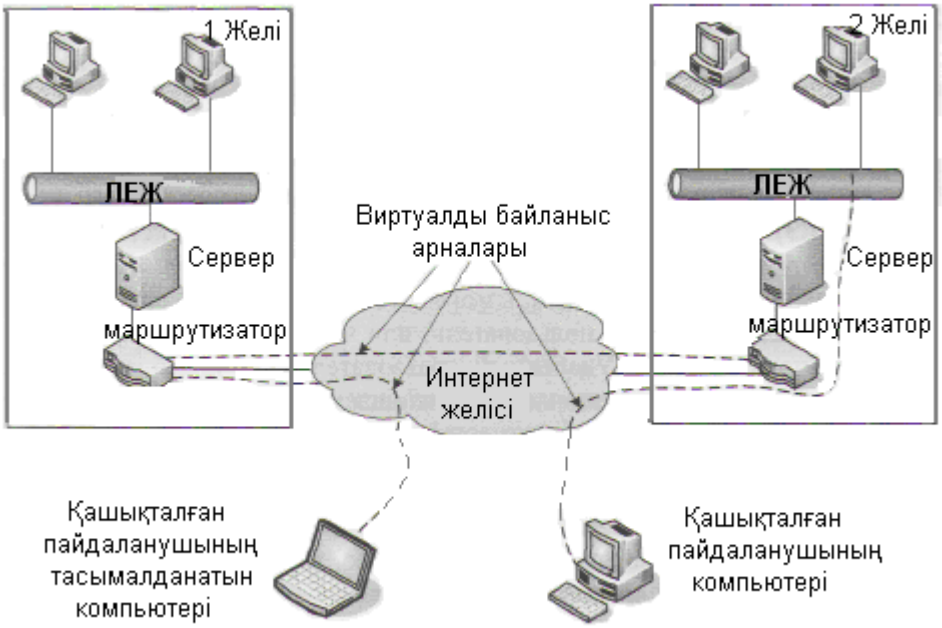
- ақпараттың жасанды алмасуын және жоғалуын, жойылуын тоқтату;
- тұлғаның, халықтың, мемлекеттің ақпараттық қауіпсіздік әсерлерін тоқтату;
- ақпараттың тұйықталуына, көшірмесі жасалуына, бұрмалануына түрленуіне жойылуына рұқсат етілмеген әсерлерді тоқтату.

Коммерциялық және коллективті рұқсат пунктерінің пайдаланушыларын, бюджетті ұйымдардың, мемлекеттік билік органдардың қосылуын қауіпсіздендіру және бұқаралық телекоммуникациялық желі арқылы кез-келген пайдаланушылардың жұмысын максималды қорғау, осы әдістерді қолдану арқылы жүзеге асырылады.



1.1 сурет– Ақпараттың өзара алмасу қауіпсіздігін қамтамасыз ету мәселелері

Ақпаратты таратудың ашық сыртқы ортасындағы деректерді таратудың жылдамдатылған ортасына бөлуге болады. Оның есебінде IP-желісін немесе Интернетті пайдалануға болады және де баяуырақ жалпы рұқсатталған байланыс арналарын, оның орнына телефонды желі арналарын пайдалануға болады. Локалды желілер мен қашықтатылған компьютерлерді біріктірудің ең қарапайым әдісі болып глобалды Интернет желісінің негізінде біріктіру болып табылады 1.2 сурет көрсетілген. [1]



1.2 сурет– Интернет негізінде виртуалды жеке желіні құру

Интернет негізінде виртуалды желілерді ұйымдастырудың біршама артықшылықтары бар:

- локалды желінің ресурстарына қашықталған рұқсатты кең көлемді қамтамасыз етеді. Ұялы пайдаланушылар жергілікті телефонды линиялардың бойымен, Интернет қызметтерін жабдықтаушылармен қосылуға мүмкіндік береді және осылай өзінің бірлескен желісіне кіреді;
- локалды желілерге қашықталған пайдаланушылардың рұқсатын ұйымдастыру кезінде модемді пулдердің қажет болу мүмкіндігі алынып тасталынады, ал дистанционды рұқсат трафигін кез-келген Интернет трафигі сияқты басқаруға болады;
- ашық сыртқы орта арқылы ақпараттар алмасуына кететін шығындар азаяды:
- локалды желілерді біріктіру үшін Интернетті пайдалану телефонды байланыс арналарын және басқа да глобалды желілерді, мысалы ATM немесе Frame Relay желілерін жалға алуға қарағанда біршама арзан. Желінің өзіндік құнын айтпай тұрғандағыға қарағанда;

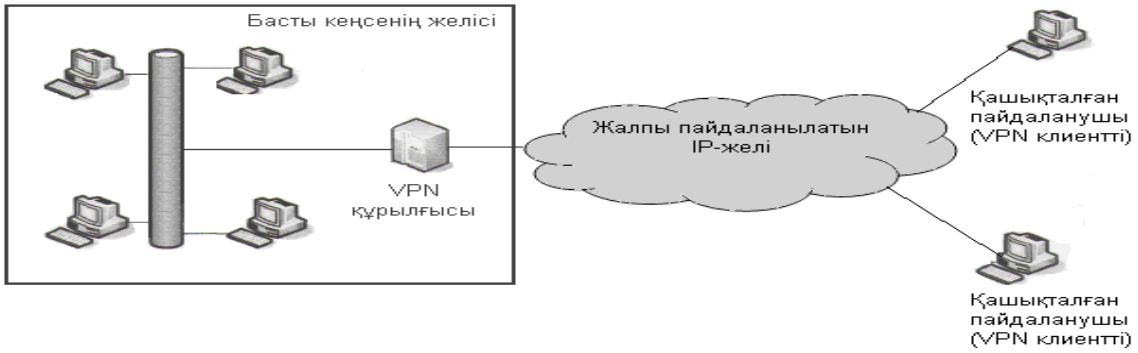
- қашықталған рұқсат кезінде қалааралық немесе халықаралық байланыс бойымен локалды желімен қашықталған пайдаланушылар Интернетке қосылады. Одан кейін сол глобалды желі арқылы өз мекемесінің желісімен байланысады.

Бірақта пайдаланушылар деректер ағыны үшін кепілденген сапалы қызмет және де олардың мүмкін рұқсат етілмеген кірісі мен толық көлемді жойылуынан тек қана бөлінген IP-желілері, ATM немесе Frame Relay жеке провайдерларға қатыстылар қамтамасыз ете алады. VPN қызметтерін көрсету үшін негіз ретінде бұқаралық ATM немесе Frame Relay желілерін қолдану Интернетке қарағанда бір маңызды артықшылығы, ал IP протоколы базасында желінің таралымдығы, олардың әмбебабтылығы мен тиімділігі бұл желілерді VPN құрудың көптеген мекемелер мен кәсіпорындар үшін жағымды негізі. Одан басқа да белгіленген IP-желілерінде (RSVP, DiffServ және MPLS QoS, Quality of Service) сияқты қызмет көрсету сапасын басқару технологиясы мен пртоколдар кең көлемде еңгізіліп жатыр.

1.2 VPN қызметтері

VPN технологиясы базасында төрт негізгі қызмет түрі жүзеге асырылады.

1. Қашықталған рұқсатымен виртуалды жеке желі (Remote Access VPN) 1.3 сурет көрсетілген. Бірлескен желі (орталық кеңсе немесе кәсіпорын бөлімшелері) мен қашықталған пайдаланушылар сегменттерінің арасында өзара әсерін қоғауды жүзеге асыруға мүмкіндік береді. Олар үйден (үй үсті пайдаланушы) бірлескен ресурстарға немесе тасымалданушы компьютерлер (ұялы пайдаланушы) арқылы қосыоуы мүмкін. Шарт бойынша қашықталған пайдаланушылардың статистикалық IP адресі болмайды және қорғалған ресурстарға VPN белгіленген құрылғылары арқылы емес, ал тікелей өзінің компьютері арқылы қосылады. Онда VPN клиентінің функцияларын іске асыратын бағдарламалық қамтамасыздандыру орнатылады.



1.3 сурет– Қашықталған рұқсатпен виртуалды жеке желі (Remote Access VPN)

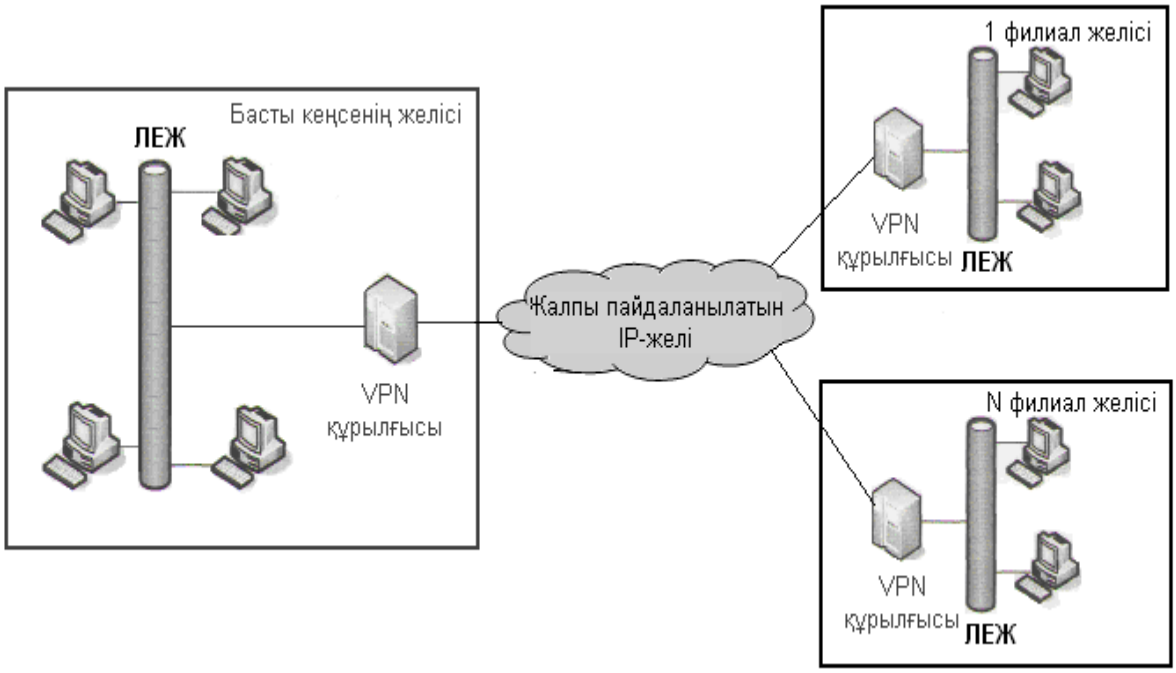
VPN бұл нұсқасы сервис-провайдерге қашықталған үй үсті қосылу мен ұялы қызметтердің бірлескен желіге қосылуын қамтамасыз етеді. Кәсіпорындар сервис-провайдер қамтамасыз ететін рұқсаттың инфрақұрылымымен қамтамасыз етілуі мүмкін. Керісінше өзіне меншікті сервер рұқсаттарын орнатпай, қоспай. Пайдаланушы жақын маңдағы болу нүктесіне (байланыс шығындарын төмендетіп) жалпы пайдалану телефонды желісі мен аналогты модем немесе ISDN желісінің базалық рұқсат көмегімен қосылады. Содан кейін пайдаланушының идентификаторы немесе терілген нөмір бойынша ол бірлескен желіге рұқсат алғысы келетін абонент сияқты таниды. Бұдан соң динамикалық режимде абонент пен бірлескен желі арасында қауіпсіз туннелі жүргізіледі (немесе ескі туннель қолданылады, егерде ол болған жағдайда). Осы туннель бүткіл желі бойымен бірлескен маршрутизаторға дейін PPP (Point-to-Point Protocol) протоколының сессиясын логикалық кеңейтеді. Ол үйдік шлюз деп аталады. Үйдік шлюз абонентті тануды және оған IP-адресті тағайындауды және басқа да парамметрлерді орындайды. Басқарылатын үйдік шлюзбен виртуалды желі рұқсаттарын құру нұсқалары бар. Бұл оқиға кезінде бірлескен тапсырыс беруші сервис-провайдерге үйдік шлюздің функцияларын береді. Бұл функциялар хостинг пен басқарудан, деректер базасын пайдалану хостингінен (RADIUS сервер) тұрады және де шифрлеу мен желіаралық экрандар көмегімен қауіпсіздікті қамтамасыз етеді.

Роумингпен виртуалды желі рұқсаттары жүзеге асырылуы мүмкін. Халықаралық роумингті пайдаланғанда дүние жүзінің кез-келген қаласынан бірлескен желіге рұқсат етіледі. Пайдаланушының бірлескен желісі қосылған байланыс операторымен роумингке өзара келісімі бар пайдаланушы кез-келген сервис-провайдердің желісіне қосылуы мүмкін. Ол қашықталған мен бірлескен желі арасында туннелді орнатуға мүмкіндік береді. Осы туннель кез-келген мәнді аралық оператор желісіне өту мүмкін, бірақта аралық сервис-провайдермен келісім шартқа отыруы керек жоқ.

2. Ішкі бірлескен виртуалды жеке желі, интранет (Intranet VPN) 1.4 сурет көрсетілген. IP-желісі ашық байланыс операторлар бойымен өзара әсерлесетін бір мекеменің бірнеше таратылған бөлімшелерін біріңгай қорғалған желіге біріктіруге мүмкіндік береді. Бүткіл дүние жүзінде осы нұсқа кең көлемде таралды. VPN интранеті Интернет немесе бөлінген IP-желісі арқылы кәсіпорындар бөлімшелері арасындағы байланысты орнатуды мекемелерге мүмкіндік береді. Осы технология GRE (Generic Router Encapsulation), L2TP (2 Деңгейде туннелдеу протоколы) немесе IPSec (IP Security) сияқты IP-туннелдеу әдістерін қолданады. «Нүктеден нүктеге дейінгі» принципі бойынша кеңселер арасындағы виртуалды жеке қосылуды ұйымдастыру үшін кеңсе маршрутизаторлары арасында осы туннелдеу орнатылады. Қауіпсіздік деңгейін жоғарылату үшін виртуалды арнадағы деректер кепілденген сапалы қызмет көрсетудің (Quality of Service, QoS) әртүрлі әдістері қолданылуы мүмкін. Сонымен әртүрлі қосымшалар үшін QoS әртүрлі деңгейлерін қолдану әдістері пайдалану мүмкін. Оларды дәстүрлі виртуалды желі технологиялар

көмегімен жүзеге асыруға болмайды. Мысалы, Frame Relay немесе ATM сияқты.

Масштабтау аумағында көрсетілген туннелдеу протоколдарының мүмкіндіктері шектелген. Себебі, кеңселер арасында туннелді конфигурациялауды қолмен жасау керек. Соңғы кездері VPN іске асыру үшін MPLS белгілеулері бойынша көппротоколды коммутация технологиялары кең көлемде қолданылып жатыр. Олар сервис-провайдерлерге виртуалды желілердің қызметтерін кеңейтумен, IP-VPN иілімдігімен, қызмет көрсету сапасымен және Frame Relay немесе ATM виртуалды желілер деңгейінде қауіпсіздік функцияларымен қамтамасыз етеді. MPLS технологиясын «таза» IP-желілерінің үстінен немесе IP-желілері мен ATM/ Frame Relay технологияларынан тұратын желілер үстінен орнатуға болады.

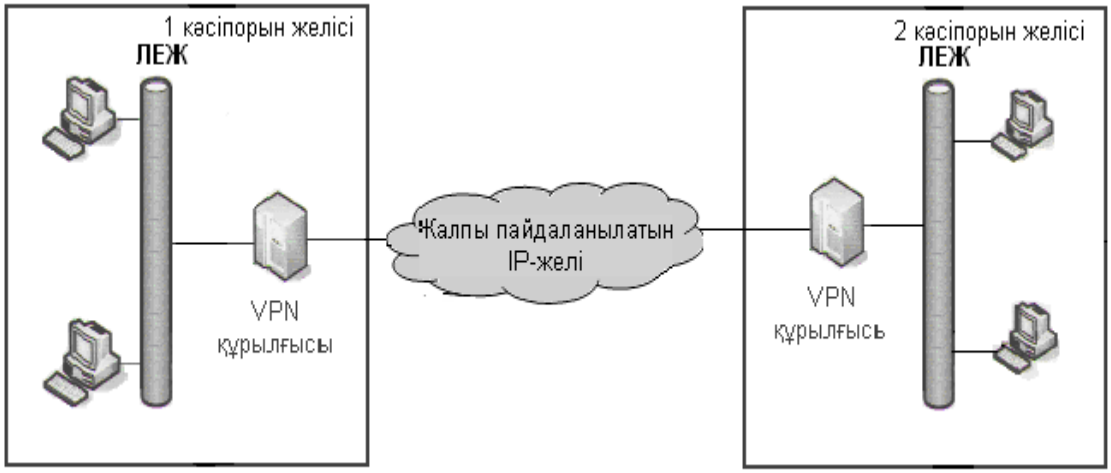


1.3 сурет– Ішкі бірлескен (Intranet VPN)

3. Бірлескендер арасындағы желі, экстранет (Extranet VPN) 1.5 сурет көрсетілген. Бір кәсіпорын желісінен келесі кәсіпорын желісіне тура рұқсатты қамтамасыз ететін қызмет түрі. Осылай іскери ынтымақтастық кезінде байланыс сенімділігін жоғарылатады. «Экстранет VPN» желісі ішкі бірлестік виртуалды жеке желілерге ұқсас, тек қана олар әртүрлі кәсіпорындардың бұқаралық IP-желісі арқылы өзара әсерлеседі. Мұндай кезде ақпаратты қорғау мәселесі маңызды орын алады. Бірнеше кәсіпорын бірлесіп жұмыс істеуді шешкен кезде де және бір-біріне өз желілерін ашқанда олардың жаңа серіктестіктері тек қана белгілі ақпаратқа рұқсатын ұйымдастыру керек. Бірлескендер арасындағы экстранет желісін құру мүмкіндігі, оларға кіретін соңғы нүктелеріне сәйкесінше VPN-ID идентификаторын белгілеуінше жүзеге

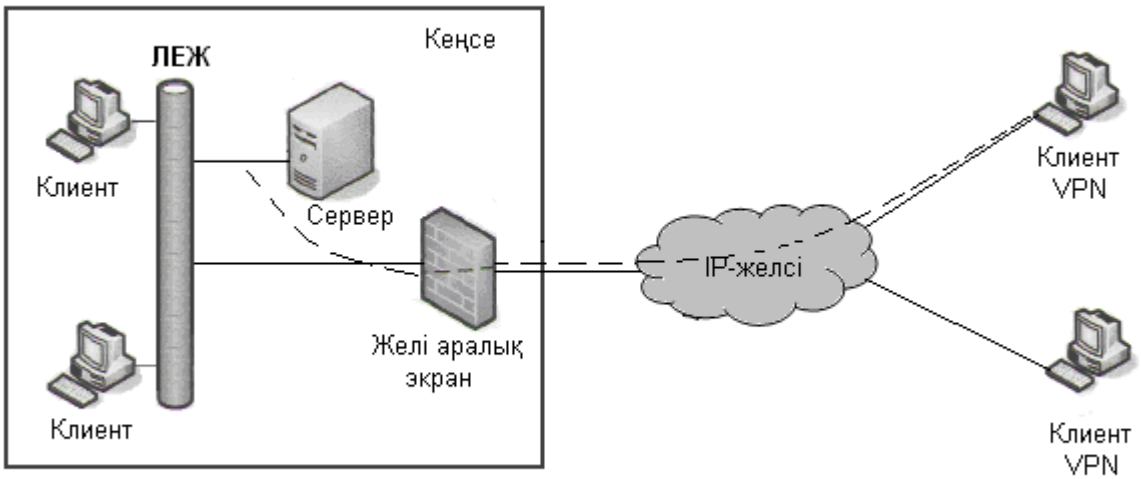
асырады. Ол нақты виртуалды желіге тиістілігін көрсетеді. Кәсіпорынның нақты бір кеңсесі бір уақытта жеке бірлескен виртуалды желіге және экстранетке кіруі мүмкін.

MPLS-VPN технологиясын еңгізу сервис-провайдерлердің пайдаланушыларға толық интегралданған рұқсатты ұсынады. Яғни жалпы тағайындалған байланысты, бір рұқсат арнасындағы экстранет желісі мен жеке желілерді қолдайды. Мұндай кезде жалпы рұқсатты Интернет желісі басқа VPN-ID (әдеттегіде VPN-ID 0) идентификаторын алады. Әртүрлі типті қосылулар, әртүрлі пайдаланушылар мен қосымшалар үшін қызмет көрсетудің әртүрлі деңгейдегі сапасы болу мүмкін. Осылай пайдаланушының жалпы рұқсаттағы, жеке, дауыстық байланыстағы барлық қажеттіліктерін қанағаттандыратын біртұтас рұқсат арнасы болады. «IP бойымен дауыс» (VoIP) технологиясының көмегімен дауысты хабарлар кеңселер арасында жеке виртуалды желілер арқылы таратылады, ал жалпы пайдалану телефондарына рұқсат сервис-провайдерлермен ұсынылған шлюздер арқылы іске асады.



1.5 сурет– Бірлескендер арасындағы желі (Extranet VPN)

4. «Клиент-сервер» (Client/Server VPN) 1.6 сурет көрсетілген. Бір бірлескен желінің екі қашықталған түйіндер арасындағы таратылған деректердің қорғанысын қамтамасыз етеді. Берілген нұсқаның ерекшелігі болып желінің бір сегментінде орналасқан түйіндер арасында VPN құрылады. Мысалы, жұмыс станциясы мен сервер арасында. Мұндай қажеттілік бір физикалық желіде бірнеше логикалық желі құру керек болған жағдайда туады. Мысалы, бір физикалық сегментте орналасқан серверлерге үндейтін бір кәсіпорынның әртүрлі бөлімдері арасындағы трафикті бөлуге қажет болған жағдайда. Бұл нұсқа виртуалды локалды есептеу желілеріне ЛЕЖ (VLAN) ұқсайды. Ол арналы деңгейден жоғары әсер етеді және де трафикті бөлу үшін оның шифрленуі пайдалынады.



1.6 сурет–«Клиент-сервер» VPN (Client/Server VPN)

Көптеген мамандардың айтуынша VPN үш маңызды технологиялардың ішіні кіреді. Оларды кәсіпорындар келешекте қолданайын деп жатыр. Оны енгізуге байланысты экономикалық тиімділігі бюджетті мекемелер, кез-келген кәсіпорындар үшін осы технологияның маңызы зор. Infonetics Research кәсіпорынның бақылауынша VPN қолданылатын кәсіпорындар «желі-желі» байланысы кезінде 20-дан 40% ресурстарды үнемдеуі мүмкін. Ал қашықталған пайдаланушыларды қосқан кезде 60-80% дейін үнемдеуі мүмкін.

1.1 кесте әртүрлі кәсіпорындардың VPN қызметтерінің қажеттіліктері көрсетілген.

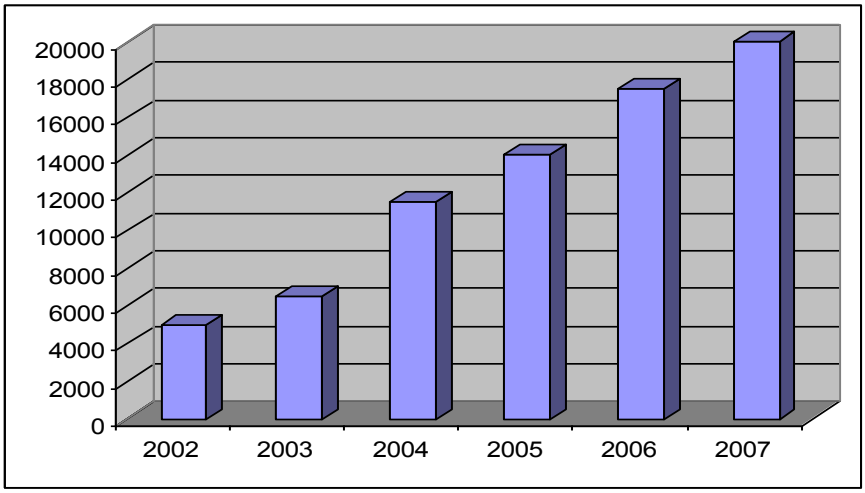
1.1 кесте – VPN пайдаланушылары және олардың әртүрлі VPN қызметтерінің қажеттіліктері

Қызмет түрі	Кіші кәсіпорындар	Орта кәсіпорындар	Үлкен кәсіпорындар	Өнідірістік кәсіпорындар
Қашықталған рұқсатпен VPN	Жаңа және мобильді серіктестіктерді қолдау үшін қажет	Арлардың өткізгіштік қабілетін жоғарылату мүмкіндігі	Орналасу географиясын кеңейту	Қашықталған жұмыс күші қолданылатын, барлық салалар үшін міндетті талап

1.1 кесте – жалғасы

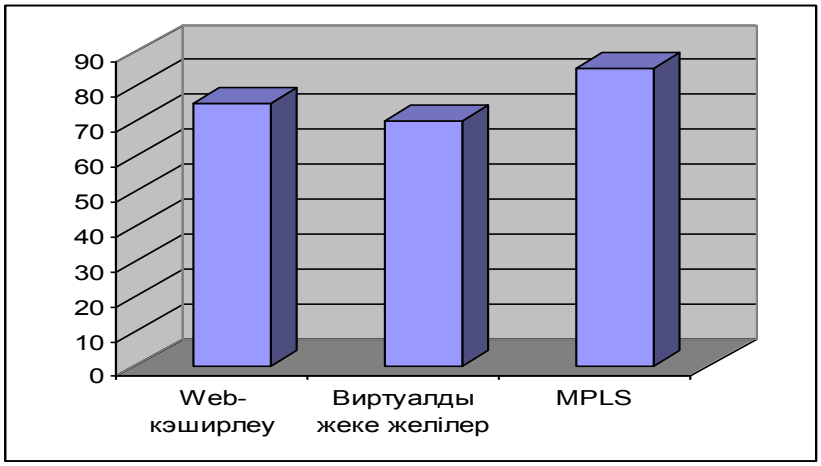
Қызмет түрі	Кіші кәсіпорында р	Орта кәсіпорындар	Үлкен кәсіпорындар	Өнідірістік кәсіпорынд ар
VPN Интранет	Глобалды желі функциялар ын атқарады (WAN)	Өзіне мешікті желіні құрмай филиалдарды тиімді жалғау	Үлкен аумағына қарағанда WAN алмастырмайды , үлкен емес немесе қашықталған кеңселер үшін	интранет VPN еңгізу бойынша денсаулық сақтау саласы алдыңғы орында
Қызмет түрі	Кіші кәсіпор.-р	Орта кәсіпорындар	Үлкен кәсіпорындар	Өнідірістік кәсіпорынд ар
VPN Экстранет	SSL түріндегі төменгі деңгейдегі қауіпсіздік, бастапқы даму деңгейлерінд е жеткілікті	(E-commerce) электронды коммерция приоритетті бағыт болып келеді	Серіктестер санын көбейткен кезде желі аралық VPNшығындар ды төмендетеді және басқаруды жеңілдетеді	экстранет VPN еңгізу бойынша бөлшек сауда мен денсаулық сақтау салалары алдыңғы орында
Қосымша сервистарме н VPN	Бөлек қызметтерді көрсетуге қарағанда, десте қызметтерін көрсету артығырақ	Күшейтілеген қорғаныс, әсерлі және коммуникацион ды қосымшаларды қолдану мүмкіндігі	QoS/SLA қолдауымен қорғаныстың күшейтілуі, VPN арқылы контентті тарату қажеттілігі (дистанционды басқару)	Осы салада болатын өзгерістер мен жаңа оқиғаларды білуге мүмкіндік береді.

Келесі ұрпақ мультисервисті желілерінде MPLS мен VPN технологияларын пайдалану болашақтығын соңғы жылдары берілген технологиялардың өсу қарқыны көрсетіп тұр. VPN технологиясына байланысты шетел сервис-провайдерлердің табысы мен бірлескен тапсырысшылардың шығынының анализі 1.7 сурет көрсетілген. [2]



1.7 сурет– Дүние жүзіндегі VPN кететін шығындар (АҚШ млн. долларда) (Ovum кәсіпорынының деректері)

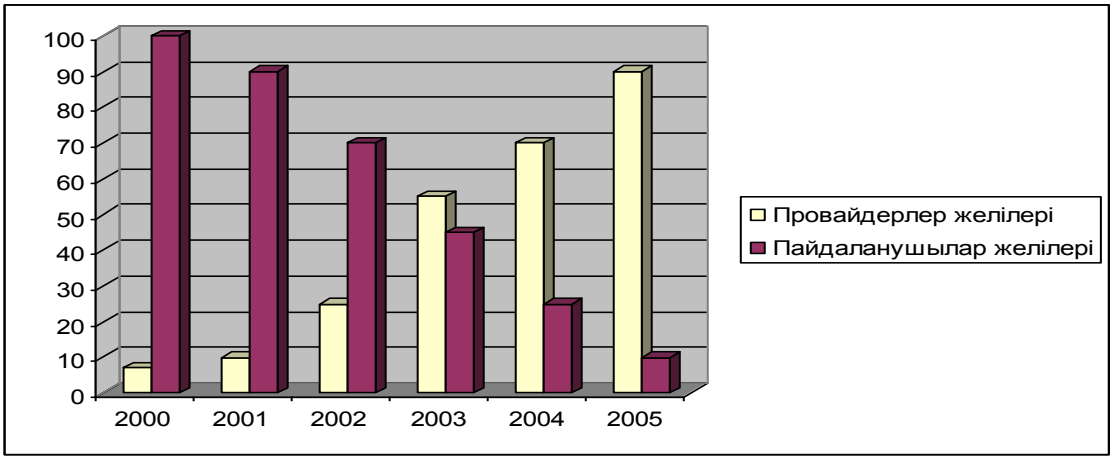
Infonetics кәсіпорынының деректерінде сервис-провайдерлер арасындағы MPLS технологиясының кең таралуы мен қадірленуі көрсетілген. Бұл технологияны VPN қызметтерін қолдау үшін негіз есебінде қарастырады. Осылай 83% респоденттер MPLS көмегімен виртуалды жеке желілерді құруды жоспарлайды 1.8 сурет көрсетілген.



1.8 сурет– VPN еңгізу бойынша европалық дәстүрлі байланысоператорларының жоспары (жалпы санынан процентте) (Infonetics кәсіпорынының деректері)

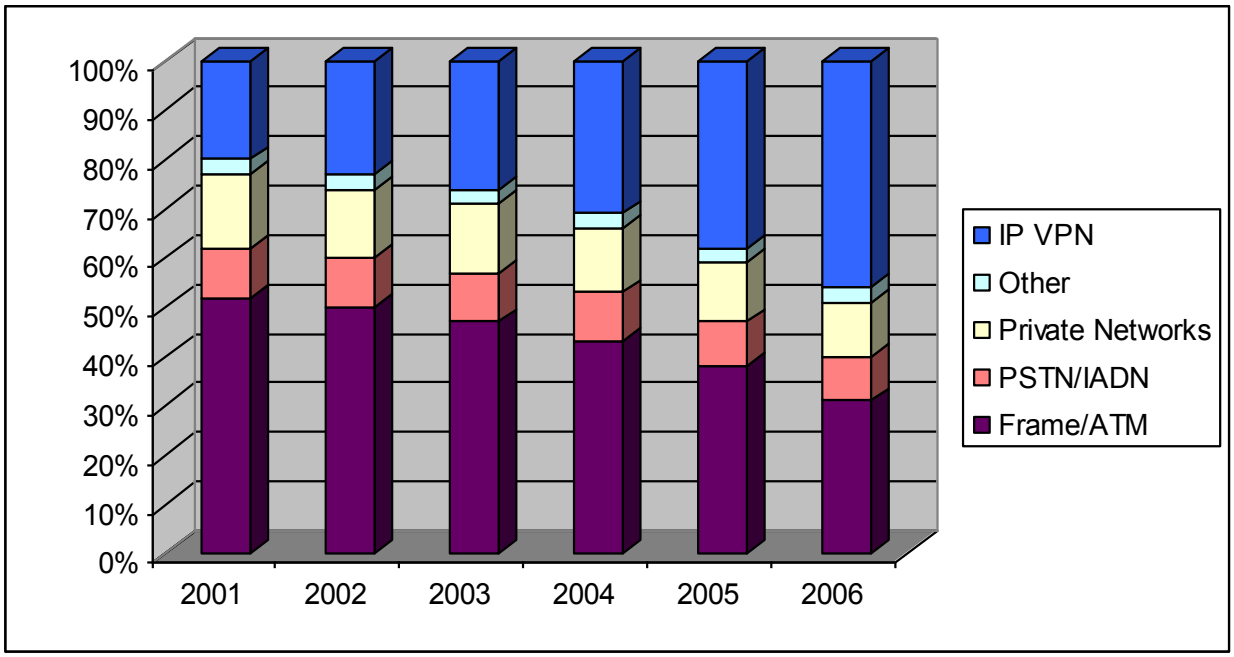
Cahners In-stat Group кәсіпорны виртуалды жеке желілерді операторларға аутсорсингке берілгендерін нарықтағы VPN ретінде ең көп таралғанын ескертеді 1.9 сурет көрсетілген. Соңғы пайдаланушылар кепілденген сапалы қызметті (SLA), желінің масштабтылықтығы мен

кепілдігін және VPN қызметтерінің кең таңдаулы тұрақты рұқсатын талап етеді. Осының барлығы көптеген кәсіпорындарды өзіне меншікті «үйлік» VPN желілерін сыртқы мамандармен қызмет көрсетілетін және орнатылатын жасайды.



1.9 сурет– Пайдаланушыларға тиісті VPN желілері мен провайдерлер желілерінің арақатынасы (Cahners ln-stat Group кәсіпорынының деректері)

АҚШ-та VPN желілерінің көп бөлігі ATM мен Frame Relay технологияларын пайдаланумен жүзеге асады. Бірақта, Yankee Group кәсіпорынның болжауымен жыл өткен сайын VPN жүзеге асыру үшін IP технологиясының орны өсуде 1.10 сурет көрсетілген.

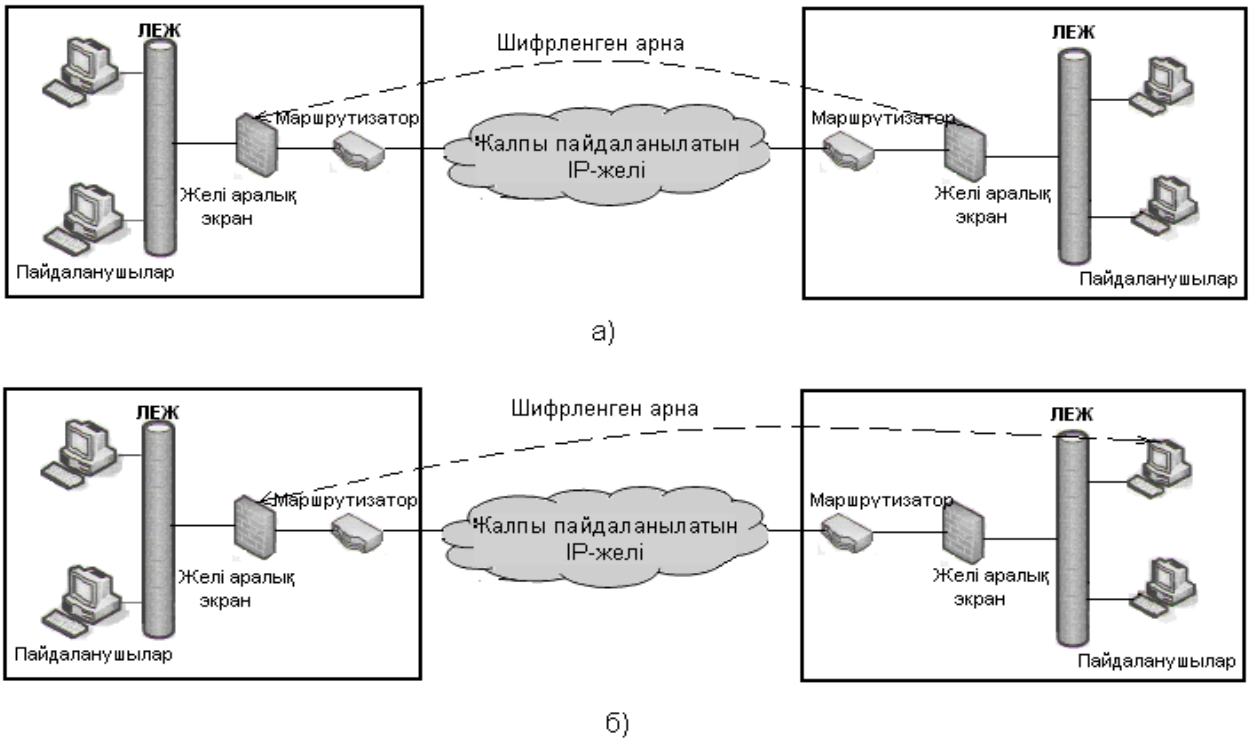


1.10 сурет– Солтүстік Американың трансдәстүрлі кәсіпорындарындағы деректерді тарату үшін қолданылатын технологиялардың арақатынасы (Yankee Group кәсіпорынның деректері)

1.3 Техникалық жүзеге асыру нұсқалары

VPN техникалық жүзеге асырудың бірнеше нұсқалары бар. Нұсқаны таңдаудың негізгі белгілеріне VPN құру қорларының өнімділігі мен олардың бағасы жатады. Виртуалды жеке желіні құру үшін аппаратты, бағдарламалық ресурстар немесе олардың комбинациясы қолданылуы мүмкін. Әдеттегіде аппаратты ресурстар өнімдірек, бірақта қымбатырақ болып келеді. Аппаратты шифрлеу әдістері бағдарламалыққа қарағанда қауіпсіздіктің жоғарғы деңгейін қамтамасыз етеді. Себебі деректерді тарату кезінде кідірістің үлкеюісіз үлкен разрядты кілттерді қамтамасыз етеді.Одан басқа, аппаратты ресурстар ең жақсы масштабтылықты қамтамасыз етеді. Дегенмен бағдарламалық ресурстардың ең басты артықшылығы бағасының төмендділігі. Төменде VPN техникалық жүзеге асырылуының негізгі нұсқалары көрсетіледі.

1.3.1 Желі аралық экрандар базасындағы. VPN. VPN көптеген жүзеге асырушылар желі аралық экрандарды (ЖЭ) VPN қосымша функциялармен қолдануға негізделген. (Firewall терминін ағылшын тілінен аударғанда - «брандмауэр» немесе «өртті қабырға»). Бұқаралық IP-желі арқылы басқа ЖЭ-мен 1.11 а суретінде көрсетілген, немесе VPN клиенттерімен шифрленген қосылу орнатылған кезде 1.11 б суретінде көрсетілген. [1]



1.11 сурет– Желі аралық экрандар базасындағы VPN жүзеге асыру: а – екі ЖЭ арасында, б – ЖЭ мен VPN клиенттері арасында

Желі аралық экрандар барлық кіріс пен шығыс трафиктерін фильтрлеу арқылы, тек қана авторланған деректерді өткізу арқылы сыртқы желіден ішкі

желіге бақылау рұқсат механизмін жүзеге асырады. Көптеген желі аралық экрандар туннелденген және шифрленген деректерді қамтамасыз етеді. Мұндай кезде бағдарламалық қамтамасыздандырудың желі аралық экранына шифрлеу модулі жалғанады.

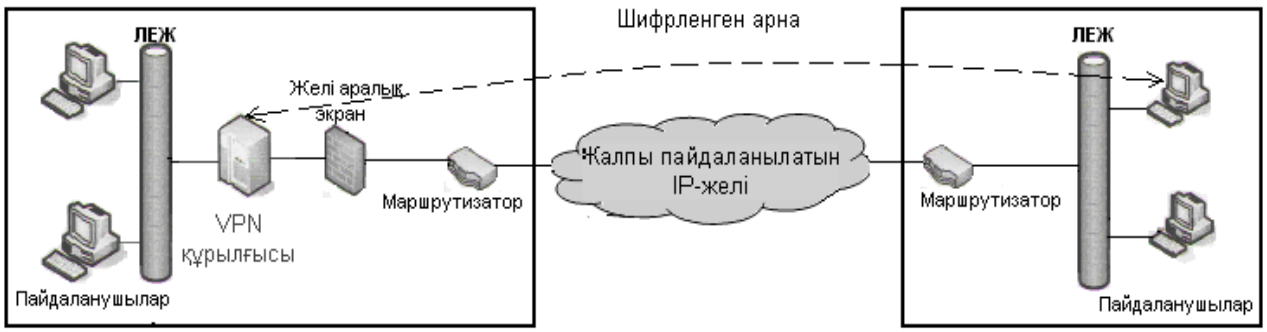
Бұл шешімнің негізгі артықшылығы бар қорғаныс қорларын әкімшілік ету сапасын жоғарылату болып саналады. Әдістің кемшілігі – желі аралық экран жұмыс істейтін ақпаратты қамтамасыздандырудан өнімділігінің тәуелділігі. Сондықтан желі аралық экрандарды дербес компьютер базасында жүзеге асыру аз көлемді ақпаратты таратуға арналған кішкентай желілер үшін қолданылады. Одан басқа желі аралық экрандар базасындағы VPN жүзеге асырудың кемшілігіне авторланған пайдаланушылардан және жаңа желілік сервистерден қорғаныстың болмауын жатқызуға болады.

1.3.2 Маршрутизаторлар базасындағы VPN. Қорғалған арналарды құру үшін VPN құрудың басқа әдісі маршрутизаторларды пайдалану болып саналады 1.12 сурет көрсетілген. Локалды желіден шығатын барлық ақпарат маршрутизатор арқылы өткендіктен маршрутизаторға шифрлеу есептерін қойған мақсатқа сәйкес орындалады.

1.12 сурет– Маршрутизаторлар базасындағы VPN

Бұл әдістің негізгі артықшылықтарына рұқсатпен басқару бойынша интегралданған әкімшіліктендіру функцияларының ыңғайлылығын жатқызуға болады. Басты кемшілігіне трафикті шифрлеу функциясын қосқаны үшін маршрутизатордың өнімділгіне жоғарғы талаптың болуы. Виртуалды желіні құрудың бұл әдісін бөлінген филиалдар желісі бар мекемелерде пайдаланған орынды.

1.3.3.Бағдарламалық қамтамасыздандыру базасындағы VPN. VPN құрудың келесі әдісі толық бағдарламалық шешім болып келеді. Мұндай әдісті жүзеге асыру кезінде маманданған бағдарламалық қамтамасыздандыру қолданылады. Ол белгіленген компьютерде жұмыс істейді және көптеген жағдайларда proxy-сервер ролін орындайды. Мұндай бағдарламалық қамтамасыздандыруы бар компьютер желі аралық экран артында орналасуы мүмкін 1.13 сурет көрсетілген.



1.13 сурет– Бағдарламалық қамтамасыздандыру базасындағы VPN

1.3.4 Желілік операциялық жүйе базасындағы VPN**.** Операциялық жүйе базасында құрылған виртуалды жеке желілерді қорғалған арналар инфроқұрылымын құруға ыңғайлы және арзан болып келеді. Windows NT/2000 мен UNIX жүйелер тұқымдастары VPN құрудың операциялық жүйелер арасындағы ең көп таралғандары.

Windows NT базасында құрылған VPN жұмысында дестелерді шифрлеу үшін Microsoft кәсіпорынының Point-to-Point Encryption қосылу кезінде алынған 40 және 128 битті кілтімен стандартты емес протоколы қолданылады. Бұл жүйенің кемшілігі деректердің бүтіндігін тексерудің жоқтығы мен қосылу кезінде кілттерді алмастыру мүмкіндігінің болмауы саналады: Артықшылығы Windows-пен интеграция жеңілдігі мен төменгі бағасы.

Windows 2000 базасында VPN құру үшін IP-Sec пртоколымен үйлестірілген PPTP мен L2TP (Layer 2 tunneling protocol) протоколдары қолданылады. Windows 2000 ортасында VPN қосылуларын локалды есептеу жүйесі бойымен ұйымдастыруға болады. Сонымен қатар коммутация қосылу үстімен жасайды. Еңгізілген Dial-Up networking бағдарламалық қамтамасыздандыру бірлескен желіге қашықталған рұқсат үшін қосылуды ұйымдастыруға мүмкіндік береді. IP-Sec шлюзіне қосылған жүйелерге желілік адрестерді динамикалық тағайындайды. UNIX жүйесінде IP-Sec протоколын ұстап тұрады. Шифрлеу алгоритмі ретінде DES және 3DES қолданылады. Аутентификация алгоритмі ретінде MD5 (Message Digest 5) және SHA (Security Hash Algorithm) қолданылады.

Операциялық жүйе базасындағы виртуалды жеке желілерді ұйымдастыру әдісінің кемшілігі операциялық жүйенің жеткілікті қауіпсіздігін қамтамасыз етпеуі. Microsoft кәсіпорынның өнімдері үшін бұл өте өзекті мәселе.

1.3.5 Арнаулы аппаратты құралдар базасындағы VPN. Арнаулы құрылғылар базасындағы құру нұсқасы трафикті шифрлеумен жоғарғы өнімділікті талап ететін желілерде пайдалану мүмкін 1.14 сурет көрсетілген. Әдеттегіде арнаулы құралдар ретінде, бөлек аппаратты құрылғы ретінде жүзеге асырылған VPN шлюздері алынады.

1.14 сурет– Маманданған аппаратты құралдар базасындағы VPN

Апаратты құралдар базасындағы VPN құру әдісінің негізгі артықшылығына ыңғайлылығы мен инсталляция қарапайымдылығын және де трафикті шифрлеудің жоғарғы өнімділігін жатқызуға болады. Басты кемшілігіне берілген құрылғы түрінің қымбаттылығы.

1.4 VPN құру сұлбалары

Виртуалды жеке желілерді құрған кезде VPN қызметтерінің провайдерлері мен мекемелердің арақатынасы үлкен орын алады және де олардың арасындағы VPN құрылғыларын эксплуатациялау мен конфигурирлеу функцияларын тарату. Мекемелер ретінде әртүрлі бірлескен пайдаланушылар тұспалданады. Мысалы, мемлекеттік билік органдары, бюджетті мекемелер және де әртүрлі коммерциялық кәсіпорындар.

Виртуалды желілердің қорғалған арналарын құрған кезде VPN құралдары провайдер желісінде және пайдаланушы желісінде де орналасуы мүмкін. Осы факторларға тәуелді виртуалды желілерді құрудың үш сұлбасы бар:

- бірлескен сұлба – VPN барлық құралдары мекеме желісінде орналасады;
- провайдерлік сұлба – VPN барлық құралдары провайдер желісінде орналасады;
- аралас сұлба – VPN құралдарының бір бөлігі мекеме желісінде орналасады, ал қалған бөлігі – мекеме желісінде орналасады.

Төменде осы үш сұлба толығымен қарастырылады.

1.4.1 Бірлескен сұлба. Бірлескен немесе пайдаланушы сұлбасында мекеме жалпы пайдаланылатын IP-желісі бойымен таратылатын деректерді дербес қорғайды, өзінің желісі мен өзінің аумағында VPN-шлюздері мен VPN-клиенттерін орналастырады 1.15 сурет көрсетілген. Мекеме толығымен өзіне қауіпсіздікті қамтамасыз ету мәселесін алады, ал провайдерден тек қана кепілденген немесе кепілденбеген өткізгіштік қабілетті алады. Локалды желілер көбінесе VPN-шлюздерінің көмегімен қорғалады. Мұндай шешім тиімдірек. Себебі, бір шлюз оның артында орналасқан бірлескен желінің барлық түйіндерін қорғайды.

Бір мекеменің әртүрлі локалды желі шлюздерінің арасында қорғалған арналар құрылған кезде VPN технологиясы қорғалған интражелілер қызметтерін жүзеге асыру үшін пайдалану мүмкін. Локалды желінің әкімшісі

VPN-шлюзін төмендегідей бағыттауы керек. Ол қорғалған арналарды қосуды тек қана өзінің мекемесінің нақты шлюздерімен (интражелі аумағында) және құпиялы ақпаратпен алмасатын филиалдар (экстражелі аумағында) арасында ұйымдастыруы керек.

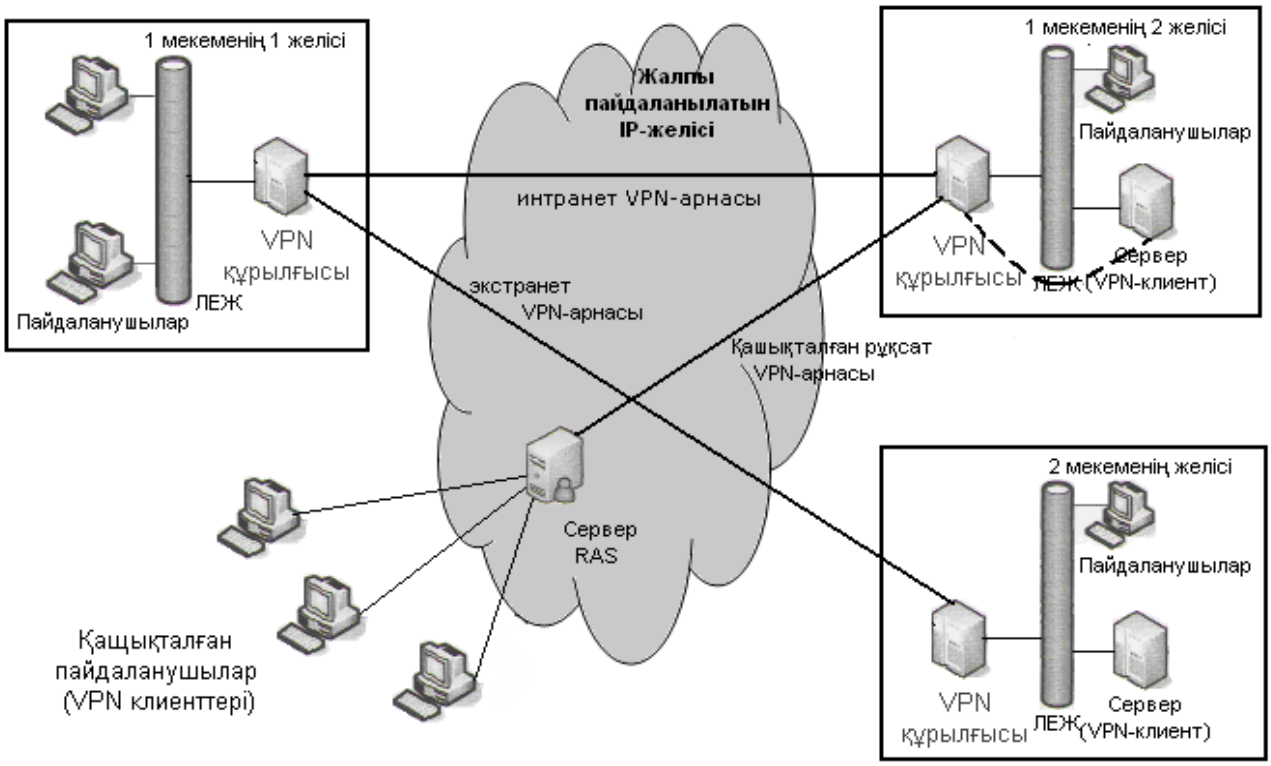
Мекеменің ұялы және қашықталған бөлек компьютерлер қорғалған байланысты құру үшін VPN-клиенттеріне бағдарламалық қамтамасыздандыруды дербес ұйымдастыруы керек. Өзінің VPN-клиенттерінің көмегімен бұл компьютерлер өз мекемесінің VPN-шлюздерімен қашықталған рұқсатты, қорғалған арналарды орната алады.

Кейбір жағдайларда локалды желінің серверлерінде VPN-клиентінің бағдарламалық қамтамасыздандыруы орнатылады. Мысалы, 1 мекеменің 2 желісінде сервер- VPN-клиент 1.15 сурет көрсетілген. Осылай нақты түйіндер мен қосымшалар үшін бірлескен желінің ішінде ақпараттың құпиялылығын қамтамасыз етуі керек болған жағдайда жасалынады. Осындай міндетті шлюз орындай алмайды. Себебі, қорғалған арна онымен біткеннен кейін барлық ақпарат дешифрленген түрле таратылады. Сондықтан араласқан нұсқада болуы мүмкін. Қашықталған пайдаланушы екі қорғалған арнаны орнатқан кезде – желіні толық қорғайтын біреуін шлюзбен, ал екіншісін – желінің ішінде нақты сервермен. Бірінші қорғалған арна артық көрінгенімен, одан басқа таратуға болмайды. Себебі, деректер шлюз арқылы желіге өте алмайды. Артықшылығының тағы бір көрінісі әрбір VPN компьютері дестелерді шифрлеу мен аутентификация операцияларын орындау үшін кететін қосымша есептеу жүктемесін жүргізеді. Ол оның негізгі функцияларын баяулатады. Сондықтанда VPN-клиенті қашықталған қорғалған рұқсат үшін немесе ерекше маңызды дербес байланысты құру үшін қолданылады.

Бірлескен сұлбаның артықшылықтарына жатқызуға болады:

- Бірлескен желі бойынша мәселе бойымен VPN әкімшілігінің толық бақылауы. (Қорғалған арна протоколдарын таңдау, тек қана нақты абоненттермен немесе желілермен өзара әсерді түзету парольді ауыстыру стратегияларын таңдау және т.б.);
- Қосымшалар үшін қорғалған арнаның өткізгіштік қабілетіне таралуды толық бақылау. Мұндай кезде провайдер транспортты қызмет көрсету сапасына кепілдеме бергенде, пайдаланушы шығыс трафигі үшін басымдылықты өзі белгілейді. Себебі, провайдер шифрленген дестелерді алғанда ешқандай белгілеулер қалмайды, содан ол дифференциалды қызмет көрсете алмайды;
- Қауіпсіздік «соңынан соңына» іске асырылады: пайдаланушының орналасқан орнына белгіленген жерге дейін. Деректер пайдаланушының локалды желісінен шыққанға дейін қорғалады. Өте құпиялы деректерді таратқан кезде, мұндай қорғаныс қажет болу мүмкін.

VPN құрылғыларының бағасының қымбаттылығы негізгі кемшілігі және де қолданылған сұлбаның орталықтанбағаны үшін олардың қызмет көрсетілуі мен VPN масштабтылығының төменгі дәрежесі.



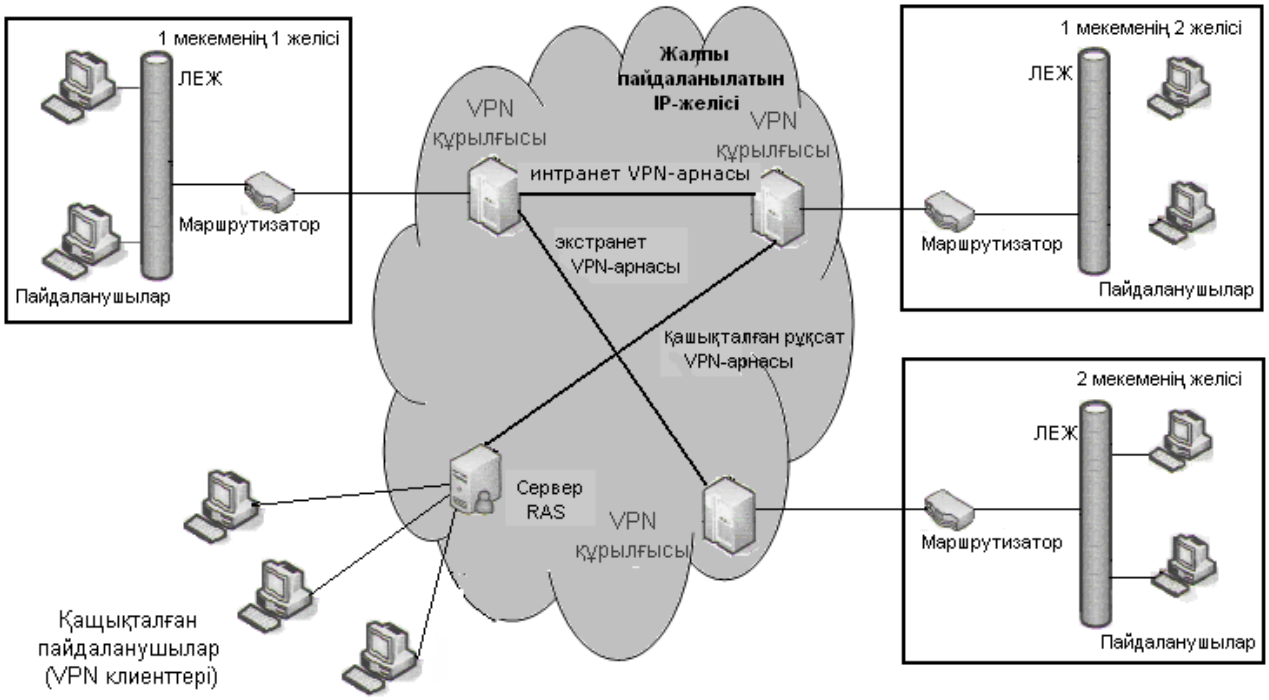
1.15 сурет– VPN құрудың бірлескен сұлбасы

VPN кеңейткен кезде әр жаңа қосылған филиалда жаңа VPN-шлюзін орнатып және конфигурирлеу керек, ал жаңа қашықталған компьютерде – VPN клиенттік бағдарламалық қамтамасыздандыру керек. Провайдердің қызметтерін пайдаланғанда барлық қорғалған арналар оның бірнеше шлюздері арқылы өтеді. Сондықтанда жаңа филиалды немесе қашықталған пайдаланушыны қосқанда аз материалды және әкімшлік шығындарды қажет етеді. Себебі, бар шлюздерге кішкене конфигурациялық өзгертулер енгізіледі.

1.4.2 Провайдерлік сұлба. Провайдерлік сұлбаны қолданғанда виртуалды жеке желі провайдер құралдарын қолдану арқылы жүзеге асырылады 1.16 сурет көрсетілген. Провайдер өзінің желісінде VPN қызметін пайдаланып клиенттер үшін жалпы пайдаланылатын ішкі желінің қорғалған арналарын жасайтын VPN-шлюздерін орнатады. Берілген сұлба провайдер желісінің әкімшісімен орталықтанған басқарумен жақсы масштабталатын және тиімді шешім болып саналады.

Бірлескен желінің (автономды сияқты, локалды желілерге біріктірілген) компьютерлер үшін қорғалған арна мөлдір. Осы ақырғы түйіндердің бағдарламалық қамтамасыз етуі өзгертулерсіз қалады. Ал пайдаланушыда өзінің VPN-шлюзін қабылдау, конфигурирлеу мен қолдау қажеттілігі жойылады. Провайдерлік сұлбаны жүзеге асыру кезінде бірлескен желінің VPN әкімшісі мекеменің интражелі мен экстражелісіне кіретін адрестер тізбегін провайдерге ұсынуы керек. Пайдаланушыларды аутентификациялау үшін және бірлескен желінің құралдары үшін деректерді ұсынуы керек.

Берілген сұлбаның иілгіштігі қорғалған арналарға жаңа пайдаланушыларды олардың орналасу орнына тәуелсіз оңай қосу мүмкіндігі. Бұл экстражеліге қосқанда пайдалы. Әр арнаның соңында VPN құралдарын индивидуалды конфигурирлеудің орнына берілген мекеменің VPN-шлюзіне және серіктестік мекемесінің провайдеріне өзгертулер енгізіледі. Мұндай кезде екі провайдер бір-біріне сәйкес VPN құралдарын пайдалануы керек. Берілген сұлбаның кемшіліктері қорғаныстың төменгі сенімділігінде көрінеді: біріншіден, жалпы пайдаланылатын желіге рұқсат арналары қорғалмайды, екіншіден, пайдаланушы толығымен провайдердің адалдылығына толығымен тәуелді болады. Жалпы пайдаланылатын IP-желі – көптеген кәсіпорындар мен мекемелердің әкімшлік бақылауында болатын желілердің жиынтығы 1.16 сурет көрсетілген. Егер де VPN қызметтерін А провайдері көрсететін болса, ол өзіне меншікті IP-желісінің магистральді бөлігін басқарады 1.17 суретте көрсетілген. Онда оның аумағында провайдер өзінің клиенттеріне IP-желі құралдарын қолданбай таратылатын деректердің қауіпсіздігін қамтамасыз етеді және де жалпы пайдаланылатын IP-желісімен өзінің желісінің қосылу нүктелерінде VPN-шлюздерін орнатады. Сондықтанда интражелі мен экстражелі клиенттер трафигі бір А провайдерінің магистралды желісі арқылы өткенде, ол VPN қорғалған арналарын қолданбай қызмет көрсетеді. Тек қана бұқаралық IP-желісі арқылы бір провайдердің желілерін қосу керек болған жағдайда немесе әртүрлі провайдерлерге жалғанған мекемелер үшін экстражеліні құру керек болған жағдайда VPN технологиясы пайдаланылады.

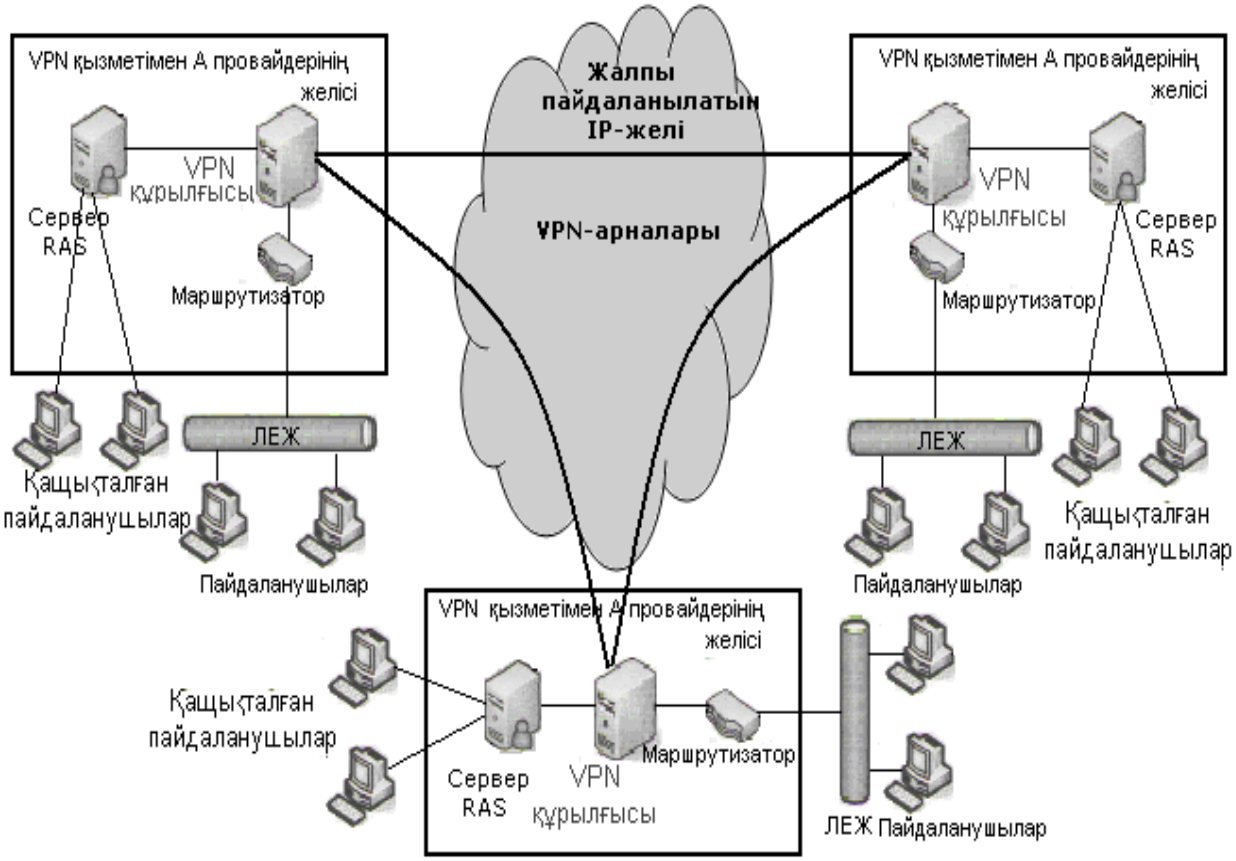


1.16 сурет– VPN құратын провайдерлік сұлба

Пайдаланушының көз-қарасымен VPN құру бойынша провайдерлік сұлбаның артықшылығына қымбат және күрделі VPN-құрылғыларын сатып

алу мен қызмет көрсету қажет еместігі. Кемшілігіне пайдаланушының провайдерге құпиялы ақпаратты тапсыру қажеттілігі жатады (парольдармен, кілттерді). Және де ескеру қажет, пайдаланушы мекемесінің орны мен провайдер құрылғысының арасындағы аумақ, глобалды желіге рұқсат арнасымен және VPN-провайдері мен рұқсат провайдерінің арасындағы аралық арналар қорғалмаған.

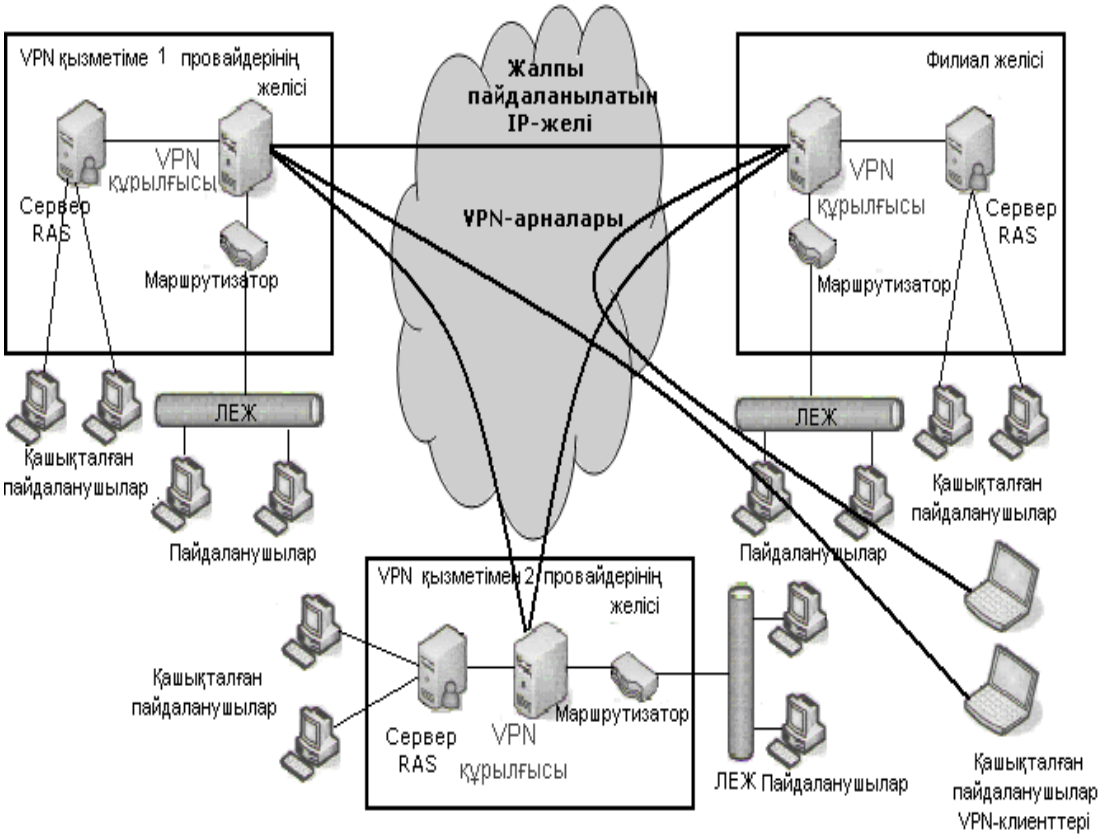
Провайдердің көз-қарасымен берілген сұлбаның артықшылығына VPN жоғарғы дайындығын қамтамасыз етуі. Ол провайдерлік класстағы құрылғыларды пайдалануы, заказ берушіге желідегі мәселелерді шешу үшін қызмет етушінің шығуысыз шешуі, пайдаланушы қосымшалары үшін қызмет көрсетудің дифференциалданған сапасын көрсету мүмкіндігімен VPN-қызметтерін интеграциялауы.



1.17 сурет– Провайдердің өзіне меншікті магистралімен VPN құратын провайдерлік сұлба

1.4.3 Аралас сұлба. Аралас сұлбаны қолданған кезде VPN-құралдары провайдер желісінде де, бірлескен желіде де орнатылады. VPN құру үшін мекеме бір провайдердің қызметтерін пайдаланатын болса, бірақта басқа провайдерлер желілері арқылы жалпы пайдаланылатын IP-желілеріне қосылған бірнеше желілер мен қашықталған пайдаланушылары бар болған

жағдайда орынды. Мұндай кезде мекемеге басқа провайдерлердің қызметтеріне бет бұратын қашықталған пайдаланушылардың компьютерлері мен желілерінде өзіне меншікті VPN құралдарын орнату керек болады 1.18 сурет көрсетілген. Бұл нұсқа алдыңғы нұсқаның артықшылықтары мен кемшіліктеріне ие.



1.18 сурет–VPN жүзеге асырудың аралас сұлбасы

1.5 VPN жабдықтарын желіде орналастыру нұсқалары

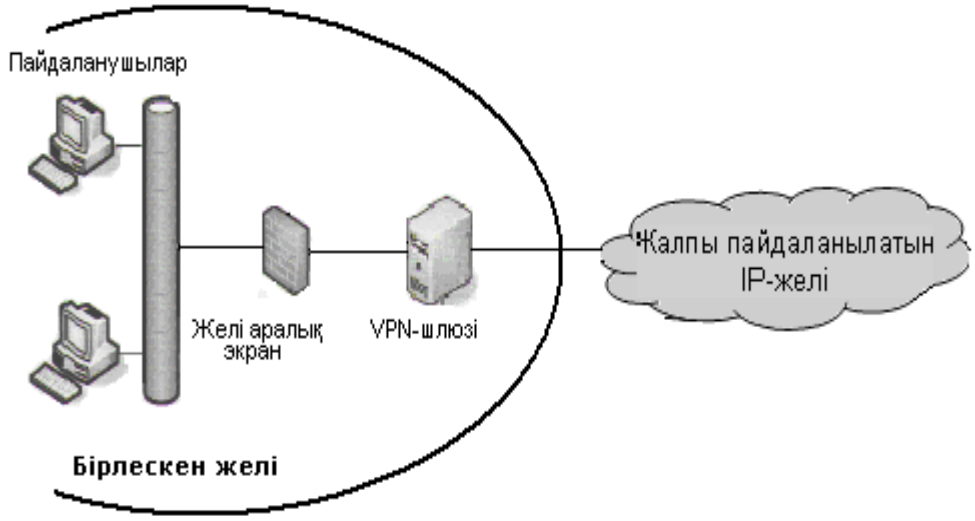
VPN тәжірибелік тұрғыда жүзеге асыру кезінде ен басты мәселе желіні қорғайтын басқа құрылғылармен салыстырғандағы VPN-құралдарының тиімді орналасу орнын анықтау. Шарт бойынша, VPN құру кезінде әкімші бірлескен желінің қауіпсіздігін қамтамасыз ету үшін онда басқа қорғаныс құрылғысының болуымен қақтығысады (көбінесе ол желі аралық экран немесе осы функцияны орындайтын фильтрлейтін маршрутизатор). Мұндай кезде желі аралық экран немесе VPN-шлюзін орналастыру мәселесі туады. Желі аралық экран мен VPN-шлюзінің функцияларын сәйкестендіру осы мәселені шешеді, бірақта бір бөлігін. Біріншіден, бұл тенденция абсолютті емес және бәсекелестері бар, екіншіден, қазіргі кезде желі аралық экран функцияларысыз VPN-шлюздерінің және желі аралық экрандар VPN-шлюздерісіз көптеген түрлер шығарылады және шығарылып жатыр.

VPN-шлюзі мен желі аралық экранның өзара орналасу нұсқаларын таңдау кезде бірнеше факторларды ескеру қажет. Біріншіден, шифрленген дестелер негізінде желі аралық экран желілік рұқсатты басқара алмайды. Екіншіден, жалпы пайдаланылатын желінің қауіп-қатерінен VPN-шлюз өзі қорғанысты қажет етеді. Үшіншіден, шлюзбен және желі аралық экранмен жасалынған байланыстар конфигурациясы жалпы пайдаланылатын IP-желімен бірлескен желінің қосылу сенімділігі әсер ету мүмкін.

Төменде тәжірибеде жиі кездесетін VPN-шлюзі мен желі аралық экранның өзара орналасу орнының нұсқалары көрсетілген

Шлюзді желі аралық экран алдында орналастыру

Шлюзді желі аралық экран алдында орналастыру кезінде шлюз арқылы толық трафикті тарату керек: ашық және шифрленген 1.19 сурет көрсетілген. Мұндай кезде желі аралық экран барлық трафикті өңдеумен жүктеледі. Алдын-ала шифрленген деректердің фильтрациясы шлюзбен дешифрленгеннен кейін орындалады. Мұндай сұлбаның кемшілігіне – жалпы пайдаланылатын желі жағынан барлық шабуылдар үшін шлюздің ашықтығы (Ол транзитпен шифрленген емес трафикті өзі арқылы өткізу керек, осындай трафиктердің көмегімен бірлескен желіге шабуыл жасалынады).

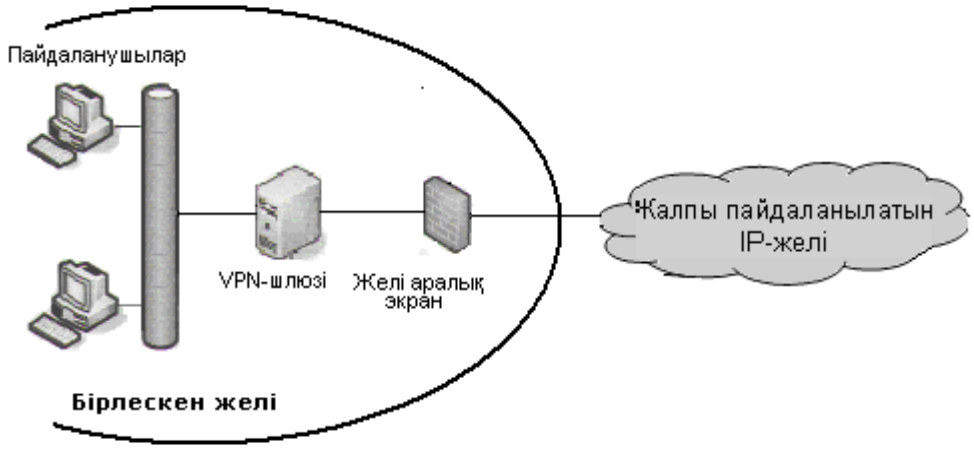


1.19 сурет– Шлюзді желі аралық экран алдында орналастыру

Шлюзді желі аралық экран артында орналастыру

Шлюзді желі аралық экран артында орналастыру кезінде ол шабуылдардан соңғы қорғалады 1.20 сурет көрсетілген. Бірақта, бірлескен желінің әкімшісі желі аралық экранды шифрленген трафикті жүргізетін, дестелерді өткізетіндей конфигурирлеуі керек. Шлюз жалпы пайдаланылатын желіден шифрленеген және шифрленбеген трафиктерді қабылдауы керек. Бірақта оның қауіп-қатері төмен, себебі шифрленбеген трафик алдын-ала желі аралық экранмен өңделеді. Шлюзді желі аралық экран алдында орналастырған

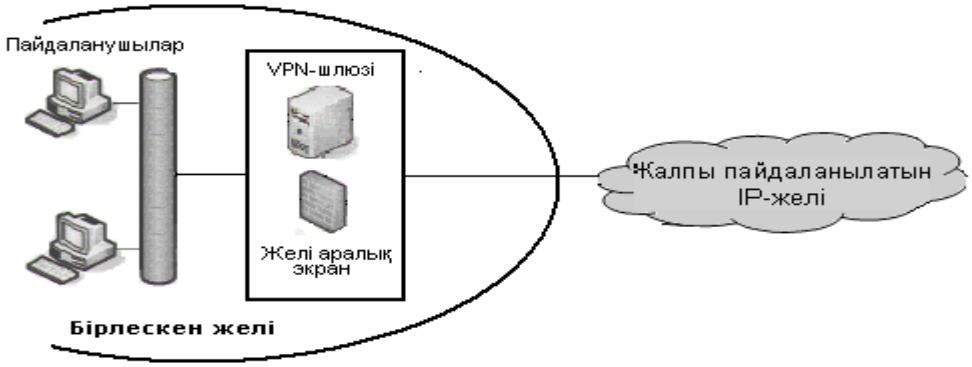
нұсқа сияқты, мұнда жалпы пайдаланылатын IP-желімен бірлескен желінің байланысын резервілеу болмайды.



1.20 сурет– Шлюзді желі аралық экран артында орналастыру

Шлюз функцияларын желі аралық экран ішінде жүзеге асыру

Мұндай шешім желілік компоненттермен басқарумен және әкімшіліктендіруді консолидирлеу мүмкіндігінің болуымен жағымды 1.21 сурет көрсетілген. Бірақта, бір құрылғыда маршрутизация, рұқсатпен басқару және оқиғаларды тіркеу операцияларын еңгізу қиынға соғады. Сондықтанда, VPN функцияларын бөлек орындау тиімді.

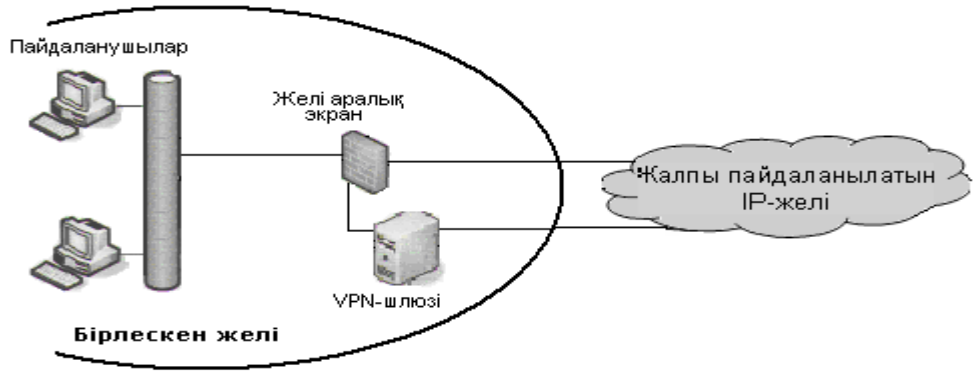


1.21 сурет– Шлюз функцияларын желі аралық экран ішінде жүзеге асыру

Шлюз бен желі аралық экранды бөлек қосу

Мұндай кезде шлюз бен желі аралық экранның жалпы пайдаланылатын IP-желімен өзіне меншікті байланысы бар 1.22 сурет көрсетілген. Шлюз тек қана шифрленген трафикті өңдейді, ол шифрленгеннен кейін желі аралық экранға өтеді де, онда сол кәсіпорын саясатымен өнделеді. Осылай шлюз бен желі аралық экран бірлескен желіні қорғау бойынша бірігеді, ал жалпы

пайдаланылатын желімен байланыс сенімділігі екі тәуелсіз арналардың болуымен жоғарыланады. Көптеген мәселелерде осы нұсқа кең таралған.

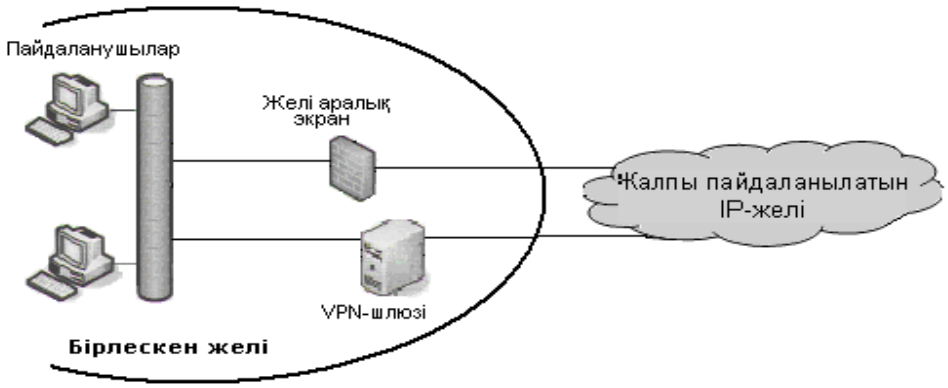


1.22 сурет– Шлюз бен желі аралық экранды бөлек қосу

Шлюзді желі аралық экранға параллельді қосу

VPN-өнімдерін өндірушілер жалпы пайдаланылатын желімен қосылудың көбінесе екі нұсқасын ұсынады – біреуін желі аралық экран үшін, ал екіншісін VPN-шлюзі үшін 1.23 суретте көрсетілген. Бұл архитектура алдыңғы қарастырылған сұлбаларға қарағанда қауіпті. Трафик желі аралық экранмен, VPN-шлюзбен тізбектей немесе параллельді өңделеді. Мұндай кезде бірлескен желі мен жалпы пайдаланатын желіден тек қана бір құрылғы бөлінеді – шлюз немесе желі аралық экран. Олар трафикті тәуелсіз өңдейді және олардың қорғаныс функциялары бірікпейді. Берілген сұлбаның сенімділігі өте жоғары, себебі бірлескен желі жалпы пайдаланылатын IP-желімен екі тәуелсіз арнамен байланысты.

VPN-шлюзі мен желі аралық экранның орналасу сұлбасын таңдаған кезде желінің өте жақсы қорғанысы соңғы екі нұсқамен қамтамасыз етіледі. Ол жалпы пайдаланылатын IP-желімен екі арна байланысын қолдану арқылы жүзеге асады, бірақта қосымша шығындарды қажет етеді.



1.23 сурет– Шлюзді желі аралық экранға параллельді қосу

2 Қызмет сапасын қамтамасыз ететін базалық технологиялар

2.1 Базалық технологиялардың сипаттамалары

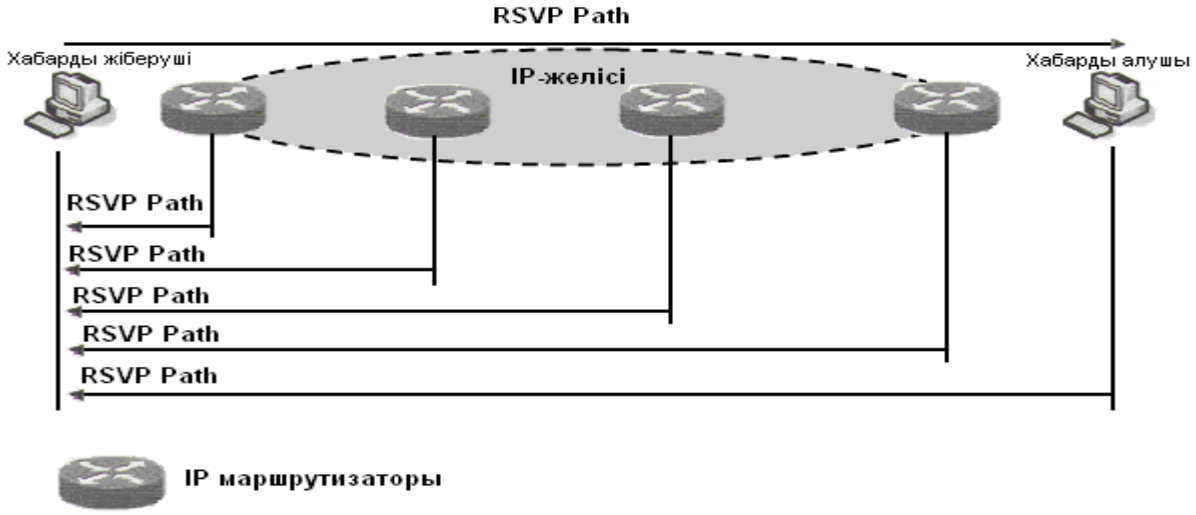
Берілген қызмет көрсету сапасын қолдау (QoS — Quality of Service) виртуалды жеке желілерді енгізу бойынша басты мәселе болып саналады. Бірақта, мұндай мәселені шешу қиынға соғады, әсіресе берілген қызмет көрсету сапасын Интернетте қамтамасыз ету керек болса. Глобалды желіде көптеген провайдерлер жұмыс істейді. Өтпелі қызмет көрсету сапасын қамтамасыз ету үшін оларға бір-бірімен келісу қиынға соғады. Сондықтанда VPN желілерінде кепілденген қызмет көрсету сапасы бір немесе бірнеше провайдерлер аралығында жүзеге асырылуы мүмкін. Олардың арасында берілген бағытта нақты бір келісім болуы керек.

2.1.1 RSVP протоколының базасында сапаны қамтамасыз ету. IP-желілерінде сапаны қамтамасыз ету әдістерінің бірі IETF коммитетімен ұсынылған резервілеу протоколын (Resource Reservation Protocol, RSVP) қолдану. RSVP протоколының көмегімен видео және аудиосигналдарын тарату кезінде, желіде кепілденген қызмет көрсету сапасын қамтамасыз етуге болады.

RSVP протоколы әр шақыру үшін IP-желілерінде белгіленген арналарды эммуляциялаудың арқасында (қажет өткізгіш жолағын резервілеу) QoS қамтамасыз етеді

RSVP сигнализация протоколы болып саналады. Ол интегралды сервисті көрсету мақсатымен оларды басқару және желілік ресурстарды резервілеуді қамтамасыз етеді. RSVP қолдану хабарды жіберуші RSVP Path хабарымен қажет желілік ресурстар көлемі туралы хабарды алушыға периодты түрде мәлімет беріп тұрады 2.1 суретте көрсетілген. Транзитті маршрутизаторлар сол хабардың өту көлеміне қарай өзіндегі бос ресурстар санын анализдейді және оны қарсы бағытта таратылған RSVP Resv сәйкес хабарымен дәлелдейді. Егер ресурстар жеткілікті болса, хабарды жіберуші таратуды бастайды. Егер ресурстар жеткіліксіз болса, хабарды жіберуші талаптарды төмендету немесе ақпаратты таратуды тоқтату керек.

RSVP ең негізгі қызықты ерекшелігі болып, ресурстарды резервілеу сауалдары тек қана хабарды алушылардан хабарты жіберушілерге бағытталады, керісінше емес. Мұндай шешім тек қана алушы құрылғысы ғана аудио және видеосигналдарын сенімді декодалау үшін қандай жылдамдықпен деректерді алатындығын білетіндігіне негізделген. RSVP басқа бірегейлі ерекшелігі резервілеу тек бір бағытқа ғана жүргізіледі. Одан басқа, RSVP резервіленген арнада аудио және видеосигналдарының ығысуына жол бермейді. [4]



2.1 сурет– RSVP протоколын қолдану

RSVP-бағдарламалары байланыс сеансы біткен кезде жою функциясын шақыруы керек. Ол осы протоколмен қарастырылған. Жою функциясы бағдарламамен жасалынған ресурстарға барлық сауалдарды жояды және басқа қосымша бағдарламалардың IP-желісінің коммуникациялық мүмкіндіктерін қолдануға мүмкіндік береді. Егер де бағдарлама жоюды орындай алмаса, онда протоколмен қарастырылған құралдар уақыт өткеннен кейін оны көріп автоматты түрде ресурстарға сауалды жояды.

RSVP протоколының кемшілігіне ақпарат көзіне бөлінген өткізу жолағы көздің активтілігі төмендегенде басқа ақпаратты тарату үшін қолданылмайды. RSVP протоколы QoS жүзеге асыру үшін ресурстарды немесе байланыс арналарын резервілеуді талап етеді. QoS сеанстарын бірнеше рет қайталап, ұқыпсыз және көнбіс пайдаланушылар желі ресурстарын тартып алуы мүмкін. Арна резервіленгеннен кейін басқа пайдаланушылар оны пайдалана алмайды, егер тіпті резервілеген пайдаланушы ештеңе таратпаса. Өкінішке орай RSVP протоколында осындай оқиғаларды болдырмайтын механизм жоқ және осы мәселені шешу желілік әкімшіліктерге қойылады.

Бұл әдіске альтернатива ретінде басымдылық жүйесі негізіндегі ағындарды басқару алгоритмі қолданылуы мүмкін. Бірақта IPv.4 нұсқасында ол механизм дұрыс жетілмеген. Басымдылықтармен басқару механизмі келесі IP алтыншы нұсқасында жүзеге асырылған. Онда 16 басымдылыққа дейін жүргізу қарастырылған және де бір физикалық қосылу аумағындағы бірнеше логикалық ағындарды жүзеге асыру мүмкіндігі қарастырылған.

Аралық түйіндердің (көп жағдайларда маршрутизаторлардың) сәйкестігіне RSVP тәуелділігі көбінесе глобалды желіде шарасыз мәселелерді тудырады. Егер кез-келген маршрутизатор өз мүмкіндігінің шегіне жетсе, QoS тапсырылған деңгейін кепілдей алмаса, одан кейінгі келесі тапсырыстар

ескерілмейді және жойылады. Тек қана бір түйіннің тапсырысына қызмет көрсетілмесе толық құрылған RSVP жүйесі бірнеше бөлшектерге бөлінеді.

Бірлестік деңгейінде RSVP біршама жақсы болашағы бар. Онда QoS көрсету тапсырыстарына қызмет көрсету үшін маршрутизатордың қандай парамметрлерін қолданатындығын әкімшісі анықтай алады. Глобалды желілерде тапсырыс жасайтын хостардың, қосымшалардың орналасқан юрисдикциясында маршрутизаторлардың орналасуының қажеті жоқ. Ол QoS кепілдігін күрделендіреді.

2.1.2 Дифференциалды қызмет көрсету базасында сапаны қамтамасыз ету. QoS қамтамасыз етудің басқа технологиясы дифференциалды қызмет көрсету (Differentiated Services, DiffServ) бойынша IETF жұмыс тобымен өңделген. Осы топ интегралды қызмет көрсету (Integrated Services, IntServ) бойынша жұмыс тобынан бөлінген. Оның есебі нақты уақыт ішінде Интернет трафигін қолдау үшін стандарттарды өңдеу.

IntServ аумағында жүргізілетін жұмыс RSVP тұжырымдамаларының кейбір ерекшеліктерін көрсетеді. Интегралданған қызмет көрсету соңынан соңына дейін сигнализацияны ұсынады және RSVP протоколын іс жүзінде хабар беруші мен алушы арасында қолданады.

IntServ технологиясы IP-желісінде қызмет көрсетудің үш классын анықтайды:

1) мүмкін болу мәніне – қазір Интернет ұсынатына байланысты;
2) бақыланатын жүктемесімен – аз жүктелген желіде болатындай сол қызмет көрсету деңгейі үстемені алады;
3) кепілденген қызметпен – толық сеанс кезіндегі қажет өткізу қабілеті қызмет көрсету сапасы парамметрлеріне кепілдемесімен ұсыналады.

RSVP протоколы сияқты интегралды қызмет көрсету масштабталуымен мәселелері бар. Сонымен, осындай технология бірлескен желілерде қолданылады. Жоғарыда көрсетілгендей RSVP протоколы сигналды ақпаратпен мәнді алмасуды ұсынады. Себебі, дестелердің жүру жолындағы әр түйін сұралған қызмет сапасының көрсетілу мүмкіндігін растау керек.

Дифференциалды қызмет көрсету нақты уақыт қосымшалары үшін QoS қарапайым және масштабталатын әдісін ұсынады. DiffServ технологиясының кілтті моменттерінің бірі болып IPv4 протоколының десте тақырыпщасында «Сервис типі» 8- битті өрісін қайта анықтауы саналады. «Дифференциалды қызмет көрсету» (DS) деп аталынған өріс ақпаратты өзінде сақтауы мүмкін. Маршрут бойымен дестелерді қалай өңдеу керектігін және келесі маршрутқа қалай тарату керектігін түйіндер анықтайды.

Қазіргі уақытта DS өрісінде 8 биттің 6 биті анықталған және тек бір ғана мәні стандартталған. Сол мән үндемей қабылдауға жатады - Default (DE) және «мүмкін болу мәніне байланысты» (Best Effort, BE) қызмет көрсету классын анықтайды. Басқа жобаланатын тағайындауға – шұғыл жіберу (Expedited Forwarding, EF) — дестелердің жоғалуы мен кідірісінің төмендеуін қамтамасыз етуі керек.

Трафиктің желіге түсуі кезінде шекаралық маршрутизатор DS өрісіндегі ақпаратқа сәйкес трафикті жіктейді. Сол ақпаратты келесі маршрутизаторға таратады. Соған сәйкес олар берілген нақты ағынды қалай өңдеу керектігін анықтайды.

Одан басқа DiffServ қызмет трафигін RSVP және IntServ қарағанда салыстырып қысқартады. DiffServ анықталған ережелерге сәйкес ағындарды жіктейді және бір типті ағындарды біріктіреді. Осындай механизм IntServ қарағанда DiffServ одан да масштабтырақ жасайды. Бірдей белгілермен толық трафик бірдей қарастырылады. Сондықтан да үлкен кәсіпорын желісінде немесе глобалды желі арналарында DiffServ жүзеге асыру нақты есеп болып табылады.

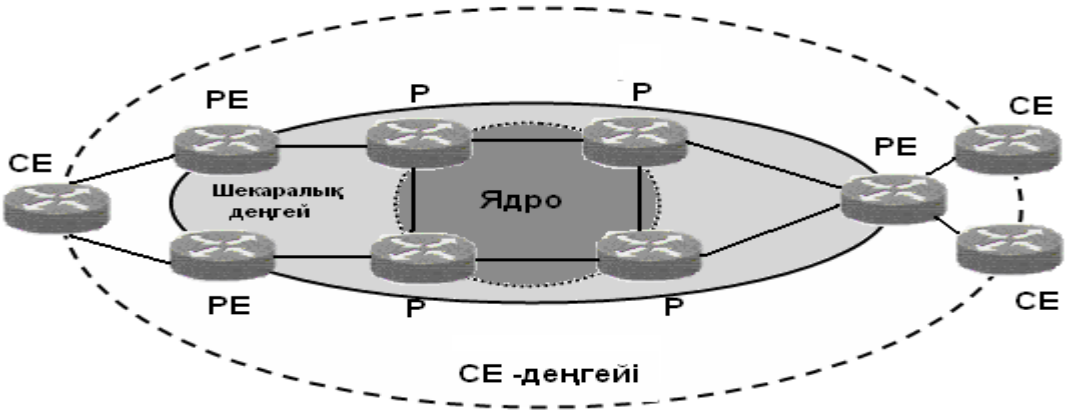
DiffServ технологиясын жүзеге асыру үшін «белгіленген ағындарды» маршрутизаторлар анықтай алатындығы және оларға сәйкес әрекет ету алатындығы қажет. Ол маршрутизаторлардың микробағдарламалық қамтамасыздандыруының жетілуін талап етеді. Қазіргі кезде көптеген өндірушілер өз өнімдерінің жаңа нұсқаларында DiffServ архитектурасын қолдайды

2.1.3 MPLS технологиясының базасында сапаны қамтамасыз ету. MPLS (Multi Protocol Label Switching) белгі коммутация технологиясының негізінде виртуалды жеке желілер кең таралып жатыр. Отандық қызмет көрсету провайдерлерінің саны өсуде. Олар өз клиенттеріне интранет және экстранет желілерін тиімді құру үшін берілген сервис түрін қолдануға шақырады. Виртуалды жеке желілерін құрудың басқа әдістерінен MPLS VPN жоғарғы масштабтылығы, автоматты жіктелу мүмкіндігі және IP басқа сервистерімен табиғи интеграциясы тиімді ерекшелендіреді.

MPLS технологиясының базасында виртуалды жеке желілерді құруға ат салысатын негізгі компоненттер 2.2 сурет көрсетілген.

Жалпы жағдайда әр клиенттің бірнеше аймақтық бөлінген IP-желілері болуы мүмкін. Олардың әрқайсысы маршрутизатормен байланысты бірнеше қосымша желілерден тұруы мүмкін. Осындай аймақтық бөлінген бірлескен желі «аралдарын» VPN соңғы нүктелері деп атау керек. Бір клиентке бағынышты соңғы нүктелер провайдер желісі арқылы IP-дестелерімен алмасады және сол клиенттің виртуалды жеке желісін құрайды. Соңғы нүкте шегінде түйіндер маршрутты ақпаратпен алмасу үшін маршрутизацияның ішкі протоколын (Interior Gateway Protocol, IGP) қолданады. Оның жұмыс істеу аймағы RIP, OSPF немесе IS-IS автономды жүйелерімен шектелген.

Маршрутизатор көмегімен провайдер магистраліне қосылатын клиенттің маршрутизаторын пайдаланушының шекаралық маршрутизаторы (Customer Edge router, CE) деп атайды. Пайдаланушы желісінің компонентті болғанымен CE VPN болуы туралы ештеңе білмейді. Ол бірнеше арналар арқылы провайдердің магистралды желісімен қосылуы мүмкін. Провайдердің магистралды желісі MPLS желісі болып келеді. Онда IP дестелері IP-адрестер негізінде жүрмейді, ал локалды белгілеу негізінде жүреді. Осы белгі QoS деңгейінің әр дестесі үшін қажет ақпаратты ұстайды.



2.2 сурет– MPLS VPN компоненттері

MPLS желісі белгі коммутация маршрутизаторларына (Label Switch Router, LSR) тұрады. Олар белгі коммутациясымен (Label Switching Path, LSP) белгі мәніне сәйкес алдын-ала жасалынған жолдармен трафикті бағыттайды. LSR құрылғысы ол – IP-маршрутизаторы мен коммутаторының өзгеше болады. Сонымен қатар, IP-маршрутизаторларынан маршрутизаторлар протоколдары көмегімен желі топологиясын анықтау қасиеті және трафиктің жүру жолдарының тиімдісін таңдау қасиеті алынады. Ал коммутаторлардан – коммутацияның локалды кестелері мен белгілерін қолданып дестелердің жүру техникасы алынады. LSR құрылғысын қысқа қарапайым түрде маршрутизатор деп атайды. Себебі, олар IP-адресі негізінде дестелерді сондай жетістікпен маршруттауы мүмкін, егер де MPLS қосылулы болмаса.

Провайдер желіндегі LSR құрылғылары арасынан шекаралық маршрутизаторларды бөледі (Provider Edge router, PE). Оларға CE маршрутизаторлары арқылы пайдаланушылардың соңғы нүктесі және провайдердің магистралды желісінің ішкі маршрутизаторлары (Provider router, P) қосылады. CE және PE маршрутизаторлары әдетте олар физикалық арналармен байланысты Онда кез-келген каналды деңгей протоколы жұмыс істейді. Мысалы PPP, FR, ATM және Ethernet. CE мен PE арасындағы қатынас TCP/IP стек стандартты протоколдарының негізінде жүреді. MPLS қолдауы тек тек қана PE ішкі интерфейстеріне және P барлық интерфейстеріне қажет.

Виртуалды жеке желілерді қолдау үшін провайдердің магистралды желісінде шекаралық маршрутизаторлар болуы керек. Сондықтан, тек қана олар қандай VPN бар екендігін «біледі». Егер де желіні VPN жағынан қарастырса, онда провайдер маршрутизаторлары мен тапсырыс беру маршрутизаторлары бір-бірімен іс-әрекет етпейді де тек қана ішкі және сыртқы маршрутизаторлар туннелінде орналасады.

PE маршрутизаторлары провайдер маршрутизаторларына қарағанда функционалды түрде күрделі келеді. Оларға VPN құру бойынша күрделі тапсырыстар қойылады. Соның ішінде әртүрлі клиенттерден түсетін маршрутты және деректерді айыру. PE маршрутизаторлары

пайдаланушылардың соңғы нүктелері арасындағы LSR жолдарының ақырғы нүктесі ретінде қызмет етеді. Оның ішінде IP дестесіне белігіні PE қойып, P маршрутизаторларының ішкі желісі арқылы оның транзиті үшін арналған.

LSR жолдары екі әдіспен жүргізілуі мүмкін. Біріншісі, LDP (Label Distribution Protocol) белгілерін үлестіру протоколдарының көмегімен ішкі шлюздің тездетілген маршрутизация IGP (Interior Gateway Protocol) технологиясын қолданумен. Екіншісі, RSVP немесе CR-LDP протоколдары көмегімен TE (Traffic Engineering) трафикті инжинирингілеу технологиясының негізінде қолданумен. LSR құру PE және P барлық маршрутизаторларының белгілерінде берілген LSR жасайтын коммутация кестесін құру екендігін білдіреді. Осы кестелер қосылғанда клиенттердің әртүрлі трафигі үшін көп жолдарды белгілейді.

2.2 Ақпараттық қауіпсіздіктің базалық технологиялары

Виртуалды жеке желілерді жүзеге асыру кезінде сенімді қорғанысты қамтамасыз ету ең басты мәселе. VPN технологиясының артықшылығы дәлелді, себебі қазіргі кезде көптеген кәсіпорындар ашық желіні қолдану бойынша өзінің стратегияларын жасауда. Соның ішінде ең басты ақпаратты тарату құралы ретінде Интернетті. Сондықтан, халықаралық және қоғамдық мекемелер, бөлек кәсіпорындар, құрылғы және бағдарламалық қамтамасыздандыру өндірушілері ақпаратты қорғау жөнінде ашық стандарттар мен протоколдарды жасауға күш жұмсауда. Оларға мына протоколдарды PPTP, L2TP, IPSec, SKIP, SSL/TLS, SOCKS, SHTTP, S/MIME, PGP жатқызуға болады. [5]

Көрсетілген протоколдар әртүрлі деңгейде ақпаратты қорғауды қарастырады. Ашық жүйелердің өзара байланысының эталанды моделі (АЖӨБЭМ) 2.3 сурет көрсетілген.

АЖӨБЭМ деңгейлері	Қорғаныс протоколдары	
Қолданбалы деңгей	SHTTP,PGP	
Түсіну деңгейі		
Сеанстық деңгей	SOCKS, SSL/TLS	
Транспорттық деңгей		Қорғалған арналар деңгейлері
Желілік деңгей	IPSec, SKIP	
Арналық деңгей	PPTP, L2TP,L2F	
Физикалық деңгей		

2.3 сурет– АЖӨБЭМ деректерді қорғау протоколдары

Қазіргі кезде осы протоколдар базасында ақпаратты қорғауды ұйымдастыруға бірнеше тәсіл құрастырылды. Содан бірнеше класс өнімі пайда болды:

- дестелер филтрі, желілік және арналы деңгей протоколдарында базаланатын;

- SOCKS протоколының негізіндегі proxy-сервер;
- қолданбалы деңгей пртоколын қолданылатын өнімдер.

Дегенмен, бірінші екі класстарды VPN жүзеге асыру үшін арналған өнімдерге жатқызуға болады. Сонымен қатар, виртуалды жеке желілерді жүзеге асыру кезінде кейбір жалпы заңдылықтарды жоққа шығару қажет.

- қорғаныс ұйымдастырылған АЖӨБЭМ деңгейі төмен болса қосымшалар үшін мөлдірлеу және пайдаланушылар үшін байқалмайды. Бірақта қауіпсіздік қызметін жүзеге асыру жиыньтығытөмен болған сайын содан басқаруды ұйымдастыру күрделене түседі;
- қорғаныс жүзеге асырылған АЖӨБЭМ деңгейі жоғары болған сайын қауіпсіздік қызметінің жиынтығы кеңдеу, рұқсат қадағалануы сенімді және рұқсат ережелерін конфигурирлеу қарапайымдырақ; Бірақта, қосымшалар мен пайдаланушылар үшін қорғаныс көзге көрінерліктей болады.

VPN жүзеге асыру үшін қолданылатын протоколдар кез-келген бағытта одан да жоғарғы деңгей протоколдары үшін мөлдір болады.

2.2.1 IP базасында VPN қауіпсіздікті қамтамасыз ету жабдықтары. Шифрлеу – нақты математикалық алгоритммен сәйкес деректерді кодалау. Шифрлеу алгоритммі кілт функциясын орындайтын, кодалық комбинация көмегімен деректерді түрлендіруге негізделген. Осындай комбинацияда сандар көп болған сайын кілтті таңдау үшін потенциялды ұрыға көп уақыт қажет болады. Осыдан, кілт ұзын болған сайын берілген алгоритм сенімді қорғанысты қамтамасыз етеді. Шифрлеудің бірнеше әдістері бар. Ол симметриялы (жеке кілт), асимметриялы (ашық кілттер).

Симметриялы шифрлеу құпиялы кілтпен шифрлеу деп жиі атайды. Көбінесе деректердің құпиялығын қамтамасыз ету үшін пайдаланады. Екі пайдаланушы бірігіп бірдей математикалық алгоритмді таңдауы керек. Ол деректерді шифрлеу мен шифрді шешу үшін қолданылады. Одан басқа оларға ортақ кілт таңдау қажет (құпиялы кілт).

Қазіргі кезде осындай шифрлеу алгоритмдері кең қолдануда. Оларға Data Encryption Standard (DES), 3DES (немесе «DES үшеуленген»), International Data Encryption Algorithm (IDEA) жатады. Осы алгоритмдер хабарды блокпен шифрлейді. Мысалы 64 битпен. Егерде хабар көлемі 64 биттен жоғары болса, онда оны 64 битпен блоктарға бөлу қажет. Содан кейін оны қалайда болса біріктіру қажет. Осындай біріктіру келесі төрт әдістің біреуімен орындалады: электронды кодалық кітлпен (ECB), шифрленген блоктар тізбегімен (CBC), х-битті кері байланыспен шифрленген (CFB-x) немесе шығыс кері байланыспен (OFB).

Құпиялы кілт көмегімен шифрлеу деректердің құпиялығын қолдау үшін жиі қолданылады. Өзгерілмейтін бағдарламалар (firmware) көмегімен тиімді жүзеге асырылады. Осы әдісті аутентификация және деректердің бүтіндігін қамтамасыз ету үшін қолдануға болады.

Құпиялы кілттер әдісінің келесідей кемшіліктері бар:

- құпиялы кілттерді жиі ауыстырып тұру қажет. Себебі, оларды кездейсоқ біліп қою мүмкіндінгі бар;

- генерирлеу қауіпсіздігін және құпиялы кілттің таралуын қамтамасыз ету қиынға соғады.

Асимметриялы шифрлеу ортақ кілт көмегімен шифрлеу деп жиі атайды. Шифрлеу мен шифрді шешу үшін әртүрлі алгоритмдер және кілттер қолданылады, бірақ бір-бірін өзара толықтырып тұрады. Осы механизм екі өзара байланысқан кілттен тұрады: ортақ және жеке. Ортақ кілт алгоритммін қолданатын типтік мысалдар:

- деректердің құпиялығын қамтамасыз ету;
- хабарды берушінің аутентификациясы;
- цифрлы қолтаңба;
- бірге пайдалану үшін ортақ кілттерді қауіпсіз алу.

Асимметриялы шифрлеудің маңызды аспектісі жеке кілт құпияда сақталынуы керектігі. Егер жеке кілт ашылған болса, онда соны білген адам сіздің атыңыздан хабарларды таратып және сізге келген хабарларды оқуы мүмкін.

Ортақ/жалпы кілттер жұбын математикалық генерирлеу қағидасы күрделі емес. Бірақта, есептеу жағынан қарасақ өте үлкен жәй сандармен жұмыс істеу керек болады. Ортақ кілттер көмегімен шифрлеу алгоритмін қосымшаларда пайдаланады. Онда аутентификация цифрлы қолтаңба мен кілттерді басқару көмегімен жүргізіледі.

Ортақ кілттер ішіндегі ең танымалдарына RSA мен ElGamal жатқызуға болады.

Ақпаратты қорғау құралдарының ерекше тобын хэш-алгоритмдер құрайды. Әртүрлі ұзындықтағы деректер дестесін бірдей белгіленген биттер санымен хэширленген дестелерге түрлендіре алады. Осындай хэштарды деректердің бүтіндігін тексеру үшін қолданады. Мысалы, цифрлық қолтаңба алгоритмдерінде. IPsec дестесін құру кезінде оның құрамындағы хэш-функциясы есептелінеді. Ал сол есептеудің нәтижесі дестеге салынады. Дестені алған кезде сол алгоритмді пайдаланып тура сондай есептеу жүргізіледі. Содан кейін, оның нәтижесі дестемен келген нәтижемен салыстырылады. Егер де нәтиже сәйкес келмесе, онда хабарды алушы станциясы хабардың жоғалғанын біледі. Соның ішінде кең таралған алгоритмдеріне MD5 және SHA1 жатады.

Аутентификация (authentication) «түпнұсқалығын орнату» қажет емес тұлғалардың желіге рұқсатын тоқтадады және ашық пайдаланушылардың рұқсат етілген кірісін қамтамасыз етеді. Фактіге негізделген аутентификация – пайдаланушының дұрыстығын дәлелдейтін процедура, соның ішінде сол пайдаланушымен енгізілген идентификатор сонікі екенін дәлелдейді.

Аутентификация процедурасында екі жақ қатысады: бір жағы өзінің аутентификациясын дәлелдейді, екінші жағы – аутентификатор - сол дәлелдемелерді тексеріп шешім қабылдайды. Аутентификацияның дәлелдемесі ретінде әртүрлі тәсілдер қолданылады:

- аутентификацияланатын екі жақ құпиясы үшін ортақ білімін көрсете алады: сөздерді (парольдар) немесе фактілерді (оқиғалар орны мен болған уақыты, адамның аты және т.с.с.);
- аутентификацияланатын бір ерекше заты бар екендігін көрсете алады (физикалық кілтпен). Мысалы, сол ретінде электронды магнитті карта қолданылуы мүмкін;
- аутентификацияланатын өзінің биомінездемелерін қолданып өз сәйкестігін дәлелдей алады. Мысалы, аутентификатор деректер базасына алдын-ала еңгізілген көз қабықшасының суреті немесе саусақтар таңбасы.

Аутентификацияның желілік қызметтері жоғарыда келтірілген тәсілдердің негізінде құрылады. Бірақта, пайдаланушының сәйкестігін дәлелдеу үшін көбінесе парольдерді қолданады. Парольдер негізіндегі аутентификация тәсілінің негізгі артықшылықтарына механизмнің қарапайымдылығы мен логикалық анықтылығы жатады. Берілген әдістің кемшіліктеріне парольдің ашылуы мен оны шешуге болатындығы, желілік трафикті анализдеу арқылы парольді естіп қою. Парольдердің ашылуына түсетін қауіп-қатердің деңгейін төмендету үшін тағайындау саясатын құру мен парольдерді қолдану үшін қондырылған бағдарламалық құралдарды пайдаланады: парольдің минималды және максималды жұмыс істеу уақытын белгілеу, алдында қолданылған парольдердің тізімдерін сақтау, бірнеше рет дұрыс емес еңгізілген логикалық кірістен кейінгі жүйенің әсерін бақылау және т.б. Сондай жүйелерге S/Key протоколымен аутентификация әдісін жатқызуға болады. MD4 және MD5 стандарттары негізінде ұқсас парольдердің генерирлеу жүйесін және RFC 1760 анықталғанын көрсетеді. Ол «қайталанатын шабуылдар» деп аталанатындарға қарсы тұру үшін арналған. Хакер арнаны «білдірмей тыңдаған» кезде трафиктен пайдаланушының идентификаторын және оның паролін бөледі. Содан кейін оны рұқсатсыз кіруге пайдаланады.

Берілген технология екі баламалы сұлбалардың біреуімен жұмыс істейді:
- тапсырыс-жауаб сұлбасы бойынша;
- уақыт бойынша синхронизациямен аутентификация сұлбасы.

Тапсырыс-жауаб сұлбасында пайдаланушы аутентификация серверіне қосылады. Ол өз ретінде дербес идентификационды нөмерді (PIN) немесе пайдаланушы идентификаторын (user ID) сұрайды. Пайдаланушы серверге PIN немесе user ID таратады. Ол содан кейін тапсырысты жасайды (пайдаланушы экранында шығатын кездейсоқ санды таратады). Пайдаланушы сол санды кредитті картаға ұқсас арнайы аппаратты құрылғыға еңгізеді. Ол сонда пайдаланушының шифрленген кілтімен шифрленеді. Шифрлеу нәтижесі экранда көрінеді. Пайдаланушы сол нәтижені аутентификация серверіне жібереді. Аутентификация сервері осы нәтижені барлық пайдаланушы кілттері сақталынатын, деректер базасын қолданып өз бетінше есептейді. Пайдаланушыдан жауабты алғаннан кейін, сервер оны өз есептеулерімен салыстырады. Егер нәтиженің екуі де бірдей болса, онда

пайдаланушы серверге рұқсатты алады. Егер де нәтижелер ұқсас болмаса, онда пайдаланушының серверге рұқсаты болмайды.

Сервер мен пайдаланушының аппаратты құрылғысындағы уақыт бойынша синхронизация сұлбасын пайдалану кезінде құпиялы алгоритм қолданылады. Ол нақты бір синхронизацияланған уақыт аралығы өткеннен кейін бірдей парольдерді өзгертеді және ескі парольдерді жаңа парольдерге ауыстырады. Пайдаланушы сервер аутентификациясына қосылады. Ол пайдаланушыдан рұқсат кодын сұрайды. Содан кейін, пайдаланушы аппаратты карточкалы құрылғыға өзінің PIN енгізеді. Соның нәтижесінде, бір рет қана қолданылатын пароль экранда шығады да, серверге жіберіледі. Сервер өзінде есептелінген парольмен салыстырады. Егер парольдер сәйкес келсе, пайдаланушы желіге рұқсатын алады.

Аутентификацияны талап ететін обьектілер ретінде тек қана пайдаланушылар шықпай, әртүрлі құрылғылар мен қосымшалар, мәтінді және басқа ақпараттар болуы мүмкін. Мысалы, пайдаланушы бірлескен серверге тапсырыспен қайта үндейтін және өзінің жариялылығын дәлелдейтін, сонымен қатар ол өз кәсіпорынының серверімен сұхбат жүргізіп жатқандығына көз жеткізуі керек. Басқа сөзбен айтқанда, сервер мен клиент өзара аутентификация процедурасынан өтеді. Сол жерде қосымшалар деңгейінде аутентификация жүреді. Екі құрылғылар арасында байланыс сеансын орнатқан кезде оданда төмен арналық деңгейдегі өзара аутентификация процедурасы қарастырылған. Осындай процедура мысалы ретінде, PPP протоколдар тұқымдастарына кіретін PAP және CHAP протоколдарымен аутентификация жатады.

Деректердің аутентификациясы осы деректердің бүтіндігін дәлелдеуді білдіреді және де соны хабарлаған нақты бір адамнан түскенін көрсетеді. Мұндай кезде электронды жазбалар қолданылады.

Есептеу желілерінде аутентификация процедуралары авторизация процедуралары сияқты жиі тура сол бағдарламалық құралдармен жүзеге асады. Ашық және ашық емес пайдаланушыларды танитын аутентификацияларға қарағанда, авторизация жүйесі аутентификация процедурасынан ойдағыдай өткен тек қана ашық пайдаланушылармен жұмыс істейді.

Авторизация. Авторизация (authorization) амалдары жүйе ресурстарына ашық пайдаланушылардың рұқсатын қадағалайды. Олардың әрқайсысына әкімшімен анықталған құқықты береді. Пайдаланушылардың каталогтарға, файлдерге және принтерлерге рұқсат құқығын беруден басқа авторизация жүйесі пайдаланушымен әртүрлі жүйелік функциялардың орындалу мүмкіндігін талап етуі мүмкін. Мысалы, серверге локалды рұқсатты, жүйелік уақытты орнату, деректердің резервті көшірмесін жасау, серверді өшіру және т.б. Авторизация жүйесі VPN қолданылатын дестелерді шифрлеу амалдарына немесе тіпті нақты VPN-құрылғыларына пайдаланушының рұқсатын реттеуі мүмкін.

Авторизация процедуралары бағдарламалық құралдармен жүзеге асады. Олар операциялық жүйеге немесе қосымшаларға қондырылуы мүмкін және бөлек бағдарламалық өнім ретінде қамтамасыз етілуі мүмкін. Авторизацияның бағдарламалық жүйелері екі сұлба негізінде құрылады:

- серверде базаланатын авторизацияның орталықтанаған сұлбасы;
- жұмыс станцияларында базаланатын орталықтанбаған сұлба.

Бірінші сұлбада сервер пайдаланушыға ресурстарды қамтамасыз ету процесін басқарады. Осындай жүйелердің басты мақсаты – «біртұтас кіріс принципін» жүзеге асыру. Пайдаланушы орталықтанған сұлбасымен сәйкес желіге бір рет логикалық түрде кіреді және барлық жұмыс уақытына желі ресурстарына рұқсатты алады. TACACS (Terminal Access Controller Access Control System) және RADIUS (Remote Access Dial-In User Service) жүйелері қашықталған рұқсат жүйелерімен жиі қолданылады. Осы амалды жүзеге асырады.

Екінші тәсілде жұмыс станциясы өзі қорғалған болады. Қорғаныс амалдары әр машинада жұмыс істегендіктен, сервердің қажеті жоқ. Бірақта, бірлескен желі әкімшісіне қауіпсіздік механизмінің жұмысын қадағалап тұру қажет. Барлық қосымшалар типін қолданылады – электронды почта, локалды желі каталогтар қызметі, хостың базалық деректері және т.б. Әкімшіге пайдаланушыларды қосу немесе жою керек болған жағдайда әр жүйеге немесе бағдарламаға рүұсатты жиі қолмен конфигурирлеу қажет болады.

Үлкен желілерде пайдаланушыларға желі ресурстарына рұқсат құқығын берудің араласқан амалы қолданылады. Қашықталған рұқсат сервері бірлескен желі серверлеріне немесе қосалқы желілер пайдаланушыларына рұқсатты шектейді. Мысалы, үлкейтілген желі элементтеріне. Желінің әр жеке сервері өз бетінше өзінің ішкі ресурстарына каталогтармен, принтерлермен немесе қосымшалармен бөлінген рұқсатты шектейді. Қашықталған рұқсат сервері бірлескен желі серверлеріне немесе қосалқы желілеріне, соның ішінде желінің үлкейтілген элементтеріне пайдаланушының рұқсатын шектейді. Ал желінің бөлек сервері өз бетінше пайдаланушының каталогтармен, принтерлермен немесе қосымшалармен өзінің ішкі ресурстарына, бөлінген рұқсатты шектейді. Қашықталған рұқсат сервері өзіндегі пайдаланушылар рұқсат құқығының тізімі (ACL — Access Control List) негізінде рұқсатты қамтамасыз етеді. Желінің әр жеке серверінің ресурсы, онда сақталған рұқсат құқығының негізінде рұқсат етіледі. Мысалы, ACL файлды жүйесі. Аутентификация мен авторизация жүйелері бірігіп бір есепті шешеді. Сондықтан оларға бірдей талап деңгейін қою керек. Мұндағы бір звеноның сенімсіздігі басқа звеноның жоғарғы сенімділігімен есесін қайтара алмайды. Егер аутентификация кезінде парольдер қолданылса, онда олардың қорғанысы қажет болады. Бір рет ұрланған пароль пайдаланушының осы парольмен ашық рұқсаты болған барлық қосымшалар мен деректерге рұқсатты ашады. Ешқандай жүйе жүз пайызды қорғанысты қамтамасыз етпегендіктен, соңғы қорғаныс аудит жүйесі болады.

Аудит (auditing) — қорғалған жүйелік ресурстарға рұқсатпен байланысты, оқиғалар журналының жүйесінде белгілеу. Шындығында да, қаскүнемдіктің табысты шабуылы жасалынғаннан кейін, пайдаланушыға тек қана аудит қызметіне хабарласу керек. Егер аудит қызметіне іздеу қажет болатын оқиғалар дұрыс берілген болса, онда журналдағы толық жазбалар анализі көптеген пайдалы ақпаратты береді. Осы ақпарат қаскүнемді табуға мүмкіндік береді немесе осындай оқиғаның қайталануына жол бермейді.

Туннелдеу. Қорғалған арна протоколдары өз жұмыстарында туннелдеу (инкапсуляция) механизмін жиі қолданады. Туннелдеу кезінде төменгі деңгей десте протоколы жоғарғы немесе тура сондай деңгейдегі ротоколдың дестенің деректер өрісінде орналастырылады. Мысалы, Ethernet кадрын туннелдеу кезінде IP дестесінде орналасу мүмкін. Ал IPX дестесі – IP дестесінде. IP дестесі IP дестесінде орналасатын нұсқада болу мүмкін. Туннелдеу бұқаралық желі арқылы деректерді тарату қауіпсіздігі үшін қолданылады. Сыртқы қабықшаға дестелерді буып-түю арқылы жүзеге асырылады. Туннель екі шекаралық құрылғылар көмегімен құрылады. Олар бұқаралық желі кірісінің нүктелерінде орналасады.

Туннелдеудің ерекшелігіне берілген дестені тақырыпшасымен бірге толығымен шифрлеуге мүмкіндік береді. Ол өте маңызды себебі көптеген тақырыпша өрістері ақпаратты құрайды. Ол қаскүнемдермен пайдаланылуы мүмкін. Тақырыпшадан ол желінің ішкі құрамы туралы түйіндер мен қосалқы желі сандарын және олардың IP-адрестері туралы деректерді алуы мүмкін. Сондай ақпараттар бірлескен желіге әртүрлі шабуылдарды ұйымдастыру үшін қолданылады немесе кәсіпорынның жұмыс активтілігі туралы деректерді алу үшін шығыс және кіріс трафиктерін анализдеуде қолданылады.

Басқа жақтан қарағанда, егер тақырыпша шифрленген болса, желі бойымен дестені транспорттауды қамтамасыз ету үшін ол онда өзінің тура арналуымен қолданылмайды. Тура осындай жағдай кезінде дестені қорғау үшін туннелдеуді қолданады. Шыққан дестені тақырыпшамен бірге толығымен шифрлейді де, осы шифрленген дестені басқа ашық тақырыпшамен сыртқы дестеге орналастырады. «Қауіпті» желі бойымен деректерді транспорттау үшін сыртқы дестенің ашық тақырыпша өрістері қолданылады. Ал қорғалған арна бойымен десте соңғы нүктеге жеткен кезде оның ішінен ішкі дестені шығарады. Содан кейін оның шифрын шешіп оның тақырыпшасын «қауіпсіз» желі бойымен ашық түрде тарату үшін қолданады.

Туннелдеу тек қана десте құрамының құпиялығын қамтамасыз етіп қана қоймай, оның бүтіндігі мен дұрыстығын қамтамасыз етеді. Мұндай кезде ақпаратты қорғау толығымен жүзеге асырылады. Әдеттегіде туннелдеу жалпы пайдаланылатын желі аймағында жасалынады. Онда деректердің құпиялығы мен бүтіндігіне қауіп-қатер туып отырады. Мысалы Интернет бұқаралық желісіне кіру нүктесі мен бірлескен желіге кіру нүктесінің арасында. Осындай кезде сыртқы дестелер үшіносы екі нүктелерде орналасқан шекаралық маршрутизаторлар адрестері қолданылады. Ал соңғы түйіндердің ішкі адрестері қорғалған түрде ішкі дестеде орналасады.

Туннелдеу әртүрлі транспортты технологияларды сәйкестендіру үшін жиі қолданылады. Мысалы, егер IPX протоколының деректерін транзитті IP-желісі арқылы тарату керек болса. Онда IPX және IP-желі шекарасындағы маршрутизатор шыққан IPX дестесін жаңа құрылған IP-дестесіне буады да, содан кейін маршрутизаторға адрестейді. Ол транзитті IP-желісін IPX-желісімен қосады. Осы маршрутизатор келген IP-дестесінен IPX дестесін бөліп шығарады да, одан кейін IPX-желісі бойымен қайта жібереді.

Туннелдеу механизмінің өзі қандай мақсатпен туннелдеу қолданатындығынан тәуелсіз – транспортты технологияларды келісуі үшін немесе деректерді қорғау үшін. Осы механизмді үш түрлі протоколдар жұмысының нәтижесі ретінде көрсетуге болады:

- жолаушы протоколы;
- жүргізуші протоколы;
- туннелдеу протоколы.

Біріктірілетін желілердің транспортты протоколы (IPX протоколы) жолаушы протоколы болады, ал транзитті желі протоколы (IP протоколы) жүргізуші протоколы болады. Жолаушы протокол дестелерін жүргізуші протоколының дестелерінің деректер өрісіне орналастыру процедурасы туннелдеу протоколының негізін құрайды. Жолаушы протокол дестелері транзитті желі арқылы жүргізілгенде ешқалай өңделмейді. Туннелдеу әдеттегіде шекаралық құрылғыны орындайды (маршрутизаторды немесе шлюзді). Ол соңғы және транзитті желілер арасында орналасады, бірақ-та осындай жұмыспен қайтарушы-түйінде айналысу мүмкін. Жүргізуші дестелерінен жолаушылар дестелерін бөліп шығаруын екінші шекаралық құрылғы орындайды. Ол транзитті желі мен белгілеу желісінің шекарасында орналасады.

Туннелдеу өз еркімен рұқсат етілменген рұқсаттан немесе бұрмаланулардан деректерді қорғамайды. Тек қана соңғы дестелердің барлық өрістерін қорғау үшін алғышарттарды құрайды. Таратылатын деректердің құпиялығын қамтамасыз ету үшін соңғы жолаушы-дестелері шифрленеді немесеэлектронды қолтаңбамен қамтамасыз етіледі. Содан кейін жүргізуші протокол дестелерінің көмегімен транзитті желі бойымен таратылады.

2.2.2 Арналық деңгейде деректерді қорғау. PPTP, L2F және L2TP арналық деңгей протоколдары локалды желіге қашықталған рұқсат кезінде көбінесе ақпараттық өзара байланысты қорғау үшін қолайлы (Remote Access VPN).

Жоғарыда көрсетілген протоколдар арналық протоколдарын желілік деңгей протоколдарына инкапсуляциялайды. Желілік протоколдар арқылы деректер құрастырылған желі бойымен таратылады. Одан басқа бұқаралық желі арқылы бірлескен желі ресурстарына көппротоколды қорғалған қашықталған рұқсат есептерін шешуі осы протоколдардың негізгі қолдану аймағы. Себебі кез-келген клиенттік бағдарламалық қамтамасыз ету қашықталған рұқсат үшін PPP арналық деңгейдің стандартты протоколын қолданады. PPTP, L2F және L2TP протоколдары желілік деңгей

протоколдарына PPP кадрларының инкапсуляциясынан негізделген. Осындай қасиетте біріншіден IP-протоколдары қолданылады.
PPTP протоколы. Жоғарыда көрсетілген протоколдар қорғалған арна құру протоколдарына жатқанымен. Тек қана PPTP протоколы осы анықтамаға сәйкес келеді. Ол деректердің туннелденуін және шифрленуін қамтамасыз етеді. L2F және L2TP протоколдары туннелдеу протоколдарына жатады, ал деректерді қорғау функциялары (шифрлеу, аутентификация, бүтіндігі) онда қамтамасыз етілмейді. Оларды қолдану кезінде туннелденген деректердің қорғанысы үшінші протокол көмегімен жүзеге асырылуы болжанады. Мысалы IPSec протоколы.

PPTP (Point-to-Point Tunneling Protocol) — Microsoft кәсіпорынымен бірге Ascend Communications, 3Com/Primary Access, ECI-Telematics және US Robotics кәсіпорындарымен өңделген «нүкте-нүкте» тоннелді протоколы. Осы протокол «PPP Extentions» IETF жұмыс тобына қорғалған арнаны стандартты құру протоколы ретінде берілген. Бірақта стандарт ретінде бекітілмеді. Ол Cisco Systems кәсіпорынының тура сол уақытта өзінің протоколын L2F (Layer 2 Forwarding) IETF көрсетті. Сондықтан екі протоколдың біреуін де жақтамады да, тек қана екеуін біріктіріп L2TP (Layer 2 Tunneling Protocol) протоколын жасады. Бірақта PPTP протоколы өзінің жеңілуіне қарамастан, Microsoft кәсіпорынының операциялық жүйесінде Windows NT қолдану арқасында кең таралды. Желі аралық экрандар мен VPN шлюзін кейбір өндірушілері PPTP қолданады.

Берілген протокол әртүрлі протоколдармен IP, IPX немесе NetBEUI деректермен алмасу үшін қорғалған арналарды құруға мүмкіндік береді. Глобалды желіге түсетін PPP кадрлеріне буылған осы протоколдардың деректері IP протоколының дестелеріне PPTP протоколының көмегімен инкапсуляцияланады. Оның көмегімен кез-келген TCP/IP желісі арқылы шифрленген түрде таралады. Қабылдайтын түйін IP дестелерінен PPP кадрлерін бөліп шығарады. Содан кейін оларды стандартты әдіс арқылы өңдейді. Сонымен PPP кадрінен IP, IPX немесе NetBEUI дестелерін бөліп шығарады да, локалды желі бойымен таратады.

Көппротоколдылық – арналық деңгейдің инкапсуляциялайтын протоколдарының негізгі артықшылығы. Оларға қорғалған арна протоколдарының алдындағы жоғарғы деңгей протоколдары PPTP протоколы жатады. Мысалы IPSec немесе SSL протоколдары желілік деңгейдің тек қана бір протоколымен байланыса алады – IP. Сондықтан олар егер де бірлескен желіде IPX немесе NetBEUI қолданылса пайдаланылмайды.

Арналық деңгейде деректерді қорғау қолданбалы және желілік деңгей протоколдары үшін мөлдір болады.

PPTP протоколында оның екі қолдану сұлбасы анықталған. Бірінші сұлбада PPTP протоколы қашықталған рұқсат серверімен ISP және бірлескен шекаралық маршрутизатормен қолданады. Екінші сұлбада қорғалған арна қашықталған рұқсат серверімен RAS (Remoute Access Server), ISP (Internet Service Provider) Интернет провайдерімен және шекаралық

маршрутизатормен жасалынады. «Шлюз-шлюз» типті қорғалған арна нұсқасы, сондықтан қашықталған пайдаланушы компьютері PPTP протоколын қолдамауы керек. Пайдаланушы ISP орнатылған PPP стандартты протоколының көмегімен RAS серверімен байланысады және провайдерден аутентификациядан өтеді.

L2F (Layer 2 Forwarding)—екінші деңгейдегі дестелердің жылжу протоколы. Берілген протоколда аутентификация мен шифрлеу әдістері протоколдың өзгешеліктерін анықтамайды. PPTP протоколына қарағанда L2F протоколы Интернет провайдеріне қашықталған рұқсат үшін PPTP протоколынан басқа SLIP протоколын қолданады. Глобалды желі бойымен Интернет провайдеріне қорғалған арналарды құрастырған кезде адрестердің конфигурациясы мен аутентификациясын орындау қажет емес. Одан басқа қорғалған тоннель бойымен деректерді тасу үшін желілік деңгейдің әртүрлі протоколдары қолданылу мүмкін. PPTP пртоколында сияқты тек қана IP емес. L2F протоколы Cisco Systems кәсіпорынының IOS (Internetwork Operating System) операциялық жүйесінің компоненті болды және осы кәсіпорынмен шығарылатын қашықталған рұқсатпен және желі аралық өзара байланыс барлық құрылғыларында қолданылады.

L2TP (Layer 2 Tunneling Protocol) – екінші деңгейдің тоннелді протоколы. PPTP мен L2F протоколдарының ең жақсы қасиеттерін алған. Оны көптеген өндірушілер және Cisco, Microsoft, 3Com, Ascend кәсіпорындары қолдайды. L2TP протоколы PPP протоколының арналық деңгейдегі кеңейтілуі болып табылады және кез-келген жоғарғы деңгейдегі протоколдарды қолдай алады.

2.2.3 Желілік деңгейде деректерді қорғау. Үлестірілген бірлескен желілерді (VPN интранеті мен VPN экстранеті) құру кезінде желілік деңгей протоколдарын SKIP және IPsec қолдану мақсатқа лайықтырақ.

SKIP (Simple Key mamagement for Internet Protocol) протоколдары - 1994 жылы Sun Microsystems кәсіпорынмен өңделген, Интернеттегі криптографиялық кілттермен басқару протоколы. SKIP протоколының негізіне Диффи-Хеллман ашық кілттер криптографиясы жатады. SKIP протоколы бар трафикті шифрлеу жүйелеріне қарағанда бірнеше маңызды ерекшеліктері бар:

- әмбебаптылығы – Оларды жасайтын процестер немесе пайдаланушылар, қосымшалар туралы ештеңе білмей IP дестелерін шифрлейді. Компьютерде орналасқан дестелік драйвер үстіндегі, жоғары жатқан бағдарламалық қамтамасыздандыруларға және оларқолданылатын физикалық арналарға ешқандай шектеулер жасамай толық трафикті өңдейді.

- сеансттан тәуелсіздігі - өзара әсерлесу қорғанысын қамтамасыз ету үшін қосымша ақпараттық алмасу қажет.

- шифрлеу жүйесінен тәуелсіз – пайдаланушы жабдықтаушымен немесе өзінің кез-келген ақпаратты шифрлеу алгоритмін қолдана алады.

IPsec протоколдар жүйесі. Internet Protocol Security (IPSec) ашық стандарттар жүйесі болып табалады. Қазіргі кезде оны жаңа протоколдармен, алгоритмдермен және функциялармен толықтыруға мүмкіндік береді.

Ipsec жүйесі төмендегідей негізгі қорғалған арнаны қолдау мен орнату есептерін шешеді:

- қорғалған арнаны инницияциалау кезінде компьютерлерді немесе пайдаланушыларды аутентификациялау;
- қорғалған арнаның соңғы нүктелері арасында таратылатын деректерді аутентификациялау және шифрлеу;
- арнаның соңғы нүктелерін автоматты түрде құпиялы кілттермен қамтамасыз ету, деректерді шифрлеу мен аутентификация жұмыстары үшін қажет.

Қойылған талаптарды шешу үшін IPsec жүйесі үш түрлі протоколдарды қолданады:

- AH (Authentication Header) таратылатын дестелердегі деректер көзінің аутентификациясы мен бүтіндігін қамтамасыз етеді.
- ESP (Encapsulation Security Payload) таратылатын деректердің бүтіндігі мен аутентификациясын қамтамасыз етеді;
- IKE (Internet Key Exchange) қорғалған арнаның инициациалау әдісін анықтайды және де қорғалған қосылу аумағында құпиялы кілттермен алмасу мен басқару процедураларын қамтамасыз етеді.

IPSec деректерді шифрлеу үшін құпиялы кілттерді қолданатын кез-келген симметриялы шифрлеу алгоритмі қолданылуы мүмкін. Деректердің аутентификациясы мен бүтіндігі деректердің дайджестін есептеу арқылы, біржақты функция көмегімен орындалады. Оның ішіндегі парамметрлер құриялы кілттер болып келеді.

IPSec негізгі шектеулеріне IP протоколымен желілік деңгейдегі деректерді тарату үшін қолданылатын қосымшаларды ғана қолдайды. Ол IPX немесе NetBEUI қосымшаларының IPSec қамтамасыз ететін қорғаныс функцияларын қолдана алмайды. Осындай шектеулер таратылатын деректерді қорғау бойынша барған сайын азая береді. Себебі қазіргі кезде компьютерлерің аз бөлігі ғана IP қолдамайды. Компьютерлердің көбі оны жалғыз протокол немесе көп протоколдың бірі ретінде қолданады.

IPSec протоколы L2TP немесе L2F протоколдарымен жұмыс істей алады. Олар тек қана туннелдеуді орындайды, деректердің шифрленуі мен аутентификациясын қамтамасыз ете алмайды.

3 Виртуалды жеке желілердің моделін құру

3.1 VPN жүзеге асыру үшін желілік ресурстарды тиімді үлестіру мәселелері

Қызмет көрсету сапасы SLA (Service Level Agreement) келісімінде анықталатын VPN нақты қызмет сапасына кепілдеменің орындалуын талап етеді. Егер жалға алынған арналар толығымен оқшауланған болса және желінің кепілденген сипаттамаларын қамтамасыз етсе (өткізу жолағы, кідіріс, джиттердің ығысуы, дестелердің жоғалуы және т.б.) SLA анықталған қызмет сапасының кепілдемелерін қамтамасыз ету үшін VPN сәйкес механизмдер қарастырылуы керек. Осында әртүрлі VPN жалпы бөлінетін желілік ресурстарына қақтығыс талаптарына мәселелер туады. VPN қызметтер провайдерінің қазіргі заманғы жоғарғы бәсекелестік базарындағы шарттарында осы мәселені шешу қарастырылған. Бір жағынан – желінің максималды жүктелуін қамтамасыз ету және максималды желілік табыс алу, екінші жағынан пайдаланушыларға қызметтің сапалы кепілдемесін және оның минималды бағасын қамтамасыз ету.

Соңғы уақытта деректер дестесінің трафигі кез-келген деңгей мен түрлі телекоммуникациялы операторлар үшін табыс көзі болды. Сондықтан IP желілері қарқынды орнатылуда. Оператор желіден мүмкіндігінше көп алуға тырысады. Сондықтан IP желілерінде ресурстарды тиімді үлестіру әдістері кең таралуда.

IP желісінің біріншіден, маршрутизаторлар мен байланыс арналарының, толық желілік ресурстарын рационалды түрде қолданылмай максималды коммерциялық әсері болмайды. Дестелік желіні қолдануды әсерлі деуге болады. Әр желі жүктелген, бірақ шегінен аспауы керек. Ол ресурстарды қолдану коэффициентті бірге жақын екендігін көрсетеді. Бірақта, қатты жақын болмауы керек. Себебі, дестелердің кезегі үлкен болса, маршрутизаторлардың ішкі буферінің толуынан жоғалтулар мен кідірістерді туғызады.

IP желісін басқару мәселерін екі мақсатқа жетуден құралады. Біріншіден, таратылатын трафиктің көрсетілетін қызметінің сапасын жоғарылату жатады. Кідірістерді төмендету, жоғалтуларды азайтуға және трафиг ағынының интенсивтілігін жоғарылату керек. Ол пайдаланушылардың санын көбейтеді және бәсекелестер соғысында жеңіске жетуге мүмкіндік береді. Екіншіден, желінің толық ресурстарын жүктеу таратылатын трафик көлемін жоғарылату үшін максималды болу керек.

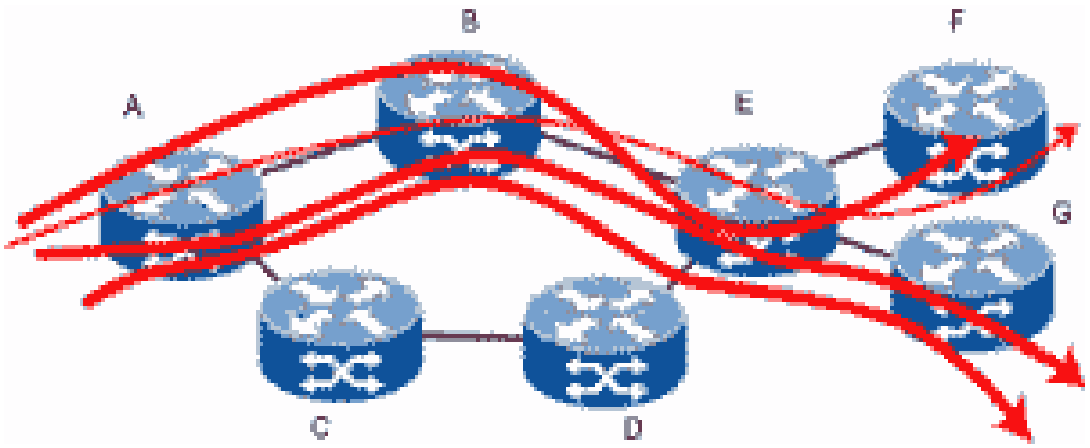
Соңғы уақытқа дейін IP желісіндегі ресурстарды тиімді қолдану есептері жеке маршрутизаторлар арқылы өтетін әртүрлі ағындарды үлестіру көмегімен жүзеге асырылатын. Қызмет көрсету сапасы QoS (Quality of Service) деп аталатын әдістер жиынтығы осындай есептерді шешеді. IP желісінде дәстүрлі қолданылған желі арқылы трафиктің өту жолдарын таңдау әдісі өте аз масштабта қолданылған. Трафиктің жүру жолдарынан біріншіден

маршрутизаторлар мен арналардың жүктелуі тәуелді болады. Осыдан шығатыны желінің тиімділігі.

Маршрутизацияның барлық протоколдары – дистанционды-векторлы сияқты (мысалы, RIP), олар байланыстың жағдайынан негізделген (OSPF және IS-IS), нақты желіге бағытталған трафик үшін қысқа жолды анықтайды. Таңдалған жол байланыс арналарының номиналды өткізу қабілеті немесе олармен жасалынған кідірістер есепке алынса тиімді болады. Бастапқы және соңғы желілер арасындағы аралық маршрутизаторлар санын есепке алса, онда таңдалған жол тиімсіз болуы мүмкін.

Мұндай әдістің тиімсіздігінің классикалық мысалы ретінде 3.1 сурет көрсетілген желі топологиясы жатады. Мұндай топология «балық» деп аталады. А және Е маршрутизаторларының арасында екі жол болғанына қарамастан: жоғарғысы, В маршрутизаторы арқылы, ал төменгісі С және D маршрутизаторлары арқылы, - толық трафик IP желісінде қабылданған, маршрутизация қағидаларына сәйкес А-дан Е-ға дейін жоғарғы жолмен бағытталады. Төменгі жол кішкене ұзын болғандықтан ескерілмейді. Бірақта жоғарғы жолмен параллельді жұмыс істеуге болар еді.

Екере кету қажет, желіде бір-біріне бағалары ұқсас маршруттар болған кезде трафик олардың арасында бөлінеді және байланыс арналары мен маршрутизаторларға жүктеме теңдей үлестіріледі. Бағасы ұқсас маршруттардың қысқа жолдан төмен болса, онда мұндай құрылғы жұмыс істемейді. [6]



3.1 сурет– Маршрутизация протоколдарымен анықталатын, жолдарға ресурстарды тиімсіз жүктеумен желі топологиясының мысалы

IP желісіндегі трафикті дәстүрлі маршрутизация әдістерінің негізгі кемшілігі желі ресурстарының жүктелуін ескерусіз жолды таңдау жатады. Егер қысқа жол жүктелген болса, онда дестелер бәрібір соны күтіп тұрады. 3.1 сурет көрсетілген желіде А-дан Е-ға дейін трафикқа қызмет көрсету үшіноның ресурстары жетіспейтін болса, онда жоғарғы жол жұмыс істейді. В және С маршрутизаторлар ресурстары сапалы қызметке жеткеннің өзінде де төменгі

жол тоқтап тұрады. Желі ресурстарын үлестіру әдісінің кемшілігіне - оның біреуі артығымен жүктеледі де, ал қалғандары бос болып тұрады. QoS ешқандай әдістері мұндай кемшілікті шеше алмайды. Басқа сапалы механизмдер қажет.

IP желілерінде бұрын қолданылмайтын, бірақ күшті әдістерінің біріне желі ресурстарын тиімді қолдануына әсер ететін Traffic Engineering (TE) технологиясы жатады. Сөзбе-сөз аударғанда «трафиктің инжинирингі» деп аталады. TE желі арқылы трафиктің өту жолдарын тиімді таңдау арқылы желі ресурстарын тиімді жүктеу механизмдері мен әдістері жатады.

Жолдарды таңдау үшін бастапқы мәліметтерге жатады: біріншіден, таратын желі сипаттамалары – топология, және оны құрайтын байланыс арналары мен маршрутизаторлар өнімділігі. Екіншіден, желі жүктемесі туралы ақпараттар, өзінің шекаралық маршрутизаторлары арқылы таратын трафик ағындары жатады. Әр ағын желіге кіретін нүктесімен, одан шығатын нүктесімен және басқа да трафиктің парамметрлерімен сипатталады. Себебі, жолды таңдау кезінде байланыс арналары мен маршрутизаторлардың бірдей жүктелуін қамтамасыз етуге тырысады. Онда әр ағын үшін оның орта интенсивтілігін ескеру керек. Желідегі трафиктің тиімділігі үшін әр ағынды оданда нақты бейнелеу керек. Мысалы, трафиктің мүмкін болатын пульсация мәні немесе көрсетілетін қызмет сапасына қойылатын талап – кідірістерге сезімділік, кідірістер түрленуі және дестелердің жоғалуының рұқсат етілген пайызы. Бірақта, мұндай трафик парамметрлерін бағалау қиынға соғатындықтан, орта интенсивтілікке қарағанда, олардың желі жұмыс істеуіне әсері маңызды емес. Әдеттегіде, желі арқылы ағындардың өтуінің тиімді үлестірілген жолын анықтаған кезде, олардың орта интенсивтілігінің парамметрі ескеріледі.

TE есебіне желі арқылы трафик маршруттар ағынын анықтау жатады. Әр ағын үшін аралық маршрутизаторлардың тізбегін және ағынның кіріс пен шығыс нүктелері арасындағы жолдағы олардың интерфейстерін көрсету қажет. Сонымен қатар, желінің барлық ресурстары тиімді жүктелген болуы керек. Бұл шартты әртүрлі әдістермен жүзеге асыруға болады. Мысалы, ресурсты қолданатын максималды коэффициент: барлық желі ресуртар бойымен минималды болуы керек, себебі трафикке аз залал келтіру үшін. RFC 2702 «Requirements for Traffic Engineering Over MPLS» TE есбі нақ осылай құралады. Берілген құжатта Инженерлі қолдау тобының жалпы рекомендацияларынан тұратын TE есептерін шешу бойынша MPLS белгі бойынша коммутация технологияларының көмегімен жолдарды тиімділеу функциясы ретінде төмендегі формула ұсынылған:

$$\min (\max Ki), \qquad (3.1)$$

мұндағы K_t — і-ші ресурсты қолдану коэффициентті.

ТЕ есебін шешудің басқа әдісіне ресурсты қолданатын барлық коэффициенттер $K_{тлх}$ берілген шекті аспауы керек. Мұндай әдісті жүзеге асыру өте оңай, ол көбінесе тәжірибеде қолданылады.

ТЕ терминін мүмкін болатын парамметрлерді өзгерту арқылы желіні глобалды тиімділеу түсінігі жатады: маршрутизаторлардың саны мен өнімділігі, олардың арасындағы байланыс топологиялары, деректерді тарату арналарының жылдамдығы, ағындардға қызмет көрсету жылдамдығы және т.б. Басқарылатын парамметрлерге жүктеме парамметрлері қосылады. Мысалы, желімен таратылатын ағындардың интенсивтілігі – желі артық жүктелген кездеоны белгілі-бір шекке дейін шектеуге болады. [7]

Мұндай глобалды әдіс Traffic Engineering (TEWG) IETF RFC 3272 «Overview and Principles of Internet Traffic Engineering» жұмыс тобының негізгі құжатында қабылданған. Көрсетілген құжатта ТЕ технологиясына келесі негізгі уақыттық масштабтар жатады:

1. Нақты уақытта басқару. Парамметрлер бір секунд периодпен немесе микросекунд периодпен өзгертіліп отыры. Мұндай тұрге маршрутизаторларда қызмет көрсету сапасын қамтамасыз ету әдістері жатады.

2. Бірнеше минут немесе күндер периодымен парамметрлерді оперативті басқару. Желі арқылы трафиктің өту жолдарын таңдау әдістері жатады. Трафиктің жүру жолдары бірнеше сағат немесе күндер ұзақтығымен ағындар интенсивтілігінің өзгеру тұрақтылығын көрсететін мәндер кезінде өзгереді. Әр түйінде QoS әдісі арқылы тез орындалады.

3. Желіні жобалау. Бірнеше жетіде немесе күнде желі парамметрлерінің өзгеруін регламенттейді. Мұндай жағдайда парамметрлер ретінде желінің құрылымдық сипаттамалары айтылады: маршрутизаторлар саны мен түрі, байланыс арналарының топологиясы мен түрі және басқа да парамметрлер қаражат пен уақытты қажет ететін.

Тафикті инжинирингілеу кезінде жалпы жағдайда желі арқылы трафик ағындарының жүру жолдарын басқару желі тиімділігінің бір ғана әдісі ретінде болады. IETF «A Framework of Network Engineering» құжатында Internet Draft дәрежесі бар мүмкін болатын желіні тиімділеу әдістерінің ішінен екі классты бөліп шығарды:

- желілік инжинерия әдісі (Network Planning). Маршрутизаторлар арасында физикалық арналардың өткізу қабілетін оперативті өзгеруін қамтамасыз етеді;
- желіні жобалау әдісі (Network Planning). Желідегі маршрутизаторлар санының өзгеруіне, олардың өнімділігі және байланыс арналарының топологиясына негізделетін ұзақ уақытты шешімді жүзеге асырады.

Сонымен қатар, Traffic Engineering терминіне желі арқылы трафик жолдарын таңдау жатады. IP Желілерінде жолдарды таңдау мен орнату құралдарына қазіргі кезде MPLS технологиясы жатады. Ол X.25, Frame Relay және ATM желілерінде виртуалды арналар концепциясын дамытады және қолданады.

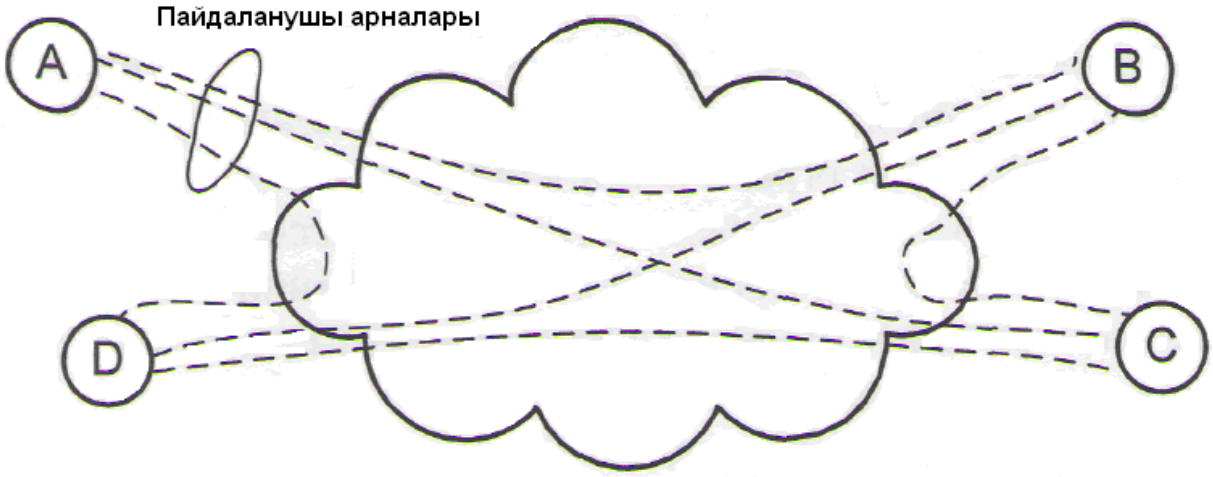
MPLS технологиясы IETF құжаттарында жеткілікті стандартталған және IP желісі үшін құралдарды шығаратын алдыңғы қатарлы өндірушілермен қолданады.

Кезек бойынша жолдарды іздеу TE сапасын төмендетеді – бір уақыттың ішінде ағындарды қарастырған кезде ресурстардың тиімді жүктелуін табуға болады. Қазіргі кезде шығарылатын құрылғыларда ағындарды тізбектей қарастырумен MPLS TE нұсқасы қолданылады. Ол OSPF және IS-IS протоколдары үшін стандарттарға жақын және жүзеге асырылуы қарапайым. Одан басқаға, жағдайдың өзгеруі кезінде жаңа ағындардың пайда болуы немесе бар ағындардың интенсивтілігі өзгерген кезде бір ағын үшін жолды табуға болады.

Бірақта, сыртқы ағындар жиыны үшін тиімді шешім табуға болады, автономды режимде. Осы жүйе қосымша жүйелер есептеулерінен тұруы керек. Тиімді шешімді тапқаннан кейін жолдарды іздеуді оперативті режимде өзгертуге болады.

3.2 Арналық модель

3.2.1 Арналық модель түсінігі. Әртүрлі жеке виртуалды желілер бойымен жалпы қолдану желі ресурстарын үлестіру VPN соңғы бір нүктесінен басқа нүктелерге жеке линияларын классикалық эмуляция арқылы жүзеге асыруға болады. Осындай әдіс арналық (pipe) модельді қолданады. VPN арналық моделі жалға алған (жеке) линия қызметіне ұқсас.Пайдаланушы жеке виртуалды арналарды (customer-pipes) жалға алу керек және VPN «көз - алушы» сәйкес өткізу жолағын сұрау керек. 3.2 сурет VPN арналық моделі көрсетілген. Желілік провайдер әр арна үшін толық желі бойымен трафиктің нақты қызмет көрсету деңгейіне кепілдеме беріп, өткізу жолағын қамтамасыз етуі керек.



Провайдер желісі VPN қызметтерінің

3.2 сурет– Пайдаланушы арналарының моделінің негізіндегі VPN

Мұндай әдістің негізгі кемшілі пайдаланушы матрица түрінде берілген VPN барлық соңғы нүктелерінің арасында берілген трафикті алдын-ала білу керек. Одан басқа, бір пайдаланушы арнасы үшін арналған желілік ресурстар басқа пайдаланушының трафигін тарату үшін қолданылмайды. Ол желілік провайдер үшін өте маңызды. Себебі ол әртүрлі көздердегі бір магистралды арна ақпаратын статистикалық мультиплексирлеу арқасында пайдаға жете алмайды.

Арналық модель базасындағы VPN құрудың негізгі мәселесі әртүрлі арналар бойымен желілік ресурстарды тиімді үлестіру болып табылады. Әр желі аймағындағы шектелмеген өткізу жолағы кезінде, осы мәселе бөлшектенген есептерді шешуге тіреледі. Тиімділік тұжырымдамаларына сәйкес әр VPN тиімді топологиясын таңдау: пайдаланылатын өткізу жолағының бағасының қосындылары, берілген парамметрлердің тарату трафигінің сапасы, берілген арналардың қосындысы. Сонымен қатар, бір VPN үшін мұндай тиімділік есебін шешу басқа VPN үшін әсер етпейді. Бірақта, іс жүзінде желінің бөлек аймақтарының өткізу қабілеті шектелген болады. Мұндай кезде бір VPN үшін арналған өткізу жолағы басқа VPN үшін желілік ресурстарды үлестіру есептеулеріне әсер етеді. Осының бәрі әртүрлі VPN пайдаланушылары үшін арналған провайдердің желілік ресурстарды тиімді үлестіру есептеулерін күрделендіреді.

3.2.2 Арналық модель базасында VPN үйлесімділеу мәселелері. Арналық модель базасында виртуалды жеке желілерді тиімді құру мақсатына IP- желінің магистралды арналарында өткізу қабілетін үлестіру жатады. Пайдаланушылардың трафигі VPN тиімді маршрутталуы керек. Сонымен қатар, оператордың немесе сервис-провайдерлің инфрақұрылымы арқылы таратылған трафиктің өлшенген топталған мәні максималды болу керек. Мұндай өлшенген өлшемге желіде жүзеге асырылған VPN провайдерге әкелген табыс жатады. Ескере кету қажет, VPN құру есебіне – ол екі жақты есеп. Себебі, ол әр VPN мен әр VPN трафик желісінде тиімді маршрутизацияны біріктіріп жүзеге асыру үшін желі ресурстарын тиімді үлестіру есептерінің жинағы болып табылады. Мультиплексирленген трафикті жүзеге асыру берілген қызмет сапасын қамтамасыз ету үшін әр VPN ішіндегі маршруты мен қызметі арқылы жасалынады, желідегі жүзеге асырылған барлық VPN емес. VPN құру кезінде қызмет провайдері әртүрлі клиенттермен SLA (Service Level Agreement) қызмет деңгейімен қорытынды келісім шартқа отырады. Ол өз желісінің инфроқұрылымы бойымен олардың мультисервисті трафигін әсерлі таратуын қамтамасыз ету керек. Берілген есепті шешу үшін сәйкесінше математикалық модельдер, оларды анализдеу әдістері мен сәйкес қолданбалы бағдарламалық өнімдер қажет. Одан әрі арналық модель негізіндегі VPN тиімді құру есептерін шешу әдістері қарастырылады.

Әр VPN - ол берілген жұптың соңғы нүктелері арасындағы нақты түрдегі трафикті өткізетін жеке желі. Әрине, VPN соңғы нүктелері арасындағы трафикті тарату маршруттының жеке жиынтығы әр VPN болады.

Сонымен қатар мультисервисті трафиктің мәні соңғы нүктелер жұбының арасында әр VPN сипаттайтын маңызды компонент болып табылады.

VPN құру есебінің соңғы мақсаты болып, берілген желіде жүзеге асырылған барлық VPN желідегі табысының қосындысын максималды жасау. Берілген есепте түрленетін айнымалыларға жеке VPN үшін желінің жеке тармақтарының өткізу қабілетін тиімді үлестіру немесе желіде рұқсат етілген VPN әр соңғы нүктелеріне түсетін жүктеменің мәндері жатады. Сонымен, берілген желіні құру есебі VPN арасында желілік ресурстарды үлестірумен немесе VPN трафигінің бақылау маршрутизациясымен теңдестіріледі. Бірақта, құру әдісі жеке VPN үшін желінің өткізу қабілетін үлестіруді ескерумен трафикті маршрутизациялау есептерін бірігіп шешу арқылы жүзеге асырылады. Себебі, өткізу жолағын алған кезде оның бағасын ескеру қажет. VPN құру есебін шешу минималды шығындармен жүзеге асырылу керек.

ATM технологиясында қолданылатын VPN жүзеге асырудың арналық моделін зерттеуге 90 жылдардың ортасында жарияланған бірнеше жұмыстар арналған. Ең алдымен D. Mitra, J.A. Morrison, K.G. Ramakrishnan және тағы басқалардың жұмыстары. VPN жеке звеноларының өткізу қабілетін тиімді үлестіру есептерін шешу жұмыстарында бастапқы нүктемен теңдеулерін рекуррентті шешумен базаланады және желідегі табыстардың жоғалуын есептеу әдістерін қолданады.

VPN құрудың ең басты мәселесіне қолданылатын есептеу әдістерінің масштабтылығын қамтамасыз ету жатады. Аналитикалық әдістер бірдей стандартты жылдамдықтар үшін (мысалы, негізгі цифрлы арналар үшін) әсерлі. Олар E1 немесе E3 ағындары үшін масштабталмауы мүмкін. Мұндай кезде асимптотикалық аппроксимацияның әртүрлі әдістері қолданылмауы мүмкін. Іс жүзінде араласқан әдіс қолданылады. Кішкентай өткізу жолағымен звенолары үшін таңдалған нақты әдістер қолданылады және үлкен өткізу қабілетімен звенолары үшін асимптотикалық әдістер қолданылады.

VPN кейбір жиынтығының желісінде жүзеге асыру есептеріне желілік ресурстарды тиімді бөлу (Complete Partitioning) әдістерін таңдау жатады. Мысалы, желілік инфроқұрылымның ресурстарын толық бөлуді қолданғанда жеке VPN арасында табыстың жоғалуы пайда болады. Альтернативті әдіске барлық VPN желі ресурстарын (Complete Sharing) бірігіп қолдану жатады. Звенолар ресурсы толығымен қолданылады. Бірақта, онда әртүрлі VPN жүктемелерін қорғау мен қауіпсіздігін қамтамасыз ету қыйынға соғады. Одан басқа иерархиялық виртуалды бөлу қолданылу мүмкін. Осы әдіс VPN бойынша желілік ресурстарды және де әр VPN ішінде қызмет көрсету класстаран бөлуді басқаруды орындайды.

3.2.3 Арналық модельді үйлесімділеу әдістемесі. Желі инфроқұрылымы N түйіндермен және M цифрлы линиялардан тұрсын. Олар екі түйінді өткізгіш қабілеті U_m бит/с тең m звеномен қосады. Звенолар еркін нөмірленген және бірбағытты болып келеді. Трафикті бір бағытта ғана таратады. Сонымен қатар желіде K жүктеме ағыны таратылады деп болжаймыз. m звеносындағы $к$ классты тапсырыс қызметі үшін $Wкm$ бит/с тең өткізу жолағы қажет.

Негізгі тарату бірлігі δ түсінігі еңгізілген. Ол желідегі барлық сандық қосылу линияларының $u_1,...,u_м$ өткізу жолағының және *к** классты шақыруға қызмет көрсету үшін қажетті өткізу жолағына қойылатын талаптардың w_1, ..., w_K, ең үлкен бөлгіш ретінде δ тарату бірлігі еңгізілген (ЕҮБ). Сонымен,

$$\delta = НОД(u_1,...,u_м, w_1...,w_K). \qquad (3.2)$$

Нәтижесінде m-ші звеносының өткізу жолағының бүтін санды бейнелейміз $u_m = U_m$ /δ негізгі тарату бірлігі ретінде және *к* классты шақыру үшін өткізу жолағына қойылатын талаптарды бүтін санды нәтиже аламыз
$Wkm = W_{km}/\delta$ негізгі тарату бірлігі ретінде.

Жоғарыда көрсетілген әдіс араналар коммутациясымен желілердің моделін зерттеген кезде телетрафик теориясында дамыған дестелік коммутациямен желілер үшін модельдер мен әдістерді қолдануға мүмкіндік береді.Арнаның аналогы ретінде тарату бірлігі болады.

Барлық VPN үшін желі ресурстары берілген болсын, олардың саны *S* тең.
к звеносындағы s-ші VPN үшін өткізу жолағын былай белгілейміз u_{ks}. Содан, шығады $\sum_{s=1}^{S} u_{ks} = u_k$. Атап кету қажет, берілген формулада қосу *к* звеносынан өтетін VPN тарату трафигінің маршруттарына жүргізіледі.

«Көз және адресат» түйіндерін *h* символы бейнелесін, ал *(k,h)* - «көз және адресат» *h* арасындағы *к* сервис түрімен шақыру ағындары. Олардың мәндері *s* VPN қатысты болады. Олар төменгі *s* индекспен бейнеленген. $(k,h)_s$ ағындары үшін мүмкін маршруттардың жиыны $R_s(k,h)$ былай бейнеленген. Олар анықталған және белгіленген деп болжанады. Жалпылығы үшін маршруттар жиыны сервис түрінен тәуелді деп аламыз. Мысалы, кідірістерге сезімтал трафик (дыбыстық, видео және т.б.) қысқа маршруттармен жүреді.

Шақыру жоғалып қалу мүмкін, егер маршрут бойымен қажетті өткізу жолағын қамтамасыз ететін звено болмаса. Шақыру қабылданаған болса, осы шақыруға қажетті өткізу жолағы әр звенода шақырудың ұзақтығына қажетті өткізу жолағы алынады.

VPN $(k,h)_s$ түсетін шақырулар $L(k,h)_s$ орта мәнімен Пуассон заңына сәйкес үлестірілген болсын, ал $r \in R_s(k,h)$ - *h* жұбының арасында нақты маршрут. Сонымен қатар, резервіленетін өткізу жолағын алу уақыты $1/ z_{khs}$ орта мәнімен экспоненциалды заңмен үлестірілген болсын және алдындағы қызмет көрсетілген шақырулар мен оларға кеткен уақыттан тәуелсіз болады.

Нақты *r* маршрутпен $(k,h)_s$ шақыруларының арасындағы интервалдар $l(k,h)_s$ орта мәнімен пуассонды үлестірілген.

$$\sum_{r \in R_s(k,h)} l(k,h)_s \le L(k,h)_s \qquad (3.3)$$

Сәйкес трафиктің интенсивтілігі $q(k,h)_s = l(k,h)_s/z(k,h)_s$, осыдан шығады,

$$\sum_{r \in R_s(k,h)} q(k,h)_s \le Q(k,h)_s \qquad (3.4)$$

мұндағы $Q(k,h)_s=L(k,h)_s/z(k,h)_s$.

Жоғарыда көрсетілген моделді қолданып арналық модель базасында VPN жүзеге асыру үшін желілік ресурстарды тиімді қолдану есебін жасаймыз.

s-ші VPN r маршрутымен *к* түрлі шақыруды таратудың бірлік уақыт ішіндегі алынған $d(k,h)_s$ арқылы табысты белгілейміз. Ал $P(k,h)_s$ — r маршрутындағы шақырудың жоғалуының ықтималдығы.Себебі, $q(k,h)_s$ (1 - $P(k,h)_s$) *r* маршрутындағы *к* түрлі өткізілген жүктеме. s-ші VPN үшін орта табыс төмендегі формуламен анықталады:

$$D_s = \sum_{(k,h)_s} \sum_{r \in R_s(k,h)} d(k,h)_s q(k,h)_s (1 - P(k,h)_s). \qquad (3.5)$$

Барлық *S* VPN алынатын жалпы табыс

$$D = \sum_{s=1}^{S} D_s \qquad (3.6)$$

Әдеттегіде табыс $d(k,h)_s$ шақыру түрі талап ететін қажетті өткізу жолағына пропорционалды. Бірақта, басқа да критерилер қолданылуы мүмкін. Мысалы, табыс көзбен адресат арасындағы арақашықтыққа байланысты болады.

VPN тиімді жобалаудың есебін жалпы түрде төмендегі формуламен көрсетуге болады:

Табу

$$\max_{\{u_{ms}\},\{q_{khs}\}} D \qquad (3.7)$$

Кезінде

$$\sum_{r \in R_s(k,h)} q(k,h)_s \le Q(k,h)_s, \forall (k,h)_{s,} \forall s; \qquad (3.8)$$

$$q(k,h)_s \ge o, \quad \sum_{s=1}^{S} u_{ms} = u_m \forall m, u_{ms} \ge 0 \quad \forall s, \forall m. \qquad (3.9)$$

Желідегі VPN трафигінің тиімді маршрутизация есептерімен және ресурстарды үлестіру есептерінің қосылуы (3.2) есебінде көрсетілген. Алгоритмде есепті шешудің әр итерациясында VPN жүзеге асыру үшін желідегі звенолардың өткізу жолағын қайта үлестірумен жүргізіледі.

Әр VPN үшін өткізу жолағын қайта үлестіру есептері әр қайсысына жеке-жеке жүргізіледі және сызықсыз бағдарламалау есебіне жатады, ол (3.2) есебінде көрсетілген. Өткізу қабілетін қайта үлестіру есептері алдыңғы итерациялардағы тиімді маршрутизация есептерінен шығатын нәтижелермен есептелінеді. VPN арасындағы желі аймақтарының өткізу қабілетін қайта үлестіруді барлық VPN түсетін табыс өсіп тұратындай жасау керек. Ол үшін *m* звенодағы *s-ші* VPN берілген өткізу жолағының өзгеруінен табыстың тәуелділігін анықтау қажет:

$$\frac{\partial D_s}{\partial u_{ms}} \approx d_{ms} \qquad (3.10)$$

Онда табыстың жоғалу мәндерінің экстрополяциясы алынатын өткізу жолағын $\{u_{ms}\}$- ден $\{u_{ms} - b_{ms}\}$ *–ге* дейін төмендеткенде төмендегідей болады:

$$D_s(u_s - b_s) - D_s(u_s) \approx -\sum_{m=1}^{M} d_{ms} b_{ms.} \qquad (3.11)$$

Соңғы қадамда $\{b_{ms}\}$ тиімді мәнін таңдау үшін сызықты бағдарламалау есебі шығарылады және VPN арасындағы өткізу қабілетін жаңа үлестірулер шығарылады.

VPN әр звеносындағы жоғалтулар ықтималдығын және болжанатын табыс жоғалуын анықтау үшін Кауфмана-Робертс рекурсиясын қолданумен бастапқы нүктемен теңдеуді шешу әдістерін қолданамыз. VPN үшін бастапқы нүкте теңдеуі звенолар тәуелсіздігінен болжанатын негізден шығады. Әр *r* машруттан *к* типті сервис түрі таратылады және *r* маршрутына жататын *m* звеносы қолданылады $u_{km;r}$ өткізу жолағын алады. *m* звено қолданылатын r барлық маршруттарының $u_{кm;r}$ қосып, біз u_{km} *m* звеносына түсетін *к* классты жалпы жүктемесін аламыз.

Берілген есептің шешімінің алгоритммін екі бөлікке бөлуге болады: VPN бойынша желі ресурстарын үлестіру алгоритммі және VPN трафигін маршрутизациялау алгоритммі. Ә қосымшада алгоритмнің құрылымдық сұлбасы көрсетілген.

Есепті шешу үшін бастапқы мәндер болып:

S – VPN саны;

N — желідегі түйіндердің жалпы саны;

M — желідегі түйіндерді қосатын звенолардың жалпы саны;

К — көрсетілетін қызметпен қолданылатын сервис түрлерінің саны;

$u_m, 1 \le m \le M$, — әр звеноның жалпы өтткізу қабілеті;

w_{km}, $1 \le m \le M$, $1 \le k \le K$, — *m* звеносындағы *к* классты шақыруға қызмет көрсету үшін қажет өткізу жолағы;

$R_{(k,h)}$, $1 \le k \le K$, $h \in N \times N$, $1 \le s \le S$, — *s-ші* VPN үшін *h* кез-келген екі түйін арасындағы *к* сервис түрі үшін маршруттар жиыны;

$\bar{q}_{khs,}$, $1 \le k \le K$, $h \in N \times N$, $1 \le s \le S$, — *s-ші* VPN үшін *h* кез-келген екі түйін арасындағы *k* типті трафигінің интенсивтілігі;

d_{khs}, $1 \le k \le K$, $r \in R_s(k,h), h \in N \times N$, $1 \le s \le S$, — *s-ші* VPN *r* маршрутындағы *к* типті шақырудың бірлік уақыт ішіндегі алынған табыс.

Сонымен 3.2 есептің шешімінің нәтижесіне:

m звеносындағы *s-ші* VPN үшін белгіленген $1 \le s \le S, 1 \le m \le M$, U_{ms} өткізу қабілеті жатады;

s-ші VPN алынған $1 \le s \le S$, D_s жалпы табыс.

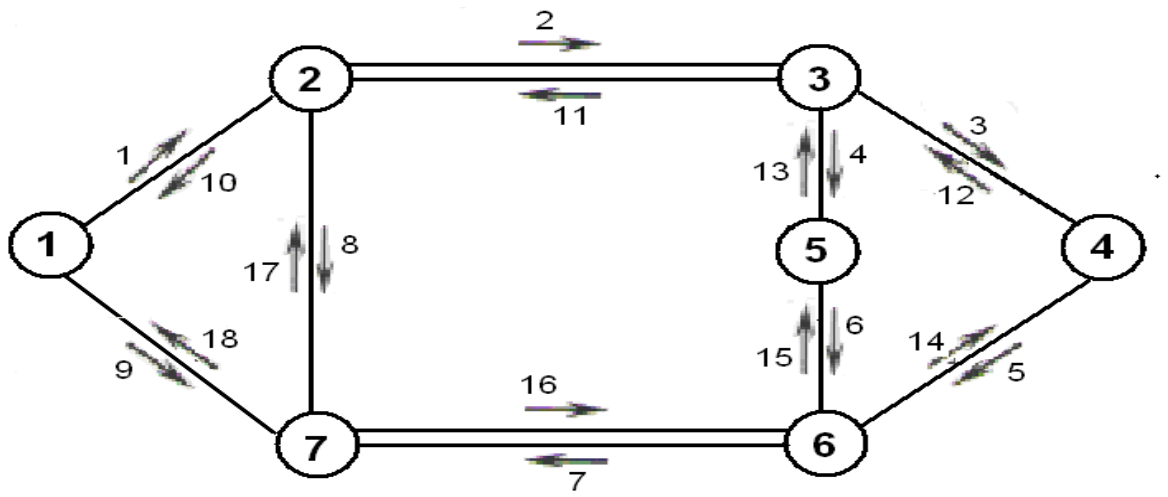
Алгоритмді шешу әдісі итерационды болғадықтан, әр итерацияда жеке VPN бөлінген өткізу қабілетін үлестіру қажет. Содан кейін алынған мәндерді әр VPN үшін тиімді маршрутизация әдісін шешу керек. Қызметті жабдықтаушымен алынған жалпы табысты максималды жасау керек. Басқаша айтқанда, өткізу қабілетін табыстың қосындысы үлкен болатын бір VPN беру керек. Алгоритмнің ұқсастығын тексеру үшін ұқсастық шегі түсінігін еңгіземіз.

$$\varepsilon = \frac{D_j - D_{j-1}}{D_j} \tag{3.12}$$

мұндағы *Dj* — j-ші итерациядан алынған табыс, ал D_{j-1} - (j - 1)-ші итерациядан алынған табыс.

Алгоритмнен көрінгендей, маршрутизацияны тиімді шешу есебінің шешімі әр VPN үшін бөлек орындалады. Сонымен, әр итерацияда маршрутизация есебін шешу үшін модуль *S* рет қолданылады.

Нақты мысалда VPN желілік ресурстарды тиімді үлестіру әдісін қарастырайық. Қарастырылатын желі жеті түйіннен *(N* = 7) және он сегіз бірбағытты еркін нөмірленген звенодан *(M* = 18) тұрсын 3.3 сурет көрсетілген.



3.3 сурет– Желі мысалы

VPN1							
Звено нөмірлері	1	2	3	4	5	6	7
1	0	70,8	48,0	7,2	62,4	34,8	13,8
2	82,8	0	165,6	21	214,2	103,8	41,4
3	55,2	172,8	0	13,8	127,8	62,4	24
4	7,2	21	10,2	0	12,0	6,0	3,6
5	76,2	227,4	134,4	15,0	0	70,8	31,2
6	34,8	96,6	55,2	6,0	62,4	0	13,8
7	13,8	34,8	21,0	3,6	27,6	13,8	0

VPN2							
Звено нөмірлері	1	2	3	4	5	6	7
1	0	18,0	48,0	3,6	31,2	17,4	7,2
2	21,0	0	165,6	10,2	106,8	51,6	21,0
3	55,2	172,8	0	27,6	255,6	124,2	48,0
4	3,6	10,2	21,0	0	12,0	6,0	3,6
5	37,8	114,0	269,4	15,0	0	70,8	31,2
6	17,4	48,0	110,4	6,0	62,4	0	13,8
7	7,2	17,4	41,4	3,6	27,6	13,8	0

VPN3							
Звено нөмірлері	1	2	3	4	5	6	7
1	0	18,0	24,0	3,6	31,2	17,4	13,8
2	21,0	0	82,8	10,2	106,8	51,6	41,4
3	27,6	86,4	0	13,8	127,8	62,4	48,0
4	3,6	10,2	10,2	0	12,0	6,0	7,2
5	37,8	114,0	134,4	15,0	0	70,8	62,4
6	17,4	48,0	55,2	6,0	62,4	0	27,6
7	13,8	34,8	41,4	7,2	55,2	27,6	0

VPN4							
Звено нөмірлері	1	2	3	4	5	6	7
1	0	18,0	24,0	7,2	62,4	34,8	7,2
2	21,0	0	82,8	21,0	214,2	103,8	21,0
3	27,6	86,4	0	27,6	255,6	124,2	24
4	7,2	21,0	21,0	0	47,4	23,4	7,2
5	76,2	227,4	269,4	59,4	0	283,8	62,4
6	34,8	96,6	110,4	23,4	248,4	0	27,6
7	7,2	17,4	21,0	7,2	55,2	27,6	0

3.4 сурет– VPN жүктеменің интенсивтілігінің матрицасы

Бір бағытты звеноның өткізу қабілеті 155 Мбит/с тең. Бірақта 2-ші мен 3-ші және 7-ші мен 6-шы түйіндері арасындағы звеноларынаның өткізу қабілеті 2х155 = 310 Мбит/с тең. Желіде үш сервис классы қолданылады. Осы қызметтердің бір шақыруының өткізу қабілетінің тиімділігі сәйкесінше 16, 48 және 160 кбит/с тең. Берілген мәндерді ескере отырып негізгі тарату бірлігі

ретінде 16 кбит/с тең жолағын аламыз. Сонымен, әр сервис классы үшін қажетті нормаланған жолақ *к* = 1, 2, 3 сәйкес барлық *m* үшін w_{km} = 1, 3, 10. Өткізу жолақтары 155 және 310 Мбит/с тең звенолардың сәйкесінше тарату бірліктері ретінде 9688 және 19375 көрсетуге болады. *m* = 1, *2, ..., M* үшін u_m —9688 немесе 19375 ретінде көрсету.

Провайдер желісі төрт VPN пайдаланушыларына қызмет етеді. Осы VPN соңғы нүктелері әр сервис түрінен әр нүктеден нүктеге трафикті құрайды. Түсетін жүктемені көрсету үшін әр VPN үшін NxN өлшемімен Y_s жүктеме интенсивтілігінің матрицасын қолданамыз 3.4 сурет көрсетілген. Ал к нақты сервисінің жүкеме интенсивтілігін анықтау үшін c_k коэффициентін қолданамыз. Ол 3.1 кестеде көрсетілген. Онда түсетін жүктеме интенсивтілігі і түйінінен j түйіні үшін $\bar{q}_{khs} = c_k Y_{ijs}$ тең, мұндағы $h = (i, j)$.

s VPN үшін *r* маршрутындағы бірлік уақыт ішндегі *к* классты шақыруының табысы, $d_{kh} = d_k \forall r, \forall s.$. Мұндай мән кезінде табыс өткізу жолағының бірлігіндегі өткізіген жолаққа тең.

Келесі қарапайым ереже негізінде маршруттар жиынтығы генерирленген: $R_s(k,h)$ = { *r*< 3 маршруттағы аралықтар саны} .

Әр VPN үшін маршруттардың жалпы мәні 90 тең. Сонымен желіде 360 маршруттар бар.

3.2 кестеде тиімді құру кезіндегі VPN арқылы түсетін және таратылған жүктеменің мәндері, барлық маршруттарға жүктеменің бірқалыпты үлестірілгені және сәйкесінше звенолардың өткізу жолағының пропорционалды үлестірілгені көрсетілген. Ескере кету қажет, бастапқы мәндерді ескерумен таратылған жүктеме желіден түскен табысқа ұқсас.

3.1 кесте– Нақты сервистің жүктемесінің интенсивтілігін анықтау үшін арналған коэффициенттер.

Сервис *к*	1	2	3
Коэффициент c_k	0,5	1,0	0,5

3.2 кестесінде көрінгендей жалпы желі бойынша тиімділеу алгоритммін қолдану табысты орта мәмен 5,4% үлкейтеді және жоғалтулар ықтималдығын екі есе төмендетеді.

3.2 кесте– Жүктемені бірқалыпты және тиімді үлестірілген кездегі VPN арқылы түскен және берілген жүктеме

VPN	Максималды табыс	Жүктемені бірқалыпты үлестіру		Жүктемені тиімді үлестіру	
		Табыс	Жоғалту ықтималдығы, %	Табыс	Жоғалту ықтималдығы, %
1	19721,7	17620,0	10,7	18871,5	4,3
2	18263,1	16074,8	12,0	17282,5	5,4

3.2 кесте – жалғасы

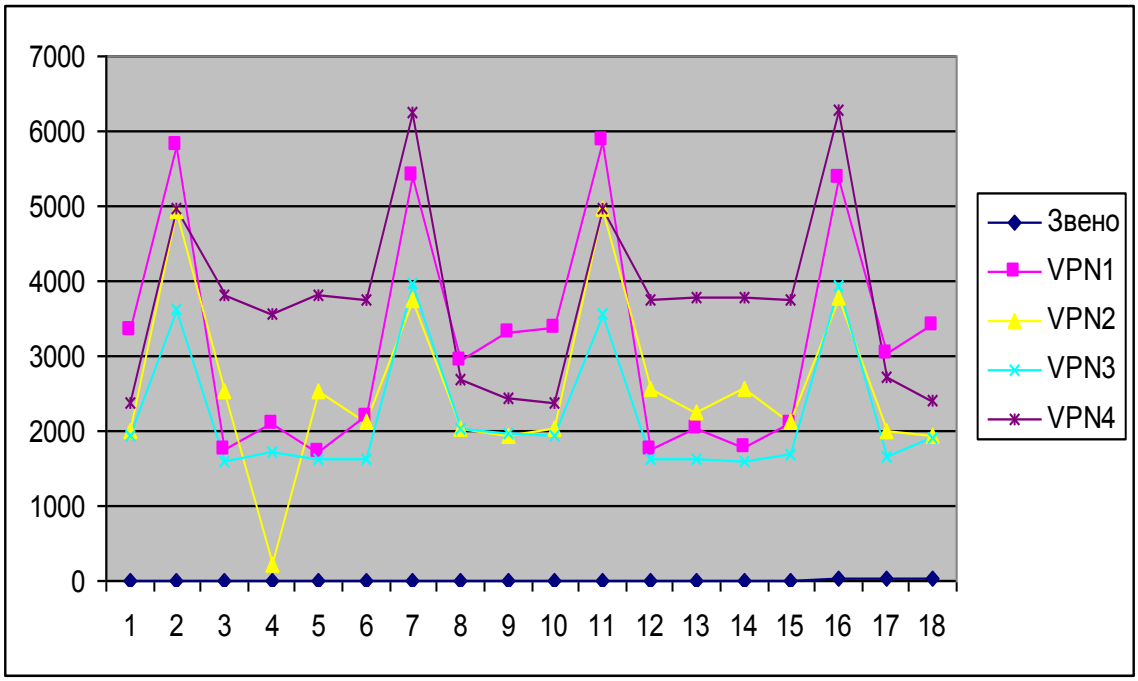
VPN	Максималды табыс	Жүктемені бірқалыпты үлестіру		Жүктемені тиімді үлестіру	
		Табыс	Жоғалту ықтималдығы, %	Табыс	Жоғалту ықтималдығы, %
3	14178,0	12469,9	12,0	13397,9	5,5
4	25035,9	21850,5	12,7	23430,0	6,4
Толық желі	77198,7	68015,2	11,9	72981,9	5,5

3.3 кестеде VPN арасында желінің жеке звеноларының өткізу жолағын үлестіру көрсетілген. Алынған мәндер бастапқы мәндерден 20% ауытқиды.

3.3 кесте– VPN арасында желінің жеке звеноларының өткізу жолағын үлестіру

Звено нөмірі	VPN1	VPN2	VPN3	VPN4
1	3355	2011	1942	2380
2	5828	4953	3626	4968
3	1756	2530	1591	3811
4	2102	229	1710	3577
5	1728	2535	1623	3802
6	2173	2128	1632	3755
7	5392	3753	3976	6254
8	2947	2021	2030	2690
9	3321	1947	1977	2443
10	3362	2016	1942	2368
11	5864	4974	3578	4959
12	1738	2578	1613	3759
13	2035	2245	1628	3780
14	1766	2573	1579	3770
15	2106	2139	1696	3747
16	5380	3780	3937	6278
17	3021	1992	1644	2731
18	3415	1943	1909	2421

3.5 сурет VPN арасында желінің жеке звеноларының өткізу жолағын үлестіруінің графигі көрсетілген.

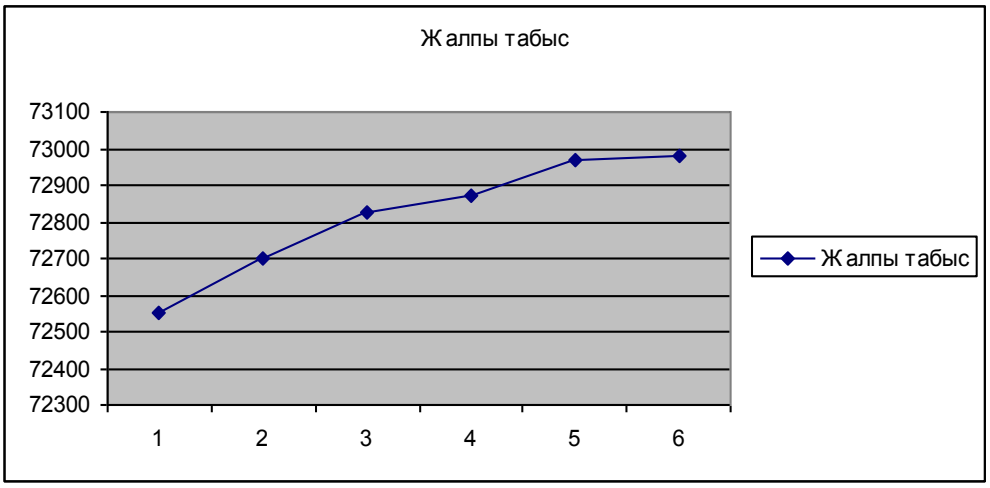


3.5 сурет– VPN арасында желінің жеке звеноларының өткізу жолағын үлестіруінің графигі

Алгоритмдердің үйлесімділігі негізгі сұрақ болып табылады. Қарастырылып отырылған мысалға 10^{-3} шектік ұқсастыққа жету үшін 5 итерация қажет болды. 3.4 кестеде желідегі әр итерациядан кейінгі жалпы қолданылған өткізу жолағы көрсетілген. 3.6 сурет әр итерациядан сайын жалпы табыстың өсуін көруге болады.

3.4 кесте– Әр итерация сайын жалпы табыс

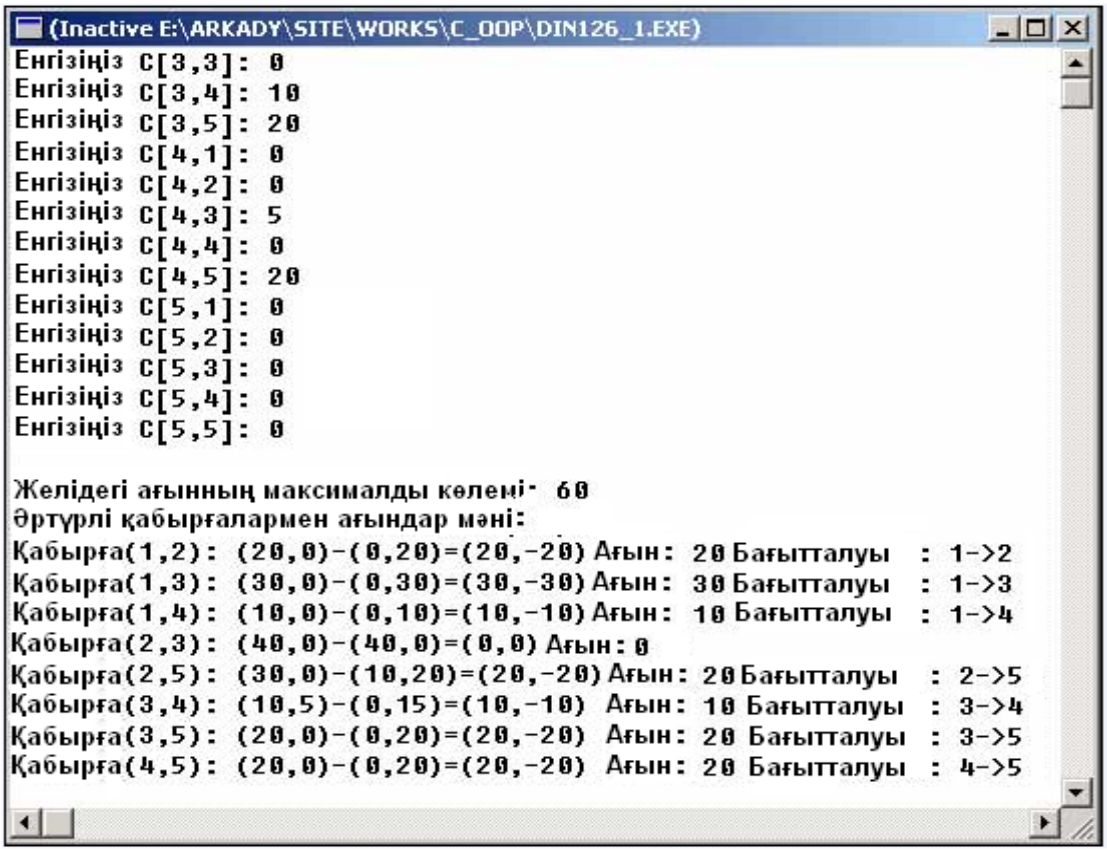
Итерация	0	1	2	3	4	5
Жалпы табыс	72552,3	72700,6	72827,9	72872,3	72967,2	72981,8



3.6 сурет– Әр итерациядан кейінгі жалпы табыстың өсуі

А қосымшада С++ бағдарламасының листінгі көрсетілген.

Ә және А қосымшаларының С++ алгоритмдік тілінің негізгі терезесі 3.7 сурет көрсетілген



3.7 сурет– С++ алгоритмдік тілінің негізгі терезесі

3.2 VPN желісінің өміршеңдігін есептеу

Виртуалды жеке желіні құрғанда, жобалағанда оның өміршеңдігін қамтамасыз ету жолдары қарастырылады. Тәжиірибеде көріп жүргендей көп байланыс желілері қажетті талаптарды орындай алмай, оны жаңартуға көптеген шығын шығуда. Сондықтанда желінің өміршеңдігін желіні жобалар алдында есептейді. Байланыс желісі белгілі бір себептермен үзіліп, бастапқы үзіліссіз өміршеңді желі екі бөлікке бөлініп әрқайсысы тәуелсіз жұмыс істей береді. Мұндай себептерді туғызатын табиғи апат, террористік әрекеттер болып табылады. Көп есептеулердің нәтижесінде жолдың орта ұзындығы $l(n+1)/3$ – тең желілерге қарағанда, жұлдыз тәрізді топологиялы желілердің өміршеңдігі жоғары болады. Өйткені онда жол ұзындығы екі доғадан тұрады(мұндағы l – доға ұзындығы , n – торап саны). Бірақта ең қысқа жол кестесімен өміршеңдік арасында ешқандай байланыс анықталған жоқ. Ең қысқа жол кестесі дегеніміз ол бір тораптан желідегі басқа тораптарға бағытталған ең қысқа жол жиынтығы. Толық қатынастағы желіде тораптан басқа тораптарға баратын жол саны келесі теңдеумен анықталады:

$$\gamma = n(n-1) \tag{3.13}$$

Бізге граф түрінде тораптар мен қабырға доғаларының жиынтығы берілді дейік. Радиалды желіде доға ұзындығы бірдей, ал торап аралық ағында бірдей. Мұндай ескерулерді қарастырғанда желіні симетриялы деп қарастырамыз. Симетриялық желіде жолдың ең қысқа жолы бәріне бірдей, ал доғадағы жүктеме тең. Өміршеңдік көрсеткіші ретінде белгілі доғалар мен тораптың аман қалу ықтималдығын ескеру арқылы, аман қалған байланыстың бөлігі мен математикалық үмітін пайдаланамыз. Тораптар толық қатынасты сондықтанда барлық тораптар арасында байланыс бар. Доғалардың екі күйі бар олар бар немесе жоқ. Екінші мәселе ол ең қысқа жол кестесімен, желінің өміршеңдігі арасында қандай байланыс барын анықтау. Бұл есептеудің мақсаты ең қысқа жолды ескерумен желінің өміршеңдігін есептеуді жеңілдету болып табылады.

Желіде біздің процесс n – мүшесінің формуласы үшін және арифметикалық қатарлар құрылымын қолданып екі жұлдызшаның әртүрлі аумақтың p үшін коэффициенттерін есептеуге болады.

ЭВМ көмегімен автоматтандырылған болуы үшін анақталған қадаммен 0≤ p ≤1 үшін $D(\alpha)$ анықтау мәндерін және қысқа жолды ағаш (ДКП) құру процедурасы. ДКП желінің басқа қалған тораптармен тамырлар қосу ұзындығы математикалық үміттін қатнасының құруға рұқсат береді. Коэффициенттер p, p^2, p^3 кезде бір, екі және үш доға желідегі ұзындықтардың қанша қосулар $M(\alpha)$ қатнасы көрсетеді.

Бір доға желідегі үзілу кезінде әлсіздігін жолдың орта ұзындығы ағаш тәрізді желіге тура шағылыстырады. Орта жол ұзындығы (СПД) аз болған сайын соғурлым әлсіздік азаяды және қарамақарсы желінің өміршеңдігі көп болады. Жұлдыз тәрізді желіде $D_{ij} 2L(n-1)/n = 2L/n$ – жолдың орта ұзындығы, $D(\beta) = 2/n$ – үзілген қосулардың орта ұзындығы. Желінің ұзындығын бірге тең деп шартты қабылдасақ онда СПД және әлсіздік тең болады. Сондықтан желінің өміршеңдігі қамтамассыз етудің әдістердің бірі жолдың минималды орта ұзындығының құрылымын іздеу болып келеді. Біздің желіміз үшін төмендегі формула бойынша анықталады.

$$M(\alpha) = 16p + 31p^2 + 24p^3 + p + (n-1)\left[2p + (n-2)p^2\right] \tag{3.14}$$

мұндағы $M(\alpha)$ – қабырғалар үзілген кездегі аман қалған қосулар санының математикалық үміт.

$$D(\alpha) = \frac{M(\alpha)}{72} \tag{3.15}$$

$D(\alpha)$ – аман қалған қосулардың орта бөлігі.

$$M(\alpha) = 16*0.9 + 31*0.9^2 + 24*0.9^3 + 0.9 + (7-1)\left[2*0.9 + (7-2)*0.9^2\right] = 58{,}62$$

$$D(\alpha) = \frac{58{,}62}{42} = 1{,}38$$

Үстіндегі шығарылған нәтижелерді Delphi бағдарламасы көмегімен шыққан нәтижелерді салыстырып көреміз. Виртуалды жеке желінің өміршеңдігінің блок сұлбасы Б қосымшдада және бағдарлама листингі В қосымшада көрсетілген. Өміршеңдік бағдарламасы 3.8 сурет көрсетілген.

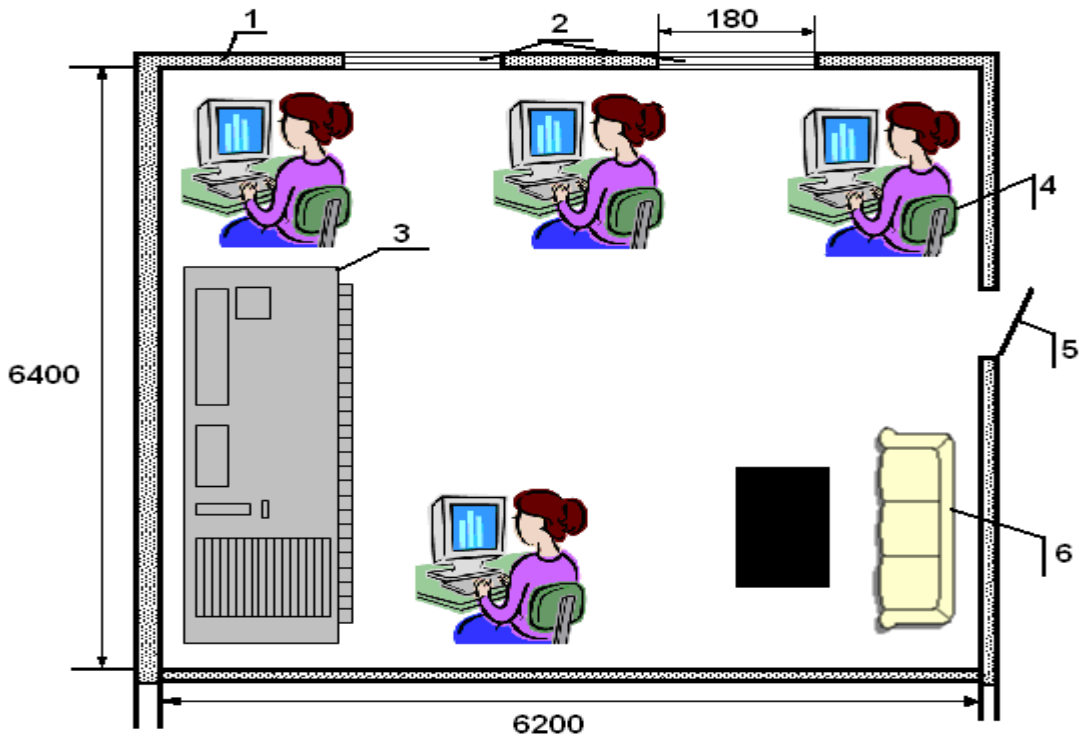
4 Өміртіршілік қауіпсіздігі

4.1 Еңбек жағдайларын талдау

Қарастырылып отырылған бөлме он этажды ғимараттың алтыншы этажында орналасқан. Бөлме тіктөртбұрышты формалы. Оның парамметрлері: ұзындығы – 6,4 метр, ал ені – 6,2 м, биіктігі – 3,2 метр ақ төбемен, қабырғалары ақ түске әктелген, терезелерінде жалюзі орнатылған. Бөлме 3 жұмыс орнына есептелінген (жұмыс істеушілер саны 6, ауысымды жұмыс) және де демалыс орны бар. Жұмыс құралдары ретінде 4 компьютер, оның 3 қызметкерлерге арналған және қалған 1 компьютер құрылғы мониторингі үшін және қосымша оргтехникаға арналған.

Жұмыс екі ауысымға бекітілген: таңғы 8.00-ден кешкі 20.00-ге дейін және кешкі 20.00-ден таңғы 8.00-ге дейін.

Бөлме ауданы $S_{контр}$=6,2×6,4=39,7 м^2, көлемі $V_{контр}$=39,7×3,2=127 м^3. Осыдан бір адамға жұмыс ауданы 39,7/3=12,3 м^2, жұмыс көлемі 31,8 м^3. Ол бекітілген нормалармен (көлем – кем дегенде 15м^3, ал аудан – кем дегенде 4,5м^2) салыстырғанда минималды аудан мен көлемнен артық. Бөлменің көрінісі сурет 4.1 көрсетілген.



1-қабырға; 2- терезе; 3- коммутатор құрылғысы 4 - оператордың орны; 5 – есік; 6 – қызметкерлердің демалыс орны;

4.1 сурет– Бөлменің көрінісі

Бөлменің оптималды микроклиматы кондиционерлеу жүйесі көмегімен жүзеге асырылады.

Бөлмеде тұрақты шу және діріл көздері жоқ. Сыртқы шу көздерінен бөлмені пластикалық терезерелер қорғайды.

Бөлмеде электромагнитті сәуле көздері жоқ. Жұмыс істеу үшін сұйыққристалды негіздегі мониторлар қолданылады. Олар адам организміне қатты әсер етпейді электронды-сәулелі мониторлар сияқты емес.

Бөлмеде кеңселі құрылғылардың тоққа жақын бөлігіне адамның жақындау мүмкіндігі ескерілген. Барлық жалғану сымдары мен линиялар сапалы изоляцияланған. Құрылғыға қоректі беру үшін евророзеталар, жерлеу клеммалары қолданылады, олар ортақ қорғаныс жерлеу жүйесімен қосылған. Ортақ қорғаныс жүйесі контурлы болып келеді. Жерленетін құрылғы бойымен контур бойынша жерлеуіш құрылғылары орнатылады.

Оператордың жұмыс орнын құрылымдағанда келесесі шарттарды орындаймыз: құрылғыға техникалық қызмет көрсету мен эксплуатациялау кезінде қажет барлық іс-әрекеттерге мүмкіндік жасау үшін жұмыс істейтін адамға жеткілікті кеңістікті қамтамасыз ету; құрылғы мен жұмыс істейтін адам арасында жеткілікті физикалық, көру, есту байланыстары және де жұмыс істеу барысындағы қызметкерлер арасындағы оптималды жұмыс орындарын белгілеу; жұмыс істеу үшін қажетті табиғи және жасанды жарықтандыруды қамтамасыз ету және т.б.

Оператордың жұмысы құрылғыны бақылау үшін және құрылғы жұмыс істемей қалған кезде жөндеу үшін арналған. Сонымен операторлардың жұмыс істеуін орта нақтылыққа жатқызамыз, көздің жұмыс істеуінің IV разрядына.

Бөлмедегі жарықтандыру араласқан (табиғи және жасанды). Табиғи жарықтандыру екі терезенің арқасында ұйымдастырылған. Олардың өлшемдері 180х175 см. Терезелер бір метр биіктіктен кейін басталады. Күн сәулесінен қорғану үшін алынып тасталынатын жалюзілер қолданылады.

Орта нақтылықпен жұмыс істегенде табиғи жарықтандырудың коэффициентті 1,2% төмен болмауы керек.

Біздің жағдайда ол жеткіліксіз, себебі жұмыс істеу екі ауысымға бекітілген. Табиғи жарықтандыру люминесценциялық жарық көздерін пайдалану арқылы жүзеге асырылады.

4.2 Бөлме жарықтандыруын есептеу [12]

4.2.1 Бөлменің табиғи жарықтандыруын есептеу. Бөлменің өлшемі: ұзындығы L = 6.4 м, бөлменің ені B=6,2 м, биіктігі H=3,2 м.

Еденнен бастап жұмыс орынның биіктігі 0,5 м. Терезелер 1м биіктіктен басталады, оларбың биіктігі 1,8м.

ТЖК нормаланған мәні жарық климатының III белбеуі үшін келтірілген, жарық климатының қалған белбеулері үшін ТЖК-ң нормаланған мәні келесі формула бойынша анықталады:

$$e_H^{IV} = e_H^{III} \cdot m \cdot C, \qquad (4.1)$$

мұндағы e_H^{III} - III класс үшін ТЖК мәні;

m - жарық климатының коэффициенті;

C - ашық климат коэффициенті, мекеменің сыртқы қабырғаларының жарық ойықтары.

1.1 Кестеде қазақстан аудандары үшін m мен с мәндері келтірілген.

Ғимарат Алматы қаласында IV жарық белбеуінде орналасқан.

Кеңсе орналасқан ғимараттың қасында 10 арақашықтықта 7 метрлі ғимарат орналасқан. Басқа жақтарынан қараңғы түсіретін ғимараттар жоқ.

Жұмыс орынның нормаланған жарықтандыруын болдыру үшін автозалдың бүйір жарық ойықтарының ауданын есептеу қажет.

ТЖК-ң нормаланған мәнің қамтамасыз ету үшін бүйір жарықтандыру кезінде *S* жарық ойықтарының ауданы келесі формула бойынша анықталады:

$$100 \times \frac{S_0}{S_n} = \frac{e_н^{IV} \times \eta_0}{\tau_0 \times r_1} \times к_{зд} \times к_з \qquad (4.2)$$

(4.2) формуладан жарық ойығының ауданың есептейміз

$$S_0 = \frac{S_n \times e_н^{IV} \times \eta_0 \times к_{зд} \times к_з}{100 \times \tau_0 \times r_1} \qquad (4.3)$$

мұндағы S_n - бөлменің еден ауданы;

e_H - ТЖК-ң нормаланған мәні;

$K_З$ - қор коэффициентті;

τ_0 - жалпы жарық өткізу коэффициентті

$$\tau_0 = \tau_1 \times \tau_2 \times \tau_3 \times \tau_4 \qquad (4.4)$$

η_0 терезенің жарық сипаты

r_1 – коэффициент, бөлме бетінің сәулеленуі және төселінетін қабат, мекемеге іргелесетін жарық арқасында бүйір жарықтандыру кезінде ТЖК жоғарылатуды ескереді (1.6 кесте).

Бөлменің еден ауданы:

$$S_n = L \times B = 6.4 \times 6.2 = 39.7 \text{ м}^2 \qquad (4.5)$$

ТЖК-ң нормаланған мәнін (4.1) формуладан есептейміз:

$$e_н^{IV} = e_н \times m \times c,$$

m = 0,9 c = 0,75 (1.1 кесте)

$e_н$ = 1,2 (IV разрядты орта нақтылықты жұмыстыр үшін, 1.2 кесте)

$$e_н^{IV} = 1{,}2 \times 0{,}9 \times 0{,}75 = 0{,}81$$

1.3 кестеден. η_0 анықтаймыз. терезенің жарық сипатын анықтаймыз. Бұл үшін ұзындық тереңдікке қатысты болады:

6,4:3,2 = 2

Ұзындықтың тереңдікке қатынасы (терезеден ең алыс қашықтықтан) мынаған тең:

$$\frac{B}{h_1} = \frac{6{,}2}{2{,}8} = 2{,}2 \qquad (4.6)$$

h_1 = 2,8 м, 1 м. h_1 – жұмыс деңгейінің бетінен бастап терезенің үстіне дейінгі биіктік; бұдан η_0=9,5.

Жарық өткізгіштік материал ретінде стеклопакетті қолданамыз, терезе жақтаулары екеулік бөлінген металды, жүргізуші жабын түрі – болатты ферма. Күннен қорғаныс ретінде алынатын, реттелетін жалюзилерді қолданамыз. 1.5 кестеден келесі мәндерді аламыз:

τ_1 = 0,8; τ_2 = 0,8; τ_3 = 0,9; τ_4 = 1.

$$\tau_0 = 0{,}8 \times 0{,}8 \times 0{,}9 \times 1 = 0{,}58$$

Бөлмедегі шағылысудың орта коэффициенті $\rho_{ср}$ = 0,5, екі жақты бүйірлі жарықтандыруды аламыз.

1.6 кестеден r_1 мәнін аламыз r_1 - коэффициентті бөлме бетінің сәулеленуі және төселінетін қабат, мекемеге іргелесетін жарық арқасында бүйір жарықтандыру кезінде ТЖК жоғарлатуды ескереді.:

$$\frac{B}{h_1} = \frac{6,2}{2,8} = 2,2 \qquad (4.7)$$

$$\frac{H}{B} = \frac{3,2}{6,2} = 0,5 \qquad (4.8)$$

r_1=1,2 тең деп аламыз.

Р = 10м арақашықтықтағы ғимараттың биіктігі $H_{зд}$ = 7 м.

Ғимаратқа дейінгі арақашықтықпен оның биіктігіне қатынасын есептейміз:

$$\frac{P}{H_{зд}} = \frac{10}{7} = 1,42 \qquad (4.9)$$

1.7 кестеден ғимараттың қор коэффициентін есептейміз $К_{зд}$ = 1,2

(4.3) формулаға барлық мәндерді қойып жарық ойығының ауданын есептейміз:

$$S_0 = \frac{39,7 \times 0,81 \times 9,5 \times 1,2 \times 1,2}{100 \times 0,58 \times 1,2} = 6,29 = 6,3 \text{ м}^2,$$

Екі жақты бүйірлі жарықтандыруды қарастырғандықтан. Бір жақтағы жарық ойықтарының ауданы келесі формуламен есептелінеді:

$$\frac{6,3}{2} = 3,15 \text{ м}^2 \qquad (4.10)$$

Тереза ойықтары 1,8 м тең болғандықтан, олардың ұзындығы келесі формуламен анықталады:

$$\frac{3,15}{1,8} = 1,75 \text{ м} \qquad (4.11)$$

Сонымен терезе ойықтарының көлемі 3,15 $м^2$ (1,75*1,8) тең болады.

4.2.2 Бөлменің жасанды жарықтандыруын есептеу. Бөлменің жалпы жасанды жарықтандыруын жарық ағынын қолдану коэффициенті әдісі арқылы есептелінеді. Жұмыс істеудің көру аймағының разряды IV орта нақтылыққа жатады. Сондықтан жалпы жарықтандыру жүйесі тиімді болады. Онда шамдар жоғарыда орналасады, бөлменің биіктігі 3,2м, көлемі 39,7 м^2.

Осы қойылған талаптарға сәйкес оператордың жұмыс орнының жалпы жарықтандыру жүйесінің есептеулерін жүргіземіз. Есептеу жарық ағыны бойынша жүргізіледі, 300лк тең құжаттың берілген жарықтану мәні бар.

Нормаланған минималды жарықтану келесі формуламен есептелінеді:

$$E_{\min} = \frac{F_{Ё} n \eta Z}{SK}, \qquad (4.12)$$

мұндағы $F_{Ё}$ — бір шамның жарық ағыны;

n — бөлмедегі шамдар саны;

η — жарық ағынына қатысты, жарықтандыру құрылғысының толық ағынын есептеу коэффициентті;

Z — бір келкі емес жарықтану коэффициентті;

S — жарықтандырылатын бөлме ауданы;

K — қор коэффициентті, жарықтану жүйесін эксплуатациялау кезіндегі жарықтанудың төмендеуі (шамдардың кірленуі, ескіруі).

Жарық ағынын қолдану коэффициенті жарықтандырылатын ауданға жететін жарық ағыны мен бөлменің толық жарық ағынына қатынасы. Ол қабырғалардың ρ_c және төбенің $\rho_п$ шағылысу коэффициентіне тәуелді. Ол келесі формуламен есептелінеді:

$$\varphi = \frac{AB}{H_p(A+B)}, \qquad (4.13)$$

мұндағы A – бөлме ұзындығы;

B – бөлме ені;

H_p – жұмыс орнына қатысты шамдардың іліну биіктігі (жұмыс орын жерден есептегенде 0,8 м биіктікте орналасқан). Люминесцентті шамдар 3 м биіктікте орналасады.

Жұмыс істеудегі минималды жарықтандырылу нормалағандықтан, онда есептеулер жүргізілгенде Z біркелкі емес жарықтану коэффициенті еңгізіледі. Люминесцентті шамдар үшін Z = 0.9.

Шамдар санын (4.1) формуладан анықтағаннан кейін

$$F_л = \frac{E_{min} SK}{Z\eta} \qquad (4.14)$$

Осы жұмыс категориясы үшін жалпы жарықтандырылу кезінде минималды жарықтану E_{min} = 300 лк (люкс) [3].

Жарықтанудың пульсация коэффициентті 15% кем емес.

Қор коэффициентті K = 1,5

Біркелкі емес жарықтану коэффициенті Z = 0,9.

Берілген бөлме үшін жалпы жарықтандыру жүйесі кезіндегі шамдар санын анықтаймыз.

Бөлменің өлшемі: ұзындығы А = 6.4 м, бөлменің ені В=6,2 м, биіктігі Н=3,2 м.

Төбеге АОД екішамды шамдарды орналастырамыз. Люминесцентті шамдар ЛЕЦ 40. кесте 4.2 осы шамның сипаттамалыры келтірілген.

4.2 кесте– ЛЕЦ 40 шамының сипаттамалары

Типі, маркасы	Қуаты, Вт	Жарық ағыны, лм	Ұзындығы, мм	Диаметрі, мм	Бір сағаттағы жану орта мөлшері	Температурасы, К
ЛЕЦ 40	40	2200	1213,6	40	10000	3900

Қабырғалардың $p_{ст}$ =50%, және төбенің $p_{пт}$ = 70% шағылысу коэффициенті тең.

Жұмыс орнына қатысты шамдардың іліну биіктігі (жұмыс орын жерден есептегенде 0,8 м биіктікте орналасқан). H_p= 2,8 тең.

Бөлменің ауданы: S = 39,7 м^2.

АОД шамдары үшін жарық ағыны ЛЕЦ 40, бір шаммен жасалынатын жарық ағыны $F_л$ = 2200 лм (люмен).

$$\varphi = \frac{AB}{H_p(A+B)} = \frac{6.4 \times 6.2}{2.8 \times (6.4+6.2)} = 1.125$$

Осыдан бөлме көрсеткіштерін алу үшін 5.6 кестеден қабырғалардың $\rho_с$ және төбенің $\rho_п$ шағылысу коэффициентін аламыз. Жарық ағынын қолдану коэффициенті η = 0,68.

4.12 формуладан бөлмедегі қажет шамдар санын анықтаймыз:

$$n = \frac{E_{min} \times S \times K}{2F_{Л} \times \eta \times Z} = \frac{300 \times 39.7 \times 1.5}{2 \times 2200 \times 0.62 \times 0.9} = 8$$

Орта қуатпен берілген бөлме үшін жарықтану жүйесін есептейміз.

Жарықтандыратын құрылғының қуатын есептейміз:

$$W = W_0 \times S = 12 \times 39.7 = 476.4 \text{ Вт} \qquad (4.15)$$

мұндағы W_0 = 11÷15 Вт/кв.м –шамдардың орта қуаты.

Таңдалып алынған қуатты шамдардың қажетті саны:

$$n = \frac{W}{2W_0} \qquad (4.16)$$

$$n = \frac{476.1}{2 \times 40} = 5.955 < 8$$

4.1 формуладан анықтаймыз $E_{расч}$:

$$E_{расч} = \frac{F_{Л} n \eta Z}{SK} = \frac{2 \times 2200 \times 8 \times 0{,}68 \times 0{,}9}{39{,}7 \times 1{,}5} = 329{,}9 \text{ лк} > E_{\min} = 300 \text{ лк}$$

Сонымен біздің бөлмеміздің жасанды жарықтандыру жүйесін қамтамасыз ету үшін АОД типті ЛЕЦ 40 шамдарымен 8 шамдарды орнатамыз.

N тізбектер санына бөліп, әр тізбекте қанша шам орналасатынын білуге болады. Шамдар ұзындығы белгілі болғандықтан, әр тізбектегі шамдардың ұзындығын есептеу керек.

Егерде шамдардың ұзындығы бөлменің ұзындығымен тең болса, онда ол үзіліссіз орналасады. Егер де төмен болса, онда арасында арақашықтықтар қалады.

Шамдар екі тізбекке орналастырылады.

Әр тізбектегі шамдар саны $N_p = n/2 = 4$.

АОД шамының ұзындығы 1,2 м, бір тізбектің ұзындығы 4 × 1,2 = 5,2 м.

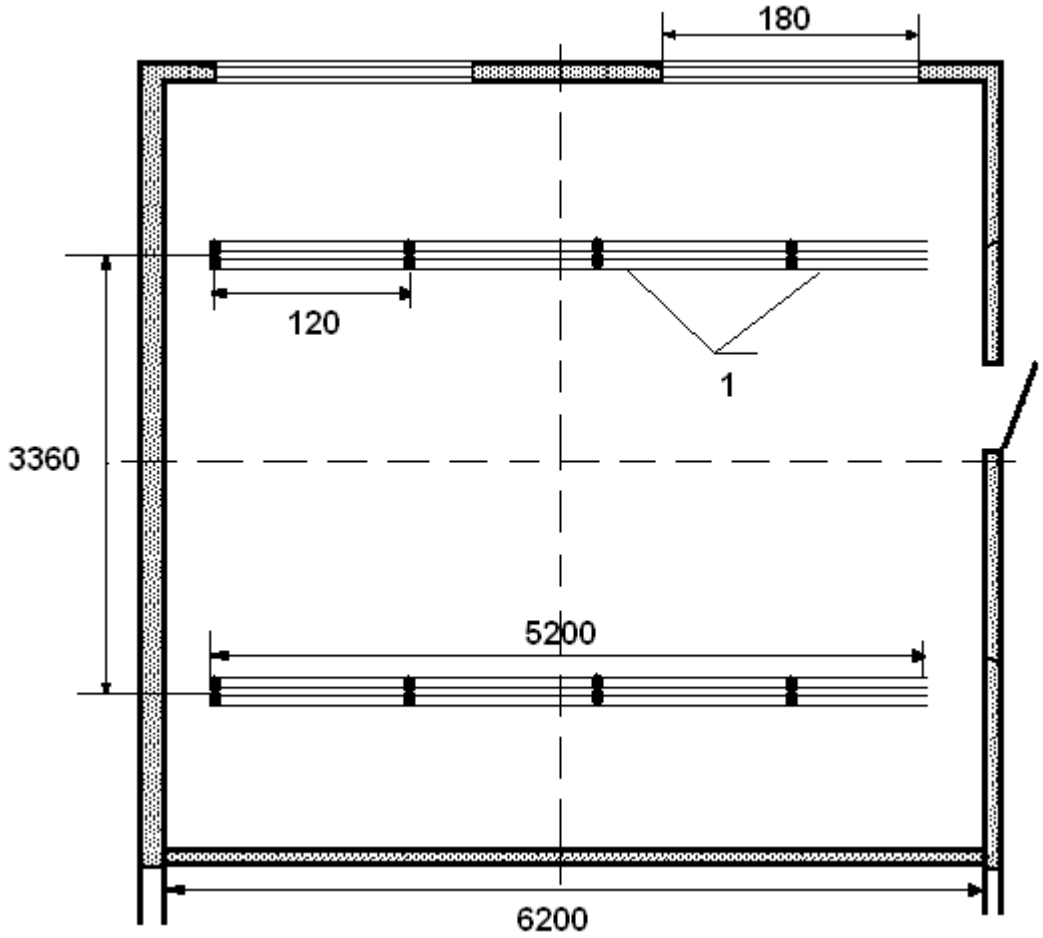
Шамдардың тізбектері арасындағы арақашықтықты келесі формуламен анықтаймыз:

$$L = \lambda \times h\ , \qquad (4.17)$$

мұндағы λ – біркелкілік емес коэффициенті, 1.2 тең;
h – іліну биіктігі.

$$L=1.2\times2.8=3,64 \text{ м}$$

Бөлмедегі шамдардың орналасу сұлбасы 4.2 суретте көрсетілген.



1 – шамдар

4.3 сурет– Шамдардың орналасу сұлбасы

4.3 Бөлменің желдендіруін есептеу

Тұрғын, жарықтанған және өндірістік бөлмелерді ауалық комфортпен қамтамасыз ету аспирация, вентиляция, жылыту жүйелеріне және ауаны кондиционерлеуге тәуелді. Вентиляциямен қосылған ауаны жылыту бөлмеде қанағатты климаттық жағдай тудырады және ауа ортасының қолайлы жағдайын қамтамасыз етеді. Ауаны кондиционерлеу жүйесі вентиляция және жылыту есептерін шешумен бірге құрамындағы фреондық суыту машинасы арқылы жазғы ыстық кезінде жайлы микроклиматты жүзеге асырады. [13]

Бір сағат ішінде бөлмеден шығару керек ететін ауаның мөлшері L ($м^3$/ч), онымен бірге қажет емес жылуды Qизб шығару формуласы төменде көрсетілген.

$$L = Q_{изб}/C_в \text{ x } t \text{ x } y_в, \qquad (4.17)$$

мұндағы $C_в$ - құрғақ ауаның жылусыйымдылығы, ккал/кг ^{0}C ($C_в$=0,24 ккал/кг^{0}C);

$t = t_{ух} - t_{вх}$, есептеулерде келесідей аламыз, t=50˚C;

$y_в$ - кететін ауа тығыздығы, температураға байланысты есептелінеді, кг/$м^3$ (есептеулерде келесідей аламыз, $\gamma_в$ =1,20 кг/$м^3$).

Артылған жылу – бөлме ішіндегі жылу бөлінулердің және сыртқы қоршаулардан қоршаған ортаға жылу беру айырымы:

$$Q_{изб} = Q_п + Q_{от}, \text{ ккал/ч} \qquad (4.18)$$

мұндағы $Q_п$ – бөлме ішіне кіретін жылу мөлшері, ккал/ч;

$Q_{от}$ – сыртқы ортаға жылуды беру (жылы мезгілдерде оны нөлге тең деп алуға болады)

Құрылғы қуатынан, қызметкерлер санынан шығатын жылу мөлшері келесі формуламен есептелінеді $Q_п$:

$$Q_п = Q_{об} + Q_л + Q_р, \qquad (4.19)$$

мұндағы $Q_{об}$ - өндірістік жабдық шығаратын жылу, ккал/ч;

$Q_л$ - жұмысшылар шығаратын жылу, ккал/ч;

$Q_р$ - күн сәулелерімен кіретін жылу, (күн радиациясы), ккал/ч;

Өндірістік жабдық шығаратын жылу:

$$Q_{об} = 860 \text{ x } P_{об} \text{ x } n, \qquad (4.20)$$

$$Q_{об} = 860 \text{ x } 1{,}98 \text{ x } 0{,}75 = 1\ 277{,}1 \text{ ккал/ч}$$

мұндағы 860 – жылу эквиваленті, 1 кВт/ч;

$P_{об}$ – жабдықтар тұтынатын қуат, 1,98 кВт/ч;

h - жылудың бөлмеге өту коэфф-і, берілген бөлме үшін 0.75.

Бөлме де үш адам жұмыс істегендіктен $Q_л$ мәнін төмендегі формуламен есептейміз:

$$Q_{қал\ 4} = n \cdot q \qquad (4.21)$$

мұндағы *n* – жұмысшы саны;

q – бір адамнан шығатын жылу (*q=102 Вт*).

$Q_{жалпы} = Q_{қал.4} = 3 \cdot 102 = 306$ (Вт)

Күн сәулелерімен кіретін жылу, (күн радиациясы) келесі формуламен есептелінеді:

$$Q_р = m \cdot F \cdot g_{ост}, \qquad (4.22)$$

мұндағы m – бөлмедегі терезелер саны;

F – бір терезенің ауданы, 3,15 $м^2$;

$g_{ост}$ - терезеден кіретін күн сәулесі, берілген бөлме үшін 145 тең деп аламыз;

$$Q_р = 2 \text{ x } 3{,}15 \text{ x } 145 = 783 \text{ ккал/ч}$$

$$Q_{изб} = Q_п = 1\,277{,}1 + 783 + 306 = 2366{,}1 \text{ ккал/ч}$$

(4.17) формуласынан қажетті ауа алмасуын есептейміз:

$$L = 2366{,}1/0{,}24 \text{ x } 50 \text{ x } 1{,}20 = 538{,}45 \text{ м}^3\text{/ч}$$

Кондиционерлеу жүйелеріне талаптарды орнату кезінде өнеркәсіптік бөлмеде жиналған зиянды заттарды, яғни жылу артылуларды, ылғалдықты, буларды, газдарды және шаңды жою қажеттілігін ескеру қажет.

Кондиционерлеу жүйесі ауаалмасуын К, қамтамасыз етуі тиіс:

$$К = L/V_п, \qquad (4.23)$$

мұндағы $V_п$ – бөлме көлемі;

К = 538,45/127 = 4,2

Берілген парамметрлерді SDA (AMICO) кондиционері қанағаттандырады. Төменгі берумен 0151 модельді.

Оның техникалық сипаттамалары:

- электрқоректендіруі – 230/1/50 В/Ф/Гц;
- ауаның шығыны макс.-1580 $м^3$/ч, мин. –1040 $м^3$/ч;
- массасы – 130 кг.

Кондиционерді орналастыру орны келесі талаптарды қанағаттандыруы керек:

- кондиционер күн сәулесінің тура түсу бағыттарынан қорғауы керек;
- кондиционердің қасында басқа жылу шығаратын құрылғылар болмау керек;
- кондиционердің алдында басқа заттар болмауы керек, оның ауаны шығаруына бөгеуіл болатын заттар.

Кондиционердің габаритті өлшемдері:

- ені 550 мм;
- биіктігі 1740 мм;
- ұзындығы 450 мм.

Берілген кондиционердің SDA (AMICO) көмегімен келесі режимдерді орнатуға болады:

- жылыту;
- суыту;
- құрғақтау;
- вентиляция;
- түнгі режим.

Бизнес-жоспар

5.1 Презентация

Қазіргі кезде желілік технологиялардың дамуы транспортты желі құру технологиясының дамуымен сипатталады. Сонымен қатар, байланыс арналарының өткізу қабілетін жоғарылатуға және ақпараттардың қорғанысын жеткілікті қамтамасыз ету керектігіне өте көп көңіл бөлінеді.

Көптеген кәсіпорындар әртүрлі трафик түрлеріне қызмет көрсетіп қана қоймай және пайдаланушыларға әртүрлі көрсетілген қызметті толығымен басқаруды қамтамасыз етуге тырысады. Мұндағы желінің жеке аймағындағы жәй ғана арнаның өткізу қабілетін жоғарылату қойған мәселені шешпейді. Іс жүзінде технологиялық және экономикалық аспектілерден шығатын мәселелерді шешу, бізден желіні техникалық сауатты құруды талап етеді. Сонымен қатар, кәсіпорынның бизнес-есептеутелерін шешу, жәй ғана ақпараттың таралуын қамтамасыз етіп қана қоймай кәсіпорынның табысқа жетуіне қол жеткізу. Қазіргі кезде көптеген коммерциялық жобалар жаңа технологиялармен жасалуда. Соған байланысты технологияларды дұрыс таңдау өте маңызды. Кез-келген үлкен масштабты жобада желінің ядросының технологиясын таңдау негізгі сұрақтарға жатады. Технологияны таңдау және қолданылатын құрылғы желінің дамуын көптеген жылдарға анықтайды. Жоғарғы деңгейде бұл шарттарды виртуалды жеке желілер VPN (Virtual Private Network) технологиясы қанағаттандырады.

Виртуалды жеке желі сол желінің басқа пайдаланушыларынан бөлінген, дестелік коммутациямен бұқаралық желінің нақты пайдаланушылары арасындағы логикалық қосылу негізінде құрылады. VPN нақты түйіндер арасында белгіленген линиялардың басқа типтеріне ауыстырады. VPN ақпаратты таратудың сапасы мен қауіпсіздігі арнаулы әдістер мен протоколдарды қолдану арқылы қамтамасыз етіледі.

5.2 Жобаның мақсаты

Берілге жұмыста қазіргі заманға сай тұжырымдамалар көз-қарасымен транспортық желі технологияларын анализдеу мен жинақтап қорыту мүмкіндігі жасалынады. Мұнда бірінші орынға жоғарыда айтылған мәселелерді шешетін желілік технологияны таңдау шығады. Айта кететін жағдай, үлкен көлемді трафикті тарату үшін арналған транспорттық желі құру технологиясының даму деңгейінің есте қаларлығы ескірген технологиялардың көбі жаңадан жаңаруда, ал келешегі зор деп танылған технологиялардың

кейбіреулері артта қалуда. Осы жағдай таңдауды оданда күрделендіреді. Дұрыс таңдалған технология көрсететін қызметті кеңейтеді, байланыс операторына желінің табысын көтеруге мүмкіндік береді.

5.3 Ғылыми зерттеу жұмыстың жоспары

Нарықтық қатынас жағдайында кез келген интеллектуалды еңбек бағалануға тиіс, сондықтан тәжірибелік сипаты бар барлық ҒЗЖ, ОКР жұмыстары бағалануы керек, яғни олардың құны мен бағасы есептелінуі қажет.

Ғылыми-зерттеу немесе тәжірибелік есептеулерді өткізуге кететін шығынды анықтаймыз.

Жобаны негізгі жасаушыларына басқарушы инжинер мен инжинер. Жобаны жасауға 60 күн бөлінеді. 5.1 кестеде жобаны жасау үшін кететін күндер көлемі көрсетілген.

5.1 кесте– Ғылыми-зерттеу жұмыстың жоспары.

Кезеңдер аты мен жұмыстың мазмұны	Орындаушы	Жұмыс-сыйымдылығы		Орындаушылар саны	Цикл ұзақтығы күндер
		Сағат нормасы	Жалпы жұмыс-сыйымдылығынан,%		
1.Жобаның мақсаты мен есептің қойылуы	Басқарушы инжинер	38,5	5	1	5
2.Интернетте ақпараттық іздеуді жүргізу	Инжинер	38,5	5	1	5
3.Бағдарламаны құрып, оның алгоритмін жасау	Басқарушы инжинер Инжинер	154 154	20 20	1 1	10 10
4.Шыққан мәндерді анализдеу	Басқарушы инжинер	38,5	5	1	5
5.Жобаны безендіру	Инжинер	38,5	5	1	5

5.1 кесте – жалғасы

Кезеңдер аты мен жұмыстың мазмұны	Орындаушы	Жұмыс-сыйымдылығы		Орындаушылар саны	Цикл ұзақтығы күндер
6.Істелінген жұмысты талқылау	Басқарушы инжинер Инжинер	154 154	20 20	1 1	10 10
Барлығы		770		2	60

5.3.1 Жұмыс-сыйымдылығы

ҒЗЖ жоспарлаған кезде оның ең күрделі бөлігі жұмыс-сыйымдылығын есептеу болып саналады. Себебі, еңбек шығындары ҒЗЖ бағасының негізгі бөлігін алады және де жұмысты жасау уақытына әсер етеді. Ғылыми-зерттеу жұмыстардың жұмыс-сыйымдылығын есептеген кезде нормативті базаның бір бөлігін ғана қолдануға болады. Жұмыс-сыйымдылығын төмендегідей формуламен есептейміз. [15]

$$T = 7 \cdot t_n \cdot q_n \cdot K \qquad (5.1)$$

мұндағы Т – кезең жұмыс-сыйымдылығы, сағат-нормасы;

g_n – кезең бойынша жұмыс істеушілер саны;

t_n – әр жұмыс түрі бойынша цикл ұзақтығы;

7 – жұмыс күнінің ұзақтығы;

К – уақыт нормасын орныдау коэффициентті (К=1,1).

№ 1 Кезең

$$T_1 = 7 \cdot t_{n1} \cdot q_{n1} \cdot K = 7 \cdot 5 \cdot 1 \cdot 1{,}1 = 38{,}5$$

№ 2 Кезең

$$T_2 = 7 \cdot t_{n2} \cdot q_{n2} \cdot K = 7 \cdot 5 \cdot 1 \cdot 1{,}1 = 38{,}5$$

№ 3 Кезең

$$T_3 = 7 \cdot t_{n3} \cdot q_{n3} \cdot K = 7 \cdot 20 \cdot 2 \cdot 1{,}1 = 308$$

№ 4 Кезең

$$T_4 = 7 \cdot t_{n4} \cdot q_{n4} \cdot K = 7 \cdot 5 \cdot 1 \cdot 1{,}1 = 38{,}5$$

№ 5 Кезең

$$T_5 = 7 \cdot t_{n5} \cdot q_{n5} \cdot K = 7 \cdot 5 \cdot 1 \cdot 1{,}1 = 38{,}5$$

№ 6 Кезең

$$T_6 = 7 \cdot t_{n6} \cdot q_{n6} \cdot K = 7 \cdot 20 \cdot 2 \cdot 1{,}1 = 308$$

Барлығы

$$T_{бар} = T_1 + T_2 + T_3 + T_4 + T_5 + T_6 = 38{,}5 + 38{,}5 + 308 + 38{,}5 + 38{,}5 + 308 = 770$$

$T_{бар} = 770$ сағат-нормасы

5.4 Бағдарламалық құралдардың (БҚ) бағасын анықтаудың негізгі қағидалары

БҚ жасаудың бағасына «Информатика мен есептеу техникасының бағдарламалық құралдарын қолдану мен жеткізу, өндіру, өңдеу реттерінің ережелерімен» сәйкес келесі шығын түрлері қосылады:

- теориялық (іздеу) зерттеулері, техникалық ұсыныстарды өңдеу, есептеу жұмыстарын жүргізу, есептеу тәжірибелерін жүргізу жұмыстарын моделдеу шығындары;
- тақырып бойынша ғылыми-техникалық әдебиетті оқу мен іздеу, ұқсас зерттеулерді жүргізу, жұмысты орындау әдістерін құру, техникалық тапсырмалар мен құжаттық жоспарларды жүргізу, техника-экономикалық дәлелдемелер жүргізу;
- жұмыс құжаттарын өндеу, жобалау шығындары;
- БҚ тестілеу, БҚ мәндерін өңдеу мен анализдеу, тәжірибе жүргізу мен орнату шығындары;
- БҚ өңдеудің техникалық дайындық шығындары және де оларды жасау технологиясын орындау шығындары;
- БҚ өңдеу жұмыстарына кететін басқа да тура шығындары жатады

Ғылыми-зерттеу жұмыстарды орныдаудың өзіндік құны келесі шығындардың қосындысынан тұрады:

- негізгі өңдеушілердің еңбекақысын төлеу;
- қосымша еңбекақыларын төлеу;
- еңбекті төлеу қоры;
- еңбекақы төлеу қорынан әлеуметтік салыққа бөліп шығару (13%);
- амортизационды аударылымдар;
- коммуналдық төлемдермен қоса арендалық төлем,
- материалдар шығыны (қағаз, картридж және т.б.).

5.2 кестеде негізгі жұмысты орындаушылардың еңбекақысы келтірілген.

5.3 кестеде материалды шығындар келтірілген.

5.5 Бағдарламалық құралдардың сметалық құнын есептеу реті

а) Еңбекті төлеу қорын (ЕТҚ) есептеу

$$ETK = \sum_{j=1}^{N} K_{Ti} \cdot N_i \text{ (теңге)} \qquad (5.2)$$

мұндағы $К_т$ – тарифтік ставка мың.теңге/адамға;

$$K_T = \frac{Ж \cdot t_n}{N} \text{ (теңге/адам)} \qquad (5.3)$$

мұндағы Ж – орындаушылар жалақысы;

tn – әр жұмыс түрі бойынша цикл ұзақтығы;

N – мамандар саны.

$$K_{T(бас)} = \frac{Ж \cdot t_n}{N} = \frac{1500 \cdot (5+10+5+10)}{1} = 45000 \text{ (мың.теңге/адам)}$$

$$K_{T(инж)} = \frac{Ж \cdot t_n}{N} = \frac{1250 \cdot (5+10+5+10)}{1} = 37500 \text{ (теңге/адам)}$$

$$ЕТК = \sum_{j=1}^{N} K_{Ti} \cdot N_i = 45000 + 37500 = 82500 \text{ (теңге)}$$

5.2 кесте– Жұмысты орындаушылардың еңбекақы төлемдерінің көрсеткіштері

Жұмыстың мазмұнының атаулары	Орындаушы	Жұмыс-сыйымдылығы сағат-нормасы	1 күн ішіндегі еңбекақы	Толық еңбек ақы
Жобаның мақсаты мен есептің қойылуы	Басқарушы инжинер	30	1500	45000
Тапсырмамен танысқандар	Инженер	30	1250	37500
Барлығы				82500

б) Еңбекті төлеу қорынан әлеуметтік салыққа бөліп шығару (11%)

Әлеуметтік қорға 13 % пайыз көлемінде еңбекті төлеу қорынан алынады.

$$С_{СК}=0,13 \cdot З, \qquad (5.4)$$

$$С_{СК} = 0,13*З = 0,13 \cdot 82500 = 10725 \text{ (теңге)}$$

в) «Материалдар» шығынын есептеу

г)«Ғылыми-зерттеу жұмыстар үшін арнайы құрылғылар» шығындарын есептеу

Нақты БҚ өндіру үшін кететін техникалық және бағдарламалық құралдар, типтік және дайындау қосымшаларын сатып алу шығындары жатады. [17]

Техникалық құралдар:

- Pentium 233/ 1.3Gb/l6Mb/Modem компьютерін сатып алу оны орнату үшін кететін шығын 47000 теңге кетеді;
- NE2000 базасындағы компьютерлік желіні сатып алып және ортнатуға кететін шығын 5000 теңгені құрайды;

5.3 кестеде жобалауға кететін материалды шығындар көрсетілген.

5.3 кесте– Материалды шығындар

Материал аты	Өлшеу шамасы	Саны	Біреуінің тұратын бағасы (теңге)	Барлығы (теңге)
Катридж	дана	1	5000	5000
Қағаз (пачкасы)	пачка	1	900	900
Дискета	дана	10	90	900
Барлығы				6800

Сонымен, Материалға кететін шығындар $С_{мат}$=6800 теңгені құрайды.

Сонымен, жобалау кезінде 2 компьютер қолданылады (жобалаудың бастапқы кезінде орнатылған уақыты 1 жылды құрайды, бастапқы бағасы 50000 теңге), принтер (сатып алынған уақыты жарты жыл, бастапқы бағасы 26000 теңгені құрайды),компьютерлік желі.

$Н_а$=40% амортизациялық норма орнатылған кезде 1 жылдық амортизациялық бөліп шығару құрайды:

$$А=0,4\ 47000+0,4\cdot5000+0,4\cdot50000+0,4\cdot26000=51200 \text{ (теңге)} \qquad (5.5)$$

Техникалық құралдарды сатып алу, орнату мен эксплуатациялау үшін кететін шығындар төмендегідей есептелінеді:

$$С_{тех}=47000+5000+50000+26000+51200=179200 \text{ (теңге)} \qquad (5.6)$$

Бағдарламалық құралдар:

- Windows 10 операциялық жүйе бағасы 11400 теңгені құрайды;
- С++ бағдарламалық тілінің бағасы 28000 теңгені құрайды.

Сонымен, бағдарламалық құралдарды сатып алу және орнату шығындары төмендегідей формуламен есептелінеді:

$$С_{баг}=11400+28000=39400 \text{ (теңге)} \qquad (5.7)$$

Сонымен ғылыми жұмыс үшін арнайы құрылғыларға кететін барлық шығындар келесі формуламен есептелінеді:

$$С_{АҚ}= С_{тех}+С_{баг}= 179200+39400=218600 \text{ (теңге)} \qquad (5.8)$$

д) Қосымша шығындар есептеу

Машиналық уақытқа кететін шығын төмендегідей формуламен есептелінеді

$$С_м=К_м+З_м \text{ (теңге)} \quad (5.9)$$
$$С_м=0,12\cdot 87000=10440 \text{ (теңге)}$$

мұндағы $К_м$ – машиналық уақыттың бір сағатына кететін тарифтік құн, өндеу-мекемесіндегі машиналық уақыттың өзіндік құнының жоспары бойынша 120 теңге/сағ алыналы;

$З_м$ – БҚ өндеу үшін кететін машиналық уақыт, 87 сағатқа сәйкес.

Бағдарламалау үшін арнайы оқу құралы «С++ энциклопедиясы» $С_{ок}$=3000 теңге

Байланыс қызметін қолдану шығындары (Интернет)

- абоненттік төлем 1500 теңгені құрайды;
- сағат бойынша төлем 110 теңге/сағат;
- жобалау үшін ақпаратты іздеу мақсаты бойынша Интернетті қолдану уақыты 0,5 сағ/күн

Барлығы:

$$С_{БҚ}=1\cdot 5\cdot 0,5\cdot 110+1500\cdot 1=1775 \text{(теңге)} \quad (5.10)$$

Сонымен барлық қосымша шығындарды келесі формуламен есептейміз:

$$С_{ҚШ}=С_М+С_{ОК}+С_{БҚ}=10440+3000+1775=15215 \text{(теңге)} \quad (5.11)$$

ж) «Қосымша үстеме шығындарды» есептеу

Ғылыми-зерттеу жұмыстарын ұйымдастыру мен басқару үшін бірнеше тақырып бойынша орындауға байланысты кететін шығындар,

- жоба басқарушысының әлеуметтік мұқтаждыққа алынып тасталғандағы еңбекақысы 3000 теңгені құрайды;
- инжинерлердің социалды мұқтаждыққа алынып тасталғандағы еңбекақысы 1500 теңгені құрайды.

Сонымен «Қосымша үстеме шығындары» $С_{ҚСШ}$=4500 теңге болады.

е) «Электрэнергия» шығындарын есептеу

$$С_{ЭЛ}=P_{n\cdot}\cdot t\cdot m_1 \text{(теңге)} \quad (5.12)$$

мұндағы P_n – 1,5+1=2,5кВт

$t\cdot$ - 7·30=210сағ

m_1 – 8 теңге, кВт/сағ

$С_{ЭЛ}=2,5\cdot 210\cdot 8=4200$

Бағдарламалау құралдарын өндеу құнын есептеу келесі формуламен анықталады:

$$С=С_{ЕҚ}+С_{СҚ}+С_{МАТ}+С_{АҚ}+С_{ҚШ}+С_{ҚҮШ}+С_{ЭЛ} \text{(теңге)} \quad (5.13)$$

С=82500+10725+6800+218600+15215+4500+4200=342540 теңге

5.4 кесте– БҚ өңдеудің сметалық құны

Шығындар атауы	Тақырып бойынша барлығы (теңге)
1. ЕТҚ	82500
2. Әлеуметтік сақтандыру	10725
3. Материалдар	6800
4. Ғылыми жұмыстар үшін арнайы құрылғылар	218600
5. Қосымша шығындар	15215
6. Қосымша үстеме шығындар	4500
7. Электрэнергия	4200
Барлығы	342540

5.1 сурет– БҚ өңдеудің сметалық құнының құрылымдық сұлбасы

5.6 Интелектуалды еңбек құнын анықтау

Ғылыми-зерттеу жұмысының құны келесі формуламен анықталады:

$$Қ=Ө+Т(теңге) \quad (5.14)$$

мұндағы Ө- өзіндік құны, теңге;

Т- таза табыс.

Өнімнің бастапқы құнын анықтаған кезде қажет тиімділіктің деңгейі анықталады. Мен рентабелділікті 30% деп аламын

$$Қ_Ө=Ө(1+Р/100)(теңге) \quad (5.15)$$

мұндағы Р- рентабелділік (Р=30%)

$$Қ_Ө=342540\cdot(1+30/100)=445300(теңге)$$

Содан кейін ҚҚС-пен (13%) қоса есептегендегі жүзеге асыру құны есептелінеді:

$$Қ=Қ_Ө\cdot 1{,}13(теңге) \quad (5.16)$$

$$Қ=445302\cdot 1{,}13=503000(теңге)$$

Сонымен соңғы мәні

$$Қ=503000(теңге)$$

5.1 кесте– Негізгі экономикалық көрсеткіштер

Көрсеткіш атаулары	Өлшем бірліктері	Барлығы
1.Штат саны	бірлік	2
2.БҚ өңдеудің сметалық құны	теңге	342540
3.Рентабельділік	%	30
4.Интелектуалды еңбектің бастапқы бағасы	теңге	445300
5.ҚҚС бірге бағасы	теңге	503000

5.7 Қорытынды

Менің дипломдық жобалауы бойынша осы бөлімінде бағдарламалық өнім жұмысын үлгідеуді жасауға 503 мың теңге кетеді. Сонымен қатар, осы жұмысты көптеген фирмалар сатып алуы мүмкін, соған қарағанда бұның бағасы көп емес.

Қорытынды

Бұл бітіру жұмысында VPN технологиясы базасында төрт негізгі қызмет түрі жүзеге асырылды. VPN техникалық жүзеге асырудың бес нұсқалары бар. Нұсқаны таңдаудың негізгі белгілеріне VPN құру қорларының өнімділігі мен олардың бағасы жатады. Виртуалды желілердің қорғалған арналарын құрған кезде VPN құралдары провайдер желісінде және пайдаланушы желісінде де орналасуы мүмкін. Осы факторларға тәуелді виртуалды желілерді құрудың үш сұлбасы бар. VPN тәжірибелік тұрғыда жүзеге асыру кезінде ен басты мәселе желіні қорғайтын басқа құрылғылармен салыстырғандағы VPN-құралдарының тиімді орналасу орнын анықтадық.

Қызмет көрсету сапасын қамтамасыз ететін базалық технологияларды зерттедік. MPLS белгі коммутация технологиясының негізінде виртуалды жеке желілер кең таралып жатыр. Соңғы кезде GMPLS белгі бойынша жалпы коммутация технологиясы алдыңғы орынды алуда.

Қазіргі кезде VPN құру үшін бірнеше протоколдар IPSec, PPTP, L2TP қолданылады. Осы протоколдар деректерді шифрлемейді. Олар тек қана VPN құру үшін шифрлеу алгоритмдері және басқа көптеген шарттардың қалай қолданылатындығын анықтайды.

VPN желісінде желілік ресурстарды тиімді үлестіру моделі зерттелген. Ол арналық модель базасында жүргізілді. Оған C++ тілінде бағдарлама құрылды. VPN желісінің өміршеңдігіне есептеу жүргізілді, оған Delphi тілінде бағдарлама жасалынды.

Сонымен қатар өміртіршілік қауіпсіздігі бөлімінде бөлмедегі еңбек жағдайы талданды, жасанды жарықтандыру мен ауа баптау қарастырылды.

Осы жобаны енгізудің техника-экономикалық негіздемесі мен бизнес-жоспар жасалынды. Бұл бағдарламалық өнім жұмысын үлгідеуді жасауға 503 мың теңге қажет.

Қысқартылған сөздер тізімі

АЖӨБ	Ашық жүйелердің өзара байланысы
АЖӨБЭМ	Ашық жүйелердің өзара байланысының эталанды моделі
ЖЭ	Желі аралық экран
ЛЕЖ	Локалды есептеу желілері
ИТҚ	Интегралданған телекоммуникациялы инфроқұрылым
ЖПТЖ	Жалпы пайдаланылатын телефонды желі
ATM	Asynchronous Transfer Mode
VPN	Virtual Private Network — виртуалды жеке желі
QoS	Quality of Service — қызмет көрсету сапасы
CE-router	Customer Edge router — шекаралық маршрутизатор
IOS	Internetwork Operating System — желі аралық операциялық жүйе
IP	Internet Protocol — Интернет протокол
IPSec	Internet Protocol Security — IP-қауіпсіздігі
IPX	Internet Package Exchange — желі аралық дестелік алмасу
ISP	Internet Service Provider — Интернет провайдері
L2F	Layer 2 Forwarding — 2 деңгей дестелерінің жылжуының протоколы
L2TP	Layer 2 Tunneling Protocol — 2 деңгейдің тоннелді протоколы
LDP	Label Distribution Protocol — белгілерді үлестіру протоколы
MPLS	Multiprotocol Label Switching — көп протоколды коммутация белгісі

Әдебиеттер тізімі

1. Росляков А.В. Оптимальное распределение сетевых ресурсов для реализации виртуальных частных сетей // Труды учебных заведений связи / СПб., СПбГУТ. — 2004.— С. 65-74.

2. Браун С. Виртуальные частные сети. — М.: Лори, 2001. — 508 с.

3. Запечников СВ., Милославская Н.Г., Толстой А.И. Основы построения виртуальных частных сетей: Учебн. пособие для вузов. — М.: Горячая линия-Телеком, 2003. — 249 с.

4. Сериков И. Виртуальные частные сети http://www.pcmag.ru/archive/5/ 059932.asp 20.10.2002.

5. Леонов С. Реальная виртуальность http://www.computerra.ru/offline/8/ 237/1149 25.11.2002.

6. Зима В., Молдовян А., Молдовян Н. Введение в защищенные виртуальные сети http://www.cobra.ru/ra/articles/p-vvzvs.html 10.10.2002.

7. Даффи Д. Поддержка качества в виртуальных сетях // Сети. — 2001. № 09. — С. 21.

8. Олифер В., Олифер Н. MPLS на службе VPN http://www.abn.ru/inf/lan/mpls. shtml 2.12.2002.

9. Олифер В., Олифер Н. Новые технологии и оборудование IP-сетей. СПб.: БХВ-Петербург, 2001. — 512 с.

10. Жанг Р. Сетевые услуги нового поколения http://www.osp.ru/lan/2001/12/ 032.htm 25.11.2002.

11. Воронин А., Курилов О. Организация услуг VPN на базе операторских сетей // Технологии и средства связи / Ежегодный отраслевой каталог. — 2002. — С. 68-73.

12. ГОСТ 21.958-76. Система “человек-машина”. Зал и кабины операторов. Расположение рабочих мест. Общие эргономические требования. – М.: Изд-во стандартов,1982.- с.91-98.

13. Охрана труда на предприятиях связи: Учебник для вузов / Под ред. Н.И. Баклашова. – М.: Радио и связь, 1985. – 280 с.

14. Кошулько Л.П., Суляева Н.Г., Генбач А.А. Производственное освещение. Методические указания к выполнению раздела «Охрана труда» в дипломном проекте (для студентов энергетических специальностей всех форм обучения). – Алматы.: РУМК, 1989. – 40 с.

15. Сухова Л.Ф., Чернова Н.А. Практикум по разработке бизнес-плана и финансовому анализу предприятия. – М.:Финансы и статистика, 1999.–с250

16. Демина Е.В., Иодко Е.К., Майесиф Л.И., Резникова А.П. Организация, планирование и управление предприятиями связи. – М.: Радио и связь, 1990.- с.24-71.

17. Основы экономики телекоммуникаций (связи) / Под ред. М. Н. Горелик, К.С. Голубицкой.– М.: Радио и связь, 1997. – 280 с.

18. Ұйым стандарты.Оқу әдістемелік және оқу жұмыстары. Оқу-әдістемелік және оқу жұмыстарының құрылуына, жазылуына, рәсімделуіне

және мазмұнына қойылатын жалпы талаптар. КЕАҚ СТ 56023-1910-04-2014. - Алматы: АЭжБУ, 2015.

19. Хакимжанов Т.Е. Безопасность жизнедеятельности. Расчет аспирационных систем. Методические указания к выполнению раздела в дипломных проектах. – Алматы: АИЭС, 2002.

20. Дюсебаев М. К. Безопасность жизнедеятельности. Методические указания к выполнению раздела в дипломных проектах. – Алматы: АИЭС, 2003. – 27 с.

21. Аманжолова К.Б., Алибаева С.А. Экономика предприятий телекоммуникаций: Учебное пособие. – А.: АИЭС 2000

А қосымшасы

Алгоритм листінгі

```
#include <iostream>
#include <cmath>  //
#define TRUE 1
#define FALSE 0
#define MaxNodes 5   //Төбе саны.
#define MaxInt 100000  //Шексіздіктің машиналық эквивалентті.
//Түйін түрін бейнелеу.
struct Uzel
{
int Element; //Берілген төбе номірі.
int Propusk; //Өткізгіштік қабілеті.
int Metka;   //Төбе белгіленген немесе жоқ.
};
class Spisok
{
  private:
      int C[MaxNodes][MaxNodes];     //Бастапқы өткізгіштік қабілеттің матрицасы.
      int c[MaxNodes][MaxNodes];      //Соңғы өткізгіштік қабілеттің матрицасы.
      int Put[MaxNodes][MaxNodes];  //Тесіп өткен жолдардың матрицасы.
int Potok [MaxNodes];                      //Ағындар.
      int Est (Uzel*,int,int);
      int Tpk (int*,int,int);
  public:
      void Vvod_Ves();
      int Reshenie ();
      void Vyvod(int);
};
void main()
{
  Spisok A;
  A.Vvod_Ves();
  A.Vyvod(A.Reshenie());
}
void Spisok::Vvod_Ves()   //Өткізгіштік қабілеттіліктердің матрицасын енгізу.
{
  cout << "Қабырғалардың өткізгіштік қабілеттіліктерін енгіз:\n";
  for (int i=0;i<MaxNodes;i++)
   for (int j=0;j<MaxNodes;j++)
     {
       cout << "C енгізіңіз[" << (i+1) << "," << (j+1) << "]: ";
       cin >> C[i][j];
       c[i][j] = C[i][j];
     }
}
void Spisok::Vyvod(int n) //Нәтижелерін қорытындылау.
{
  //Максималды ағын көлемін есептеу.
  for (int i=0,sum=0;i<=n;sum+=Potok[i++]);
```

А қосымшаның жалғасы

```
  cout << "\n Желідегі максималды ағын көлемі: " << sum;
  cout << "\n Әртүрлі қабырғалармен ағындар мәні:\n";
  for (i=0;i<MaxNodes;i++)
   for (int j=i;j<MaxNodes;j++)
     if (C[i][j])
     {
        cout << "Ребро (" << (i+1) << "," << (j+1) <<"): ";
        cout << "(" << C[i][j]  << "," << C[j][i] << ")-(";
        cout << c[i][j]  << "," << c[j][i] << ")=(";
        cout << (C[i][j]-c[i][j]) << "," << (C[j][i]-c[j][i]) << ") ";
        cout << "Поток: " << abs(C[i][j]-c[i][j]) << " ";
        if (C[i][j]-c[i][j]!=0)
        {
          cout << "Бағыты: ";
          if (C[i][j]-c[i][j]>0)
             cout << (i+1) << "->" << (j+1);
          else
             cout << (j+1) << "->" << (i+1);
        }
        cout << endl;
     }
}

int Spisok::Reshenie()
{
  Uzel SS[MaxNodes]; //Ауысуға болатын түйіндер жиынтығы.
  Uzel S[MaxNodes]; //Жол.
  int i,j=0,k,el,mx,mn;
  int m; //Жолдағы түйіндер саны.
  int nomer=-1; //Тесіп өтетін ағындар саны.
  int Tupik[MaxNodes]; //Тұйық төбелердің саны.
  int N_Tupik; //Массивтегі элементтер саны.
  while (j!=-1)
  {
    i=m=0;
    S[i].Element=0;
    S[i].Propusk=MaxInt;
    S[i].Metka=TRUE;
    el=0;
    N_Tupik=-1;
    while (el!=MaxNodes-1)
    {
      j=-1;
      for (k=0;k<MaxNodes;k++)
       if (c[i][k]!=0) //Егер нолінші ағын болса...
        if (i>0)   //Онда жолға төбелер қосылды
        {
          if (!Est(&S[0],m,k) && !Tpk(&Tupik[0],N_Tupik,k))
                          //онда келесі төбені қосамыз, егер ол тұйықталған болмаса.
          {
```

А қосымшаның жалғасы

```
          SS[++j].Element=k;
          SS[j].Propusk=c[i][k];
          SS[j].Metka=FALSE;
        }
      }
      else
        if (!Tpk(&Tupik[0],N_Tupik,k)) //Қайтадан артқа көшкен жоқпыз ба?
            //Ағын нолінші емес, онда ол бірінші төбе.
        {    //Осы төбені жолға қосамыз.
            SS[++j].Element=k;
            SS[j].Propusk=c[i][k];
            SS[j].Metka=FALSE;
        }
    if (j!=-1) //Жалғасы бар.
    {
      mx=SS[0].Propusk;
      el=0;
      for (k=1;k<=j;k++)
       if (SS[k].Propusk>mx)
         { el=k; mx=SS[k].Propusk; }
      S[++m].Element=SS[el].Element;
      S[m].Propusk=mx;
      S[m].Metka=TRUE;
      if (SS[el].Element==MaxNodes-1) //Тесіп өту жолы табылды.
      {
        nomer++;
        //Тесіп өтетін жолды есте сақтаймыз.
        for (k=0;k<=m;k++)
           Put[nomer][k]=S[k].Element;
        //Минималды ағынды іздейміз.
        mn=S[0].Propusk;
        el=0;
        for (k=1;k<=m;k++)
         if (S[k].Propusk<mn)
           { el=k; mn=S[k].Propusk; }
        Potok[nomer]=mn; //Оны есте сақтаймыз.
        //Қалған өткізгіштік қабілеттіліктерді есептейміз.
        for (k=0;k<m;k++)
        {
          c[S[k].Element][S[k+1].Element] -= Potok[nomer];
          c[S[k+1].Element][S[k].Element] += Potok[nomer];
        }
        el=MaxNodes-1; //Келесі итерацияға көшу.
        j=0;
      }
      else i=S[m].Element;
    }
    else //Жалғасы жоқ. Ол мүмкін болады, егер:
```

А қосымшаның жалғасы

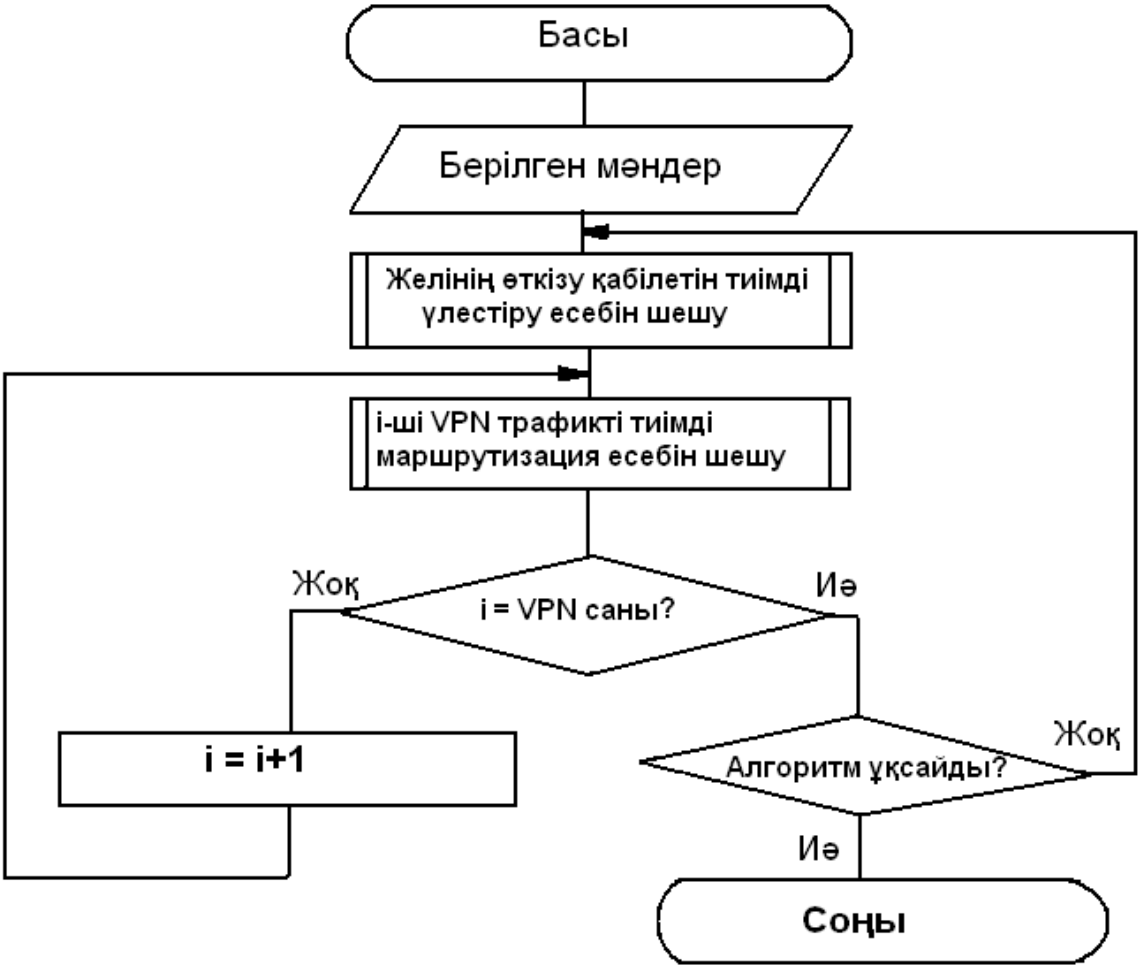
```
      {
        if (i==0)  //а) барлық өткізгіштік қабілеттер нолденген болса.
                //   Мұндай кезде - шығу
            el=MaxNodes-1;
        else       //б) Біз тұйықталған төбеге тірелдік. Массивте ұйықталған төбені есте
сақтаймыз және бір жолға артқа қарай шегінеміз.
        {
          Tupik[++N_Tupik]=S[m].Element;
          m--;
          i=S[m].Element;
        }
      }
    }
  }
  return nomer; //Тесіп өткен ағындарды қайтарады.
}

int Spisok::Est(Uzel S[], int m, int k)
//S жолында k төбесі бар екендігін функция тексереді.
//m – жолдағы элементтер саны.
// Егер төбе болса, 1 қайтарады және керісінше болған жағдайда 0 қайтарады.
{
  for (int l=0;l<=m;l++)
    if (S[l].Element==k) return 1;
  return 0;
}

int Spisok::Tpk(int Tupik[],int N_Tupik, int k)
// Тұйықталған төбелер массивінде k төбесі бар екендігін функция тексереді.
//N_Tupik – массивтегі қалған төбелер саны.
// Егер төбе болса, 1 қайтарады және керісінше болған жағдайда 0 қайтарады.
{
  if (N_Tupik==-1) return 0;
  for (int l=0;l<=N_Tupik;l++)
    if (Tupik[l]==k) return 1;
  return 0;
}
```

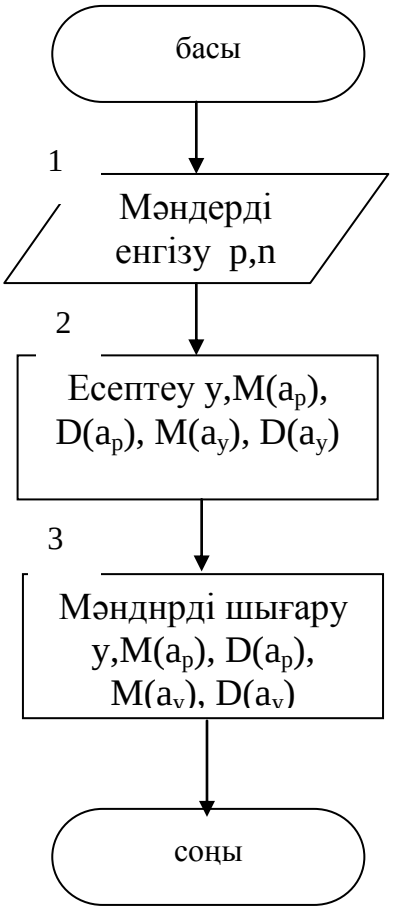
Ә қосымшасы

Құрылған модельдің блок сұлбасы



Б қосымшасы

Желі өміршеңдігінің блок сұлбасы



В қосымшасы

Желі өміршеңдігінің бағдарлама листінгі

```
unit Unit1;
interface
uses
  Windows, Messages, SysUtils, Variants, Classes, Graphics, Controls, Forms;
type
  TForm1 = class(TForm)
    GroupBox2: TGroupBox;
    Label1: TLabel;
    Label2: TLabel;
    Label3: TLabel;
    Button1: TButton;
    Button2: TButton;
    GroupBox1: TGroupBox;
    Label6: TLabel;
    Edit1: TEdit;
    Edit2: TEdit;
    Label8: TLabel;
    Label9: TLabel;
    Label10: TLabel;
    Label11: TLabel;
    procedure Button1Click(Sender: TObject);
    procedure Button2Click(Sender: TObject);
  private
    { Private declarations }
  public
    { Public declarations }
  end;
var
  Form1: TForm1;
implementation
{$R *.dfm}
procedure TForm1.Button1Click(Sender: TObject);
var
n,y,p,mar,dar,mau,dau:real;
begin
p:=strtofloat(edit1.text);
n:=strtofloat(edit2.text);
y:=n*(n-1);
  mar:=(n-1)*(2*p+(n-2)*(2*p));
    dar:=(2*p+(n-2)*(p*2))/n ;
     mau:=p*mar;
      dau:=p*dar;
      label1.Caption:=floattostr(y);
       label2.Caption:=floattostr(mar);
       label3.Caption:=floattostr(dar);
end;
procedure TForm1.Button2Click(Sender: TObject);
begin
```

В қосымшаның жалғасы

```
close;
end; end.
```