ҚАЗАҚСТАН РЕСПУБЛИКАСЫ БІЛІМ ЖӘНЕ ҒЫЛЫМ МИНИСТРЛІГІ

Коммерциялық емес акционерлік қоғамы
АЛМАТЫ ЭНЕРГЕТИКА ЖӘНЕ БАЙЛАНЫС УНИВЕРСИТЕТІ

«Компьютерлік технологиялар» кафедрасы

«Қорғауға жіберілді»
Кафедра меңгерушісі
ф.-м.ғ.д., проф. Құралбаев З.Қ.
_____
(қолы)
«_____»_____2014 ж.

ДИПЛОМДЫҚ ЖОБА

Тақырыбы: ««Trust company» ЖШС корпоративтік желісінің қауіпсіздігін бұлттық технология негізінде қамтамасыз ету»
5В070400 – «Есептеу техникасы және бағдарламалық қамтамасыз ету» мамандығы бойынша

Орындаған Сейдахмет Мейірімбек Төленұлы тобы: ВТк-10-2

Жетекші аға оқытушы Рахимжанова З.М.

Кеңесшілер :

. Экономикалық бөлім бойынша :
доцент Боканова Г.Ш.
_____«29»05_____ 2014ж.
(қолы)

Өмір тіршілігі қауіпсіздігі бойынша:
аға оқытушы Муташева Г.С.
_____«28»04._____ 2014 ж.
(қолы)

Есептеу техникасын қолдану бойынша :
аға оқытушы Рахимжанова З.М.
_____«23»05_____ 2014 ж.
(қолы)

Мөлшер бақылаушы:
аға оқытушы Рахимжанова З.М.
_____«26»05_____ 2014 ж.
(қолы)

Пікір жазушы :
ҚазҰТУ, РЭжТ кафедрасының аға оқытушысы: Усембаева С.Г.
_____«____»_____ 2014 ж.
(қолы)

Алматы 2014

ҚАЗАҚСТАН РЕСПУБЛИКАСЫ БІЛІМ ЖӘНЕ ҒЫЛЫМ МИНИСТРЛІГІ

Коммерциялық емес акционерлік қоғамы
АЛМАТЫ ЭНЕРГЕТИКА ЖӘНЕ БАЙЛАНЫС УНИВЕРСИТЕТІ

«Ақпараттық технологиялар» факультеті
«Есептеу техникасы және бағдарламалық қамтамасыз ету» мамандығы
«Компьютерлік технологиялар» кафедрасы

жобаны орындауға берілген

ТАПСЫРМА

Студент Сейдахмет Мейірімбек Төленұлына

Жоба тақырыбы «Trust company» ЖШС корпоративтік желісінің қауіпсіздігін бұлттық технология негізінде қамтамасыз ету
ректордың «115» 24 қаңтар №2013 бұйрығы бойынша бекітілген.

Аяқталған жұмысты тапсыру мерзімі: «29» наурыз 2014 ж.

Жобаға бастапқы деректер (талап етілетін жоба нәтижелерінің параметрлері және нысанның бастапқы деректері):
"Trust Company" ЖШС корпоративтік желісінің қауіпсіздігін ұйымдастыру. Қауіпсіздікке қатысты құралдарды таңдау.

Диплом жобасындағы әзірленуі тиіс сұрақтар тізімі немесе диплом жобасының қысқаша мазмұны:
– қауіпсіздік мәселесі, ақпарат алмасудағы қорғаныс шаралары, желіге келетін қауіп-қатер және желінің қауіпсіздік қызметі жайлы жалпы мағлұмат;
– компьютерлік желінің қауіпсіздігін ұйымдастыру үшін қолданылатын технологиялар, құралдар, программалық сипаттамаларға мен ұйымдастыру.

Сызба материалдарының (міндетті түрде дайындалатын сызуларды көрсету) тізімі:

– жасалған жобаның жұмыс істеу қабілеттілігі мен функционалдылығын көрсететін графикалық материалдар;
– жобаланған жеңіл фауіпсіздігінің сызбасы.

Негізгі ұсынылатын әдебиеттер:

1. Marvin Washeke Cloud standards: Agreement that Hold Together Clouds. Ugg-Bo Apress, 2012.-380c.
2. Aidan Finn, Hans Vredevoort, Patrick Lownds. Microsoft Private Cloud Computing Ugg-Bo John Wiley, 2012.
3. Цуриов В.А Основы информационной безопасности автоматизированных систем. Краткий курс. Феникс.
4. Стивен Б., Виртуальное частное сети. Ug-Bo Лори, 2009. - 410с

Жоба тараулары бойынша кеңес берушілер және оның мерзімі:

Бөлім	Кеңесші	Мерзімі	Қолы
Негізгі бөлім	Рахимжанова З.М.	23.05.2014	
Тіршілік қауіпсіздігі	Муташева Г.С.	22.04.2014	
Экономикалық бөлім	Боканова Г.Ш.	29.05.2014	
Норма бақылаушы	Рахимжанова З.М.	26.05.2014	
Есептеу техникасын қолдану	Рахимжанова З.М.	23.05.2014	

диплом жобасын дайындау

КЕСТЕСІ

№ р/с	Тарау аттары, әзірленетін сұрақтардың тізімі	Жетекшіге ұсыну мерзімдері	Ескерту
1	Бұлттық есептеу қауіпсіздігі	10.12.2013	
2	Виртуалды ортаның қауіпсіздігін қамтамасыз ету	20.12.2013	
3	Периметрді қорғау және желіге шек қою	06.01.2014	
4	Жеңілдікті эрандар	16.01.2014	
5	GNS3 жолының графикалық симуляторы	21.01.2014	
6	PIX Firewall эмуляциясы	12.02.2014	
7	Nexus 7010 регистрациясы	24.02.2014	
8	Мәлімет өңдеу орталығы	7.03.2014	
9	Ядро қабаты	19.03.2014	
10	Ауа кондиционерлеу жүйесінің құрылғысы, есебі	12.04.2014	
11	Ауа алмасуды есептеу	24.04.2014	
12	Бизнес-жоспар	1.05.2014	
13	Бағдарламалық қамсыздандыру шығынының есебі	8.05.2014	
14	Экономикалық тиімділікті есептеу	15.05.2014	
15	Ақпаратай құралдардың қорғалуы	19.05.2014	

Тапсырманың берілген уақыты «10» қазан 2014 ж.

Кафедра меңгерушісі _____ (қолы) ф.-м.ғ.д., проф. Құралбаев З.Қ.

Жоба жетекшісі _____ (қолы) аға оқытушы Рахимжанова З.М.

Орындалаты тапсырманы қабылдаған студент _____ (қолы) Сейдахмет Мейірімбек Төленұлы

Аңдатпа

Бұл дипломдық жобада «Trust company» ЖШС корпоративтік желісінің қауіпсіздігін бұлттық технология негізінде қамтамасыз ету қарастырылады. Жалпы жобаның басты мақсаты – бұлттық есептеу жүйесінде ақпарат алмасу процесіндегі ақпараттың қауіпсіз жетуін қамтамасыз ету. Жабдықты таңдау және желіні жобалау ұсынылған және дәлелденеді. Үзіліссіз жұмыс істейтін желі ұйымдастырылады.

Жобада техника – экономикалық сипаттағы мәселелер қарастырылады, оның ішінде осы жобаны іске асыру үшін жұмсалатын шығындарды анықтау, бизнес жоспар жасау және тіршілік қауіпсіздігі мәселелері қарастырылады.

Аннотация

В данном дипломном проекте рассматривается обеспечение безопасности корпоративной сети в основе облачной технологии для ТОО «Trust company». Основной цель проекта – организовать защиты информации в системе облачных вычислении при обмене информации. Выполнено проектирование сети и организованна ее защита, с использованием таких устройств, как коммутаторы, маршрутизаторы, межсетевые экраны. Представлены и обоснованы методы выбора оборудования и проектирования сети. Организованна бесперебойная работа сети.

В проекте рассмотрены вопросы технико-экономического характера, в частности определение затрат для реализации данного проекта, составление бизнес-план, затрагиваются вопросы безопасности жизнедеятельности и охраны труда.

Annotation

In this thesis project will be considered the security of corporate networks in the cloud-based technology for LLP «Trust company». The main objective of the project - to organize the protection of information in the system of cloud computing in the exchange of information. Achieved network design and organized its defense, using devices such as switches, routers, firewalls. Methods are presented and justified choice of equipment and network design. Organized network uptime.

The project addressed issues of technical and economic nature, in particular the definition of costs for the project, developing a business plan, addresses the issues of life safety and health.

Мазмұны

Кіріспе

Қолданыста пайда болғанына он жылдан астам уақыт болғанына қарамастан, «бұлт» сөзін естімеген адам жоқ шығар. Оған қоса көптеген қолданушылар бұлттық есептеудің өнімдерін күнделікті қолданыста өз қажеттеріне жаратуда.

Бұлттық есептеу қызметіне нарықтың сапалық және сандық баға бергеніне сүйенсек, техникалық әрі икемділік жағынан қойылатын талаптарды толықтай қанағаттандыруда және қызмет түрлерінің әр бағытында тұрақты түрде өсуде. Осы тұста қоса кететін бір мәлімет, ол Gartner компаниясының болжамы бойынша бұлттық есептеу нарығы 2014 жылдың ішінде 190 миллиард долларға жетеді. Ал Merrill Lynch компаниясы 200 миллиард долларға дейін өсуі мүмкіндігін болжауда. Ол бұлттық есептеудің компьютер индустриясында алатын орны ерекше, әрі болашағы зор дегенді білдіреді.

Бұлттық есептеу технологиясының қарқынды дамуы ақпараттың көп болуына және оның алмасу қарқынының артуына алып келіп отыр. Мұндай жылдамдық пен ауқымдылық ақпаратты жіберудегі қауіпсіздікті арттыру шараларын күшейтуді қажет етеді. Яғни жалпы бұлттық есептеудің пайда болуы ақпараттық ұрлық пен тыңшылықтың жаңа бір көрінісін алып келді. Осыған байланысты ақпаратты қорғау құралдары мен әдістерін жетілдіру ең үлкен мәселеге айналды.

Құпия ақпарат — құқықтық режімін меншік иесі коммерциялық, кәсіптік (өнеркәсіптік) құпия, мемлекеттік қызмет жайындағы және басқа заңнамалық кесімдер негізінде тағайындайтын қызметтік, кәсіптік, өнеркәсіптік, коммерциялық және т.б. ақпарат қорғауды талап ететін ақпарат.

2013 жылы құпия ақпараттардың таралуы осы жылдың алғашқы алты айының негізгі әлемдік тақырыбы ретінде қарастырылды деп мәлім етеді InfoWatch аналитикалық орталығы. Ол барлық блоктардағы және басқа ресурстардағы ақпараттардың таралуын қарастырып, мамандандырылған компаниялар бойынша бар - жоғы 382 жағдайда мәліметтердің жоғалуын мәлім етеді. Бұл орта есеппен күніне 2,1 құпия ақпараттардың таралуын құрайды.

Дипломдық жоба шеңберінде бұлттық есептеуді қорғауды іске асыру кезінде келесідей маңызды мәселелерге тоқталып, өз шешімімді ұсынамын: бұлттық есептеуде жүретін ақпарат алмасуға сырттан рұқсатсыз қолжеткізуді, нақтырақ айтсақ желіге жасалатын шабуылдардың алдын алу, байланысты қамтамасыз ететін құрылғыларда орналасқан бағдарламалардың осал тұстарын анықтау, қолданушымен ұштасатын тұсты сенімді ету.

Осы мақсатта, бұл жобамның желілік байланыс құрылымын GNS3 желілік графикалық симуляторында жасаймын. GNS3 күрделі желілерді эмуляциялай алатын желінің графикалық симуляторы болып табылады. Бұл желілік симулятордың мүмкіншіліктері мен артықшылықтары өте көп. Менің дипломдық жобамда қоданатын күрделі байланыстар мен ауыр баптамаларды іске асыруға таптырмас шешім болып табылады.

1 Бұлттық есептеудің қауіпсіздігі

1.1 Бұлттық есептеудің нарықтағы орны

Бұлттық есептеулер – қолданушыларға өз компьютерінің жұмыс істеу қабілетіне, оның бағдарламалық қамтамасының мүмкіндігіне тәуелді болмауға мүмкіндік беретін ең заманауи сервис. Қарапайым сөзбен айтар болсақ, тұтынушы өз компьютерінде белгілі бір бағдарламаны іске қосқанда, негізгі есептеулер мен ондағы дереккөздер интернеттегі шалғай серверлерде орындалып, сол жерде сақталады да, ал жұмыс нәтижесі жаңағы тұтынушының компьютерінде стандартты веб–браузердің терезесіне шығарылып көрсетіледі.

Осындай сервисті қолданушы кәсіпорындар саны күннен күнге артуда. Өздерінің ішкі мәлімет өңдеуші орталықтарын сыртқы коммерциялық қызмет көрсететін аутсорсингке тапсыруда. Бұлттық технология қызметін қолданушы кәсіпорындар өздерінің құнды мәліметтері қаншалықты дәрежеде сақталып және өңделіп жатқан процестің қауіпсіздігі туралы уайымдауы мүмкін. Әрине орынды, себебі ондағы мәліметтер өзге тұлғалардың қолына түссе орасан зор зиян тиеді.

Бұлттық есептеу қызметіне нарықтың сапалық және сандық баға бергеніне сүйенсек, талаптарды қанағаттандыруда және тұрақты түрде өсуде.

Gartner компаниясының болжамы бойынша бұлттық есептеу нарығы 2014 жылдың ішінде 190 миллиард долларға жетеді деп есептеуде. Ал Merrill Lynch компаниясы 200 миллиард долларға дейін өсуі мүмкіндігін болжамдауда. 1.1 – суретте көрсетілгендей, қазіргі уақытта 200 жуық бұлттық қызмет көрсетуші жүйелер бар.

Сурет 1.1 – Бұлттық есептеудің қолданыс аясы

Аналитикалық фирманың жүргізген сауалнамасы бойынша IT–менеджерлер жартысынан көбі бұлттық есептеу технологиясын қолдануға ниет білдірген. Heavy Reading Insider атты компанияның бұлттық есептеудің қауіпсіздігіне арналған «Cloud Service Fly Into Some Turbulence» атты жүргізген зерттеулерінде келесі кезектегі провайдер–компаниялардың қызметтері қолданылған: Amazon Web Services, AT&T, GoGrid Cloud Hosting; Google, IBM, Joyent, Rackspace Hosting, Savvis, Terremark Worlwide, VMWare және Verizon Communications. 1.2 – суретте бұлттық технологияның платформасын, гипервизорды және аппаратпен қамтамасыз ететін провайдер–компаниялардың сұлбасы көрсетілген.

Бұндай қызметтердің негізгі проблемасы – нарықтың көп бөлігімен келісілген бұлттық есептеудің қауіпсіздігін қамтамасыз ететін стандарттың жоқтығы. Көптеген сертифицияланған процедуралар мен әдістердің бар екендігіне қарамастан, басты талаптарға негізделген қауіпсіздікті қамтамасыз ететін біртұтас тәсіл мен методика әлі күнге дейін жоқ. Тұтынушылар өз ақпараттарының қауіпсіздігіне тек көптеген кепілдік беретін сертификаттар, заңдар немесе қызмет көрсету уақытының ұзақтығымен ғана кепілдік бере алады, нақты шешім жасалынбаған. Бұндай қызметпен қамтамасыз ететін провайдерлердің өздері қауіпсіздіктің қаншалықты дәрежеде қажет екеніне сенімді бола алмайды. Сол себепті виртуализацияға көп көніл бөледі.

2009 жылы сәуірінде Cloud Security Alliance (CSA) атты бұлттық есептеудің қауіпсіздік жөніндегі ассоциация қауіпсіздікке байланысты бүкіл критери жиынтығын жасаған болатын. Бірақ біз оны тұтынушыларға әмбебап әрі толық қапіпсіздік қорғанысын қамтамасыз ететініне кепілдік бере алмаймыз.

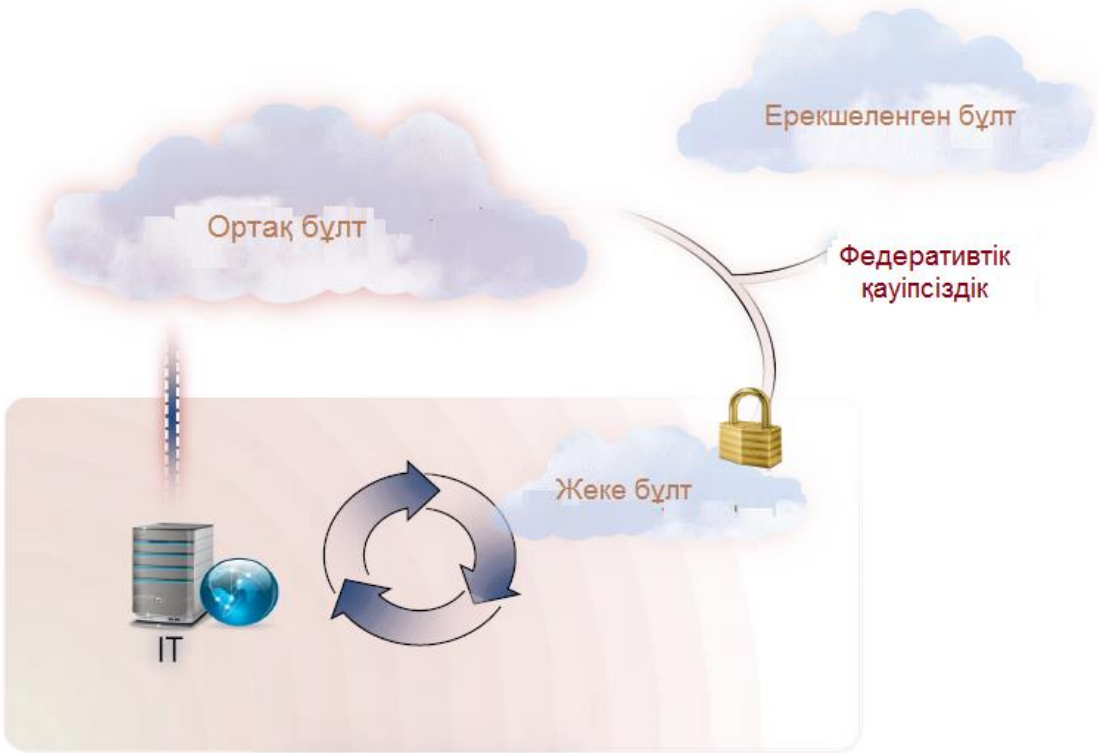
Сурет 1.2 – Бұлттық есептеуде қызметі колданылатын провайдер–компаниялар

Бұлттық есептеудің қауіпсіздік моделі дәстүрлі қауіпсіздік моделінен маңыздырақ, себебі өңделетін мәліметтердің қорғалмаған ортаға жіберілуі өте қауіпті, оған қоса мүлде жоғалып кетуі мүмкін. Бұған қарамастан нарықта бұлттық есептеудің қауіпсіздігін қамтамасыз ететін провайдерлер көптеп кездеседі. Яғни оған деген сұраныс та қызығушылықта артып келеді дегенді білдіреді. Бірақ бұлттық есептеудің қауіпсіздігін қамтамасыз ету оңай шаруа емес, уақытты көп алатын әрі бұлттық есептеудің дамуымен бірге қиыншылықтарыда артып отыратын мәселе.

Қазіргі кезде тұтынушыларға бұлттық есептеудің қауіпсіздігі өте жоғары дәрежеде қорғалғандығы жөнінде толықтай көз жеткізудің бір–ақ жолы бар. Ол – тұтынушыларды белсенді түрде төніп тұрған қауіп жайлы хабардар етіп, оны шешу жолында жасалған жұмыстарды түсіндіріп отыру қажет. Және оны тек CSA дәрежесінде емес, өзгеде қызмет ұсынушы провайдерлерге де жүктелу керек.

1.2 Бұлттық есептеулерге төнетін қауіп және оны қорғау әдістері

Мәлімет өңдеу орталығы қауіпсіздік пен тиімділікті арттыру мақсатында бір кеңістікте орналасқан серверлер жиынтығын білдіреді. Мәліметтерді өңдеу орталықтарын желілік, физикалық, сенімді электрлік қамтама мен жұмыстың тұрақтылығын қорғау керек. Қазіргі уақытта нарықта мәлімет өңдеу орталығын әр түрлі қауіп–қатерден қорғаудың кең спектрлі шешімдері бар. Оларды тапсырманы тар спектрда шешуі біріктіреді. Дегенмен, бұл тапсырмалардың спектрі классикалық аппараттарды виртуалды платформалардың аппараттық жүйелері ығыстырып шығуына байланысты біраз кеңейтілді. Белгілі қауіп түрлеріне (желілік шабуыл, операциялық жүйедегі бағдарламадағы әлсіздік, қауіпті бағдарламалық қамтама) ортаны (гипервизор) бақылауға байланысты, машиналар арасындағы трафик, қолжетімділік құқығын шектеу секілді қауіп түрлері қосылды. Мәлімет өңдеу орталығының ішкі қорғау сұрақтары мен саясаты, сыртқы реттеуге деген талаптар кеңейтілді. Жаңа мәлімет өңдеу орталықтарының салалардағы жұмысында техникалық сұрақтардың жабылуы мен қауіпсіздікке қатысты сұрақтарға талап күшейді. Виртуализация платформасының келуі қолданушы компаниялардың қауіпсіздікке қатысты мәселемен шындап кірісу дәрежесіне жетті. Бір жыл бұрын компаниялар бұл мәселеге теориялық тұрғыдан ғана қараған болатын. Маңызды бизнес жүйелер мен бағдарламаларды қауіпсіздікпен қамтамасыз ету уақыт өткен сайын қиындай түсуде. Виртуализацияның пайда болуымен көптеген жүйенің виртуальды машинаға көшуінің белсенді себебі болды. Дегенмен жаңа ортада бағдарламаның эксплуатациясына қатысты қауіпсіздікпен қамтамасыз ету ерекше шешімді қажет етеді. Көптеген қауіп түрлері зерттеліп қойған және оларға қорғаныс құралдары ойлап табылған, бірақ оларды бұлтта қолдану үшін икемдендіру қажет. 1.3–суретте бұлттық есептеулерді қорғау әдістері көрсетілген[1].



Сурет 1.3 – Бұлттық есептеулердің қорғау әдістері

Бұлттарды бақылау және басқару–қауіпсіздік проблемасы болып табылады. Бұлттың барлық қорлары түгел және онда бақыланбайтын виртуалды машина жоқ, артық процесстердің қосылмағандығына, бұлт элементтерінің өзара конфигурациясы бұзылмағандығына кепілдік жоқ. Бұл жоғары дәрежелі қауіп түрі.

Ол бұлтты басқарумен қатысты болғандықтан, біріңғай информациялық жүйе ретінде оған жалпы қорғауды жеке құрастыру керек. Бұл үшін бұлттық инфраструктураға қауіп–қатерді басқару моделін қолдану қажет. Физикалық қауіпсіздікпен қамтамасыз етудің негізінде серверлер мен желілік инфраструктураларға физикалық қолжетімділікке қатаң бақылау жатады. Физикалық қауіпсіздіктен желілік қауіпсіздіктің айырмашылығы басып ену мен желіаралық экранды қорғайтын сенімді қауіп моделін тұрғызу.

Желіаралық экран фильтр жұмысын білдіреді. Яғни, мәлімет өңдеу орталығының ішкі желілерін әр түрлі дәрежелі сенімсіз желілерге шектеу қою. Ол интернеттен қолжетімді жеке серверлер немесе ішкі желідегі серверлер болуы мүмкін. Бұлттық есептеулерде платформа ретінде маңызды рөлді виртуализация технологиясы атқарады. Мәліметтің тұтастығын сақтау және қауіпсіздікпен қамтамасыз ету үшін бұлттық есептеулерге негізгі қауіп–қатердің түрлерін атап өтеміз. Келесі кезекте бұлттық есептеуге физикалық тұрғыдан және виртуалдық тұрғыдан келетін қауіп–қатерлердің түрлерімен оларды шешу жолдарына тоқталамыз.

Операциялық жүйелердің, модульді компоненттердің, желілік протоколдардың әлсіздігі – дәстүрлі қауіп түрлері. Олардан сақтану үшін

желіаралық экрандарды, firewall, антивирус, IPS және басқа да компоненттерді орнату жеткілікті. Сонымен қатар бұл құрылғылардың виртуализация шартында тиімді жұмыс істеуі шарт.

Шифрлау–мәліметті сақтаудың ең тиімді жолдарының бірі. Мәліметке рұқсат беруші провайдер тұтынушының мәліметтерді өңдеу орталығында орналасқан мәліметтерін шифрлауы тиіс. Егер қажеттілік болмаса, қайтарымсыз жоюға болады.

Шифрланған мәліметтер жіберілу кезінде аутентификациядан кейін ғана қолжетімді болу керек. Мәліметтерді оқу немесе өзгеріс енгізу тіпті сенімді түйіндерден енген болса да мүмкін болмайды. Ондай технологиялар бұрыннан белгілі. Мысалы, AES, TLS, Ipsec бұрыннан провайдерлермен қолданылып келеді.

Бұл шабуыл түрі жалпы қауіпсіздік принципімен бұлттың көп қабаттылығымен байланысты. Бұлтқа төнетін қауіп–қатер жөніндегі статьяда келесі шешімдер жарияланған: Бұлттың әрбір бөлігіне жасалатын функционалды шабуылдан келесі сақтандыру шараларын жасау керек: прокси үшін – DoS–шабуылдан тиімді қорғаныш; веб–сервер үшін– беттің бүтіндігін бақылау; бағдарлама серверіне–бағдарлама деңгейінің экраны; СУБД үшін – SQL–инъекциядан қорғаныш, мәліметті сақтау жүйесіне–дұрыс бэкаптар (резервті көшірме), қолжетімділікті шектеу. Бұл қорғаныш механизмдері бөлек шығарылған. Бірақ олар бұлттың комплексті қорғалуы үшін әлі жинақталмаған. Сондықтан, оларды біріңғай жүйеге интеграциялау тапсырмасын бұлтты жасалу уақытында ұйымдастыру керек.

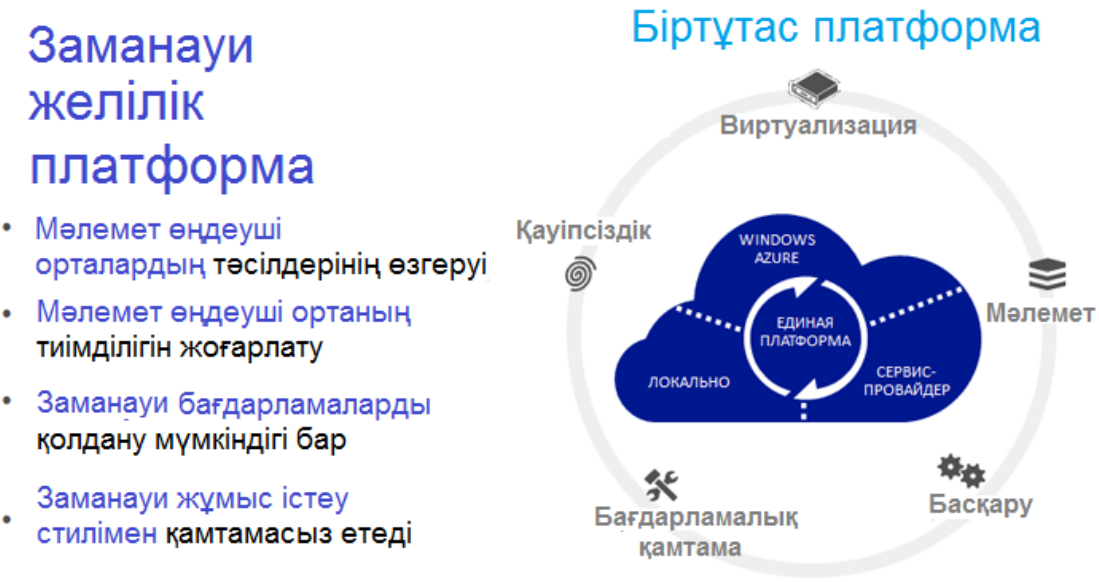
Жеке виртуалды машина мен виртуалды желіні қолдану. Виртуалды машиналар VPN (Virtual Private Network), VLAN (Virtual Local Area Network) және VPLS (Virtual Private LAN Service) секілді технологиялармен кеңейтілуі керек. Провайдерлер тұтынушыларды бір–бірінен біріңғай программалық ортада мәлімет кодының өзгеруіне байланысты оқшаулайды. Бұл шешімнің стандартсыз кодта тесік тауып, мәліметтерге қолжетімді қылатын қауіптері бар. Кодта мүмкін қателіктердің болуына байланысты тұтынушы өзінің емес, басқа адамның мәліметін алуы мүмкін. Соңғы уақытта мұндай инцидиенттер біраз кездесіп жүр[2].

1.3 Қарапайым серверлерді бұлттық есептеулерге ауыстыру кезінде туындайтын қиындықтар

Бұлттық есептеулерді қорғауға қойылатын талаптар мәліметті өңдеу орталықтарын қорғауға қойылатын талаптармен бірдей. Дегенмен, мәлімет өңдеу орталығын виртуализациялау мен бұлттық ортаға өту жаңа қауіптердің тууына әкеліп соғады.

Есептік қуатты интернет арқылы басқару бұлттық есептеудің негізгі мінездемесі болып табылады. Дәстүрлі мәлімет өңдеу орталықтарында инженерлердің мәліметке қолжетімділігі физикалық тұрғыда өтсе, бұлттық ортада ол Интернет арқылы жүзеге асады. Қолжетімділікті бақылауды шектеу

мен жүйелік деңгейде өзгерістің мөлдірлігі, білінбеуі қауіпсіздіктің негізгі критериі болып табылады.



Сурет 1.4 – Біртұтас заманауи желілік платформаның сұлбасы

1.4 Виртуалды машиналардың динамикалығы

Виртуалды машиналар динамикалылығының артықшылықтары мен кемшіліктеріне тоқталар болсақ. Жаңа машинаны жасап, оның жұмысын тоқтату, қайта қосуды кішкентай уақыт аралығында жасауға болады. Олар клондалады және физикалық серверлер арасында ауыстырыла алады. Бұл өзгергіштік қауіпсіздік жүйесінің біртұтастығына кері әсерін тигізеді. Дегенмен, виртуалды ортада операциялық жүйе мен бағдарламаның әлсіздігі бақылаусыз таралады және ерікті уақыт аралығынан кейін қайта пайда болып отырады (мысалы, резервті көшірмені қайта орнату кезінде). Бұлтты есептеулер ортасында оның орналасуы мен күйіне қарамастан жүйенің қауіпсіздік күйін жазып отыру керек.

Қазіргі таңда резервті көшірудің бағдарламалық қамтаманы ұсынушылардың ішінен CommVault, EMC, Symantec және IBM секілділер ерекше көзге түседі. Резервтік көшіру бір тұсынан виртуалды серверлердің қауіпсіздігін қамтамасыз ететін болса, екінші тұсынан физикалық серверді қорғауғада өз үлесін қосады. Сол себепті виртуалды машинаны резервті көшіру әдісін таңдағанда селқос қарамау қажет. Нарықтың 43 пайызын виртуалды машинаның агенттерін қолдану арқылы тұрақты резервті көшіру жасау әдісі алып отыр. Екінші кезекте виртуалды машинаның резервті көшірмесінің бағдарламаларды тұрақты түрде көшіру опциясын қолданады екен. 18%–ы виртуалды машинаға арнап жасалған резервті көшіру бағдарламасын қолданады екен. Дәстүрлі әдіспен қоса виртуалды ортаға арналған резервті

көшіру өнімдерін нарықтың 5%–ы орынды деп ойлайды. VMware компаниясының өнімдерінде қолданатындар кездеседі, мысалға VMware Consolidated Backup өнімін қолданушылар 5%–ды құрайды. Қалған пайызы осы типтес өзгеде резервтеу бағдарламаларды немесе жүйелерді қолдануданады.

Сурет 1.5 – ВМ резервті көшіру әдістерін қолдану ауқымы

Администраторлардың көзқарасы бойынша 1.5–суретте көрсетілген статистика бойынша гипервизор виртуализацияға ең алғашқысы өте икемді деп ойлайды. Ерекше айта кететін тұсы, ол резервті көшіруді басқару функциясы виртуалды ортаны басқару құралдарымен тығыз байланыста болғандығы. Виртуалды машиналарды резервтеп көшіру мақсатында арнайы жасалған бағдарламалар жасаушылар олардың өнімдері виртуалды ортамен қоса, физикалық ортаны да әмбебап жүйемен жоғары дәрежеде, жаңа технологиялармен қорғайтынына толыққанды уәде береді[3].

Бұлтты есептеулер серверлері мен желілік серверлер бірдей операциялық жүйелер мен бағдарламаларды қолданады. Бұлттық есептеулер үшін алыстан бұзу қаупі мен қауіпті бағдарламалық қамтамамен жұқтыру қауіптілігі аса жоғары. Виртуалды жүйелер үшін де қауіп дәрежесі жоғары. Параллельді виртуалды машиналар «шабуыл бетін» жоғарылатады. Іздеп табу мен қауіп–қатердің алдын–алу жүйелері олардың бұлттық ортада орналасуына қарамастан қауіпті белсенділікті виртуалды машиналар дәрежесінде анықтай алуы қажет.

Виртуалды машина өшіп тұрған кезде ол жұқтырып алу қаупіне ұшырайды. Виртуалды машиналар образдарының қоймасына желі арқылы қолжетімділіктің өзі жеткілікті. Өшірулі виртуалды машинаға қорғаныш бағдарламалық қамтаманы орнату мүмкін емес. Мұндай жағдайда әрбір виртуалды машинаның ішінде ғана емес, гипервизор дәрежесінде қорғаныс жүзеге асырылуы тиіс.

Бұлтта қолданылатын виртуалды машиналардың көп бөлігі виртуалды машинаны жасау, ауыстыру, утилизациялауды сенімді басқару жүйесін талап етеді. Басқару жүйесіне араласу басқа виртуалды машиналарды бұлағаттап, басқаларын ауыстырып қою мүмкіндігі бар көрінбейтін виртуалды машиналардың пайда болуына әкеліп соғады.

1.5 Виртуалды ортаның қауіпсіздігін қамтамасыз ету

Виртуализация мен бұлттық есептеу ақпараттарды жіберу, қабылдау және қызмет ету жүйесін өзгертті. Икемді және ресурстарды нәтижелі түрде қолдануының әсерлілігін жоғарлатып, мекемелердің көздеген мақсаттарына жетуін жылдамдатты. Осымен қоса, бұл жаңа технологиялар ақпаратқа жаңа қауіп–қатердің тууына алып келді. Яғни қауіптің негізгі себептерінің бірі жұмыс процестерінің өзгерісінде болып табылады. Белгілі жетістікке жету үшін мекемелер қауіпсіздікпен қамтамасыз ету мәселесін шешу қажет.

Проблемалардың негізгі төрт тобын ерекшелеп көрсетуге болады:

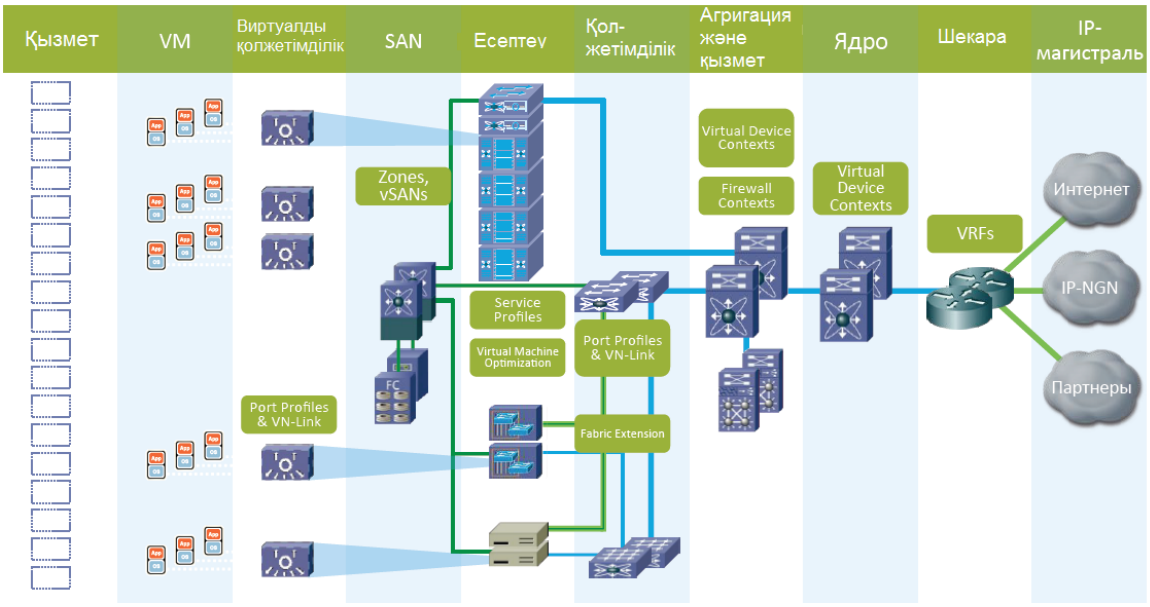
– Қауіп–қатерден сақтану. Желілерді ішкі дәне сыртқы қауіп–қатерден сақтандыру керек. Желінің инфаструктурасы мен бағдарламаларды мәлеметтерді жоғалтудан сақтау керек. Желілер мен бағдарламаларға жасалатын және де заманауи жасалатын шабуылдардан қорғау керек. Ол үшін қауіп–қатерді анализ және анықтайтын, операциялық жүйенің белгілерін пассивті түрде басқаратын, репутациясын анализдейтін және ортақ корреляциямен бірге басқарылатын, қауіпсіздіктің жоғары дәрежесін қамтамасыз ететін озық технологиялар қолданылады. Ішкі келесідей қауіп–қатерден сақтану қажет, домендік аттарға жасалынған ортақ шабуыл, наразы жұмысшылыр жағынан жасалынған порттар мен протоколдар.

– Жаңа технологиялар себебінен пайда болған проблемалар. Мысал ретінде өте көп көлемдегі адамдармен жұмыс жасау. Физикалық инфраструктурасын қоса алғанда, яғни серверлер, коммутаторлар, сақтаушы қоймалармен бірге әрбір бағдарламаға, бөлімше мен функцияға үлкен виртуалды және бұлттық орталарға арнайы логикалық бөлінділер қолданылады. Негізгі мақсаты әрбір қолданушы топты қорғалған виртуалды ортамен қамтамасыз етеді. Виртуалды орталар арасындағы мәлімет алмасуды қолданушылардың рұқсат беру құқығы арқылы басқарады.

– Айқындық. Ережені сақтап, виртуалдық және бұлттық мәлімет өңдеуші ортаның айқындығын сақтау маңызды шаруа болып табылады. Тапсырыс берушілер физикалық ортадағы ережелермен виртуалды ортада жұмыс істегісі келеді. Детальдік айқындық алдын ала ішкі, салалық және мемлекеттік стандарттың орындалу шарттарының негізі.

– Серверді виртуализацилау проблемасы. Бұл проблеманы VMware vMotion виртуалды машиналарды физикалық порттармен алдын ала берілген желілік саясатын сақтай отырып орынды шешеді. Администратор анализдеу қабілетіне ие бола отырып, желілік қауіпсіздік саясатын жергілікті байланыстағы трафикке қолдана алу қажет. Администратор функционалдық

міндеткерлікті сақтай отырып, бірмезгілде эксплуатация үздіксіздігін қамтамасыз ету керек.

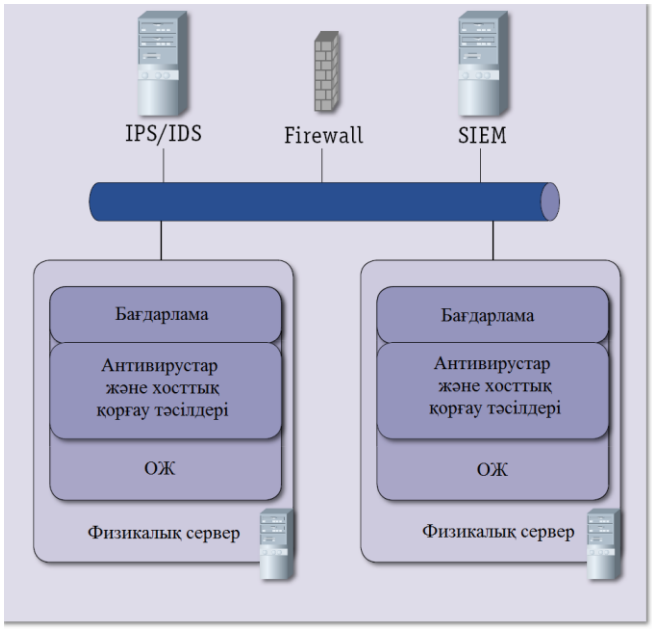


Сурет 1.6 – Виртуалды ортаның қауіпсіздік негіздері

Виртуалды ортаның қауіпсіздігін қамтамасыз етуде алғашқы орындардан Cisco көрінеді. Cisco – желілердің қауіпсіздігін сақтау аймағында ASA 5585–X мәлімет өңдеуші ортаның талаптарын қанағаттандыратын маштабтау қабілетін қолдайтын ең жоғары жылдамдықты желіаралық экранды ұсынады. 1.6–суретте виртуалды ортаның негізгі қауіпсіздік негіздері көрсетілген. Cisco архитектурасы қауіпсіздік қамтамасыз етуде өте икемді. Cisco VSG және ASA 1000V көмегімен виртуалды машиналар мен өте үлкен мөлшердегі қолданушыларды байланыстырады.

Физикалық ортада хосттың қауіпсіздігін сақтауға ешқандай шектеулер жоқ. Желілік трафик стандартты желілік құрылғымен филтірленуі мүмкін, соның арқасында зиянды кодтың енуін алдын–ала айқындау жүйесімен және контентті фильтірлеумен оқшаулайды.

Ал виртуалды ортада дәстүрлі қорғау тәсілдерін қолдану ешқашан мүмкін емес, оған қоса қауіпті. Мысалға, бірмезетте бірнеше виртуалды машиналардың қатты дискілерін антивирустың тексеруі құрылғыны айтарлықтай жүктеп қояды. Виртуалды ортаның ерекшеліктері мен осал тұстарына мән бере отырып, жаңа бұлттық есептеу тұсында ашылып жатқан өндірушілердің шешімдеріне жүгіне отырып шешуіміз қажет. Алдында айтып өткендей физикалық орта мен виртуалды ортаның қауіпсіздігін қорғағанда көптеген ерекшеліктер бар. Ал төменде 1.7–суретте қауіпсіздікті қамтамасыз ететін физикалық ортаның элементтері көрсетілген.



Сурет 1.7 – Физикалық ортаның элементтері

Виртуалды машиналар арасындағы желілік трафик физикалық серверден кетпейді, осыған байланысты дәстүрлі желілік әдістер қорғаныс бола алмайды. Оған қоса қосымша бағдарламалық қабат бар, оныда қоса қорғау қажет. Сол себепті виртуалды ортаның қауіпсіздігіне аса маңызды көңіл бөлу керек. Ол мәселені толығырақ қарастырамыз, бұл дипломның негізгі тереңірек зерттелетін тұсы болып табылады.

Сурет 1.8 – Виртуалдық ортаның элементтері

Стандартты қорғаныс әдістері кез–келген кезде виртуалды серверлерге қолданыла бермейді, бірақта виртуализация платформасының дамуы бұл кемшілігін оның артықшылығына айналғанын көрсетеді. Мысалға, VMware платформасы бұрыннан VWsafe интерфейс жиынтығын өзге құралдармен бірге жұмыс істеу мақсатында жасалған. Виртуалдық ортаның элементтері 1.8–суретте көрсетілген. Бұл дәрежедегі қауіпсіздікті жоғарлату үшін келесідей талаптар қажет:

– Антивирустық қорғаныс. Антивирустарға, яғни виртуалды серверлерде орнатылған олардың агенттеріне алдын ала толық тексеру күнтізбесін ұйымдастыру қажет. Себебі құрылғыны жүктеу қаупінен құтылу үшін. Егер мүмкін болса API көмегімен бірге гипервизермен интеграцияланған агентсіз антивизустардың виртуалды машиналарды және олардың дискілерін машина өшірулі тұрған сәтінде де тексере алу қабілеттілігін пайдалану. Оған қоса, ол құрылғының ресурстарына бәсекелестікті жояды.

– Сенімділік аймағына қарай витруалды машиналарды бөлу. Бәлкім бір физикалық серверде компанияның сыртқы веб–сервермен қоса ішкі бизнес–бағдарламасы болуы мүмкін. Бірақ бұл жағдайдада кем дегенде физикалық сервердің жайылу принциптерін сақтау қажет. Платформаның виртуализациясын қорғаудың жинақталған тәсілдерін ұсынатын Trend Micro, Reflex System атты өндірушілердің өнімдері сенімділік аймақтарына қарай әртүрлі машиналарды оқшаулауға, жеке профилдер мен қорғаныс саясатын жасауға және автоматтандырылған баптамаларды қолдануға мүмкіндік береді. Бұндай профиль машинаны басқа серверге ауыстырғанда ішкі желінің қателесіп сыртқы желіге қосылуының алдын алады.

– Өз уақытында бағдарламалық қамтаманы жаңартып, ақпараттық қауіпсіздікті периодты түрде сканерлеп және мониторингтен өткізіп отыру қажет.

– Қорғаныс құралдарын жаңарту. Физикалық серверлерге қарағанда виртуалды серверлерде машиналардың қосылуы, өшірілуі және клондалуы тезірек жүреді. Гипервизормен интеграция жасаған қорғаныс тәсілдерін қолданғанда виртуалды машиналардың атына кір келмейді.

1.5.1 Гипервизорға шабуылдар

Гипервизор виртуалды жүйенің негізгі элементтерінің бірі болып табылады. Оның негізгі қызметі виртуалды машиналар арасындағы қорларды бөлу болып табылады. Гипервизорға шабуылдың соңында бір виртуалды машина екіншінің жады мен қорларына қолжетімді бола алады. Сонымен қатар ол желілік трафикті, физикалық қорларды тартып алып, виртуалды машинаны серверден ығыстырып шығара алады. Қорғаныштың стандартты методтары ретінде виртуалды ортаға бейімделіп шығарылған бағдарламаларды, Active Directory каталогының қызметімен хост–сервер интеграциясын , хост–сервердің басқарушы құрылғыларына қолжетімділіктің стандартты процедураларын, виртуализация хостының кіріктірілген бранмауэрларын қолдану керек.

Сонымен қатар, жиі қолданылмайтын виртуализация серверіне веб–қолжетімділік секілді қызметтерді өшіріп қою дұрыс.

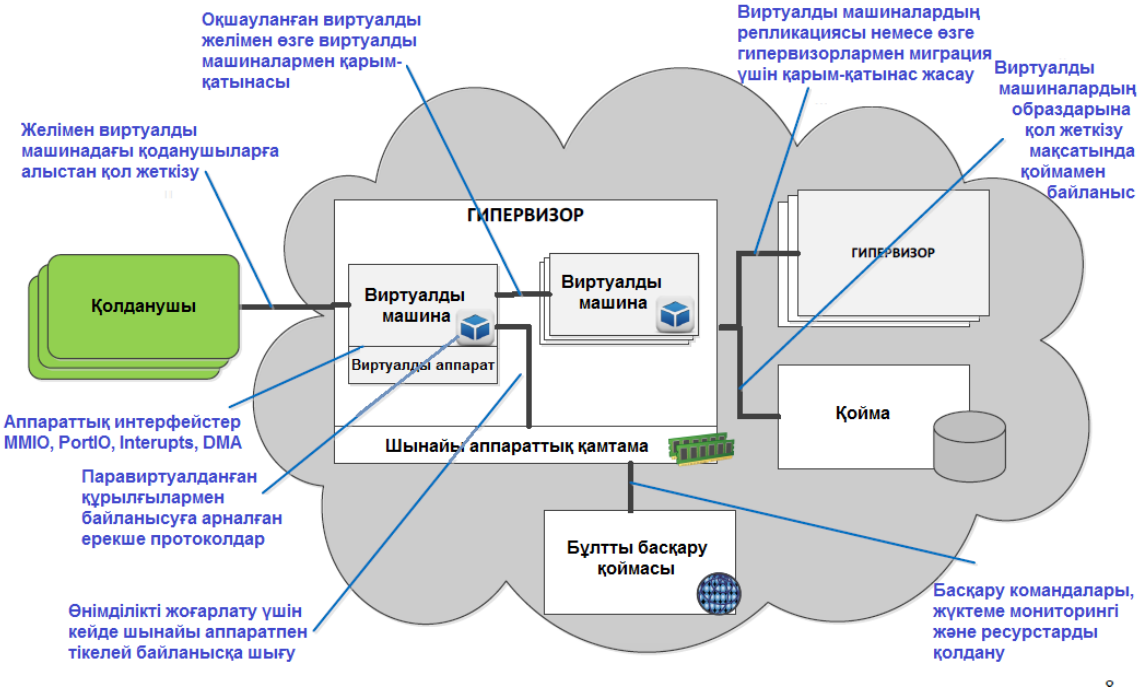
Буфердің лық толуы және еркін кодтардың өздігінен іске қосылуы гипервизердегі қателіктерді анықтауы мүмкін.

Гипервизердің негізгі қателіктері бір жағынан оларды пайдалану сырт жақтан болғанда виртуалды инфаструктураны басқару жағында болса, екінші жағынан виртуалды машина тұсынанда болуы мүмкін. Екінші жағдайда виртуалды машинаның сыртына шығып, кез–келген командаларды өз бетінше орындап кетуі мүмкін.

ESXi 4.0–5.0 және ESX 3.5–4.1 дегі VMX процессоры RPC командасын өңдеу барысында пайда болатын қателіктерге байланысты осал тұстары гипервайзердің жұмыс істеуіне кедергі келтіреді. Осыған ұқсас, алыстатылған қолданушы арнайы дайындалған пакеттерді ESXi 4.0–5.0 және ESX 3.5–4.1–ге жіберіп, буфердің лық толуына алып келтіре алады.

Виртуалды инфаструктураны басқару тұсына келетін шабуылдардың қауіп–қатерінен виртуализацияның жаңа қорғаныс әрекеттері гипервизорға келетін бүкіл трафикті филтірден өткізу арқылы қорғайды.

Виртуалды машиналар тұсынан келетін бұл секілді қауіптерден жаңа қорғаныс әрекеттерімен қауіпсіздігін сақтау қиынға түседі, бірақ конфигурация тұтастығын басқару құралы арқылы шабуылды әрекетсіздендіруге болады. Гипервизердің бұлттық есептеудегі рөлі 1.9–суретте көрсетілген.



Сурет 1.9 – Гипервизердің бұлттық есептеудегі атқаратын рөлі

Гипервизердің әлсіз тұстарының арқасында қонақ операциялық жүйенің виртуалды машинадағы жұмысын істеуін бұзып, қолданушылардың құқығын жоғарлатуға мүмкүндік алады. ESX/ESXi ортасында ондай шабуылдар

қарапайым екі жолмен іске асырылады. Олар VMware Tools осалдығын пайдалану арқылы немесе гипервизердегі қонақ операциялық жүйені орап өту арқылы виртуалды машинасының есте сақтау жадына тікелей қол жеткізе алады.

Осындай шабуылдардан құтылу үшін, ең алдымен VMware Tools–ты қолданудан бас тарту қажет, екіншіден физикалық компьютердегідей қонақ операциялық жүйеге рұқсат етілмеген кіруден классикалық түрде қорғау қажет.

1.5.2 Аутентификация

Қолданушылардың көпшілігі бұлттарға қосылу үшін браузерлерді қолданады. Бұл жерде Cross Site Scripting сияқты шабуыл түрлері қарастырылады. Яғни, парольды «ұрлау», веб–сессияны қағып әкету, «ортадағы адам» және т.б. Бұдан қорғанудың жалғыз жолы дұрыс аутентификация және өзара аутентификацияланған шифрланған қосылысты (SSL) қолдану. Дегенмен, бұл қорғану шаралары айтарлықтай ыңғайлы емес және бұлтты жасайтын адамдар үшін ысырап болып келеді. Информациондық қауіпсіздіктің бұл саласында әлі шешілмеген тапсырмалар бар. Бұлттық есептеудің дамуымен бірге жетіле түседі.

Аутентификация – парольмен қорғау. Жоғары сенімділікті қамтамасыз ету үшін токен немесе сертификаттардың көмегіне жүгінеді. Пайдаланушы аутентификациясы негізінен мына екі үлгінің бірінің негізінде іске асырылады: қарапайым PIN–аутентификация және қорғалған PIN–аутентификация. Бұл екі үлгіде пайдаланушының PIN–кодын эталонмен салыстыру арқылы пайдаланушының жалғандығын тексереді.

Қарапайым PIN–аутентификация кезінде PIN–кодын келтке (смар–карта) жай ғана жібереді, кілт оны өз жадысында сақталатын эталонмен салыстырады және ары қарай не істейтіндігі жөнінде шешім қабылдайды.

Қорғалған аутентификация процесі келесі үлгі бойынша іске асырылады:

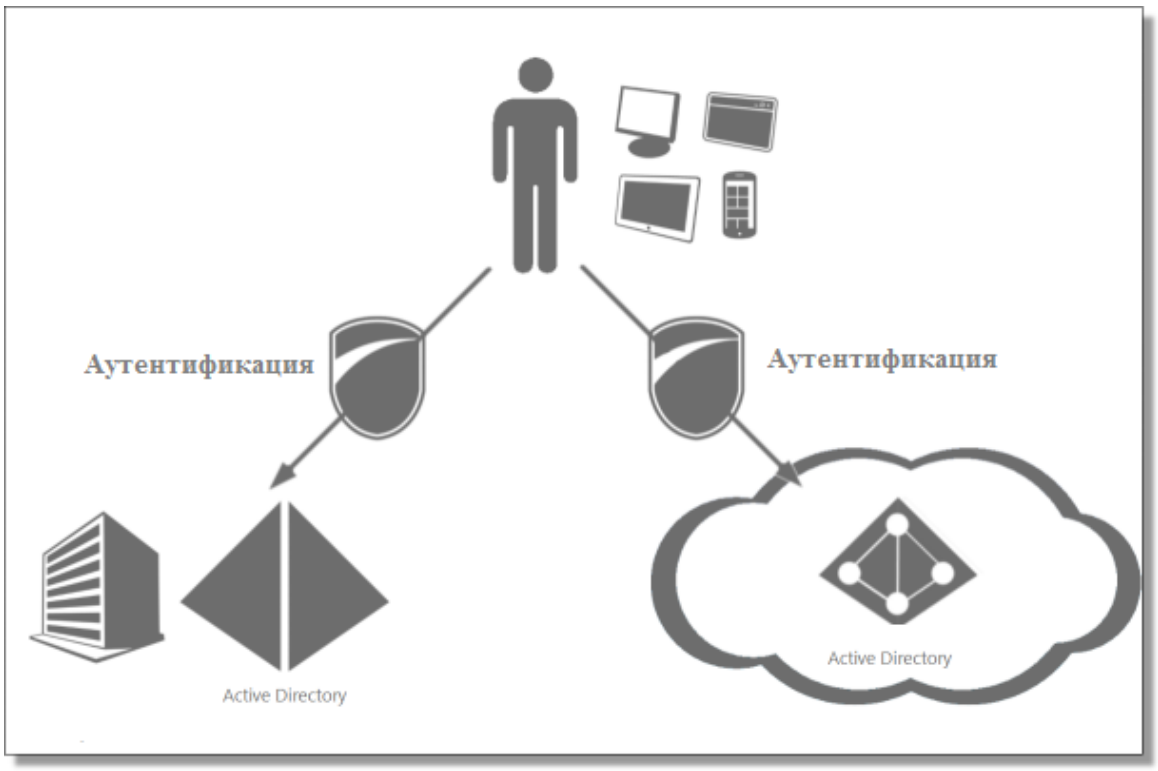
– қорғалған қосымшалар кілтке (смарт–карта) PIN–аутентификация үшін сұраныс жібереді;

– кілт (смарт–карта) кезкелген 64–разрядтық сандарды қайтарады;

– қосымша кілттің иесі енгізген PIN–кодты қабылдайды да оны DES–алгоритмі бойынша шифрлейді, нәтижесін кілтке жібереді;

– кілт жіберілген мәліметтерді өңдеуді іске асырады және өзінінің жадысындағымен салыстырады.

1.10–суреттен аутентификациядан өту сұлбасын көре аласыздар.



Сурет 1.10 – Аутентификациядан өту сұлбасы

Сәйкес болған жағдайда аутентификация сәтті өтті деп есептеледі және пайдаланушы ары қарай жұмысын жалғастыра берсе болады.

Провайдердің идентификация жүйесімен өзара қызметінің мөлдірлігі үшін авторизация кезінде LDAP (Lightweight Directory Access Protocol) және SAML (Security Assertion Markup Language) қолданған жөн.

1.6 Периметрді қорғау және желіге шек қою

Бұлттық есептеуді қолданған кезде желінің периметрі шайылып немесе жойылып кетеді. Бұл өте аз қорғалған желі бөлігінің қорғанысы, яғни жалпы қорғаныстың деңгейін көрсетеді. Виртуалды машиналар бұлттағы әр түрлі деңгейдегі сенімділікке байланысты сегменттерді шектеуі керек. Олар желілік периметрлерді виртуалды машинаның өзіне ауыстырып, өздерін қорғанышпен қамтамасыз етуі керек. Корпоравтивтік firewall – IT қауіпсіздіктің саясаты мен желі сегменттерін шектеуде қолданылатын негізгі компонент. Ол бұлтты ортада орналасқан серверлерге әсер ете алмайды.

Желі периметрлерін қорғау үшін желіні жоғары сапада және толық қорғауды іске асыратын арнайы құралдар мен әдістерді таңдау қажет. Таңдау Майкрософт компаниясының өнімдеріне келіп тоқтады. Желіні қорғауда Майкрософт компаниясының серверлік өнімдері мен желіні қорғау программалары тиімді болып табылады.

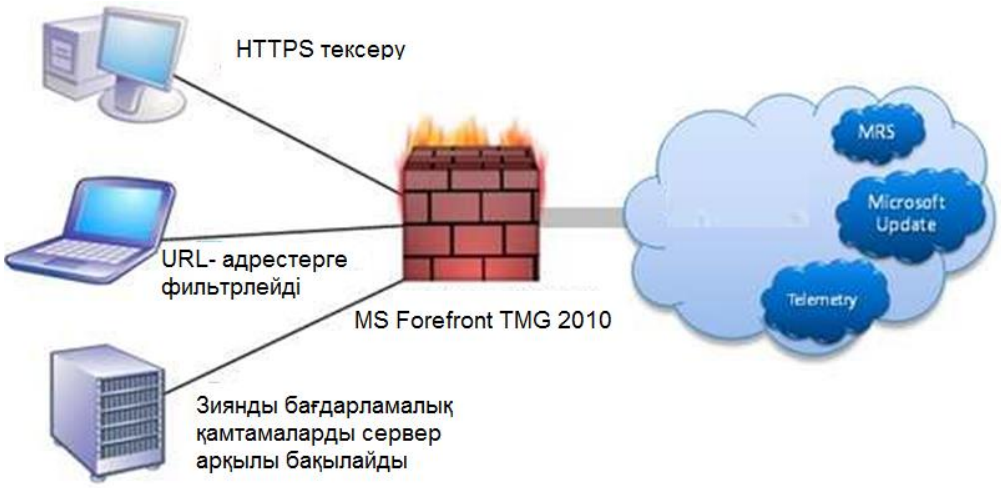
Біз көбіне ғаламдық желіде хакингтік шабуылдарға тап болып жатамыз. Microsoft Forefront өнімдерін ақпаратты кешенді қорғауды және ғаламдық

желіде пайда болып тұратын жаңа қауіптерді алдын ала отырып, операциялық жүйелер мен серверлерге қол жетерлікті басқаруды қамтамасыз етеді. Қауіпсіздікті қамтамасыз ететін жеке өнім ретінде таралған көптеген құралдар бар.

Microsoft Forefront желілік инфроқұрылымынды қорғанысты және қауіпсіздік жүйесін басқаруға мүмкіндік жасайды. Жеңілдетілген басқару, анализ жасау, есеп берулерді құру процесстер арқасында администраторлар ақпараттық ресурстарын тиімді қорғайды және қосымшалар мен серверлерге оңай қол жеткізе алады. Программаны жиі жаңартып отыру жаңадан туындайтын қауіптермен күресуге және бизнестің өсіп келе жатқан сұраныстарын қанағаттандыруға көмектеседі.

Microsoft Forefront Threat Management Gateway 2010 – қызметкерлерді Интернеттегі қауіптерден қорғайтын желі периметрі үшін кешенді қорғау жүйесі. Жергілікті желіні ғаламдық желіден келетін қауіптерден қорғауды ұйымдастырады және жергілікті желі пайдаланушыларын Интернет ресурстарына қол жетерлігін анықтауға мүмкіндік жасайды[4].

Forefront TMG (1.11–сурет) трафиктерді есептеу, жиі пайдаланылатын ресурстарды анализ жасау құралдарымен қамтылған. Аутентификация мен тіркелудің түрлерін иемденеді және Active Directory аутентификациясын қолдайды. Қорғалған VPN–туннель құруды қолдайды және қашықта орналасқан қызметкердің желіге қосылуына мүмкіндік жасайды. Forefront TMG сервері URL–фильтрлеуді жүзеге асырады, желілік экран құрады, қауіпті программалық қамтамаларды анықтайды, сонымен қатар HTTP/HTTPS, FTP трафиктеріне анализ жасайды. Forefront TMG Web Protection Service қызметі антивирустық базаға және зиянды URL–адрестерге онлайн жаңартуды іске асырады.



Сурет 1.11 – Microsoft Forefront Threat Management Gateway 2010 жүйесінің жұмыс істеу принципі

Flood – шабуылдарға кеңейтілген тұрақтылық пен оларды бақылау қызмет етуді тоқтату типіндегі кең таралған қарапайым шабуылдарға қарсы тұруды қамтамасыз етеді. Шабуылдарға қарсы кеңейтілген мүмкіндіктер хабарлау мен қарсы тұруды құрудың әмбебап құралдардын пайдалана отырып, желі администраторының желідегі қауіптерді жылдам анықтауға мүмкіндік жасайды.

Forefront TMG программалық жүйесін басқарудың қарапайым қолданылуы мен оқылуы, оны орнату мен ұйымдастыруды іске асыруды жеңілдетеді.

Көп деңгейлі тексеру, жан–жақты икемді саясат, протоколдардың орнатылатын фильтрлері және желі арасындағы маршруттау қатынасы Интернет арқылы келіп түсетін қауіптерді анықтауға арналған.

Ұйым Forefront TMG 2010 қауіпсіздік қамтамасыз етуге және желінің жіберу мүмкіндіктерін қолдануға пайдалануға болады. Бұл, филиалдарды ғаламдық желі ресурстарын пайдалану кезінде енетін қауіптерден қорғаудың зор мүмкіндіктерін көрсетеді. Корпоративтік саясаттың жылдам таралуы, серверлерді аз пайдалану мен желінің жіберу мүмкіндігінің төмендігін қолайлы ету тиімді басқаруды қамтамасыз етеді. HTTP трафигі қысу мен кэштеу пайдаланушылар үшін WAN арналарының құнын төмендетеді. Желіаралық экрандарды қауіпсіз алыстан басқару мүмкіндігі желідегі веб кештеу мүмкіндіктерін сапалы атқаруға жағдай жасайды.

1.6.1 Демилитариленген жергілікті желі

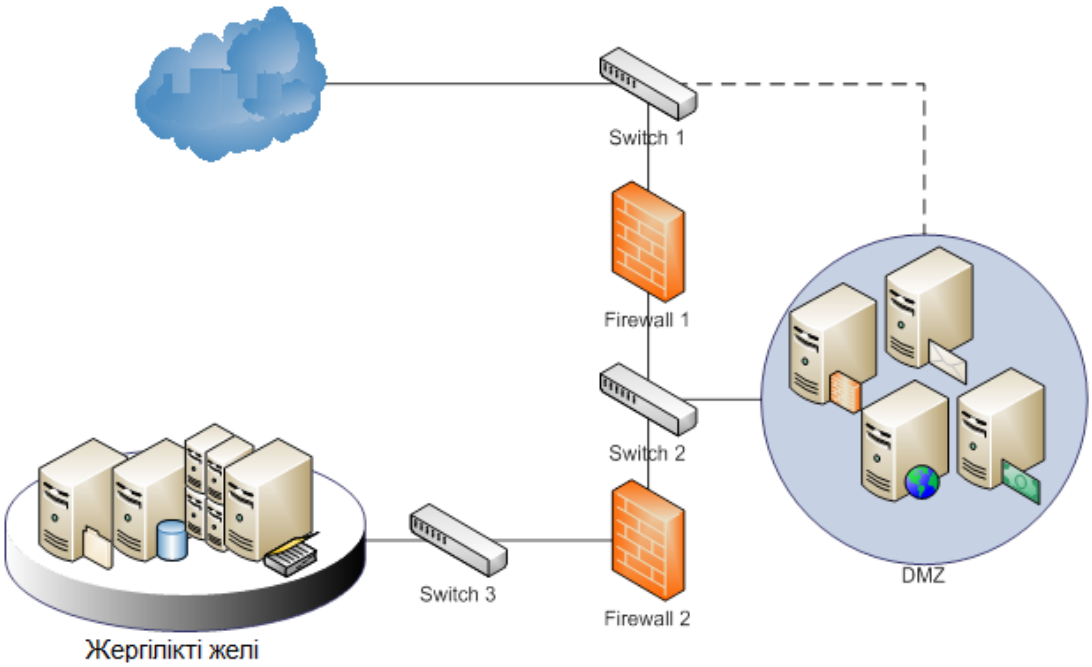
Demilitarized zone (DMZ) – бұл оқшаулаған желі (немесе желілер 1.12–суретте көрсетілген), ол әдетте сыртқы желіден пайдаланушыға қол жетімді. Firewall солайша конфигурациялануы керек, сыртқы аймақтан ішкі немесе демилитариленген аймаққа енуге қамтамасыз ету үшін. Демилитариленген аймаққа ену үшін рұқсат жасау компанияға ақпаратты беретін компанияға және қызмет етушілерге сыртқы пайдаланушыларды ену қауіпсіздігін ұйымдастыруға мүмкіндік береді. Осылайша, бұл аймақ олардың қауіпсіз ішкі аймаққа енуінсіз сыртқы пайдаланушылармен жұмыс істеуге мүмкіндік береді.

Көптеген ұйымдар өзінің желілерінде демилитариленген зонаны, DMZ пайдаланбайды. Олар мұның орнына сол ішкі желідегі (мысалы, Web–серверлерді) онда компанияның серверлері мен жұмыс станциялары болады. Ішкі желіден жалпы қол жетімді серверлер DMZ болмаған жағдайда, соңғыны қосымша қатерге душар етеді. Шабуылдаушы Web–серверлермен басқаруға мүмкіншілік алған кезде, ол оны маңызды қорларға шабуыл үшін пайдалана алады, айталық қаржылық айқындауыш және файлдық серверлер сияқтылар бұл арада “қашан”, ал “егер” емес. Сондықтан неден болса да тәуелсіз болатын сол, Web–серверлер қорғалған сияқты, ерте ме кеш пе ол шабуылға душар болады. Демек, желі мен жұмысшы процесстерді енуден зиянды ең кіші болатынын ескеріп жобалау қажет және олардың тез қайта қалпына келуін

кепілдеу керек. Мұндай стратегиялардың бірі жұмысшы зонасын бөлу стратегиясы және демилитариленген зонаны (DMZ) пайдалану.

DMZ–нің негізгі тағайындалуы – желінің сыну салдарын барынша кішірейту (желіні сындырудың жалғыз әдісі – жабдықты сындыру), осы кезде сындырушы DMZ серверлеріне бақылау (толық немесе ішінара) алады, бірақ ішкі серверлерге немесе жұмысшы станцияларға ене алмайды (оның енуі ішкі файэрволды шектейді).

DMZ–ның шешуші ерекшеліктерінің бірі ішкі файэрволде тек трафикті сүзу ғана емес, мұнымен қатар DMZ мен ішкі желінің белсенді жабдықтары мен арасындағы өзара әрекеттесу кезінде күшті міндетті криптографияның талап етілуі. Атап айтқанда болмайтын ситуация сол, онда авторизацияланбай ақ DMZ–да серверден алған сұранысты өңдеу мүмкін. Егер өзінің ішінен периметр ішіндегі шығып кетуден ақпаратты қорғауды қамтамассыз ету үшін пайдаланылатын болған жағдайда,ішкі желіден пайдаланушылардың сұраныстарын өңдеу үшін ұқсас талаптар.



Сурет 1.12 – Демилитариленген аймақ

DMZ қалыптасқан кезде желінің екі физикалық бөлінуі жасалады: бірі – жалпы қолжетімді серверлер үшін, басқасы – ішкі серверлер мен жұмысшы станциялар үшін. DMZ типімен пайдаланылатын брандмауэрлердің санынан тәуелділікте, желілердің әрқайсысы үшін сол немесе басқа маршрутизация политикасы қолданылады және олардың арасындағы ену қатаң бақыланады:

– Internet және DMZ;
– Internet және ішкі желімен;
– DMZ және ішкі желімен.

Жай брандмауэрдің орнына DMZ–ны пайдаланудың басты айырмашылығы сонда, жалпы қол жетімді серверлерге шабуыл кезінде ішкі серверлердің компрементациясының тәуекелі төмендейді өйткені жалпы қол жетімді және ішкі серверлер бірінен–бірі ажыратылған. Егер скомпроментирленген серверлер DMZ да болса, қаскөй ішкі желіде орналасқан, аса маңыздылау серверлерді, басқаларды тура шабуылдай алмайды. Брандмауэр арнайы рұқсат етілген қосылудан басқа компьютердің ішкі желісіне қосылатын DMZ ішіндегі компьютерлердің кез келген ұмтылысын шектейді. Мысалы, брандмауэрді солай орналастыруға болады, ол Web–серверге рұқсат ететіндей, және DMZ ішінде болатындай арнайы TCP–порт арқылы Microsoft SQL ішкі желісіне қосылады. Егер Web–серверді қармап алса, ол осы порт арқылы сол сервер жүйеге шабуылды ұйымдастыруға болады. Бірақ та қаскөй басқа қызметтер мен SQL Server порттарын ішкі желінің басқа компьютерлерінде шабуылдай алмайды.

1.7 Желіаралық экрандар

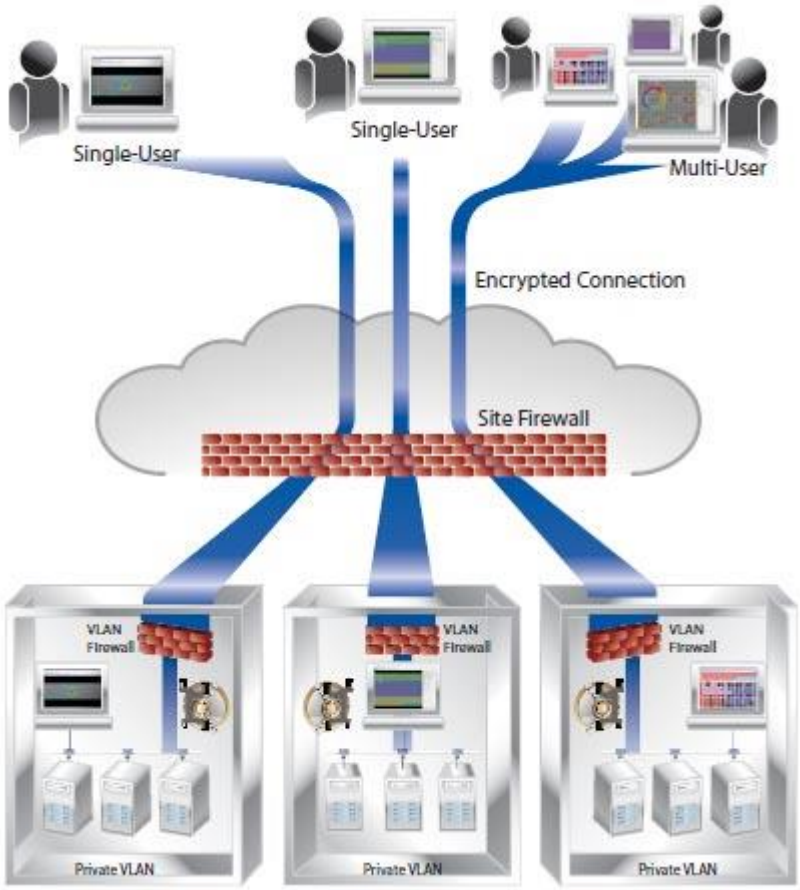
Біріккен желілер (Internet work) термині деп біріне бірі қосылған көптеген желілерді түсінеді. Біріккен желілерде арнайы аймақтар жасалады, олардың әр–қайсы белгілі ақпаратты өңдеу және сақтау үшін тағайындалған. Олардың қауіпсіздігін қамтамасыз ету мақсатымен бұл аймақтарды ажырата бөлу үшін арнайы құрылғыларды пайдаланады, оларды Firewall деп атайды, немесе желіарлық экрандар дейді. Firewall–лар жабық желілерді және жалпы пайдаланудағы желілерді бөлу үшін тағайындалған дегендей пікірлер бар, әйтседе бұд әркез бұлай бола бермейді. Firewall–ларды жабық желілердің сегменттерін шектеу үшін де айтарлық жиі қолданады.

Firewall түсінігі «маршрутизатор немесе ену сервері (бір немесе бернеше) ретінде анықталған, ол жабық желілермен ашық желілер арасында қорғаушы экран ролін анықтайды. Firewall–маршрутизаторды жабық желілердің қорғаудың басқа құралы және ену тізбесі түрінде қолданады».

Әдетте Firewall–ларды алдын ала ескерілгені сол, ол ең аз дегенде, үш интерфейстің бұрынырақтағы пайдалануында екі іске асады. Осы себеп бойынша, дағды болып кеткенге орай қазіргі кезде Firewall–ларда негізінен үшеуден небәрі екі интерфейс пайдаланылады. 1.13–суретте олардың жұмыс істеу принципі көрсетілген. Мұндай жағдайда, үш қалыптасқан интерфейсі бар Firewall пайдалынған кезде, бөлінген үш желілік аймақты жасау мүмкіншілігі бар. Бұл аймақтардың арқайсысы төменде қысқаша баяндалған.

– Ішкі (inside) аймақ, жабық аймақ құрылғысының жұмысы үшін тағайындалған және оны біріккен желілердің сенімді аймағы болады. Бұл құрылғылар сыртқы желілермен жұмыс істеген кезде (мысалы, Internet–пен) қауіпсіздіктің белгілі саясатына бағынады. Алайда іс жүзінде Firewall сенімді аймақтың сегмент бөліктерін ажырату үшін айтарлықтай жиі пайдалынады. Мысалы, Firewall–ды жалпы желіден кәсіпорынның қандай да бір бөлімшесінен желіні бөлу үшін пайдалануға болады[5].

– Біріккен желінің сыртқы (outside) аймағы сенімсіздігі төмен аймақ болып келеді. Firewall–дың негізгі қызметі сыртқы аймақта болатын, құрылғыдан ішкі құрылғылар мен демилитариленген аймақтарды қорғау. Мұнан басқа, қажет болған жағдайда Firewall демилитариленген аймақта болатын, құрылғыларға сыртқы аймақтан қауіпсіз таңдаулы ену үшін бағытталған бола алады. Аса қажет болған жағдайда Firewall ішкі аймаққа сыртқы аймақтан енуді қамтамасыз ету үшін бағытталған болады. Бірақ та бұл әрекеттерге ерекше жағдайларда ғана баруға болады, өйткені сыртқы аймақтан ішкі аймаққа ену едәуір қауіп қатер көрсете алады, ал мұндай ену демилитариленген шектелген аймаққа енуден көрі кемшімдеу келеді.



Сурет 1.13 – Firewall жұмыс істеу қызметі

Желіаралық экрандар желілік инфраструктураның қауіпсіздігін қамтамасыз ету тұрғысынан ұзақ уақыт бойы бірінші орынды алып келеді. Олар желіге тұтынушылардың қосылу жөніндегі информациясын желіге қолжетімділіктің қолжетімділікке сұраныс берген әрбір тұтынушының корпоративті саясатымен салыстырып, мәліметке кіруге рұқсат береді. Тұтынушылардың саясаты мен қосылыс жөніндегі информация сәйкес келуі керек, немесе брандмауэр желілік қорға кіруге рұқсат бермейді. Бұл бұзудың алдын алуға көмектеседі. Яғни желіаралық экранның жұмыс істеу принципі мен атқаратын қызметінің маңыздылығын байқағандай, оған зор көңіл бөлу керек.

Бұлттық есептеудің түріне байланысты қорғаныстың масштабтығын таңдаймыз. Соған байланысты қызметін ұсынушы өндіруші компаниялардың өнімдерін таңдаймыз.

1.7.1 Қолжетімділіктің барлық нүктелерін қорғаудың негізі

Мемлекеттік жеке желі шекарасы көп бұзылуға әлі де әлсіз болып есептеледі, себебі Интернет жалпыға қолжетімді желі және бірнеше желілік операторлардың басқаруына ұшырайды. Сол себепті, Интернет сенімсіз желі болып есептеледі.

Ол бұрынғыша LAN–WAN шекараларын қорғайтын шешуші қорғаныш. Ішкі желідегі қызметкерлер желі мен қор мәліметіне қолжетімділік болмауы үшін, желілік бранмауэрлар желінің ішкі сегменттерімен байланыста болу керек. Корпоративті желіні брандмауэрлармен бөлгенде организация ішіндегі бөлімдер басқа мекемеден келетін қауіпке қарсы қосымша қауіпсіздендірілуі керек.

Сонымен қоса, желіні қолдану жылдан жылға өсіп келеді, қызметкерлер географиялық тұрғыдан филиалдарға бөлінгендіктен, әр түрлі мобильді құрылғылар мен алыстатылған желіні қолданады. Бизнес технологияға сандық тұрғыдан әсерге бағытталған Nemertes Research фирмасының мәліметіне қарағанда енді қызметкерлердің 90 пайызы филиал офистарында жұмыс істейтін болады. Нәтижесінде, әрбір филиалдық шекарада демилитаризделген аймақ болады. Ол жерде WAN қолжетімділік маршрутизаторы интернет пен басқа да ғаламдық желіге қолжетімділікті күтіп алады. Бұл шекара да қорғалған болуы тиіс.

Қауіпсіздіктің бірінші жолында тұрған брандмауэр желінің келесі сегменттерінде орын алады:

– периметрдің дәстүрлі корпоративті желісінде (МӨО WAN мен Интернет үшін жауап беретін жерде);

– қолданушылар тобындағы саясатқа байланысты мекемелердің арасындағы бөлінген қолжетімдікте;

– веб және корпоративті LAN коммутатор порттарында, мәлімет өңдеу орталығындағы бағдарламалар мен сәліметтер серверында;

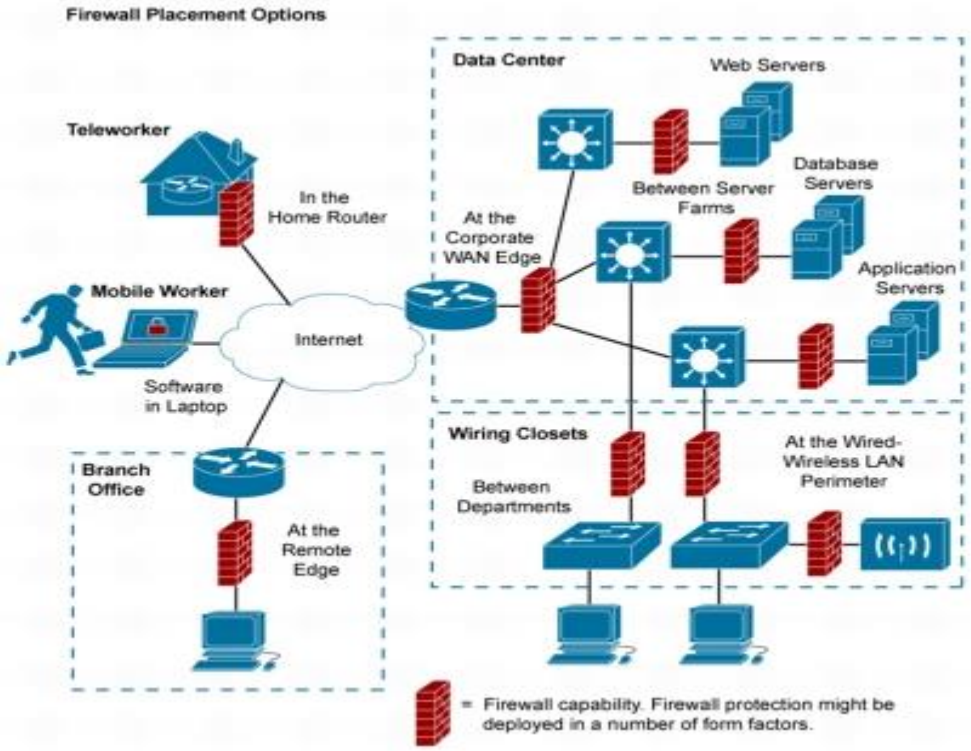
– сымды локальды есептеу желісі мен сымсыз локальды желі сәйкес келгенде (Ethernet LAN коммутаторлар мен сымсыз локальды желі бақылаушылары арасында);

– филиал байланысындағы WAN шекарасында;

– корпоративті мәліметтерді сақтайтын мобильды немесе алыстатылған қызметкерлер болған жағдайда ноутбук, смартфон және әр түрлі интеллектуалды мобильды қондырғыларда.

1.14–суретте бүкіл мекемеде орналасқан желіаралық экрандардың конфигурациясы көрсетілген. Бұл суретте желіаралық экрандардың нақты қолданылуына тәуелді орындарын ерекшелеп көрсеткен. Себебі шеттен тыс әрі дұрыс бапталмаған желіаралық экрандар желі арқылы байланысту қиындатып,

кей жағдайларда ішкі жанжалдарға душар етеді. Бұл жағдайда корпоративті желінің барлығында әрбір шекарада негізгі брандмауэр фильтрациясын жүргізу ұсынылады. Әрі бұл ұсыныс өзінің икемділігін қорғаныс дәрежесімен дәлелдеді[6].



Сурет 1.14 – Корпоративті желінің барлығында әрбір шекарада негізгі брандмауэр фильтрациясын жүргізу ұсынылады

1.7.2 Cisco ASA 5500 көп функционалды желіні қорғау құрылғысы

ASA 5500 Series жүйесі техникалық жағынан Cisco–ның PIX Security Appliance, IPS 4200 Series және VPN 3000 Concentrator сияқты құраушыларында болатын қуатты қорғаныс құралдарына сүйенеді. Осыған байланысты тапсырыс берушіге VPN қызметінің кең тізімін ұсынады. Сондай–ақ олар IPSec және SSL VPN технологияларның қолданумен дистанционды қорғалған қолжеткізуді қамтамассыз етеді. Сонымен қатар, ең маңызды телекоммуникациялық байланысты демеу арқасында ASA 5500 Series өнім сериялары интеграциялау және кәдімгі трафик пен бизнес қосымшасына залал келтірмей–ақ бар желілік құрылымға қондырылу мүмкіндігіне ие екенін атап айтқан жөн.

Негізгі қолданылу аймағы:

– кіші және орта бизнес пен ірі корпорациялар үшін арналған;

– интегриленген сервистердің масштабталуы мен оларды унифицирленген басқаруын қамтамасыз ету үшін арналған;

– көптеген қорғаныс механизмдерін падалану процесінің еш бір қиындықсыз жұмыс істеуіне, сонымен қатар жоғары өндірістігіне кепілдік береді;

– желілік және қосымша трафикті басқарады;

– жеке виртуалды желі арқылы сенімді байланысты қамтамассыз етеді;

– меншіктің бағасын төмендетеді.

Сурет 1.15 – Cisco ASA 5500 көп функционалды желіні қорғау құрылғысы

Қазіргі кезде желілермен қорғаныс құралдарынсыз жұмыс істеу қиынға соғады, сондықтан Cisco Systems компаниясы қазіргі таңдағы желілерді ішкі және сыртқы қауіптен қорғаудың ең озық шешімін ұсынады – ASA 5500(1.15–сурет). Осы класстағы қорғаныс құрылғылардың түрлі модельдері түрлі масштабтағы инфрақұрылым үшін жобаланған (шағын офистерден бастап ірі корпорацияларға дейін).

CISCO ASA–ның негізгі мінездемесі мен мүмкіншіліктері:

– Cisco Adaptive Securiti Device Manager көмегімен басқару;

– бұрыс жауапқа тұрақтылық конфигурациясын демеу (Active/Standby и Active/Active);

– Risk Rating,Meta Event Generator дабылды басқару механизмдерін демеу;

– OSPF,PIM,Ipv6,QoS демеу;

– мөлдір және виртуалды МСЭ демеу;

– хаттамалар мен қосымшаларды бақылау (Web,e–mail,FTP дыбыс және мультимедия, СУБД, GTR/GPRS,ISQ,P2P операциялық жүйелері және т.б.);

– «буфердің шектен тыс толуы» шабуылынан қорғау, RFC–тың бұзылуы, аномалиялар;

– SSL және IPSec VPN ұйымдастыру;

– HTTP,FTP,SMTP және POP3 протоколдарында вирустар, құрттар және зиянды программаларға төтеп беру;

– Syslog to ACL Correlation механизмі;

– басқарылатын интерфейс саны – 8 дейін.

Cisco Self–Defending Network (SDN) қорғаныс стратегиясының басты құраушысы – Cisco ASA 5500 үш модельден тұрады: ASA 5510, 5520 және 5540 (мінездемесі төменгі кестеде көрсетілген), сонымен қатар түрлі масштабтағы инфрақұрылым үшін арналған (шағын офистерден бастап ірі корпорацияларға дейін). Алайда оның арзандығы мен бір құрылғыда бірнеше кілтті қызметтердің

шоғырлануына байланысты олар SMB секторындағы компаниялардың аса қызығушылығын тудырады[7].

Cisco ASA 5500 Series–тың негізгі техникалық артықшылығы – түрлі қауіп алдында қорғану деңгейінің жоғарлауы, және офистердің өзара қорғалған әрекеттестік құру мүмкіншілігі. Cisco AIM–нің кеңейтіліп жатқан архетиктурасы мен Cisco ASA 5500 Series ұяшығының мультипроцессорлық архитектурасы бір мезгілде жұмыс атқарып жатқан қорғаныс механизмдердің жоғарғы өндіргіштігін қамтамассыз етеді. Cisco ASA 5500 Series–тің әр платформасы өз ішіне қоса жұмыс істейтін бірнеше өндірістік процесстерді біріктіреді. Олар өз кезегінде қосымшалардың корғанысын, белгісіз шабуылдардан қорғалуын, масштабталған IPSec/SSL VPN қызметін және т.б. қамтамассыз етеді. Енуді болдырмау және кеңейтілген қорғаныс қызметі сияқты ұсыныстар қарастырылған. Ол үшін Cisco ASA 5500 Series құрылғысында адаптивті тексеру мен AIP–SSM шабуылды болдырмау модульдері орнатылады. Осының арқасында Cisco ASA 5500 Series құрылғылары жылдам дамитын қауіп ортасында қорғанысты қамтамасыз ете отырып, оңай адаптивтену қасиетіне ие болады.

Cisco ASA 5500 Series жүйесі Adaptive Threat Defense атымен танымал шабуылдан қорғайтын дамыған адаптивті механизімін ұсынады. Оның құрамына белгісіз қауіптен қорғау құрылғысы (Anti–X), бизнес қосымшасының қорғау әдісі (Application security) және желіні бақылау мен қорғау технологиясы (Network containment and control) жатады. Олар кәсіпорынды көптеген заңсыз әрекеттерден толық және унифицирленген қорғанысқа кепілдік береді. ASA 5500 Series жүйесі трафик құпиялығын қамтамассыз ететін механизмдер жиынтығын ұсынады. Олар IPSec пен SSL хаттамаларын қолдануға негізделген және адаптивті қорғану технологиясымен біріктірілген. Cisco ASA 5500 Series құрылғыларындығы IPSec және SSL Frame Relay қосылысы олардың Frame Relay–ның кез келген сценариіне бейімденуге жол ашады. Біріккен құрылым және бақыланатын инфрақұрылым көмегімен кез–келген пайдаланушы үшін жоғарғы дәрежедегі алшақтанған енуді қамтамассыз етуге болады. Cisco ASA 5500 Series құрылғыларының Cisco VPN3000 кластэрлерімен бірігуі тапсырыс берушілерге оларда бар Frame Relay құрылымын пайдалануға мүмкіндік ашады.

Cisco ASA 5500 Series 7.1 версиясы көмегімен ASA 5500 Series–ның әрбір құрылғысы SSL VPN–ның бірмезеттегі 5000–ға дейінгі сессиясын қадағалайды. Осылайша кез–келген көлемдегі ұйым өз қызметшілеріне әлемнің кез–келген нүктесінен жүйеге жеңіл әрі қорғалған енуді қамтамассыз ете алады. VPN жүктемесін қадағалау функциясы IPSec VPN–ның кең масштабты функционалдығы – мыңдаған пайдаланушылардың бір мезеттегі жұмысын қадағалауға керекті құрылғылар санын азайтуға мүмкіндік береді. Сонымен қатар түрлі типтегі VPN функцияларын қадағалауға керекті платформалар санын азайтады. ASA 5500 Series 7.1–да SSL VPN желілеріндегі контентті жеткізу механизімі жетілген. Web–контент пен Web–парағының трансформациясының қуатты функциялары пайда болған. Қосымшалардың

өндірістігін оңтайландыру, түрлі браузерлерді қадағалау мен оңтайландырылған пайдаланушылар порталы ұйымдағы қызметшілер үшін корпоративті ресурстарға оңай қол жеткізуге жол ашады.

Cisco SSL Frame Relay–ның барлық платформаларында Cisco Secure Desktop функциясы жүзеге асырылды. Ол желіге қосылып баратын әрбір құрылғының автоматты түрде қорғаныс жүйесі жағдайын тексереді. Бұл операция үшін байланыс сеансының соңында компьютерді «тазалап», құпия деректерді сақтайтын «қауіпсіз виртуалды машина» құрылады.

Функционалдықпен қатар Cisco ASA 5500 Series жүйесі бірқатарлы экономикалық және пайдаланушылық артықшылықтарға ие. Оған кіретіндер аппараттық модульдер мен БЖ есебінен сервисін өсіру, түрлі объектілерде платформаларды қалыптастыру және ыңғайланған іздеу процессі мен ақаусыздықты жою. Басқа сөзбен айтқанда, сол міндеттерді орындау үшін көптеген платформалар мен басқару жүйелері қажет етілетін. Бұндай адаптивті көзқарас – «бір құрылғы – көптеген тағайындау» – платформалардың санын азайтады. Бұл мән–жай мониторингті, техникалық қызметті, қауіпсіздік қызметінің оқытуын жеңілдетеді.

Cisco ASA 5500–де қолжетімді унифицирленген басқару қызметерінің көбісі Adaptive Security Device Manager арқылы жүзеге асады. Оның көмегімен бір құрылғыны басқаруға болады және Cisco Security Management Suite арқылы – бірнеше құрылғыны басқаруға болады.

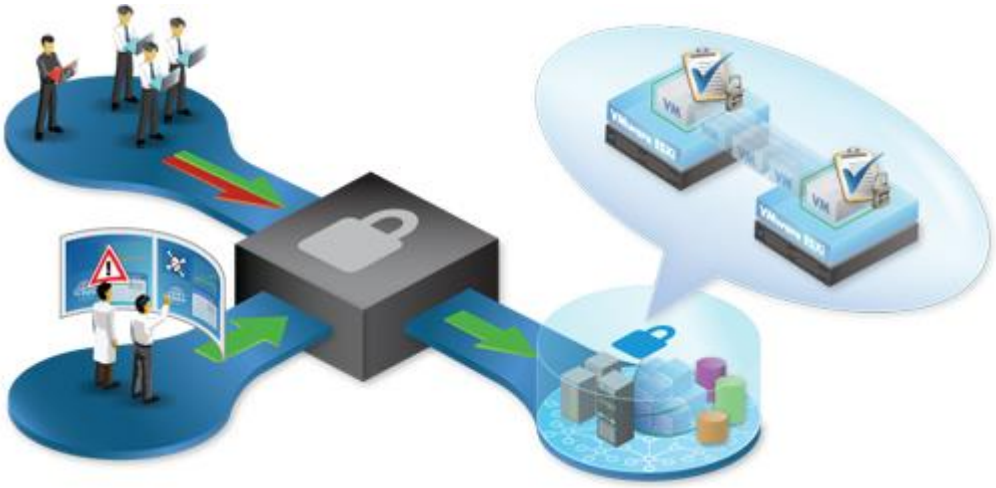
1.8 Желілік мәлімет өңдеуші ортаның қауіпсіздігі

Корпаративтік мәлімет өңдеуші орталарда орналасқан ресурстар, бағдарламалар және мәлеметтер көбіне қастық ойлаушылардың желілік шабуылының астында қалады. Есептеу жүйесінің құрамындағы ақпаратты жүйеге енгізуге және ақпаратты жүйеден шығаруға арналған құрылғылар, мысалға мәлемет өңдеуші орталардың серверлері қастандық ойлаушыларға «жылтық сыр бөлігі» болып табылады. Сол себепті сенімді қорғауға мәжбүр болады. 1.16–суретте желілік мәлімет өңдеуші ортаның қауіпсіздігінің сұлбасы көрсетілген.

Топтық серверге қарсы жасалған шабуылдар коммерциялық электронды бағдарламалардың және B2B типіндегі бағадарламалардың жұмыс істеу қызметінің бұзылуына алып келсе, оған қоса құпия ақпараттар мен қолданушы кәсіпорынға маңызды болып табылатын мәлететтердің ұрлануына себеп болады. Бұндай зиянды әсерінен сақтану үшін, кәсіпорындар жергілікті желінің қауіпсіздігін қамтамасыз еткендей желілік мәлеметтер сақтауды (SAN) да қорғау қажет.

SAN желісі дәстүрлі түрде қауіпсіз болып саналады, себебі SAN қосылу әдісі өзге мәлеметтер орталығының компоненттерімен шектеулі қолжетімділігі бар тұстарымен байланысады. Табиғатына сәйкес, SAN өзі оқшауланған желі болып табылады. SAN бұндай сипаттамасы өте қарапайым болар еді. Жалғыз зиянға ұшыраған хосттың өзі потенциалды түрде SAN желісімен байланысқан

басқа хосттардың жұмысын тоқтатуы мүмкін. Оған қоса SAN шегінде болмайтын мәлеметтерге рұқсатсыз қол жеткізіп және Fibre Channel байланысы бар IP каналдардың үстінен желіаралық экран мен рұқсатсыз енуді анықтау жүйесін орап өтуі мүмкін[8].



Сурет 1.16 – Желілік мәлемет өңдеуші ортаның қауіпсіздігінің сұлбасы

Оған қарамастан, SAN желілерінің ішінде мәлімет өңдеуші ортаның физикалық шегінен шығып кететін түрлеріде кездеседі. Оның негізгі мақсаты – бизнестің үздіксіз жұмыс істеуі мен апат болған жағдайда жылдам қалпына келтіру. TCP/IP протоколын трапспорт ретінде қолданатын SCSI over IP (iSCSI) және Fibre Channel over IP (FCIP) технологиялары SAN барлық талаптарын қанағаттандыратын сенімді қорғаныспен қамтамасыз етеді. Бұндай технологиялар ортақ қолданушы желі арқылы конфиденциалық мәлеметтерді жіберуді болжап жатыр.

Бұл дипломдық жұмыста коммутацияға арналған Cisco өнімдерінің мәлемет өңдеуші ортаның «премьера» класынан Cisco Catalyst 6500 Series отбасылық коммутаторлары мен «директор» класынан Cisco MDS 9000 отбасылық коммутаторларын қолдана отырып, желілік шабуылдардың алдында сервер топтарының әлсіз тұстарын төмендетеді.

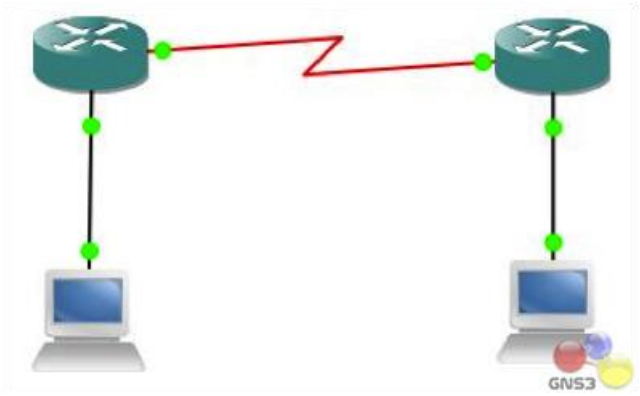
2 GNS3 желінің графикалық стимуляторы

2.1 GNS3 бағдарламасының сипаттамасы

GNS3 күрделі желілерді эмуляциялай алатын желінің графикалық стимуляторы болып табылады. Виртуалды ортада әртүрлі операциялық жүйелерді эмуляциялайтын VMWare, VirtualBox және Virtual PC атты бағдарламалармен таныс шығарсыз. Бұл бағдарламалар компьютердің виртуалды ортасында Windows XP Professional немесе Ubuntu Linux операциялық жүйелерін іске қоса алады. GNS3–та сол типті эмуляция қызметін Cisco–ның желіаралық операциялық жүйелерін қолдану арқылы атқарады. Ол Cisco IOS–ты компьютердің виртуалды ортасында іске қоса алады. Dynamips сол бағдарламаның IOS–ты эмуляцилау үшін қолданатын ядросы болып табылады. GNS3 желілік графикалық стимуляторы Dynamips–пен бірге өте қолайлы графикалық ортаны қолданысқа ұсынады. GNS3 желілік графикалық стимуляторының жалпы түсінігі 2.1–суретте көрсетілген.

GNS3 өзгеде Qemu, Pemu және VirtualBOX секілді эмуляциялық бағдарламалармен бірге жұмыс істеуді қолдайды. Бұл бағдарламалық қамтамалар Cisco ASA және PIX брандмауэрлерін, Cisco IPS, Juniper маршрутизаторларын, оған қоса Linux, Windows, Mac OS X, FreeBSD атты операциялық жүйелермен эмуляцилау үшін қолданылады. GNS3 осы барлық эмуляциялардың жұмысын тығыз байланысты қылады, мысалға Cisco маршрутизаторларын Linux жүйесімен тікелей, қиындықсыз байланыс орнатады. Практикалық түрдегі мүмкіндіктері шексіз.

Бұл желілік графикалық стимулятор Cisco IOS–ты компьютердің Windows, Linux және Mac OS X жүйелерінде эмуляция жасауға мүмкіндік береді. EtherSwitch картасын қолданып маршрутизаторлар және коммутациялық платформаларда картаның функционалды қолдау көрсету дәрежесіне дейін эмуляция жасай алады.

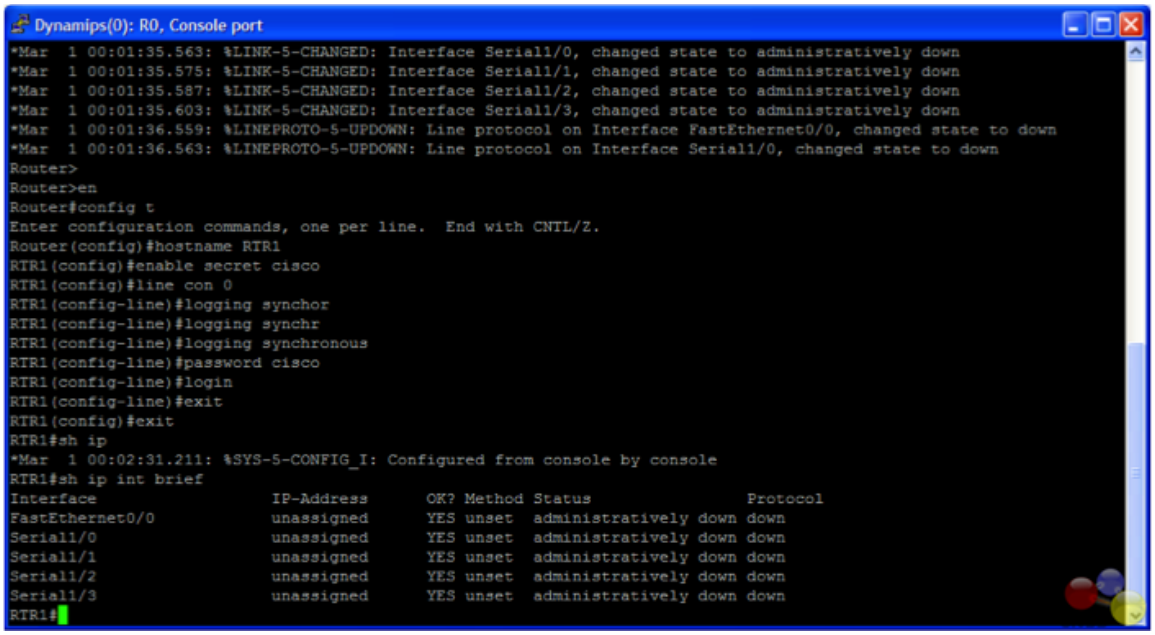


Сурет 2.1 – GNS3 желілік графикалық стимуляторының жалпы түсінігі

Бұл дегеніміз, GNS3 желілік графикалық стимуляторы Cisco сертификаттарын дайындау үшін, оған қоса CCNA, CCNP және CCIE үшін таптырмас шешім.

Жоба жасау барысында қолданушыға қажет, бірақ командалары шектелген бірнеше маршрутизатор симуляторы кездесуі мүмкін. Көп жағдайда практикалық жұмыстарда қолдау көрсетілмейтін командалар немесе баптаулар кездеседі. Біз GNS3–пен жұмыс істегенде нақты Cisco IOS істейміз, яғни IOS–қа қажетті барлық командалар мен баптамаларға қолжетімді болады.

GNS3 желілік графикалық симуляторы ашық бастапқы код болып табылады, оған қоса бағдарлама тегін. Тек қана Cisco IOS–тың лицензиялық шектеуі болғандықтан GNS3–пен жұмыс істеу үшін ақылы түрде қолданамыз. Негізгі артықшылықтарының бірі болып виртуалды ортада GNS3–тің секундына 1000 пакет өткізе алу қабілеті. GNS3 лабораториялық немесе тесттік мақсатта қолдануға болады. Қалған жағдайларда қолданатын болсақ, өндіруші компанияның келісіміне қарсы келген боламыз. GNS3–тің Dynamips ядросы төмендегі 2.2–суретте көрсетілген.



Сурет 2.2 – GNS3–тің Dynamips ядросы

Тағы бір GNS3–тің ерекшелігі, ол біз жобамызда жасап жатқан топологиямызды шынайы құрылғыларға қоса аламыз. Кейбір CCNA мен CCNP зерттеулерге шынайы веб–браузер немесе Cisco құрылғысының қауіпсіздік диспечеріне қосылу қажет болады. Қарапайым түрде өз топологиямызды компьютерімізбен байланыстырамыз. Қажет болса компьютердегі VMware немесе Virtual PC ішінде орнатылған виртуалды машиналарға қосыла аламыз. Бірақ ескерте кертетін бір мәселе, GNS–тің шынайы құрылғыларға қосылған виртуалды топологиясының жұмыс істеуі сал ерекше болады. Яғни шынай құрылғылардағы процестер толық қаны орындалмыйды. Сол себепті жоғарыда

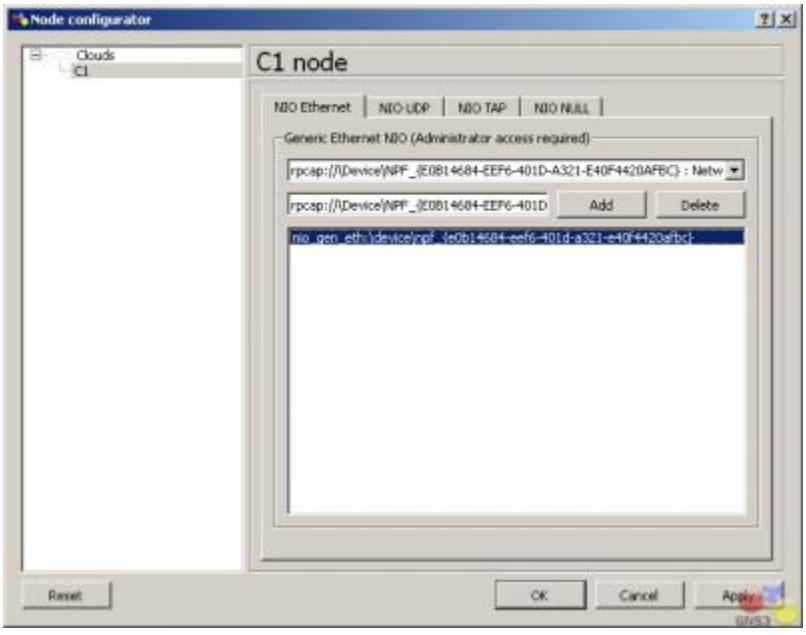
ескертіп кеткендей, GNS3–ті тек лабораториялық немесе машықтану мақсатында қолдану керек.

2.2 GSN3 бағдарламасының компоненттерін қолданумен танысу

Осы дипломдық жұмыстың топологиясын құру кезеңінің бір бөлігіне тоқталып кетейік. Cloud компанентін жұмыс үстеліне қоямыз (2.3–сурет). Келесі кезекте Cloud компанентінің үстіне тышқанның оң жақ батырмасын басып, баптау бөлімін таңдаймыз.

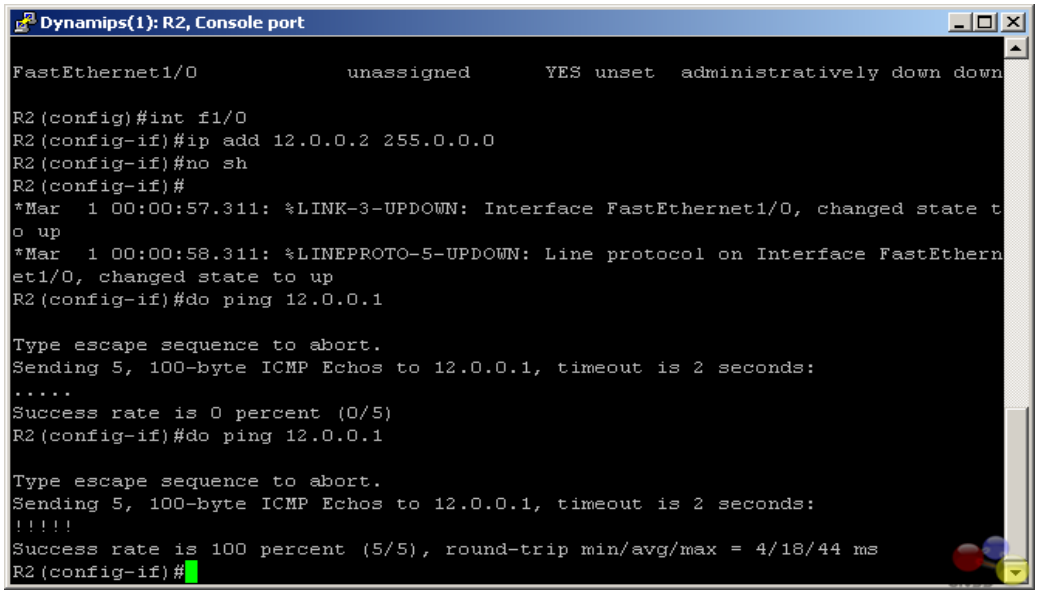
Сурет 2.3 – Cloud компонентімен байланысу

Cloud–тың астындағы C1–ді басып, оның ішінде NIO Ethernet қосымша бетін таңдаймыз (2.4–сурет). Біздің жағдайда Windows операциялық жүйесі болғандықтан, Generic Ethernet NIO–ның астында орналасқан аймаққа басып, біз қолданатын желілік адаптерді таңдаймыз. Add және Ok батырмасын басамыз. Компьютер адаптері үшін IP баптамаларын орнату қажет. Келесі кезекте саймандар қатарынан Add link батырмасы арқылы байланыс орнату керек.



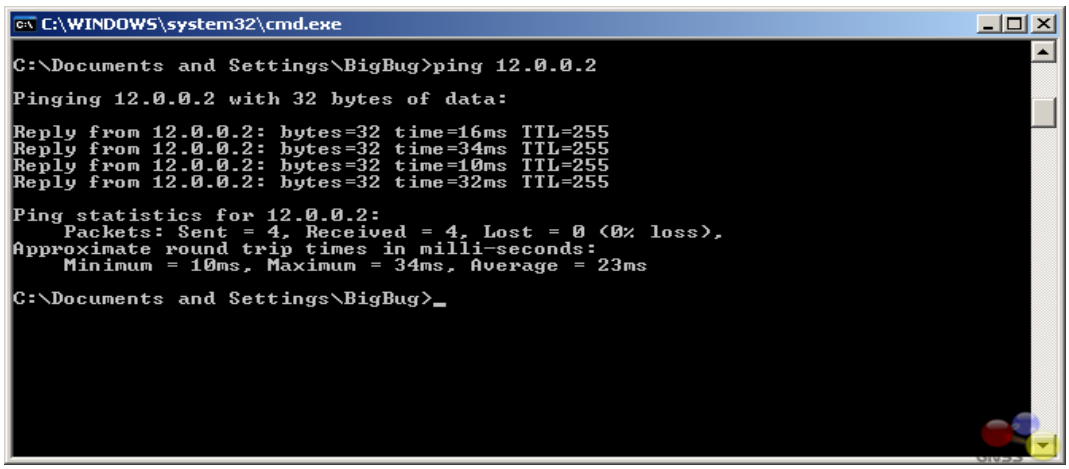
Сурет 2.4 – Cloud компонентінің баптамасы

Қарапайым желілік адаптерді қолдансақ та болады, бірақ біздің жобада MS Loopbak адаптерін пайдаланамыз. Windows жүйесінде басқару панеліндегі құрылғыларды орнату мастерін қолданамыз. «Иә, мен құрылғыны қостым» таңдаймыз. Келесі экрандағы тізімнің соңындағы «Жаңа құрылғы қосу» таңдап, одан кейін «Келесі» батырмасын басамыз. «Құрылғыны қолмен орнату» таңдаймыз және «Келесі» батырмасын басамыз. Өндіруші ретәнде Microsoft–ты таңдап, ал желілік адаптер ретінде Microsoft Loopback Adapter таңдаймыз. Мастердің жұмысы осымен аяқталады. Тышқанның оң жақ батырмасы арқылы «Желілік аймақты» басып, баптауар бөлімін таңдаймыз. Осы жерден «Локальді желі арқылы қосылысты» MS Loopback адаптері ретінде өзгерте аламыз. Топологияға қосылу үшін IP–адрестің дұрыс баптамаларын орнату қажет. 2.5–суретте Dynamips көмегімен баптаулар жүргізу көрсетілген.



Сурет 2.5 – Dynamips көмегімен баптаулар жүргізу

Енді маршрутизаторды қосып, біздің бұлтпен байланысқан IP–адрес интерфейсін тағайындаймыз. Біз осы тұста маршрутизатордан компьютерге кері байланыс интерфейсімен пингтаймыз және кері бағытта.

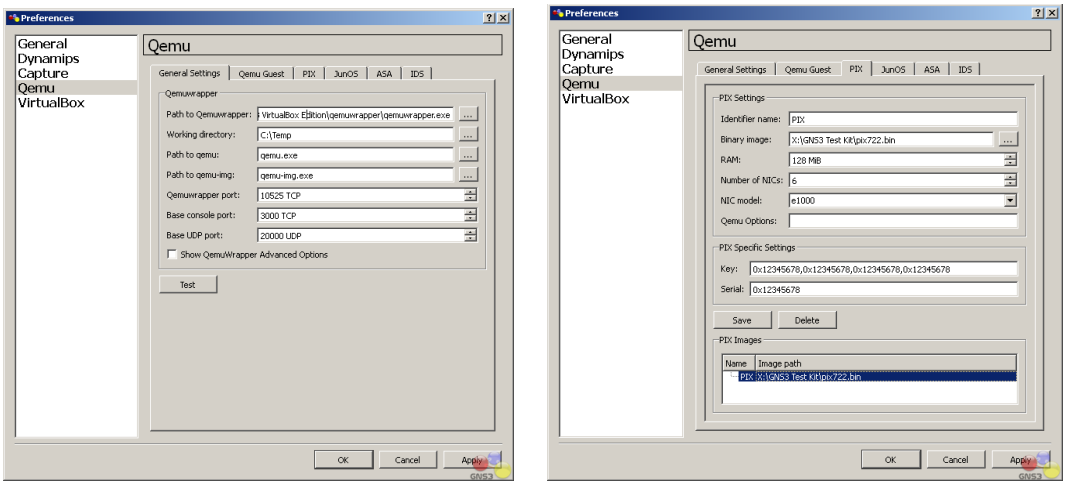


Сурет 2.6 – Маршрутизатордан компьютерге пингтеу

Қолайсыз жағдайлардың болмауын алдын алып, кедергі келтіретін кез–келген брандмауэрлерді өшіріп тастаймыз. Маршрутизатордан компьютерге пингтеу 2.6–суретте көрсетілген.

2.3 PIX Firewall эмуляциясы

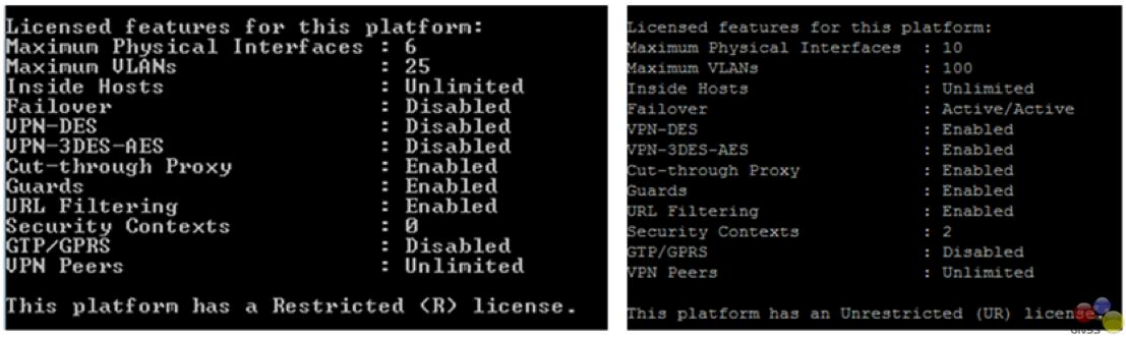
GNS3–тің тағы бір мүмкіндіктеріне PIX брандмауэрін эмуляциялай алатындығында. Бірақ PIX кескінін өзіміз бөлек иеленуіміз қажет болады. Qemuwrapper мен Cisco Pix кескінінің баптамасына ерекше тоқталып өтейік. Алғашқы әрекетпен GNS3–тің түзету мәзіріндегі баптамалар бөлігіне кіреміз. Qemu–дің сол бөлік панеліне басамыз. Үнсіз келісім бойынша Qemuwrapper–дің жолы көрсетіледі, бірақ өз қалауымызбен өзге орындарды көрсете аламыз. Ерекше көніл бөлетін орындардың бірі, өзіміз байқағандай Qemuwrapper жинақталған Pemu версиясымен бірге ұсынылады. Сол себепті Pix Firewall–ын Qemu–мен байланыстыра отырып қолдау жасаймыз. GNS3 пен Pix Firewall–ың байланыстырудың баптамалары 2.7– суретте көрсетілген.



Сурет 2.7 – Qemu баптамалары

Ріх мәзірінде Ріх операциялық жүйесінің образын көрсету үшін бинарлы кескіннің қпсындағы батырманы қолданамыз. Өзгеде параметрлерін өзгерткеннен кейін, мысалға оперативті есте сақтау жадының немесе интерфейс көлемін өзгерткеннен кейін «Сақтау» батырмасын басамыз.

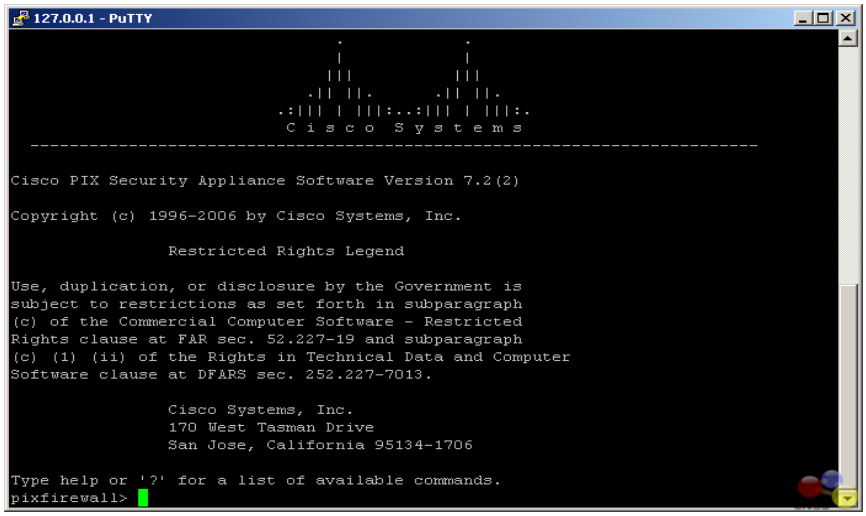
Біздің жағдайда үнсіз келісім берілген кілт пен сериалық номерді қолданамыз. Бірақ ол кейбір мүмкіншіліктерге тосқауыл болады. Қосымша функцияларға қол жеткізу үшін шынайы кілт пен сериалық номерді алуымыз қажет. 2.8 – суреттің сол жағында шектеулер тізімі көрсетілген. VPN–DES–тің қалыпты жұмыс істеуі және VPN–3DES–AES өшірілген. Оған қоса 6 физикалық интерфейстан және 25 VLAN–нан шектеулі боламыз. Қолжетімді функциялардың тізімі төмендегі суреттің оң жақ бөлігінде көрсетілген. Шектелмеген лицензиямен бұл функцияларға қоса қосымша интерфейс және VLAN қолдауы бар. Яғни өз ішіне кірістірілген бұл қолдаулар қолданысқа өте икемді әрі тиімді. Сол үшін жобамызда қолданатын компоненттер мен бағдарламаның мүмкіншіліктерін ескере отырып лицензиялы кілт пен сериялық номерді алғанымыз жөн болады. Себебі GNS3 желілік графикалық симуляторының бұл мүмкіншіліктері көп жұмысты жеңілдетеді.



Сурет 2.8– Лицензиялы Qemu орнату артықшылықтары

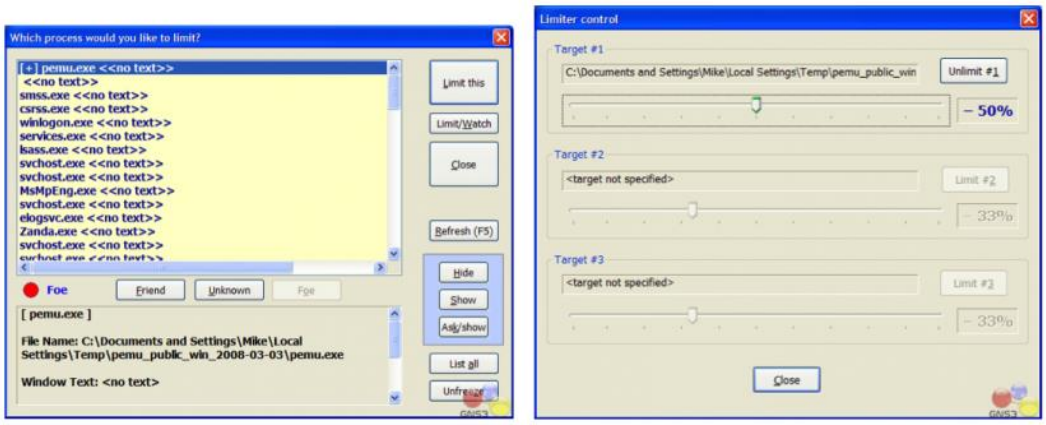
Жоғарыдағы баптамаларды орындап болғаннан соң «Ok» батырмасын басып GNS–тің негізгі интерфейсіне ораламыз. Ріх брандмауэр белгісін жұмыс орнындағы «Түрлер» аймағына алып келеміз. Тышқанның оң жақ батырмасымен FW1–ге басамыз және «Бастау» таңдаймыз. Тағы FW1–ге оң жақ батырмасын басып, «консоль» таңдаймыз. Осы іс–әрекеттен кейін 2.9 – суретте көрсетілгендей біз қолданып жатқан Ріх Firewall–дың верциясын көрсету командасы орындалады.

Ріх–тің интерфейстері Ethernet интерфейс типінен болып келеді. Сол себепті өзге құрылғыларға қосылу үшін Ethernet немесе FastEthernet интерфейсін қолдану қажетпіз. Біз келесі кезектегі интерфейске қосыла алмаймыз. Біз Ріх–тің басқа брандмауэрлеріне, маршрутизаторларына және коммутаторларына қосыла аламыз. Бірақ бұлтқа қосыла алмаймыз. Шынайы желіге немесе Virtual PC–ға қосылу үшін алдымен PIX–тің коммутаторына қосылып, келесі кезекте Cloud–тың коммутаторына қосылады.



Сурет 2.9 – Pix Firewall версиясын көрсету командасының орындалуы

Компьютерде PIX брандмауэрін эмуляциялау кезінде маршрутизатор секілді, процессордың жүктелуі маңызды сұрақтардың бірі болып табылады. Байқағандай, процессордың жүктелуі 100% көрсетеді. Себебі PIX брандмауэрмен қатар қажеті жоқ процестер іске қосылып, бағдарламаның жұмысын ұзартып әрі кішігірік проблемаларға алып келеді. Сол себепті оны бақылып отыру үшін өзге өндірушілердің өнімдерін қолдануды ұсынам. Мысалға бұл жобаны жасау барысында Windows компаниясының BES атты өнімін қолдандым. Біз PIX Firewall–ды іске қосқанда, Bes–те іске қосылады. Сол кезде «Target» батырмасын басу арқылы pemu.exe процесін таңдап, «Шектеу» батырмасын таңдаймыз. 2.10– суретте көрсетілгендей растау терезесі шығады. «Control» түймесін қанша процестің шектелетітін бақылау үшін басамыз. Мен процессордың жүктемесін минималды түрде азайту үшін 50% қылдым. Егер жобада бірнеше брандмауэр жұмыс істейтін болса, әрқайсысының жұмыс істеу процесін шектеуге болады. Бұл бағдарлама Windows жүйесінде жұмыс атқарып жатқан өзгеде процессорларды шектей алады.



Сурет 2.10 – Брандмауэрдің жұмыс процесін шектеу

Жалпы бұл PIX (Private Internet Exchange) желіаралық экранын Cisco компаниясы ұсынады. Бұл жобада қолдануға өте икемді әрі қолалы болуы мен қорғаныстың жаңа дәрежесімен қамтамасыз етеді. Бұл желіаралық экранның негізгі ерекшеліктері, оның қорғау схемасында. Ол негізі адаптерленген қорғаныс алгаритмін, яғни adaptive security algorithm (ASA) қолданады.

3 Қауіпсіздікті қамтамасыз ету

3.1 Кәсіпорын туралы жалпы сипаттама

«Trust company» ЖШС кәсіпорыны бұл қазіргі техникамен, механизмдермен және құрал-жабдықтармен өндірістің жаңадан жабдықталуын белсенді жүргізетін динамикалық дамушы кәсіпорын. Бұл кәсіпорынның негізгі қызмет түріне жылу энергиясын беруге, электр тораптарын және қосалқы станцияларын, көтергіш құрылғыларға, қысымды ыдыстар мен құбырларды пайдалануға, қысыммен жұмыс істейтін энергетикалық құрал-жабдықтардың, ыдыстар мен құбырлардың жөндеу болып табылады.

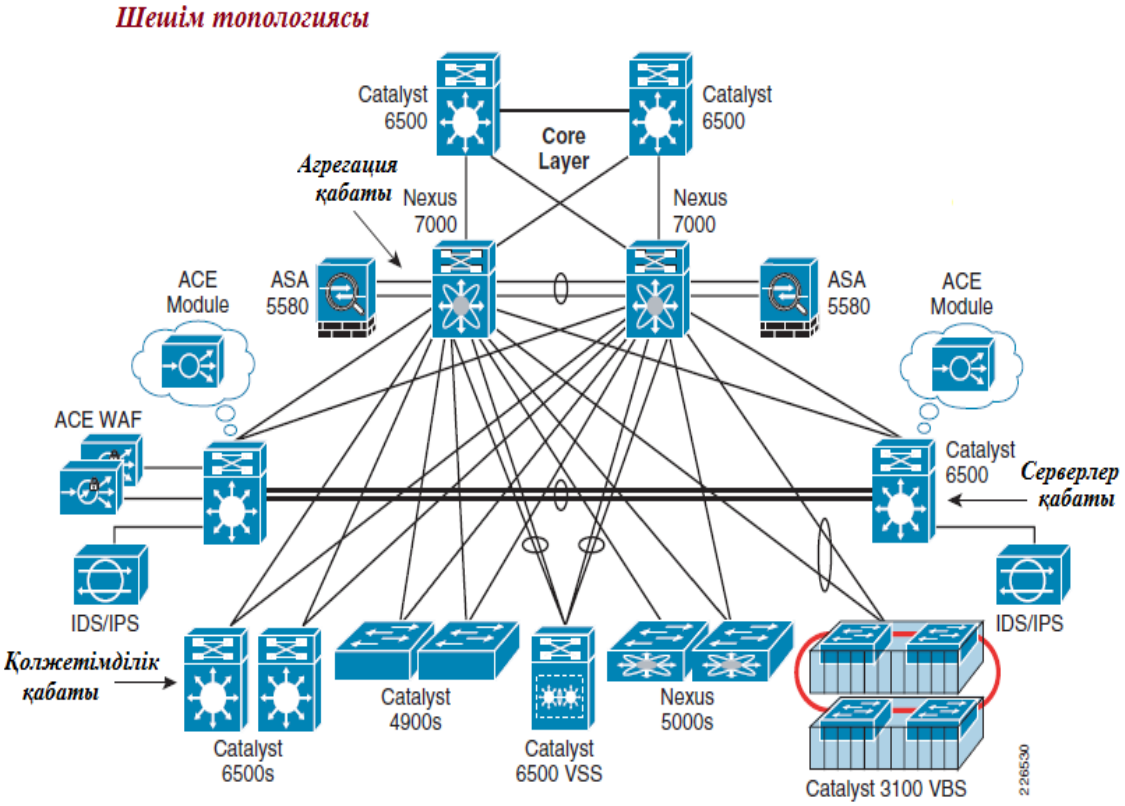
Кәсіпорынның бас ғимараты Алматы қаласыда орналасқан. Өзінде 74 бөлме және 127 жұмысшы бар үлкен кәсіпорын. Бөлме аралық желісі қарапайым желілік құрылым негізінде (5е жұп категориясы) құрылған және ерекшеленген оптоволоконды интернетке қосылған, каналдың ені 2 МБ/с.

Негізгі тапсырма кәсіпорынның қарапайым желілік құрылымын бұлттық технология негізіне ауыстыру. Осы мақсатта бұлттық есептеудің қауіпсіздік мәселесі, ақпарат алмасудағы қорғаныс шаралары, желіге келетін қауіп-қатер және желінің қауіпсіздік қызметі жайлы жалпы мағлұмат қамтамасыз ету. Бұлттық технология негізіндегі желінің қауіпсіздігін ұйымдастыру үшін қолданылатын технологиялар, құрылғылар, программалардың сипаттамаларды ұйымдастыру. Бұлттық есептеуге өту барысыда туатын проблемаларды қаржылық жағынан кәсіпорынға тиімді, ал эффиктивтілігі тұсынан жоғары қылу.

3.2 Қауіпсіздікті қамтамасыз етудің шешім топологиясы

ИТ қауіпсіздік администратордың жауапкершілігіне төнген қауіптер желіге конфиденциалды корпоративтік мәліметтерге жасалынған күрделі шабуылдар нәтижесінде өсті. Мәліметті өңдеу орталығының қауіпсіздігінің қуатты мүмкіндіктерін пайдаланып, корпоративті желідегі аса құнды мәліметтерді сақтап қалу өте маңызды мәселе болып отыр.

Мәліметті өңдеу орталығының қауіпсіздігінің мәселе жеткен жетістігімен тоқтап қалмақ емес. Қолданбалы бағдарламаларға жаңа өзгерістер, виртуализация және мөлдір периметрлерге мәлімет өңдеу орталығының қауіпсіздік архитектурасының талабына сай эволюция жасау керек. Қауіпсіздікпен қамтамасыз етудің шешім топологиясы 3.1–суретте көрсетілген.



Сурет 3.1– Шешім топологиясы

Бір қарастырғалы жатырған архитектура Cisco мәліметті өңдеу орталықтарының ең жақсы практикалық принциптерін қамтиды. Бұл көп деңгейлі архитектура келесі негізгі компоненттерден тұрады: ядро, агрегация, қызмет сонымен қатар қолжетімділік. Бұл архитектура мәлімет өңдеу орталықтарына сұраныс және жұмысбастылықтан соң қосылды.

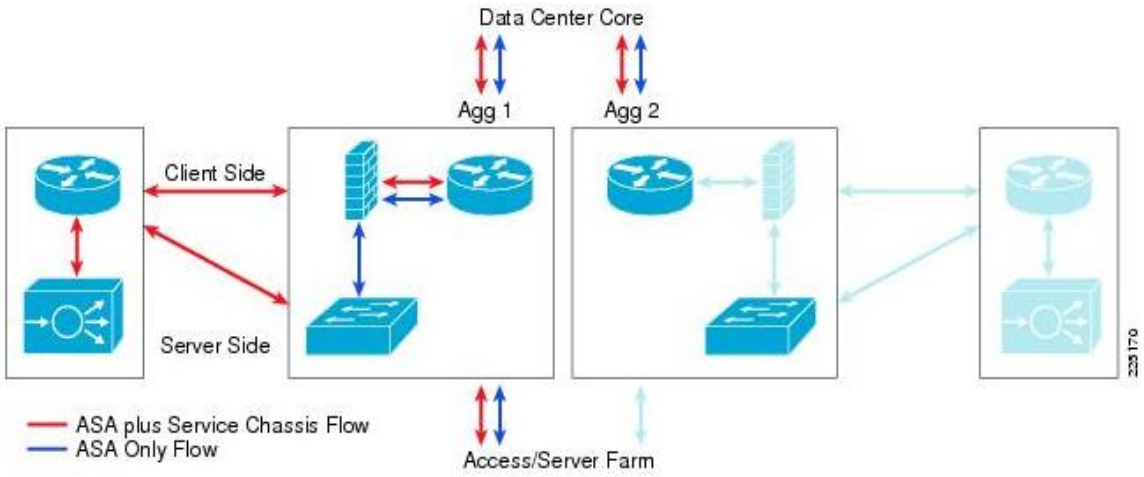
Мәлімет өңдеу орталығы мәлімет өңдеу оралығына кіріс–шығыс трафиктеріне арналған Layer–3 маршрутизация модулімен қамтылған. Мәліметтер орталығының инфраструктурасына үшін Layer–3 және Layer–2 шекараларында агрегация қабаты жұмыс істейді.

Сервер теңгерілімінің жұмысбастылығы, қауіп–қатердің алдын алу, желіаралық экрандар бағдарламасы, сонымен қатар брандмауэрдің қосымша қызметтері қызмет деңгейінде енгізілген. Мәлімет өңдеу орталықтарының қолжетімділік деңгейі серсер фермалары үшін қосылыс нүктесі болып табылады. Виртуалды қолжетімділік қабаты виртуализация үшін бапталған, физикалық серверлерде болатын виртуалды желіге жатады.

Енді осы агрегция қабатындағы Nexus 7000–ның басқа қызметтермен агрегациясын қарастырайық.

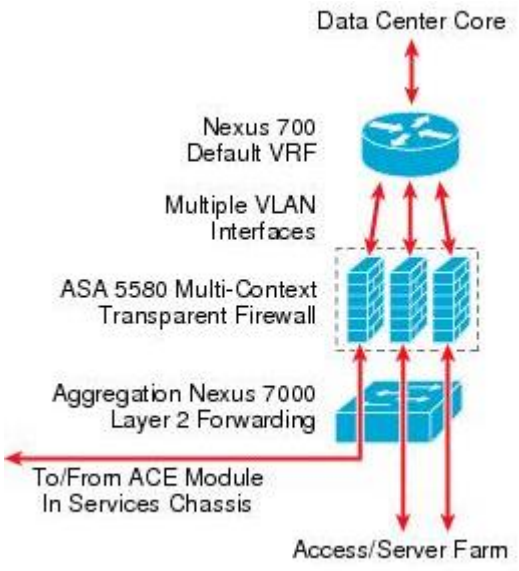
3.3 Nexus 7010 агрегациясы

Nexus 7010 агрегациясына Cisco ASA 5580 қосу мәліметтер ағынына ASA 5580, ACE модулін, шасси қызметтерін қатар қолдануға болатын логикалық конфигурацияларды жасауға мүмкіндік береді. Агрегация қабатына оны орнату желіаралық экрандардың орталықтандырылған қызметін қамтамасыз етеді. Брандмауэр қызметіне қажетті мәліметтер ASA арқылы өтіп, қолжетімділік деңгейінде сервер фермаларымен тікелей жұмыс істей алады. Бұл мүмкін ағындардың иллюстрациясы келесі 3.2–суретте көрсетілген.



Сурет 3.2 – Комбинирленген трафик ағындары шассиінің қызметі мен сервистері

Мөлдір ASA 5580–Бірнеше виртуалды контексттердің мөлдір режимінде бұл модельдің әр түрлі типтегі трафиктерді қолдауын тексерді. ASA қызметтерін ғана талап ететін трафикті қолдайтын контекст үшін коммутатор агрегациясы қабатында орналасқан серверлар фермасына маршрутизация тек үнсіз келісілген шлюз арқылы жүзеге асады. ACE модулінің қызметін қолдайтын контексттар мөлдір режимді Gatalyst 6500–дегі MSFC жүзеге асырады. Мөлдір режим конфигурациясы сервер фермаларының немесе топология маршрутизациясының өзгерісінсіз ортаға оңай енгізіледі. Коммутатор агрегациясы қабатынан өтетін мәліметтер ағыны және көптеген ASA–дағы мөлдір контексттар 3.3–сурете көрсетілген.



Сурет 3.3 – Ағынның мөлдір контексті

3.3.1 Логикалық тұрмыстық модельдің қызметі

Бұл тексеріс үшін агрегация қабатында Cisco ASA 5580 мен Nexus 7000–ның интеграциясы екі түрлі біріншілік трафик ағынын қолдайды. Біреуі трафик үшін брандмауэр қызметін талап етсе, екіншісі ACE модульдан сервердің қызмет жұмысбастылығын теңгеруді талап етеді. Бұл транспорттық ағынның қозғалысы бірнеше VLAN интерфейспен немесе ASA 5580 виртуалды мөлдір контекстерін қолданып ажыратылады. Осы ағындардың қолдауымен VLAN–ға бөлу иллюстрациясы келесі 3.4–суретте көрсетілген.

Тұтынушы компьютерлері бүкіл желінің ядросы арқылы кез келген виртуалды локальды желі сервер фермаларының жиынтығына қолжетімді болады және трафик сервердің желіде орналасуына байланысты сәйкес келетін қызмет түрі арқылы жіберіледі.

Төменде әрбір виртуалды локальді желі функцияның қысқа анализі.

ASA 5580 мөлдір Firewall тек:

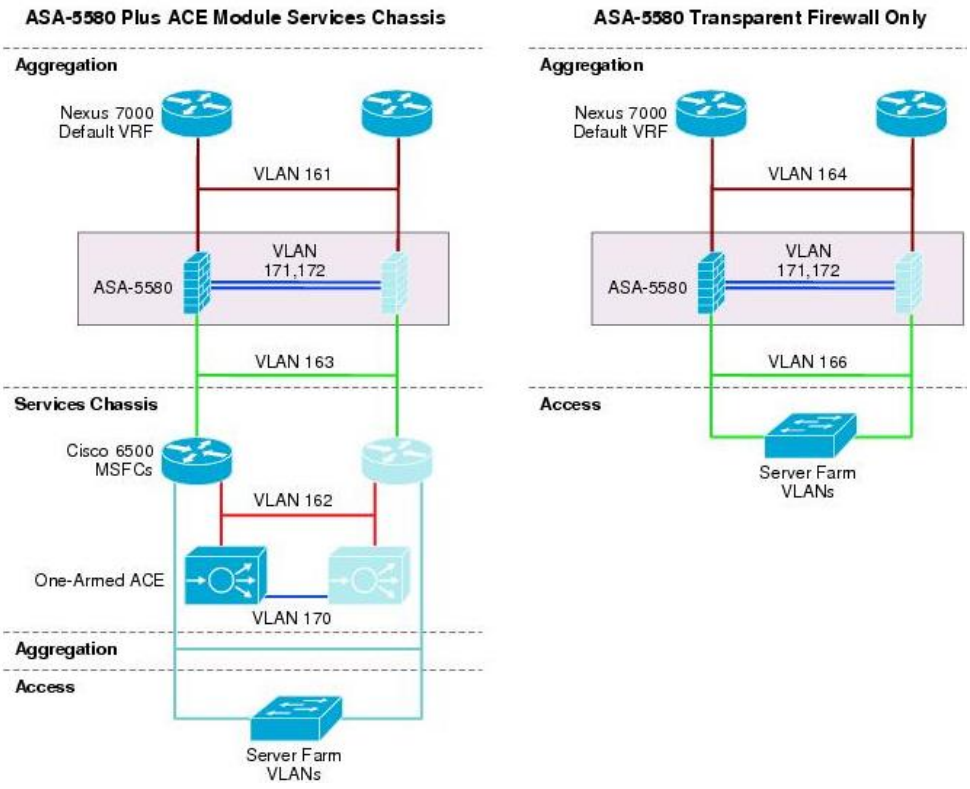
– VRF–тың үнсіз келісімімен ASA мөлдір контекстіне қосылуы–VLAN 164 ретінде көрсетілген. Бұл коммутациялар агрегациясы мен ASA құрылғысымен 10–гигабайттық жылдамдықпен байланысқан.

– ASA бас тартуға тұрақтылық–Бұл байланыстар VLAN 171 және 172 түрінде көрсетілген. Бұл VLAN желілері коммутатор агрегациясы арасындағы порт каналымен таралған. Олар өздерімен бастартуға тұрақтылық (отказустойчивость) пакеттерін алып келеді. Және желінің күйі туралы информация біріншілік және екіншілік ASA–ға олардың конфигурациясын синхронды ұстауға мүмкіндік береді.

– Сервер фермасының мөлдір ASA контексті – бұл байланыс VLAN 166 ретінде көрсетілген. ASA VLAN 164 пен 166–ны бір IP–ішкі желілік Layer–2

кең таратылымды доменге қосады. Бұл ішкі желі үшін негізгі шлюз коммутатор агрегациясы интерфейсі VLAN 164–ке HSRP–мен жабдықталған.

– Қолжетімділік қабатындағы коммутаторларда VLAN 166–да орналасқан сервер фермаларының порттары бар. Бұл порттар VLAN 164–ке ішкі желі ASA мөлдір контекстілі қосылысы арқылы қосылатын ішкі желінің жалғасы болып табылады[9].



Сурет 3.4 – Шассидың логикалық тұрмыстық модельмен қызметі

Шассидың ACE модульді қызметі мен ASA 5580:

– VRF–ның үнсіз келісімімен мөлдір ASA контекстінің агрегациясы VLAN 161 арқылы көрсетілген. Бұл коммутациялар агрегациясы мен ASA құрылғысымен 10–гигабайттық жылдамдықпен байланысқан.

– ASA байланыстың жұмыстан бас тартуға тұрақтылығы – бұл қосылыстар VLAN 171 және 172 түрінде көрсетілген. Және жұмыстан бас тартуға тұрақтылық (отказоустойчивость) пен жүйенің күйін білу үшін ASA виртуалды контексті арқылы мобилизацияланған.

– MSFC қызметі үшін мөлдір ASA контексті– бұл байланыс суретте VLAN 163–пен көрсетілген. ASA VLAN 161 пен 163–ті бір IP–ішкі желілік Layer–2 кең таратылымды доменге қосады. MSFC шассидың қызметі мен үнсіз келісімді VRF коммутаторлар агрегациясы мысалдары Layer 2 домені арқылы маршрутизацияланады немесе HSRP адрестарды көрсететін статикалық маршруттар немесе IGP–ді қолдану арқылы жіберіледі. Бұл VLAN шасси қызметінен кейін екі деңгейден соң коммутаторлар агрегациясына жетеді, сонымен қатар коммутаторлар агрегациясы арасндағы порт каналы бар.

– Бір қолды ACE–ге 6500 MSFC шассидың сервисінен. Бұл ссылка суретте VLAN 162 түрінде көрсетілген. Бұл трафик үшін кіріс те шығыс та интерфейсі ACE модулі арқылы жүзеге асады. ACE сервер фермаларына жіберілетін пакеттердің адресін өзгертетін Nat–ты жасайды. Осылайша қайта келген пакеттер ACE арқылы өтуі тиіс. Ол жерде клиент түйіні сұраған пакет бастапқы мөлшерге айналдырылады.

– ACE жұмыстан бас тартуға тұрақтылық байланыс модулі–Бұл байланыс суретте VLAN 170 ретінде көрсетілген. Екі шасси сервистері арсында физикалық байланысады. Бұл байланыс трафикті жүргізеді және екі ACE модулі арасындағы баптауды синхрондайды.

3.3.2 Енгізудің спецификалық ерекшеліктері

ASA Firewall әдістері. Cisco ASA 5580 бірнеше виртуалды контексті маршрутизация режимінде немесе мөлдір режимді де қабылдайды. Барлық конфигурацияланған контексттер сол режимде жұмыс істеуі тиіс. Динамикалық маршрутизация протоколы тек қана біртұтынушы контекст режимінде ғана емес EIGRP мен OSPF–ты қолдайды. Бұл тексеру жұмысы үшін мөлдір режим сервер фермаларының архитектурасының интегрциясының қарапайымдылығы үшін таңдалды. Бранмауэрден тыс сервер фермаларының ішкі желісіне үнсіз келісім бойынша шлюздың қолдауы сонымен қатар әр түрлі ішкі желіде орналасқан серверлік қабаттар арасында брандмауэрді орнату үшін қажет.

Шасси серверіне маршрутизация

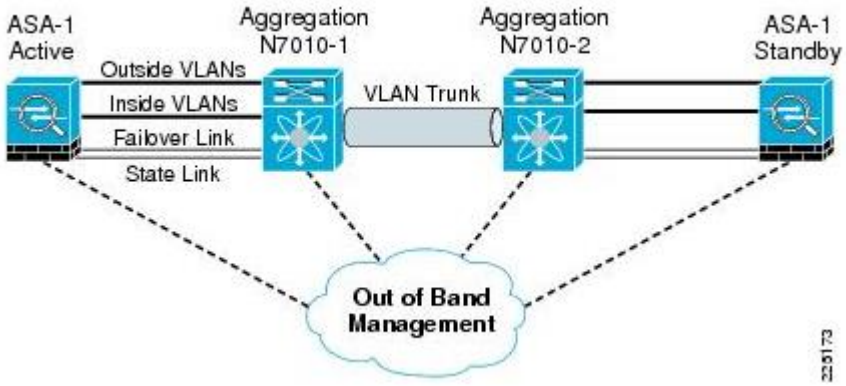
ASA мөлдір режимде жұмыс жасайды және FWSM шасси сервері моделінен өшірілген. Layer 3 шасси серверінің MSFC–і коммутатор агрегациясымен тікелей маршрутизациялық көршілер. Бұл маршрутизация статикалық маршрутизация немесе EIGRP секілді OSP мен IGP–дің көмегімен іске асады.

Шасси серверімен архитектуралы топологияны іске асыру тақырыбында айтылғандай, егер коммутатор агрегациясында қос басқарушы көркейтілген болса, қызметті интеграциялау үшін статикалық маршрутизацияны пайдаланған жөн. Екі бағытта HSRP адрестарды көрсететін статикалық маршрутизаторды пайдалану қозғалыс жолын толық бпасқаруға көмектеседі. HSRP–ның артықшылықтарын объектті аңду арқылы манипуляциялауға болады.

Егер жалғыз supervisor коммутаторлар агрегация деңгейінде көркейтілген болса, статикалық маршрутизация немесе IGP–мен динамикалық маршрутизация шасси сервисі мен коммутатор агрегациясы арасында қолданылады. HSRP–ді көрсететін статикалық маршрутизация Layer 3 физикалық белгіге барар жолды бақылайтын шасси сервис орталығында артықшылығы бар[10].

3.3.3 Физикалық кабельдік детальдар

ASA 5580 басқару үшін орнатылған Gigabit Ethernet порты мен 9 слоттан тұратын шасси болып табылады. Бұл тексеру қолданылған конфигурация құрамында екі порты 10–Gigabit Ethernet–тің картасы және төрт порттық бір Gigabit Ethernet картасы бар. 5580s ASA үшін мөлдір режим конфигурациясы үшін физикалық байланыс әрбір 5580s ASA тұтынушы мәлімет трафигінің коммутаторлар агрегациясы деңгейіне біреуі ғана бекітілетіндей етіп жасалған. Тексерілетін жобалау моделінде физикалық байланыс 3.5–суретте көрсетілген.



Сурет 3.5 – ASA 5580 Құрылғыларды қосатын физикалық порт

Сыртқы VLAN желілері – бір 10–Gigabit Ethernet интерфейсі 802.1Q VLAN trunk ретінде конфигурацияланған. Ол Қауіпсіздік жағынан қарастырғанда брандмауэрдің «сыртында» орналасқан бірнеше виртуалды локальды желіні қолдау үшін жасалынған.

Ішкі VLAN желілері– бір 10–Gigabit Ethernet интерфейсі 802.1Q VLAN trunk ретінде конфигурацияланған. Ол Қауіпсіздік жағынан қарастырғанда брандмауэрдің «ішінде» орналасқан бірнеше желіні қолдау үшін жасалынған.

Жұмыстан бас тартуға тұрақтылық (отказоустойчивый) байланыс– Жұмыстан бас тартуға тұрақтылық байланысы ASA–ның артық бірліктері, желі байланысы дәрежесін, белсенділікті қолдау, MAC фдрестарды айырбастау, және синхронизацияны баптау үшін қажет. Бұл баптауда Жұмыстан бас тартуға тұрақтылық байланысы әрбір ASA блогы жалпы VLaN–ға қосылған, яғни екі коммутатор агрегациясы арасындағы мульти–гигабиттік канал порты арқылы ұзартылған. Бір Gigabit Ethernet ASA–дан коммутатор агрегациясы аралығын қосу үшін қолданылған.

Байланыс күйі – жұмыстан бас тартуға тұрақтылық кезінде қолданылады, күй информациясын жіберуге жауапты. Ол егер маршрутизация режимінде болса, мәліметті жіберу интерфейсінің біреуіне жіберіледі, немесе көшіру интерфейсына. Бірақ бұл тапсырманың орындалуы үшін физикалық интерфейсті қолданған дұрыс.

Келісілген топологияда ASA–дан бөлек байланыс үшін Gigabit Ethernet интерфейсы қолданылады. Ал VLAN күй туралы информацияны жіберу үшін содан соң екі коммутатор агрегациясы арасындағы мулти–гигабиттік порт каналдарына таратылады.

Ішкі–сыртқы басқару– әр құрылғыдағы Gigabit Ethernet–тің орнатылған порттарының бірі сыртқы басқаруға арналған және бөлек басқару желісіне қосылған. Жоғарғы суретте көрсетілгендей ереже бойынша коммутатор агрегациясы секілді басқа мәлімет өңдеу орталығының құрылғыларымен бірге қызмет жасайды.

3.4 Мәлімет өңдеу орталығы

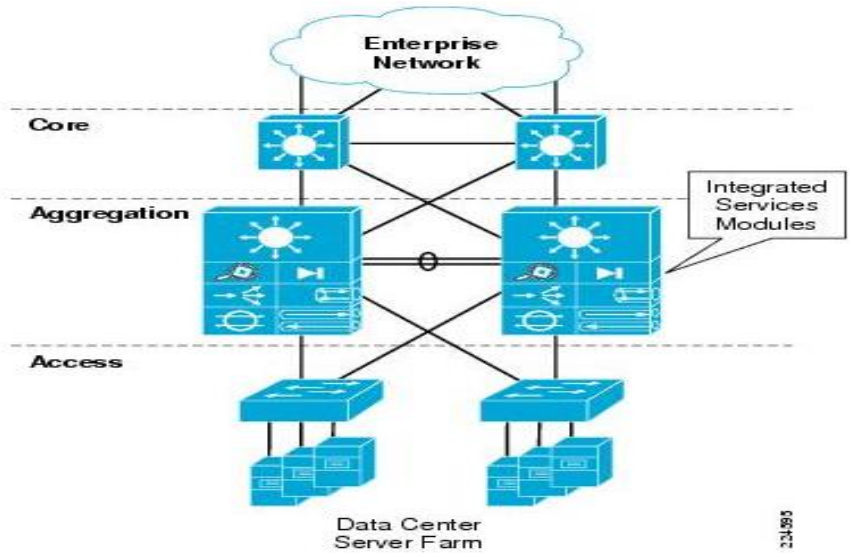
Мәлімет өңдеу орталығы корпоративті желінің негізгі бөліктерінің бірі болып табылады. Мәлімет өңдеу орталығының желі жобалары кез келген құрылғы мен каналдың бас тартуы секілді жоғарғы талаптарды шеше білуі керек. Бұл сонымен қатар, брандмауэр, сервер мен бағдарламаның артық жүктілігін теңгеру секілді қызметтерді атқару үшін желіден жоғары интелектті талап етеді.

Интеграцияланған сервистер физикалық моделі

Cisco Catalyst 6500 платформасы шасси картасы үшін бағандағы бағалы кеңістік пен қуат, мәлімет өңдеу орталығы желісінің кабельдерін сақтай отырып, сервистік модульдерді интеграциялау қызметін ұсынады. Көп таралған модель жобасы иерархиялық желі құрылысындағы коммутаторлар агрегациясы деңгейінде модульдердің интеграциясы болып табылады және ол төменде көрсетілген.

Бұл шешім агрегация қабатындағы коммутаторлар рамкасында қолжетімді слоттар бар болса немесе бастапқы құрылыста шасси слотының сыйымдылығы жобаланып, сервисті модульдерге бөлінген болса қолданылады.

3.6–суретте көрсетілгендей жан–жақты таралған модель жобасының негізінде құрылған иерархиялық желі құрылысында ерекше әрі орынды түрде қолданылған коммутаторлар агоегациясы деңгейінде, жоғарыда атап кеткендей модульдердің интеграциясының сұлбасы көрсетілген. Core, Aggregation және Access модульдерінің интеграциясының жекелеп көре аламыз.



Сурет 3.6 – Сервистер интеграциясының физикалық моделі

3.5 Шасси қызметтерінің физикалық моделі

Мәлімет өңдеу орталығының желілері өскен сайын уақыт талабына сай масштабы да үлкейе түседі. Агрегация қабатында қызмет модульдері көп тығыздықта орнату мақсатында қолданатын слоттарды қайта орнатуға тапсырыс болуы мүмкін. Бұл екінші агрегация блогының қажетінсіз қолжетімділік қабатындағы коммутаторларды агрегациялауға мүмкіндік береді. Басқа факторлар қызмет интеграциясынан миграциялауды басқара алады, мысалы, агрегация деңгейінде Cisco Catalyst 6500 сервистік модулі қолдай алмайтын жаңа жабдықты енгізу тілегі. Мысалға, Cisco Nexus 7000 сериялы коммутаторларда әр түрлі өнімділік формасы факторлары бар, дегенмен Cisco Catalyst 6500 сервистік модульдері қолдамайды. Алғашқы Cisco Catalyst 6500 виртуалды коммутация жүйелері 1440 шассиге сервисті модульдерді қондыруды қолдамайды, бұл қолдау үшін жаңа бағдарламалық қамтама қажет. Ол Cisco IOS Release 12.2 (33) SXI–те жоспарланған.

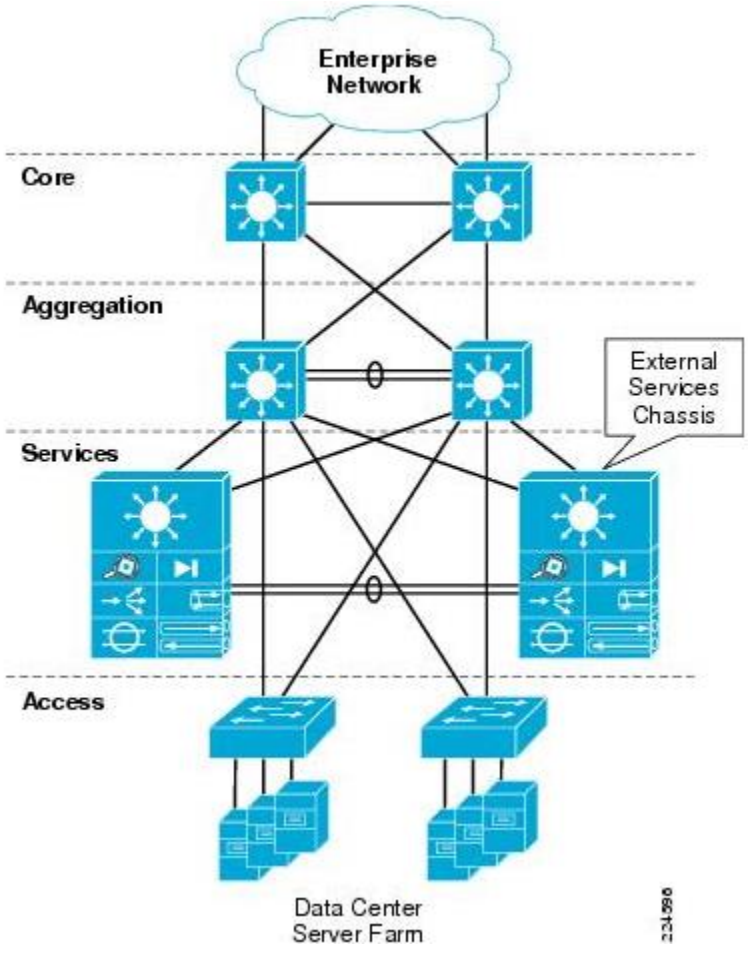
Бұл модульдер қуат пен желілік қосылыс үшін Cisco Catalyst 6500 қажет етеді. Мәлімет өңдеу орталығын желісінде құрылғылардың интеграциясы үшін жаңа шешімдер қарастырылуы мүмкін. Осы шешімдердің бірі мәлімет өңдеу орталығының агрегация қабатында қосымша Cisco 6500 шассиларын қосу. Бұл коммутаторлар әдетте шасси қызметтері деп аталады. Шасси қызметтерінің физикалық моделі 3.7–суретте көрсетілген.

Шасси қызметтерінің физикалық моделі 3.7–суретте көрсетілгендей агрегация қабаты коммутаторларының екеуінде шасси қызметтерінің қосылыс жолы үшін қос қосылысты шешімді қолданады. Бұл шешім белгілі агрегауия коммутаторына байланысты қызмет модульдерін шешеді. Бұл жүйеге қызмет ету үшін, коммутаторлар агрегациясы немесе қызмет коммутаторларының агрегациясына қажетті эксплуатационды икемділікпен қамтамасыз етеді.

Жоғары қолжетімділік тұрғысынан арастыратын болсақ, егер бір коммутаторлар агрегациясы жұмыс істемейтін болса, трафик келесі агрегация коммутаторлары арқылы белсенді қызмет модульдеріне ешқандай бас тартусыз аға алады. 802.1q каналдары каналдардың бұзылуы немесе бас тартуы болған жағдайда жоғары қолжетімділікпен қамтамасыз ету үшін, қызмет модульдері қабаттарының аралығында жатқан виртуалды локальды желілер сонымен қатар VLAN трафиктер желілерінің кіру шығуын жалпы физикалық байланыстар алып жүруі үшін қос қосылысты байланысты қолданады.

Бөлек физикалық канал екі шасси қызметтері арасында қатеге тұрақты трафик пен активті және резервті модульдар арасындағы күйдің информациясын репликациясын тарату үшін қолданылады.

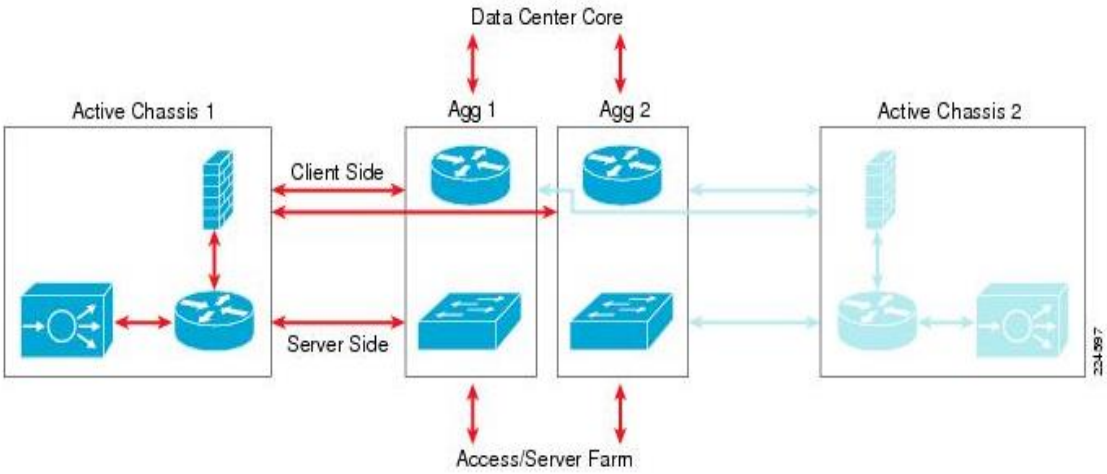
Резервтеу бұл бөлек байланыс, қатеге тұрақты басқару трафигі қолданушы мәлімет трафигімен ұсталынбайтындығына кепілдік береді. Резервтеу барлық агрегация қабаттарында қатеге тұрақты трафиктің қауіпсіздігі үшін қызмет сапасына (QoS–қа) мұқтаждықты ауыстырады[11].



Сурет 3.7 – Шасси қызметтерінің физикалық моделі

3.5.1 Active– Standby Service Chassis

Екіншілік шасси қызметтері және онымен байланысты модульдер егер негізгі шасси мен модульдердің біреуі бұзылған болса, қатеге тұрақтылық ретінде, құрылғылардың ыстық резервтері секілді ерекше әрекет етеді. Active–Standby модульдері үшін транспорттық ағын иллюстрациясы келесі 3.8 – суретте көрсетілген.



Сурет 3.8 – Активті–резервті трафик ағыны

3.5.2 Атрибуттар архитектурасы

Бұл модель құрылысы келесі мінездемелермен айқындалған:

Маршрутизацияланған FWSM.

Маршрутизацияланған қызмет құрылғылары жүзеге асыру мен қателерді жөндеуде тұжырымды түрде қарапайым болады. Себебі онда VLAN желілері мен ішкі желілерде бірден–бірге корреляциясы жұмыс істейді, және VLAN–дар арасында BPDU пакеттері жіберілмейтіндіктен қарапайымдатылған Spanning Tree құрылғысы бар.

Бір қолдық ACE желіге оңай енгізіледі және жолында виртуалды IP адрестерді ұруға мұқтаж ететін басқа трафиктер болмайды. ACE–ден бас тарту және басқа ресурстарға өту тек нағыз уақытта артық жүктіліктің теңгерілімімен немесе SSL–дың үдетлуі секілді ACE–нің басқа қызметтерін қолданып жатқан кезде ғана болады.

Трафиктің жойылу механизмі протокол айырбастаудың екі жағынан да ACE арқылы өтуді талап етеді, немесе маршрутизация саясатының негізінде (PBR), немесе желілік адрестер трансляциясын (NAT) қолдануы мүмкін.

Қызмет модулі мен тұтынушы арасындағы транспорттық ағын.

Тұтынушы/сервер трафигі үшін тұтынушы жағындағы кіріс және шығыс трафиктері ғаламдық MSFC 6500 дің қос агрегациясында теңгеріледі.

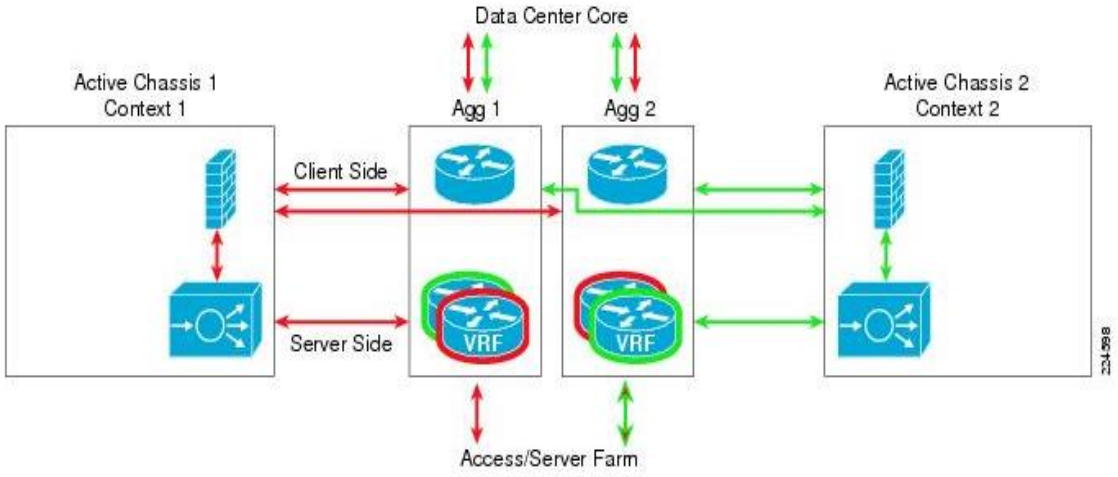
Сервер фермалары мен қызмет модульдері арасындағы транспорттық ағын.

Тұтынушы/сервер трафиктері үшін серверде (қолжетімділік деңгейі) кіріс–шығыс трафиктері жақтары коммутатор агрегациясының бір деңгейіне топталған.

3.5.3 Актив–Актив шасси қызметі

Екінші эталондық жоба моделі шасси қызметінің активті–активті моделі деп аталады. FWSM виртуализациясы мүмкіндіктері мен ACE модульдерді қос шасси қызметтеріне тарату үшін қолданады.

Трафик құрылғылар арасында автоматты түрде бірдей таралмайды, бірақ желі администраторы ішкі желі сервер фермаларын белгілі шарттарға тағайындай алады. Виртуализацияның маршрутизациясы коммутатор агрегациясында VRF жағдайында актив–актив моделін қолданады. Барлық Layer–3 процесстері агрегация деңгейінде өтеді және көмекші коммутаторлармен қатысты таза Layer–2 деңгейін сақтай отырып шасси қызметтерінің іске асуын жеңілдетеді. Бірақ, егер де модель тұтынушылардың спецификиялық талаптарын қолдайтын болса, FWSM немесе ACE маршрутизацияларын жүзеге асыруды қолдауға икемді жоба. Active–Active модульдері үшін транспорттық ағын иллюстрациясы келесі 3.9–суретте көрсетілген.



Сурет 3.9 – Active–Active трафик ағыны

Бұл модель жобасы келесі мінездемемен айқындалған:

– Мөлдір FWSM. Мөлдір желіаралық экран баптау немесе қолдау үшін статикалық маршруттар тізіміне арналған маршрутизация протоколы жоқ болғандықтан брандмауэр маршрутизациясына қарағанда аз конфиграцияны қажет етеді. Бұл тек мост группалар интерфейсында жалғыз ғана IP ішкі желілерін талап етеді. Және BPDU пакеттерді қосылған сегменттерде болатын

мост құрылғыларына жібереді. Әр түрлі мөлдір FWSM интерфейстеріндегі VLAN желілері әр түрлі VLAN сандарымен бірге жүреді. Мөлдір құрылғы VLAN желілермен бірге «тігілген» немесе «бау» деп жиі аталады.

– Мөлдір ACE. Мөлдір ACE–ның орындалуы FWSM–дардың орындалуымен бірдей. Бір IP ішкі желіні тасымалдау үшін VLAN желілері бірге «тігілген» және көрші коммутаторлар Spanning Tree есептеулерін жүргізу үшін BPDU адрестері қайта адресталады. Бірқолдық ACE–ге қарағанда мөлдір ACE трафикпен бірге қозғалады. Және протокол айырбастаудың екі жағы да құрылғы арқылы өтуі үшін трафиутің жоғалу механизмінің болмауын талап етеді. ACE мост группаға махимум екі VLAN интерфейсінің Layer–2 деңгейін және жүйеге махимум 2000 BVI–ді қолдайды.

– Қызмет модуліндегі қос активті контекст. Cisco Catalyst 6500 Services Modules–тің виртуализация мүмкіндіктерімен өздерін бөлек виртуалды құрылғы ретінде ұстайтын екі бөлек контекстар жасалды. Бірінші FWSM және ACE бірінші контекста біріншілік және екінші контекстта күту болады. Екінші FWSM және ACE екінші контекст үшін біріншілік, ал бірінші контекст үшін күтуші болады. Бұл жобадағы модульдың екі жағына да трафиктің бөлігінде біріншілік болуға көмектеседі. Бір модуль жиынтығы күтуші режимде бос тұрғаншы, администратор артық жүктілікті
Топология бойынша бөліп тастауға болады.

– Қызмет және тұтынушы арасындағы модуль транспорттық ағын.

Клиент/сервер трафигі үшін ғаламдық MSFC және 6500 агрегациясы арқылы тұтынушы жағындағы кіріс және шығыс трафиктері теңгеріледі.

Қызмет модулі мен Сервер фермалары арасындағы трафик ағыны.

Клиент/сервер трафигі үшін сервер жағындағы кіріс/шығыс трафигі коммутаторлар агрегациясы қабатындағы сервер фермасы ішкі желілеріне үнсіз келісім бойынша IP шлюз ретінде жасалынған VRF экземплярларға көп көңіл бөледі.

Ыстық резерв шлюзінің конфигурациясы (Hot Standby Router Protocol (HSRP)) Коммутатор агрегациясы 1–ді контекст 1 үшін біріншілік,ал Коммутатор агрегациясы 2–ні контекст 2 үшін біріншілік болып бекітілген.

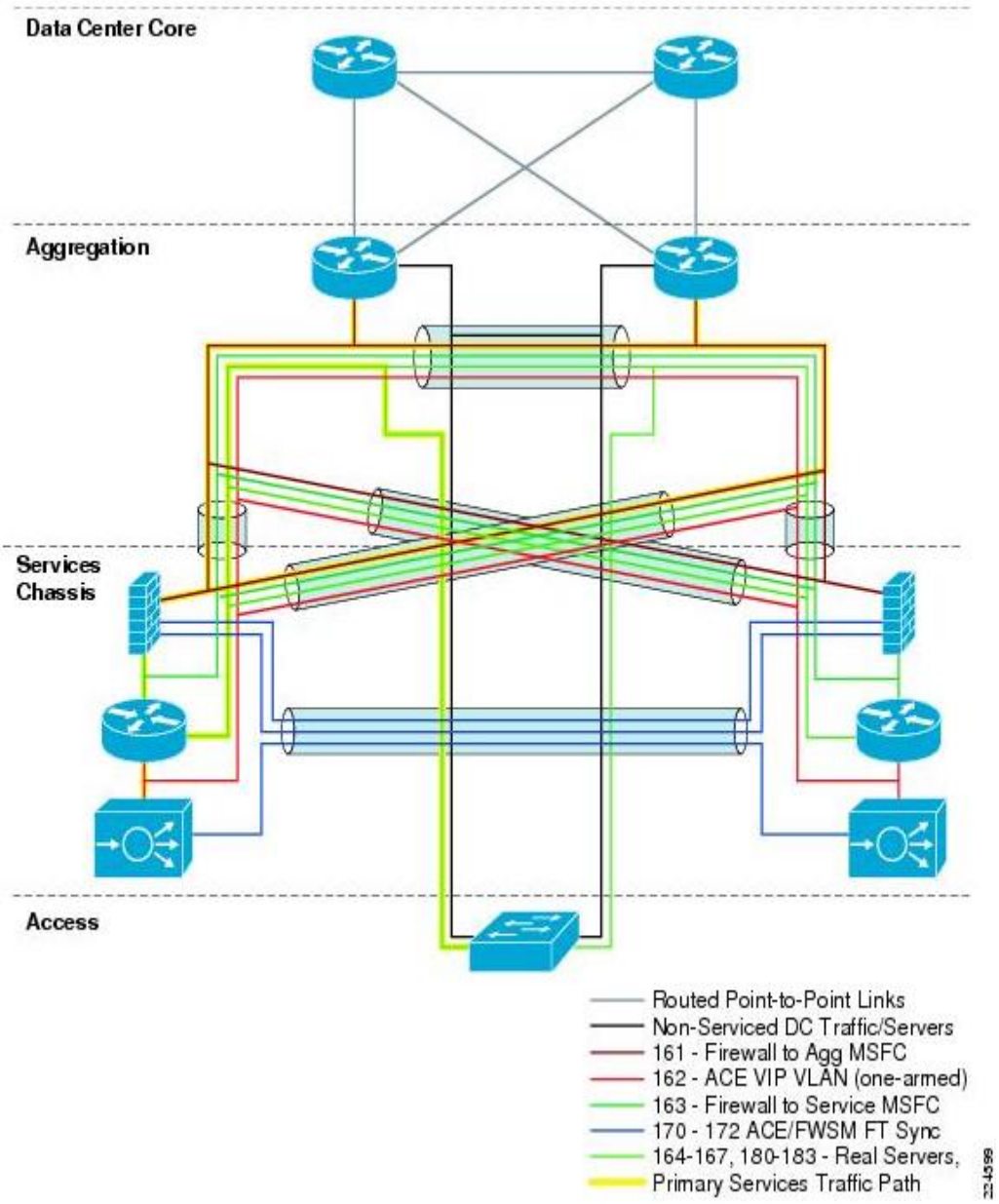
3.5.4 Активті/Күту режимі шасси жобалау қызметі

Шасси қызметінің активті/Күту режимі моделі енгізу, қолдау және кемшіліктерді жою ыңғайлылығы үшін жасалған қарапайым модель.

Ол қос қосылысты физикалық шасси қызметіне негізделіп жасалған 3.10 – суретте көрсетілген.

Сервисті модульдер арқылы қозғалыс ағынын бақылау үшін мліметті өңдеу орталығындағы қызметтің жасалуы қозғалыс ағынын мен VLAN желілері мен IP ішкі желілері секілді логикалық құрылымды мұқият жобалауды қажет етеді.

Активті/Күту режимі–нің логикалық архитектурасының физикалық инфраструктасын 3.10–суреттен көре аласыздар.

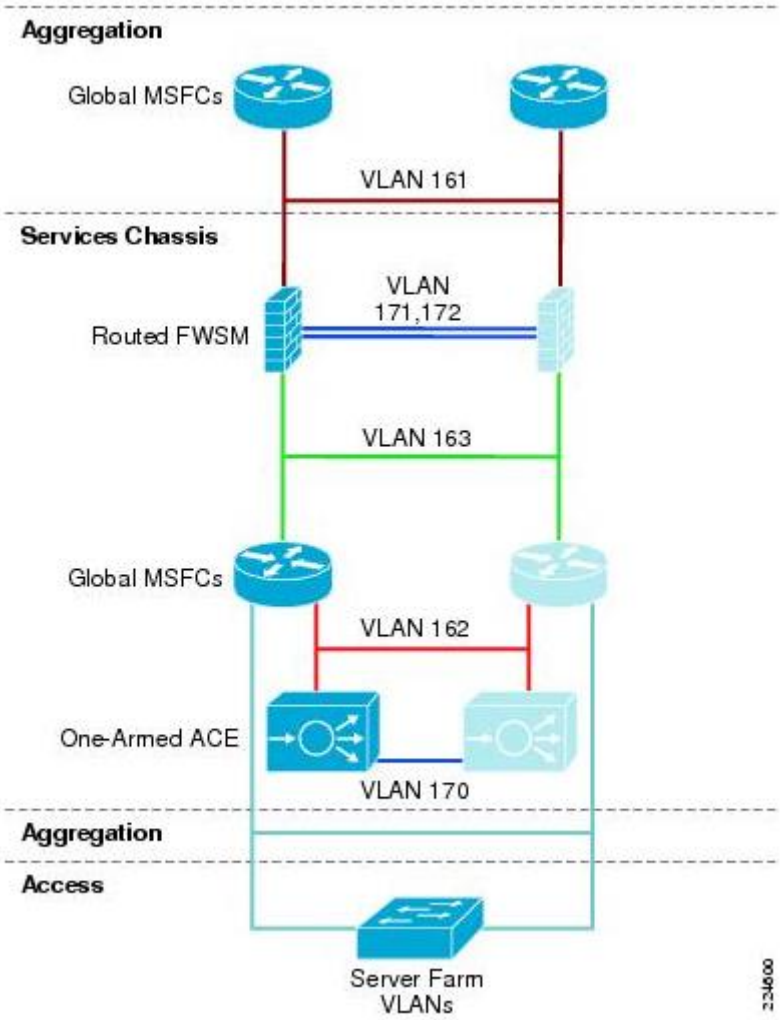


Сурет 3.10 – Актиті/Күту режимінің логикалық және физикалық комбинирленген көрінісі

Бұл топология арқыла трафик ағынын анализдеу үшін тура осы архитектураның логикалық құрылысын қарасақ болады (3.11–сурет).

Екі шасси қызметінің арасында кеңейтілген VLANжелісінің мәлімет жолы агрегация қабатынан сервердің екі бағыттық байланысы арқылы өту керек. Сервер мен клиент желісінің қосылу жолы болып табылатын VLAN–ның кіріс/шығыс желісі желінің Ядро қабаты мен Қолжетімділік қабатына қосылуы үшін Агрегация қабатынан өтуі керек. VLANs 163 және 162 секілді қызмет қабаттары арасындағы аралық VLAN желілері жұмыстан бас тарту болған жағдайларда трафиктегі қара тесіктердің алдын алу үшін таралады.

Бұл аралық VLAN желілері трафиктің жұмыстан бас тарту мен күй модуліне арналған шасси қызметіне тікелей байланыс болу үшін Агрегация қабатымен кесе көлденең таралады (3.11–сурет).



Сурет 3.11– Активті/Күтуші режимнің логикалық диаграммасы

Логикалық жобалау рамкасындағы әрбір виртуалды локальды желінің қысқаша талдамасы төменде келтіріледі. Бұл топологияда ешқандай мөлдір режим болмағандықтан, әрбір VLAN жеке IP ішкі желіге сәйкес келеді.

– FWSM –ға бағытталу үшін ғаламдық MSFC–тің агрегациясы. Бұл суретте VLAN 161 ретінде көрсетілген. Бұл VLAN шасси қызметі мен Агрегация қабаты арасында қос қосылыстпен физикалық байланысып таралады да, тұтынушы жағындағы қызмет модуліне трафиктің кіріс–шығысын қамтамасыз етеді.

– FWSM Fault Tolerance байланысы. Суретте ол VLAN 171 мен 172 ретінде көрсетілген. Екі шасси қызметі арсында бөлінген физикалық байланыс арқылы таратылады. Олар бас тартуға тұрақтылық пакеттерін, күй информацияларын алып жүреді және біріншілік және екіншілік FWSM–ға конфигурацияны теңгеріп тұруға мүмкіндік береді.

– Ғаламдық MSFC–тің шасси қызметіне маршрутизацияланған FWSM (Routed FWSM to Services Chassis Global MSFC's). Бұл суретте VLAN 163 ретінде көрсетілген. Бұл VLAN шасси қызметі мен агрегация қабаты арасында қос қосылысты физикалық байланыс арқылы тарайды. Сервер фермаларына тікелей осы байланыста трафикті бағыттау немесе VIP адрес тағайындау болса бірқолдық ACE модуліне бағыттауға MSFC шасси қызметі экспедиторлық рұқсат береді.

– Бірқолдық ACE–ге ғаламдық MSFC шасси қызметі (Services Chassis Global MSFC's to One–Armed ACE). Бұл суретте VLAN 162–мен көрсетілген. Бұл ACE модулімен қызмет жасалатын трафикке кіріс шығыс интерфейсі болып табылады.

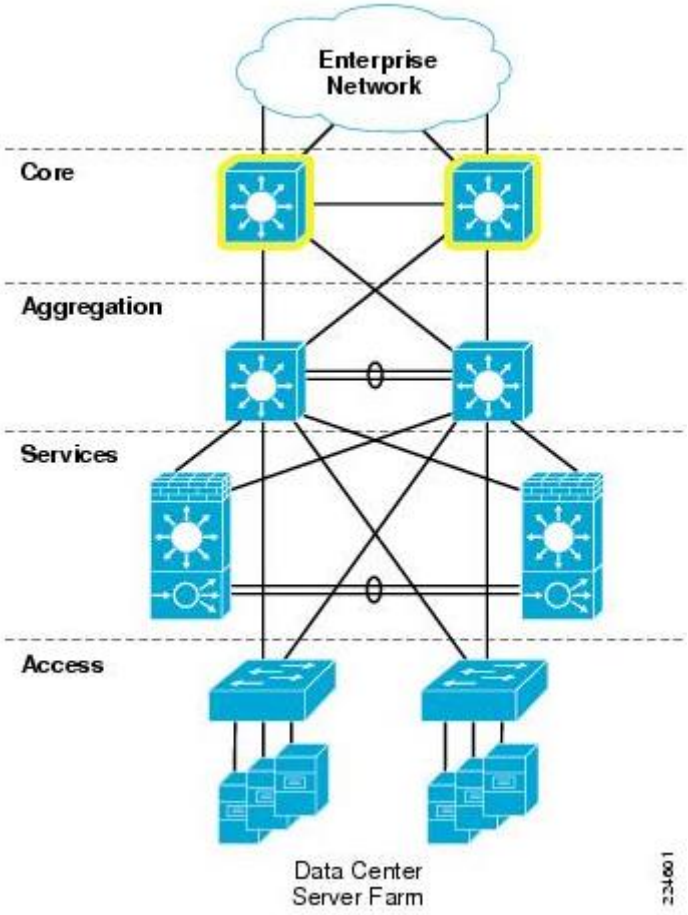
– ACE сервер фермаларына жіберілетін пакеттердің адрес көзін өзгертетін Source NAT–ты жасайды. Осылайшы, қайтып келетін пакеттер де ACE арқылы өтуі керек. Олардың адрес белгілеулері бастапқы сұраныс жіберген клиент түйініне қайта өзгертілуі осы жерде болады (ACE–да). Бұл VLAN шасси қызметі мен агрегация қабаты арасында қос қосылысты физикалық байланыспен жалғанады.

– ACE Module Fault Tolerance link. Бұл байланыс суретте VLAN 170–пен көрсетілген. Екі шасси қызметі аралығында бөлінген физикалық байланыс арқылы таралады. Бұл байланыс екі ACE модулі арасындағы баптауды теңгереді және трафиктерді өзімен алып жүреді.

– VLAN сервер фермалары үшін ғаламдық MSFC шасси қызметі (Services Chassis Global MSFC's to Server Farm VLANs). VLAN желілері «виртуалды локальды желі сервер фермаларына» ссылка ретінде қарастырылады. Бұл VLAN желілері агрегация қабатында қос қосылысты байлаыспен таралады. Серверге қосылысты қолдау үшін төменгі Қолжетімділік қабатына кеңейтілген. Тіректік топологияда әр түрлі қызмет түрлерін таситын VLAN–ның 8 түрлі желісі(дауыс, файеруолданған мәлімет, SLB мәлімет) бапталған. Айқындалған сан мен VLAN мақсаты осы тапсырыс берушілер үшін өзіндік айқындаған.

3.6 Ядро қабаты

Active–Standby шасси қызметі моделінің (Active–Standby Services Chassis) ядро қабаты бәрінен бұрын тұрақтылық пен Layer 3 IP–пакеттер переадресациясының жоғары өнімділігін арттыруға бағытталған. Ол агрегация қабатындағы мәлімет өңдеу орталығының Spanning Tree домендері мен желідегі басқа орындар арасындағы оқшауланған қабатты қамтамасыз етеді. Ол машрутизацияланған режимге бапталған екі Cisco Catalyst 6500 коммутаторлар мен Gigabit Ethernet или Gigabit EtherChannel–дің 10 интерфейсынан тұрады. Өндірістің кәсіптендірілген талабы мен масштабына байланысты мәлімет өңдеу орталығының ядро қабаты немесе campus, WAN/branch, немесе Internet edge секілді байланыс агрегация блоктары немесе басқа бөліктердегі бөлінген ядроны көрсетеді. Active–Standby шасси қызметі моделі ядро қабатындағы екі коммутатор 3.12–суретте бөлініп көрсетілген.



Сурет 3.12 – Ядро қабатының мәлімет орталығы

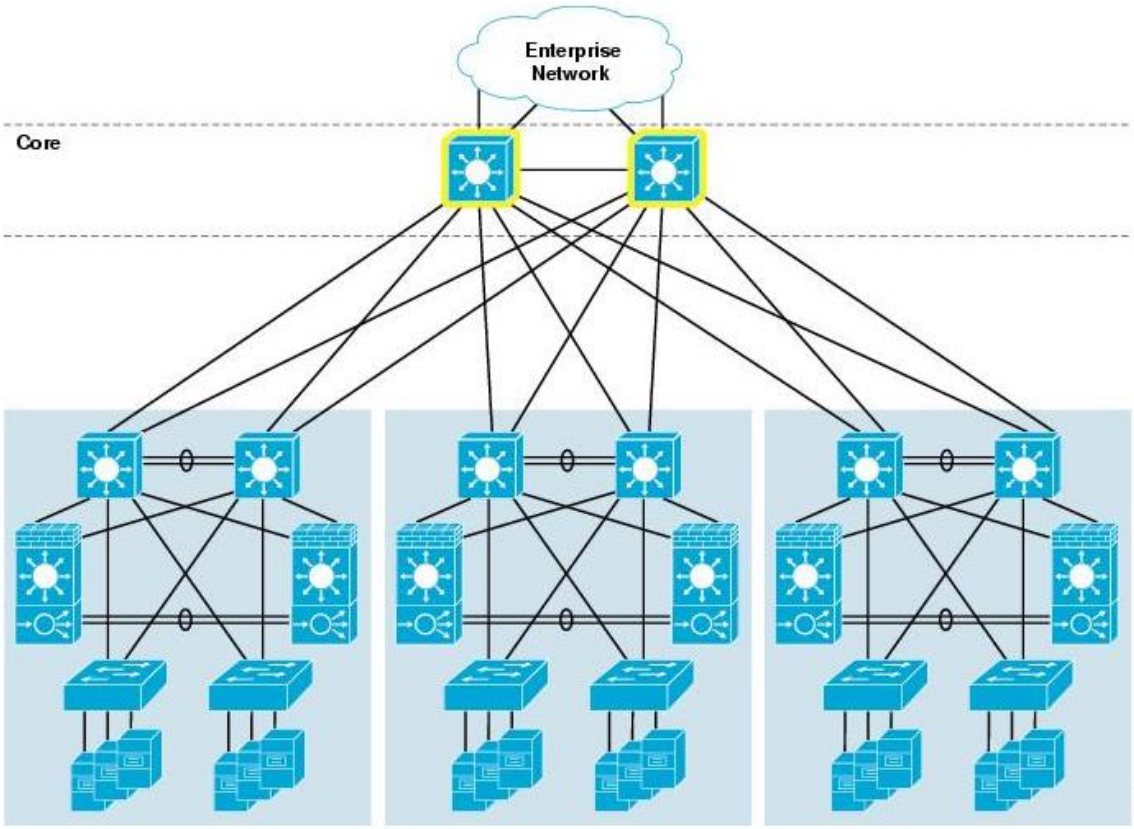
Мәлімет өңдеу орталығын масштабтау.

Ядро қабатындағы белгіленген мәлімет өңдеу орталықтары агрегация қабатындағы бірнеше блоктарды ашуға мүмкіндігі бар. Бұл мәлімет өңдеу орталығына Қолжетімділік қабатындағы коммутаторлардың көп санын қолдауға мүмкіндік береді.

Ол процесс көп сервер санын қолдауға әкелетін Аргегация қабатының порт санын көбейтуге жол ашады. Ол жерде сонымен қатар бірнеше агрегация блоктарын ашуға алып келетін желілік архитектор салдары эксплуатациялық факторларға алып келеді.

Мысалы, бірнеше бөлек бизнес бірліктері бар екі компания немесе өндіріс біріккен соң техникалық қызмет пен қауіпсіздік үшін құрылғыларды физикалық бөлуді талап етуі мүмкін[12].

3.13–суретте мәлімет өңдеу орталығы топологиялық желісінің бірнеше блок агрегациясы көрсетілген.



Сурет 3.13 – бірнеше агрегациялық блокпен мәлімет өңдеу орталығы ядросы

Егер бірнеше блок агрегациясы мәлімет өңдеу орталығының ядросына қосылған болса, ең жақсы тәжірибе –әрбір коммутатор агрегациясы рамкасында Layer 2 мен Layer 3 арасындағы шекараны сақтау. Бұл шекараны сақтау Қолжетімділік қабатындағы коммутаторлар үшін VLAN желілерін кеңейтуге мүмкіндік береді, бірақ агрегация деңгейіндегі блоктар шегінде ғана. Layer 2 тасымалдауы және Spanning Tree домендеріндегі жұмыстың тоқтатылуы тек осы агрегация блоктары шегінде болатын болғандықтан, бұл шешім үлкен тұрақтылықты қамтамасыз етеді.

Бірнеше агрегация блоктары бар мәлімет өңдеу орталығындағы шасси қызметін көркейту әрбір Агрегация қабатындағы коммутатор жұптарына бөлек шасси жұптарынан шектетілуі тиіс. Егер жұмыстың үлкен сыйымдылығы қажет болса, бірнеше шасси сервисі жұптары бір блок агрегациясынан қолданыла алады. Шасси қызметінің бір жұбын, дұрыс емес баптау болған жағдайда, екі Layer 2 домендерін қосуға әкеліп соғатын бірнеше агрегация блогына бермеуге ең жақсы практика. Жалпы, блок агрегациясының өткізу қуаты мына қызмет жиынтығынан біраз артық. Мәлімет өңдеу орталығын бірнеше агрегация блоктарына масштабтаған кезде, қызмет модулінің бірнеше жиынтығы ереже бойынша қажет болады.

4 Тіршілік қауіпсіздігі

4.1 Ауа кондиционерлеу жүйесінің құрылғысы және есебі

Дипломдық жобаның тақырыбы – «Trust company» ЖШС корпоративтік желісінің қауіпсіздігін бұлттық технология негізінде қамтамасыз ету. Бұл жоба кіші және үлкен бизнесті басқаруды жеңілдетудің ең қолайлы жолы болып табылады. Өміртіршілігі қауіпсіздігі бөлімінде оператор бөлмесі қарастырылады және әр жұмысшы үшін ыңғайлы еңбек шарртарын ұйымдастыру қажет.

Оператор бөлмесі 4.1–суретте көрсетілген. Бөлменің ұзындығы 20 м, ені 8 м және биіктігі 4 м, ұзындығы 2 м екі терезе бар. Бөлмеде 3 адам жұмыс істейді, жұмыс графигі – аптасына бес күн, күніне сегіз сағат. Дербес компьютер операторының жұмысы ұзақ көру жұмысымен байланысты болғандықтан, Оператор бөлмесіндегі жарықтануды есепке алу қажет. Жарықтану деңгейі психикалық функциялардың күйіне және ағзадағы физиологиялық үрдістерге әсер етеді. Бөлме компьютерлік құрылғылар мен оргтехникамен жабдықталған, сол себептен Оператор бөлмесінің персоналы артық жылулық сәулеленуге шалдығады. Сондықтан персоналдың қолайлы еңбек ету шарттарын қамтамасыз ету үшін микроклимат параметрлерін нормалау қажет. Микроклиматтың бөлек параметрлерінің ұсынылған мәндерінен ауытқуы жұмысшының еңбекке қабілеттілігін төмендетеді, көңіл күйін нашарлатады және кәсіби ауруларға әкелуі мүмкін. 4.1–кестеде ГОСТ 12.0.003–88. ССБТ сәйкес категориясы I а жеңіл физикалық жұмыс үшін қалыпты микроклиматтық шарттар келтірілген. Оператор бөлмесіндегі жаз уақыт кезіндегі температура +26°С–ге дейін көтеріледі, ал қыс кезіндегі температура +18-ден +20°С-ге дейін. Қажетті микроклиматтық шарттарды сақтау үшін бөлме кондиционермен жабдықталған. Бөлменің терезелер арқылы түсетін табиғи жарықтануы, және тәуліктің қараңғы уақытында жұмыс істеу мүмкіндігін беретін жасанды жарықтануы бар. Жасанды жарықтану жоғары дәлдікті көру жұмысының III, а разрядының талаптарына сәйкес келеді. Жасанды жарықталу люминесцентті шамдар арқылы жүзеге асырылады. Қызмет көрсетушілердің қауіпсіздігін қамтамасыз ету үшін бөлме қызметкерлеріне әсер ететін барлық мүмкін факторларды талдау қажет. Бөлмеде құрылғылардың мынадай түрлері қолданылады:

Дербес компьютерлер саны – 5. Зиян электрмагнитті сәулелердің әсері оларды операторлардан алысырақ орналастырудан және дербес электрондық есептеуіш машина (ДЭЕМ) мониторына қорғаныс экранын орнатудан төмендейді. Газдылықтың, шаңдылықтың және қондырғының изоляциясынан туындайтын зиян булардың әсері табиғи желденуді қамтамасыз ететін құрылғыларды дұрыс орналастыру есебінен жойылады. Көрермен залы мен дыбыстық қамтамасыз етудің аппараттық бөлмесі арасындағы әуе шуының изоляция индексі 50 дБ–ден кем болмауы керек. Дыбысты қамтамасыз етудің

аппараттық бөлмесінің қабырғалары мен төбесі 500 – 2000 Гц жиіліктер диапаонында дыбысты жұту коэффициенті 0,6–дан кем болмайтын дыбысты жұтқыш материалдармен қапталуы керек. Дыбысты қамтамасыз ету жүйесінің барлық техникалық аппараттық бөлмелерінің едендері шаң тудырмайтын болмауы және күнделікті ылғалды жинастыру жұмыстарын өткізуге мүмкіндік беретін (метлах тақтасы, линолеум) болуы керек.

Дербес электрондық есептеуіш машина қолданушысының жұмыс орнын ұйымдастыруда келесі негізгі талаптар сақталуы қажет:

– жұмыс орнының құрамына кіретін құрылғылардың оптималды орналасуы;

– барлық қажет қозғалыстар мен орын ауыстыруларды жүзеге асыруға мүмкіндік беретін жеткілікті жұмыс аймағы;

– қызметтерді іске асыру үшін табиғи және жасанды жарықтандыру қажет;

– акустикалық шудың деңгейі рұқсат етілген мәнінен аспауы керек.

Бөлмеде келесі құрал-жабдық қолданылады:

1) Дербес компьютер – 5 дана.

Құрылғының техникалық сипаттамалары:

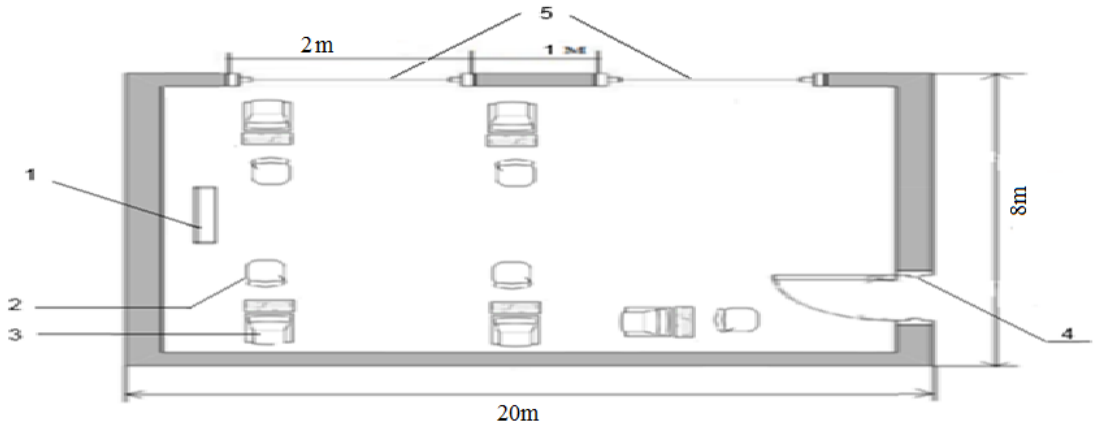
– Samsung dx2300 Intel Core i5 3210/4Gb/500Gb/Combo/DOS дербес компьютері;

– SAMSUNG LS19A100N мониторы;

– мөлшерлер1200х750х1150 мм (дербес компьютер + үстел);

– электрлік қоректену көзі: айнымалы кернеу 220-250 В, 50 Гц жиілігі, қуаты 400 Вт.

2) Сплит-жүйе плазма Sony NT/PS-3 25 NKDW– кондиционер, қуаты 15кВт.



Сурет 4.1 – Оператор бөлмесі: 1–кондиционер, 2–орындық, 3–үстел және дербес компьютер, 4–есік, 5–терезе

К е с т е 4.1 − Микроклимат параметрлерінің қалыпты нормалары

Жыл мезгілі	Жұмыс категориясы	Температура, °С	Ауа қозғалысының жылдамдығы, м/с
Салқын	I а	18–26	0,1
Жылы	I а	20–30	0,2

Операторлар бөлмесінің микроклиматтық шамалары: жыл мезгілінің суық кездерінде ауа қозғалысының жылдамдығы және салыстырмалы ылғалдылығы 0,1 м/с, 60% ауа тепературасы 18–26ºС шамасында болады.

Ал жыл мезгілінің жылы кездерінде ауа қозғалысының жылдамдығы және салыстырмалы ылғалдылығы 0,2 м/с, 60–70%. Келтірілген шамалар адам организміне ыңғайлы нормаларға сай келмейді. Сондықтан операторлар бөлмесінде ауаны кондицианерлеу мәселесі қарастырылған.

Адамның электр тогынан зақымдану ықтималдығына әсер ететін біздің бөлмеміздің класын анықтайық:

– едендер бір қабатты поливинилхлоирдті антистатикалық линолеуммен қапталған, сондықтан ол ток өткізбейтін болып табылады;

– ауаның салыстырмалы ылғалдылығы 60%-дан аспайды, сондықтан бөлме құрғақ;

– ауа температурасы Цельсий бойынша плюс 30 градустан аспайды;

– адамның бір уақытта бір жақтан жермен байланысы бар технологиялық жабдықтардың корпустарымен және басқа жерлендірілген бөліктермен, екінші жақтан электр жабдықтарының металл корпустарымен немесе ток өткізуші бөліктермен жанасу мүмкіндіктерінің болмауы (кернеу 1000В мәнінен аспағандықтан сымдардың өте жақсы изоляциясында);

– химиялық белсенді заттар жоқ.

ГОСТ 12.1.013-78.ССБТ сәйкес осы бөлмені маңызды қаупі жоқ бөлме ретінде классификациялауға болады.

Біздің жағдайымызда электр қауіпсіздігін қамтамасыз ету үшін ГОСТ 12.1.030–81 бойынша жерлендіру мүмкіндігін қарастыру қажет. Біздің жағдайымыздағы кернеу – 220В, сондықтан жерлендіру мен нөлдеу міндеттелмейді, бірақ ұсынылады.

Құрылыс конструкцияларын дайындау үшін кірпіш, темір бетон, әйнек, металл және басқа жанбайтын материалдар қолданылады.Сонымен қатар жанбайтын материалдардан жасалған қоршаулар түріндегі өртке қарсы өткелдерді ескеру қажет, олар біздің офистің бөлмелері арасында орнатылады. Ғимараттарда өрт крандары дәлістерде, баспалдақ торларында және кіре беріс аумақтарында орнатылады. Дербес электрондық есептеуіш машинаны қолданушылар бөлмелерінде, архивте және қосымша, қызметтік бөлмелердегі өртті өшіру үшін су қолданылады. Дербес электрондық есептеуіш машина бар бөлмелерде, ақпаратты тасушыларды сақтау бөлмелерінде, қымбат құрылғыларды бұзу немесе толықтай істен шығару қаупінен бақылау-өлшеуіш жабдықтары бар бөлмелерде суды қолдану тек кейбір жағдайларда ғана рұқсат

етіледі, мысалы өрт қауіпті ірі көлмеде болғанда. Бірақ судың мөлшері минималды болуы және дербес электрондық есептеуіш машинаны, дыбыстық құрылғыларды брезентпен немесе матамен жауып судан қорғау керек. Барлық бөлмелерді стационарлы автоматты өрт өшіргіш қондырғылармен жабдықтау қажет. Ауа құрамындағы оттегіні тез азайтатын от өшіргіш газбен бөлмені бірден толтыруға негізделген өртті газбен өшіру қондырғыларын қолданған тиімдірек болып табылады. Зиян химиялық заттардың деңгейін нормалау. Бөлмені ластау көздері сыртқы ортаның және ғимараттың құрылыс материалдарынан, жиһаздардан, киімнен, аяқ-киімнен бөлінетін жүздеген әрекеттесулердің зиян заттары және адамның биоактивті әрекеттесулері (антропотоксиндер) болып табылады.

Бөлменің сыртқы ортаның зиян заттарымен ластануын қарастыра отырып, ең алдымен ғимараттың орналасқан орнын ескеру қажет, біздің жағдайымызда ол автострадаға жақын орналасқан. Бөлмеге сыртқы ортадан келетін жиі ластағыштар көміртек оксиді, азот диоксиді, күкірт диоксиді, қорғасын, шаң және тағы басқалары болып табылады.

Құрылыс конструкциялары бөлменің радон және торонмен ластануын көзі болып келеді, сонымен қатар ең көбірек концентрация нашар желдетуі бар бетоннан жасалған үйлерде кезедеседі.

Жиһаз, киім және аяқ-киімдер минералды талшықты, көмір сутегісі, полиэфир қара майы және тағыбасқа зиянды заттары бар шаңды бөледі. Биоктивті әрекеттесулердің ең маңыздысы көміртек диоксиді, күкірт сутегісі және тағы басқалары болып табылады.

Дербес электрондық есептеуіш машина қолданушысының, оператордың, жұмыс орнындағы шу көздері – сөйлесіп тұрған адамдар, сыртқы ортаның – компьютердің, принтердің, желдеткіш қондырғының шуы болып табылады. Олар болмашы мәнде шуды тудырады, сондықтан бөлмеде дыбысты жұтқыштарды қолдану жеткілікті.

Ең жақсы дыбысты жұту қасиеті талшықты-ауа көлемді материалдарда: фибролитті плиталарда, жарықталшықтарында, минералды мақтада, полиуретанды поропластта, ауа көлемді поливинилхлоридте және басқаларында болады. Дыбыс жұтқыш материалдарға дыбыс жұту коэффициенті 0,2 мәнінен төмен емес материалдар жатады.

Дербес электрондық есептеуіш машинамен жұмыс істеуге арналған бөлменің тиімді жарықтандырылуы табиғи және жасанды жарықтың болуы есебінен жасалады.

Жеткіліксіз жарықтандыру көздің, адамның тез шаршауына, жақыннан көргіштікке, жұмыс сапасының төмендеуіне, ақаудың көбеюіне соқтырады. Тым жарық көз қабықшасын тітіркендіреді, шағылыстырады, көз тез шаршайды, өндірістік травматизм көбейеді.

Қаралып жатқан бөлмеде жұмыс істеуге қажетті жарықтандыру қалып бойынша Ен=300 лк,осылайша бөлмедегі қажетті жарықтандыруды қамтамасыз етеміз.

Жұмыс бөлмесінде белсенді кондицианерлеу және вентиляция жүйесі жоқ. Операторлар залын талдау барысында жұмыс аумағының қалыпты микроклиматтық шарттарын міндетті түрде қарастыру қажет. Мұндай әмбебап жүйе ретінде автономдық кондиционерлер болып табылады.

ГОСТ 12.1.005–88 ССБТ "Жұмыс істеу аймағының ауасы, жалпы санитарлы-гигиеналық талаптар" сәйкес, компьютерлермен жабдықталған бөлмедегі адамдардың жұмысы жеңіл физикалық жұмысқа жатады. Ағзаның энергия жұмсау жұмыстарының категориялары 5.2 – кестеде келтірілген.

Кесте 4.2 – Адам ағзасының энергия жұмсау жұмыстарының категориялары

Жұмыс	Категория	Ағзаның энергия жұмсауы, Ккал/сағ, Дж/с	Жұмыс сипаттамасы
Жеңіл	I а	<138	Жұмыс отырып жүргізіледі

4.2 Кондиционерлеу және ауаны жаңарту жүйелерін есептеу

Ауаны технологиялық кондиционерлеудің талаптары өнеркәсіптің әр түрлі салаларындағы технологиялық процестерді жүргізуде, сондай-ақ компьютерлік жабдықтың, басқа құралдар мен аспаптардың және т.б. жұмыс қабілеттілігін қамтамасыз ету үшін ауа ортасының белгілі бір параметрлерін (ауаның температурасын, ылғалдылығын және қозғалысын) өндіріске сай қолдауға негізделеді. Өзінің тағайыны бойынша кондиционер жүйесі қолайлы және технологиялық болып бөлінеді. Қолайлы жүйелер үйлесімді санитарлық-гигиеналық талаптарға жауап беретін ауаның температурасын, ылғалдылығын, тазалығы мен қозғалыс жылдамдығын жасау және автоматты қолдау үшін тағайындалады. Кондиционердің технологиялық жүйелері белгілі бір өндірістік және технологиялық процесс талаптарына басым дәрежеде жауап болатын ауа параметрлерін қамтамсыз ету үшін тағайындалады.

Аумағы 15–тен 140 м^2 дейінгі тұрғын және қоғамдық бөлмелерде сплит–жүйе кондиционерлері кең таралуда. Олар сыртқы блоктан (компрессорлы-конденсаторлы) және ішкі блоктан (буландырғыш) тұрады. Сыртқы блок ғимарат қабырғасына,шатырға немесе шатыр астына, қосалқы бөлмеге, балконға, яғни ыстық конденсатор төменірек температурасы бар атмосфера ауасымен салқындатылатын жерге орнатылуы тиіс. Ішкі блок тікелей кондиционерленетін бөлмеге орнатылады және ауаны салқындату немесе жылыту, сүзу және бөлмедегі ауаның қажетті қозғалысын жасау үшін тағайындалады. Ішкі блоктар берілген температураны ұстайды және бөлмедегі ауаның тең бөлінуін қамтамасыз етеді және шусыз жұмыс істейді (шу деңгейі 35–38 дБ). Кондиционерленген ғимараттың жылулық және ылғал теңгерімін белгілі әдістермен орындалады. Мұнда ғимараттың ауа ортасының қалпы өзгеруіне әкеп соғатын, барлық факторлар есепке алынуы керек[14].

Кондиционерді таңдау үшін алдымен артық жылудың қосындысын, сонымен қатар оған күннің радиациясынан бөлінетін жылу кіреді, өндірістік жарықтануды, жұмыс істейтін адамдар санын, оргтехникаларды және т.б. есептеу қажет. Салқын өндіргіштік бойынша қосындысы сондай немесе шамалы үлкен мәнді, сонымен қатар қажетті ауа алмасу қамтамасыз ететін кондиционер моделі таңданылады.

Бөлмедегі жылулық баланс мына формуламен есептелінеді:

$$Q_{жылу.б} = Q_{қоршау} + Q_р + Q_а^а + Q_{жарықтану} + Q_{құрал}, Вт \quad (4.1)$$

мұнда $Q_{қоршау}$ – температура айырымы нәтижесінде алынатын жылу және жылу жоғалту;

$Q_р$ – шынылау арқылы күннің сәулеленуінен келетін жылу;

$Q_а^а$ – адамдардан келетін жылу түсу;

$Q_{жарықтану}$ – жарықтандыру аспаптарынан келетін жылу;

$Q_{құрал}$ – оргтехника және құрылғылардан келетін жылу.

4.3 Температура айырымы нәтижесінде алынатын жылу және жылу жоғалту

4.3.1 Әйнек арқылы күннің радиациясынан түсетін жылу

Күннен бөлінетін жылу әйнектің түріне байланысты 90%-ға дейін бөлме ортасымен жұтылады, қалған бөлігі шағылысады. Ең үлкен жылу жүктемесі тура және шашырай түсетін күн сәулесінің ең үлкен деңгейінде алынады. Сәуле түсу қарқыны жергілікті кеңдікке, жыл мезгіліне және тәулік уақытына байланысты.

Салқын мезгіл үшін есептік сыртқы температура ($t_{сырт.есеп}$) ең салқын айдың 13 сағатындағы орташа температурасына, жылы период үшін – ең ыстық айдың 13 сағатындағы орташа температурасына сәйкес келеді. Ал ішкі ($t_{іш.есеп}$) жайлылық шартын және өндірістік процесстерде көрсетілетін технологиялық талаптарын ескере отырып таңдалады:

$$Q_{қоршау} = V_{бөлме} X_0 (t_{шыққан} – t_{келген}), Вт \quad (4.2)$$

мұнда $V_{бөлме}$ – бөлменің көлемі, $м^3$. $V_{бөлме}$=20 х 8 х 4 = 640 $м^3$;

$X_о$ – меншікті жылулық сипаттама, $Вт/м^3\ ^оС$;

$X_о$ = 0,42 $Вт/м^3\ ^оС$;

$t_{сырт.есеп}$ = 27,6° – жылдың жылы мезгіліне арналған сыртқы есептік температурасы;

$t_{сырт.есеп}$ = –25° – жылдың суық мезгіліне арналған сыртқы есептік температурасы;

$t_{іш.есеп}$ = 24° – жылдың жылы мезгіліне арналған ішкі есептік температурасы;

$t_{іш.есеп}$ = 20° – жылдың суық мезгіліне арналған ішкі есептік температурасы.

Жылы мезгіл үшін:

$Q_{қоршау}$ = 640 х (27,6 – 24) х 0,42 = 967,68Вт.

Салқын мезгіл үшін:

$Q_{қоршау}$ = 640 х 0,42 х (– 25 – 20)= –12096Вт.

4.3.2 Шынылау арқылы күннің сәулеленуінен келетін жылу

Күннің сәулеленуінен (радиация) келетін жылу терезе арқылы сәуле бөлмеге кіріп, күннен шынылау сәулелену периоды үшін:

$$Q_р = (q_{тура} + q_{шашыр.})\ К_1^{с}\ К_2\ ß_{ж.ө.} n\ H_0\ B_0,\ Вт \qquad (4.3)$$

Күннің сәулелері терезеден кірмейтін көлеңке периоды үшін (шашыраңқы радиация):

$$Q_{р\ .} = q_{шашыр.}\ К_1^{Т}\ К_2\ ß_{ж.ө.} n\ H_0\ B_0,\ Вт \qquad (4.4)$$

мұнда $q_{тура}$; $q_{шашыр.}$ − тура және шашыраңқы радиациядан келетін жылулық ағындар, Вт/м^2;

$F_о$ = n H_0 B_0 – жарықтық ойықтың ауданы, м^2 (n – терезелердің саны, биіктігі H_0 және ені B_0);

$К_1$ – қапсырмамен шынылаудың көлеңкелену коэффициенті ($К^с_1$ – сәулеленген ойықтар үшін; $К_1^{Т}$ – көлеңкедегі ойықтар үшін);

$К_2$ – шынылаудың ластану коэффициенті;

$ß_{ж.ө.}$ – жылу өткізу коэффициенті.

1) Оператор бөлмесіндегі шынылаудың ауданы, 44^0 солтүстік-шығыс (СШ) [12, кесте 3] F_0 = 2 х 2,5 х 2 = 10 м^2.

2) Шынылаудың бағыты: оңтүстік-шығыс (ОШ).

3) Ішінде жарық перделері бар. $ß_{ж.ө.}$= 0,4 [12, кесте 4] деп қабылдаймыз.

Түске дейін ОШ үшін, яғни сағат 9–дан 12–ге дейін 44^0 СШ ендікте тура радиацияның мәні (П) $q_{тура}$ = 387 Вт/м^2 және шашыраңқы радиацияның мәні (Р) $q_{шашыр.}$ = 101 Вт/м^2 тең [12, кесте 5]. 44-68 ^{0}СШ ендік диапозонында металды қапсырмалы екі қабатты шынылау үшін: $К_1$ = $К_1^{С}$ = 0,72, егер ойық күнмен сәулеленген болса, яғни 9–10 және 13–14 сағат аралығындағы период үшін. $К_1$ = $К_1^{Т}$ = 1,15, 14–15 және 19–20 сағат аралығында болады. Әйнектің бірқалыпты ластануы коэффициенті $К_2$ = 0,9 қабылданады.

Тура сәулелену периодында 9 бен 14 сағат аралығында жүреді

$Q_р$ = (387 + 101) х 0,72 х 0,9 х 10 х 0,4 = 1265 Вт,

ал көлеңкелену периодында 14 пен 20 сағат аралығында жүреді

$Q_р$ = 22 х 1,15 х 0,9 х 10 х 0,4 = 91 Вт.

Максималды есептелу уақыты: 9–10 сағат, жылу түсу 1265 Вт.

4.3.3 Адамдардан келетін жылу

Адамдардан түсетін жылу қоршаған ауа параметрлеріне және орындалатын жұмыс қарқынына байланысты. Адам бөлетін жылу ауаға конвекция арқылы сезілетін және өкпеден, теріден бөлінетін байқалмайтын жылудан тұрады. Адамдардың жылу таратуы 4.3 – кестемен сипатталады:

К е с т е 4.3 - Адамның сыртқы ортаға жылу таратуы

Сыртқы орта температурасы ^{o}C	Отырғандағы жағдай			Тұрғанда немесе жеңіл қозғалыс			Ауыр жұмыс		
	Анық	Жасырын	Жалпы	Анық	Жасырын	Жалпы	Анық	Жасырын	Жалпы
22	76	26	102	84	48	132	117	132	249

Бөлмеде 5 әйел адам-операторлар отырады. t = 24 ^{0}C температурада отырған күйде бір ер адам 67 Вт анық жылу, ал жалпы – 102 Вт жылу бөледі [12, кесте 8]. Әйел адам ересек ер адамның жылу бөлу нормасының 85 %-ын, ал кішкентай бала– 75 %-ын бөледі деп саналады. Бөлмедегі адамдардың бөлетін анық жылуы: $Q_a^{а}$ = 67 х 5 х 0,85 = 288 Вт. Ал жалпы жылу:

$Q_a^{ж}$ = 102 х 5 х 0,85 =434 Вт.

t = 20 ^{0}C температурада бір ер кісі 82 Вт анық жылу және 103 Вт жалпы жылу бөледі [12, кесте 8]. Бөлмедегі адамдардың бөлетін анық жылуы:

$Q_a^{а}$ = 82 х 5 х 0,85 = 349 Вт.

Ал жалпы жылуы: $Q_a^{ж}$ = 103 х 5 х 0,85 = 438 Вт.

t = 24 ^{0}C үшін ылғалдылық және көміртегі қышқылының мәндерін 9-кестеден [12] интерполяция жолымен табамыз: бір адамнан 50 г/сағ ылғалдылық, 45 г/сағ көміртегі қышқылы бөлінеді. Ал 5 адамның ылғалдылығы 5 х 50 = 250 г/сағ, көміртегі қышқылы мөлшері 5 х 45 = 225 г/сағ құрайды .

t = 20 ^{0}C үшін: 1 адамнан бөлінетін ылғалдылық – 40 г/сағ, көміртегі қышқылы – 45 г/сағ. 5 адамнан бөлінетін ылғалдылық: 5 х 40 = 200 г/сағ.

5 адамнан бөлінетін көміртегі қышқылы мөлшері: 5 х 45 = 225 г/сағ.

К е с т е 4.6 – Бөлмедегі адамдардан бөлінетін зиянды заттардың есептелуінің нәтижелері

Жыл мезгілі	Температура ^{0}C	Жылу, Вт		Ылғалдылық,W г/сағ	CO_2 г/сағ
		$Q_a^{а}$	$Q_a^{ж}$		
Жылы	24	288	434	250	225
Салқын	20	349	438	200	225

4.3.4 Жарықтану аспаптарынан, оргтехникадан және құрылғылардан келетін жылу

Шамдардан келетін жылу мына формуламен есептеледі:

$$Q_{жарықтану} = \eta N_{жарықтану}, Вт \quad (4.5)$$

мұнда η - электр энергиясының жылулыққа ауысу коэффициенті.

Люминесцентті шамдарды қолдану кезінде η = 0,5–0,6;

$N_{жарықтану}$ – шамдардың орнатылған қуаты 65 Вт/м^2;

Оператор бөлмесінің еденінің ауданы $F_{еден}$ = 20 х 8 = 160 м^2;

$Q_{жарықтану}$ = 0,6 х 65 х 160 = 6240 Вт.

Оргтехниканың әсерінен пайда болатын жылу ағыны бір компьютерге орташа есеппен 300 Вт алады. Оператор бөлмесінде 5 дербес компьютер болғандықтан:

$Q_{құрал}$= 5 х 300 = 1500 Вт.

Орындалған есептеулерден формула бойынша оператор бөлмесіне келетін жылу балансын құрамыз. Жылдың жылы мезгілінде: температура айырымы нәтижесінде келетін жылу $Q_{қоршау}$ = 218 Вт; күн радиациясынан $Q_р$ = 1265 Вт; адамдардан $Q_а^а$ = 349 Вт; жарықтану аспаптарынан $Q_{жарықтану}$ = 1872 Вт; оргтехника мен құрылғылардан $Q_{құрал}$ = 1500 Вт. Оператор бөлмесінің жылулық балансы жазда:

$$Q_{жылу.б} = Q_{қоршау} + Q_р + Q_а^а + Q_{жарықтану} + Q_{құрал} \quad (4.6)$$

$Q_{жылу.б}$ = 1265 + 288 + 968 + 6240 + 1500 = 10260.68 Вт=10,261кВт.

$Q_{жылу.б}$ = 10,261х 3600 = 36938.45 кДж/сағ құрайды.

Жылдың салқын мезгілінде: температура айырымы нәтижесінде жоғалатын жылу $Q_{қоршау}$ = – 2722 Вт; күн радиациясынан келетін жылу $Q_р$ = 1265 Вт; адамдардан $Q_а^а$ = 349 Вт; жарықтану аспаптарынан $Q_{жарықтану}$ = 1872 Вт; оргтехника және құрылғылардан $Q_{құрал}$=1500 Вт. Оператор бөлмесінің жылулық балансы қыста:

$$Q_{жылу.б} = Q_{қоршау} + Q_р + Q_а^а + Q_{жарықтану} + Q_{құрал} \quad (4.7)$$

$Q_{жылу.б}$ = 1265 + 349 – 12096 + 6240 + 1500 = -2742 Вт=-2,742кВт.

$Q_{жылу.б}$ = -2,742 х 3600 = -9871.2 кДж/сағ құрайды.

4.4 Ауа алмасуды есептеу

$Q_{жылу.б}$ жазда > $Q_{жылу.б}$ қыста болғандықтан, $Q_{жылу.б}$ жазда мәнімен ауаның жылу кернеулігін мына формуламен есептейміз:

$$Q_к = \frac{Q_{жылу.б} \cdot 860}{V_{бөлме}} = \frac{10.26 \cdot 860}{8 * 20 \cdot 4} = 13.78779 \frac{ккал}{м^3} \quad (4.8)$$

$Q_{н.}$ <20 ккал/м^3 болғанда $\Delta t = 8^0 C$.

Бөлмеге қажет ауаның мөлшері жылулық баланстан алынып, мына формуламен анықталады:

$$L = \frac{Q_{жылу.б} \cdot 860}{C \cdot \Delta t \cdot \gamma} = \frac{10.26 \cdot 860}{0,24 \cdot 8 \cdot 1,206} = 3810.887\ м^3/сағ \quad (4.9)$$

мұнда С = 0,24 ккал/кг$^0 C$ – ауаның жылу сыйымдылығы;

γ = 1,206 кг/м^3 – ағынды ауаның сыбағалы массасы.

Кондиционердің техникалық сипаттамалары:

– қалқын 9,20 кВт; жылу 15,80 кВт;
– қорек кернеуі 220В, 50 Гц;
– салқынның жұмсайтын қуаты, кВт 1,47;
– жылудың жұмсайтын қуаты, кВт 1,54
– салқын/жылу жұмыс тогы, А 2,3 /3,1;
– EER, А 4,36 ;
– COP, А 4,41;
– жылдық ток пайдалануы 940 кВт*сағ;
– шудың деңгейі, ішкі (жоғ/орт/төм), дБ(А) 40/30/28;
– шудың деңгейі, сыртқы, дБ(А) 47;
– габаритті өлшемдері, Ш/В/Г, Ішкі, мм 400*1270*540;
– габаритті өлшемдері, Ш/В/Г, сыртқы, мм 965*785*230;
– салмағы, кг 25.

Қорыта келгенде барлық артық жылулар 18515 кДж/сағ құрайды, немесе 18515 : 3600 = 5,1 кВт. Бөлмеге қажетті ауа мөлшері L = 1910 м^3/ч=31,8м^3/мин. Өз таңдауымызды Sony NT/PS-3 25 сплит-жүйесі кондиционеріне тоқтатамыз.

4.5 Тіршілік қауіпсіздігі бөлімі бойынша қорытынды

Менің дипломдық жұмысымның тіршілік қауіпсіздігі бөлімінде жұмыс орнының ауа кондиционерлеу жүйесінің есептеп қаншалықты дәрежеде қажет екендігін анықтаймын. Жұмысшының жұмыс белсендігіне тікелей әсер ететін факторлардың бірі болып табылатын температура айырымы мен жылу жоғалту жөнінде есептеулер жүргіздім.

Операторлар бөлмесінің микроклиматтық шамалары: жыл мезгілінің суық кездерінде ауа қозғалысының жылдамдығын және салыстырмалы ылғалдылығын, ауа тепературасы шамасын анықтадым.

Ал жыл мезгілінің жылы кездерінде ауа қозғалысының жылдамдығы және салыстырмалы ылғалдылығы 0,2 м/с, 60–70%. Келтірілген шамалар адам

организміне ыңғайлы нормаларға сай келмейді. Сондықтан операторлар бөлмесінде ауаны кондицианерлеу мәселесін қарастырдым.

Маңызды мәселелердің бірі, кондиционерді таңдау үшін алдымен артық жылудың қосындысын, сонымен қатар оған күннің радиациясынан бөлінетін жылу, өндірістік жарықтандыруды, жұмыс істейтін адамдар санын, оргтехникаларды есептеу қажет. Септеу барысында жылы мезгіл үшін: $Q_{қоршау}$ = 967,68Вт тең болса, салқын мезгілде -12096Вт сәйкес келді.

Шынылау арқылы күннің сәулеленуінен келетін жылудың максималды есептелу уақыты, яғни 9-10 сағат ұзақтығында жылу түсу 1265 Вт екенін анықтадым. Осы мәлеметтерге сүйене отырып, оператор бөлмесінің персоналы артық жылулық сәулеленуге шалдығатындығын көреміз.

Қорыта келгенде барлық артық жылулар 18515 кДж/сағ құрайды. Бөлмеге қажетті ауа мөлшері L = 1910 $м^3$/ч=31,8$м^3$/мин. Осы талаптарды толық қанағаттандыратын Sony NT/PS-3 25 сплит-жүйесі кондиционеріне таңдадым.

5 Бизнес– жоспар

5.1 Жобаның мақсаты мен міндеттері

Бұлттық есептеулер – қолданушыларға өз компьютерінің жұмыс істеу қабілетіне, оның бағдарламалық қамтамасының мүмкіндігіне тәуелді болмауға мүмкіндік беретін ең заманауи сервис. Қарапайым сөзбен айтар болсақ, тұтынушы өз компьютерінде белгілі бір бағдарламаны іске қосқанда, негізгі есептеулер мен ондағы дереккөздер интернеттегі шалғай серверлерде орындалып, сол жерде сақталады да, ал жұмыс нәтижесі жаңағы тұтынушының компьютерінде стандартты веб–браузердің терезесіне шығарылып көрсетіледі.

Осындай сервисті қолданушы кәсіпорындар саны күннен күнге артуда. Өздерінің ішкі мәлімет өңдеуші орталықтарын сыртқы коммерциялық қызмет көрсететін аутсорсингке тапсыруда. Бұлттық технология қызметін қолданушы кәсіпорындар өздерінің құнды мәліметтері қаншалықты дәрежеде сақталып және өңделіп жатқан процестің қауіпсіздігі туралы уайымдауы мүмкін. Әрине орынды, себебі ондағы мәліметтер өзге тұлғалардың қолына түссе орасан зор зиян тиеді.

Бұлттық есептеу қызметіне нарықтың сапалық және сандық баға бергеніне сүйенсек, талаптарды қанағаттандыруда және тұрақты түрде өсуде.

Gartner компаниясының болжамы бойынша бұлттық есептеу нарығы 2014 жылдың ішінде 190 миллиард долларға жетеді деп есептеуде. Ал Merrill Lynch компаниясы 200 миллиард долларға дейін өсуі мүмкіндігін болжамдауда. Қазіргі уақытта 200 жуық бұлттық қызмет көрсетуші жүйелер бар.

Қазіргі кезде тұтынушыларға бұлттық есептеудің қауіпсіздігі өте жоғары дәрежеде қорғалғандығы жөнінде толықтай көз жеткізудің бір–ақ жолы бар. Ол – тұтынушыларды белсенді түрде төніп тұрған қауіп жайлы хабардар етіп, оны шешу жолында жасалған жұмыстарды түсіндіріп отыру қажет. Дипломдық жобада «Trust Company» ЖШС-ның корпоративтік желісінің қауіпсіздігін бұлттық технология негізінде қамтамасыз ету[15].

Жобаның маркетингтік жоспары төмендегі кестеде көрсетілген.

К е с т е 5.1 – Табыстың маркетингтік болжамы

Бағдарлама іске асырылатын облыстар	2014 ж.	2015 ж.	2016 ж.	2017 ж.
Мекеме №1	4000000		5000000	5500000
Мекеме №2		4500000		
Мекеме №3	4000000		5000000	5500000
Мекеме №4		4500000		
Мекеме №5	4000000	4500000	5000000	5500000
Барлығы	12000000	13500000	15000000	16500000

Жобаның артықшылықтары:

– Қызметке байланысты туындайтын мәселелер азаяды. Cloud Computing–тің енгізілуімен физикалық серверлер азайып жатқандықтан, оларға қызмет ету жеңіл әрі тез. Бағдарламалық қамтамаға келетін болсақ, соңғы бағдарламалар «бұлтта» орналасады, жаңартылады, реттеледі.

– Бағдарламалық қамтамаға кететін шығын азаяды. Әрбір желілік қолданушыға қажетті бағдарламалық пакетті сатып алудың орнына компаниялар қажетті бағдарламаны «бұлтта» сатып алады. Бұл бағдарламаларды жұмысқа қажетті қолданушылар ғана қолданады. Сонымен қатар, Интернет арқылы алуға болатын бағдарламалар бағасы дербес компьютер бағдарламалары аналогтарынан арзанырақ болады. Егер бағдарламалар ұзақ қолданылмайтын болса, сағаттық төлеммен жалға алуға болады.

– Бағдарламалардың әркез жаңартылуы. Кез келген уақытта қолданушы алыстатылған бағдарламаны қосқанда ол бұл бағдарламаның соңғы нұсқасы екендігіне сенімді болуына болады.

Жобаның кемшіліктері:

– Баяу Интернетпен жұмыс істеу нашар. Көптеген «бұлттық» бағдарламалар үлкен өткізгіштік қасиетімен Интернет–қосылысты талап етеді. Егер сіз 56К модемінің «бақытты» иесі болсаңыз, сізге тек аяушылық танытамыз. Қазір Интернет үшін талшықсыз магистралдар өте аз кездеседі, қолжетімділіктің жылдамдығы арта түсуде, ал бағасы төмендеуде.

– Локальды желіге қарағанда бағдарламалар баяу жұмыс істеуі мүмкін. Кейбір информацияның қомақты бөлігі жіберілу керек бағдарламалар локальды компьютерде тезірек жұмыс істеу себебі тек қана Интернеттің жылдамдығы емес, алыстатылған серверлердің жұмысбастылығынан немесе қолданушы мен бұлт арасындағы мәселеден болуы мүмкін.

5.2 Бағдарламамен қамтамасыз етудегі еңбек сыйымдылығын есептеу

Еңбек шығыны құрамдасын есептеудегі базалық көрсеткіш мына формуламен есептелінеді:

$$Q = q \times c\ , \qquad (5.1)$$

$$Q = q \times c = 5300 * 1{,}38 = 7314$$

мұндағы Q – шартты командалар саны;

q – есеп түріне қарай шартты командалар санын ескеретін коэффициент;

c – бағдарламаның қиындығы мен жаңалығын ескеретін коэффициент.

Атап өткен q коэффициентінің мәнін қосымшадағы Б қосымшадан таңдап алуға болады.

Атап өткен *«с»* коэффициенті қосымшадағы Б қосымшадан анықталады, ол күрделік тобы бағанасы мен жаңалықтық дәрежесі бағанасының қиылысуы.

Ары қарай бағдарламалық өнімді әзірлеуге кететін уақытты есептеу керек.Бағдарламалық өнімін дайындауға кеткен әр кезеңнің уақытын анықтаймыз:

1) $T_{ПО}$ (мақсат сипатын дайындау уақыты), нақтылы деректер бойынша алынады және келесі мәнге тең деп алынады (3–тен 5 күнге дейін, 8 сағаттан):

$$T_{ПО} = 24 \text{ адам / сағ.}$$

2) T_O (мақсат сипаттамасы уақыты) келесі формуламен анықталады:

$$T_O = Q \times B / (50 \times K), \quad (5.2)$$

$$T_O = Q \times B / (50 \times K)=7314*1,2/(50*1)=175,5 \text{ адам / сағ.}$$

мұндағы B – мақсат есебі өзгерісінің коэффициенті, B коэффициенті мақсат күрделігіне және өзгеріс санына тәуелді – 1,2–ден 1,5–ке дейін (2– кестені қара).

K – бағдарлама жасаушы білектілігін ескеретін коэффициент. Қосымшадан 5.3–кестеден көре аласыз.

3) T_A (алгоритм құруға кеткен уақыт) мына формуламен есептейміз:

$$T_A = Q / (50 \times K). \quad (5.3)$$

$$T_A = Q / (50 \times K)=7314/(50*1)=146,28 \text{ адам / сағ.}$$

4) $T_{БС}$ (блок – сұлба құруға кеткен уақыт) T_A сияқты 3 формуламен есептеленеді.

5) T_H (бағдарламаның тілінде жазуға кеткен уақыт) келесі формуламен анықталады:

$$T_H = Q \times 1,5 / (50 \times K). \quad (5.4)$$

$$T_H = Q \times 1,5 / (50 \times K)=7314*1,5/(50*1)=219,42 \text{ адам / сағ.}$$

6) $T_П$ (бағдарлама теру уақыты) келесі формуламен анықталады:

$$T_П = Q / 50. \quad (5.5)$$

$$T_П = Q / 50=7314/50=146,28 \text{ адам / сағ.}$$

7) $T_{ОТ}$ (бағдарламаны реттеу және тестілеу уақыты) келесі формуламен анықталады:

$$T_{ОТ} = Q \times 4{,}2/50 \times K. \quad (5.6)$$

$$T_{ОТ} = Q \times 4{,}2/50 \times K = 7314*4{,}2/50*1 = 614{,}38 \text{ адам / сағ.}$$

8) $T_Д$ (құжаттарды рәсімдеу уақыты), нақтылы деректер бойынша алынады және құрылады (3–тен 5 күнге дейін, күніне 8 сағат):

$$T_Д = 24 \text{ адам / сағ.}$$

Еңбек шығындарының сомасы еңбек шығынының құрама сомасы ретінде 7 формуламен есептеленеді:

$$T = T_{ПО} + T_{ТО} + T_А + T_{БС} + T_Н + T_П + T_{ОТ} + T_Д. \quad (5.7)$$

$$T = 24 + 175{,}53 + 146{,}28 + 146{,}28 + 219{,}42 + 146{,}28 + 614{,}38 + 24 = 1496{,}17 \text{ адам / сағ.}$$

5.3 Бағдарламалық қамсыздандыру шығынының есебі

Бағдарламалық қамсыздандыру шығыны ішіне еңбек ақы шығыны да, еңбек ақыдан аударылымдар, амортизациялық және тағы да басқа шығындар кіреді, олар мынандай формуламен анықталады:

$$C = ФОТ + О_{СН} + А + С_{ЭЭ} + С_{МжК} + С_{ТО} + С_{ПР} + С_Н, \quad (5.8)$$

Еңбек ақы екі жасаушыдан құрылады: негізгі еңбек ақы және қосымша еңбек ақы сомасы (немесе еңбек ақы қоры, *ЕАҚ*) негізгі еңбек ақы және қосымша еңбек ақы сомасы мына формуламен есептеленеді:

$$ФОТ = З_{осн} + З_{доп}, \quad (5.9)$$

мұндағы $З_{осн}$ – негізгі еңбек ақы, мың теңге;

$З_{доп}$ – қосымша еңбек ақы, мың теңге.

Негізгі еңбек ақы төмендегідей анықталады:

$$З_{осн} = T \times ТС/t_{орт}, \quad (5.10)$$

$$З_{осн} = T \times ТС/t_{орт} = 1496{,}17*3000/21 = 213738{,}86 \text{ тг}$$

5 қызметкердің негізгі еңбекақысы: *213738,86 *5=1068694,29 тг*

мұндағы T – еңбек шығының сомасы, (7) формуламен анықталады;

$t_{орт}$ – бір айдағы орташа жұмыс күндерінің саны (21), жұмыс ұзақтығына көбейтіледі (8 сағат);

$ТС$ – тарифтік мөлшерлеме.

Қосымша еңбек ақы негізгі еңбек ақының 20 % құрайды және келесі формуламен есептелінеді;

$$З_{доп} = 0,2 \times З_{осн}. \quad (5.11)$$

$$З_{доп} = 0,2 \times 213738,86 = 42747,77 \text{ тг}$$

5 қызметкердің қосымша еңбекақысы $З_{доп} = 42747,77 * 5 = 213738,86$ *тг*

$$ФОТ = З_{осн} + З_{доп} = 1068694,29 + 213738,86 = 1282433 \text{ тг}$$

Әлеуметтік салық ЕАҚ 11 % құрайды (ҚР СК 358 б. 1–тарау) жұмыскердің табысынан, мынандай формуламен есептеледі:

$$О_{СН} = (ФОТ – ЗА) \times 11\%, \quad (5.12)$$

$$О_{СН} = (1282433 – 128243,3) * 11\% = 126960,88 \text{ тг}$$

мұндағы ЗА – зейнетақы аударылымдар, ЕАҚ–нан 10% құрайды және әлеуметтік салықпен міндеттелмейді:

$$ЗА = ЕАҚ – 10\%. \quad (5.13)$$

$$ЗА = ЕАҚ – 10\% = 1282433 * 10\% = 128243,3 \text{ тг}$$

Амортизациялық аударылымдар амортизацияның тағайынды шамаларымен орындалады, пайыздармен жабдықтың баланстық құнына және мына формуламен есептеледі:

$$А = \frac{Б_{бас} \times А_{ш} \times N}{100 \times 12 \times t} = 27999972 * 23,75 * 62.34 / 100 * 12 * 1272.64 = 27146,01 \text{ тг} \quad (5.14)$$

мұндағы $А_{ш}$ – амортизация шамалары;

$Б_{бас}$ – жабдықтың бастапқы бағасы;

N – жұмыс орындалуына кеткен күннің саны;

t – дербес компьютерді қолдануға кеткен жалпы уақыт.

Амортизация шамалары ($А_{Ш}$), мына формуламен есептеледі:

$$H_A = \frac{Б_{бас} - К_{тар}}{T_{норм} \cdot Б_{бас}} \times 100\%, \ =(27999972\text{-}1399998,6)/4*27999972=23,75\% \ (5.15)$$

мұндағы $К_{тар}$ – таратылым құны, жабдықтың құнынан 5% құрайды (нұсқа бойынша);

$T_{норм}$ – жабдықтың нормативтік қызмет ету мерзімі (дербес компьютер үшін – 4 жыл).

Жабдықтың бастапқы бағасы төмендегі 5.2 –кестеде көрсетілген:

К е с т е 5.2– Жабдық құны [Б қосымша]

Жабдықтардың аталуы	Саны	Құны Тг	Барлығы
Компьютер: Жүйелік блок Alser Mega Pro №2362(Intel Core I7)	3	305390	916170
GNS–тің лицензиялы бағдарламасы	3	8960	26880
Бағдарламаны қондыру ақысы	3	3000	9000
Wi–Fi қолжетімділік нүктесі +сыртқы қатқыл диск Apple MD032RS/A Refurbished Time Capsule–2TB	1	66990	66990
Fijitsu Siemens/PY BF200 4xFC/4 xGbE сервері	3	2699982	8099946
Маршрутизатор Cisco 3825 with AC PWR	3	1627000	4881000
Cisco Asa5510–BUN–K9	3	147420	737100
Барлығы:	19	4858742	27999972

Дербес компьютерде жалпы жұмыс істеу уақыты мына формуламен есептеленеді:

$$T = T_A + T_{БС} + T_H + T_П + T_{ОТ}. \qquad (5.16)$$

$T =$ 146.28+146.28+219.42+146.28+614.38=1272.64 адам/сағ

Электрэнергия шығындары мына формуламен есептеледі:

$$C_{ЭЭ} = К \times k_з \times T \times C_{кВт–сағ}, \qquad (5.17)$$

$C_{ЭЭ} = К \times k_з \times T \times C_{кВт–сағ}$ = 0,45*0,8*12,34*1272.64=5653,56 тг

мұндағы $К$ – ЭЕМ қуаты (450 Вт);

$k_з$ – жүтеме коэффициенті (0.8);

$C_{кВт.с}$ – 1 кВт–сағ электрэнергиясының құны;
T – жұмыс уақыты, сағ.

Материалдар мен көмекші бөлшектер шығыны, бағдарламалық өнімді жазу барысында қолданылды ($С_{МжК}$), сонымен қатар техникалық қызмет көрсету шығыны ($C_{ТО}$), жабдықтың құнынан 1.5% және 2.5% құрайды және мына формулалар мен есептеледі (18 – 19):

$$C_{МжК} = 0,015 \times C_{обор,} = 0,015*27999972 = 419999,58 \text{ тг,} \quad (5.18)$$

$$C_{ТО} = 0,025 \times C_{обор}. = 0,025*27999972 = 699999,3 \text{ тг.} \quad (5.19)$$

Басқару мен қызмет көрсетуге байланысты үстеме шығындар, сондай–ақ жабдықты пайдалану кезіндегі және де кәсіпорын үдерістері мен айналымдарынан қосымша шығындар еңбек ақы қорынан 50% құрайды және де мына формуламен есептеледі:

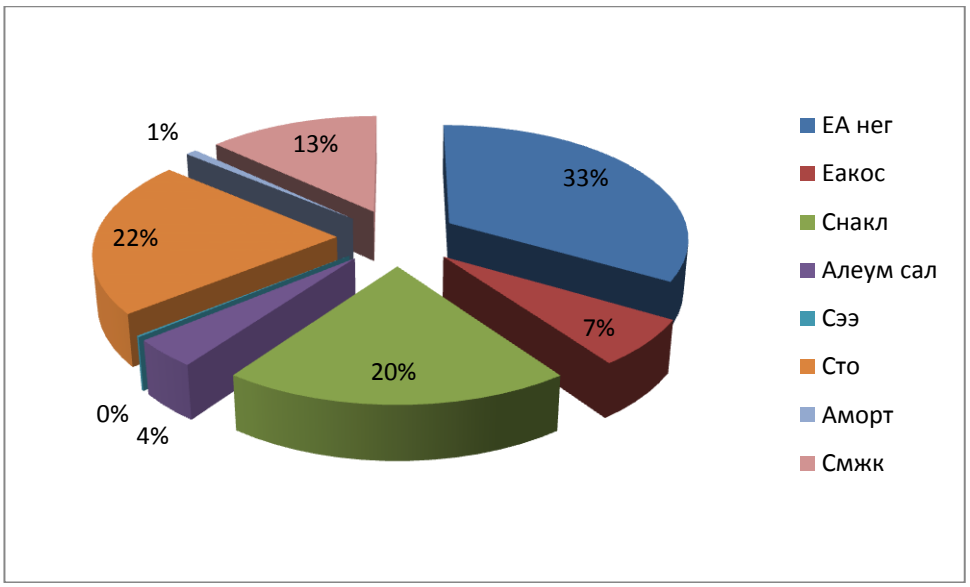
$$C_{Н} = 0,5 \times ЕАҚ = 0,5* 1282433 = 641216,57 \text{ тг.} \quad (5.20)$$

Бағдарламалық өнімнің өзіндік құнының есебінің жиынтық нәтижелерін кесте түрінде ұсыну керек, шығын статьясын атап, және оның ортақ құндағы сыбағаларын пайызбен есептеу керек[15].

К е с т е 5.3 – Өзіндік құнның қорытынды кестесі

Шығын бабы атауы		Сомасы, теңге	Әр баптың үлесі, %
ЕАҚ	$ЕА_{нег}$	1068694	33,36
	$ЕА_{қос}$	213738,9	6,67
Үстеме шығындар, $С_{Накл}$		641216,6	20,01
Әлеуметтік салық шығыны, $ӘС$		126960,9	3,96
Пайдалану шығындары	$С_{ээ}$	5653,558	0,17
	$C_{ТО}$	699999,3	21,85
	$А_{жыл}$	27146,01	0,84
Материалдар және көмекші, $С_{МжК}$		419999,6	13,11
Барлығы:		3203409	100%

Бағдарламалық өнімнің өзіндік құнының есебінің жиынтық нәтижелері диаграмма түрінде:



Сурет 5.1– Бағдарламалық өнімнің өзіндік құнының есебінің жиынтық нәтижелері

Бағдарламалық өнімді жүзеге асыру бағасы оның құны мен таза кірістің қосындысынан тұрады:

$$Ц = С + П \quad (5.21)$$

мұндағы, С – өнім бағасы;

П – таза кіріс.

Бастапқы бағаны анықтауда бағдарламалық өнімді жүзеге асыру үшін керекті рентабелдік деңгейін анықтау қажет (20%):

$$Ц_п = С \cdot (1 + \frac{Р}{100}) \quad (5.22)$$

мұндағы, Р – рентабельдік (20%).

$Ц_п$ = 3203409* (1 + 20/100)= 3844091 теңге.

Бағдарламаның орындалу бағасы келесі формула арқылы табылады.

$$Ц_р = Ц_п + НДС. \quad (5.23)$$

Қазіргі таңда ҚР-да НДС 12% құрайды:

$$НДС = Ц_п \cdot 12\%, \quad (5.24)$$

НДС=3844091 * 12%=461291 теңге;

$Ц_р$=3844091+461291=4305381 теңге.

5.4 Бағдарлама өнімін сатып алуға кеткен бір жолғы шығындар есебі

Бағдарлама өнімін сатып алуға және оны өндіріске енгізу шығындары келесі шығындардан тұрады:

$$ЗЗ = C_C + C_{TP} + C_O, \quad (5.25)$$

мұндағы C_C – жүйенің құны, мың теңге;

C_{TP} – көлік шығыны, жүйе құнынан – 25 %, мың теңге;

C_O – өнімді игеруге деген шығыннан, мың теңге.

Жүйе құны үстінде есептелінді, ал қалғандары келесі түрде есептелінеді. Өнімді игеруге деген маманды оқыту шығыны, оқытуға кеткен уақыт пен оған деген консалтингті фирмадағы мөлшерлемеден тұрады:

$$C_O = T \times C_{ОП}, \quad (5.26)$$

$$C_O = T \times C_{ОП} = 8*3*3000=72000 \text{ тг}$$

мұндағы T – оқытуға кеткен уақыт, сағ.;

$C_{ОП}$ – консалтингті фирмадағы мөлшерлеме, сағатына 2500–3000 теңгедей.

Бағдарлама өнімін сатып алуға кеткен бір жолғы шығындар есебін 6–кестеге келтіру керек.

$$ЗЗ = C_C + C_{TP} + C_O = 4305381+0,25* 4305381+72000+ 27999972=33453699 \text{ тг}$$

К е с т е 5.4 – Ақпарат жүйелерін енгізуге керекті бір жолымғы шығындар есебінің жиынтығы

Шығын бабы атауы	Сомасы, мың теңге
Жүйенің құны	4305381
Көлік шығыны	1076345
Жүйені оқуға кеткен шығыны	72000
Капиталдық шығындар	27999972
Барлығы:	33453699

5.5 Ақпараттық жүйе енгізуден үнем мен табыс мөлшерінің есебі

Ақпараттық жүйе енгізген ұйымда үнем көзі, оны енгізуден кейін түскен пайда немесе шығын үнемделенетіні болып табылады. Ұйымда ақпараттық жүйе енгізу барысында деректерді өңдеуге, пайдалануға уақыт азайып, еңбек өнімділігі өсіп, құрылғылар саны азайатын үнемдідікке кез келеді. Құрылғының азаюынан түскен үнемділікті келтірінді шығындардың базалық ($Р_о$) және ұсынылған ($Р_1$) нұсқалар айырмасы ретінде шығарып алуға болады.

$$\Delta P = P_o - P_1, \quad (5.27)$$

мұндағы P_o – база мезгілінде құрылғыларға кеткен келтірінді шығындар (қол жұмысын қолданған кезде), мың теңге;

P_1 – ұсынылған мезгілінде құрылғыларға кеткен келтірінді шығындар (бағдарламалық өнімді енгізгеннен кейін), мың теңге.

Кәсіпорында бұрын HP Z400 [http://almaty.satu.kz/p2591638-rabochie-stantsii-z400.html] компьютерлері қолданылған болатын. 436 790 теңгеден 113 компьютердің құны:

$$P_o = 436\,790 * 113 = 49357270 \text{ тг},$$

$$\Delta P = 49357270 - 33453699 = 15903571 \text{ тг}$$

Шығынның азаюы мен IT инфраструктураның тиімділігінің артуы. Орташа компаниялардың дағдылы серверлері 10–15%–ке артық мөлшерде қуатты қажет етеді. Белгілі бір уақыт аралығында қосымша есептеуші ресурстарға мұқтаждық бар, ал басқаларда бұл қымбат тұратын ресурстар тұрып қалып жатады. «Бұлтта» есептеуіш ресурстардың (мысалы, Amazon EC2) қажетті санын қолданып, компания өзінің құрылғылар мен қызметке кететін шығынын бірнеше пайызға дейін азайта алды.

5.6 Салыстырмалы экономикалық тиімділіктің көрсеткіштерін есептеу

Нормативтік күрделі қаржы салымын өтелу мерзімі, АТ моральдық тозуы техникалық құралдардың және жоба шешімдерінің тозуына байланысты ($T_н$ = 1, 2, 3…n) бағдарлама өнімдерінің өтеу мерзімі 4 жыл.

Есептік күрделі қаржы салымының экономикалық тиімділігінің коэффициенті:

$$E_p = \frac{Э_{уг}}{K} = 15903571/33453699 = 0{,}47 \quad (5.28)$$

мұндағы E_p – есептік күрделі қаржы салымының экономикалық тиімділігі;

K – жүйеге күрделі қаржы салымы, теңге.

Есептік күрделі қаржы салымын өтелу мерзімі:

$$T_p = \frac{1}{E_p} = 1/0{,}48 = 2{,}1 \text{ жыл.} \quad (5.29)$$

Ақпараттық жүйелер енгізудің салыстырмалы экономикалық тиімділігінің көрсеткіштерін есептеу қорытындыларын келесі кестеге сомасын, баптарын көрсетіп толтырыңыз (9 кестені қара).

К е с т е 5.5 – Бағдарлама өнімін енгізудің салыстырмалы экономикалық тиімділігінің көрсеткіштері

Көрсеткіштер атауы	Мәні
Шартты жылдық шығынды үнемдеу, мың теңге	15903571
Күрделі қаржы салымының экономикалық тиімділігінің коэффициенті (E_p)	0,48
Күрделі қаржы салымын өтелу мерзімі (T_p), жыл	2 жыл 1 ай

5.7 Ақшалай құралдардың қозғалысы

Ақшалай құралдардың қозғалысы келесі кестеде келтірілген.

К е с т е 5.6 – Ақшалай тәсілдердің қозғалысы, теңге

Аты	Барлығы				
	2014	2015	2016	2017	
Бірмезгілдік шығындар	33453699				33453699
Операциялы кәсіп		15903571	15903571	15903571	47710713
Дисконттау коэффициенті (20% мөлшерінде)		0,83	0,69	0,57	
Таза дисконтталған табыс (ТДТ)	-33453699	13252975	11044146	9203455	46878
ТДТ өспелі нәтижесімен	-33453699	-20200724	-9156577	46878	93756

5.8 Экономикалық тиімділікті есептеу

5.8.1 Таза ағымдағы құндылықты есептеу (Net present value, NPV)

Шығындары бірмезгілде тек жобаның басында күрделі салымдар (C_0) ретінде іске асатын жобалар үшін NPV келесі формуламен есептеледі:

$$\text{NPV}=\sum_{k=1}^{n}\frac{\text{B}_\text{i}}{(1+\text{r})^\text{i}}-\text{C}_0 \qquad (5.30)$$

мұндағы B_i –і-ші жылдағы жобадан алынатын пайда;

r – дисконттеу мөлшері.

NPV=13252975+11044146+9203455-33453699=46878

NPV>0 біздің жобамыз табысты жоба

5.8.2 Пайда индексін есептеу (Profitability index, PI)

Табыстық индексі (ИД) келтірілген әсерлердің сомасының күрделі қаржы салымына қатынасы. Ол келесі формуламен есептеледі:

$$ИД = \frac{1}{K}\sum_{t=1}^{T}\left(P_t - З_t\right)\cdot\frac{1}{\left(1+E\right)^t}$$

мұндағы K – күрделі қаржы салымы немесе инвестицияның құны.

$$ИД = \frac{33500577{,}39}{33453699} = 1.$$

PI салыстырмалы көрсеткіш болып табылады, енгізілген қаражаттың тиімділігін көрсетеді және бірнеше жобаларды салыстыру үшін қолданылады. Пайда индексінің жоғарғы мәнімен берілген жобалар тұрақты болып табылады.

5.8.3 Табыстың ішкі нормасын есептеу (Internal rate of return, IRR)

$$IRR = \text{r1} + \frac{\text{f(r1)}}{\text{f(r1)}-\text{f(r2)}} * (\text{r2} - \text{r1}) \qquad (5.31)$$

Егер күрделісалымдар қаражаттарды тарту есебінен ғана іске асса сонымен қоса кредит і мөлшерінде алынса, онда (IRR - і) айырымы инвестициялық істің тиімділігін көрсетеді. IRR < і болғанда салынған қаражаттардың қайтарымы мүмкін болмайды[16].

Барьерлік қойылым үшін r_a=20% деп аламыз:

NPV(ra)=46878 тг

Барьерлік қойылым үшін r_b=40% деп аламыз:

NPV(40%)=11359693+8114066+5795762-33453699=-8184177 тг,

IRR = r_a + (r_b - r_a)*NPVa/(NPVa - NPVb) = 20 + (40 - 20)* 46878/ /(46878+8184177)= 46%.

5.8.4 Өтімділік периодын есептеу (Payback period, PBP)

PBP = n, мұндағы:

$$\sum_{i=1}^{n} \frac{B_i}{(1+r)^i} = \sum_{j=1}^{n} \frac{C_j}{(1+r)^j}, \quad (5.32)$$

$$T_{ок} = 2 + \frac{33453699 - (13252976 + 11044146)}{9203455} = 2{,}99 = 2 \text{ жыл } 11 \text{ ай.}$$

К е с т е 5.7 – Бағдарлама өнімін әзірлеуінің және енгізуінің экономикалық пайдалылығының көрсеткіштері

Көрсеткіштер атауы	Мәні
Бағдарлама өнімін әзірлеуге және енгізуге шығын, мың теңге	33453699
Бағдарлама өнімін енгізгеннен кейінгі болжалды үнем, мың теңге	15903570
Таза дисконттық табыс, мың теңге	46878
Табыстық индекс	1
Ішкі табыстық мөлшері	46%
Дисконталған өтелу мерзімі, жыл	2 жыл 11 ай
Моральдық ескіру мерзімі, жыл	3

Қорытынды

Бұл дипломдық жобаны жасау барысында бұлттық есептеуге төнетін бүкіл қауіп-қатермен анықталып, қауіптің алды алушаралары қарастырылды. Нақтырақ айтсақ, бұл жобада бұлттық есептеудің тұтынушылардың мәліметке қолжетімділігінің желілік қауіпсіздігін қамтамасыз етілді. Яғни, компьютерлік желіні қорғау іске асырылды. Компьютерлік желіні құруға қажетті құралдарды толығымен жаңарту қарастырылды.

Қол жетімділік, тұтастылық және құпиялылық сияқты ақпарат сипаттамалары жобада ескерілді. Ақпарат сипаттамаларын ескере отырып, ақпаратты физикалық және программалық-аппараттық қорғау әдістері қарастырылды және ұйымдастырылды.

Серверлік бөлмені ұйымдастыру тәсілдері жасалынды. Компьютерлік желідегі барлық жабдықтар бірлесе және үздіксіз жұмыс атқаруы үшін қорғаудың басты жүйелері қарастырылды, сонымен бірге, барлық сипаттаманы қолдайтын құралдар ұсынылды.

Желі құрылымын жобалау қорғаныс тәсілдеріне бағынышты болып келеді. Сол себепті, желіні программалық және аппараттық қорғау әдістері қарастырылды және алынған мәліметтер негізінде бұлттық есептеу желісінің толық құрылымы жасалынды.

Дипломдық жобамда бағдарламаның өзіндік құны есептеп шығарылды. Өзіндік құн кестесіне қажетті салымдар мен шығындарды енгізе отырып, өзіндік құнның 3203409 теңгеге теңдігіне көзім жетті.

Экономикалық тиімділікті есептеу нәтижесі көрсеткендей, жоба іске аса алады және тиімді. Бұл курстық жоба барысында NPV–дің, PI, IRR–дің мөлшерін есептей келе жоба нарықта жүзеге аса алатын, тиімді проект екеніне көз жеткіздік.

Әдебиеттер тізімі

1 Marvin Washcke. Cloud Standards: Agreement That Hold Together Clouds. Изд–во Apress, 2012. – 380 с.

2 Тұрым А.Ш., Берікұлы Ә. Компьтерлік желілер: желілік шабуылдар және желіаралық экрандар: Оқу құралыю. – Алматы: АИжБИ, 2007. – 80 бет.

3 Уэнстром М. Организация защиты сетей Cisco. – М.: Издательский дом «Вильямс», 2005. – 768 с.

4 Цирлов В.Л. Основы информационной безопасности автоматизированных систем: Краткий курс. Феникс, 2008. – 173 с.

5 Каторин Ю.Ф., Разумовский А.В. Спивак А.И. Защита информации техническими средствами.Общий курс. НИУ ИТМО. 2011. – 418 с.

6 Rajkumar Buyya, Christian Vecchiola, S. Thamarai Selvi. Mastering Cloud Computing: Foundations and Applications Programming. Изд–во Morgan Kaufmann, 2013. – 580 с.

7 Цирлов В.Л. Основы информационной безопасности. Краткий курс. Феникс, 2008. – 250 с.

8 Aidan Finn, Hans Vredevoort, Patrick Lownds. Microsoft Private Cloud Computing. Изд–во John Wiley & Sons, 2012. – 407 с.

9 Платонов В.В. Программно-аппаратные средства обеспечения информационной безопасности вычислительных сетей. Издательство «Академия», 2006. – 240 с.

10 Запечников С. В., Милославская Н. Г. Информационная безопасность открытых систем. Том 2. Средства защиты в сетях. Издательство: Горячая Линия – Телеком, 2008. – 560 с.

11 Лиза Хендерсон, Frame Relay межсетевый взаймодействие, Издательство: Горячая Линия – Телеком, 2008. – 365 с.

12 Домарев В.В. Безопасность информационных технологий. Методология создания систем защиты. – К.: ООО «ТИД ДС», 2007. – 688 с.

13 Хакимжанов Т.Е. Расчет аспирационных систем. Дипломное проектирование. Для студентов всех форм обучения всех специальностей. – Алматы: АИЭС, 2002. – 30 с.

14 Дюсебаев М.К. Безопасность жизнедеятельности. Методические указания к выполнению раздела в дипломных проектах. – АИЭС, 2001. – 10с.

15 Экономика: Учебник / Под ред. Р. П. Колосовой. – М.: Норма, 2011. – 345 с.

16 Экономика: Учебное пособие /Под ред. А.С. Булатова. – М.: Юристъ, 2009. – 896 с.

17 Базылов К.Б., Алибаева С.А., Бабич А.А.. Выпускная работа бакалавров. Экономический раздел. Методические указания для студентов всех форм обучения специальности 050719 – Радиотехника электроника и телекоммуникации. – Алматы: АИЭС, 2008. – 17 с.

Қосымша А

```
hostname R1
ip dhcp excluded-address 10.1.40.1 10.1.40.24
ip dhcp excluded-address 10.1.10.1 10.1.10.10
ip dhcp excluded-address 10.1.20.1 10.1.20.10                    *создаем пул адресов
ip dhcp excluded-address 10.1.30.1 10.1.30.10
ip dhcp excluded-address 10.1.88.1 10.1.88.24
!
ip dhcp pool B1_VLAN10
 network 10.1.10.0 255.255.255.0
 default-router 10.1.10.1
 dns-server 10.0.1.4
ip dhcp pool B1_VLAN20
 network 10.1.20.0 255.255.255.0
 default-router 10.1.20.1
 dns-server 10.0.1.4
ip dhcp pool B1_VLAN30
 network 10.1.30.0 255.255.255.0
 default-router 10.1.30.1
 dns-server 10.0.1.4
ip dhcp pool B1_VLAN88
 network 10.1.88.0 255.255.255.0
 default-router 10.1.88.1
 dns-server 10.0.4.1
!
ip ssh version 1
!
interface FastEthernet0/0
 no ip address
 duplex auto
 speed auto
!
interface FastEthernet0/0.10                    *настройка  фрэймрелэй для каждого в-лана
 encapsulation dot1Q 10
 ip address 10.1.10.1 255.255.255.0
!
interface FastEthernet0/0.20
 encapsulation dot1Q 20
 ip address 10.1.20.1 255.255.255.0
!
interface FastEthernet0/0.30
 encapsulation dot1Q 30
 ip address 10.1.30.1 255.255.255.0
!
interface FastEthernet0/0.88
 encapsulation dot1Q 88
 ip address 10.1.88.1 255.255.255.0
!
interface FastEthernet0/0.99
 encapsulation dot1Q 99 native
```

```
 ip address 10.1.99.1 255.255.255.0
!
interface FastEthernet0/1
 no ip address
 duplex auto
 speed auto
 shutdown
!
interface Serial0/0/0
 ip address 10.255.255.2 255.255.255.252
 encapsulation frame-relay
 frame-relay lmi-type q933a
 ip summary-address eigrp 100 10.1.0.0 255.255.0.0 5
!
interface Serial0/0/1
 no ip address
 shutdown
!
interface Vlan1
 no ip address
 shutdown
!                          *настройка протокола маршрутизации
router eigrp 100
 redistribute static
 passive-interface FastEthernet0/0
 passive-interface FastEthernet0/0.10
 passive-interface FastEthernet0/0.20
 passive-interface FastEthernet0/0.30
 passive-interface FastEthernet0/0.99
 network 10.1.0.0 0.0.255.255
 network 10.255.255.0 0.0.0.3
 network 10.0.0.0
 no auto-summary
!
ip classless
ip route 0.0.0.0 0.0.0.0 10.255.255.1
!
!
line con 0
line vty 0 4
 login
!
end

hostname R2
!
ip dhcp excluded-address 10.2.40.1 10.2.40.24
ip dhcp excluded-address 10.2.10.1 10.2.10.10
ip dhcp excluded-address 10.2.20.1 10.2.20.10
ip dhcp excluded-address 10.2.30.1 10.2.30.10
ip dhcp excluded-address 10.2.88.1 10.2.88.24
```

```
!
ip dhcp pool B2_VLAN10
 network 10.2.10.0 255.255.255.0
 default-router 10.2.10.1
 dns-server 10.0.1.4
ip dhcp pool B2_VLAN20
 network 10.2.20.0 255.255.255.0
 default-router 10.2.20.1
 dns-server 10.0.1.4
ip dhcp pool B2_VLAN30
 network 10.2.30.0 255.255.255.0
 default-router 10.2.30.1
 dns-server 10.0.1.4
ip dhcp pool B2_VLAN88
 network 10.2.88.0 255.255.255.0
 default-router 10.2.88.1
 dns-server 10.0.4.1
!
ip ssh version 1
!
interface FastEthernet0/0
 no ip address
 duplex auto
 speed auto
!
interface FastEthernet0/0.10
 encapsulation dot1Q 10
 ip address 10.2.10.1 255.255.255.0
!
interface FastEthernet0/0.20
 encapsulation dot1Q 20
 ip address 10.2.20.1 255.255.255.0
!
interface FastEthernet0/0.30
 encapsulation dot1Q 30
 ip address 10.2.30.1 255.255.255.0
!
interface FastEthernet0/0.88
 encapsulation dot1Q 88
 ip address 10.2.88.1 255.255.255.0
!
interface FastEthernet0/0.99
 encapsulation dot1Q 99 native
 ip address 10.2.99.1 255.255.255.0
!
interface FastEthernet0/1
 no ip address
 duplex auto
 speed auto
 shutdown
!
```

```
interface Serial0/0/0
 ip address 10.255.255.6 255.255.255.252
 encapsulation frame-relay
 frame-relay lmi-type q933a
 ip summary-address eigrp 100 10.2.0.0 255.255.0.0 5
!
interface Serial0/0/1
 no ip address
 shutdown
!
interface Vlan1
 no ip address
 shutdown
!
router eigrp 100
 redistribute static
 passive-interface FastEthernet0/0
 passive-interface FastEthernet0/0.10
 passive-interface FastEthernet0/0.20
 passive-interface FastEthernet0/0.30
 passive-interface FastEthernet0/0.99
 network 10.2.0.0 0.0.255.255
 network 10.255.255.4 0.0.0.3
 network 10.0.0.0
 no auto-summary
!
ip classless
ip route 0.0.0.0 0.0.0.0 10.255.255.5
!
no cdp run
!
line con 0
line vty 0 4
 login
!
End

hostname R3              *основной маршрутизатор
!
username ISP password 0 ciscochap                              *настройка PPP
username NewB password 0 ciscopap
!
ip ssh version 1
!
interface FastEthernet0/0
 ip address 10.0.1.1 255.255.255.0
 ip nat inside
 duplex auto
 speed auto
!
interface FastEthernet0/1
```

```
 no ip address
 duplex auto
 speed auto
 shutdown
!
interface Serial0/0/0
 no ip address
 encapsulation frame-relay
 frame-relay lmi-type q933a
!
interface Serial0/0/0.41 point-to-point
 ip address 10.255.255.1 255.255.255.252
 frame-relay interface-dlci 41
 ip nat inside
!
interface Serial0/0/0.42 point-to-point
 ip address 10.255.255.5 255.255.255.252
 frame-relay interface-dlci 42
 ip nat inside
!
interface Serial0/0/0.43 point-to-point
 ip address 10.255.255.9 255.255.255.252
 frame-relay interface-dlci 43
 ip nat inside
!
interface Serial0/0/1
 ip address 10.255.255.253 255.255.255.252
 encapsulation ppp
 ppp authentication pap
 ppp pap sent-username HQ password 0 ciscopap
 ip nat inside
 clock rate 4000000
!
interface Serial0/1/0
 ip address 209.165.201.1 255.255.255.252
 encapsulation ppp
 ppp authentication chap
 ip nat outside
!
interface Serial0/1/1
 no ip address
 shutdown
!
interface Vlan1
 no ip address
 shutdown
!
router eigrp 100
 redistribute static
 passive-interface FastEthernet0/0
 passive-interface Serial0/0/1
```

```
 passive-interface Serial0/1/0
 network 10.0.1.0 0.0.0.255
 network 10.255.255.0 0.0.0.3
 network 10.255.255.4 0.0.0.3
 network 10.255.255.8 0.0.0.3
 network 10.255.255.252 0.0.0.3
 network 10.0.0.0
 no auto-summary
!
ip nat pool XYZCORP 209.165.200.241 209.165.200.245 netmask 255.255.255.248
ip nat inside source list ACL pool XYZCORP
ip nat inside source list NAT_LIST pool XYZCORP
ip nat inside source static 10.0.1.2 209.165.200.246
ip classless
ip route 0.0.0.0 0.0.0.0 Serial0/1/0
ip route 10.4.5.0 255.255.255.0 Serial0/0/1
!
ip access-list extended NAT_LIST
 permit ip 10.0.0.0 0.255.255.255 any
!
line con 0
line vty 0 4
 password cisco
 login
!
End
```

*Настройка маршрутизатора для работы с IP-телефоном

На маршрутизатор Cisco необходимо загрузить файлы работы с Cisco CallManager Express – например, для версии 4.0.0.1 - cme-basic-4.0.0.1.tar и cme-gui-4.0.0.1.tar. Скопируем эти файлы во flash-память маршрутизатора:

```
#archive tar /xtract tftp://IP_адрес_tftp_сервера/ cme-basic-4.0.0.1.tar flash:
#archive tar /xtract tftp://IP_адрес_tftp_сервера/ cme-gui-4.0.0.1.tar flash:
```

Настроим пул IP адресов для работы пользователей и IP телефонов. Разделим сеть на два сегмента – голосовую сети (TLAN) и сеть передачи данных (DLAN):

```
(config)# ip dhcp pool TLAN
(config)# network <маска_сети>
(config)# option 150 ip      #TFTP-сервер тоже будет работать на маршрутизаторе
(config)# default-router
(config)# ip dhcp pool DLAN
(config)# network <маска_сети>
(config)# default-router
(config)# service dhcp
```

Настроим TFTP-сервер для того, чтобы IP-телефоны Cisco могли загружать прошивки (firmware) и конфигурации (файлы прошивок закачиваем для всех используемых IP-телефонов):

(config)# tftp-server flash:<имя_файла>
tftp-server flash:ATA030100SCCP040211A.zup
tftp-server flash:CP7902040000SCCP040701A.sbin
tftp-server flash:CP7905040000SCCP040701A.sbin
tftp-server flash:P00403020214.bin
tftp-server flash:CP7912040000SCCP040701A.sbin
tftp-server flash:S00103020002.bin
tftp-server flash:P00503010100.bin
tftp-server flash:cmterm_7936.3-3-5-0.bin
tftp-server flash:P00303020214.bin
tftp-server flash:P00305000301.sbn
tftp-server flash:cmterm_7920.3.3-01-08.bin
tftp-server flash:TERM70.6-0-3SR1S.LOADS
tftp-server flash:TERM70.DEFAULT.loads
tftp-server flash:TERM71.DEFAULT.loads
tftp-server flash:cnu70.63-0-1-4.sbn
tftp-server flash:Jar70.63-0-1-4.sbn
tftp-server flash:jvm70.603ES1R4.sbn

Настроим сам CallManager Express:

(config)# telephony-service
(config-telephony)# max-ephones 48 # максимальное количество телефонов
(config-telephony)# max-dn 96 # максимальное количество номеров – исходя из 2 линий на IP-телефон
(config-telephony)# no auto-reg-ephone # отключим авто-регистрацию – для тестовой эксплуатации можно включить
(config-telephony)# load 7960-7940 <версия_прошивки> # загружаем прошивку для моделей IP-телефонов Cisco 7940-7960
(config-telephony)# ip source-address # откуда IP-телефонам брать прошивку и конфигурацию
(config-telephony)# user-locale ru # далее – настройки языка, даты и времени
(config-telephony)# network-locale ru
(config-telephony)# date-format dd-mm-yy
(config-telephony)# time-format 24
(config-telephony)# create cnf-files

Наконец, для каждого телефона настроим (повторяем для всех, меняя номер, пользователя (отображаемое имя), MAC-адрес и прошивку (если другая модель телефона)):

(config)# ephone-dn 1
(config-ephone-dn)# number 1001
(config-ephone-dn)# name Ivan, Ivanov
(config)# ephone 1
(config-ephone)# mac-address
(config-ephone)# type <тип_телефона>

(config-ephone)# button 1:1
(config-ephone)# keypad-normalize

Настройка коммутатора для работы с IP телефоном/ Настройка Cisco IOS

Switch(config-if)#switchport mode’access

Switch(config-if)#switchport access vlan »’vlan id

Switch(config- if)#switchport voice vlan Vlan id

Switch(config-if)#no shutdown

Либо альтернативный метод:

Switch(config-if)#’switchport trunk’ encapsulation dot1q

Switch(config-if)#switchport trunk native vlan id

Switch(config-if)#switchport mode trunk

Switch(config-if)#switchport voice vlan id

Switch(config-if)#spanning-tree portfast trunk

Қосымша Б

К е с т е 1 – q коэффициентінің мәні

Тапсырма түрлері	Коэффициенттің өзгеру аралығы
Есептеу тапсырмалары	1400 ден 1500
Оперативті басқару тапсырмалары	1500 ден 1700
Жоспарлау тапсырмалары	3000 ден 3500
Көп вариантты	4500 ден 5000
Комплекстік тапсырма	5000 ден 5500

Ке с т е 2 – Еңбек сыйымдылығын есептейтін коэффициент

Бағдарлама тілі	Күрделілік тобы	Жаңалықтық дәрежесі				B коэффициенті
		A	Б	В	Г	
Жоғарғы деңгей	1	1,38	1,26	1,15	0,69	1,2
	2	1,30	1,19	1,08	0,65	1,35
	3	1,20	1,10	1,00	0,60	1,5
Төменгі деңгей	1	1,58	1,45	1,32	0,79	1,2
	2	1,49	1,37	1,24	0,74	1,35
	3	1,38	1,26	1,15	0,69	1,5

3 к е с т е – Бағдарламалық өнімді жасауға жалпы уақыт құрамы

Кезең №	Дәл кезеңдегі уақыт белгісі	Кезеңнің мазмұны
1	$T_{ПО}$	Мақсат сипатын дайындау
2	$T_{О}$	Мақсат сипаттамасы
3	$T_{А}$	Алгоритм құру
4	$T_{БС}$	Алгоритмнің блок-схемасын құру
5	$T_{Н}$	Бағдарламаны ... тілде жазу
6	$T_{П}$	Бағдарламаны теру
7	$T_{ОП}$	Бағдарламаны реттеу және тестілеу
8	$T_{Д}$	Құжаттарды рәсімдеу, пайдаланушыға нұсқаулар және түсіндірмелер жазу

4 к е с т е – Бағдарлама жасаушы білектілігін ескеретін коэффициент

Жұмыс тәжірибиесі	Біліктілік коэффициенті
Екі жылға дейін	0.8
2-3 жыл	1
3-5 жыл	1.1 – 1.2
5-7 жыл	1.3 – 1.4
7 жылдан көп	1.5 – 1.6

Бірыңғай тарифтік сеткадан көшірме (БТС)

5 к е с т е – Бірыңғай тарифтік сеткадан көшірме (БТС)

Еңбек ақы разряды	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18
Тарифтік коэффициент	1,0	1,07	1,15	1,24	1,33	1,43	1,54	1,66	1,78	1,91	2,05	2,25	2,37	2,55	2,74	2,95	3,17	3,41

5 кестенің жалғасы

Еңбек ақы разряды	19	20	21
Тарифтік коэффициент	3,67	3,94	4,24

1.alser.kz
2. lumadownload.com
3.sulpak.kz
4.alsi.kz
5. almaty.satu.kz
6. wit.ru
7. Ebay.com asa