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. З.Қ. Құралбаев

_____«____»_____**2014 ж.**
(қолы)

ДИПЛОМДЫҚ ЖОБА

Тақырыбы: «Қазақтелеком» акционерлік қоғамына басып кірулерді бақылау жүйесін орындау»

5В070400 – Есептеу техникасы және бағдарламалық қамтамасыз ету мамандығы бойынша

Орындаған: ВТк-10-1 Амангельдиева К.Ж.

Жетекші: ф.-м.ғ.к., проф. Құралбаев З.Қ.

Кеңесшілер :

Экономикалық бөлім бойынша :
доцент Боканова Г.Ш.
_____«09»_____ 2014 ж.
(қолы)

Өмір тіршілігі қауіпсіздігі бойынша:
т.ғ.к., аға оқытушы Муташева Г.С.
_____«09»_____ 2014 ж.
(қолы)

Есептеу техникасын қолдану бойынша :
ф.-м.ғ.к., проф. Құралбаев З.Қ.
_____«____»_____ 2014 ж.
(қолы)

Мөлшер бақылаушы:
аға оқытушы Ержан А.А.
_____«____»_____ 2014 ж.
(қолы)

Пікір жазушы :
АТУ, т.ғ.д., проф. Заурбеков Н.С.

_____«____»_____ 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 Амангельдиева Карлыгаш Жинисбеккызы

Жоба тақырыбы «Қазақтелеком» акционерлік қоғамына басып кірулерді бақылау жүйесін орындау
Ректордың «___» _____№____ бұйрығы бойынша бекітілген.

Аяқталған жұмысты тапсыру мерзімі: «____»_____2014 ж.

Жобаға қажетті алғашқы мәліметтер (талап етілетін жоба нәтижелерінің параметрлері) және нысананың бастапқы деректері:

Қазақтелеком акционерлік қоғам үшін Cisco Systems құрылғысын қолданып корпоротивтік желіге басып кіру жүйесінін құру.

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

– Техникалық тапсыма.
– қауіптілікті уақытылы анықтау, аумағын анықтау және жою;
– қауіптілікті анықтайтын механизмдерін жасап шығару және қауіптілікке әсер етуді анықтау;
– көптеген қауіптерге қарсы әрекет етуі, әдістері мен шаралары;
– себептер мен шарттарын анықтау;
– қолданылатын қорғаныс шараларының тиімділігі мен жеткіліктілігін бақылау;
– мәліметтік қауіпсіздікті қамтамасыз ету үшін тор аралық экран пайдаланылатын болады, себебі осы аппараттық кешен мәліметтік қауіпсіздікті қамтамасыз ететін мақсаттар мен тапсырмалардың орындалуын толығымен қамтамасыз ете алады.

Негізгі ұсынылатын әдебиеттер

1. Лукацкий А. Обнаружение Атак. – СПб.: БХВ – Санкт - Петербург, 2003.

2. 2005 CSI/FBI Computer Crime and Security Survey. Spring 2005. Computer Security Institute. Federal Bureau Investigation's ComputerIntrusion Squad.

3. Курушин В. Д., Минаев В. А. Компьютерные преступления и информационная безопасность. Справочник. М.: Новый Юрист, 1998.

4. Лукацкий А. В. Анатомия распределенной атаки. PCWeek/RE, № 5, 2000.

5. Концепция информационной безопасности корпоративной сети Акционерного общества «Казахтелеком». Проект, 2006.

6. Олифер В., Олифер Н. Компьютерные сети. Принципы, технологии, протоколы. – СПб: Издательский дом «Питер», 2005. – 864 с.

Жоба бойынша бөлімшелерге қатысты белгіленген кеңесшілер

Бөлім	Кеңесші	Мерзімі	Қолы
Негізгі бөлім	Құралбаев З.Қ.		
Тіршілік қауіпсіздігі	Муташева Г.С.		
Экономикалық бөлім	Боканова Г.Ш.		
Норма бақылаушы	Ержан А.А.		
Есептеу техникасын қолдану	Құралбаев З.Қ.		

диплом жобасын дайындау

КЕСТЕСІ

№ р/с	Тарау аттары, әзірленетін сұрақтардың тізімі	Жетекшіге ұсыну мерзімдері	Ескерту
1	Техникалық тапсырма		
2	қауіптілікті уақытылы анықтау, аумағын анықтау және жою;		
3	қауіптілікті анықтайтын механизмдерін жасап шығару және қауіптілікке әсер етуді анықтау		
4	көптеген қауіптерге қарсы әрекет етуі, әдістері мен шаралары;		

Тапсырманың берілген уақыты «_____»_____2014ж.

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

Жоба жетекшісі _____ ф.-м.ғ.д., проф. Құралбаев З.Қ.
(қолы)

Орындалатын тапсырманы қабылдаған студент _____ Амангельдиева Қ.Ж.
(қолы)

Аннотация

В данном дипломном проекте рассматривается вход в систему корпоративной сети АО «Қазақтелеком» с применением оборудование Cisco Systems. Цель данного проекта – провести обзор угрозбезопасности корпоративной сети, анализировать систему безопасности корпоративной сети, обосновать выбор системы обнаружения атак –модуль межсетевого экрана для Cisco Catalyst 6500 Series, обосновать выбор системы позволяющую обеспечить эффективную маршрутизцию, защиту трафика данных, голоса, видео – модуль Cisco NME-RVPN для маршрутизаторов семейств Cisco 2800 Seriesи 3800 SeriesIntegratedServicesRouters.

Аңдатпа

Бұл дипломдық жобада «Қазақтелеком» акционерлік қоғамы үшін Cisco Systems құрылғысын қолданып корпоративтік желіге басып кіру жүйесіне құру қарастырылады.Жобаның басты мақсаты – «Қазақтелеком» акционерлік қоғамы корпоративті желіде жүретін ақпарат алмасуға сырттан рұқсатсыз қолжеткізуді, нақтырақ айтсақ желіге жасалатын шабуылдардың алдын алу. Желіаралық бейне беттің модулыі Cisco Catalyst 6500 Series шабуылды анықтау жүйесін таңдауын түсіндіру,әсерлі бағыттаушымен қамтамасыз етудің, мәліметтер трафигінің қорғанысын, дауыстың, бейнебаян – модуль Cisco NME-RVPN, бағыттаушылар Cisco 2800 Series және 3800 Series Integrated Services Routers жүйесін таңдауын түсіндіру.

Annotation

In this diploma project the included in the system of corporate network of propulsion MODULE of "Қазақтелеком" is examined with application equipment of Cisco Systems. Aim of this project - to conduct the review of threats of safety to the corporate network, analyse the system of safety of corporate network, ground the choice of the system of finding out attacks is the module between a network screen for Cisco Catalyst 6500 Series, to ground the choice of the system allowing to provide effective маршрутизцию, defence of traffic of data, voice, video is the module of Cisco NME - RVPN for the routers of families of Cisco 2800 Series and 3800 SeriesIntegratedServicesRouters.

Мазмұны

1.Корпоративтік желілердің қауіпсіздігінен төнген қаупі**.**

1.1Басып кіру ұғымы

1.1.1Шабуыл үлгілері

1.1.2 Шабуылдарды іске асыру кезеңдері.

1.1.3 Шабуылдар нәтижесі.

1.2Корпоративтік тордың ерекшеліктері

1.3 Корпоративтік тордың мәліметтік қауіпсіздігін қамтамасыз ету мақсаттары мен тапсырмалары

2 Корпоративтік тордың қауіпсіздік жүйесі.

2.1 Корпоративтік тордың жалпы құрылымы.

2.2 Мәліметтік қауіпсіздікке қауіптер

2.2.1 Қауіптер көздері

2.2.2 Қауіптер моделі

2.3 Басып алушылықтарды бақылау жүйесінің құрылымы

2.3.1 Шабуылдарды анықтау технологисы

2.3.2 Шабуылдарды анықтау әдістері

2.3.3 Кәсіби жүйелер

2.3.4 Шабуылдарды анықтау

3 Басып алуларды бақылау жүйелерін іске асыру

3.1 Техникалық шешімді таңдау

3.2 CiscoCatalyst 6500 Series үшін тор аралық экранының сервистік модулін таңдауды негіздеу

3.2.1 Cisco Catalyst 6500 Series үшін FWSM модулінің артықшылықтары

3.3 Cisco 2800 Series және 3800 SeriesIntegratedServicesRouters мршрутизаторлар жанұясы үшін сервистік модуль CiscoNME-RVPN-ны таңдауды негіздеу.

3.3.1 NME-RVPN модуль артықшылықтары

3.4 NME-RVPN модульдың архитектурасы

3.5 Өнімнің техникалық сипаттамасы

3.6 Функциялық мүмкіндіктері

3.7 Сертификаттау мен мемлекеттік реттеу

3.8 Жүйелік талаптар

3.9 Қауіпсіздік политикасы

3.9.1.Қорғаныс стратегиясын таңдау

3.9.2 Торлық сенсорлардың қауіпсіздік политикасын орнату.

3.10 Тордың пайдалы өтімділік қабілетін есептеу

4 Тіршілік қауіпсіздігі

4.1 Еңбек жағдайын талдау

4.2Кондиционерлеу және ауаны жаңарту жүйелерін есептеу

4.2.1 Температура айырымы нәтижесінде алынатын жылу және

жылу жоғалту

4.2.2Шынылау арқылы күннің сәулеленуінен келетін жылу

4.2.3Адамдардан келетін жылу

4.2.4 Жарықтану аспаптарынан, оргтехникадан және құрылғылардан келетін жылу

4.2.5Ауа алмасуды есептеу

Кіріспе

Ақпараттық жүйелер қорғалған болуы тиіс. Бұл тезиспен ешкім бақталаспайды. Ақпараттық жүйелердің қауіпсіздігін екі әдіспен қамтамасыз етуге болады. Бірінші әдіс – толық қауіпсіздік жүйесін құру арқылы, рұқсат етілемеген барлық әрекеттердің алдын-алу. Алайда мұндай әдісті тәжірибе жүзінде жүзеге асыру мүмкін емес, оған келесідей себептер қатары бар:

- Қатесіз бағдарлама әлі де арман болып келеді. Өкінішке орай өндірушілер мұндай бағдарламаны ойлап табуға құштарсыз. Олар өздерінің өнімдерін неғұрлым жылдам шығарып, және сол арқылы ірі көлемде пайда табуға тырысады. Бағдарламалық жасақтамадағы қателіктердің кесірінен, толық қорғарғал жүйені шасап шығару мүмкін емес болып тұр. Ең қызығы әртүрлі қателіктердің кесірінен қорғау құрылғылары да зардап шегуде;
- Тіпті ең жоғарғы қорғалған жүйенің өзі, жоғарғы білікті қолданушының алдында осал. Мүмкіндігі жоғары қолданушылар қорғау саясатының талаптарын бұзуға қауқарлы. Бұл өз кезегінде, қорғаныс деңгейінің төмендеуіне әкеп соғады;
- Жүйенің қорғанысын неғұрлым жоғарылатқан сайын, соғұрлым онымен жұмыс істеу ыңғайсыз.

Осы саладағы ең беделді ақпарат көзі – Сан-Францискодағы ФБР бөлімшесінің компьютерлік жанжалдардың статистикалық мәліметтерін қолданамыз.

- 90 % респонденттер (ірі корпорациялар және мемлекеттік мекемелер) өз ақпарат қорларына сан түрлі шабуыл жасағанын тіркеген.
- 80 % респонденттер осындай шабуылдар себебінен көптеген қаржы жұмсады, бірақ соның ішінде тек 44 % -ы ғана сол жұмсалған қаржыларды есептей алды.

Соңғы жылдары қорғаныс саясатының бұзылуы салдарынан шығын көлемі өсті. Оған мысал: 2002 жылы – зардап сомасы 266 млн. АҚШ долларына тең келді, 2005 жылы – 365 млн. АҚШ доллары жұмсалса, ал 2007 жылы бұл зардап көрсеткіші 460 млн. АҚШ долларына жетті.

Шабуыл жиілігі және саны үнемі жоғары болған сайын, шабуылдың бастапқы кезеңін анықтап, жекешелендіру өте маңызды болып отыр. Және оған дер кезінде әрекет ету керек. Шиеленіскен жағдайда шабуылға араласу адамның әрекет етуінен де өте жоғары жылдамдықта болуы тиіс.

Ақпараттық жүйеге шабуыл жасаушылар, шабуыл жасаудың автоматтандырылған түрін қолданатын болғандықтан, шабуылды анықтау үрдісін автоматтандыруға себеп болды. Бір жарияланған мысалда, 8 сағаттың ішінде, 500 жерден, 2000-ға жуық Ғаламтор серверіне кіру әрекетін жүзеге асыру дерегі тіркелген (ол дегеніміз, 1 минут ішінде 4 шабуыл жасау деген сөз). Бұл жағдайда, шабуылды анықтаудың автоматтандырылған жүйесі шабуыл көзін іздеп табуға көмектесті. Бұл жүйе болмаса, шабуыл жасаушының әрекетін, шабуылдың өзін анықтау тапсырмасы мүмкін болмас еді.

Сол себепті, егер біз толық қорғаныс жүйесін құра алмасақ онда екінші тәсіл ретінде – ең болмаса, қауіпсіздік саясатын бұзудың барлығын анықтап,

оған лайықты түрде әрекет ету керек. Қарастырылып жатқан жұмыстағы дәл осы әрекет шабуылды анықтау жүйесін құруға мүмкіндік берді.

Шабуылды анықтау жүйесі, компьютерлік жүйеге шабуылға дайындалуға және оған қарсы тұруға көмектеседі. Олар желілер мен ақпараттық жүйелердің толық нүктелер қатарының ішінен ақпараттар жинап және осы ақпараттағы қорғаныс мәселесінің бар-жоғын талдайды. Қорғаныс әлсіздігін анықтау мақсатында, әлсіздікті іздеу жүйесі желілер мен жүйелерді тексеріп, баптау қателіктері мен жүйелік мәселелерінің бар-жоқтығын анықтайды. Әлсіздікті талдау технологиясы да, шабуылды анықтау технологиясы ретінде мекелерлерге жүйелік қорғаныс мәселелерімен байланысты өз ақпараттық қорларын жоғалтудан сақтауға мүмкіндік береді.

Желіаралық экранның сервистік модулы Cisco Catalyst 6500 Series және модуль Cisco NME-RVPN, ал бағыттаушыларға Cisco 2800 Series және 3800 Series Integrated Services Routers – ті таңдау арқылы, біз – желіаралық экран/VPN бағыттаушы, желінің қорғанысының жоғары деңгейін қамтамасыз ететін, өндіргіш және сенімді құрылғыларды аламыз. Бұл құрылғылар өз кезегінде мекемелерге желілердің қауіпсіздігін қамтамасыз етіп, сондай-ақ рұқсат етілмеген әрекеттерден қорғауға, байланыс арналары арқылы ауырлықты бөліп, әкімшіліктендіруді оңтайландыруға көмектеседі.

Осы дипломдық жобада корпоративтік желіге басып кірудің бақылау жүйесін үйлестіру сұрақтарын қарастыру қажет.

Көбінесе, келесідей жұмыстарды жүргізу керек:

– корпоративтік желілердің қауіпсіздік қаупін анықтау жұмыстарын жүргізу;

– корпоративтік желілердің қауіпсіздік жүйесін талдау;

– желіаралық бейне беттің модулы Cisco Catalyst 6500 Series шабуылды анықтау жүйесін таңдауын түсіндіру;

– әсерлі бағыттаушымен қамтамасыз етудің, мәліметтер трафигінің қорғанысын, дауыстың, бейнебаян – модуль Cisco NME-RVPN, бағыттаушылар Cisco 2800 Series және 3800 Series Integrated Services Routers жүйесін таңдауын түсіндіру;

– қажетті құралдарды орналастыруды жоспарлау.

1 Корпоративтік желілердің қауіпсіздігінен төнген қаупі

1.1 Басып кіру ұғымы

Желілік қорғаныс (Network Security) – бұл компьютерлік жүйелер мен желілердің мінездемесі ретінде орнататын, қарастырылған жүйелер және олардың элементтерінің сенімді жұмыс істеуін, тұтастығын, өз иесінің және пайдаланушылардың ақпараттарын сақталуын қамтамасыз етеді.

Қорғаныс мақсаттарына келесілер кіреді:

- құпиялылық (тек тіркелген пайдаланушылар ғана оқи алатынын немесе файлды не нысанды көшіре алатынын кепілдендіреді);
- басқару (тек тіркелген пайдаланушылар ғана ақпаратқа қол жеткізу туралы шешім қабылдай алады);
- тұтастығы (тек тіркелген пайдаланушылар ғана файл не нысанды өзгерте немесе өшіре алады);
- сенімділік (нысанды сипаттаудың немесе бөлшектеріне дәреже берудің дұрыстығы);
- кіру мүмкіндігі (тіркелмеген пайдаланушы тіркелген пайдаланушыларға файлдар немесе басқа да жүйе көздеріне енуге уақытша кіру мүмкіндігін шектей алмайды);
- айдалылығы (нақты мақсатқа қол жеткізудің жарамдылылығы).

Шабуылды анықтау жүйесі – жүйелік және желілік қорлардың тұтас қатарын пайдалану ақпараттарын жинап, содан кейін ақпаратқа басып кірулердің (мекеменің сыртынан келетін шабуылдар) және зиян келтіре пайдаланулардың (мекеменің ішінен келетін шабуылдар) бар-жоқтығына талдау жасайды.

Қауіпсіздік саясаты – өзінің қорғаныс жүйесінің қатынасында мекеменің алатын орны. Ол мекеменің өте маңызды қорларына қайсысы кіретінін анықтап және олардың қандай деңгейде қорғалуы керек екендігін орнатады.

Қауіпсіздік оқиғасы – желі торабының қызмет ету кезінде тораптардың жағдайын өзгертетін әртүрлі оқиғалар (events) орын алады. Бұл оқиғалар қауіпсіздік қызметі тарапынан – қызмет (action) және адресат (target) сияқты екі құрамдастың көмгімен ұсынылуы мүмкін.

Қызмет – бұл қадамдар, қандайда бір нәтижеге жету үшін жүйенің субъектісі қолданатын әдіс (пайдаланушымен, үрдіспен және т.с.с.)

Адресат – бұл жүйенің логикалық (есеп жүргізу, барысы немесе көрсеткіші) немесе физикалық (желі торабы, желі, құрасдас бөлік) объектісі.

Ақпараттық жүйенің әлсіздігі (vulnerability) – бұл ақпараттық жүйенің кез-келген мінездемесі болып табылады, және осындай жағдайлар бұзушының қолдануы қауіптің жүзеге асуына әкеп соғады.

Ақпараттық жүйенің қаупі (threat) деп – жүйелік қорларға зардап (материалды, моральді немесе басқадай) келтіруі мүмкін, болуы мүмкін жағдайлар, іс-әрекеттер, оқиғалар немесе құбылыстарды айтамыз.

Әлсіздіктер келесідей болып жіктеледі:

А) жобалау әлсіздігі – бұл өте маңызды әлсіздік түрі болып табылады, себебі оның салдарын жою қиындыққа әкеп соғады;

Б) жүзеге асыру әлсіздігі – алгаритимнің немесе жобаның қауіпсіздігі тарапынан, бағдарламалық немесе аппараттық қамтамасыз етуді жүзеге асыру сатысында байқалады;

В) кескін әлсіздігі – бағдарламалық немесе аппараттық қамтамасыз етудегі кескін қателіктері;

Ақпараттық жүйеге шабуыл (attack) дегеніміз – осы ақпараттық жүйенің әлсіздігін пайдалану арқылы қауіпті жүзеге асыруына әкеп соғатын іс-әрекет немесе бұзушының өзара байланысты іс-әрекетінің жалғасы.

Шабуылдың, қауіпсіздік оқиғасынан айырмашылығы – шабуыл жасалған жағдайда, бұзушы қандай да бір нәтижеге жетуге тырысады. Бұл қауіпсіздік саясатына қайшы келетін іс-әрекет.

Сигнатуралар – бұл белгілі шабуылдар немесе жүйелердегі зиян келтіре пайдаланулардың салыстырмалы үлгісі. Олар оңай (белгіленген шарттар немесе әмірлерді іздеуге лайықты белгілер қатары) немесе қиын (заңды математикалық тұрғыда жазылған, іс-әрекет және тіркеу журналы жолағы жинағының ізінше, қорғаныс жағдайын өзгерту).

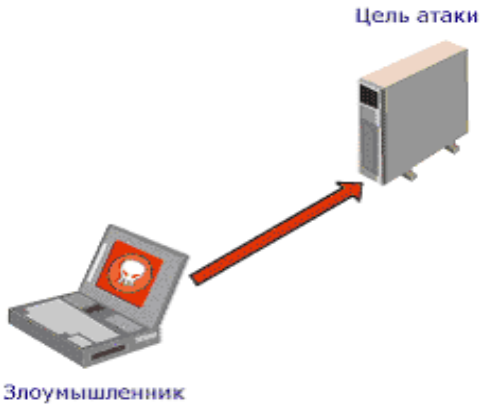
Мекеменің желісіне ену – сәтті жасалған (яғни жүзеге асырылған) шабуыл.

Intrusion Detection System (IDS) – шабуылды анықтау жүйесі.

1.1.1 Шабуыл үлгілері

«Дәстүрлі» шабуыл үлгісі

Дәстүрлі шабуыл үлгісі «біреуі-біреуіне» (1.1 сурет) немесе «біреуі-көбіне» (1.2 сурет) деген қағида бойынша құрылады, яғни шабуыл бір нүктеден келеді. Көптеген жағдайда шабуыл көзін жасыру немесе оның табылуын қиындату мақсатында айырма әдісі қолданылады. Зиянкелтіруші өзінің шабуылдарын тікелей таңдалған мақсатқа емес, тораптар тізбегі арқылы жүзеге асырады.



1.1 Сурет – «біреуі-біреуіне» қатынасы

1.2 Сурет – «біреуі-көбіне» қатынасы

Дәстүрлі қорғаныс құралдарын ойнап табушылар дәл осы шабуылдың классикалық үлгісіне сүйенеді. Әр түрлі желі нүктелерінде консоль басқармасы орталығына ақпаратты ұсынатын сан түрлі қорғаныс жүйесінің агенттері орнатылады. Бұл жүйенің кең ауқымдатуын, қашықтандырылған басқарманың оңайлылығын және т.б. жұмысын жеңілдетеді.

«Бөлшектенген» шабуыл үлгісі.

Бұл шабуылдар – бір немесе бірнеше зиянкелтірушіге, бір немесе бірнеше тораптарға бір мезетте орындалатын жүздеген және мыңдаған шабуылдарды өткізуге мүмкіндік береді.

Бөлшектенген немесе үйлестірілген шабуылдар (coordinated attack) үлгісі «көптің біреуге» (1.3 сурет) және «көптің көпке»(1.4 сурет) деген қатынас қағидаларына сүйенеді. Барлық бөлшектенген шабуылдар (Distributed DoS, DDoS) «классикалық» шабуылдың «қызмет көрсетуде бас тарту» типіне негізделген, дәлірек айтқанда Flood немесе Storm – шабуылдар деген атаулармен белгілі жиынтығына негізделген. Дәл осы шабуылдардың мағынасы үлкен көлемде тапсырылған тораптар жүйесінде (шабуыл мақсаты) құрылады, тіпті мұндай әрекет тораптардың құрылымының бір жола жойылуына әкелуі мүмкін, себебі тіркелген пайдаланушылардың сұранысын өңдей алмайды.

1.3 – Сурет «Көптің біреуге» қатынасы

1.4 – Сурет «Көптің көпке» қатынасы

Дәл осы тәсіл шабуылдаушы тарабына келесідей артықшылықтары бар:

Құпиялылығы. Бірден бірнеше мекен-жайлармен жұмыс істеу, үйреншікті механизммен шабуылдайтындарды анықтау айтарлықтай қиындайды (желілік экрандармен, шабуылды анықтау жүйелерімен және т.б.). Қазіргі заманауи қорғаныс құралдарының барлығы бірдей қолдана бермейтін деректерді өзара байланыстыру механизімін қолдану қажет.

Шабуыл күші. Бір нүктеден жасалатын ұқсас шабуылдан гөрі, бірнеше желі нүктелерінен жасалынатын шабуылдар қысқа уақыт ішінде аса қуатты шабуылды жүзеге асыруға мүмкіндік береді. Жоғарыда айтылған жағдайдай

(құпиялылығы) бөлшектенген шабуылды оқшаулау және анықтау әдісі сияқты әрекеттердің тиімділігі аз болып келеді.

Алуан түрлі деректерді алу. Әр түрлі мекен-жайлар арқылы жұмыс істей отырып, оның ішінде әртүрлі желілерде орналасқан мекен-жайлар арқылы, үйреншікті іс-әрекетпен салыстырғанда бір нүктеден жүзеге асыратын шабуылдың толық объектісі көбірек деректер жинақтай алады. Мұндай үлгі арқылы шабуыл мақсатына дейін ең қысқа қозғалыс бағытын анықтап алуға болады, сондай-ақ әр түрлі желілік тораптардың «сенімді» қарым-қатынасы және т.б. Мысалы, А торабынан зиянкелтіруші «троянский конь» бағдарламасы арқылы шабуыл мақсатына қол жеткізе алады, ал В торабынан – қол жеткізе алмайды.

Шектеу күрделілігі. Көрсетілген артықшылықтар бөлшектенген шабуылды шектеуді қиындатады. Сонымен қатар Internet-серверды істен шығаруға жеткілікті «троянский конь» типті бағдарламалары бар түйіндердің мөлшерін санап анықтауға болады. Қалыпты 128 Кбит/с DSL-байланысы кезінде 1 с-та жіберілетін пакеттер саны 800-ден көп емес (128/(IP-пакеттың Кбит-тағы орташа өлшемі)). IP-пакеттың ең аз мөлшері 20 байт (тек атауы)болғандықтан, онда DSL-байланысы 128 000 / 20 / 8 = 800 пакет жіберуге мүмкіндік береді. Қалғаны сервердың өнімділігіне байланысты болады. Мысалы, TopLayerNetworks компаниясының тестілеуіне сай MSIIS 5.0 Pentium 400 компьютеры секундына 100-200 пакет өңдей алады. Демек, бір DSL-байланысы бар үй компьютері 6-7 өнімді емес Web-серверді істен шығара алады. Web –серверге компьютер қуаты өскен сайын, шабуылға катысатын түйіндердің саны да өседі.

Бөлінген шабуылдар әдісі бойынша құрылған шабуылдарды анықтау өте қиын. Шабуылдарды анықтаудың торлық жүйелері оларды сенімсіз анықтайды, әсіресе егер агенттер мен серверлер арасындағы байланыс құпияланған болса. Шабуылдарды анықтау жүйелерінің түйіндік дәрежесі осы мақсатқа көбірек жарамды болып келеді. Осындай шабуылдарды агентті орнату кезеңінде анықтауға болады.

Оны нәтижесінде яғни соңында жасау өте қиын себебі агент ОЖ бөлігі ретінде жұмыс істейді. Әсіресе агенттерді Linux және OpenBSD сияқты "ашық" ОЖ-лар үшін кірістіру қауіпті, себебі агент оперативтік жүйенің ядросына кірістірілуі мүмкін, ол өз кезегінде осындай агентті анықтауды қиындатады. Дәстүрлі шабуылда шабуылдаушыға периодты түрде айғақталған түйінге "кіріп тұруға" тура келеді. Ол тіркеу журналдарының анализі арқылы немесе автоматталған құралдармен анықталуы мүмкін.

Бөлінген шабуылда мұндай мәселе туындамайды, себебі агент алдын ала орнатылған, сондықтан айғақталған түйінге периодты түрде "кіріп тұрудың" қажеті жоқ, барлығын алдын ала бағдарламаланған агент орындайды.

Гибридты шабуылдар (hybridattack), сонымен қатар аралас қауіп (blendedthreat), дамыған червь (advancedworm) немесе гидра (hydraattack) деп аталатын шабуылдау әдісі ретінде дамыған.

Осындай шабуылдардың мысалы болып Nimda, CodeRed, SirCam және Klez келеді. Гибридты шабуылдардың бөлінген шабуылдардан негізгі айырмашылығы (ол бөлінген шабуылдардың бір модификациясы немесе бір кеңейтілімі) - өз демондарын басқаратын мастер -агенттердің болмауы. Сондықтан нағыз көзін,себебін анықтау тіптен мүмкін емес. Оған қоса егер бұрын пайдаланушы вирустың қосылуын ерікті немесе еріксіз түрде өзі ұйымдастыруы керек болса, онда гибридты шабуылдар үшін бұл шарт қажет емес. Олар өздері осал түйіндерді іздеп, оларға сіңіп кейін ешкімнің көмегінсіз ақ көбейіп отырады.

1.1 К е с т е - Гибридты шабуылдардан қорғаудың әдістері.

	Желі қорғанысы	Операциондық жүйе қорғанысы	Қосымша қорғанысы
Өнімдер	Желілік сканерлер	Серверлер және жұмыс істеп тұрған станциялар сканерлері	Қосымша сканерлері
	Шабуылды анықтаудың желілік жүйесі	Серверлер мен жұмыс істеп тұрған станцияларға жасалған шабуылдарды анықтау жүйесі	Деректер базасының сканерлері
	Желіаралық бейне беттер	Арнайы антивирустар	Қосымшаларға арналған антивирустар
Қызметтер	Қашықтандырылған сканерлеу	Қашықтандырылған сканерлеу	Қашықтандырылған сканерлеу
	Қашықтандырылған сканерлеу Қашықтандырылған сканерлеу	Қашықтықтан мониторинг жасау және шабуылды анықтау жүйесімен	Мониторинг және қосымшаның қорғанысы

1.1 кестенің жалғасы

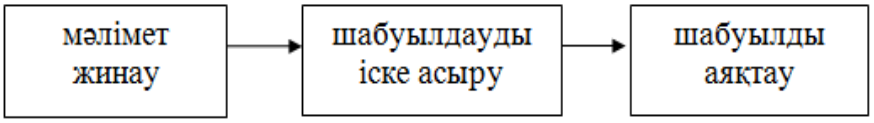
Консалтинг	Қауіпсіздік саясатын енгізу және әзірлеу	Қауіпсіздік саясатын енгізу және әзірлеу	Қосымшалардың қауіпсіздік саясатын енгізу және әзірлеу
	Қорғаныс талдауы	Қорғаныс талдауы	Қорғаныс талдауы
	Енуге байланысты сынақтар	Енуге байланысты сынақтар	Енуге байланысты сынақтар
	Баптау және конфигурация лау	Баптау және ОЖ конфигурациялау	Баптау және конфигурация лау
	Жанжалға әрекет ету	Жанжалға әрекет ету	Жанжалға әрекет ету
Оқыту	Қауіпсіздік стандарттары және саясатын зерттеу	Қауіпсіздік стандарттары және саясатын зерттеу	Қауіпсіздік стандарттары және саясатын зерттеу
	Шабуылды анықтау жүйесін, қауіпсіздік сканерлерін және желіаралық бейне беттерді зерттеу	Шабуылды анықтау жүйесін және қауіпсіздік сканерлерін зерттеу	Шабуылды анықтау жүйесін және қауіпсіздік сканерлерін

1.1.2 Шабуылдарды іске асыру кезеңдері.

Шабуылдарды іске асырудың негізгі механизмдерін қарастырайық. Ол осы шабуылдарды анықтаудың әдістерін түсіну үшін қажет. Сонымен қатар, шабуылдаушылардың іс-әрекеттерінің принциптерін түсіну, сіздің торыңыздың сәтті қорғанысына алып келеді.

Шабуылдарды іске асырудың келесідей кезеңдері бар:

- мәлімет жинау (information gathering);
- шабуылдауды іске асыру (exploration);
- шабуылды аяқтау (finishingattack).



1.5 сурет – Шабуылды іске асыру

Бірінші кезең - шабуылданатын жүйе мен түйін жайлы мәлімет жинау. Ол келесідей іс-әрекеттерден тұрады, тордың топологиясын, шабуылданатын түйіннің оперативтік жүйесінің түрі мен типін, сонымен қатар қол жетімді торлық және басқа да сервистерді анықтау.

Ол іс-әрекеттер түрлі әдістермен іске асырылады:

– айналаны сараптау. Бұл кезеңде шабуылдаушы жоспарланып отырған шабуылдау нысанының айналасындағы торлық аймақтарын саралайды. Ондай аймақтарға, мысалы, Internet-провайдерлер "құрбандар" немесе шабуылданған компанияның жойылған офисының түйіндері жатқызылады. Осы кезеңде шабуылдаушы "сенімді" жүйелер мен түйіндердің адрестерін анықтауға әрекет етуі мүмкін, олар тікелей шабуылдау нысанымен (мысалы маршрутизатор ISP) байланысты. Осындай іс-әрекеттерді анықтау әлдеқайда қиын, себебі олар қорғаныс құралдарымен басқарылатын, ұзақ уақыт бойы және аумақ сыртымен орындалады (тор аралық экрандармен, шабуылдарды анықтау жүйелерімен және т.б.);

– тор топологиясын идентификациялау. Шабуылдаушылар пайдаланылатын тор топологиясын анықтаудың екі түрін атауға болады (network topology detection),олар: "TTL өзгерту" ("TTL modulation") және "маршрутты жазу" ("record route"). Unix үшін traceroute және Windows үшін tracert программалары тор топологиясын анықтаудың бірінші әдісін пайдаланады. Олар IP-пакет тақырыпшасында Live ("өмір сүру уақыты") жолын пайдаланады, ол тор пакетының қанша маршрутизатордан өткеніне байланысты өзгеріп отырады. ping утилитасы ICMP-пакетының маршрутын жазу үшін пайдаланылуы мүмкін. Көбінде торлық топологияны көптеген торлық құралдарда орнатылған, қорғанысы қате жасалған SNMP протоколының көмегімен анықтауға болады. RIP протоколының көмегімен тордағы маршрутизацияның кестесі жайлы мәліметті алуға болады;

– түйіндерді идентификациялау. Түйінді идентификациялау (host detection), ереже бойынша, ping утилитасының көмегімен протокол ICMP ECHO_REQUEST командасын жіберу арқылы орындалады. ECHO_REPLY жауап хабарламасы, түйіннің қол жетімділігін айтады.

Еркін таратылатын бағдарламалар бар, олар түйіндердің көп мөлшерін параллельді идентификациялау процессін автоматизациялайды және жылдамдатады, мысалға fping немесе nmap. Берілген әдістің қауіптілігі,түйіндердің стандартты құралдарымен ECHO_REQUEST запростары бекітілмейді.

Ол үшіін тарфикты анализдау құралдарын пайдаланған жөн, тораралық экрандар мен шабуылдарды анықтау жүйелері.

Бірақ та бұл әдіс бірнеше кемшіліктерге ие. Біріншіден, көптеген торлық құрылғылар мен бағдарламалар ICMP-пакеттерді шектейді де оларды ішкі торға (немесе сыртқа) өткізбейді.

Нәтижесінде айқын емес бейне пайда болады. Ал бір жағынан ICMP-пакетті шектеу шабуылдаушыға маршрутизаторлардың, тор аралық экрандардың және т.б. бар екендігін хабарлайды.

Екіншіден, ICMP-запростарын пайдалану шабуылдың көзін оңай анықтауға мүмкіндік береді;

– сервистерді идентификациялау және порттарды сканерлеу. Сервистерді идентификациялау (service detection), ереже бойынша, ашық порттарды анықтау арқылы іске асады (port scanning). Мұндай порттар TCP және UDP протоколында құрылған сервистермен жиі байланысты болады. Мысалға, ашық 80-шы порт Web-сервердың, 25-ші порт -пошталық SMTP-сервердың, 31337-шы троян атының BackOrifice серверлік бөлігінің бар екендігін түсіндіреді.

Сервистерді идентификациялау мен порттарды сканерлеу үшін, түрлі бағдарламалар пайдаланылуы мүмкін, соның ішінде еркін таралатындары да бар. Мысалы, nmap және netcat;

– оперативтік жүйені идентификациялау. ОЖ (OS detection) жойылған түрде анықтаудың негізгі механизмы - запростарға келетін жауаптардың анализі, ол түрлі оперативтік жүйелердегі, түрлі TCP/IP-ағымдарды иеленуді ескереді.

Әрбір ОЖ-да TCP/IP протоколдарының ағымы өзінше ұйымдастырылған, ол арнайы запростар мен оларға жауаптар көмегімен жойылған түйінде қандай ОЖ-ның орналасқанын анықтауға мүмкіндік береді;

– түйіннің рөлін анықтау. Шабуылдаушы түйін жайлы мәлімет жинау кезеңінің соңғы қадамдарының бірі оның рөлін анықтау, мысалы, Web-сервердың немесе тор аралық экранның қызметтерін орныдау.

Бұл қадам алдын ала жиналған, яғни белсенді сервистер, түйіндердің атауы, тор топологиясы және т.б. жайлы мәліметтердің негізінде орындалады;

– түйіннің осалдығын анықтау. Соңғы қадам - осал жерлерін іздеу (searching vulnerabilities). Осы қадамда шабуылдаушы түрлі автоматталған құралдардың немесе қолдық әдістің көмегімен осал жерлерін анықтайды, олар шабуылды ұйымдастыру үшін қолданылады. Мұндай автоматталған құралдар ретінде ShadowSecurityScanner, nmap, Retina және т.б. боуы мүмкін.

Шабуылдарды іске асыру. Шабуылдаушы екінші кезеңде шабуылдарды іске асырудың екі нысанын назарға алатынын атап өту керек.

Біріншіден, түйіннің өзіне заңсыз кіру және оның мәліметтерін алу. Екіншіден, басқа да түйіндерге алдағы шабуылдарды ұйымдастыру үішн түйіннің өзіне заңсыз кіру. Бірінші нысан, ереже бойынша, тек екіншіні іске асырғаннан соң орындалады.

Демек, алдымен шабуылдаушы алдағы шабуылдарды жүргізу үшін өзіне база жасап алады, осыдан соң ғана басқа да түйіндерге кіреді. Ол шабуыл көзінің орналасуын жасыру мен оны анықтауды әлдеқайда қиындату үшін қажет.

Тікелей қол жетімділік кезінде шабуылдарды іске асыру екі кезеңге бөлінеді:

– жасырын кіру. Периметрды қорғау құралдарынан жасырын өту дегенді білдіреді (мысалы, тор аралық экранды). Ол түрлі жолдармен іске асырылуы мүмкін. Мысалы, компьютер сервисының осалдығын пайдалану, "қарауыл" сыртқа немесе қауіпті құрамды электрондық пошта арқылы (макровирустар) немесе Java аплеттері арқылы жіберу. Мұндай құрамдар тор аралық экрандарда "туннель" пайдаланылуы мүмкін (VPN туннельдерімен шатастырмау керек), олар арқылы кейін шабуылдаушы кіреді. Осы кезеңге арнайы утилитаның көмегімен (мысалы, L0phtCrack немес Crack) администратордың немесе басқа пайдаланушының құпия сөзін таңдауды жатқызуға да болады;

– бақылау орнату. Шабуылдаушы жасырын кірген соң, шабуылданатын түйінге бақылау орнатады. Ол "троянский конь" типті бағдарламаны енгізу арқылы іске асырылады (мысалы, NetBus немесе BackOrifice). Қажетті түйінге бақылауды орнатып, "іздерді жойған " соң, шабуылдаушы барлық қажетті заңсыз немесе әдетті емес іс әрекеттерді, шабуылданып жатқан компьютер иесінің білуінсіз ақ жасай алады. Сонымен қатар корпоративті тор түйінінде бақылауды орнату, ОЖ-ны қайта жүктеу кезінде де сақталуы керек. Ол жүктеліп отырған біреуін алмастыру арқылы немесе қауіпті кодты автожүктеу немесе жүйелік реестрдың файлына ссылкамен жіберу арқылы іске асуы мүмкін.

Бізге белгілі жағдай, шабуылдаушы торлық картаның EEPROM-ын қайта жобалап және кейінннен де ОЖ-ны қайта орнатудан соң да ол заңсыз немсе рұқсат етілмеген іс әрекеттерді іске асыра алды. Осы мысалдың ең қарапайым модификациясы торлық жүктелудің сценарийне қажетті кодты немесе үзіндіні енгізу болып табылады (мысалы, ОЖ үшін Novell Netware).

Шабуылды аяқтау

Шабуылды аяқтау кезеңі болып шабуылдаушы жағынан "іздерді жою" табылады. Әдетте ол түйінді тіркеу журналдарынан сәйкес жазбалар мен басқа да іс әрекеттерді жою арқылы іске асады, сол арқылы шабуылданған жүйені бастапқы қалыпқа "шабуылға дейінгі" келтіреді.

1.1.3 Шабуылдар нәтижесі

Шабуылдар нәтижесінің келесідей сыныптамасы бар:

– қол жетімділік құқықтарын кеңейту (increasedaccess) –торда немесе дәл бір бәсекелес түйінде қол жетімділік құқықтарының кеңеюіне алып келетін кез келген рұқсат етілмеген істер (компьютерде, маршрутизаторда және т.б.);

– мәліметтің өзгеруі (corruptionofinformation) – тор түйіндерінде сақталатын немесе оны тормен жөнелту кезіндегі мәліметті рұқсат етілмеген түрде өзгерту;

– мәліметті ашу (disclosureofinformation) – қол жетімділікке ие емес тұлғалардың арасында мәліметті тарату;

– сервистерді ұрлау (theftofservice) – рұқсат етілмеген түрде компьютерді немсе торлық сервистерді басқа пайдаланушыларға қызмет көрсету сапасын өзгертпей пайдалану;

– қызмет көрсетуден бас тарту (denialofservice) – өнімділікті мақсатты түрде төмендету немесе торға немесе компьютерге және оның қорларына қол жетімділікті шектеу.

1.2 Корпоративтік тордың ерекшеліктері

Корпоративтік торлар (немесе өндірсі масштабындағы торлар) өндірістің барлық аумағындағы компьютерлердің көп мөлшерін біріктіреді. Корпоративтік торды құрау кезіндегі негізгі тапсырма жеке жергілікті кеңселік және филиалдық торларды ресурстары ортақ бір жүйеге біріктіру. Осы тапсырманы шешу үшін глобалды қосылыстарды, яғни телефондық және жерсеріктік каналдарды, радиоканалдарды пайдалану қажеттілігі тууы мүмкін.

Корпоративтік торлар өзінің жоғары гетерогендік дәрежесімен ерекшеленеді, компьютер, торлық жабдықтың, операциондық жүйенің типтері әртүрлі болуы мүмкін.

Корпоративтік тор мәліметті сақтау, өңдеу мен беру құралдары, әдістері мен персоналының жиынтығы болып табылады. [5]

Корпоративтік тор компанияның профильдік және қаржылық-шаруашылық жұмысын автоматизациялау үшін арналған және келесі тапсырмаларды шешуге арналған:

– компанияның бизнестік жұмысындағы түрлі тапсырмаларды шешімін қамтамасыз ететін, автоматталған жүйелердің жұмысын қолдап тұру;

– байланыс қызметтерін ұсыну технологиялық процесін басқару;

– ұсынылатын байланыс қызметтерінің биллингін қамтамасыз ету;

– компания ішінде электронды құжат жинауды және құжаттама жүргізуді қамтамасыз ету;

– компанияның корпоративтік торын пайдаланушыларға ресурстарға қол жетімділікті қамтамасыз ету (файлдық серверлерге, принтерлрге, база серверлеріне);

– компанияның корпоративтік торын пайдаланушыларға галамторға қол жетімділігін қамтамасыз ету;

– компанияның корпоративтік торын пайдаланушыларға, сыртқы организациялар мен жеке тұлғаларға қатысты электрондық түрде қызметтік хат алмасу мүмкіндігін беру;

– корпоративтік тормен қорғалатын объекттер:

– мәліметтік ресурстар (магниттік, оптикалық және басқа да құралдардағы құжаттар мен жазбалар, сонымен қатар тор арқылы алмасатын мәліметтер);

– аппараттық құралдар (жұмыстық станциялар, серверлер, принтерлер, алшақ орналасқан жабдықтар, ақаусыз қуат алу көздері және т.б.);

– бағдарламалық құралдар (жүйелік прикладное бағдарламалық қамтамасыз етулер);

– торлық қамтамасыз етулер (маршрутизаторлар, коммутаторлар, модемдер, байланыс каналдары және т.б.);

– мәліметті тасушылар (компьютерлік, қағаздық).

1.3 Корпоративтік тордың мәліметтік қауіпсіздігін қамтамасыз ету мақсаттары мен тапсырмалары

Компанияның корпоративтік торының мәліметтік қауіпсіздігін қамтамасыз ету мақсаттары мен тапсырмаларын анықтап алу қажет.

Мысал ретінде ДИС АҚ "Қазақтелеком" компаниясының корпоративтік жүйесін аламыз.

Мәліметтік қауіпсіздікті қамтамасыз етудің стратегиялық мақсаты компанияның, клиенттерінің, серіктестерінің түсініктерін компанияның корпоративтік торының қызметі барысына араласу арқылы зиян келтіру мүмкіндігінен қорғау

Компанияның мәліметтік қауіпсіздігін қамтамасыз етудің негізгі тапсырмалары [5]:

– қауіптілікті уақытылы анықтау, аумағын анықтау және жою;

– қауіптілікті анықтайтын механизмдерін жасап шығару және қауіптілікке әсер етуді анықтау;

– көптеген қауіптерге қарсы әрекет етуі, әдістері мен шаралары;

– себептер мен шарттарын анықтау;

– қолданылатын қорғаныс шараларының тиімділігі мен жеткіліктілігін бақылау;

– мәліметтік қауіпсіздікті қамтамасыз ету үшін тор аралық экран пайдаланылатын болады, себебі осы аппараттық кешен мәліметтік қауіпсіздікті қамтамасыз ететін мақсаттар мен тапсырмалардың орындалуын толығымен қамтамасыз ете алады.

2 Корпоративтік тордың қауіпсіздік жүйесі

2.1 Корпоративтік тордың жалпы құрылымы

Мысал ретінде "Қазақтелеком" АҚ Мәліметтік Жүйе Дирекциясының корпоративтік торы алынды.

Берілген компанияның корпоративтік торы келесілерден (А Қосымшасы):

- Proxy-, Web-, пошталық серверлер;
- IP-телефониясының торы;

- торды басқару, пайдалану және мәлімет тарату,
- ұйымдастыру блогының пайдалану торы;
- серверлер торы (NAT пайдалану арқылы Ғаламторға кіру).

2.2 Мәліметтік қауіпсіздікке қауіптер

2.2.1 Қауіптер көздері

Корпоративтік торға әсері бойынша қауіп көздерін сыртқы және ішкі деп бөлуге болады. [5]

Ішкі қауіп көздеріне:

– ішкі бұзушылар;

– аппараттық құралдар (жұмыстық станциялар, серверлер, принтерлер, алшақ орналасқан құралдар);

– торлық қамтамасыз етулер (маршрутизаторлар, коммутаторлар, модемдер, байланыс каналдары және т. б.);

– өмір сүруді қамтамасыз ететін жүйелер (энергиямен қамтамасыз ету жүйелері, кондиционерлеу мен сумен қамтамассыз ету жүйелері).

Сыртқы көздерге:

– сыртқы бұзушылар;

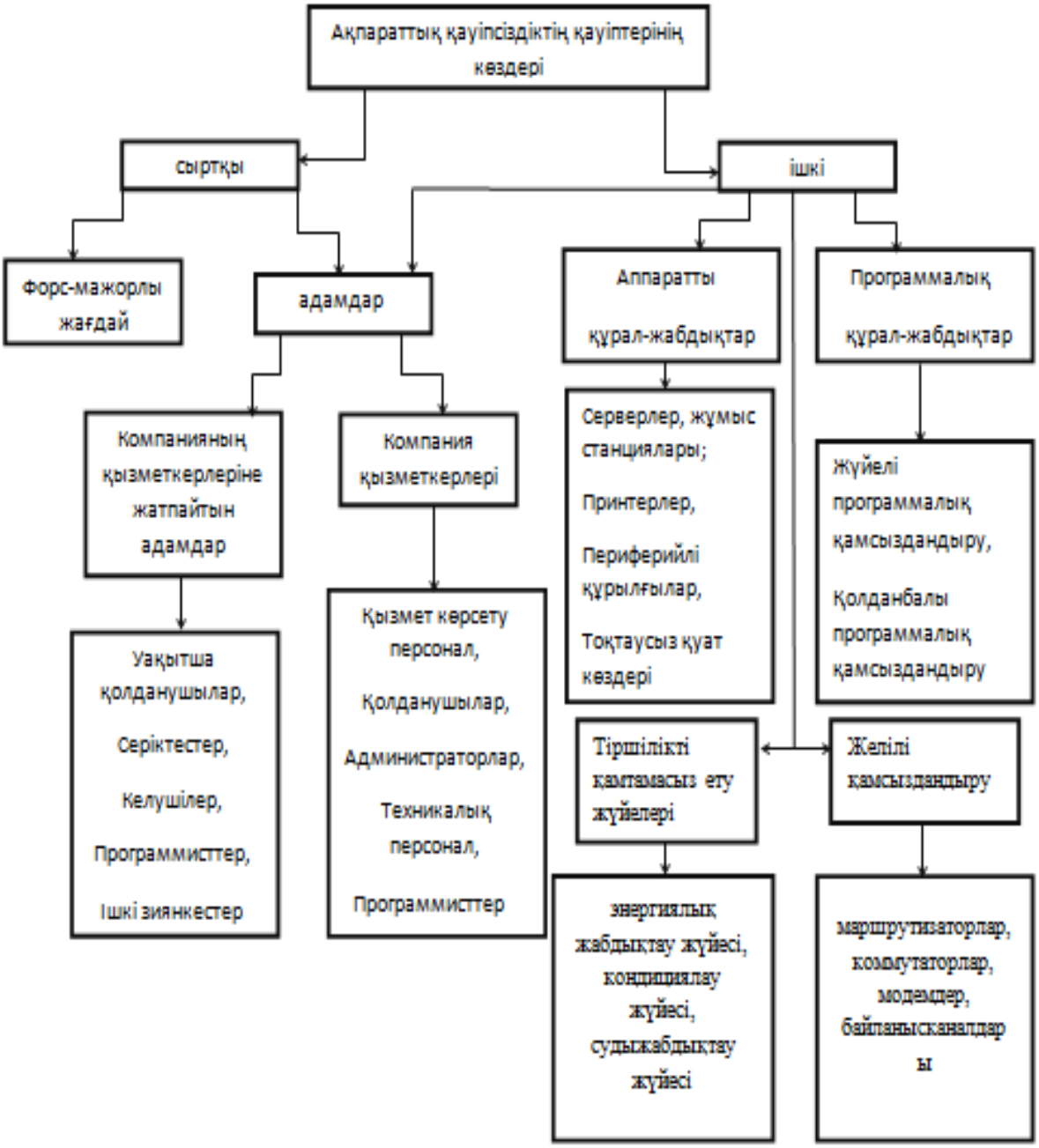
– кенеттен болатын жағдайлар.

– мәліметтік ресурстарға әсері бойынша мақсатты және оқыстан болған қауіптер.

Мақсатты (жоспарланған) қауіптер адамдардың жаман ойларымен немесе мақсаттарымен байланысты.

Оқыстан болған қауіптер корпоративтік тордың элементтерін жобалаудағы қателермен бағдарламалық қамтамасыз етулерде, қызметшілердің іс әректтерімен және т.б. пайда болған.

Қауіптер көзінің сипаттамасы 2.1 суретте көрсетілген.



2.1 сурет – Қауіптер көзі

2.2.2 Қауіптер моделі

Кесте 2.1 қауіптер моделі көрсетілген, ол мүмкін қауіптіліктерді анықтайды.

Қауіптің әрбір түрі үшін кестеде, берілген қауіптің пайда болу көзі көрсетілген.

Бөлімдердегі қауіптер түрі мен бұзушылар категориясы пункттерде мағынасы бойнша орналасқан.

2.1 к е с т е - Модель угроз информационной безопасности

№ п/п	Қауіптердің түрі	Қауіптерге сипаттама	Бастау, бұзушының дәрежесі
1.	Кесімді адам факторларының қауіпіне, себепті қасақана пайда болатын қауіптер жатады		
1.1	Жүйелерде және қосымшаларда авторластырған қолданушылардың дұрыс емес әсерлер	Оған рұқсат етілген есептік жазулар бұзушымен қолдануы, телекоммуникацияларға желілерге басқаруларға жүйелерде дұрыс емес әсерлерге шешілмеген мақсаттарда, сол санда, ,SAP/R3 және басқа жүйелерде	Әкімшілер, қолданушылар, бағдарламашылар, әріптестер, уақытша қолданушылар, алып тастаған қолданушылар
1.2	Ақау қызмет көрсетуде	Жүйелерде, қосымшаларда және базасыларда қызмет көрсетуде ақауға пайда болуға осы бағыттағанын біле тұра әсерлердің орындауы	Әкімшілер, техникалық қызметші, сыртқы қаскүнемдер, бағдарламашылар, әріптестер, қолданушылар, алып тастаған қолданушылар, уақытша қолданушылар
1.3	Енгізу зиян келтіретін немесе қиратушы программалық қамтамасыз етуді	Енгізу зиян келтіретін немесе вирустарды, « троя аттардың », « құрттарды », « логикалық бомбаларды қосатын қиратушы программалық қамтамасыз етуді » және бас-сираққа жетектеп жүнетін	Сыртқы қаскүнемдер, алып тастаған қолданушылар, қолданушылар, әріптестер, уақытша

2.1 кесте жалғасы

		немесе осал жері жүйедің үстінде толық бақылаудың бірлескен желіге, және алуға жұмыста компоненттердің бұзушылыққа	қолданушылар, өңдеушілер, бағдарламашылар, техникалық қызметші, әкімшілер
1.4	Авторластырған қолданушылармен атыға ауыстырып жіберуі	Рұқсаттың алуы (мысалы, мәліметке авторластырған қолданушылармен бөгде есептік жазудан) қолдануыдан көмекпен, рұқсат оларға тыйым салуған	Қолданушылар, техникалық қызметші, уақытша қолданушылар, әріптестер, алып тастаған қолданушылар, әкімдер
1.5	Бөтен беттермен қолданушының атыға ауыстырып жіберуі	Атының (астында рұқсаттың бөтен беттермен алу мәліметке қолданушының) авторластырған	Сыртқы қаскүнемдер, келушілер
1.6	Жүйелік қорлардың дұрыс емес қолдануысы	Жұмыс жасамайтын мақсаттарда ұйымдар аппаратты және программалық қамтамасыз етулері қолдануы, қосатын: - фильм компъютер ойындары, көруі; - функционалдық міндеттерге орындауға жататын емес мақсаттарда Интернетке рұқсаттың қолдануысы; - бөтен ұйымдар үшін жұмыстар рұқсат етілмеген орындау үшін қорлардың қолдануысы және дербес мақсаттарда.	Қолданушылар, техникалық қызметші, бағдарламашылар, әкімшілер, алып тастаған қолданушылар, уақытша қолданушылар
1.7	Операциядағы қате	Бірлескен желіден аппаратты-программалық құралдардан күйге келтірулермен басқарумен сабақтас операцияларда орындауда Қоғамдар қызметкерлермен	Әкімшілер, әріптестер

2.1 кесте жалғасы

		қателердің іске асыруы	
1.8	Аппаратты қамтамасыз етулерге қызмет көрсетуде қате	Аппаратты құралдарға техникалық қызмет көрсетулерге процессте Қоғамдар қызметкерлермен қателердің іске асыруы	Техникалық қызметші
1.9	Қолданушының қатесі	Қосымшалармен жұмыста қолданушылармен қателердің іске асыруы	Қолданушылар, алып тастаған қолданушылар
1.10	Корпаративтік желіге ену	Осы қауіпке жатады: - қолдануымен жүйеге хакердің енуі, мысалы, буферден асыра толтырумен шабуылдар; - торлық қосудан қатысушыдан ауыстырып жіберумен жүйеге ену; - ауыстырып жіберумен жүйеге ену IP-, MAC-Мекен-жайларды; - адасушылыққа белгілі енгізумен шабуылдар жүзеге асыруы	Сыртқы қаскүнемдер
1.11	Мәліметпен манипуляция жасау	Осы қауіпке жатады: - вебсайте серіктестікте мәліметтер ауыстырып жіберуі; - (спам) мәліметтер біле тұра керексіз адресатқа тарату; - жалған қатынастардың енгізуі; - мәліметтер жеткізулері кезектіліктері біле тұра бұзушылығы; - жеткізулер біле тұра тоқтау; - маршрутизациялар біле тұра бас-сирақ; - дұшпандық жұмыс станция арқылы қатынастың жіберудің	Сыртқы қаскүнемдер, әкімшілер, техникалық қызметші, уақытша қолданушылар, әріптестер, қолданушылар, бағдарламашылар, алып тастаған қолданушылар

2.1 кестенің жалғасы

		арқылы шабуылшы тараппен ұстап қалу, өзгеріс және бағыттау қатынастары.	
1.12	Мәліметтерді ұстап қалу	Осы қауіпке жатады: - мәліметтер енжар ұстап қалу; - белсенді ұстап қалу; - трафиктің барлауы рұқсат етілмеген.	Уақытша қолданушылар, техникалық қызметші, қолданушылар, сыртқы қаскүнемдер, бағдарламашылар, әріптестер, алып тастаған қолданушылар, әкімшілер
1.13	Қабылдаудың теріске шығаруы /хабарламаның берілуі	Осы қауіпке жатады: – желінің қолданушылары теріске шығарады, не олар берілулер) (теріске шығаруы қатынас жіберді; – желінің қолданушылары теріске шығарады, не олар қабылдаудың) (теріске шығаруы қатынас қабылдады.	Қолданушылар, алып тастаған қолданушылар, техникалық қызметші, бағдарламашылар, әкімшілер, әріптестер, уақытша қолданушылар.
1.14	Қызметші ұрлықтары	Серіктестіктерге, жинаушыларға қоса ғимаратта болған қызметкерлермен құжаттардың, және физикалық дүниенің ұрлықтардың іске асыруы, көмекші жұмыс және т.б	Қызмет етуші қызметші, қолданушылар, техникалық қызметші, бағдарламашылар, әкімдер
1.15	Бөтен ұрлықтар	Заңсыз ену іске асырған серіктестікке, сол санда адамдармен, болатын емес қызметкерлермен құжаттардың, және физикалық дүниенің ұрлықтардың іске асыруы қызметкерлермен құжаттардың, және физикалық дүниенің	Келушілер, уақытша қолданушылар

2.1 кестенің жалғасы

		ұрлықтардың іске асыруы	
1.16	Қызметкерлермен дүниелер қасақана бұзуы	Акт вандализмдің іске асыруы және серіктестіктерге, жинаушыларға қоса ғимаратта болған қызметкерлермен тіршілік қамтамасыздар мәліметке, жүйелерге техникалық құралдарға, сақтаушыларға физикалық залалдың келтіру, көмекші жұмыс және т.б.	Қызмет етуші қызметші, қолданушылар, техникалық қызыметші, бағдарламашылар, әкімшілер
1.17	Дүниелер қасақана бұзуы бөтен	Акт вандализмдің іске асыруы және заңсыз ену іске асырған серіктестікке, сол санда адамдармен, болатын емес қызметкерлермен тіршілік қамтамасыздар мәліметке, жүйелерге техникалық құралдарға, сақтаушыларға физикалық залалдың келтіру	Келушілер, уақытша қолданушылар
2	Бірлескен желіде әзірлеуде және пайдаланымда қолданхатын техникалық құралдармен сабақтас қауіпті. Ақпараттық қауіпсіздікке қауіптерге осы классқа жүйе, оның жеке компоненттер және қосалқы коммуникациялар техникалық құралдар физикалық бұзылулар, ақаулар және ақаулықтар себепті пайда болатын қауіптер жатады		
2.1	Жабдықтар ақаулар және бас-сирақтар	Әр түрлі факторларға ықпалдарға нәтижеде жұмыста серверлердің ақау	Техникалық құралдар
2.2	Диск сияқты массивтердің ақаулары және бас-сирақтары	Әр түрлі факторларға ықпалдарға нәтижеде жұмыста диск сияқты массивтердің ақау	Техникалық құралдар
2.3	Торлық жабдықтар ақаулар және бас-сирақтар	Әр түрлі факторларға ықпалдарға нәтижеде жұмыста торлық жабдықтар ақау	Техникалық құралдар
2.4	Байланыстар каналдардың жоғалуы	Серіктестікпен бірлескен желімен түйіндермен арасында байланыстар жойылады	Техникалық құралдар
2.5	Лента сияқты кітапханалардың ақаулары және бас-сирақтары	Әр түрлі факторларға ықпалдарға нәтижеде жұмыста лента сияқты кітапханалардың ақау	Техникалық құралдар

2.1 кестенің жалғасы

2.6	Басқарудың және барлаудың станциялардың ақаулар және бас-сирақтары	Әр түрлі факторларға ықпалдарға нәтижеде басқарудың және барлаудың жұмыста станциялардың ақау	Техникалық құралдар
2.7	Жұмыс станциялардың ақаулары және бас-сирақтары	Әр түрлі факторларға ықпалдарға нәтижеде жұмыста жұмыс станциялардың ақау	Техникалық құралдар
2.8	Маршрутизациялар қасақана емес қате	Қате мекен-жай бойынша желі бойынша жіберуде мәліметтер жеткізуі	Техникалық құралдар
3	Бірлескен желіде әзірлеуде және пайдаланымда қолданхатын программалық құралдармен сабақтас қауіпті. Ақпараттық қауіпсіздікке қауіптерге осы классқа жүйелерге компоненттерге жүйелік және функционалдық программалық қамтамасыз етуде қателер пайда болу себепті пайда болатын қауіптер жатады		
3.1	Жүйелік программалық қамтамасыз етулер ақау	Қателер бар болу себепті жүйелік программалық қамтамасыз етулерге ақауға БЖ, осалдықтардың және бас-сирақтардың влекущих пайда болуы БЖ жұмыста	Бағдармалық құралдар
3.2	Қолданбалы программалық қамтамасыз етулер ақау	Қателер бар болу себепті қолданбалы программалық қамтамасыз етулерге ақауға БЖ, осалдықтардың және бас-сирақтардың влекущих пайда болуы БЖ жұмыста	Бағдармалық құралдар
4	Техногенді қауіпті қауіптерге осы классқа жылдамдатқан-мажорлық жағдайлар себепті пайда болатын қауіптер жатады		
4.1	Энергия жабдықтаулар жүйелері ақауы	Ғимаратқа қоректенудің берулері ақауы	Техникалық құралдар
4.2	Ауа тазартулар жүйелері ақауы	Шекті мүмкін шеңберлердің артына жұмыс температуралар шығу себепті жұмысқа тоқтатуға жетектеп жүнетін әуе ауа тазартулар жүйелер ақауы	Техникалық құралдар
4.3	Өрт	Физикалық құралдардың отпен бұзылу, құрайтын жүйеді, құжаттаманы қоса	Форс-мажорлық жағдайлар

2.1. кестенің жалғасы

		және магнитті сақтаушыларды осы	
4.3	Өрт	Физикалық құралдардың отпен бұзылу, құрайтын жүйеді, құжаттаманы қоса және магнитті сақтаушыларды осы	Форс-мажорлық жағдайлар
4.4	Су басу	Физикалық құралдардың сумен бұзылу, құрайтын жүйеді, құжаттаманы қоса және магнитті сақтаушыларды осы	Форс-мажорлық жағдайлар
4.5	Күтпеген апаттар	Жер сілкінулер, селдер, дауылдар, тасқындар және басқа апатты табиғи құбылыстар	Форс-мажорлық жағдайлар

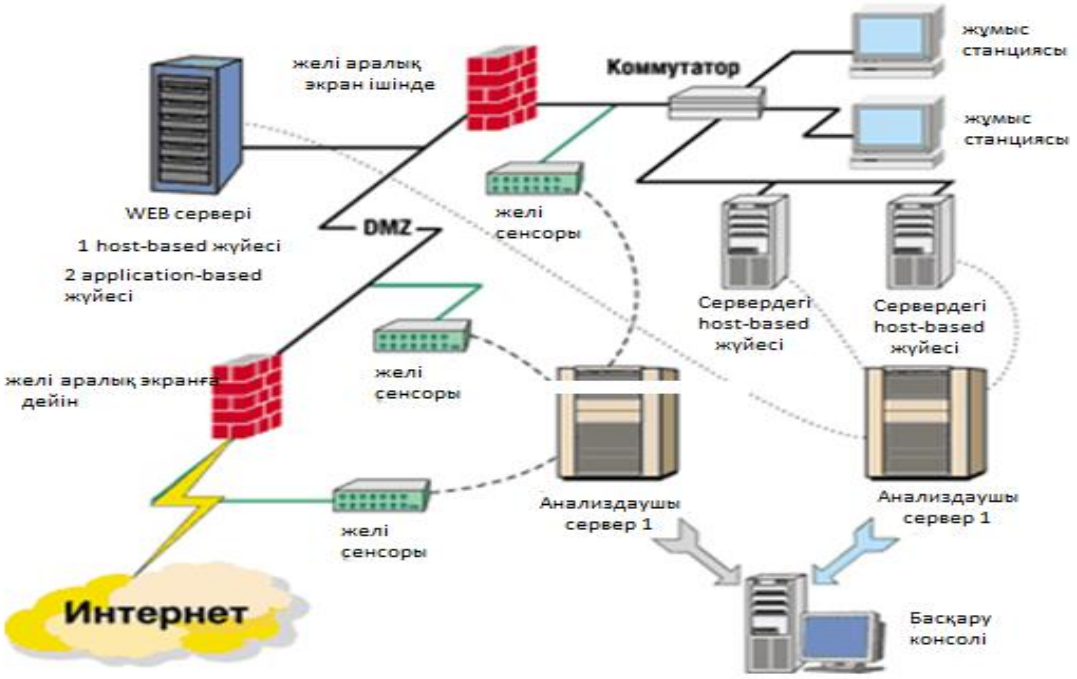
2.4 Басып алушылықтарды бақылау жүйесінің құрылымы

IDS-тың жұмыс істеуінің жалпы сұлбасы 2.2-суретте көрсетілген.

Соңғы кездерде көптеген басылымдарда distributed IDS (dIDS) деп аталатын жүйелер жайлы сөз қозғалуда. dIDS көптеген IDS-дан құралған, олар үлкен тордың түрлі бөліктерінде орналасқан және өз арасында сонымен қатар орталық басқару серверімен байланысқан.

Түрлі IDS-ден түсетін шабуыл жайлы мәліметтердің орталықтануына орай, мұндай жүйе корпоративті торшаның қорғаныстық қабілетін жоғарылатады. dIDS келесідей жүйелерден тұрады:

- орталық анализдеу серверы;
- тор агенттері;
- шабуыл жайлы мәлімет жинау сервері;



2.2 сурет – IDS –тың жұмыс істеу жалпы сұлбасы

Орталық анализдеу сервисы әдетте мәліметтер базасынан және Web-серверден тұрады, ол шабуылдар жайлы мәліметтерді сақтауға және ыңғайлы Web-интерфейстың көмегімен мәліметтерді басқаруға мүмкіндік береді.

Тор агенті- dIDS-тың маңызды бір құрамдас бөлігі болып табылады . Ол шағын бағдарлама, оның мақсаты – орталық анализдеу серверіне шабуылдар жайлы хабарлау.

Шабуыл жайлы мәлімет жинау серверы - dIDS жүйесінің бір бөлігі, логикалық түрде орталық анализдеу серверінде орналасады. Сервер параметрлерді анықтайды, олар арқылы тор агенттерінен алынған мәлімет топшыланады. Топтау келесі параметрлермен орындалуы мүмкін:

- шабуылдаушының IP-адресы;
- қабылдаушы порты;
- агент нөмірі;
- мерзімі мен уақыты;
- протокол;
- шабуыл түрі және т.б.
- пайдаланушылар коммерциялық құралдар ретінде, сонымен қатар еркін таратылатын құралдар ретінде кеңінен пайдаланады.

Жобалаушылар өздерінің өнімдерін шабуылға автоматты түрде әсер ететін жүйелер ретінде жасап шығаруда. Жүйе тек анықтап қана қоймай, сонымен қатар шабуылды тоқтатуға әсерін тигізеді, яғни шабуылдаушыға жауап ретінде шабуылдай алады.

Белсенді түрде әсер етудің ең көп таралған түрлері – сессияны бөлу мен тор аралық экранды қайта орналастыру.

Сессияны бөлу ең көп таралған, себебі ол үшін сыртқы құрылғылардың драйверлері қолданылмайды, тор аралық экран сияқты. Байланыстың екі жағына да, мысалы, жай ғана TCP RESET пакеттері жіберіледі (sequence/acknowledgement)

Алайда мұндай қорғанысты айналып өту әдістері бар және олар жақсы сипатталынған.

Екінші әдіс – тор аралық экранды қайта конфигурациялау, ол шабуылдаушыға жүйеде экранның бар екендігін білуге мүмкіндік береді.

Ping-пакеттердің үлкен ағымын хостқа жіберу арқылы келесіні байқауға болады, біраз уақыттан соң қол жетімділіктің шектелгенін (ping келмейді) шабуылдаушы келесідей нәтиже шығаруы мүмкін, IDS тор аралық экранды ping хостқа. Дегенмен осы қорғанысты айналып өтудің әдістері бар.

Солардың бірі эксплойттарды, тор аралық экранды қайта конфигурациялауға дейін пайдалануға негізделген.

Әлдеқайда жеңіл де жол бар. Шабуылдаушы, торды шабуылдай отырып, жіберуші адресі ретінде басқа танымал фирмалардың (ipspoofing) IP-адрестерін пайдалануы мүмкін.

Тор аралық экранды конфигурациялау механизміне жауап ретінде осы сайттарға (мысалға, ebay.com, cnn.com, cert.gov, aol.com) қол жетімділікті жабады, осыдан соң адамдардан шағымдар түседі, телефонға тыныштық болмайды.

Ұқсас мысал келтірсек, онда ол автомобиль сигнализациясын түнде өшіруге ұқсайды.

2.4.1 Шабуылдарды анықтау технологисы

Шабуылдарды анықтау технологиясын іске асыратын құралдардың басты тапсырмасы болып, қорғаныс жүйесінің басқаруының қиын және қарбалас қызметтерін автоматизациялау және мәліметті қорғау саласында білімі жоқ адамдар үшін ыңғайлы әрі түсінікті болатындай жасау.

Шабуылдарды анықтау технологиясы келесі элементтерге сүйенеді:

– шабуылдар белгілері;
– сигнатуралар;
– шабуылдарды анықтау.

Шабуылдар белгілері. Қорғаныс құралдарын екі шарттың біреуін орындау : немесе бақыланып отырған жүйенің күтілетін іс әрекетін түсіну немесе мүмкін шабуылдардың барлығын және модификацисын білу. Оларды анықтау үшін келесі технологияларды қолданады:

а) ауытқушылық іс-әрекеттерді анықтау технологиясы (anomalydetection);

б) зиян келтіретін іс-әрекеттерді анықтау технологиясы. Әдетте коммерциялық жүйелерде екі әдісті де пайдаланады, ол екі технологияны да максимум пайдалану үшін және кемшіліктерді жою үшін жасалады. (misusedetection).

Ауытқушылық іс-әрекеттерді анықтау.

Берілген технология келесідей нәтижеге негізделген, субъекттің (жүйе, бағдарлама, пайдаланушы) ауытқушылық іс-әрекеттері, яғни әлде бір шабуылдары немесе қарсыластық істері, ол жиі қалыпты жұмыстан ауытқуышылық деп түсіндіріледі. Қысқа уақыт ішінде бірнеше байланыс жасау, орталық процессордың қатты жүктелуі және торлық жүктеме коэффициенті ауытқушылық деп түсіндіріледі. Егер біз субъекттің қалыпты жұмысының мысалын сипаттай алсақ, онда кез келген іс-әрекетін ауытқушылық деп сипаттай алар едік.

Алайда ауытқушылық іс-әрекеттер әркез шабуыл болмайды. Мысалы, торлық басқару жүйесінен станцияның белсенділігі жайындағы запростарға жауаптар санының көптігі саналмайды. Көптеген шабуылдарды анықтау жүйелері берілген жағдайды «қызмет көрсетуден бас тарту» типті шабуыл деп атайды. Осы фактты ескере отырып келесіні байқауға болады, ауытқушылықтарды анықтау жүйесін пайдалану барысында екі шектеулер болуы мүмкін:

- шабуыл болып саналмайтын іс-әрекетті, ауытқушылық іс-әрекетті байқау және оны шабуылдар сыныптамасына (falsepositive);

- ауытқушылық іс-әрекет анықтамаларына сай келмейтін шабуылдарды өткізу(falsenegative). Бұл жағдай ауытқушылық жағдайды шабуылдар сыныптамасына қателесіп жатқызудан да қауіптірек.

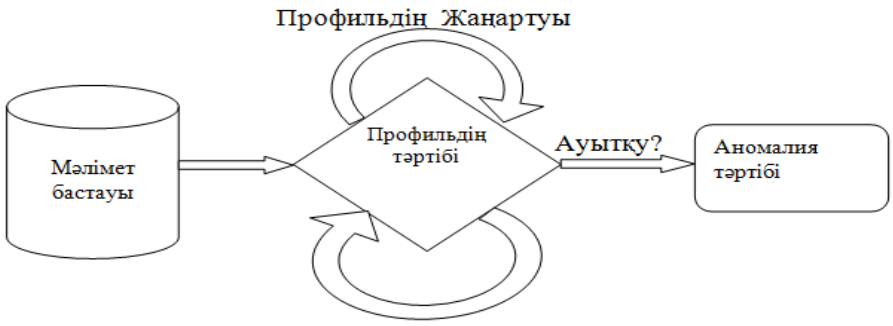
Сондықтан осындай типті жүйені пайдалану мен орнату кезінде , администраторлар екі тапсырмамен соқтығысады:

- субъектті сипаттау – күрделі және уақыт сыйымдылықты тапсырма, ол администратордан үлкен бастапқы дайындықты қажет етеді;

- субъекттің іс-әрекетінің шекті мәндерін анықтау, ол жоғарыда аталған екі шектеулердің бірінің пайда болу ықтималдығын төмендету үшін қажет.

Бұл технология қиын іске асады, себебі осы типті анықтауды жасау үшін, бақыланып отырған субъекттің барлық іс-әрекетін тұрақты түрде тіркеп отыру қажет, ол өз кезегінде қорғалатын хосттың өнімділігін төмендетеді. Осындай жүйелер орталық процессорды қатты жүктейді, жиналатын мәліметтерді сақтауға қажетті дискілік жадының үлкен көлемдерін қажет етеді, жалпы тез жұмыс істеуге критикалық түрде әсер ететін, нақты уақыт режімінде жұмыс істейтін жүйелер үшін пайдаланыла алмайды.

Жаңа профильдің динамикалық генерациясы



2.3 Сурет – Ауытқушылық іс – әрекеттерді анықтау жүйесінің сұлбасы

Жаман ойлы яғни зиян тигізу мақсатын анықтау

Шабуылдарды анықтаудың басқа әдісі зиян іс-әрекеттерді анықтауға сүйенеді, яғни шабуылдарды шаблон (pattern) немесе сигнатура (signature) түрінде сипаттап, осы шаблондарды бақыланып отырған аумақта іздеуге негізделген.

Осы технология вирустардың болуына неэвристикалық сканерлеуге (антивирустық сканерлер шабуылдарды анықтау жүйесінің жарқын мысалы бола алады) ұқсас болып келеді, яғни жүйе барлық белгілі шабуылдарды анықтай алады, бірақ жаңа әлі белгілі емес шабуылдарды анықтауға арналмаған.

Осындай жүйелерде іске асқан әдіс өте қарапайым атап айтсақ, жүйелер нарығындағы ұсынылатын барлығы шабуылдарды анықтау жүйелерінің барлығы дерлік негізделген. Бірақ администраторлар осындай жүйелерді пайдалану кезінде қиын жағдайлармен соқтығысады.

Бірінші мәселе сигнатураларды сипаттау механизмын, демек шабуылды сипаттау тілін жасап шығаруға негізделген. Екінші мәселе – шабуылдың мүмкін барлық модификацияларын біліп алу үшін қалай жазып алуға болады.

2.4.2 Шабуылдарды анықтау әдістері

Екі негізгі әдіс бар, олар:

- статистикалық;
- кәсіби.

Статистикалық анализ

Бұл әдіс ауытқушылық іс-әрекеттерді анықтау кезінде қолданыс табады. Қалыпты іс-әрекетті профильдің орташа мәннен ауытқуы (дисперсия) және администраторға шабуылдың анықталғанын хабарлайды.

Орташа жиіліктер мен шамалар әрбір қалыпты іс-әрекетке (мысалы, жүйеге кіру саны, қол жетімділікті шектеу саны, тәулік уақыты және т.б.) есептелінеді. Мүмкін шабуылдар жайында мәліметтер бақыланып отырған мәндер қалыпты мәннен яғни белгілі біршектен асқан, ауытқыған кезде хабарланады. Мысалы, статистикалық анализ қалыпты емес жағдайды анықтауда қолданылуы мүмкін, мысалы, тіркелген пайдаланушы бұдан бұрын ешқашан торға жұмыс уақытынан тыс кірмеген (алдында 6 сағатқа дейін, ал кеше таңғы 8 дйін), ал аяқ асты жүйеге түнгі 2 кіретін болса.

Жүйе субъектінің іс-әрекетінің шаблонына кіретін параметрлер, келесідей таралған топтарға жатқызылуы мүмкін:

– сандық параметрлер;

– категориялық параметрлер (файл атаулары, пайдаланушы бұйрықтары, ашық порттар және т.б.);

– белсенділік параметрлері.

Шабуылдарды анықтау жүйелері үшін бақыланып отырған параметрлерді дұрыс таңдау өте маңызды. Олардың аз мөлшері немесе дұрыс

емес таңдалған параметрлері, жүйе субъекттерінің іс-әрекетін сипаттайтын модельдің толық болмауын алып келеді, коптеген шабуылдар қаралмай қалады. Басқа жағынан мониторинг параметрлерінің тым көп саны бақыланып отырған түйіннің өнімділігінің төмендеуіне алып келеді, қолданылатын ресурстарға қойылатын талаптар көбейеді.

Дегенмен статистикалық әдістер біршама шабуылдар типтері үшін әлдеқайда тиімді және сенімді, өздерінің кемшіліктері үшін олар кең қолданыс таба алмады.

Негізгі кемшіліктерінің бірі – бастапқы мәнді беру қиындығы. Өте үлкен бастапқы мән беру көптеген шабуылдардың анықталмауына алып келеді,ал тым аз шама – жалған әске асулардың санын көбейтеді. Атап өткен жөн, шабуылдарды анықтаудың кейбір жүйелерінде (мысалы, RealSecureNetworkSensor) кейбір шабуылдар үшін сәйкес бастапқы мәндерін өзгертіп отыруға болады. Басқа кемшіліктері 2.3-кестеде көрсетілген.

2.3-к е с т е – Шабуылдарды анықтаудың статистикалық әдістерінің артықшылықтары мен кемшіліктері

Артықшылықтары	Кемшіліктері
Статистикалық жүйелері	Зиянкелтіруші шабуылды анықтау жүйесін алдай алады, және ол оны қабылдауы мүмкін
белгісіз шабуылдарды анықтай алады	Шабуылға сәйкес қызмет, жүйенің жаңа тәртіпке уақыт өтуімен және «әдеттендіру» әдісімен ақырындап жұмыс тәртібін өзгеріске ұшыратады.
Статистикалық әдістер басқа әдістерге қарағанда аса күрделі шабуылдарды анықтауға мүмкіндік береді	Статистикалық әдістерде шабуыл туралы жалған хабарламалар алу ықтималдылығы өзге әдістерге қарағанда аса жоғары болып келеді
	Әдеттегі тәртіп үлгісін зерттеу мүмкін емес, субъект тарапынан болған шабуылды анықтауға қабілетсіз болып келеді. Статистикалық әдістер субъект тарапынан болатын шабуылды меңгере алмайды, себебі олар о бастан рұқсат етілмеген әдіспен әрекет етеді. Сондықтан да, қарапайым тәртіп үлгісі оларға тек қана шабуылды енгізеді.

2.4.3 Кәсіби жүйелер

Ауытқушылықтарды анықтау кезінде, ереже бойынша, алдын ала орнатылған шаманың жетістігін анықтау үшін бастапқы шаманың мониторнигіне сүйенеді, қастық іс-әрекеттерді анықтау әдістерін ереже бойынша орындайды. Ол қастық іс-әрекеттерді анықтауға қолданылса, ережелер сценарийді сипаттайды. Анықтау механизмы мүмкін шабуылдарды келесі жағдайда идентификациялайды, егер пайдаланушы іс-әрекеті орнатылған ережелерге сай келсе.

Кәсіби жүйе – бар ережелерге сүйене отырып шабуылдарды белгілі бір сыныптамаға жатқызатын жүйе. Бұл ережелер (rules) мамандардың тәжірибесіне негізделген және арнайы сақтау орындарында сақталады. Көп жағдайларда кәсіби жүйенің ережелері бақыланатын аумақта ізделінетін сигнатураларға сүйенеді.

Сигнатуралар анализі жүйе қалыптарын сәйкестігін және пайдаланушы белсенділігін немесе жүйенің басқа субъектін бақылау, сонымен қатар торлық трафиктың белгілі шабуылдар мен осал жерлер базасымен салыстыру болып табылады.

Шабуылдарды анықтаудың коммерциялық өнімдерінің көбісі сатушы жеткізетін белгілі шабуылдар базасымен салыстырмалы түрде сигнатура анализын жүргізеді. Пайдаланушылар орнатқан қосымша сигнатуралар шабуылдарды анықтау жүйесінің конфигурациясының бір бөлігі ретінде қосылуы мүмкін.

Кәсіби жүйелер көп жағдайларда қастық әрекеттерді анықауда қолданылатынына қарамастан, ауытқушылықтарды анықтауда қолданылатын әдістер бар. Мысалы, бағдарланып отырған пайда болатын шаблондардың әдісі (predictivepatterngeneration), алдыдағы жағдай өткенде болған жағдайға қатысты болжанады дейді. Мұндай ереже келесі түрде жазылуы мүмкін: П1 – П2 => (П3 = 75%, П4 = 20%, П5 = 5%)

Бұл ереже келесіні білдіреді, егер П2 жағдайы П1 жағдайынан соң болған болса, онда келесі жағдай П3 болады деген ықтималдылық 75% құрайды, 20% ықтималдықпен П4 және П5 5% ықтималдылықпен. Алайда бұл жүйеге де басқа кәсіби жүйелердің кемшіліктер сай болады. Егер білім базасында шабуылдың әлдебір сценарии жазылмаса ,онда оны анықтау мүмкін емес. Дегенмен бұл кемшілік барлық белгісіз жағдайларды falsepositive) немесе қалыпты жағдайларды (falsenegative), шабуылдар ретінде қабылдау арқылы жойылуы мүмкін, жалпы мәселе шешілмейді.

Шабуылдарды анықтаудың заманауи коммерциялық жүйелері өздерінің жұмысында шамалай айтсақ статикалық және кәсіби әдістердің келесідей қатынасы болады - 30% және 70%. Өкінішке орай, кәсіби жүйелер актуалды болу үшін тұрақты түрде жаңартылып отыруы керек.

Қажет етілетін жаңартылуларды елемейді немесе қолдық түрде пайдаланылады (администратормен). Ең аз дегенде, ол кемшіл мүмкіндіктерге ие кәсіби жүйеге алып келеді. Ең нашары ол алып

жүрулердің болмауы тордың қорғаныстық дәрежесін төмендетеді және пайдаланушыны оның қорғаныстық дәрежесі бойынша шатастырады.

Ережелер негізіндегі жүйелер ұзақ уақыт бойында болатын шабуылдар сценариийін анықтай алмайды. Шабуылдарды уақыт өткен сайын немесе өз арасында, бір бірімен байланыссыз зиянкестер, кез келеген түрде бөлінуі де осы әдістер арқылы анықтауды қиындатады. Кәсіби жүйелердің артықшылықтары мен кемшіліктері 2.4-кестеде көрсетілген.

2.4-к е с т е – Шабуылдарды анықтау кезіндегі кәсіби жүйелердің артықшылықтары мен кемшіліктері

Артықшылықтары	Кемшіліктері
Іске асыру қарапайымдылығы	Белгісіз шабуылдарды анықтау қабілетсіздігі
Жұмыс істеу жылдамдығы	Шабуылдағы аздаған өзгерістер оны анықтау мүмкіндігін төмендетеді
Жалған дабылдың жоқтығы	Жүйе – білім базасын толықтыруда мамандардың жұмысына тәуелді

2.4.4 Шабуылдарды анықтау

Шабуылдарды анықтау модулі кез келген шабуылдарды анықтау жүйесініңең бір маңызды бөлігі болып саналады. Оны іске асыру сапасынан барлық жүйенің тиімділігі анықталады. Бұл модуль өзінің жұмысында шабуылдар белгілеріне сүйенеді (қ. 2.4.1).

Торлық трафик анализі келесідей әдістермен іке асырылуы мүмкін

– жеке торлық пакеттерді реттеуші мәндер көмегімен синтаксикалық талдауы жолымен;

– барлық бір сессияның анализі арқылы.

Бірінші әдісті пайдаланылатын жүйелер, торлық трафиктың өңделмеген пакеттерін басып алу мен оларды синтаксикалық анализатор арқылы өткізу, яғни ол осы пакеттерден шаблон мен сигнатура ұқсастарды іздейді ол осы механизмге негізделген. Осындай шаблонның мысалы ретінде мәтіндік үзінді «/etc/passwd» атауға болады, ол құпия сөз таңдау мен тор бойынша құпия сөз файлын жіберу запросын сипаттайды.

Шабуылдарды анықтаудың келесідей анализдеу әдістері қолданылады:

- pattern matching;
- stateful pattern matching;
- protocol decode-based analysis;
- heuristic-based analysis;
- CRC (тұтастықты бақылау).

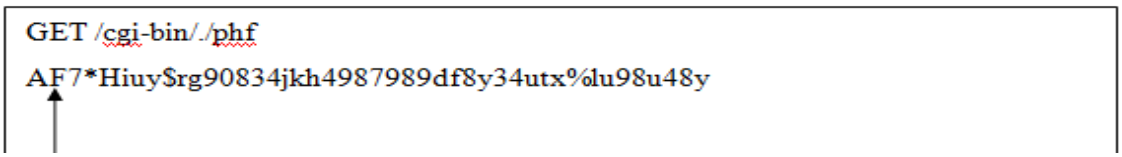
Patternmatching әдісі келесі алгоритм бойынша іске асады:

– басып алынған трафикте бір торлық кадр таңдалады, онда түрлі сигнатуралар ізделеді;

– торлық кадрдың бірінші байтынн бастап, қарастырылатын сигнатурадағыдай дәл сол ұзындықтағы байт тобы бөлінеді. Содан соң екі байттар тобы салыстырылады (сигнатура және пакет үзіндсі);

– егер екі байттар тобы бірдей болып шықса, онда шабуыл анықталды;

– егер топтар бірдей болмаса, онда торлық кадр байтына қатысты бір байтқа жылжу болады, салыстыру процесі соңына дейін жүріп отырады (2.4 - сурет);



2.4-сурет – Салыстыру

Сигнатураларды анализдеудің артықшылықтары келесідей,онда сенсорлар жүйелік мәліметтердің шағын жиынтығын жинай алады, осы арқылы жүйенің жүктелуі төмендейді.

Егер шабуылдар сигнатураларының мәліметтер базасы тым үлкен болмаса, онда сигнатура анализі статистикалық анализге қарағанда өте тиімді болады және онда есептеудің қалқымалы нүктесі болмайды.

statefulpatternmatching технологиясын пайдаланылатын жүйелер, әр пакетті тексеріп қана қоймайды, сонымен қатар олардың қозғалыс ретіне де бақылау орнатады.

Келесі әдіс protocoldecode-basedanalysis деп аталады, ол осы не басқа да протоколдарды сипаттайтын RFC-дан ауытқуларды іздеуге негізделген .

heuristic-basedanalysis әдісі бастапқы мәндердің ауытқуларын анықтауға және торлық ауытқуларды анықтауға бағытталған (статистикалық анализ).

Статистикалық анализ артықшылықтары:

– белгісіз шабуылдарды анықтай алады;

– статистикалық әдістер өте күрделі шабкуылдарды анықтауға мүмкіндік берді;

– статистикалық анализ кемшіліктері (дәл осы уақыттағы);

– қастық жасаушыға салыстырмалы түрде детекторды алдап кетуг оңай және ол бұл шабуылға сай әрекетті қалыпты деп санайды себебі жұмыс режімі уақыт өткен сайын бірінен соң бірі өзгеріп отырады;

– статистикалық детекторларда шабуыл жайлы жалған хабарламалардың келу ықтималдығы сигнатуралық жүйелермен салыстырғанда әлдеқайда жоғары;

– статистикалық детекторлар өзгерістерді онша сапалы өңдемейді. Өзгерістер жиі болып тұратын ұйымдарда бұл кемшілік үлкен қиын мәселе. Нәтижесінде қауіптілік жайлы хабарламалардың жиілігіне және әсер етулерге алып келеді.

Тұтастықты бақылау аспкетте, өзгертілген обьектте ұйымдастырылады. Ол жиі файл атрибуттарын және директориийн, мазмұнын және мәліметтер ағымын алуы мүмкін. Тұтастық анализі message digest (не hash) algorithms деп аталатын мықты криптографикалық механизмдерді жиі пайдаланылады олар тіптен маңызды емес өзгерістерді байқай алады.

Осы әдістің артықшылықтары келесіду, файлдар өзгеріске ұшыраған кез келген сәтті шабуыл, тіптен rootkits немесе торлық пакеттерді тораулдаушылар, анықтау мақсатында сигнатура ма әлде статистикалық анализ пайдаланылса да оған еш қатыссыз анықталады.

Бұл әдістің кемшілігі осы әдістің заманауи іске асуы (batch)—пакет режімінде жұмыс істеуге тырысуда ол нақты емес уақыт масштабында әсер етуіге алып келеді.

3 Басып алуларды бақылау жүйелерін іске асыру

3.1 Техникалық шешімді таңдау

Шабуылдарды анықтау жүйесін бағалау критерилерін қарастырайық және үлкен филиалдары бар корпоративтік тор үшін маңыздыларын анықтайық. Мысалға, мемлекеттік дәрежедегі осы мәліметтік технологиялар мен байланыс саласындағы үлкен компанияның корпоративтік торы болсын. Мұнда және алдыда «Қазақтелеком» АҚ-ның корпоративтік торы базасы негізінде жиналған практикалық материал қолданылады. Берілген компания мәліметтік технологиялар мен байланыс саласында мемлекеттік дәрежедегі үлкен компания болып табылады және үлкен корпоративтік торға ие сондықтан біз осы компанияны таңдадық.

Маңызды ресурстардың қандай категориялары бар және оларды қорғау үшін шабуылдарды анықтаудың қандай технологиялары қолданылатынын анықтайық (3.1-кесте).

3.1 к е с т е – Корпоративтік тордың түрлі типті түйіндері үшін шабуылдарды анықтаудың бірінші сатылы технологиялары

Қорлар	Шабуылды анықтау технологиясы
Файдық серверлер	Тұтастықты анықтау жүйелері ОЖ дәрежесінде шабуылды анықтау жүйелері
Деректер базасы серверлері	ДҚБЖ дәрежесінде шабуылды анықтау жүйелері ОЖ дәрежесінде шабуылды анықтау жүйелері ДҚБЖ дәрежесінде қорғаныс талдауы жүйесі

3.1 кестенің жалғасы

Телекоммуникациондық серверлер	Желі дәрежесінде шабуылды анықтау жүйелері ОЖ дәрежесінде шабуылды анықтау жүйелері Желі дәрежесінде қорғаныс талдауы жүйесі
Қорлар	Шабуылды анықтау технологиясы
Маршрутизаторлар	Желі дәрежесінде шабуылды анықтау жүйелері
Желіаралық бейне беттер және периметрлі өзге де қорғаныс құралдары	ОЖ дәрежесінде шабуылды анықтау жүйелері Желі дәрежесінде шабуылды анықтау жүйелері Желі дәрежесінде қорғаныс талдауы жүйесі
Web-, FTP және пошталық серверлер	Қосымшалар дәрежесінде шабуылды анықтау жүйелері ОЖ дәрежесінде шабуылды анықтау жүйелері Желі дәрежесінде шабуылды анықтау жүйелері Тұтастықты бақылау жүйесі Желі дәрежесінде қорғаныс талдауы жүйесі ОЖ дәрежесінде қорғаныс талдауы жүйесі
Жұмысшы станциялар	ОЖ дәрежесінде шабуылды анықтау жүйелері

3.1-кестеге сәйкес «Қазақтелеком» АҚ-да корпоративтік тордағы шабуылдарды анықтау үшін барлық технологиялар қажет болады.

Корпоративтік торлар келесідей сипаттамаларға ие:

3.2 – к е с т е – «Қазақтелеком» АҚ-ның корпоративтік торының жалпы сипаттамалары

IP-адрестерді қадағалау саны	10,000
Платформалар	Solaris, Windows 2000/XP, Linux
Шабуылға бағытталатын	айына 5-10 (орта есеппен)

3.2 CiscoCatalyst 6500 Series үшін тор аралық экранының сервистік модулін таңдауды негіздеу

Тор аралық экранның (FWSM) Cisco® Catalyst® 6500 Series үшін сервистік модулі тапсырыс берушілерге тор аралық экран құрастыру технологиясы саласындағы соңғы технологиялық жетістіктерді қолдануға мүмкіндік береді.

Ол келесі қызметтік ерекшеліктерге ие:

1. Жоғары масштабталуы мен өнімділігі ;

– 100 000 байланыс/с және 2,8 миллион пакет/с.

2. 2-7 дәрежесіндегі сөзсіз қорғаныс ;

– FWSM және Cisco Catalyst 6500 Series арасындағы қауіпсіздік политикасын жеңіл іске асыру үшін жеке виртуалды локалдық торды қолдау құралдарының интергациясы;

– тор аралық экранның кең функциялары, оның ішінде қолданылатын приложениялар мен протоколдарға сай трафикты тексеру.

3. Торлық құрылғының әрбір порты қауіпсіздік порты болады.

Әрбір FWSM модулі торлық құрылғының барлығын тиімді қорғау үшін басқа модульдермен бірігіп жұмыс істейді.

4. Минималды пайдаланушылық кешігулермен жаңа сервистерді жасап шығару.

Cisco FWSM модулі заманауи әдістерге сай виртуализацияны қолдау құралдарына және жоғары қол жетімділікті қамтамасыз ету құралдарына ие. Шешімдердің функциясын кеңейту қосымша фунуцияларды енгізу арқылы орындалады. Берілген интеграцияланған әдіс ерекшеліктердің арқасында салымдардың сатып алу коэффициентін максималды жоғарылатуға мүмкіндік береді:

– бар торға енгізе алу мүмкіндігі;

– басқару мен қызмет көрсетуді жеңілдетуді;

– пайдаланушылық шығындарды төмендету. Электркуаты мен кабельдерге кететін жалпы шығынды төмендету.

Қандай тапсырмаларды шешу жөн?

Торды өрістетудің толық циклына анализы кезінде,жабдықты сатып алуға кететін бастапқы шығындар, ағымдағы пайдаланушылық шығындармен (80%) салыстырмалы түрде көп емес үлесті (20%) құрайды.

Осы шығындардан басқа қосымша шығындар да бар. Олар қолданылмаған мүмкідіктер, осы не басқа да себептермен сервистың болмауынан, ұйымның қажет технологиялардың дамуына қаржылай көмек көрсетпегенінен туындаған. Пайдалану шығындары мен пайдаланбағандықтан туындайтын шығындар, арзан әрі функциялары мен сервистері жиынтығы аз коммутаторды сатып алу кезіндегі үнемделген сомадан әлдеқайда асып түседі.

Cisco Catalyst 6500Series коммутатор үшін модульдерді жасап шығарудың интеграцияланған әдісі платформаға салынған капиталды

қорғайды және пайдаланушылық шығындарды төмендетеді, сонымен қатар мүмкіндіктерін пайдаланбаудан байланысты шығындардың алдын алады.

Cisco Catalyst 6500 Series үшін FWSM модулі келесідей ерекшеліктердің арқасында торға иелік етудің құнын төмендетуге мүмкіндік береді.

– Инфраструктураны жеңілдету;
– салымдардың өтімділік коэффициентін максималды көтеру;
– барлық дәрежеде қауіпсіздікті қамтамасыз ету құралдарын қолдау;
– жаңа сервистерді енгізу.
– Cisco Catalyst 6500 Series үшін FWSM модулі
– интеграцияланған сервистік модульдің архитектурасы;
– жоғары өнімділік және масштабталуы, шығындарды азайты;
– тор аралық экранның сервистерін виртуалдау;
– мөлдір тор аралық экрандар (дәреже 2)
– жоғары қол жетімділік;
– протокол жағдайын ескеретін трафикты тексерудің икемді құралдары;

3.2.1 Cisco Catalyst 6500 Series үшін FWSM модулінің артықшылықтары

3.2.1.1 Интеграцияланған сервистері

Қорғаныстыжақсарту мен иелік етудің құнын төмендету. FWSM модулі Cisco Catalyst 6500 Series белгілі коммутаторлармен немесе 7600 Series маршрутизаторларымен пайдаланылады және инфрақұрылымды жеңілдетуді, салымдардың өтімділік коэффициентін максималды жоғарылатуды, жаңа сервистерді енгізуді қамтамасыз етеді және барлық дәрежеде қорғаныстықамтамасыз етеді. Коммутатордың кез келген физикалық порты тор аралық экранды қорғау мен пайдалану политикасы құралдары үшін қолайлы жасалуы керек, ол өз кезегінде өрістетуді жеңілдетеді және қосымша жабдықты, қосымша энергия кһздерін және кабельдерін орнатуды қажет етпейді.

3.2.1.2 Жоғары өнімділік және масштабталу, шығындарды азайту

Торлық трафик көлемін көбейту кезігндегі жұмысқа қабілеттілікті сақтау мен шығындарға сезімтал приложенияларды қорғау. Бір Cisco FWSM модулі секундына 100 000 байланыстың өңделуін өамтамасыз етеді, өтімділік қабілеті 5 Гбит/с ж»не бір уақытта 1 миллион байланысты қолдай алады. Бірнеше FWSM модульдерін бір сыныптамаға статикалық виртуалды локалдық торларды (VLAN) жасап шығару арқылы біріктіруге болады немесе Cisco IOS® бағдарламалық қамтамасыз етумен берілетін ереже негізінде маршруттау функцияларын пайдалану арқылы, осы модульдер арқылы трафикты бағыттау.

Торлық құрылғының бр тұрқысында 4 FWSM модульге дейін орналасқан, олар 20 Гбит/с өтімділік қабілетін қамтмасыз етеді.

Бір FWSM модулі 1000 (контекст үшін 256)дейін, ал бір тұрқы 4000 виртуалды интерфейстерді қолдай алады. Одан басқа, Cisco Catalyst 6500 Series тұрқысында приложенияларды бақылаудың екі модулі пайдаланылуы мүмкін (Appication Control Engine, ACE) Cisco FWSM үш модулі арасындағы жүктемені бөлу, ол 15 Гбит/с өтімділік қабілетін қамтамасыз етеді.

Тор аралық экранның барлық функциялары коммутатордың барлық магистралінде пайдаланылады, ол минималды шығынды қамтамасыз етеді (30 мс кіші кадрлар үшін). Cisco FWSM модулі жоғары жылдамдықтағы торлық процессорлардың базасында жасалған,олар жоғары өнімділікті қамтмасыз етеді, жалпы тағайындалуы бар процессорларға тән сонымен қатар икемділікті қамтамасыз етеді.

3.2.1.4 Тор аралық экранның сервистерін виртуализациялау

Тор кеңейтіліміне байланысты шығындар мен басқару қиындығын азайту. Бір FWSM модулі 3.1 версиялы Cisco FWSM БҚ-дің көмегімен 250 виртуалды тор аралық экрандарға (қорғаныс контексты) бөлуге болады, олар қызметтерді жеткізушілерге және ірі өндірістерге түрлі тапсырыс берушілерге немесе қызмет зоналарға политика орнатуға мүмкіндік береді. Ресурстар диспетчеры ресурстарды пайдалануды әр контекст үшін шектеу есебінен жоғары қол жетімділікті қамтамасыз етеді. Қол жетімділікті рөлдік басқару механизмы бірнеше ИТ-администраторларға қауіпсіздік политикасын басқару мен реттеуді жүргізуге мүмкіндік береді. Интенет торымен шекарада пайдаланылатын виртуалды тор аралық экрандар трафиктің толық бөлінуіне дейін және магистарльды тордың өауіпсіздігін қамтамасыз ету үшін маршруттаудың/ретрансляцияның (VRF) құрылғыларымен бірігуі мүмкін. Сонымен қатар маршрутизациялау протоколдарын RIP, OSPF және iBGP қолдау қамтамасыз етіледі.

3.2.1.5 Мөлдір тор аралық экрандар (дәреже 2)

Үдетуді оңтайландыру. Тор аралық 2 дәрежелі экрандар мәліметтерді өңдеу орталықтарына қауіпсіздік жүйелерін үдетуді әлдеқайда оңтайландыра алады, оны ережелердің жалпы жиынтығын реттеу арқылы ал мөлдір қорғалатын хосттар үшін. Одан басқа тор аралық экрандар еш өзгеріссіз 3 дәрежелі берілген торларға енгізіледі және 3 дәрежелі трафиктың маршрутизаторлардан мөлдір берілісін қамтамасыз етеді, олар HSRP, VRRP, GLBP протоколдарының протоколами сгрупповой адресацией, IPX, MPLS және BPDU топталған адресациялы протоколдармен сәйкестікті қамтамасыз етеді.

3.2.1.6 Жоғары қол жетімділік

Мәліметтерді өңдеудің корпоративті орталықтарының қорғаныстық сенімді функциялары. Cisco FWSM модульдерін жұптарда байланыс

қалыпын сақтау мүмкіндігін иелену арқылы үздіксіз жұмысты қамтамасыз ету, олар маңызды торлық орталардың икемді қорғанысын қамтамасыз етеді.

Құрылғылардың «Белсенді – резервті» және «белсенді – белсенді» (3.1 версиялы БҚ Cisco FWSM) конфигурациясы қолдау тапты.

3.2.1.7 Протокол қалыпын ескеретін трафикты толықтай тексеру

Тор аралық экран функциялары мен протоколдарды қолдауының кең спектрі нарықта ұсынылған ең жақсысы. Cisco FWSM модулі Cisco PIX® тор аралық экрандарының технологиясы негізінде жасалған, ол протокол қалыпын есекре отырып, трафикты тексеру сервисын ұсынады, қауіпсіздікті қамтамасыз етеді, стандарттарға сәйкестікті тексеруге мүмкіндік береді, «қызмет көрсетуден бас тарту» сияқты шабуылдардан қорғау мен приложениеларды интеллектуалды түрде тексеру. Одан басқа

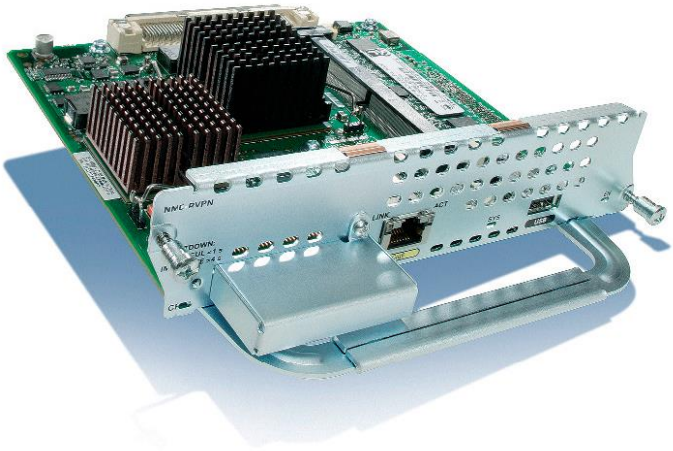
Cisco FWSM модулі мемлекеттік құпиясы жоқ мәліметтерге заңсыз қол сұғуға қарсы құрал болып табылады.

3.3 Cisco 2800 Series және 3800 SeriesIntegratedServicesRouters мршрутизаторлар жанұясы үшін сервистік модуль CiscoNME-RVPN-ны таңдауды негіздеу.

Модуль Cisco маршрутизаторларымен интергацияланған инновациялық шешім болып табылады, ол арнайы Қазақстан нарығын жоғары технологиялы шешіммен VPN-ды құрастырау үшін (виртуалды жеке торлар) қамтамасыз ету үішн жобаланған.

Шешімде ресейлік компаниялардың Cisco-ның алдыңғы қатарлы технологияларымен сертификатталған бағдарламалық қамтамасыз етулер пайдаланылады. Ол торлық әсерлесудің барлық түрлерін тиімді қорғауд заманауи талаптарын қанағаттандырады. Cisco 2800 Series и 3800 SeriesIntegratedServicesRouters мршрутизаторлар жанұясы үшін сервистік модуль CiscoNME-RVPN-ны ерекше құрылғы, ол тиімді маршруизациялау мен жіберілетін мәліметтер, дыбыстық, бейне трафиктерін қорғай алады.

Сонымен қатар құрылғы бір тұтас зат ретінде басқарылады, IOS интерфейсын пайдалану арқылы маршрутизация ережелерін жасау мен торлық әсерлесулерді басқару. Мұндай терең интеграция тор күрделілігін айтарлықтай төмендете алады, персонал квалификациясы үшін қосымша талаптарды ұсынбауға мүмкіндік береді, нәтижесінде үдету мен қолдауға кететін шығынды азайтуға мүмкіндік береді, сонымен қатар жүйешіктің үдеуінің уақытын азайтуға мүмкіндік береді.



3.1-сурет – NME-RVPN модулі

3.3.1 NME-RVPN модуль артықшылықтары

3.3.1.1 Торлық әсерлесулердің қорғаныстық қабілеті

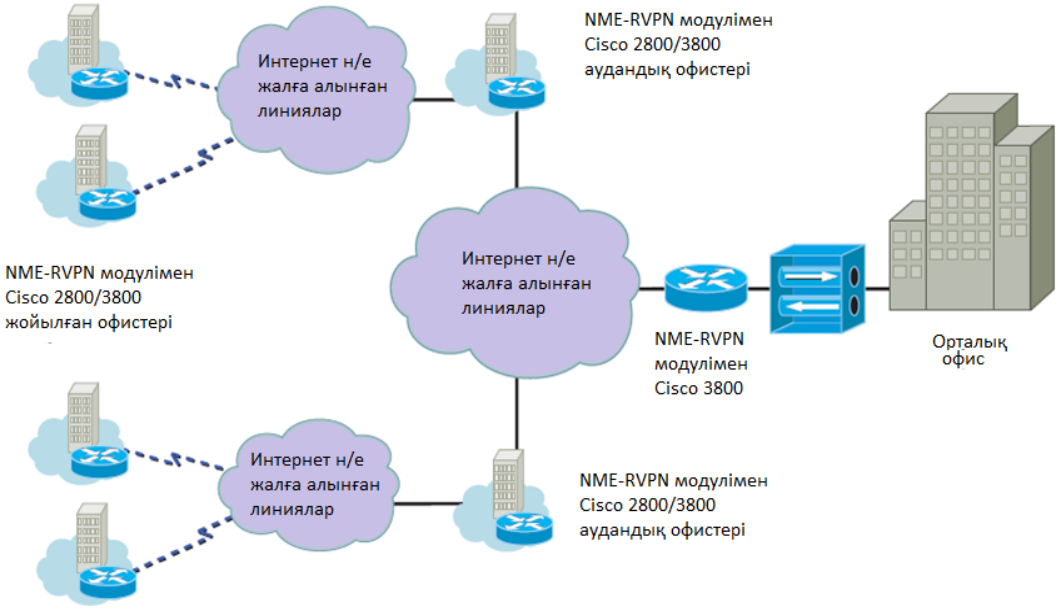
Жалпы торлары бар корпоративтік торлардың терең интеграциямен байланысты өазіргі заманда жіберілетін барлық тор аралық әсерлесудә жоғары дәрежеде яғни жоғары сапалы құралдармен қамтамасыз ету.

Сонымен қатар сыртқы абоненттер арасындағы мәлімет алмасуды мәселесін ғана емес, сонымен қатар қорғалған тоқсыз коммуникациялар бойынша шешімдерді ұсыну керек, олар қызмет көрсету сапасын сақтай отырып дыбыс пен бейнені қорғау, тағы да оператор торларындағы байланыс пен қызметтер провайдерлеріндегі тұтынушылардың максималды тиімді қорғанысын қамту.

3.3.1.2 Тор аралық әсерлесулерді қорғау

Тор аралық әсерлесулерді қорғау сценариі (Site-to-Site VPN) бөлінген корпоративтік торлардың коммуникацияларын ашық канал байланыстар арқылы қорғауға арналған. Негізінде VPN-шешімдерді осы мақсатта қолдану, мәлімет алмау каналдарының сипаттамаларына мысалы, көп протоколдарды қолдау, жоғары сенімділік, жоғары маштабталу сықты талаптардың төмендеуіне алып келмеуі керек.

Керісінше, заманауи VPN-шешімдер, жоғары экономикалық тиімділік пен осындай талаптарды іске асырудың икемділігін қамтамасыз етуі керек. Жоғары экономикалық тиімділікті мысалға мәлімет жіберу үшін жалпы каналдарды пайдалану арқылы алуға болады, ол ертеректе мүмкін емес болған. Осы мақсаттар үшін Cisco ISR маршрутизаторларын пайдалану (3.2-сурет) алдыға қойылған тапсырманы ьолығымен шешуге мүмкіндік береді.



3.2-сурет – Қорғалған корпоративтік торларды құру үшін VPN-туннельдерді пайдалану

Ірі торлық өзара әсерлесетін торлардың сенімділігі мен өнімділігін жоғарылату бойынша талаптарды сақтау, жоғарыда келтірілген мысалға қоса жүктемені резервтеу мен балансировка шешімдері қолданылуы мүмкін.

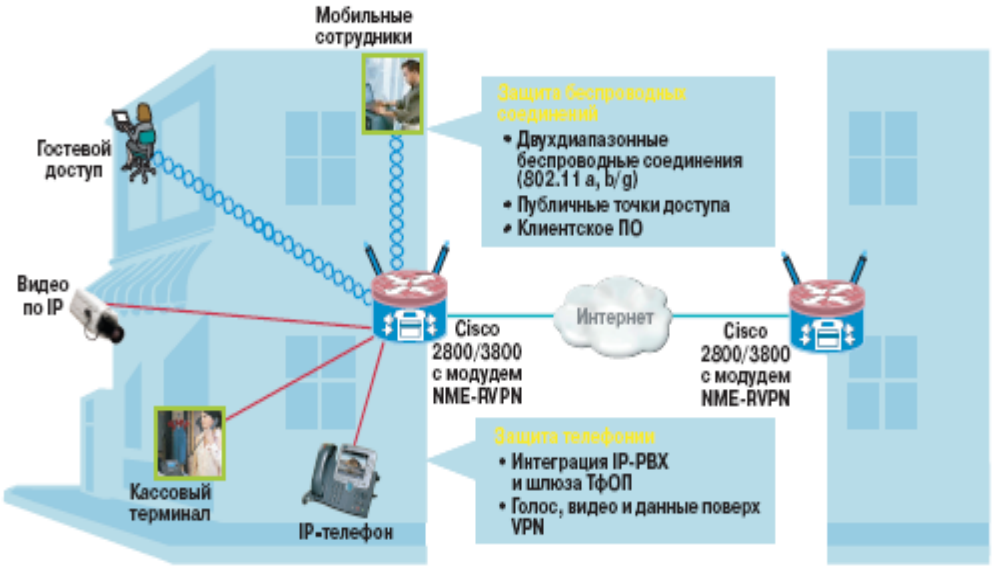
3.3.1.3 Сымсыз және мультисериялы торларды қорғау

Қарастырылып отырған шешімдер бөленген мультимедиялық торлардың және «аралас « торлардың қорғаныс сценариийін қолдай алады, келесіні қамтамасыз етеді:

– қызмет көрсету сапасы механизмын қолдау;

– мәліметтер трафигін қайта жүктеуден соң дыбыстық қорғалған торда қызмет көрсету сапасын қорғау.

NME-RVPN модулі Cisco 2800 немесе Cisco 3800 ISR маршрутизаторлар құрамында қосымша Cisco Unified CallManager Express және сымсыз қол жетімділік нүктесін қамтиды, жойылған офистерге жұмыс істеу мен қорғаныс үшін барлық қажет функциялылықпен өамтамасыз етеді.



3.3-сурет – Сымсыз және мультисервистік торларды қорғау

3.3.1.4 Жойылған және мобильдік пайдаланушыларды қорғау

Пайдаланушылардың жойылған түрде қол жетімділік сценариі (Remote Access VPN) корпоративтік желіге ортақ торлар мен байланыс каналдары арқылы жойылған немесе мобильды пайдаланушылардың қол жетімділігін қорғау үшін қолданылады.

– VPN-клиент пайдаланушылардан енгіщу кілтінен басқа ешқандай техникалық операцияларды қажет талап етпейді;

– (смарт-картаны қосу немесе или құпия сөз) қауіпсіздік администраторы берген ;

– политика безопасности доступа VPN-клиентінің қол жетімділік қауіпсіздігінің политикасы тек жүйелік администраторлармен анықталады, оны пайдаланушы өзгерте алмайды;

– корпоративтік торда пайдаланушының қол жетімділігі құқығы анықталады.

Ұсынылып отырған VPN-клиенттер әлдебір коммуникациялық ресурсы бар кез келген нүктеден сенімді байланысты қамтамасыз етеді.

Пайдаланушының мобильдігін қамтамасыз ету үшін келесідей мехнизмдер пайдаланылады:

– мекен жай аумағына бейімделушілігі;

– мәліметтер алмасудың түрлі орталарын қолдау (GPRS, CDMA, Wi-Fi, WiMAX және т.б.);

– адрестерді трансляциялайтын (NAT) шлюздар арқылы трафиктың мөлдір берілісін қамтамасыз ету.

Басқа интеграцияланбаған торлық құрылғылармен салыстырғанда ұқсас қызметтер атқаратын, NME-RVPN модулі орталық офистың торлвқ инфрақұрылымында қолдануда бірқатар артықшылықтарға ие.

– басқа құрылғылармен ортақ интерфейс. Басқару мен реттеу үшін бұйрық жолының интерфейсін пайдалануға болады. Модуль жұмысымен сонымен қатар графикалық web-интерфейстың көмегімен басқаруға болады.

– Энергияны үнемдеу мен коммутация қарапайымдылығы. Модульды пайдалану кезінде маршрутизатордың қосымша интерфейсын қажет етпейді. Модуль қуатты маршрутизатордан алады, коммутацияны қажет етпейді және торлық жабдық тұрағында орын алмайды.

– Құрылғының мобильдігін және қарапайымдылығын жоғарылату. Орталық офисте алдын ала реттелген модулі бар маршрутизаторды филиалға тұрақта басқа жабдықпен орнату үшін оңай беріп жіберуге болады. Сонымен қатар филиалда квалификацияланған мамандарды қажет етпейді.

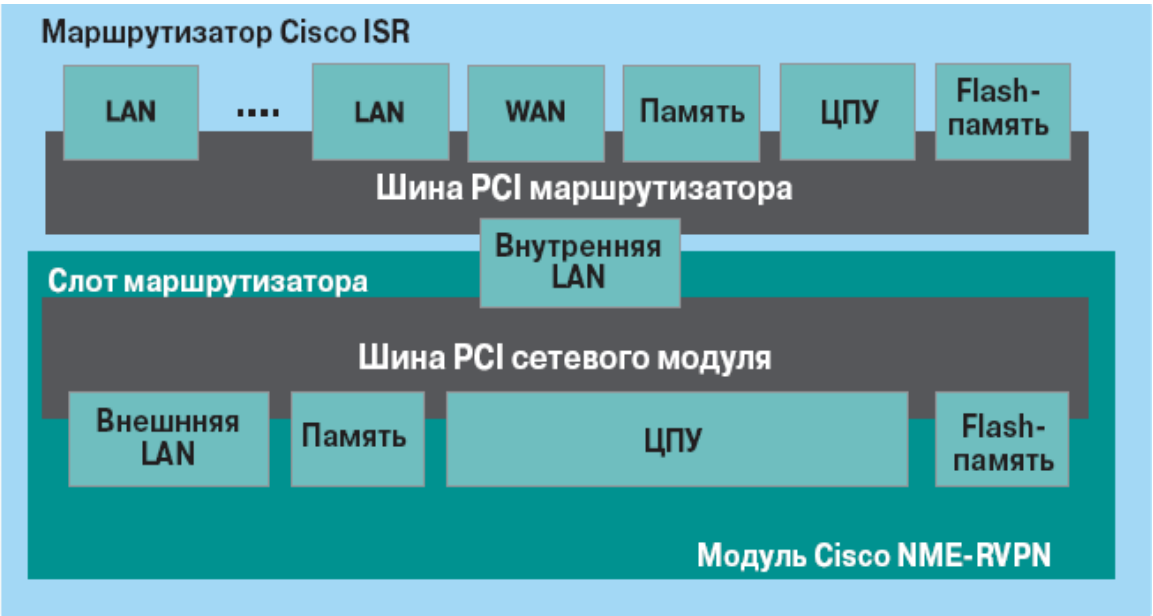
Модульдың қосымша реттемелерін жойылған түрде орындауға болады.

3.4 NME-RVPN модульдың архитектурасы

NME-RVPN модулі Cisco маршрутизаторларын ISR 2811, 2821, 2851, 3825 және 3845 IOS 12.4(11) версиялы T немесе жоғары орналастырылады. Ол кез келген функционалдық жиынтықпен жұмыс істей алады (feature set) IOS «IP base» бастап. Сонымен қатар NME-RVPN модулі маршрутизатор IOS-на қарамастан жұмыс жасайды, модульдың СҒ-картасында орнатылған серіктес компаниялардың БҚ-ін пайдаланады. Модульдың БҚ-і бейімделген ОС Linux-тың басқаруымен функциялайды.

NME-RVPN модуль аппараты процессоры IntelCeleron-M тактік жиілігі 1,0 ГГц, жедел жады 512 МБайт Compact Flash есептегіш платформа (3.4-сурет).

Жергілікті торға қосылу үшін ол сыртқы интерйеспен Gigabit Ethernet жабдықталған. Дәл осындай ішкі интерфейс модуль мен маршрутизатор арасындағы мәлімет алмасуды және әсерлесуді іске асырады.



3.4-сурет – NME-RVPN модулінің архитектурасы және Cisco Integrated Services Router

3.5 Өнімнің техникалық сипаттамасы

NME-RVPN модулінің техникалық сипаттамасы 3.3-кестеде көрсетілген.

3.3 – к е с т е – NME-RVPN модулінің техникалық сипаттамасы

Характеристики	Описание
Аппаратные характеристики модуля	
Процессор	Intel Celeron-M 1 ГГц
Память DRAM	512 МБайт DDR2
Сетевые интерфейсы	• 1 внутренний интерфейс 1000 Мбит/с Ethernet • 1 внешний интерфейс 10/100/1000 Мбит/с Ethernet
Память Flash	512 МБайт Compact Flash
Физические характеристики модуля	
Физические размеры (В x Ш x Д)	3,9 x 18,0 x 18,3 см
Вес	567 г
Относительная влажность при эксплуатации	От 5% до 95%, без конденсации
Температура эксплуатации	От 0 °С до +40 °С
Температура хранения	От -25 °С до +70 °С
Высота над уровнем моря при эксплуатации	3048 м при +25 °С
Потребляемая мощность	21 Вт
Сертификаты по электробезопасности	• Underwriters Laboratory 1950 • CSA-C22.2 No. 950 • EN 60950 • IEC 60950
Сертификаты по электромагнитной совместимости	• 47 CFR Part 15 Class A • CISPR22 Class A • EN300386 Class A • EN55022 Class A • EN61000-3-2 • EN61000-3-3 • VCCI Class I • AS/NZS CISPR 22 Class A
Сертификаты по электромагнитной помехоустойчивости	• CISPR24 • EN300386 • EN50082-1 • EN55024 • EN61000-6-1
Соответствие российским требованиям к электробезопасности	• ГОСТ Р МЭК 60950-2002 (Сертификат № РОСС US.ME61.B03697)
Соответствие российским требованиям к допустимому уровню шума	• ГОСТ 26329-84 (Сертификат № РОСС US.ME61.B03697)
Соответствие российским требованиям к электромагнитной совместимости	• ГОСТ Р 51318.22-99 (Сертификат № РОСС US.ME61.B03697) • ГОСТ Р 51318.24-99 (Сертификат № РОСС US.ME61.B03697) • ГОСТ Р 51317.3.2-99 (Сертификат № РОСС US.ME61.B03697) • ГОСТ Р 51317.3.3-99 (Сертификат № РОСС US.ME61.B03697)

3.6 Функциялық мүмкіндіктері

Функциялық мүмкіндіктер толығымен модульде орнатылған бағдарламалық қамтамасыз етуге байланысты. NME-RVPN модулінің функциялық мүмкіндіктері, CSP бағдарламалық кешенін пайдаланылатын VPN Gate «С-Терра СиЭсПи» компаниясының, бетте сипатталған http://www.s-terra.com/CSP/RU/products/nme_rvpn.htm.Функциональные NME-RVPN ViPNet модулінің функциялық мүмкіндіктері, «Инфотекс» компаниясының ViPNetCoordinator бағдарламалық кешенін пайдаланылатын сипаттамасы бетте http://www.infotecs.ru/Soft/nme-rvpn_vipnet.htm.

NME-RVPN модулінің жалпы функционлдық мүмкіндіктері 4-кестеде көрсетілген.

3.4 к е с т е – NME-RVPN модулінің жалпы функционлдық мүмкіндіктері

Характеристики	Описание
Управление	Интерфейс командной строки Графический web-интерфейс
Настройка и управление	Ведение журнала событий Поддержка сообщений SNMP-trap для удаленного оповещения о событиях

3.7 Сертификаттау мен мемлекеттік реттеу

Модуль NME-RVPN базасында жұмыс жасайтын сертификатталған бағдарламалық қамтамасыз етулер, коммерциялық құрылымдарда, мемелкеттік органдарда да қолданылуы мүмкін.

Соның ішінде құпия мәліметті техникалық қорғау (СТР-К) арнайы талаптар мен ұсыныстарға сай, CSP VPN Gate жабдықталған шлюзбен NME-RVPN модулі құпия мәліметті автоматталған 1Г типту жүйелерде байланыс каналдары бойынша беру кезінде қорғауда қолданылуы мүмкін.

«С-Терра СиЭсПи» компаниясы —Cisco Systems компаниясының технологиялық серіктесі (Cisco Solution TechnologyIntegrator) –«Модуль NME-RVPN» және «МодульNME-RVPN ViPNet» (лицензиялық келісім бойынша БҚ ViPNet Coordinator «Инфотекс» компаниясының)аппараттық-бағдарламалық кешендерді шығарушы , сонымен қатар NME-RVPN модуль үшін CSP VPN Gate БҚ-ді өндіруші .

3.8 Жүйелік талаптар

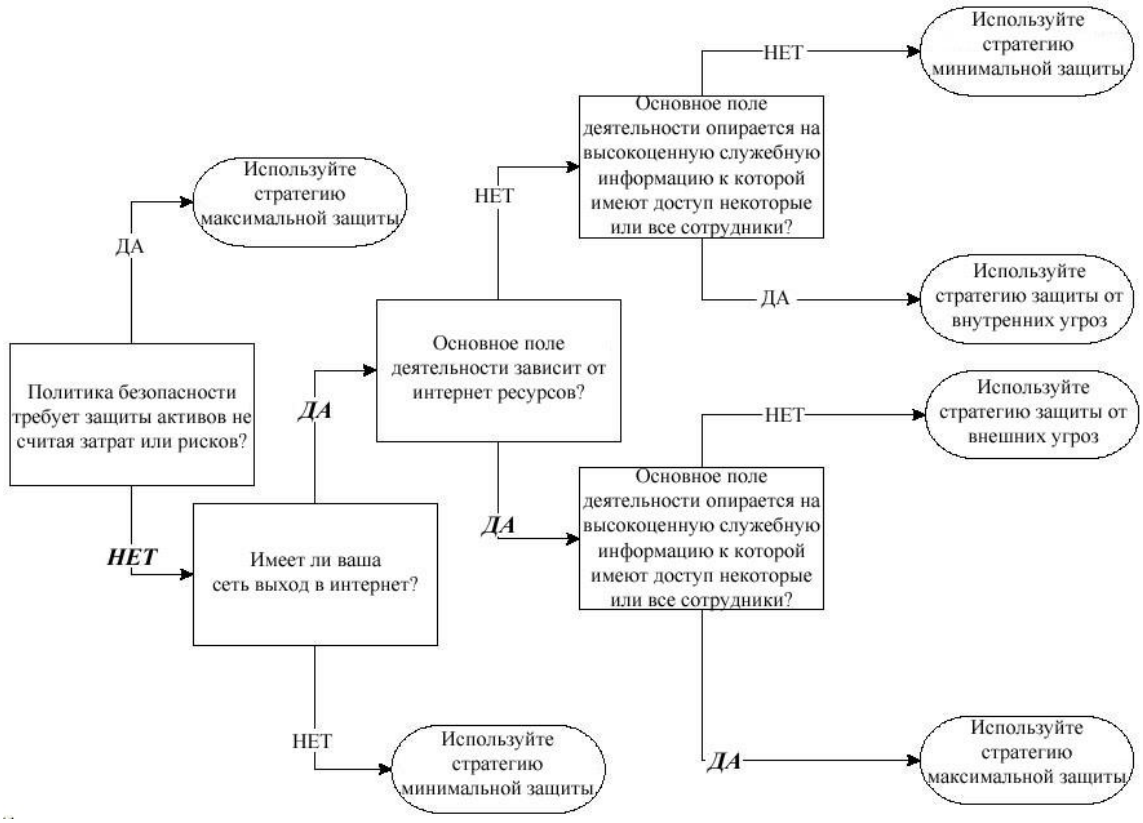
NME-RVPN модуль үшін жүйелік талаптар 3.5-кестеде көрсетілген.

3.5 – к е с т е – NME-RVPN модуль үшін жүйелік талаптар

Требования	Описание
Оборудование	Маршрутизатор Cisco 2811, 2821 или 2851 ISR Маршрутизатор Cisco 3825 или 3845 ISR
Программное обеспечение	Маршрутизатор Cisco IOS® версии 12.4(11)T или более поздней

3.9 Қауіпсіздік политикасым

3.9.1.Қорғаныс стратегиясын таңдау



3.5 сурет – корпоративтік торды қорғау стратегиясын таңдау.

Қажет стратегияны таңдау:

– қорғаныс политикасы активтерді қорғауды қажет етпейді;

– қорпоративтік тор Ғаламторға шығу мүмкіндігіне ие;

– жұмысының бас жолы Ғаламтор ресурстарына байланысты;

– жұмысының бас жолы өызметтік мәліметке сүйенеді, оған кейбір жұмысшылардың қолы жетеді.

Демек, бізге макисмалды қорғау стратегиясы қажет.

Максималды қорғау стратегиясы – бұл стратегияның мақсаты демилитаризацияланған аумақта берік қорғанысты қамтамасыз ету және корпоративтік торда да берік қорғанысты қамтамасыз ету.

3.9.2 Торлық сенсорлардың қауіпсіздік политикасын орнату.

Лабораториялық шарттарда, қорғаныс политикасының қандай түрі қажет екенін анықтау оңай. Алайда тор аралық экран нақты жұмыс істейтін торда пайдаланылса, берліген шартты политикалар мүмкін күрделі өзгерістерді талап етеді.

Жалған әсерлердің көп жағдайы тіркелсе мәліметтер базасы тез толып кетедц, кезектер пайда болады, ол тордың жұмысын баяулатады және тор

аралық бақылау модульдері арасындағы, жүйелік агенттер және консольдер арасындағы трафикты көбейтеді. Мәліметтер жинауды бірқалыпты күйге келтіру керек. Бірақ тым көп сигнатураларды алып тастаса, онда анықталмайтын шабуылға түсіп қалу мүмкін. Түрлі торлық орталар үшін түрлі қауіпсіздік политикалары қолданылатынын ескерген жөн.

Шабуылдарды анықтау жүйелерін бастапқы орнату кезінде, екі тәулік ішінде барлық дерлік жағдайлар мен сигнатуралар қосулы тұрады. Содан соң осы өткен период үшін өткен жағдайларға анализ жасалады. Себебі жағдайлар өте көп, бірақ жеңілдету үішн, сенсорлардың жұмысын оптимизациялау үшін және шабуылға уақытылы әсер ету үшін сигнатуралар санына келесі критерияларға сай азайтқан жөн:

– бақыланатын сегментте бірдей типті жүйенің болуы. Яғни, бізде демилитаризацияланған аумақта Windows ОЖ-сі жоқ. Демек,Windows-қа арналған шабуылдар үшін сигнатурларды өшіріп тастаған жөн;

– бір типті жабдық. Демилитаризацяланған аумақта серверлер ғана бар, принтерлер мен маршрутизаторлар және т.б. жоқ. Осыған сай берілген жабдыққа арналған сигнатураларды қолданбайд;

– қорғаныстағы сегменттегі жұмыс істейтін приложениялар. Мысалға, демилитаризацияланған аумақта Web-, DNS-, пошталық сервер бар. Соған сай, берілген приложениялар үшін шабуылдар сигнатуралары қосулы, олар тағы версия мен жасап шығарушыға байланысты.

3.10 Тордың пайдалы өтімділік қабілетін есептеу

Өтімділіктің пайдалы және толық өтімділігін айыра білген жөн. Пайдалы өтімділік пайдалы мәліметті жіберу жылдамдығы, оның көлемі толық жіберілетін мәліметтің көлменен әрқашан аз , себебі әрбір жіберілетін кадр қызметтік мәліметтен тұрады, ол оның адрсетқа дәл дұрыс жетуін қамтамасыз етеді. Теориялық пайдалы өтімділік қабілетін Fast Ethernet, коллизиялар мен торлық жабдықтағы белгілердің кешігулерін елемей есептейік.

Пайдалы өтімділік қабілетінің толық өтімділік қабілетінен айырмашылығы кадр ұзындығына байланысты болады. Себебі қызметтік мәліметтің үлесі әрқашанда бірдей, кадрдың жалпы өлшемі шағын болған сайын, «накладные шығындар» жоғары болады. Так как доля служебной информации всегда одна и та же, то, чем меньше общий размер кадра, тем выше «накладные расходы». Ethernet кадрларындағы қызметтік мәлімет 18 байтты құрайды (преамбуласыз және стартты байтсыз), ал кадр мәліметтер жолының өлшемі 46-дан 1500-ге дейін өзгеріп отырады. Кадр өлшемі 46+18=64 байттан 1500+18=1518 байт-қа дейін өзгереді. Сондықтан минималды ұзындықты кадр үшін пайдалы мәлімет, жалпы жіберілетін мәліметтің 46/64≈0,72-ні құрайды, ал максималды ұзындықты кадр үшін жалпы мәліметтен 1500/1518≈0,99-ды құрайды.

Тордың максималды және минималды өлшемді кадры үшін пайдалы өтімділік қабілетін есептеу үшін, кадрлардың қозғалысының түрлі жиілігін

ескеру қажет. Әлбетте, кадр өлшемі аз болған сайын уақыт бірлігінде осындай кадрлар тор арқылы көбірек өтеді, өзімен қызметтік мәліметтің көп мөлшерін алып отырады.

Осылай преамбуламен бірге ұзындығы 72 байт немесе 576 бит болатын минималды өлшемді кадрды жіберу үшін уақыт қажет болады, ол 576 bt-ға тең, ал егер кадр аралық интервалды 96 bt екерсек онда келесіні аламыз, кадрлардың қозғалысының периоды 672 bt. 100 Мбит/с жіберу жылдамдығы кезінде ол 6,72 мкс уақытына сай келеді. Онда кадрлардың қозғалыс жиілігі,тормен 1 секундта өтетін кадрлар саны, 1/6,72 мкс≈14881 кадр/с құрайды.

Максималды өлшемді преамбуламен бірге ұзындығы 1526 байт немесе 12208 бит болатын кадрды жіберу кезінде, қозғалыс периоды 12208 bt+96bt=12 304 bt, ал 100 Мбит/с жіберу жылдамдығы кезіндегі кадрлердің жиілігі1/123,04мкс=8127 кадр/с.

Кадрлердің қозғалысының жиілігін f және әрбір кадрмен жіберілетін пайдалы мәліметтің өлшемін $V_п$ (байт) біле отырып,тордың пайдалы өтімділік қабілетін есептеп табу қиын емес: $П_п$ (бит/с)=$V_п$*8*f.

Минималды ұзындықтағы кадр үшін (46 байт) теориялық пайдалы өтімділік қабілеті тең:

Ппт1 = 148 810 кадр/с = 54,76 Мбит/с, тордың максималды өтімділік қабілетінің жалпы мөшерінің тек кішкене жартысын құрайды.

Максималды өлшемді кадр үшін (1500 байт) тордың пайдалы өтімділік қабілеті тең:

Ппт2 = 8127 кадр/с = 97,52 Мбит/с.

Осылайша, Fast Ethernet торында пайдалы өтімділік қабілеті жіберілетін кадр өлшемдеріне байланысты 54,76-дан 97,52 Мбит/с дейін өзгеріп отыра алады.

5 Тіршілік қауіпсіздігі

4.1 Еңбек жағдайын талдау

Бұл дипломдық жұмыста «Қазақтелеком» акционерлік қоғамына басып кірулерді бақылау жүйесі мәселесі шешіледі. Аудан орталығына желі жүргізу барысында Cisco серверлерін қолданамыз.

Серверлер орнатылатын бөлмесі 4.1-суретте көрсетілген.Бөлменің ұзындығы 6м, ені 4м және биіктігі 3м, ұзындығы 2м екі терезе бар. Бөлмеде 5 адам жұмыс істейді, жұмыс графигі - аптасына бес күн, күніне сегіз сағат. Оператордың жұмысы дербес компьютермен және серверлармен байланысты болғандықтан, серверлер орналысқан жердегі жарықтануды, бөлменің температурасын есепке алу қажет. Жарықтану деңгейі психикалық функциялардың күйіне және ағзадағы физиологиялық үрдістерге әсер етеді. Бөлме компьютерлік құрылғылар мен оргтехникамен жабдықталған, сол себептен кафедраның 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. Әкімшілік 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, 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 мынандай түрлері қолданылады:

Дербес компьютерлер саны – 5. Серверлер саны – 2. 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 50дБ-ден кем болмауы керек. Дыбысты қамтамасыз етудің аппараттық бөлмесінің

қабырғалары мен төбесі 500 - 2000Гц жиіліктер диапазонында 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:

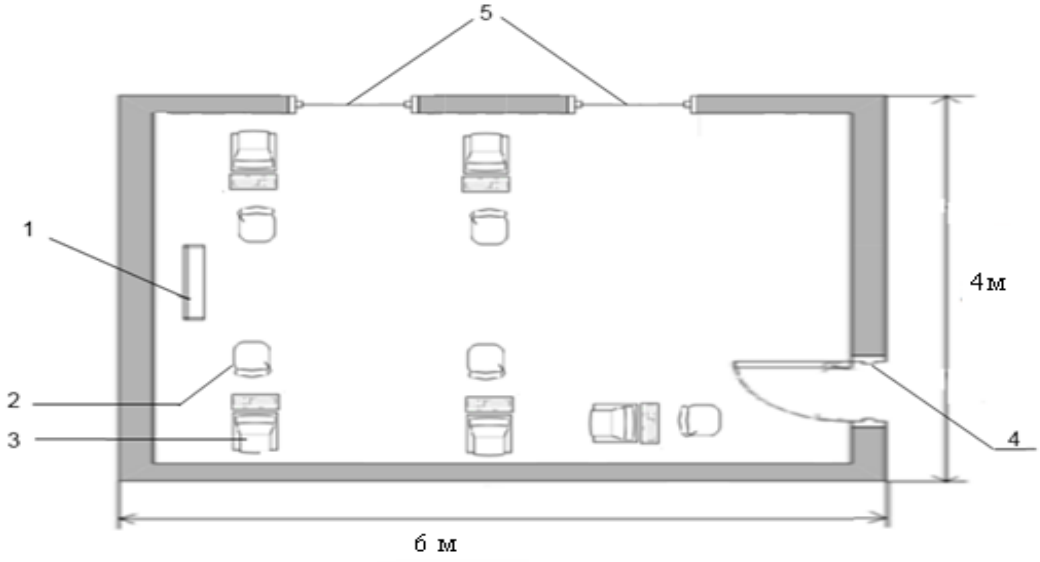
– SAMSUNGdx2300 IntelCore i7 3210/8Gb/500Gb/Combo/DOS дербес компьютері;

– 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 SAMSUNG CS/CU 5800– кондиционер, қуаты 5 кВт.



4.1 сурет – Әкімшілік бөлмесі: 1-кондиционер, 2-орындық, 3-үстел және дербес компьютер, 4-есік, 5-терезе ойықтары

4.1 к е с т е − 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

Желімен жұмыс істегенде компьютер негізгі рөль атқарады. Сондықтан, жұмысшылардың компьютермен жұмыс істеген кездегі еңбектің қауіісіздігімен жұмысқа қабілеттілігін сақтауға арналған сұрақтарды талқылауымыз қажет. Еңбек қорғау саласы бойынша бұл технологияға қатысты ауа алмасудың сипаттамалары мен әдістерін,түрлерін қысқаша сипаттап жазып есеп жүзінде дәлелдеуге тырыстым. Адам ағзасы қоршаған ортамен тұрақты жылу алмасу жағдайында болады. Бұл процесте негізгі рөлді адамның жылу реттеуі негізгі орын алады. Ол қоршаған ортамен жылу алмасуды реттеп отырады және дене температурасын 37^0С жуық сақтап отырады. Адам ағзасының қоршаған ортаға жылу беруі киім, конвекция(таралу), қоргаған беттерге сәулелену, тері бетінен ылғалдың булануы арқылы жүреді. Жылудың бір бөлігі демалатын ауаны жылытуға кетеді. Бөлмелердің микроклиматы әртүрлі ыстықтан қатал суыққа дейінгі маусымдық сыртқы әсерлерге ұшырайды.Сондықтан ғимараттарды жобалауда белгілі бір өңірдің ауа райы жағдайлары ескеріледі. Негізінде бөлме микроклиматы жасанды болып табылады, сондықтан адам оның параметрлеріне белсенді әсер ете алады. Ал ашық алаңдардың климаты табиғи болады және адамның өмірлік процестеріне әсер етуімен анықталады.

Қоршаған ортаның микроклиматының әсерінен адамның жылу сезуі физиологиялық реакциясы болып табылады, ол ағзаны жылу алмасу теңгермешілігінің бұзылуынан қорғайды және оның бұзылған жағдайында қорғаныс шараларын алады.Адамның жылу алмасуы зат алмасу реакциясы нәтижесінде және қоршаған ортадан жылу алуы немесе беруі нәтижесінде өзара қарым-қатынастарымен анықталады.Микроклиматтың әр түрлі жағдайларында адамның жылу алмасуын зерттеу сол микроклиматтың санитарлық нормаларын әзірлеуге, оған адамның бейімделу дәрежесін және жылудың, суықтың, сәуле энергиясының басы артық әсерінен қорғаудың мүмкіндіктерін береді.Микроклиматтың санитарлық нормалары оңтайлы және қолжетімді болып бөлінеді. Оңтайлы жағдайлар қолайлы жылылықты қажет ететін нысандарда:әкімшілік ғимараттарда, ауруханаларда,балалар мекемелерінде, театрларда сақталады. Өнеркәсіптің кейбір салаларында да оңтайлы жағдай талап етіледі (радиотехникада, электрондық техника, дәлдікті құрал-аспап жасау және т.б).

Оңтайлы микрокоимат жағдайлары – жылу реттеу реакциясының күштеуінсіз климат параметрлерінің қосындысында адам ағзасына ұзақ және

жүйелі әсерінде ағзаның қалыпты функционалдық және жылу жағдайын қамтамасыз етеді.Олар жылылық сезімін қамтамасыз етеді және жұмыс қабілетін арттырады.

Қолжетімді микроклимат жағдайлары физиологиялық бейімделу мүмкіндік шектерінен аспайтын, адамға ұзақ және жүйелі әсер ететін микроклимат параметрлерімен сипатталады.Бұл ретте денсаулық жағдайларының зақымдануы немесе бұзылуы болмайды, бірақ қолайсыздау жылулық сезінулер, көңіл күйдің нашарлауы және жұмыс қабілетінің төмендеуі болуы мүмкін.Бұл нормалар әзірге қазіргі техниканың оңтайлы нормаларын қамтамасыз ете алмау себептерінен болады. Әр түрлі тағайынды нысандар үшін микроклиматтың санитарлық нормаларын әдетте жылдың суық және жылы кезеңдері үшін әзірлейді, ал кей жағдайларда климаттық зоналар бойынша жасайды.

Жылдың жылы кезеңі сыртқы ауаның орта тәуліктік температурасымен сипатталады, ол 10^0С және одан жоғары болуы қажет. Жылдың салқын кезеңі орта тәуліктік 10^0С төмен болуымен сипатталады.

Тұрғын үйлердің және қоғамдық бөлмелердің микроклиматы олардың тағайыны және орындалуымен ондағы жылу,желдету, ауа баптаумен анықталады.Тұрғын үй адам баласының жер шарындағы барлық өңірлерінде өмір сүруге мүмкіндік береді. Өңірдің ауа райына және қоршаған ортамен тұрғын жайдың жылу алмасуында тұрғын үйдің төрт типін ажыратады: ашық, жартылай ашық, жабық және оқшауланған. Тұрғын жайлардың микроклиматы жұмыстан кейін физиологиялық ығысуларды қайта қалпына келтіру үшін жағдай жасау қажет, яғни, қолайлы жылу жағдайлары жасалуы тиіс. Бұл айтарлықтай қиындықтар келтіреді, себебі тұрғын жайларда әртүрлі жыныс, жас және түрліше кәсіптердің адамдары тұрады. Ең көп таралған тұрғын үйлерде және қоғамдық ғимараттарда жылу таралу көрсеткіші 21 – 23^0С шегінде, ал ең оңтайлы температура-22^0С. Ауаның 15-20^0 температурасында бөлменің биіктігіне байланысты жылытқыш төбе панельдерінің температурасы 35-45^0 градус, ал қабырғалық панельдерде 30-34^0 градус, ал жылытудың едендік жүйесінде 21-ден 28^0 градусқа дейін ұсынылады. Адамның өндірістік қызметіндегі микроклиматтық жағдайлар жұмыс істеушілердің жұмыс қабілетін және денсаулығын анықтайтын негізгі фактор болып табылады.Мысалы, тоқыма комбинатының тоқымашылары цехтағы 28 - 29^0 температурада жіптің үзілгенін жалғау операциясын 3-5 сек. орындайды, ал ауаның 34^0 градус температурасында 1,1 сек артық жұмсайды, сөйтіп еңбек өнімділігін 20 – 30%-ке төмендетеді. Көмір шахталарында ауа температурасының 25-тен 29^0-ға дейін көтерілуінде, еңбек өнімділігі әр градус есебіне 3-4% төмендейді.Ыстық цехтарда ауаның температурасы 35^0 градустан әрі жоғарыланғанында, еңбек өнімділігі 15% төмендейді. -Негізі бөлмедегі ауаны бөліктеп немесе толық алмастыру ауа алмастыру деп аталады. Егер бір сағат барысыда ауа алмасу бөлме көлемімен өрнектелсе, онда мұндай алмасу дерексіз саны ауа алмасудың еселігі деп аталады. Әкімшілік 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 әкімшілік 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.

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 4.2-кестеде келтірілген.

4.2-к е с т е – Адам ағзасының энергия жұмсау жұмыстарының категориялары

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

4.2Кондиционерлеу және ауаны жаңарту жүйелерін есептеу

Бөлменің ауа баптауы үшін жылу және ылғал теңгермешілігін жасау жылыту-желдету техникасында қабылданған жалпы белгілі әдістермен жүргізіледі. Мұнда бөлменің ауа ортасының өзгеруіне әсер ететін барлық

факторлар есепке алынуы қажет. Түрлі тағайынды бөлмелерде: негізінен бөлме сыртындағы жылу жүктемелері; бөлме ішіндегі жылу жүктемелері әрекет етеді.

Сыртқы жылу жүктемелері келесі құраушылардан тұрады:

– қабырға, еден, терезе, есіктер арқылы ғимарат сыртындағы және ішіндегі жылу айырымы нәтижесінде түсетін жылулар мен жылу шығындары;

– жазда ғимараттың ішкі, сыртқы температура айырымы оң, ал қыста теріс болады, осы себепті бөлме ішіндегі белгіленген режім температурасын ұстау қажет болады;

– күн сәулесінен шыныланған беттер арқылы түсетін жылулар; бұл жүктеме сезілетін жылу ретінде байқалады;

– инфильтрация түсетін жылулар;

Қызмет көрсетілетін бөлмелерге жататын тұрғын және офистік бөлмелердегі жылу негізінен келесі жылудан тұрады:

– адамдар бөлетін жылу;

– электр тұрмыстық құралдар, шамдар, жарық беретін аспаптар бөлетін жылу;

– компьютерлер, баспа құрылғылары, фотокөшірме машиналар және т.б (офистік және басқа бөлмелерде) жылуы.

Түрлі тағайынды өндірістік және технологиялық бөлмелерде жылу көздері келесілер болуы мүмкін: қызған өндірістік жабдық; жанған материалдар, соның ішінде сұйықтар жартылай өнімдер; жану өнімдері және химиялық реакциялар.

Жылдың жазғы мезгілінде қоршалған құралымдар арқылы сырттан келетін жылу есебін шығару тәулік ішінде елеулі өзгерістерге ұшырайтындықтан және күн сәулесі әсерінен сырт қоршаулардың беттері жылу ағынының бұдан да көбірек ауытқуға ұшырауы себепті қиындық келтіреді. Сондай-ақ сырт қоршаулардың көлемділігі оның беттеріне түсетін сәуле жылуын азайтуы себепті жылу алмасуға елеулі әсер етеді.

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:

$$Q_{жылу.б} = Q_{айыр} + Q_{сәу} + Q_{адам} + Q_{жар\text{-}у} + Q_{құр\text{-}ғы}, \text{ Вт} \qquad (4.10)$$

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

$Q_{сәу}$ – шынылау арқылы күннің сәулеленуінен келетін жылу;

$Q_{адам}$ – адамдардан келетін жылу түсу;
$Q_{жар\text{-}у}$ – жарықтандыру аспаптарынан келетін жылу;
$Q_{құр\text{-}ғы}$ – оргтехника және құрылғылардан келетін жылу.

4.2.1 Температура айырымы нәтижесінде алынатын жылу және жылу жоғалту

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 ($t_{Сесеп}$) ең салқын айдың 13 сағатындағы орташа температурасына, жылы период үшін – ең ыстық айдың 13 сағатындағы орташа температурасына сәйкес келеді. Ал ішкі ($t_{Иесеп}$) жайлылық шартын және өндірістік процесстерде көрсетілетін технологиялық талаптарын ескере отырып таңдалады:

$$Q_{қоршау} = V_{бөлме} X_0 (t_{шыққан} - t_{келген}),\ Вт \qquad (4.11)$$

мұнда $V_{бөлме}$ – бөлменің көлемі, $м^3$. $V_{бөлме}$=6х 4 х 3 = 72 $м^3$;

X_o – сыбағалы жылулық сипаттама, $Вт/м^3\ ^oC$.

X_o = 0,42 $Вт/м^3\ ^oC$.

Жылы мезгіл үшін: $t_{Сесеп}$ = 27,6 ^oC [12, кесте 3], $t_{Иесеп}$ = 24 ^oC

$Q_{айыр}$ = 72 х (27,6 - 24) х 0,42 = 108,86 Вт.

Салқын мезгіл үшін: $t_{Сесеп}$= -25 ^oC [12, кесте 3], $t_{Иесеп}$ = 20 ^oC

$Q_{айыр}$ = 72 х 0,42 х (- 25 - 20)= -1360,8 Вт.

4.2.2Шынылау арқылы күннің сәулеленуінен келетін жылу

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

$$Q_р = (q_{вп} + q_{вр})\ К_1^{с}\ К_2\ ß_{с.з.}\ n\ H_0\ B_0,\ Вт \qquad (4.12)$$

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

$$Q_{р\ .} = q_{вр}\ К_1^{Т}\ К_2\ ß_{с.з.}\ n\ H_0\ B_0,\ Вт \qquad (4.13)$$

мұнда $q_{вп}$; $q_{вр}$ – тура және шашыраңқы радиациядан келетін жылулық ағындар, $Вт/м^2$;

$F_o = n\ H_0\ B_0$ – 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;

$ß_{с.з.}$ – жылу өткізу коэффициенті.

1) аудан орталығы бөлмесіндегі шынылаудың ауданы, 44^0 СШ [12, кесте 3] $F_0 = 2 \times 2 \times 2 = 8$ м^2;

2) шынылаудың бағыты: оңтүстік-шығыс (ОШ);

3) ішінде жарық перделері бар. $ß_{с.з.}$ = 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) $q_{вп}$ = 387 Вт/м^2 және шашыраңқы радиацияның мәні (Р) $q_{вр}$ = 101 Вт/м^2 тең 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 аралығындағы период үшін . Әйнектің бірқалыпты ластануы коэффициенті $К_2 = 0,9$ қабылданады.

Тура сәулелену периодында 9 бен 14 сағат аралығында есептелу мына формула арқылы жүреді (4.12):

$Q_р = (387 + 101) \times 0,72 \times 0,9 \times 0,4 \times 8 = 1012$Вт,

ал көлеңкелену периодында 14 пен 20 сағат аралығында мына формуламен есептелінеді (4.13):

$Q_р = 22 \times 1,15 \times 0,9 \times 8 \times 0,4 = 73$ Вт.

Максималды есептелу уақыты: 9-10 сағат, жылу түсу 1012 Вт.

5.2.3 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:

4.3 к е с т е – Адамның сыртқы ортаға жылу таратуы, Вт

Сыртқы орта темпера-турасы ^{o}С	Отырғандағы жағдай			Тұрғанда немесе жеңіл қозғалыс			Ауыр жұмыс		
	Анық	Жасы рын	Жал-пы	Анық	Жасы рын	Жал-пы	Анық	Жасы рын	Жал -пы

4.2 кестенің жалғасы

24	67	35	102	72	60	132	95	154	249
20	82	21	103	92	42	133	140	110	250

4.4 – к е с т е – Адам бөлетін ылғал және көміртегі саны

Параметрлер	Бөлме ауасының температурасындағы мәндер ^{0}C				
	15	20	25	30	35
Ылғал г/сағ	40	40	50	75	115
Көміртегі қостотығы г/сағ	45	45	45	45	45

Бөлмеде 5 ер адам серверларды бақылап отырады. t = 24 ^{0}C температурада отырған күйде бір ер адам 67 Вт анық жылу, ал жалпы – 102 Вт жылу бөледі 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 = 335 Вт. Ал жалпы жылу: $Q_a^ж$ = 102 х 5 =510Вт.

t = 20 ^{0}C температурада бір ер кісі 82 Вт анық жылу және 103 Вт жалпы жылу бөледі . Бөлмедегі адамдардың бөлетін анық жылуы: $Q_a^а$ = 82 х 5 = 410 Вт. Ал жалпы жылуы: $Q_a^ж$ = 103 х 5 х = 515 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.

4.6 к е с т е – 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	335	510	250	225

Салқын	20	410	515	200	225

4.2.4 Жарықтану аспаптарынан, оргтехникадан және құрылғылардан келетін жылу

Шамдардан келетін жылу мына формуламен есептеледі:

$$Q_{жар\text{-}у} = \eta N_{жар\text{-}у}, \text{ Вт} \qquad (4.14)$$

мұнда η - электр энергиясының жылулыққа ауысу коэффициенті. Люминесцентті шамдарды қолдану кезінде η = 0,5-0,6;

$N_{жар\text{-}у}$ – шамдардың орнатылған қуаты 65 Вт/м^2.

Әкімшілік бөлменің ауданы $F_{еден}$ = 6х 4 = 24 м^2.

$Q_{жар\text{-}у}$ = 0,6 х 65 х 24 = 936 Вт.

Оргтехниканың әсерінен пайда болатын жылу ағыны бір компьютерге орташа есеппен 300 Вт алады. Әкімшілік бөлмеде 5 Дербес компьютер болғандықтан:

$Q_{құр\text{-}ғы}$ = 5 х 300 = 1500 Вт.

Орындалған есептеулерден (4.10) формуласы бойынша әкімшілік бөлмесіне келетін жылу балансын құрамыз. Жылдың жылы мезгілінде: температура айырымы нәтижесінде келетін жылу $Q_{айыр}$ = 109 Вт; күн радиациясынан $Q_р$ = 1012Вт, Вт; адамдардан Q_a^a = 335 Вт; жарықтану аспаптарынан $Q_{жар\text{-}у}$ = 936 Вт; оргтехника мен құрылғылардан $Q_{құр\text{-}ғы}$ = 1500 Вт. Әкімшілік бөлменің жылулық балансы жазда:

$$Q_{жылу.б} = Q_{айыр} + Q_{сәу} + Q_{адам} + Q_{жар\text{-}у} + Q_{құр\text{-}ғы}, \text{ Вт} \qquad (10)$$

$Q_{жылу.б}$ = 109+1012+335+936+1500= 3892 Вт= 3,892кВт,

$Q_{жылу.б}$ = 5,143 х 3600 = 14011 кДж/сағ құрайды.

Жылдың салқын мезгілінде: температура айырымы нәтижесінде жоғалатын жылу $Q_{айыр}$ = -1360,8 Вт; күн радиациясынан келетін жылу $Q_р$ = 1012 Вт. Вт; адамдардан Q_a^a = 410 Вт; жарықтану аспаптарынан $Q_{жар\text{-}у}$ = 936 Вт; оргтехника және құрылғылардан $Q_{құр\text{-}ғы}$ = 1500 Вт. Әкімшілік бөлменің жылулық балансы қыста:

$Q_{жылу.б}$ = -1360,8 + 1012 + 410 + 936 +1500 = 2497Вт=2,497кВт

$Q_{жылу.б}$ = 2,497 х 3600 = 8989 кДж/сағ құрайды.

4.2.5Ауа алмасуды есептеу

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

$$Q_н = \frac{Qжылу.б \cdot 860}{V_{помещ}} = \frac{3,892 \cdot 860}{6 \cdot 4 \cdot 3} = 46,5ккал/м^3 \quad (4.15)$$

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

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

$$L = \frac{Qжылу.б \cdot 860}{c \cdot \Delta t \cdot \gamma} = \frac{3,892 \cdot 860}{0,24 \cdot 8 \cdot 1,206} = 1445\ м^3/сағ \quad (4.16)$$

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

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

Барлық артық жылулар 14011 кДж/сағ немесе 14011: 3600 = 3,9 кВт құрайды. Бөлмеге қажетті ауа мөлшері L = 1445 м^3/ч = 31,8 м^3/мин. Өз таңдауымызды SAMSUNG CS/CU 5800 сплит-жүйесі кондиционеріне тоқтатамыз.

Кондиционердің техникалық сипаттамалары:

- салқын 5,20 кВт; жылу 5,80 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;
- EER, А 4,36;
- COP, А 4,41;
- жылдық ток пайдалануы 940 кВт*сағ
- шудың деңгейі, ішкі (жоғ/орт/төм), дБ(А) 44/37/34;
- шудың деңгейі, сыртқы, дБ(А) 47;
- габаритті өлшемдері, Ш/В/Г, Ішкі, мм 280*1050*240;
- габаритті өлшемдері, Ш/В/Г, сыртқы, мм 695*875*320;
- салмағы, кг 14.

5 Жобаның техника-экономикалық негізделуі

5.1 Жоба мақсаты

Берілген жобаның басты мақсаты корпоративті желіде жүретін ақпарат алмасуға сырттан рұқсатсыз қолжеткізуді, нақтырақ айтсақ желіге жасалатын шабуылдардың алдын алу, қауіптілікті анықтайтын механизмдерін жасап шығару және қауіптілікке әсер етуді анықтау, себептер мен шарттарын анықтау. Байланыс қосымшаларды тиімді орындауға жеткілікті дәрежеде жоғары жылдамдыққа ие болуы тиіс. Қосымшалар құрамында жаңа инновациондық қызметтер мен бизнесті жүргізудің жаңа тәсілдерін ұсынатын бағдарламалар да болуы тиіс.

Алыстатылған жұмыскерлер желі арқылы басқа қалада жүріп ақ жұмысын жалғастырып, істелген жұмыстары бойынша есеп бере алады.

5.2 Жоба туралы жалпы ақпарат

Қазіргі таңда мемлекеттік басқару саласы жоғары қарқынмен дамуда. Сол себепті жылдан жылға мемлекеттік қызметкерлер саласындағы IT саласының рөлі артуда. Мемлекеттік қызметкерлердің мамандарының жаңа технологияларды игеруі және қолдануы қоғамға үлкен әсер тигізеді. Осы дипломдық жобада корпоративтік желіге басып кірудің бақылау жүйесін үйлестіру сұрақтарын қарастыру қажет.

Көбінесе, келесідей жұмыстарды жүргізу керек:

– корпоративтік желілердің қауіпсіздік қаупін анықтау жұмыстарын жүргізу;

– корпоративтік желілердің қауіпсіздік жүйесін талдау;

– желіаралық бейне беттің модулы Cisco Catalyst 6500 Series шабуылды анықтау жүйесін таңдауын түсіндіру;

– әсерлі бағыттаушымен қамтамасыз етудің, мәліметтер трафигінің қорғанысын, дауыстың, бейнебаян – модуль Cisco NME-RVPN, бағыттаушылар Cisco 2800 Series және 3800 Series Integrated Services Routers жүйесін таңдауын түсіндіру;

– қажетті құралдарды орналастыруды жоспарлау.

5.3 Құрылғылар мен программалық қаматама таңдаудың негізі

«Қазақтелеком» акционерлік қоғамы үшін сәйкестендірілген құрылғы тасмалдайтын дара мекеме. Ол бақылау рұқсатын, Mobile Device Management құрылғыларының желіге қосылуына мүмкіндік береді(MDM). Инновациалы тақташалар қатарына Cisco Identity Services Engine (ISE) құрылғысы да жатады.Ғаламтор желісі телефон желісі мен байланыс туралы ойымызды түбегейлі өзгертті. Телефон желілері мен мәліметтер жіберу желісінің пайда болғанына он жыл болғанына қарамастан, бір-біріне тәуелсіз ретте дамыған.

5.4 Қаржылық жоспар

5.4.1 Капиталдық салымдарды есептеу

Желі құру үшін жұмсалатын шығын негізгі жабдықты сатып алу мен (көлік шығыны негізгі жабдық құрамына кіреді) жобалау шығындарынан тұрады және келесі өрнекпен есептеледі:

$$К_{\sum} = К_{ж} + К_{жш} \quad + К_{кш} \qquad (5.1)$$

мұндағы $К_{ж}$ – негізгі жабдықтарды сатып алу шығыны;

$К_{жш}$ – жобалау шығыны;

$К_{кш}$ – көлік шығыны.

Негізгі қажетті жабдықтар тізімі мен олардың құны 5.1-кестеде келтірілген. [16].

5.1-кесте – Жобаны жүзеге асыру үшін алынатын негізгі жабдыққа жұмсалатын шығын

№	Жабдықтардың аталуы	Саны	Құны (ҚҚС-мен), тг	Құны (ҚҚС-сыз), тг	Қосынды, (ҚҚС-сыз), тг
1	Контроллер Cisco 4402	3	350000	308000	924000
2	Платформа Cisco ISE	3	261750	230340	691020
3	Коммутатор Cisco Catalyst 6500 Series	3	156940	140125	420375
4	Маршрутизатор Cisco 2800 және Series 3800	3	399616	356800	1070400

5	Желілік экран Cisco ASA5505-50-BUN-K8	3	77550	68245	204735

5.1 кестенің жалғасы

6	IP ТЕЛЕФОН GXV3175.	3	105280	94000	282000
7	Intel Core i7-3770K	3	125440	112000	336000
Қорытынды					3928530

5.4.2 Желіні жобалауға жұмсалатын шығындарды есептеу

Желіні жобалау шығындары келесі құрамалардан тұрады:

– қызметкерлердің еңбекақысы;
– әлеуметтік салық;
– өндірістік қажеттіліктер үшін жұмсалатын электр энергиясы;
– амортизациялық аударылымдар;
– жылдық шығын сомасы өндірістің өзіндік құнын құрайды немесе жылдық пайдалану шығынының мөлшерін анықтайды.

Желіні жобалау шығындары келесі өрнекпен есептеледі:

$$К_{жш} = ЖТФ + С_С + А_О + Э + Н \quad (5.2)$$

мұндағы *ЖТФ* – жалақы төлеу фонды;

$О_с$ - әлеуметтік салық;

А - амортизациялық аударма;

Э - электр энергиясына кететін шығын;

Н - үстеме шығыны.

Еңбекақы қоры негізгі және қосымша еңбақыдан құралады және келесі өрнекпен есептеледі:

$$ЖТФ = Ж_{нег} + Ж_{кос} \quad (5.3)$$

мұндағы $Ж_{нег}$– негізгі еңбекақы,

$Ж_{кос}$– қосымша еңбекақы.

Негізгі еңбекақы барлық қызметкерлердің еңбекақысының қосындысы ретінде есептеледі:

$$Ж_{негг} = \sum_{i=1}^{n} Ж_i \cdot T_i \quad (5.4)$$

мұндағы $Ж_i$ – і-ші қызметкердің бір күндік еңбекақысы, теңге;

T_i - і-ші қызметкердің уақыт шығыны, күн.

Қосымша еңбекақы негізгі еңбекақының 10% -ын құрайды:

$$Ж_{кос} = 0.1 * Ж_{нег} \quad (5.5)$$

Берілген жобаның штатында 4 қызметкер бар. Қызметкерлердің еңбекақысы 5.2-кестеде келтірілген.

5.2 – к е с т е – Жобаға қатысушы қызметкерлердің еңбекақысы туралы мәліметтер

Орындаушы	Айлық еңбекақы, теңге
Жоба жетекшісі	150 000
Құрушы инженер	130 000
«Экономика» бөлімі бойынша кеңес беруші	130 000
«ТҚ» бөлімі бойынша кеңес беруші	100 000
Қорытынды	**510 000**

Бір адамның бір күндік еңбекақысын есептеу үшін кестеде келтірілген айлық жалақыны орташа жұмыс күніне (24) бөлеміз:

$$T = \frac{Ж_a}{Жк} \quad (5.6)$$

мұндағы $Ж_a$ – бір айлық еңбекақы мөлшері; [16].

Жк – ай ішіндегі жұмыс күндерінің саны (24 күн – алтыкүндік жұмыс аптасы).

Жоба жетекшісі үшін:

$$T = \frac{150000}{24} = 6250 тг/күн;$$

Құрушы инженер үшін:

$$T = \frac{130000}{24} = 5416{,}66\ тг/күн;$$

«Экономика» бөлімі бойынша кеңес беруші үшін:

$$T = \frac{130000}{24} = 5416{,}66\ тг/күн;$$

ТҚ бөлімі бойынша кеңес беруші үшін:

$$T = \frac{100000}{24} = 4166{,}66\ тг/күн;$$

Әр жұмыс түріне байланысты күн есебінде циклдің ұзақтығын, іріленген түрінде төменгі өрнек бойынша табуға болады:

$$t_n = \frac{T}{q_n \cdot z \cdot K} \qquad (5.7)$$

мұндағы Т – кезеңнің еңбек сыйымдылығы, норма – сағат;

q_n – кезеңдегі орындаушылар саны;

z – жұмыс күнінің ұзақтығы, сағат, z = 7 сағат;

К – уақыт нормасының орындалу коэффициенті, К = 1.1.

Алынған t_n шамасын бүтін санға жуықтаймыз.

Жоба жетекшісі, тапсырманың қойылуы:

$$t_1 = \frac{21}{1 \cdot 7 \cdot 1{,}1} \approx 3 \text{ күн};$$

Құрушы инженер, бастапқы мәліметтерді жинау:

$t_2 = \frac{35}{1 \cdot 7 \cdot 1,1} \approx 5$ күн;

Жоба жетекшісі, құрылатын желінің сапалылығы мен тиімділігі деңгейлерін таңдау және негіздеу:

$t_3 = \frac{14}{1 \cdot 7 \cdot 1,1} \approx 2$ күн;

Құрушы инженер, енгізу стратегияларын қарастыру:

$t_4 = \frac{7}{1 \cdot 7 \cdot 1,1} \approx 1$ күн ;

Құрушы инженер, жабдықты таңдау:

$t_5 = \frac{14}{1 \cdot 7 \cdot 1,1} \approx 2$ күн ;

Құрушы инженер, жабдықты сатып алу:

$t_6 = \frac{14}{1 \cdot 7 \cdot 1,1} \approx 2$ күн ;

Құрушы инженер, қолданылатын платформамен құрылғылардың бірігуі:

$t_7 = \frac{21}{1 \cdot 7 \cdot 1,1} \approx 3$ күн ;

Құрушы инженер, аутентификация мен авторизация ережелерін баптау:

$t_8 = \frac{21}{1 \cdot 7 \cdot 1,1} \approx 3$ күн ;

Құрушы инженер, құрылғыларды қосу:

$t_9 = \frac{14}{1 \cdot 7 \cdot 1,1} \approx 2$ күн ;

Құрушы инженер, сертификаттарды жүктеу:

$t_{10} = \frac{7}{1 \cdot 7 \cdot 1,1} \approx 1$ күн ;

Құрушы инженер, бағдарламаларды таңдау:

$$t_{11} = \frac{7}{1 \cdot 7 \cdot 1,1} \approx 1 \text{ күн ;}$$

Жоба жетекшісі, бақылау:

$$t_{12} = \frac{14}{1 \cdot 7 \cdot 1,1} \approx 2 \text{ күн ;}$$

«Экономика» бөлімі бойынша кеңес беруші, «Экономика» бөлімін дайындау:

$$t_{13} = \frac{14}{1 \cdot 7 \cdot 1,1} \approx 2 \text{ күн ;}$$

«ТҚ» бөлімі бойынша кеңес беруші, «ТҚ» бөлімін дайындау:

$$t_{14} = \frac{14}{1 \cdot 7 \cdot 1,1} \approx 2 \text{ күн ;}$$

Жоба жетекшісі, ҒЗЖ дайындау:

$$t_{15} = \frac{7}{1 \cdot 7 \cdot 1,1} \approx 1 \text{ күн ;}$$

Жоба жетекшісі, есеп беруді тапсыру:

$$t_{16} = \frac{14}{1 \cdot 7 \cdot 1,1} \approx 2 \text{ күн ;}$$

t_n = 3+ 5 + 2 + 1 + 2 + 2 + 3 + 3 + 2 + 1 + 1 + 2 + 2 + 2 + 1 + 2 = 34 күн

Осылайша, ҒЗЖ барлық жұмыстарын орындауға 34 күн қажет.

ЛСБЖ жобалаудың сатылары мен қатысушылары 5.3-кестеде көрсетілген.

5.3-к е с т е – Жобаның орындалу сатылары мен мерзімі, қатысушылары

Жұмыс сатылары	Жұмыстың құрамы	Жұмыстың ұзақтығы және жоба қатысушылары	
		Қызметі	Күндер
Желіні құрудың қажеттілігін негіздеу	Тапсырманың қойылуы	Жоба жетекшісі	3
	Бастапқы мәліметтерді жинау	Құрушы инженер	5
	Құрылатын желінің сапалылығы мен тиімділігі деңгейлерін таңдау және негіздеу	Жоба жетекшісі	2
	Telepresence енгізудің стратегияларын қарастыру	Құрушы инженер	1
Жабдықты таңдау және сатып алу	Жабдықты таңдау	Құрушы инженер	2
	Жабдықты сатып алу	Жоба жетекшісі	2

5.3 кестенің

жалғасы

Жабдықты баптау және саясат құру	Жабдықты платформамен қосу	Құрушы инженер	3
	Аутентификация мен авторизация ережелерін баптау	Құрушы инженер	3
	Құрылғыларды қосу	Құрушы инженер	2
	Сертификаттарды жүктеу	Құрушы инженер	1
	Бағдарламаларды таңдау	Жоба жетекшісі	1
Есеп берулерді дайындау	Бақылау жасау	Құрушы инженер	2
	«Экономика» бөлімін дайындау	«Экономика» бөлімі бойынша кеңес беруші	2
	«ТҚ» бөлімін дайындау	«ӨТҚ» бөлімі бойынша кеңес беруші	2
	ҒЗЖ дайындау	Жоба жетекшісі	1
	Есеп беруді тапсыру	Жоба жетекшісі	2

Желіні құру жобасына қатысушы қызметкерлердің негізгі еңбекақысын есептеудің мәліметтері 5.4-кестеде келтірілген.

5.4-к е с т е – Еңбек шығындары

Орындаушы	Бір күндік еңбекақы, теңге	Күн саны	Қосынды, теңге
Жоба жетекшісі	6250	11	68750
Құрушы инженер	5416,16	19	102907
«Экономика» бөлімі бойынша кеңес беруші	5416,16	2	10832
«ТҚ» бөлімі бойынша кеңес беруші	4166,66	2	8332
Қорытынды		34	190821

Қосымша еңбекақы негізгі еңбекақының 10%-ын құрайды және 5.5-өрнекке сәйкес:

$Ж_{қос}$ = 0,1·190821=19082,1 тенге құрайды.

Еңбекақы қорының қосындысы (ЖТФ):

ЖТФ = 190821+ 19082,1 = 209903,1 тенге

5.4.3 Әлеуметтік аударылымдарды есептеу

Әлеуметтік салық шығындары ҚР СК 358-бап 1-б. сәйкес аударылған пайда мөлшерінің 11%-ын құрайды және келесі өрнекпен есептеледі:

$$О_с = 0.11 \cdot (\text{ЖТФ} - \text{ЗҚ}) \quad (5.8)$$

мұндағы ЗҚ – зейнетақы қорына аударылымдар.

Зейнетақы қорына аударылымдар мөлшерінің 10%-ын құрайды, ҚР СК сәйкес әлеуметтік салық салынбайды және келесі өрнекпен есептеледі:

$$\text{ЗҚ} = 0.1 \cdot \text{ЖТФ} \quad (5.9)$$

Зейнетақы қорына аударылымдар:

ЗҚ = 0,1·209903,1 =20990,31 тенге

Сонда, әлеуметтік қажеттіліктерге аударылымдар:

$О_с$ = 0,11·(209903,1 – 20990,31) = 20780,4 тенге құрайды

5.4.4 Электр энергиясын жұмсалатын шығындарды есептеу

Электр энергиясы шығындары жабдыққа жұмсалатын электр энергиясы шығындары мен қосымша қажеттіліктерге жұмсалатын шығындардан құралады. Жабдықтың үздіксіз жұмыс істеу қажеттілігін ескере отырып, шығын қосындысы келесі өрнекпен есептеледі:

$$Э = Ш_{эл.эн.} + Ш_{қос.қаж} \quad (5.10)$$

мұндағы $Ш_{эл.эн.}$ – жабдыққа жұмсалатын электр энергиясы шығындары;

$Ш_{қос.қаж.}$- қосымша қажеттіліктерге жұмсалатын шығындар (жабдыққа жұмсалатын электр энергиясы шығындарының 5%-ын құрайды).

Жабдыққа жұмсалатын электр энергиясы шығындары келесі өрнекпен есептеледі:

$$З_{эл.эн} = W \cdot T \cdot S \qquad (5.11)$$

мұндағы W – пайдаланылатын қуат, 2 кВт;

T – жұмыс уақыты, T = 238 с;

S – тариф, 1 кВтч = 12,5 теңге (ҚҚС-сыз);

$З_{эл.эн} = 2 \cdot 238 \cdot 12,5 = 5950$ теңге;

$З_{доп.нуж.} = 0,05 \cdot 5950 = 297,5$ теңге.

Электр энергиясы шығындары 5.10 өрнекке сәйкес:

Э = 5950+ 297,5 = 6247 теңге құрайды.

5.4.5 Амортизациялық аударылымдарды есептеу

Қазіргі таңда компьютерлік жабдыққа амортизация нормасы ($Н_А$) барлық жабдық құнының 40% құрайды және келесі өрнекпен есептеледі:

$$A_0 = \frac{H_A \cdot K_0 \cdot N}{100\% \cdot 12 \cdot n} \qquad (5.12)$$

мұндағы $К_0$ – жабдық құны;

N – жұмысты орындауға кететін күн саны

n – ай ішіндегі күн саны.

$$A_0 = \frac{40 \cdot 3928530 \cdot 34}{100 \cdot 12 \cdot 24} = 185514 тенге.$$

5.4.6 Үстеме шығындарды есептеу

Үстеме шығындар еңбекақы қоры шығындарының 25%-ын құрайды және келесі өрнекпен есептеледі:

$$Н=0,25 \cdot ЖТФ, \quad (5.13)$$

$Н = 0,25 \cdot 209903,1 = 52476$ тенге.

Осылайша, желіні жобалауға жұмсалатын капиталдық салымдарды 5.2-өрнекке сәйкес есептейміз:

$К_{жш}$= 209903,1 +20780,4 + 185514 + 6247,5 + 52476 = 474921 тенге

Желіні жобалауға жұмсалған шығындардың нәтижелері 5.7-кестеде келтірілген.

5.7-к е с т е – IP телефонияны қолдана отырып желіні жобалауға жұмсалатын капиталдық салымдар

Көрсеткіш	Сомасы, теңге	Пайыздық бөлігі %
ЖТФ, теңге	209903,1	44,19
Әлеуметтік қажеттіліктерге аударылымдар, теңге	20780,4	4,3
Амортизациялық аударылымдар, теңге	185514	39,06
Электр энергиясы шығындары,	6247,5	1,3

теңге		
Үстеме шығындар, теңге	52476	11,04
Қорытынды	474921	100

Капиталды салымдардың есептеу 5.1 формулаға сәйкес:

∑К = 3928530+ 474921 = 4 403 451 теңге.

5.4.7 Жобаның экономикалық тиімділігін анықтау

Аудандық әкімшілік үшін IP телефония қолдану арқылы компьютерлік желісін құру әлеуметтік маңызды жобалар қатарына жатады.

Telepresence технологиясын ендірудің әлеуметтік эффектісі:

– аудан орталығындағы жұмыскерлердің еңбекті ұйымдастыруын жоғарлату;
– қазіргі басқару шешімдерін шешу үшін мәліметтерді қабылдау сапасын жоғарлату;
– төтенше жағдайлар кезінде жедел байланыс орнату;
– қашықтан оқыту әдісін пайдалана отырып кадрларды дайындауға және қайта дайындауға кететін шығынды азайту.

5.4.8 «Бизнес жоспар» бөлімі бойынша қорытынды

Жобаны жүзеге асыруға қажетті капиталдық салымдар - 4 403 451 теңгені құрады, соның ішінде жабдыққа жұмсалатын шығын – 3928530 теңге, желіні жобалауға жұмсалатын шығын – 474921теңге.

Қазіргі таңда интернет желісі қарқынды дамуда. Соның әсерінен жаңа технология мен мемелекеттік басқару саласы тығыз байланыста бола отырып, мемлекеттік басқару саласы заманға сай жабдықтандыру мен ақпараттарды орталықтандырылған желіге біріктіру мәселесі өзекті болып отыр.

Берілген дипломдық жұмыста «Қазақтелеком» АҚ Мәліметтік Жүйелер Дирекциясының корпоративтік торын басып алуларды бақылау жүйесін ұйымдастыру іске асырылды.

ҚОРЫТЫНДЫ

Берілген дипломдық жұмыста «Қазақтелеком» АҚ Мәліметтік Жүйелер Дирекциясының корпоративтік торын басып алуларды бақылау жүйесін ұйымдастыру іске асырылды. Корпоративтік тордың мәліметтік қауіпсіздігінің келесідей сұрақтары қарастырған:

– корпоративтік компьютерлік торда қорғаныс жүйелерін пайдалану қажеттілігін негіздеу;

– техникалық шешімді таңдауды негіздеу, оның ішінде CiscoCatalyst 6500 Series үшін тор аралық экранның модулін шабуылдарды анықтау жүйесін таңдаудың негіздеу;

– маршрутизация тиімділігін, мәліметтер трафигын, дыбыстық, бейне қорғауды қамтамасыз ететін жүйені таңдау, CiscoNME-RVPN модулі Cisco 2800 және Series 3800 үшін маршрутизаторлар жанұясы SeriesIntegratedServicesRouters;

– қажетті жабдықты орналастыру жоспарын жасау мәселесі қарастырылған;

– шабуылдарды анықтау жүйелерінің политикасын реттеу.

Бұл жобаны жасау барсында басып алуларды бақылауға кететін шығындардың тиімділігі ҚР-ғы экономикалық жағдай мен еңбекті қорғау нормативті құжаттарын ескере отырып есептелінді.

Пайдаланылған әдебиеттер тізімі

1. Лукацкий А. Обнаружение Атак. – СПб.: БХВ – Санкт - Петербург, 2003.

2. 2005 CSI/FBI Computer Crime and Security Survey. Spring 2005. Computer Security Institute. Federal Bureau Investigation’s ComputerIntrusion Squad.

3. Курушин В. Д., Минаев В. А. Компьютерные преступления и информационная безопасность. Справочник. М.: Новый Юрист, 1998.

4. Лукацкий А. В. Анатомия распределенной атаки. PCWeek/RE, № 5, 2000.

5. Концепция информационной безопасности корпоративной сети Акционерного общества «Казахтелеком». Проект, 2006.

6. Олифер В., Олифер Н. Компьютерные сети. Принципы, технологии, протоколы. – СПб: Издательский дом «Питер», 2005. – 864 с.

7. Беклешев В.К. Технико-экономическое обоснование дипломного проекта. – Москва, 1991. – 202 с.

8. Алибаева С.А. Дипломное проектирование. Методические указания. – Алма-Ата, 2001. – 20 с.

9. Методические указания к выполнению раздела «Охрана труда и окружающей среды в дипломном проекте», Алма-Ата: АЭИ, 1984. – 42с.

10. Кошулько Л.П., Суляева Н.Г. Производственное освещение. Методические указания к выполнению раздела «Охрана труда» в дипломном проекте. – Алма-Ата, 1989. – 40 с.

11. ГОСТ 12.1.004-91 Пожарная безопасность. Общие требования. – Москва: Издательство стандартов, 1992. – 264 с.