ҚАЗАҚСТАН РЕСПУБЛИКАСЫ БІЛІМ ЖӘНЕ ҒЫЛЫМ МИНИСТРЛІГІ
«АЛМАТЫ ЭНЕРГЕТИКА ЖӘНЕ БАЙЛАНЫС УНИВЕРСИТЕТІ»
коммерциялық емес акционерлік қоғамы
«Ақпараттық қауіпсіздік жүйелері» кафедрасы

«ҚОРҒАУҒА ЖІБЕРІЛДІ»
Кафедра меңгерушісі с.ғ.к., доцент Бердібаев Р. Ш.
_____ «_____» _____ 2019 ж.
(қолы)

ДИПЛОМДЫҚ ЖОБА

Тақырыбы: «Локальді желілердегі ақпаратты қорғауды жобалау»
Мамандығы: 5В100200 – «Ақпараттық қауіпсіздік жүйелері»
Орындаған: Батырханов Дастан Тобы: СИБк-15-1
Ғылыми жетекші: аға оқутышы Ургенишбаев К. М.

Кеңесшілер:
Экономикалық бөлім бойынша:
э.ғ.к., проф. Аренбаева Ж.Г.
(ғылыми дәрежесі, атағы, аты-жөні)
_____ «28» 05 2019 ж.
(қолы)

Тіршілік қауіпсіздігі бөлімі бойынша:
аға оқытушы Торбаев Д.Д
(ғылыми дәрежесі, атағы, аты-жөні)
_____ «13» 05 2019 ж.
(қолы)

Есептеу техникасын қолдану бойынша:
аға оқутышы Ургенишбаев К.М
(ғылыми дәрежесі, атағы, аты-жөні)
_____ «04» 15 2019 ж.
(қолы)

Мөлшер бақылаушы:
Аға оқытушы, э.ғ.м., Макарова Н.Ф
(ғылыми дәрежесі, атағы, аты-жөні)
_____ «30» 05 2019 ж.
(қолы)

Пікір беруші:
Алешев Сырым Бимуратович
(ғылыми дәрежесі, атағы, аты-жөні)
_____ «31» мамыр 2019 ж.
(қолы)

Алматы 2019

ҚАЗАҚСТАН РЕСПУБЛИКАСЫ БІЛІМ ЖӘНЕ ҒЫЛЫМ МИНИСТРЛІГІ
«АЛМАТЫ ЭНЕРГЕТИКА ЖӘНЕ БАЙЛАНЫС УНИВЕРСИТЕТІ»
коммерциялық емес акционерлік қоғамы

Басқару және ақпараттық технологиялар институты
Ақпараттық қауіпсіздік жүйелері кафедрасы
5В100200 – «Ақпараттық қауіпсіздік жүйелері» мамандығы

Дипломдық жобаны орындауға берілген

ТАПСЫРМА

Студент: Батырханов Дастан
(аты-жөні)

Жобаның тақырыбы: Локальді желілердегі ақпаратты қорғауды модельдеу

2019 ж. «03» 01 № 33 университет бұйрығымен бекітілді.

Аяқталған жұмысты тапсыру мерзімі: «____»_____20___ ж.

Жобаға алғашқы деректер (талап етілетін зерттеу (жоба) нәтижелерінің параметрлері және зерттеу нысанының алғашқы деректері): Radius Server-тұрмыс желілік қызметтерге қосылатын пайдаланушылардың орталықтандырылған аутентификациясын, авторизациясын және есебін қамтамасыз етуге арналған желілік хаттама. Radius Server - таңдаулардағы көп жағдайда түсіндіріледі: ескірген жабдықпен жұмыс істеу әдебиетін сақтамалы отырып, жаңа функционалдылықта жұмыс істейді.
Локальді желілердегі ақпаратты сенімді қорғауды қамтамасыз ету үздіксіз процесс, ол қорғаудың түйіні туралы басқарылады, қорғау жүйесіндегі әсіз жерін анықтау

Диплом жобасындағы әзірленуі тиіс мәселелер тізімі немесе диплом жобасының қысқаша мазмұны:
1. Локальді желілердегі ақпаратты қорғаудың жолдары мен тәсілдері;
2. Ақпаратты қорғау тәсілі;
3. Локальді желілердегі ақпаратты қорғау тәсілдерін талдау;
4. Идентификация және аутентификация;
5. Компьютерлік жүйелер қауіпсіздігінің негізгі ұғымдары;
6. Техникалық - экономикалық негіздеме;

7. Өмір тіршілік қауіпсіздігі;
8. Қорытынды

Графикалық материалдардың (міндетті түрде дайындалатын сызбаларды көрсету) тізімі:

1. Ақпаратты ағудан қорғау және техникалық арналар арқылы ұстап қалу мәселесінің шешімінің блок-сызбасы;
2. Ұйымдық бағдарламалық құралдардың түрлері;
3. Ақпараттық қауіпсіздіктің жүйелерін іске асыру моделі;
4. Radius Server-дің схемасы

Негізгі ұсынылатын әдебиеттер:

1. Золотов, С.Н. Протоколы Internet / С.Н. Золотов. – СПб.: BHV - Санкт-Петербург, 2002. – 212 с.
2. Олифер, В.Г. Компьютерные сети. Принципы, технологии, протоколы / В.Г. Олифер, Н.А. Олифер. – СПб.: Издательство „Питер", 2000. – 672 с
3. Расторгуев С.П. Программные методы защиты информации в компьютерах и сетях. Издательство агентства „Яхтсмен", М.: – 1995

Жоба бойынша жобаның бөлімдеріне қатысты белгіленген кеңесшілер

Бөлімдері	Кеңесшілері	Мерзімі	Қолы
Экономика бөлімі	Арендаева Ж.Г.	04.03 – 28.05.19	[signature]
Өмір тіршілік қ-і б-і	Бураев Э.Э.	01.04-13.05	[signature]
Есептеу техникасы бойынша	Ургенишбаев К.М.	01.04 – 01.05	[signature]

Диплом жобасын дайындау
КЕСТЕСІ

Бөлімдердің атауы, әзірленетін мәселелердің тізімі	Ғылыми жетекшіге ұсыну мерзімдері	Ескерту
1. Локальді желілердегі ақпаратты қорғаудың нормативтік құжаттары мен талаптары	10. 02. 2019	
2. Тұқсат сөз кіруді ұйымдастыруда ақпаратты қорғау құралдарының және талаптарының жіктелуі	20. 02. 2019	
3. Локальді желілердегі ақпаратты қорғау талаптарын талдау	1. 03. 2019	
4. Локальді желілердегі ақпаратты қорғаудың негізгі бағыттары	20. 03. 2019	
5. Radius Server	01. 05. 2019	
6. Техникалық - экономикалық негіздеме	22. 05. 2019	
7 Өміртіршілік қауіпсіздігі	13. 05. 2019	
8. Жұмыстың нәтижесі	29. 05. 2019	

Тапсырманың берілген уақыты «____»_____20___ж.

Кафедра меңгерушісі _____ (_____)
(колы) (аты-жөні)

Жобаның
ғылыми жетекшісі _____ (Аға оқытушы Ургенишбаева Ж.)
(колы) (аты-жөні)

Орындалатын тапсырманы
қабылдаған студент _____ (Бектурханов Д. Ә.)
(колы) (аты-жөні)

АҢДАТПА

Бұл дипломдық жұмыста локальды желілердегі ақпаратты қорғауды жобалау бойынша мәліметтердің қауіпсіздігін қамтамасыз ету мақсатында, бағдарламалық интерфейс құрылды.

Radius Server – түрлі желілік қызметтерге қосылатын пайдаланушылардың орталықтандырылған аутентификациясын, авторизациясын және есебін қамтамасыз етуге арналған желілік хаттама. Сондай-ақ екі жақты қорғаныс жасалды.

АННОТАЦИЯ

В данном дипломном проекте создан программный интерфейс для обеспечения безопасности данных по проектированию защиты информации в локальных сетях.

Radius Server – сетевой протокол, предназначенный для обеспечения централизованной аутентификации, авторизации и учета пользователей, подключаемых к различным сетевым услугам. Также была создана двусторонняя защита.

ANNOTATION

In this thesis project created a software interface to ensure the security of data on the design of information security in local networks.

Radius Server – is a network Protocol designed to provide centralized authentication, authorization and accounting of users connected to various network services. Bilateral protection was also created.

Мазмұны

Кіріспе

Ақпаратты қорғау мәселесі адамдар жазу сауатына үйренген кезден бастап көтеріліп келе жатыр. Кей кездері барлығы біле беруге болмайтын ақпараттар болады. Осындай ақпаратқа ие адамдар, оны қорғау үшін әртүрлі амалдар қарастырып отырды. Ең танымал қарастырулар ретінде құпия жазулар яғни цифрлауды айтамыз. Қазіргі таңда жалпылай компьютерлеу кезінде көп адамдардың денсаулығы мен өмірі ақпаратты өңдеу компьютерлік жүйелерінің қауіпсіздігіне байланысты болып отыр, сонымен қатар әр түрлі нысандарды бақылау және басқаруға да байланысты. Мұндай нысандарға телекомуникация жүйелері, банк жүйелері, атомдық стансалар, әуе және жер транспорттарын басқару жүйелері, құпия және жасырын ақпараттарды сақтау және өңдеу жүйелері жатады. Бұл жүйелердің қалыпты және қауіпсіз жұмыс істеуі үші олардың қауіпсіздігі мен тұтастығын сақтап отыру маңызды.

Компьютерлік желілердің артықшылықтары олардың несие-қаржы саласының, мемлекеттік басқару және жергілікті өзін-өзі басқару органдарының, кәсіпорындар мен ұйымдардың ақпараттық жүйелерінде кең таралуына себепші болды. Сондықтан осы дипломдық жобаның мақсаты компьютерлік желілерді құру және жұмыс істеу негіздерімен танысу болып табылады, қойылған мақсатқа жету үшін бірқатар міндеттерді шешу қажет:

а) компьютерлік желілермен танысу, олардың ерекшеліктері мен ерекшеліктерін анықтау;

ә) елілерді құрудың негізгі тәсілдерінің сипаттамасы (желі топологиясы);

б) желі ресурстарына рұқсатсыз қол жеткізуден қорғау әдістерімен танысу;

в) желідегі пайдаланушылардың келісілген өзара іс-қимылынқамтамасызететін желінің негізгі хаттамаларының қысқаша сипаттамасы;

г) жұмыстың қорытындысын шығару және осы тақырып бойынша ұсыныстар енгізу.

Қойылған міндеттерді шешу кезінде негізгі әдіс осы тақырып бойынша әдебиетті талдау болып табылады. Локальді желідегі (ЛЖ) ақпаратты қорғау мәселесі осы жүйені қолданылатын мамандардың қарауында ғана емес, сонымен қатар осы жүйені пайдаланатын кең қолданушылар назарында болады. Ақпаратты қорғау дегеніміз ЛЖ ақпаратты жоғалтып алмас үшін қолданылатын арнайы құрылғылар, әдістер мен шараларды пайдалану деген сөз. Есептеуіш техниканың кең таралуы мен оны барлық жерде пайдалану ЛЖ сақталатын, өңделетін, жиналатын ақпараттардың осал тұстарын арттырып отыр.

Ақпараттың осалдығын көрсететін үш нақты аспект көрсетілді:

а) физикалық жою мен бұрмалануға ұшырау;

ә) рұқсатсыз модификация мүмкіндігі (байқаусызда немесе қаскүнемдік-пен);

б) ақпаратты қолдануға рұқсаты жоқ тұлғалардың ақпаратты қолдануына қол жеткізуі.

ЛЖ ақпаратты қорғаудың негізгі бағыттары:

ЭЕМ ақпаратты өңдеу құрылғысының ұйымдастырылған техникалық және ұйымдастыру шараларын жетілдіру;

ЭЕМ ақпаратты рұқсатсыз алуды тоқтату;

техникалық құрылғылардың көмегімен ақпаратты рұқсатсыз алуды тоқтату;

ЛЖ ақпаратты қорғау кезінде мәселені шешудегі басты қиындықтар:

а) қолданудың жалпылығы;

ә) қызмет етудің әрдайым қиындай беруі;

дербес компьютерлердің бағдарламалық қамтамасыздандыруының, архитектуралық шешімдерінің әртүрлілігі және қолданушының әр түрлі міндеттерін шешу үшін оңай бейімделуі.

Қазіргі заманғы компьютерлік желілер жүйе болып табылатындығын атап өткен жөн, оның мүмкіндіктері мен сипаттамалары жалпы дербес компьютерлер желісінің құрамдас элементтерінің қарапайым сомасының тиісті көрсеткіштерінен айтарлықтай асып түседі.

Ақпаратты сенімді қорғау үшін, қорғау жүйесі үнемі қауіпсіздікті қамтамасыз етуі қажет:

а) бөгде тұлғалардан бөлек ақпаратты өңдеу;

ә) қолданушылардан бөлек ақпаратты өңдеу жүйесі;

б) қолданушылар бір бірінен және әр қолданушы өзінен бөлек.

в) өз өзінен бөлек ақпаратты өңдеу.

Бұл дипломдық жобаның мақсаты АБЖ-нің осы бөліміне жалпы ұсынымды жасау болып табылады, яғни ЛЖ ақпаратты қорғауды қамтамасыз етіп, қызметтік және құпия ақпаратқа рұқсатсыз енуді болдырмас үшін құжаттардың типтік пакетін дайындау.

Мен тақырыбымның өзектілігі:

- ақпараттық күрес жағдайында мекеменің қауіпсіздік саясатын құрау;
- ЛЖ ақпараттық қауіпсіздікті арттыруға бағытталған бірқатар маңызды мәселелерді зерттеу және тереңірек анықтау;
- мекемедегі ақпараттық қауіпсіздік бойынша құжаттар пакетін құру және жұмыс жағдайына енгізу.

1 Локальді желілердегі ақпаратты қорғаудың жолдары мен тәсілдері

1.1 Рұқсатсыз кірудің жолдары, ақпаратты қорғау құрылғылары мен тәсілдерінің жіктелуі

Локальді желі – бұл сапалы байланысты қамтамасыз ететін компьютерлік желі. Локальды желіге келесі қасиеттер тән:

а) ақпаратты тасымалдаудың жоғары жылдамдығы, орташа 100 Мбит/с;

ә) тасымалдау қателерінің төмен болуы;

б) желіге қатынас құру әдісінің жоғарғы жылдамдықта жұмыс орындауы, қатынас құру уақыты 10 мс;

в) желідегі компьютерлердің сандарының шектеулігі.

Компьютерлер – бұл ең алдымен мәліметтерді бейнелеуде екілік сандар (биттер) қолданатын сандық құрылғылар. Сондықтан желі арқылы мәліметтерді бір компьютерден екіншісіне жіберу биттерді тасымалдау ортасы арқылы алмасуын жүзеге асыруымен бірдей. Байланыс жүйелерінде ақпаратты жіберу үшін электр тогы, радиотолқындар немесе жарық сәулесі сияқты физикалық тасымалдағыштар қолданылады.

Компьютерлік желілер көп машиналы ассоциациялардың жоғарғы нысаны болып табылады. Компьютерлік желінің көп машиналы есептеу кешенінен негізгі айырмашылықтарын атап көрсетеді.

Бірінші айырмашылық-өлшемдік. Көп машиналы есептеу кешенінің құрамына әдетте екі, ең көбі үш ЭЕМ кіреді. Есептеу желісі бір-бірінен бірнеше метрден мың километрге дейінгі қашықтықта орналасқан ондаған және тіпті жүздеген ЭЕМ тұрады.

Екінші айырмашылық – ЭЕМ арасында функцияларды бөлу. Егер көп машиналы есептеу кешенінде деректерді өңдеу, беру және жүйені басқару функциялары бір ЭЕМ-де іске асырылса, онда есептеу желілерінде бұл функциялар әртүрлі ЭЕМ арасында бөлінген.

Үшінші айырмашылық – желіде хабарламаларды маршруттау міндетін шешу қажеттілігі. Бір ЭЕМ-ден екіншісіне хабарлама ЭЕМ-ді бір-бірімен Қосатын байланыс арналарының жай-күйіне байланысты әртүрлі бағыттар бойынша берілуі мүмкін

Локальді желі – [local area network – LAN] шектелген бір аумақта орналасқан, бір-бірімен байланысқан компьютерлер тобы. Локальді желіде компьютерлер арасының қашықтығы бірнеше километрге дейін жетуі мүмкін.

Локальді желілердің дамуы бірнеше себептерге байланысты:

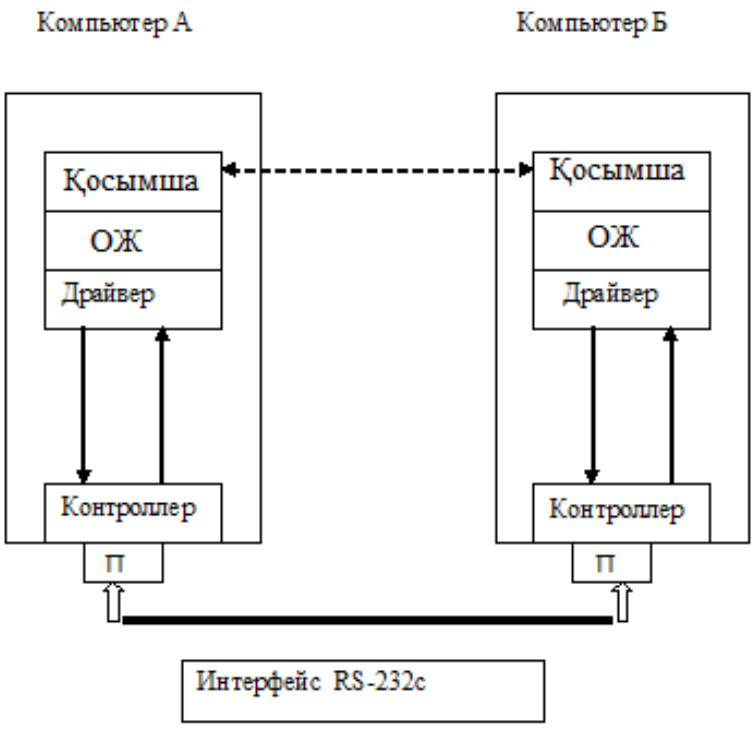
а) компьютерлерді бір желіге қосу компьютерлерді күтуге кететін шығынды азайту арқылы қаржыны үнемдеуге мүмкіндік береді (файл-серверде (желінің басты компьютері) бірнеше компьютерлер қолданатын бағдарламалар орнатылған белгілі бір дисктік кеңістік болса жеткілікті) [1].

ә) локальді желілер арқылы компьютерлер тез арада бір-біріне мәліметтер жібере алады;

б) арнайы бағдарламалық құрал бар болса, локальді желілер файлдарды бірлесіп қолдануға мүмкіндік береді (мысалы, 1С бағдарламасы бойынша бухгалтерлер бірнеше компьютерлерде бірігіп жұмыс жүргізе алады);

в) локальді желі арқылы түрлі стансалардағы пайдаланушылар бірігіп перифериялық құрылғыларды қолдана алады (мысалы, принтер немесе сканер);

г) желі пайдаланушылары ғаламторға модемсіз ене алады, яғни, модем тек серверге байланысады, ал, пайдаланушылар Ғаламторға локальді желінің осы сервері арқылы енетін болады.(1.1 сурет)



Сурет 1.1 – Екі компьютердің бір-бірімен мәлімет алмасу алгоримі

Локальді желілерде болатын ақпаратқа рұқсатсыз енудің жолдары:

а) жанама – Локальді желі бөлшектеріне физикалық мүмкіндіктерсіз ену;

ә) тікелей – Локальді желі бөлшектеріне физикалық қолжетімділікпен ену.

Ақпаратқа рұқсатсыз кіру себептері:

а) конфигурация қателері (қатынау құқықтары, брандмауэрлер, дерекқор сұрауларының негізгі бөлігіндегі шектеулер);

ә) авторизациялау құралдарының әлсіздігі (парольдерді ұрлау, смарт-карталар, нашар қорғалған жабдыққа жеке қол жеткізу, қызметкерлер болмаған кезде қызметкерлердің жұмыс орындарының ашылуына жол бермеу);

б) бағдарламалық жасақтама қателері;

в) ресми өкілеттікті асыра пайдалану (резервтік көшірмелерді ұрлау, ақпаратқа қол жеткізу құқығымен сыртқы БАҚ-на көшіру);

г) LAN желісіндегі қорғалмаған қосылымдарды пайдаланғанда байланыс арналарын тыңдау;

д) Қызметкерлердің компьютерлеріндегі кілттерді, вирустар мен трояндарды жеке тұлғасыздандыру үшін пайдалану.

1.1.1 Ақпаратты қорғау құрылғылары

Ақпаратты қорғау құралдары – үлкен, толық техникалық құралдар жиынтығы. Олар электронды, оптикалық немесе электрлік болып табылады және қоғамдық және жеке қауіпсіздік үшін әр түрлі ақпаратты қорғау үшін қолданылады. Бұл құрылғыларда, ең алдымен, 3G, GSM және CDMA режимдерінде ұялы телефон сигналдарын үзетін құралдар болуы керек. Мұндай құрылғылар алдын-ала белгіленген белгілі бір жиілікте қосылулар арналарында кедергілерді қалыптастыру үшін жасалады. Ұялы үндеткіштер белгілі бір радиуста жұмыс істейді, онда көптеген жиіліктерді тоқтатады. Бұл қауіпсіздік құрылғылары портативті және бекітілген, бірақ олар сымсыз арналардың ұялы байланысына кедергі келтіретін түріне қарамастан, бейнені бүлдіріп, бейнекамера жұмысына әсер етеді. Ауыстырғыштардың әсері түрлі факторларға байланысты болуы мүмкін. Олар негізгі ұялы мұнарадан, сепараторды қосатын бөлмені, қабырғаның қалыңдығына дейінгі қашықтық болуы мүмкін. Нәтижесінде кептелістің өзіндік күші әсер етеді.

Ақпаратты қорғау мәселесін шешу үшін қолданылатын негізгі құрылғылар, яғни қорғау механизмі үшін пайдаланылатын құрылғылар:

а) техникалық құрылғылар – электр, электромеханикалық, электронды құрылғылар түрінде болады. Техникалық құрылғылар келесідей болып бөлінеді:

ә) аппараттық құрылғылар, олар тікелей аппаратқа немесе құрылғыға орналастырылады, олар стандартты интерфейс бойынша (жұп бойынша ақпаратты басқару схемасы, кілт бойынша жады алаңын қорғау схемасы, арнайы регистрлер);

б) физикалық – олар автономды құрылғы болып және бақылау жүйесі (бақылаудың және күзет дабылының электр-механикалық құрылғысы. Есіктегі құлып, терезелердегі торлар) түрінде іске асырылады;

в) бағдарламалық құрылғы– ақпаратты қорғаумен байланысты жұмысты атқаратын арнайы бағдарламалар;

г) ақпаратты қорғау концепциясының даму жолдары барысында мамандар мынадай қорытындыға келді, осы жоғарыда айтылған ақпаратты қорғау тәсілдерінің бірін қолдану, ақпаратты сенімді сақтаудың кепілі бола алмайды. Ақпаратты қорғау тәсілдері мен құрылғыларын пайдалану және дамытудың кешенді амалдары қажет болып табылады [2].

1.1.2 Ақпаратты қорғау тәсілі

Ақпаратты қорғаудың әдістері мен тәсілдері ақпараттық қауіпсіздік проблемаларын шешу үшін нақты шаралар мен технологияларды қамтиды.

Қазіргі уақытта қорғау әдістерін бірнеше негізгі топтарға бөлуге болады. Ақпаратты қорғаудың әдістері мен тәсілдерінің жіктелуі:

а) желіде ақпарат берудің және оны сақтаудың түрі мен құрылымын өзгерту тәсілдері, мысалы қорғаудың криптографиялық әдістерін қолдану;

б) ақпараттық жүйелерді басқаруға және қауіпсіздік ережелерін регламенттеуге негізделген деректерді қорғаудың ұйымдастырушылық әдістері;

в) арнайы бағдарламалық және аппараттық құралдарды пайдалануды білдіретін ақпаратты қорғаудың техникалық және технологиялық әдістері.

Ақпаратты қорғау технологиялары ақпараттың жылыстауын және оның жоғалуын болдырмайтын қазіргі заманғы әдістерді қолдануға негізделеді. Локальді желілердегі ақпаратты қорғаудың алты негізгі әдісі қолданылады:

- кедергі;
- бүркемелеу;
- регламенттеу;
- басқару;
- мәжбүрлеу;
- ынталандыру.

Барлық аталған әдістер ақпаратты қорғаудың тиімді технологиясын құруға бағытталған, бұл кезде немқұрайлылық себебі бойынша жоғалтулар алынып тасталған және қауіптердің түрлері көрініс табады.

а) кедергі – қорғалған ақпаратқа қаскүнемнің жетуі үшін физикалық кедергі келтіру (аппратурасы бар аудан мен ғимаратқа, ақпаратты тасымалдаушыға);

б) кіруге рұқсатты басқару – жүйенің барлық ресуртарын реттеу арқылы ақпаратты қорғаудың тәсілі (техникалық, бағдарламалық құрылғылар, мәліметтер бөлшегі) кіруге рұқсатты басқару қорғаудың келесі функцияларынан тұрады:

1) қызметкерлер мен жүйе ресурстарын, қолданушыларды сәйкестендіру, сәйкестендіру дегеніміз жоғарыда айтылған әр нысанға ат, код және құпия сөз беру, сонымен қатар оларға ұсынылған сәйкестендіргіш бойынша субьекті немесе объектіні тану;

2) өкілеттілігін тексеру, белгіленген регламент бойынша апта күні, тәулік уақыты, сонымен қатар сұранылатын ресурстар мен шараларды сәйкестікке тексеру;

3) белгіленген регламенттер шеңберінде жұмыс жағдайын жасау және рұқсат ету;

4) қорғалатын ресурстарға келетін өтініштерді тіркеу;

5) жауап қайтару (жұмыстың кешігуі, қабыл алмауы, өшірілуі, дабыл), рұқсатсыз әрекет кезіндегі.

в) бүркемелену – Локальді желілердегі ақпаратты криптографиялық түрлендіру арқылы қорғау тәсілі. Ұзақ арақашықтыққа ақпаратты байланыс

желісі арқылы жіберген кезде криптографиялық жабу оны қорғаудың жалғыз сенімді жолы болып табылады;

г) регламенттеу – Локальді желі қызмет істеу барысында қорғалатын ақпараттың автоматтандырылған өңдеу және сақтау жағдайын жасау үшін, осы мүмкіндік кезінде оған рұқсатсыз кіру минимумға дейін жету жағдайын қамтамасыз ететін кешенді шара болып табылады. Тиімді қорғау үшін локальді желінің құрылымдық ретін қатаң түрде регламенттеу қажет (ғимарат архитектурасы, ғимартты жабдықтау, аппаратураларды орнату), ақпаратты өңдеуге қатысатын барлық қызметкерлердің жұмысын ұйымдастыру және қамтамасыз ету;

д) мәжбүрлеу – Локальді желі қолданушылары мен қызметкерлері материалдық, әкімшіліктік және қылмыстық жауапкершілік қауіпінде қорғалатын ақпаратты қолданудың және өңдеудің ережелерін сақтаулары тиіс.

Қарастырылған ақпаратты қорғаудың тәсілдері әртүрлі қорғайтын амалдардың нәтижесінде іске асады, сонымен қатар әртүрлі техникалық, бағдарламалық, ұйымдық, заң шығарушы және моральдік-этикалық әдістермен де іске асады [3].

Қорғаудың ұйымдастырылған тәсілдері деп локальді желі жасау және пайдалану кезіндегі ақпаратты қорғауды қамтамасыз ету үшін ұйымдастырылған құқықтық шараларды айтады. Ұйымдастыру шаралары локальді желінің барлық кезеңінде барлық құрылымдық бөлшектерін қамтиды: ғимараттың құрылысы, жүйені жобалау, жабдықтарды монтаждау және дұрыстау, сынау және тәжірбие, пайдалану. Әрбір кәсіпорында тұтас технология құрылатын ақпараттық қауіптердің негізгі түрі зиянкестердің деректерге рұқсатсыз қол жеткізуі болып табылады. Зиянкестер алдын ала қылмыстық әрекеттерді жоспарлайды, олар құрылғыларға тікелей қол жеткізу жолымен немесе ақпаратты ұрлау үшін арнайы әзірленген бағдарламаларды пайдалана отырып, алыстан шабуыл жасау жолымен жүзеге асырылуы мүмкін.

Қорғаудың заңнамалық тәсілдеріне мемлекеттің заңнамалық актілері жатады, ол шектелген рұқсаты бар ақпаратты қолдану және өңдеуге қатысты ережелерді регламенттейді, осы ережелерді бұзғаны үшін шаралар қолданылады.

Қорғаудың моральдік – этикалық тәсіліне дәстүрлі түрде және сол елдегі немесе қоғамдағы есептеуіш құралдардың таралу сипатына байланысты жасалған әртүрлі нормалар жатады. Бұл нормалар көп жағдайда міндетті болып табылмайды, яғни заңнамамен салыстырғанда, бірақ бұл шараларды орындамау адам мен адамдар тобының абыройы мен беделінің төмендеуіне алып келеді.

Жоғарыда аталған қорғау тәсілдері келесілерге бөлінеді:

а) формальді – қорғау функциясын алдын ала қарастырылған шараны қатаң түрде орындау және адамның қатысуымен болатын шаралар;

ә) формальді емес – адамдардың мақсатты түрдегі қызметімен анықталады, немесе осы қызметті регламенттейді [2].

1.2 Локальді желілердегі ақпаратты қорғау тәсілдерін талдау

Локальді желілердегі ақпаратты сенімді қорғауды қамтамасыз ету үздіксіз процесс, ол қорғаудың жүйелі түрде басқарылуы, қорғау жүйесіндегі әлсіз және тар орындарын анықтау, жетілдірудің оңтайлы жолдарын іске асыру және түсіндіру, сонымен қатар қорғау жүйесін дамытудан тұрады.

Зиянды бағдарлама (malware) – бұл жеке компьютерге немесе компьютерлік желіге залал келтіру үшін арнайы жасалған кез келген бағдарламалық қамтамасыз етуді белгілейді. Зиянды бағдарламалардың негізгі түрлерін қарастырайық:

- компьютерлік вирус – өз көшірмелерін жасауға (түпнұсқамен міндетті түрде сәйкес келмейтін) және оларды файлдарға, компьютердің жүйелік аймақтарына енгізуге, сондай-ақ басқа да деструктивті әрекеттерді жүзеге асыруға қабілетті бағдарлама. Бұл ретте көшірмелер одан әрі тарату қабілетін сақтайды;

- логикалық бомба – белгілі бір шартты орындау кезінде кейбір функцияны іске асыратын бағдарлама немесе Код фрагменті, мысалы, берілген күннің басталуы шарт болуы мүмкін. "Жарылу", логикалық бомба пайдаланушы үшін қажетсіз функцияны іске асырады, мысалы, кейбір деректерді жояды;

- трояндық жылқы – құжаттамада сипатталмаған негізгі іс-қимылдарға қосымша ретінде әрекет ететін бағдарлама. Трояндық жылқы – бастапқы зиянсыз бағдарламаға енгізілген командалардың қосымша блогы. Трояндық жылқы әдетте бір пайдаланушының өкілеттілігі шеңберінде, бірақ басқа Пайдаланушының (қаскүнем) мүддесінде әрекет етеді;

- құрт (желілік құрт) – компьютерлік желіде таратылатын, қорғау жүйелерін еңсеруге, сондай-ақ өз көшірмелерін жасауға және одан әрі таратуға және басқа да зиянды әрекеттерді жүзеге асыруға қабілетті зиянды бағдарламалардың түрі. Қорғаудың ең жақсы тәсілі - желіде жұмыс істеу кезінде сақтық шараларын қабылдау.

- құпия сөзді басып алушы – бұл құпия сөзді ұрлау үшін арнайы әзірленген бағдарлама. Сценарий келесідей болуы мүмкін. Бағдарлама экранға жұмыс сеансының аяқталғаны туралы хабарды, содан кейін жүйеге кіру үшін логин мен құпия сөзді енгізу сұрағын шығарады. Пайдаланушы енгізген деректер басып алушы бағдарламаның иесіне жіберіледі.

- клавиатуралық шпион (кейлоггер) – бағдарламалық немесе аппараттық құрал, оның негізгі мақсаты пернелерді басудың жасырын мониторингі және осы басулардың журналын жүргізу болып табылады. Кейлоггер жүйе үшін қауіпсіз, бірақ ол пайдаланушы үшін өте қауіпті болуы мүмкін: кейлоггер көмегімен парольдерді және пернетақта арқылы пайдаланушы енгізген басқа да құпия ақпаратты алуға болады. Вирусқа қарсы бағдарламалардың көпшілігі белгілі кейлоггерлерді таниды және олардан қорғау әдісі кез келген басқа

зиянды бағдарламалық қамтамасыз етуден қорғау әдістерінен айырмашылығы жоқ. Ақпарат қауіпсіздігіне қауіп-қатердің көптеген түрлерін іске асыруға ықпал ететін шарт бағдарламалық кодта "люктердің"болуы болып табылады. Люк – бұл бағдарламалық өнім құжаттамасында сипатталмаған осы бағдарламалық өніммен жұмыс істеу мүмкіндігі. Нәтижесінде пайдаланушы әдеттегі жағдайларда оған жабық (атап айтқанда, артықшылықты режимге шығу) мүмкіндіктер мен деректерге қол жеткізеді. Люктер көбінесе әзірлеушілерді ұмытудың нәтижесі болып табылады. Мысалы, Люк ретінде жөндеу процесін жеңілдету үшін құрылған және оның аяқталуы бойынша алыстатылмаған бағдарламаның бөліктеріне тікелей қол жеткізудің уақытша тетігі пайдаланылуы мүмкін. Люктерден тек бір ғана қорғау - олардың бағдарламада пайда болуына жол бермеу.

Локальді желілердегі ақпараттың қауіпсіздігі барлық қорғау құралдарын кешенді түрде пайдаланған кезде ғана қамтамасыз ете алады.

Қолданушылардың қажетті түрде дайындығы мен олардың қорғау ережелерін сақтауы.

Бірде бір қорғау жүйесі толық сенімді болып табылмайды. Ақпаратқа ену үшін қаскүнем қандай да бір шешім тауып алады деген ойда болу қажет.

1.2.1 ДЭЕМ ақпаратты қорғау. Ақпараттың жайылып кету арналары

Ақпаратты тарату арналарын өткізу түрлері бойынша ірі екі негізгі түрге – физикалық және ақпараттық бөлуге болады. Ақпараттық арналар әлеуетті ағу ықтималдығы мен көлемі бойынша физикалық арналардың мүмкіндіктерінен асып түседі.

Ақпараттың таралып кетуінің барынша таралған физикалық арнасы классикалық құжат айналымына – ұйым ішіндегі құжаттармен алмасуға, қызмет көрсету мен тауарларды клиенттермен және жеткізушілермен, сондай-ақ мұрағаттық сақтаумен байланысты. Ақпараттың таралып кетуі құжатты басып шығарғаннан кейін (мысалы, бас бухгалтердің немесе бас директордың принтері жалпы кеңсе кеңістігінде орналастырылған кезде), құжаттарды уақтылы жоймау (егер компания қызметкерлерді тиісті оқытуды жүргізбесе және шредерлерде үнемдесе), мұрағаттық құжаттары бар шкафтарға еркін кіру (сейфтердің болмауы), компанияларды ауыстыру немесе қайта ұйымдастыру кезінде құжаттарды дұрыс ауыстыру және жою және т. б. салдарынан болуы мүмкін.

Ақпараттық арналар әртүрлі және деректер көлемін өздері арқылы жіберуге қабілетті. Олардың негізгілері мыналар болып табылады:

а) ақпаратты ашудың ойдан тыс жағдайларының көп санымен сипатталатын корпоративтік пошта арқылы ағып кету ("жылдам қолдың" жылыстауы);

ә) хабар алмасу сервистерін қоса алғанда web-арналар арқылы ағып кету (IM);

б) алмалы-салмалы тасығыштар арқылы ағып кету;

в) ұялы құрылғылар арқылы ағып кету.

Серверлік компоненттен тікелей деректердің корпоративтік процестер мен технологияларда осалдықтар болған кезде жылыстауы мүмкін:

а) деректерді өңдеу және сақтау жүйелеріне қолжетімділікті сегменттеу және сүзу ұйымдастырылмаған;

ә) деректерге қолжетімділікті бақылау ұйымдастырылмаған – пайдаланушы құжаттармен жұмыс істеу кезінде қажет болған жағдайда көбірек артықшылықтар алады немесе деректерге қол жеткізу құқығын беру процесі дұрыс ұйымдастырылмаған;

б) артық пайдаланушыларды бақылау жоқ.

Ақпараттың таралып кетуінің web-арналары әртүрлі:

а) көптеген қол жетімді бұлтты сервистердің біріне деректерді түсіру;

ә) web-mail арқылы деректерді жіберу;

б) туннельді үй немесе басқа да сыртқы ресурстарға дейін ұйымдастыру және ол арқылы қызықты деректерді түсіру, сонымен бірге қашықтағы қосылуды іске асыру браузерлер үшін кеңейтулер түрінде қатардағы пайдаланушыларға да қол жетімді болады;

г) хабарламаларды жіберу сервистері (IM) арқылы деректерді жіберу.

DLP-шешімді кәсіпорында енгізу кезінде қорғаныс тиімділігі тәуелді бірқатар нюанстарды ескеру қажет:

а) SSL таратып жазу – DLP-шлюзді инсталляцияның міндетті элементі, бірақ барлық DLP-жүйелер осы функцияны орындай алмайды, сондықтан SSL-offload үшін жиі қосымша шешім талап етіледі;

ә) офлайн-режим саясатын пысықтау – DLP-агент белсенді сканерлеу режимінде, сондай-ақ офистік желіден тыс жұмыс істеуді жалғастыруға тиіс;

б) саясаттарды тұрақты өрнектермен ғана емес, сондай-ақ берілген үлгі-фингерпринттер (метадер файлдары ықтималдық анализі бар мәтін блоктарының хэши және т. б.);

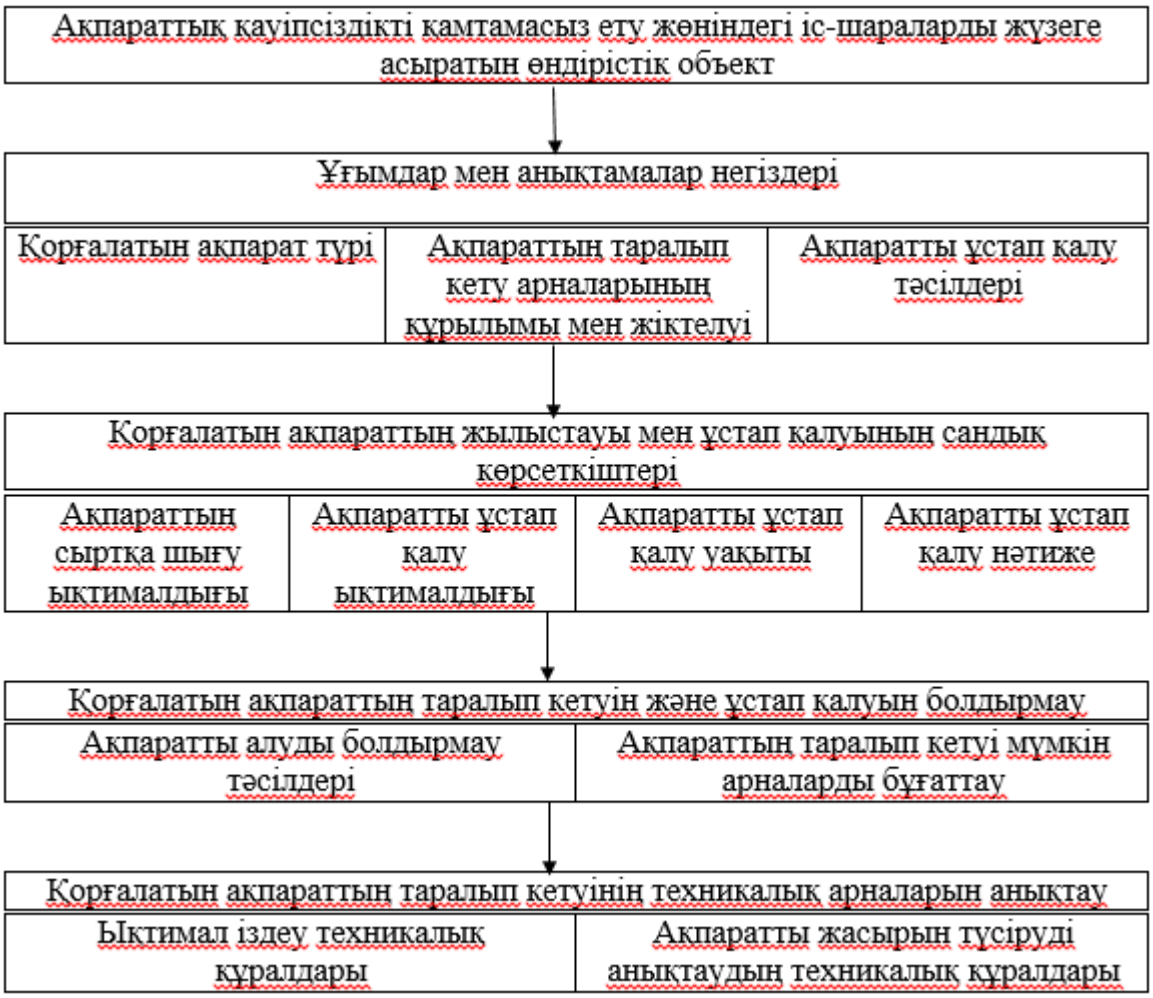
в) әр түрлі пошта агенттері мен web-браузерлерді пайдалануды шектеу, өйткені DLP агенттері бағдарламалық қамтамасыз етуді іске асырудың барлық нұсқалары үшін әзірленген емес.

ДЭЕМ ақпаратты қорғау – ДЭЕМ сақталатын және өңделетін ақпаратты бұрмалаудың алдын алатын және жайылып кету арналарының пайда болуын азайтатын, құқықтық шаралар мен амалдар (ұйымдастыру, техникалық, бағдарламалық), тәсілдерідің ұйымдастырылған жиынтығы болып табылады.

Қорғаудың ұйымдастыру шаралары – жалпы сипаттағы шаралар, ол ақпаратты өңдеудің тәсілі мен ақпараттың жайылып кету арнасының ерекшеліктеріне қарамастан бөтен тұлғалар үшін бағалы ақпаратқа қол жеткізуін қиындатады.

Қорғаудың ұйымдастырылған техникалық шаралары – жайылып кету арнасы мен ақпаратты өңдеудің тәсілімен байланысты шара, бірақ ол іске асу үшін стандартты емес жабдықтар мен тәсілдерді талап етпейді.

Қорғаудың техникалық шаралары – жайылып кету арнасымен қатаң түрде байланысты және ол іске асу үшін арнайы тәсілдер, жабдықтар мен бағдарламалық құралдарды талап етеді [4].



Сурет 1.2 – Ақпаратты ақаудан қорғау және техникалық арналар арқылы ұстап қалу мәселесінің шешімінің блок-сызбасы

Бағдарламалық вирус - бұл компьютердің қалыпты жұмыс істеуін бұзуға арналған компьютерлік бағдарлама. Вирусты қосымша кедергі ретінде қарастыруға болады, бірақ ол сақтаудағы мәліметтерге ие болатын қылмыс болып саналады. Бағдарламалы вирустар – бұлар өзін өзі қосарлау қасиетіне ие және өзінің жұмысын жасыра алатын, ДЭЕМ ақпараттарға зиян келтіретін бағдарламалар болып табылады [5].

Вирустар:

а) файлдық – іске асырылып жатқан файлдарға қосылады;

ә) жүктемелік – ДЭЕМ жүктемелік секторларында орналасады.

1.2.2 Мәліметтерді өңдеу жүйесінде ақпаратты қорғаудың ұйымдық-техникалық шаралары

Ақпаратты қорғаудың ұйымдастыру құралдарының кешенін әзірлеу қауіпсіздік қызметінің құзыретіне кіруі тиіс. Көбінесе қауіпсіздік мамандары:

а) компьютерлік техникамен және құпия ақпаратпен жұмыс істеу ережелерін белгілейтін ішкі құжаттаманы әзірлейді;

ә) қызметкерлерге нұсқаулық және мерзімді тексеру жүргізеді;

жұмыс бойынша белгілі болған мәліметтерді жария еткені немесе заңсыз пайдаланғаны үшін жауапкершілік көрсетілген еңбек шарттарына қосымша келісімдерге қол қоюға бастамашылық етеді;

б) ең маңызды деректер массивтері қызметкерлердің бірінің қарамағында болатын жағдайларды болдырмау үшін жауапкершілік аймағын шектейді;

в) құжат айналымының жалпы бағдарламаларында жұмысты ұйымдастырады және аса маңызды файлдар желілік дискілерден тыс сақталмауын қадағалайды;

г) кез келген пайдаланушының, оның ішінде ұйымның топ-менеджментінің көшіруінен немесе жоюынан деректерді қорғайтын бағдарламалық өнімдерді енгізеді;

д) кез келген себептер бойынша істен шыққан жағдайда жүйені қалпына келтіру жоспарларын жасайды.

Ұйымдастыру шаралары мыналарды қарастырады:

а) құпия ақпаратты өңдеп жатқан ғимаратқа кіруге деген рұқсатты шектеу;

ә) ДЭЕМ құпия және жасырын ақпараттарды өңдеу үшін тексерілген лауазымды тұлғаларды кіргізу;

б) магниттік тасымалдаушыларды дұрыс, берік жабылған шкафтарда сақтау;

в) бір немесе бірнеше ДЭЕМ бағалы ақпаратты өңдеу үшін орнату, кейін барлық жұмыстарды тек осы ДЭЕМ жасау;

г) дисплейді, клавиатураны және принтерді өңделетін ақпараттың мазмұнын бөгде адамдар көре алмайтындай етіп орнату;

д) бағалы ақпаратты шығаратын материалдық тасымалдаушылар мен принтерлердің жұмысын әрдайым бақылап отыру;

е) бағалы ақпараттар мен басқа да материалдарды жою;

ж) бағалы ақпаратты өңдейтін тұлғалардың оның мазмұны туралы келіссөздерді қатыстырмау.

Ақпаратты қорғаудың техникалық құралдарының тобы аппараттық және бағдарламалық құралдарды біріктіреді. Негізгі:

а) компьютерлік жүйеде деректердің аса маңызды массивтерін резервтік көшіру және қашықтан сақтау – тұрақты негізде;

ә) деректердің сақталуы үшін маңызы бар желілердің барлық кіші жүйелерін қайталау және резервтеу;

б) жеке элементтердің жұмысқа қабілеттілігі бұзылған жағдайда желі ресурстарын қайта бөлу мүмкіндігін құру;

в) резервтік электрмен қоректендіру жүйелерін пайдалану мүмкіндігін қамтамасыз ету;

г) жабдықтарды өрт немесе сумен зақымдаудан қауіпсіздікті қамтамасыз ету;

д) деректер қорын және басқа ақпаратты рұқсатсыз кіруден қорғауды қамтамасыз ететін бағдарламалық жасақтаманы орнату.

Техникалық шаралар кешеніне компьютерлік желілер объектілерінің физикалық қолжетімдігін қамтамасыз ету бойынша шаралар да кіреді, мысалы, үй-жайды камералармен және сигнализациямен жабдықтау сияқты практикалық тәсілдер.

Ұйымдық-техникалық шаралар:

а) ДЭЕМ корпус ішіне бекіту құрылғыларын орнату арқылы оған кіруді шектеу;

ә) ДЭЕМ жөндеуге жіберу кезінде, төмен деңгейдегі жоюды пайдалану көмегімен оның винчестеріндегі барлық ақпаратты жою;

б) ДЭЕМ қуаттандыруды жеке қуат көзі арқылы іске асыру немесе жалпы (қалалық) электр жүйесінен кернеудің стабилизаторы арқылы қуат-тандыру (желілік сүзгі);

в) ақпаратты көрсету үшін сұйық кристаллды немесе плазмалы дисплейлерді пайдалану, ал басып шығару үшін – бүріккіш немесе лазерлі принтерлерді пайдалану;

г) дисплейді, жүйелік блокты, клавиатура мен принтерді жарықтандыру, ауаны салқындату, байланыс, металл құбыр, телевизия және радиоаппаратура, сонымен қатар құпия емес ақпаратты пайдаланатын ДЭЕМ 2,5-3,0 метр арақашықтықта орналастыру;

д) ДЭЕМ ақпаратты өңдеген кезде оны локальді желіден және қашықтан қатынасу желісінен өшіру;

е) принтер мен клавиатураны акустикалық арнадан ақпарат жайылып кетпес үшін жұмсақ төсемеге орналастыру;

ж) ДЭЕМ бағалы ақпаратты өңдеу барысында басқа да шуыл фонын жасайтын құрылғыларды қосып қою ұсынылады (ауа салқындатқыш, желдеткіш);

и) ақпаратты қолданып болған соң оны міндетті түрде жою [5].

1.2.3 ДЭЕМ электромагниттік арна бойынша ақпараттың жайылып кетуін қоғаудын негізгі тәсілі

Жоғары сапалы электромагнитті сәулеленудің негізгі көзі ол – дисплей. Ондағы бейнені жүздеген метр арақашықтықта қабылдауға болады. Ақпараттың жойылып кетуін толықтай жою үшін шуыл генераторын қолдануға болады. Қорғаудың басқа тәсілі – плазмалы және сұйыққристалды пайдалану.

Тағы бір қорғаудың сенімді түрі ол ғимаратты жуандығы 1 мм кем емес, толықтай болат, алюминий және арнайы пластмасса табақшаларды жерге тұйықтау арқылы жасауға болады. Бұл жағдайда терезелерге ұялы сүзгіні пайдаланған жөн – мөлшері 1 см көп емес квадрат ұяшықтары бар алюминдік торды пайдалану.

Принтер электромагниттік сәулеленудің қуатты төменжиілікті көзі болып табылады, ол арақашықтық артқан сайын тез өше бастайды. Бірақ та, бұл сәулелену де қауіпті. Онымен күресу өте қиын, себебі ол күшті магниттік құрамдас бөліктен тұрады, ол нашар бейнелі және шуылданбайды.

ДЭЕМ арнайы орнатылған таратушы мен радиомаяктар өте қауіпті (бағдарламалық немесе техникалық құрал, ол жайылып кету арналарынан ақпараттың шығуын жеңілдетеді және ДЭЕМ жазылған жұмыс алгоритмін бұзады). Осы себептен бағалы ақпаратты кездейсоқ ДЭЕМ өңдеуге болмайды. Егер компьютер жөндеуге жіберілсе, онда басқа белгі жоқ екеніне көз жеткізіп алу қажет.

Сыртқы сымдардан және ДЭЕМ кабелдерінен сәулелену өте көп емес, бірақ олар ғимарат сыртынан шығатын сымдармен түйіспеуін бақылауда ұстап отыру қажет.

Бастапқы құрылғыдан жерге тұйықталу монтажын бақыланатын аудан шегінде жасау керек. Жерге тұйықталу басқа сымдармен түйіспеуін қадағалап отыру керек. ДЭЕМ сыртқы ортамен барлық байланыстарын электрлік түйін арқылы іске асырған жөн:

а) қауіпсіздіктің басты қызметтері;

ә) сәйкестендіру және теңнұсқаландыру;

б) кіруді басқару;

в) хаттамалау және аудит;

г) криптография;

д) бейнелеу.

1.2.4 Идентификация және аутентификация

Идентификация мен аутентификацияны қауіпсіздік құралдарының бағдарламалық – техникалық негізі деп атауға болады, себебі басқа қызмет көрсетулер атаулы субъектерге арналған. Идентификация мен аутентификация – қорғаныстың бірінші желісі болып табылады, ол ұйымның ақпараттық кеңістігінің кіреберісі.

Субъектіге идентификация – белгілі бір нақты қолданушы атынан, өзінің атын атап, қолданушыға және процеске өзін атауға мүмкіндік береді. Аутентификацияның арқасында екінші жақ, субъект өзін көрсетіп тұрған тұлға екеніне көз жеткізеді. Аутентификация сөзіне синоним ретінде «шынайылықты тексеру» сөзі қолданылып жүр. Субъект өзінің шынайылығын келесі бір болмысын көрсету арқылы дәлелдейді:

а) өзі білетін бір нәрсе: құпия сөз, жеке сәйкестендіру нөмері, криптографиялық кілт және т.б;

ә) өзінде бар бір нәрсе: жеке карточка немесе осыған ұқсас басқа да құрылғы;

б) өзінің бір бөлігі ретіндегі нәрсе: дауыс, саусақ таңбасы және т.б, яғни биометриялық сипаттамасы.

Сенімді идентификация мен аутентификация бірқатар себептердің кесірінен қиын болып табылады.

Біріншіден, компьютерлік жүйе ақпаратты қандай күйде алды соған негізделеді: яғни, ақпарат дереккөзі белгісіз болып қалады [6]. Қаскүнем алдыңғы ұрланған мәліметтерді қосуы мүмкін. Осылайша, идентификацияланған және аутентификацияланған ақпаратты қауіпсіз түрде енгізу және тарату үшін шаралар қолданылады; желелік ортада бұл өте қиын болады.

Екіншіден, барлық аутентификацияланған мәндерді біліп қоюға, ұрлап алуға және қолдан жасауға болады.

Үшіншіден, аутентификацияландырудың сенімділігі тұрғысынан және қолданушы мен жүйелік әкімшілік жайлылығы арасында келіспеушіліктер бар. Қауіпсіздік тұрғысынан белгілі бір жиілікте қолданушыдан аутентификацияландырудың ақпаратын қайта теруді сұрау қажет (оның орнына басқа адам отыруы мүмкін), бұл енгізу кезінде қарау мүмкіндігін арттырады.

Төртіншіден, құрылғы сенімді болған сайын, ол қымбат болады.

Сенімділік, бағасы бойынша қолжетімділік пен қолданудың ыңғайлылығы және идентификация мен аутентификация құрылғылары арасында келісім табу қажет.

Аутентификацияландырудың ең көп тараған түрі ол – құпия сөздер. Жүйе енгізілген және осы қолданушыға бұрыннан тән құпия сөзді салыстырады; егер сәйкес келсе қолданушының шынайылығы дәлелденеді. Қазіргі таңда танымал болып келе жатқан және өте тиімді болып табылатыны ол –қолданушының криптографиялық кілті.

Құпия сөз аутентификацияландырудың ең басты артықшылығы – қарапайымдылық және дағдыланғандығы. Құпия сөздер бұрыннан операциялық жүйелер мен басқа да сервистерде де бар. Құпия сөзді дұрыс пайдаланған жағдайда ол көптеген ұйымдарға қажетті деңдейдегі қауіпсіздікті қамтамасыз етеді. Бірақ та бұл сипаттамаларының жиынтығы бойынша шынайылықты тексерудің ең әлсіз түрі болып табылады. Құпия сөздің сенімділігі оларды есте сақтауда және құпия түрде сақтау болып табылады. Құпия сөзді енгізуді қарап алуға болады. Құпия сөзді теру арқылы білуге болады. Егер құпия сөздің файлы шифрленген болса, бірақ оқуға мүмкін болса, оны өз компьютеріңе жүктеп алып, теруді толықтай бағдарламалап, құпия сөзді табуға болады [6].

Құпия сөздер электрондық қағып алу тұрғысынан әлсіз болып тұр – бұл оның ең негізгі кемшілігі, оны администрациялауды және қолданушыларды оқыту арқылы жақсарту мүмкін емес. Шығудың бір ғана жолы бар – байланыс

желісімен жібер алдында құпия сөзді шифрлеу үшін криптографияны пайдалану немесе оны мүлде жібермеу.

Бірақ та келесі шаралар құпия сөз арқылы қорғаудың сенімділігін біршама арттырады:

а) техникалық шектеулер орнату (құпия сөз қысқа болмауы тиіс, ол әріптерден, сандардан, тыныс белгілері мен т.б тұруы қажет);

ә) құпия сөзді мерзім бойынша басқару, оларды мерзімді түрде ауыстыру;

б) құпия сөз файлына қолжетімділікті шектеу;

в) жүйеге кіру үшін сәтсіз енгізулерді шектеу, терудің әдісін қиындатады; қолданушыларды оқыту және тәрбиелеу.

Құпия сөздің бағдарламалық генераторын пайдалану, ол қиын емес ережелерге негізделе отырып, дұрыс және есте қалатын құпия сөздерді тудырады.

Биометриялық сипаттарды басқару құрылғысы өте қиын және арзан емес, сондықтан да олар қауіпсіздік шарасын жоғары деңгейде талап етілетін ұйымдарда ғана қолданылады.

Идентификация мен аутентификация қызметінің ең маңызды және қиын міндеті ол – әкімшілдендіру [6]. Әрдайым құпиялылықты, тұтастықты және қажетті ақпаратқа қолжетімділікті қамтамасыз ету қажет, бұл желілік әртекті ортада өте қиын болып табылады. Автоматтандырумен қатар, ақпаратты максималды түрде орталықтандыруды қолданған жөн. Олардың әрқайсысы деректерді тоқтатуы, немесе бірден «екінші жаққа» жібере алады. Бұған қол жеткізу үшін шынайылықты тексерудің белгіленген серверлері немесе орталықтандырылған әкімшілік құрылғыларын пайдалануға болады. Кейбір операциялық жүйелер желілік сервистерді ұсынады, олар әкімшілік мәліметтерінің орталықтандырылған негізі болып табылады.

Орталықтандыру тек жүйелік әкімшілік жұмысын жеңілдетпейді, ол қолданушылардың да жұмысын жеңілдетеді. Себебі бірегей кірудің маңызды концепциясын іске асыруға мүмкіндік береді. Шынайылықты тексеруден бір рет өтіп, қолданушы өзінің өкілеттігі шеңберінде желідегі барлық ресурстарға қол жеткізе алады.

1.2.5 Қолжетімділікті басқару

Дәстүрлі тұрғыдан қатынауды басқару құралдары субъектілер (пайдаланушылар мен процестер) объектілерге (ақпаратқа және басқа да компьютерлік ресурстарға) орындай алатын іс-әрекеттерді сипаттауға және бақылауға мүмкіндік береді. Бұл бөлімде сөз физикалық ерекшелікке қарағанда бағдарламалық құралдармен іске асырылатын қолжетімділікті логикалық басқару туралы болып отыр. Қол жетімділікті логикалық басқару – бұл объектілердің құпиялылығы мен тұтастығын қамтамасыз етуге арналған көп пайдаланушылық жүйелердің негізгі механизмі және кейбір дәрежеде олардың қол жетімділігі (авторланбаған пайдаланушыларға қызмет көрсетуге тыйым салу арқылы).

Дәстүрлі түсіндіруде есептің формалды қойылымын қарастырайық. Субъектілердің жиынтығы және объектілер жиынтығы бар. Қолжетімділікті логикалық басқару міндеті әрбір жұп үшін "субъект-объект" рұқсат етілген операциялардың (кейбір қосымша шарттардан тәуелді болуы мүмкін) көптігін анықтау және белгіленген тәртіптің орындалуын бақылау болып табылады.

Қолжетімділікті логикалық басқару тақырыбы – ақпараттық қауіпсіздік саласындағы ең күрделі тақырып. Себебі, ұғымы объектінің (көп түрлерінің қолжетімділігі) өзгеріп отырады сервис – сервисі. Операциялық жүйе үшін нысандарға файлдар, құрылғылар және процестер жатады. Файлдар мен құрылғыларға қатысты әдетте оқу, жазу, орындау (бағдарламалық файлдар үшін), кейде жою және қосу құқықтары қарастырылады. Жеке құқық басқа субъектілерге (иелену құқығы деп аталатын) қол жеткізу өкілеттігін беру мүмкіндігі болуы мүмкін. Процестерді құруға және жоюға болады. Қазіргі операциялық жүйелер басқа да объектілерді қолдай алады.

Бұл жағдайда, егер бұл мәліметтер базаларын басқару жүйесі үшін объект – деректер базасы, кесте, көрініс, сақтау процедурасы. Кестелерге деректерді іздеу, қосу, түрлендіру және жою операциялары, басқа нысандардағы басқа қол жеткізу түрлері қолданылады. Қолжетімділік құқығын басқару бағдарламалық ортаның әр түрлі компоненттерімен жүзеге асырылады – операциялық жүйенің ядросы, қауіпсіздіктің қосымша құрылғылары, мәліметтер базасын басқару жүйесі және т.б.

Объектілер мен оларға қолданылатын операциялардың әртүрлілігі қолжетімділікті логикалық басқарудың принципті орталықсыздандырылуына алып келеді. Әрбір сервис нақты субъектіге қандай да бір операция жасауға мүмкіндік бере ме? Теориялық тұрғыдан бұл заманауи объектілі-бағытталған тәсілмен келісіледі, іс жүзінде елеулі қиындықтарға алып келеді. Басты мәселе - көптеген объектілерге түрлі сервистер көмегімен қол жеткізуге болады(кейбір техникалық қиындықтарды еңсеру керек болуы мүмкін). Мысалы, реляциялық кестелерге дейін ДББЖ құралдарымен ғана емес, сонымен қатар операциялық жүйе қолдайтын файлдарды немесе дискілік бөлімдерді тікелей оқу арқылы (деректер қоры объектілерін сақтау құрылымында алдын ала бөлшектеліп) жетуге болады. Нәтижесінде қол жеткізу матрицасын беру кезінде әрбір сервис үшін артықшылықтарды бөлу принципін ғана емес, сервистер арасындағы қолданыстағы байланыстарды да назарға алу қажет (матрицаның әр түрлі бөліктерінің келісімділігіне қамқорлық жасауға тура келеді). Осыған ұқсас қиындық деректерді экспорттау/импорттау кезінде туындайды, ол кезде қол жеткізу құқықтары туралы ақпарат, әдетте жоғалады (себебі жаңа сервисте мағынасы жоқ). Демек, әртүрлі сервистер арасындағы деректер алмасу қолжетімділікті басқару тұрғысынан ерекше қауіп төндіреді, ал әр текті конфигурацияны жобалау және іске асыру кезінде субъектілердің объектілерге қол жеткізу құқықтарын келісілген бөлу туралы және деректерді экспорттау/импорттау тәсілдерінің санын азайту туралы қамқорлық жасау қажет.

Қолжетімділікке рұқсат беру шешімін қабылдау кезінде келесі ақпараттар талданады:

а) субъект сәйкестендіргіші (қолданушы сәйкестендіргіші, компьтердің желілік мекен жайы). Мұндай сәйкестендіргіштер қолжетімділіктің еркін басқаруының негізі болып табылады;

ә) субъект атрибуттары (қауіпсіздік таңбасы, қолданушылар тобы). Қауіпсіздік белгілері – қолжетімділікті басқарудың мәжбүрлі негізі:

1) әрекет орны (жүйелік консоль, желінің сенімді түйіні);

2) әрекет уақыты (көптеген әрекеттерді жұмыс уақыты кезінде жасаған жөн);

3) сервистің ішкі шектеулері (бағдарламалық өнімге лицензия бойынша қолданушылар саны);

4) қолжетімділікті логикалық басқару құрылғыларын оңтайлы қондырмасы шектеуші интерфейс болып табылады, яғни қолданушыға көрінетін объектілер қатарына оған рұқсат етілгендерді ғана қосып, рұқсатсыз әрекет жасау мүмкіндігінен айыру [7].

1.2.6 Хаттамалау және аудит

Хаттамалау дегеніміз кәсіпорынның ақпараттық жүйесінде болып жатқан жағдайлар туралы ақпаратты жинау және сақтау. Әр сервисте мүмкін болатын жағдайлардың өз жиынтығы бар, бірақ та оларды сыртқы – басқа сервистердің әсерінен, ішкі – сервистің өзі және клиенттік – қолданушы немесе әкімшілік әрекетінен болған жағдайларды айтады.

Хаттамамен кәсіпорынның ақпараттық жүйесінде болып жатқан оқиғалар туралы ақпарат жинау және жинақтау болып табылады. Әрбір сервистің ықтимал оқиғалар жиынтығы бар, бірақ кез келген жағдайда оларды сыртқы (басқа сервистердің әрекеттерінен туындаған), ішкі (сервистің өзінің әрекеттерінен туындаған) және клиенттік (пайдаланушылар мен әкімшілердің әрекеттерінен туындаған) бөлуге болады. Тіркелетін оқиғалар қатарына жатады:

- жүйеге кіру;
- жүйеден шығу;
- қашықтағы жүйелерге жүгіну;
- файлдармен операциялар;
- артықшылықтарды немесе қауіпсіздіктің өзге де атрибуттарын ауыстыру.

Ықтимал тіркеуге жататын оқиғалардың толық тізбесі жүйенің ерекшелігіне және таңдалған қауіпсіздік саясатына байланысты.

Тіркелу керек ақпараттар мыналар:

- күні мен уақыты;
- Пайдаланушының ID;
- оқиға түрі (кіру, шығу);
- әрекет нәтижесі (табыс немесе сәтсіздік);
- сұрау салу көзі;

- қозғалған нысандардың атаулары;
- қорғау ДБ-ға өзгерістер жазу;
- қауіпсіздік белгілері.

Бұл жиналған ақпаратты талдау, ол нақты уақытты тез және мерзімді түрде іске асырылады. Аудит – бұл нақты уақытта немесе мезгіл (мысалы, күніне бір рет) жедел (дерлік) жүргізілетін жинақталған ақпаратты талдау.

Хаттамалау мен аудитті іске асыру барысында келесі мақсаттар алға қойылады:

- қолданушылар мен әкімшіліктің есеп берушілігін қамтамасыз ету;
- оқиғалар жүйелілігін реттеу мүмкіндігін қамтамасыз ету;
- ақпараттық қауіпсіздіктің бұзылу әрекетін анықтау;
- мәселелерді анықтау және талдау үшін ақпаратпен қамтамасыз ету.

Есеп берушілікті қамтамасыз ету біріншіден, тежеу құралы ретінде маңызды. Егер қолданушылар мен әкімшілік олардың әрекеті назарда екенін білсе, онда олар заңсыз операцияларға бармауы мүмкін. Егер бір қолданушыны заңсыз әрекетке барды деп есептесе, оның әрекетін толықтай, тіпті әр клавишті басқанына дейін тіркеу қажет. Сонымен қатар мұнда қауіпсіздік режимін бұзуды тергеу ғана емес, дұрыс емес өзгертулерді де қайтаруға болады. Осылайша, ақпараттық тұтастығы қамтамасыз етіледі.

Оқиғалар ретін қайта жөндеу қоғау сервисіндегі әлсіз тұстарды анықтау, басып кірудің кінәлі тұлғасы, келтірілген шығын көлемін анықтауға көмектесіп, қайта қалыпты жұмысқа оралуға көмек береді.

Хаттамалау мен аудиттің тағы бір ерекшелігі – басқа қауіпсіздік құралдарына тәуелділік. Идентификация және аутентификация пайдаланушылардың есеп беру нүктесі болып табылады, қолжетімділікті логикалық басқару тіркеу ақпаратының құпиялылығы мен тұтастығын қорғайды. Қорғау үшін криптографиялық әдістер де тартылуы мүмкін.

1.2.7 Криптография

Адам тарихында қандай да бір ақпаратты шифрлеу қажеттілігін бастан кешірді. Бұл қажеттіліктен бүкіл ғылым – криптография өсті. Егер бұрын криптография көбінесе мемлекеттік мүдделерге қызмет етсе, интернет арқылы оның әдістері жеке тұлғалардың игілігіне айналды және хакерлер, ақпарат бостандығы үшін күресушілер және желіде өз деректерін шифрлеуге ниет білдірген кез келген тұлғалар кеңінен пайдаланады. Криптография тарихының дамуы 4 мың жыл шамасында. Криптографияны кезеңдеудің негізгі өлшемі ретінде қолданылатын шифрлау әдістерінің технологиялық сипаттамаларын пайдалануға болады.

Қолжетімді Интернеттің пайда болуы криптографияны жаңа деңгейге көтерді. Криптографиялық әдістерді жеке тұлғалар электрондық коммерциялық операцияларда, телекоммуникацияларда және басқа да көптеген орталарда кеңінен қолдана бастады. Ақпараттың құпиялылығы мен тұтастығын басқарудағы ең қуатты құрылғылардың бірі – криптография [7]. Көп жағдайда ол қауіпсіздіктің техника-бағдарламалық реттегіштері арасында

орталық негіз болып табылады, ол іске асырудың, сонымен қатар ең соңғы қорғау межесі болады. Бұл ғылым екі бөлікке бөлінді: криптосинтез және криптоанализ. Криптосинтез ақпаратты қорғауды қамтамасыз етті, ал криптоанализ жүйені бұзу жолдарын іздейді. Бұрын айтылғандай, криптографияда кейбір әдістер анықталған. Оларды тиісті алгоритмдерде пайдаланылатын кілттердің санына байланысты бөлуге болады:

- екікілтті;
- біркілтті;
- кілтсіз.

Екі кілтті алгоритмдерде екі кілт қолданылады: ашық және құпия. Бір жақ кілтте қарапайым құпия кілт қолданылады. Және шексіз алгоритмде қандай да бір кілттер мүлдем пайдаланылмайды.

Сондай-ақ, басқа криптографиялық әдістерді де атап өткен жөн:

а) алгоритм кілттердің екі түрін қолданатын электрондық қолтаңба: құпия және ашық. Деректер мен авторлықтың тұтастығын растау үшін қолданылады.

ә) аутентификация. Бұл әдіс пайдаланушы өзі үшін кім екенін анықтауға мүмкіндік береді.

б) криптографиялық бақылау жиынтығының әдістері:

1) имитоприставкаларды есептеу;
2) кілтті және кілтті емес хеширлеу;
3) хабарларды аутентификациялау кодтарын қолдану.

Бұл әдістердің барлығы электрондық қолтаңбаны және әр түрлі аутентификация сұлбаларын пайдалану мүмкін болмаған кезде деректерді қорғауда қолданылады.

в) Кездейсоқ және жалған кездейсоқ генераторлар криптографияда, атап айтқанда:

1) құпия кілттерді генерациялау үшін;
2) электрондық қолтаңба алгоритмдерінің көпшілігінде;
3) аутентификация схемаларының көпшілігінде қолданылады.

1.3 суреттегідей шифрлау алгоритмдерін екі санатқа бөлуге болады:

а) асимметриялық шифрлау алгоритмдері;

ә) симметриялық шифрлау алгоритмдері.

Симметриялы шифрлау алгоритмінде әдетте деректерді шифрлаған сол кілт қолданылады немесе негізгі кілтпен қарапайым қатынаспен байланысты басқа кілтті қолданады. Симметриялық шифрлеудің тиімді әдістері бар. Бұндай әдістердің стандарттары мынадай: “МЕМСТ 28147-89”. Ақпаратты өңдеу жүйесі. Криптографиялық қорғау. Криптографиялық түрлендірудің алогоримті.

Ал ассиметриялық шифрлау алгоритмінде К1 шифрлау кілті қолданылады, ол кері есептеу мүмкін емес, осылайша К2 кілтінен оңай есептеледі. Олардың біреуі құпия емес, ол шифрлеу үшін қолданылады және

қолданушының мекен жайымен бірге айтылады, екіншісі –құпия, ол қайта шифрлеу үшін қолданылады және тек қабылдап алушыға белгілі. Ең атақты ассиметриялы тәсіл ол RSA (Райвест, Шамир, Адлеман), ол қарапайым үлкен сандар мен олардың туындысы негізінде жасалған [8].

Шифрлеудің ассиметриялық әдісі электрондық қолды іске асыруға мүмкіндік береді, немесе хабарламаның электрондық растамасы. Оның мәні жіберуші хабарламаның екі нұсқасын жібереді – ашық және құпия кілті бар дешифрленеген (әрине, шифрленбеген хабарламаның дешифровкасының шифрлеу формасы бар). Қабылдап алушы жіберушінің ашық кілті арқылы дешифрленген нүсқаны шифрлеп, ашықпен салыстыра алады. Егер олар сәйкес келсе, жіберушінің қолы мен тұлғасын анықталды деп есептеуге болады.

Асимметриялық тәсілдің кемшілігі олардың төмен тез әрекет етуі, сондықтан да оларды симметриялықпен үйлестіруге тура келеді, ескере кеткен жөн, асимметриялық әдістер симметриялыққа қарағанда баяу. Олардың әрқайсысы деректерді тоқтатуы, немесе бірден «екінші жаққа» жібере алады. Кілтті тарату үшін хабарламаны алдымен кездейсоқ кілтпен симметриялы шифрлейді, кейін сол кілтті қабылдаушының ашық асимметриялы кілтімен шифрлеп, кейін хабарламаны және кілтті желі арқылы жібереді.

Соңғы кездері симметриялық шифрлеудің әртүрлісін пайдалану белең алды, олар құрамдық кілтті пайдалану негізінде жасалады. Оның мәнісі, құпия кілт екі бөлшекке бөлінеді, бірақ ол жеке сақталады. Әр бөлігі өздігінен қайта шифрлеуді болдырмайды. Егер құқық қорғау органдарында бір кілтті пайдаланатын белгілі бір тұлғаға байланысты күдік туса, олар кілттің бір бөлігін алып, ары қарай симметриялық қайта шифрлеуге тән нұсқада әрекеттерін жалғастырады.

Криптографияның болашақ міндеттерінің бірі-жоғары деңгейде құпиялы шифрлаудың жылдам әдістерін әзірлеу. Бұл мәселе байланыс арналарының көп санына байланысты (сымсыз желілер, ұялы байланыс), олар бойынша ақпараттың үлкен көлемі беріледі [9].

1.2.8 Бейнелеу

Бейне – бұл клиенттердің бір жиынтықтан басқа жиынтықтағы серверге кіруге рұқсатты шектейтін құрал. Бейне өз функцияларын, жүйенің екі жиынтықтарының арасындағы ақпараттық ағынды бақылау арқылы орындайды.

Қарапайым жағдайда бейне біреуі деректердің жылжуын шектейтін, екінщісі керісінше оған мүмкіндік беретін екі механизмнен тұрады. Жалпы жағдайда бейне немесе шала өткізгіш қабықты сүзгіштің жүйелілігі ретінде көрсеткен ыңғайлы. Олардың әрқайсысы деректерді тоқтатуы, немесе бірден «екінші жаққа» жібере алады. Сонымен қатар, талдауды жалғастыру үшін деректер бөліктерін келесі сүзгішке жіберу немесе адресат атынан деректерді өңдеуге және жіберушіге нәтижелерді қайтаруға жол беріледі.

Бейнелеу кіруге рұқсатты шектеу функциясынан басқа ақпараттық алмасуды хаттамалауды жүзеге асырады.

Әдетте бейне симметриялы болмайды, ол үшін «ішінде» және «сыртында» ұғымдары анықталған. Сонымен бірге, бейнелеудің міндеті ішкі ауданды сыртқы әлеуетті қастықтан қорғау болып табылады. Осылай, желі арасындағы бейнелерді Internet сияқты ашық ортаға шығуға ие ұйымның жергілікті торабын қорғау үшін орнатады. Бейненің басқа қарастыруы – басқа жүйелік қорғаныс құралдарына тәуелсіз компьютердің байланыс портына кіру рұқсатына дейін және кейін бақылайтын портты қорғайтын құрал. Бейнелеу сонымен қатар, құпиялылық режимін қолдауға жағдай жасайды, сыртқы ауданға бағытталған ақпараттық ағындарды бақылауға мүмкіндік береді.

Кез келген ұйымда локальді желіні қолданушылардың бәріне білуге тиісті емес құжаттар мен мәліметтер болады. мұндай ақпарат кіруге рұқсаты уәкілетті тұлғаларда ғана арнайы тізімдемеде сақталуы тиіс. Желіде қорғаныс жүйесін орнатудың себептерінің бірі желілік ақпаратты қолданушылардың ойластырылмаған әрекеттерінен сақтау болып табылады.

1.3 Локальді желелердегі ақпаратты қорғаудың негізгі бағыттары

1.3.1 ДЭЕМ тікелей қорғау шаралары

ЭЕМ жан-жақты қорғау тәсілінің маңызды аспектісі есептеуіш құрылғыларды тікелей қауіптен қорғау шаралары болып табылады [9]. Оларды екі категорияға бөлуге болады:

а) табиғи апаттан қорғау шаралары;

ә) зиянкестерден қорғау шаралары.

Табиғи апаттардың ішінде ең қауіпті деп өртті санауға болады. қарапайым өрттік нормаларды сақтау бұл мәселені шеше алады. Ең маңызды және қызықты екінші пункт.

Компьютерді зиянкестерден қорғау, демек ақпаратты қорғау үшін есептеуіш жүйеге тікелей кіру рұқсатын шектеу қажет. Ол үшін есептеуіш кешеннің күзетуін ұйымдастыру керек. Күзету шараларының төрт түрін көрсетуге болады:

а) аудан шекарасын күзету (кейбір аумақтарды, төңіректегі ғимараттарды);

ә) ғимараттың өзін немесе оның айналасындағы кейбір кеңістікті күзету;

б) ғимаратқа кіруді күзету;

в) сыни аумақты күзету.

Аудан шекарасын қорғау үшін дуалдарды, инфрақызыл немесе АЖЖ-детекторларды, қозғалыс құрылғысын сонымен қатар тұйықталған телевизиялық жүйелерді қолдануға болады.

Ғимаратты қорғау үшін ғимараттың темірбетоннан жасалынған, қалыңдығы 30-35 см кем емес қалың қабырғасы болуы тиіс.

Ғимаратқа кіруді қорғау кезінде ғимаратқа кірудің барлық мүмкін болатын жолдарын – әдетте қолданатын кірулер мен терезелерді және желдеткіш саңылауларды күзету қажет.

Әдеттегі кірулерді күзетшімен кірушіні танумен немесе кейбір механизмдерді қарастыруы, кілттерді немесе арнайы карточкаларды қолдану арқылы бақылауға болады.

Сыни аумаққа зиянкестердің енуін анықтау үшін дабылдағыш жүйелерін қолдануға болады. фотометриялық жүйелер жарықтылық деңгейінің өзгеруін анықтайды. Дыбыстық, ультрадыбысты немесе АЖЖ – объекттердің жылжуын анықтайтын жүйелері қозғалыстағы денеден шағылған дабыл жиілігінің өзгеруін сезеді. Дыбыстық және сейсмикалық (дабылдық) жүйелер шу мен дабылды анықтайды. Қорғалып жатқан объектіге жақындауды сезетін жүйелер электромагниттік немесе электростатикалық өріс құрылымының бұзылуын анықтайды.

1.3.2 Сәйкестендіру мен жеке басын анықтау

Аппараттық құралдарды немесе математикалық жасақтаманы қолданатын кіру рұқсатын шектейтін барлық механизмдердің жұмыс істеуі, қолданушы нақты бір түр иесі болып табылатындықтан және тұспалдауға негізделгендіктен, оның дұрыстығын анықтайтын бір механизм болуы тиіс. Бұл механизм осы қоланушы білетін немесе қолында бар, немесе қолданушының кейбір ерекшеліктерін анықтайтын айқындауларға негізделуі мүмкін.

Құлыптарды және электрлік немесе механикалық батырмалық жүйелерде таңбалар комбинациясын теру қолданылады. ЭЕМ кіру рұқсатын реттейтін мұндай жүйе құпиясөз жүйесі деп аталады. Бұл жүйенің кемшілігі құпиясөздің ұрлануы (қолданушы мұны байқамауы да мүмкін), ұмытылуы немесе жіберілуі болып табылады. Құпиясөзді ұрлауға қатысты қауіпті азайту үшін, оны жиі ауыстырылуы керек, ал ол құпиясөзді қалыптастыру мен үлестіру мәселелерін тудырады. «Қол алысу» деп аталатын ұқсас тәсіл жүйеге кіру рұқсатының жағдайы ретінде кейбір алгоритмнің ойдағыдай орындалуын қарастырады. «Қол алысу» үрдісінде қолданушы құпиясөз реттілігі алгоритмімен алмасуы қажет (олар дұрыс және дұрыс ретпен айтылуы тиіс), бірақ қолданушының өзі алгоритмді білмейді. Құпиясөз көмегімен дәлелдігін анықтау өзінің жеңілдігі есебінен есептеуіш жүйелерде кеңінен қолданылады.

Қолданушы өзімен бірге оған қарастыруы, оптикалық, магниттік немесе басқа кодты енгізумен, стандартты кілтті немесе арнайы карточканы алып жүруі мүмкін.

Қолданушының қолтаңбасын немесе жазу үлгісін зерттеуге негізделген таңба жүйелері құрастырылған. Жеке басын анықтау үшін қолданушы қолының геометрикалық сипаттамаларын немесе дауыс спектрограммын қолданатын жүйелер бар. Сонымен қатар, қолданушылардың саусақ іздерін сақталынған үлгілермен салыстыратын жүйелер де бар.

1.3.3 Электрондық және электромагниттік қағып алуға қарсы қорғау

Байланыс желісіне қосылу екі тәсілмен жүзеге асуы мүмкін. Пассивті қосылу кезінде зиянкес жіберілетін деректерді тыңдай алады, ал активті қосылу кезінде өзінің деректерін жіберіліп жатқан деректердің соңында

жібереді немесе орнына жібереді. Байланыс желісіне қосылудың қарсы әрекетінің негізгі шарасы хабарламаларды шифрлау болып табылады. Бұдан басқа, деректерді жіберу желісіне жеңіл қосылудың жалғыз орны жіберуші немесе қабылдаушы құрылғы орналасқан ғимарат ішіндегі орын болып табылатындықтан, деректерді жіберу желілері мен кабель шкафы сенімді қорғалуы тиіс. Байланыс желілерінің сыртқы аудандарына қосылу тығыздауыштың жоғары деңгейімен деректерді жіберуді талап ететіндіктен, аз тиімді және қымбат операция болып табылады.

Нақты қауіп ЭЕМ немесе терминалдан электрмагниттік сәулеленуді ұрлау болып таыблады. Мультибағдарламалау режимін қолдану салдарынан, бір уақытта қолданушылардың бірнеше міндеттері өңделгенде, мұндай жолмен есептеуіш жүйелерден алынған деректер қиын дешифрленеді. Бірақ, терминалдарды әсіресе, 6 м қашықтық шегінде тыңдау мүмкін болып табылады. Бұл операцияны орындаудың қиындығы қашықтықпен артады, сондықтан 45 м асатын қашықтықтан тыңдау қымбат операция болып табылады. Қымбаттырақ аппаратураны қолдану кезінде әлсіз дабылды күшейтуге де болады. Қарастыруы, ЭСА көптеген терминалдар бейнеленген ақпаратты уақыттың қысқа аралығы арқылы қалпына келтіреді. Сондықтан, қиын тәсілдерді қолданып, бірнеше циклдардың деректерін өңдеп, қолдануға болады.

1.3.4 Компьютерлік жүйелер қауіпсіздігінің негізгі ұғымдары

Ақпараттың қауіпсіздігі астарынан есептеуіш техника немесе автоматтандырылған жүйелермен өңделетін ақпараттың сыртқы және ішкі қауіптерден қорғалу жағдайы түсіндіріледі.

Бүтіндік астарынан есептеуіш техника мен автоматтандырылған жүйе құралдарының кездейсоқ бұрмалану мен бүліну қаупі жағдайында ақпаратты сапасы мен түрінің өзгермеуін қамтамасыз ету қасиеті түсіндіріледі [8]. Ресейдің Мемлекеттік техкомиссияның «Ақпаратты рұқсат етілмеген қол жеткізуден қорғау. Терминдері мен анықтамалары» жетекшілік құжатына сәйкес қауіпсіздік және бүтінділік қауіптері өңделіп жатқан жүйеге және ақпараттың бүтінділігі мен қауіпсіздігіне тікелей немесе жанама зиян келтіре алатын, есептеуіш жүйеге мүмкін болатын әсерден тұрады.

Ақпарат бүтінділігінің зақымы оның сапасының немесе түрінің бұзылуына алып келетін өзгертулерден тұрады.

Қауіпсіздік зақымы есептеуіш жүйеде болатын ақпараттың қорғалу жағдайын есептеуіш жүйенің объектеріне рұқсат етілмеген қол жеткізу жолы арқылы бұзуды айтады.

Рұқсат етілмеген қол жеткізу есептеуіш жүйелермен ұсынылатын, штатты құралдарды қолдану арқылы кіруге рұқсатты шектеу ережелерін бұзатын ақпаратқа кіру рұқсаты болып табылады. Рұқсат етілмеген қол жеткізуге жеңіл анықтама беруге болады: рұқсат етілмеген қол жеткізу қолданушымен немесе бағдарламамен қауіпсіздік саясаты жүйесінде рұқсаты жоқ объектке кіру рұқсатын алу болып табылады.

Қауіпті жүзеге асыру шабуыл деп аталады. Қауіпті жүзеге асыруға тырысатын адам бұзушы немесе зиянкес деп аталады. Жүйеге әсер ету сипаты мен қағидаларына, қолданылатын құралдарына, шабуыл мақсатына және т.б. байланысты көптеген классификация түрі бар. Әсер ету құралдарына байланысты есептеуіш жүйелердің қауіпсіздік қатерлерінің жалпы классификациясын қарастырайық. Бұл көзқарас бойынша барлық қатерлер келесідей класстардың біреуіне жатуы мүмкін (1.4 сурет):

Есептеуіш жүйе жұмысына адамның араласуы. Бұл классқа есептеуіш жүйенің қауіпсіздігін бұзатын ұйымдастырушылық құралдар (ақпарат иелерін ұрлау, ақпаратты өңдеу мен сақтау құрылғыларына рұқсат етілмеген қол жеткізу, жабдықты бұзу) және бұзушының есептеуіш жүйенің бағдарламалық компоненттеріне рұқсат етілмеген қол жеткізуі (есептеуіш жүйелерге рұқсатсыз кірудің барлық тәсілдері, сонымен қатар қолданушы-бұзушымен есептеуіш жүйелердің компоненттеріне заңсыз кіру рұқсатын алу тәсілдері) жатады. Мұндай қауіптерге қарсы тұратын шаралар ұйымдастырушылық сипатта болады (күзет, есептеуіш жүйелер жабдықтарына кіру рұқсатының режимдері), сонымен қатар олар кіру рұқсатын шектеудің жетілдірілген жүйелерін және шабуыл әрекеттерін анықтау жүйелерін (құпиясөзді табу әрекеті) құрайды.

Есептеуіш жүйе жұмысына аппаратты-техникалық араласу. Бұл техникалық құралдардың көмегімен есептеуіш жүйедегі қауіпсіздіктің және жалпы ақпараттың бұзылуы, қарастыруы, есептеуіш жүйе құрылғысының лектрмагниттік сәулеленуі арқылы ақпаратты алу, ақпаратты жіберу арналарына электромагниттік әсер ету және басқа тәсілдер. Мұндай қатерлерлер қорғану, ұйымдастырушылық шараларынан басқа сәйкес болатын аппаратты (аппаратура сәулеленуін бейнедау, тыңдаудан ақпаратты жіберу арналарын қорғау) және бағдарламалық шаралар (байланыс арналарында хабарламаларды шифрлау).

Бағдарламалық құралдар арқылы есептеуіш жүйелердің бағдарламалық компоненттеріне бұзушы әсері. Мұндай құралдар бұзушы бағдарламалық құралдар деп аталады. Оларға компьютерлік вирус, троян аты (немесе «бетбелгілер»), локальді және жаһандық желілерді қолданып, қашықтағы жүйелерге өту құралдары жатады. Мұндай шабуылдардан қорғану құралдары бағдарламалық және аппараттық қорғау жүйелерінен тұрады [10].

1.3.5 Ақпараттық қауіпсіздігінің қазіргі бағдарламалық қатерлері

Бұзушы бағдарламалық құралдардың (ББҚ) классы компьютерлік вирусты, троян аты (немесе «бетбелгілер»), локальді және жаһандық желілерді қолданып, қашықтағы жүйелерге өту құралдарын құрайды (1.3 Сурет).

Компьютерлік вирус – бағдарламалар тірі организмге тән, әрі ажырамастай пайда болады, көбейеді, өледі, қасиеттерге ие болады. Вирустар болуының басты шарты – есептеуіш жүйелерде ақпаратты әмбебап түсіндіру. Вирус бағдарламаға жұғу үрдісінде оны деректер сияқты, ал орындау

үрдісінде орындалатын код ретінде түсіндіруі мүмкін. Бұл қағида Фон Нейман архитектурасын қоланатын барлық заманауи компьютерлік жүйелердің негізіне салынған.

Сурет 1.3 – Бұзушы бағдарламалық құралдардың түрлері

«Компьютерлік вирус» анықтамасына формальді анықтама беру жеңіл емес. Ф. Коэнмен берілген дәстүрлі анықтама «компьютерлік вирус – басқа бағдарламаларды өзінің, мүмкін өзгертілген көшірмесін қосу арқылы түрлендіріп, жұқтыратын бағдарлама», анықтамадағы негізгі ұғым өздігінен көбею қасиеті болып табылады, бұл вирус – бағдарламаларды басқа бағдарламалардан ажырататын жалғыз белгі. Сонымен бірге вирустың «көшірмелері» шынымен құрылымдық және функционалдық бір бірінен ерекшеленуі мүмкін.

Қазіргі жағдай екі сәтпен сипатталады: полиморфизмдік вирустардың және вирустар генераторларының (конструкторларының) пайда болуы.

Полиморфизмдік вирустар вирустың әрбір жаңа көшірмесі өзінің тудырушысымен ортақ ештеңесі болмаған соң, оларды анықтау үшін әдеттегі іздеу алгоримдері қолданылмайтындығымен сипатталады. Бұл өзінің әр данасында тұрақты бірде бір биті болмайтын шифрды айырып оқушы мен вирус денесін шифрлау арқылы жүзеге асады. Вирус генераторларының пайда болуы, генератор-бағдарламаға кіру парамертлері ретінде тарату тәсілін, түрін, тудыратын әсерді енгізіп, жаңа вирустың ассемблер мәтінін алуға мүмкіндік береді. Вирустар үнемі өзінің «өмір сүру ортасын» кеңейтіп, енгізу мен жүрісінің жаңа алгоритмдерін іске асырады.

Трояндық ат – бұл істен шығудың кейбір жағдайдары пайда болғанда активтендірілетін, өзінде біраз бұзушы функциясын құрайтын бағдарлама. Әдетте мұндай бағдарламалар кейбір пайдалы утилиталарда жасырынады. Трояндық аттар қауіпсіздікті бұзатын және бүлдіргіш әрекеттермен байланысты функцияларды жүзеге асыратын бағдарламалар болып табылады. Мұндай бағдарламаларды вирустарды таратуды жеңілдету мақсатында

жасалынған жағдайларда кездеседі. Әдетте олар ойын немесе көңіл көтеру бағдарламаларында жасырынып, әдемі суреттер мен музыка астарынан қауіп төндіреді.

Бағдарламалық бетбелгілерде есептеуіш жүйеге қауіп төндіретін біраз функцияларға ие, бірақ бұл функция керісінше байқаусыз болуға тырысады, себебі, бағдарлама неғұрлым ұзағырақ күдік тудырмаса, соғұрлым ұзақ бетбелгі жұмыс жасайды.

Қарастыру ретінде, трояндық ат пен бағдарламалық бетбелгілермен іске асатын, мүмкін болатын бүлдіргіш функцияларды келтірейік:

а) ақпаратты жою;

ә) ақпаратты алу мен жіберу;

б) бағдарлама кодын мақсатты түрлендіру.

Егер вирустар мен трояндық аттар көшкін тәрізді өзіндік көбею немесе бұзу арқылы қауіп төндірсе, онда компьютерлік желіде іске асатын бұзушы бағдарламалық құралдардың негізгі функциясы – шабуылшы жүйені бұзу, яғни қауіпсіздік пен бүтіндікті бұзу мақсатымен қорғаудан өту болып табылады. Бұл үрдіс желілік құрт деп аталатын бағдарламалық құралды бұзатын арнайы түрдің көмегімен автоматтандырылған болуы мүмкін.

Құрттар деп жаһандық желі арқылы тарап, бөлек бағдарламаларды емес, толық жүйелерді зақымдайтын вирустарды атайды. Бұл вирустың ең қауіпті түрі, себебі шабуылдың объектісі мемлекеттік масштабтағы ақпараттық жүйелер болып табылады. Internet жаһандық желісі пайда болғаннан бастап, қауіпсіздікті бұзудың бұл түрі үлкен қауіп төндіреді, себебі, осы желіге қосылған 100 миллион компьютердің кез келгені кез келген жағдайда оған ұшырауы мүмкін [11].

1.3.6 Есептеуіш жүйелердегі қауіптердің негізгі түрлері

Есептеуіш жүйелер ашуының, бүтінділігінің немесе қызметінің бас тартуына жататын қауіптердің үш түрі бар. Ашу қаупі ақпараттың оны білмеуге тиіс адамның біліп қоюы болып табылады. Компьютерлік қауіпсіздік терминдерінде ашу қаупі есептеуіш жүйеде сақталатын немесе бір жүйеден екінші жүйеге жіберілетін біраз құпия ақпаратқа кіру рұқсаты алынған кезде болады. Кейде ашу қаупімен байланысты «жайылып кету» термині қолданылады.

Бүтінділік қауіптілігі есептеуіш жүйеде сақталынатын немесе бір жүйеден екінші жүйеге жіберілетін ақпараттың қасақана өзгертілуін құрайды. Бұзушылар әдейі ақпаратты өзгерткенде, ақпараттың бүтінділігі бұзылған деп айтады. Бүтінділік егер, рұқсатсыз өзгертуге кездейсоқ қате алып келген болса тағыда бұзылады. Рұқсат етілген өзгертулерге негізделген мақсатпен белгілі тұлғамен жасалынған өзгертулерді атайды (мұндай өзгертулерге деректер базасын жспарлы түзету жатады).

Қызметтің бас тарту қаупі басқа қолданушымен жасалынған қасақана істердің нәтижесінде есептеуіш жүйенің біраз ресурсына кіру рұқсатына әдейі блок қойылады. Яғни, егер бір қолданушы қызметке кіру рұқсатын сұраған

кезде, басқа қолданушы мұны болдырмауды жүзеге асырса, қызметтің бас тартуы болады. Сұралып жатқан ресурсқа ешқашан кіру рұқсаты болмас үшін блок қою тұрақты болуы мүмкін, немесе ол пайдасыз болуы үшін сұралып жатқан ресурстың ұзақ кідірісін тудыруы мүмкін. Мұндай жағдайда, ресурс таусылған деп айтады.

Қауіпсіздік саясаты жүйе қолданушыларының ақпарат пен ресурстарға кіру рұқсатын ала алатындай көптеген жағдайларға ие. Осылай, қауіпсіздік саясаты жүйені нақты іске асыруда орындалатын көптеген талаптарды анықтайды. Әлбетте, қалаулы қауіпсіздік саясатын жүргізу үшін жүйеде тиесілі механизмдер болуы тиіс. Көп жағдайда, қауіпсіздік механизмдері әкімшілік пен қолданушыларға тиесілі процедуралары бар, базалық есептеуіш ортаның (операциялық жүйенің) бөлігі болып табылатын, кейбір автоматтандырылған компоненттерді құрайды.

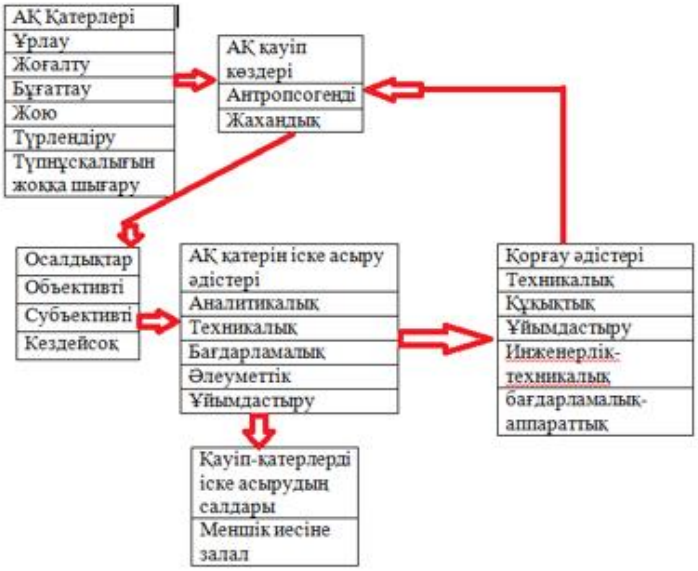
Комьютерлік жүйелердің ақпараттық қауіпсіздік мәселелерінің негізгі аспектерінің бірі бұзушы бағдарламалық құралдарға қарсы әрекет ету болып табылады. Бұл міндетті шешу жолдарын қарастырайық:

а) бұзушы бағдарламалық құралдардың нақты түрлерін іздеп және жоюға арналған арнайы бағдарламалық құралдарды құру (вирусқа қарсы бағдарлама);

ә) архитектурасы мен моделі бұзушы бағдарламалық құралдардың болуына жол бермейтін немесе олардың белсенділігі мен мүмкін болатын қатерлерді шектейтін есептеуіш жүйелерді жобалау;

б) есептеуіш жүйелердің ақпараттық қауіпсіздік қатерлерінің және бұзушы бағдарламалық құралдар бөлшектерінің болуын анықтайтын бағдарламалық жасақтама талдауын жасайтын құралдар мен тәсілдерді жасап, қолдану.

Есептеуіш жүйенің ақпараттық қауіпсіздік қатерлері барын анықтайтын бағдарламалық жасақтама талдау процедурасын бағдарламалық жасақтаманың қауіпсіздік талдауы деп аталады. Ақпараттық қауіпсіздіктің қатерлерін іске асыру моделі 1.4 суретте көрсетілген.



Сурет 1.4 – Ақпараттық қауіпсіздіктің қатерлерін іске асыру моделі

1.3.7 ЭЕЖ-дегі қашықтағы шабуылдардың классификациясы мен талдауы

Компьютерлік жүйелердің қауіпсіздігінің кез келген талдауының негізі оларға тиесілі негізгі қауіптерді білу болып табылады. Осындай талдау жүргізу үшін, қауіптер көптеген түрінен жинақталған түрлерін, олардың сипаттамаларын және классификациясын айыру қажет.

ЭЕЖ-дегі қашықтағы шабуылдардың классификациясы.

Қашықтағы шабуылдарды келесі сипаттар бойынша жіктеуге болады:

а) Әсер ету сипатына қарай:

1) активті;

2) пассивті.

Желілік жүйеге активті әсер етуге желі жұмысына (желі конфигурациясын өзгерту, желі жұмысының бұзылуы) және жүйеде қабылданған қауіпсіздік саясатының бұзылуына тікелей әсер етушілер жатады. Қашықтағы шабуылдардың барлығы дерлік активті болып саналады.

Желілік жүйеге пассивті әсер ету желі жұмысына тікелей әсер етпейтін, бірақ оның қауіпсіздік саясатын бұзатын әсер етулер жатады. Желі жұмысына тікелей әсер болмағандықтан, пасивті қашықтықтан әсер етуді анықтау мүмкін емес. Пасивті түрдегі қашықтықтағы әсер етудің жалғыз қарастыруы желідегі арналарды тыңдау болып табылады.

ә) Әсер ету мақсатына қарай:

1) ақпаратты қағып алу;

2) ақпаратты бұрмалау.

Кез келген шабуылдың негізгі мақсаты – ақпаратқа рұқсатсыз қол жеткізу болып табылады. Ақпаратқа қол жеткізудің негізгі екі мүмкіндігі бар: қағып алу және бұрмалау. Ақапаратты қағып алу мүмкіндігі оған қол жеткізуді, бірақ оны түрлендіре алмауды білдіреді. Ақпаратты қағып алуды

қарастыру желіде арнаны тыңдау болып табылады. Бұл жағдайда ақпаратқа оны бұрмалау мүмкіндігісіз рұқсатсыз қол жеткізіледі.

Ақпаратты бұрмалау мүмкіндігі ақпараттық ағынды толық бақылауды білдіреді. Ақпаратты қағып алу сияқты тек оқуға емес, сонымен қатар оны түрлендіруге болады.

б) Әсер етуді бастау шарты бойынша.

Ақпаратты қорғау ақпараттық қауіпсіздікті қамтамасыз етуге бағытталған шаралар кешенін құрайды. Тәжірибеде ол деректерді енгізу, сақтау, өңдеу және жіберу үшін, ақпаратты және ресурсты бүтінділікте, кіруге рұқсатта және керек жағдайда құпиялылықта сақтау болып табылады.

Ақпараттық жүйелермен жұмыс жасайтын қызметкерлерге қарай компьютерлік кешеннің ортасына әсер ететін операциондық реттеуіштер қолданылады. Яғни, қызметкерлерді таңдау, оларды оқыту, тәртіппен қамтамасыз етуді білдіреді. Мұнда ғимаратты және жабдықтар мен басқаларды физикалық қорғау шаралары да жатады.

Қандайда бір қорғаныс шараларын қолдану алдында қауіптер талдауын жүргізу қажет.

Жиі таралған қауіптер:

а) зияндылық мөлшері жағынан ең жиі кездесетін және ең қауіптілері ақпараттық жүйелерге қызмет көрсететін қолданушылардың, қызметкерлардың, жүйе әкімшілігінің және басқа тұлғалардың әдейі жасалмаған қателері болып табылады [9]. Кейде мұндай қателер қауіпті: деректі дұрыс енгізбеу, бағдарламадағы қателер, ал кейде олар зиянкестер қолданатын әлсіздікті тудырады – басқарудың әдеттегі қателері болып табылады. Статистикаға сәйкес жоғалтудың 65%-ы – байқаусыз жасалған қателердің салдары болып табылады. Өрт пен су басуды сауатсыздық пен салғырттықтың жанында болмашы нәрсе ретінде санауға болады. Байқаусыз жасалынған қателермен күресудің негізгі тәсілі – максималды автоматтандыру және жасалынатын іс әрекеттердің дұрыстығын бақылау болып табылады;

ә) зияндылық мөлшері бойынша екінші орында ұрлық пен алдау болып табылады. Ұрлық пен алдаудан болатын зиындылық өте көп, сондықтан көптеген ұйымдар белгілі себептермен мұндай жағдайларды жасырады. Тергелген жағдайлардың көбінде кінәлі жұмыс тіртібі мен қорғау шараларымен жақсы таныс ұйымның штаттық қызметкерлері болатын. Бұл ішкі қауіптің сыртқаға қарағанда қауіпті болып табылатынын тағы да дәлелдейді.

Бұрынғы және қазіргі ренжулі деп аталатын қызметкерлер аса қауіпті болып табылады. Әдетте, олармен ренжітуші – ұйымға зиян келтіру ықыласы билейді (жабдықты зақымдау; уақыт өткеннен кейін, бағдарламалар мен немесе деректерді бұзатын логикалық бомбаны орнату; дұрыс емес деректерді енгізу; деректерді жою; деректерді өзгерту).

Ренжулі қызметкерлер, тіпті ұйымдағы тәртіппен таныс бұрынғы қызметкерлер ұйымға нәтижелі зиян келтіре алады. Қызметкерді жұмыстан шығарған кезде оның ақпараттық ресурстарға кіру рұқсаты күшін жоюын қадағалау қажет.

Қоршаған ортадан келетін қауіптер үлкен алуан түрлілігімен ерекшелінеді. Бірінші кезекте, инфрақұрылымның бұзылуын – электркуаттаудың апаттары, уақытша байланыстың болмауы, сумен жабдықтаудағы кідіріс, азаматтық бассыздық айта кету керек. Сұрапыл апаттар болып қабылданатын, қауіпті табиғи апаттар мен оқиғалар – өрттер, су басу, жер сілкінісі, дауылдар. Статистикалық деректер бойынша, ақпараттық жүйелерге әсер еткен от, су және ұқсас «дұшпандар», соның ішінде – электр қуатының төмен сапасының үлесіне 13% жоғалтулар тиесілі.

Ақпараттық жүйелерге әсер ететін, шығындардың негізгі үлесіне сәйкес келетін негізгі қатерлер осындай болады.

Нешетүрлі криптографиялық мүмкіндіктерінде барынша жоғары әртүрлі сандардың сәйкестіктері керек. Қарастыруға А және Б пайдаланушыларға мәлім ақпаратты кілт айқын деп жорамалдадық. Бұндай ақпарат нақты бір орында өндірілуі қажет. Қажет тізгінді анықтау үшін тізгінді қадағалау мүмкіндігі әртүрлі сандардың өзгерісін пайдаланады. Алайда өзгеріс ойдағыдай қауіпсіз болмаса, төмен сападағы тізгін ауыстырылады. Осыған сәйкес жағдай Netscape зерттеулерінің бұрынғы нәтижелерінде анықталды.

Бұдан шыққан нәтиже қанағаттандырғандықтан, шыққан мәліметтің көлемі тек 28,8 битті шығарады. Шыққан мәліметтердің негізі жайында көбірек білсек, оның көлемі аз шығады.

Бүтінділік қауіптілігі есептеуіш жүйеде сақталынатын немесе бір жүйеден екінші жүйеге жіберілетін ақпараттың қасақана өзгертілуін құрайды. Бұзушылар әдейі ақпаратты өзгерткенде, ақпараттың бүтінділігі бұзылған деп айтады. Бүтінділік егер, рұқсатсыз өзгертуге кездейсоқ қате алып келген болса тағы да бұзылады. Рұқсат етілген өзгертулерге негізделген мақсатпен белгілі тұлғамен жасалынған өзгертулерді атайды (мұндай өзгертулерге деректер базасын жспарлы түзету жатады).

Жабдықтар мен басқаларды физикалық қорғау шаралары да жатады.

Жоғалту статистикасына қарай, әр-түрлі серіктестіктерге қарай компьютерлік бұзақылыққа байланысты көптеген шығындарға әкеліп соғады. Көп жағдайда компьютерлік қылмыскерлер жекеменшіктегі таза қызмет атқармай жүрген қызметшілерге байланысты болады. Алайда соңғы уақыттарда ішкі заңбұзушылық төмен жағдайға алып келе жатыр. Қандай жағдай болса да ішкі және сыртқы мекеменің желі арасындағы қауіпсіздікке көп көңіл бөлген дұрыс. Тек толыққанды іс әрекет сіздің желі ішіндегі ақпараттық қауіпсіздігіңізді сақтай алады.

Қауіпсіздік саясаты жүйе қолданушыларының ақпарат пен ресурстарға кіру рұқсатын ала алатындай көптеген жағдайларға ие. Осылай, қауіпсіздік саясаты жүйені нақты іске асыруда орындалатын көптеген талаптарды

анықтайды. Әлбетте, қалаулы қауіпсіздік саясатын жүргізу үшін жүйеде тиесілі механизмдер болуы тиіс. Көп жағдайда, қауіпсіздік механизмдері әкімшілік пен қолданушыларға тиесілі процедуралары бар, базалық есептеуіш ортаның (операциялық жүйенің) бөлігі болып табылатын, кейбір автоматтандырылған компоненттерді құрайды.

2 Centos

Әңгіме ерекше жаңа емес, бірақ, әрине, назар аударарлық CentOS дистрибутиві туралы. Бұл операциялық жүйе Red Hat Enterprise Linux негізінде жасалған, жоғары тұрақтылығымен ерекшеленеді, 64 биттік архитектурасы бар компьютерлерде де, 32 биттік компьютерлерде де жұмыс істей алады. Linux-тің негізгі айырмашылығы таратылу тегін болып табылады. Осы платформаның артықшылықтары мен кемшіліктері туралы толығырақ, сәл төмен.

Linux ортасында жұмыс істеуге арналған барлық бағдарламалық өнімдер CentOS-да жұмыс істейтіндіктен бастау керек. Сонымен қатар " дистрибутиве бірқатар вшитых шешімдер, олар айтарлықтай жеңілдетіп, өмір программистке немесе желілік әкімшісіне жұмысын арнайы бөлінген серверде.

Операциялық жүйе энтузиастармен әзірленген, дегенмен, ол тұрақты жаңартулары бар. Қазіргі уақытта соңғы алтыншы нұсқа қорғау саласындағы барлық қажетті жаңалықтардың толық пакетін қамтиды. Жаңа нұсқалар екі жылда бір рет шығарылады, әр жарты жыл сайын жаңарту пакеті.

Қазір өте өзекті мәселе болып саналады: "жаңа пайдаланушылар үшін CentOS-Linux деп санауға бола ма?"Жауап теріс. CentOS-бұл толық операциялық жүйе. Бұл тәуелсіз жоба, дегенмен, Red Hat Enterprise жасалған жалпы базалық бағдарламалық коды бар. Бірден бір маңызды түсініктеме беру керек. Бұл қарақшылық нұсқасы емес, заңды жүйе. Егер нақты айтатын болсақ, барлық тұз-бұл Red Hat өз қалауы бойынша бастапқы кодтарды ашық қол жеткізуге қояды. Әрине, мұндай қайырымдылық байқалмады. Бүкіл әлем бойынша бағдарламашылар өз жобасын құруды шешті,қазір оның қаншалықты табысты екенін білеміз.

Ең алдымен орнату процесін қарастырайық. Дегенмен, қарапайым және қатардағы пайдаланушылардан артық күш-жігерді талап етпейді. Әзірлеушілер сайтында файлды жүктеп, дискіге жазамыз, бәрін орнатамыз. Барлық осы әрекеттерді орындау үшін тіпті программист болудың қажеті жоқ, Қатардағы пайдаланушының білімі жеткілікті.

Сондай-ақ, әзірлеушілердің ресми сайтында олардың бағдарламасын пайдаланғысы келетін пайдалы кеңестер мен нұсқаулықтар бар. Ал егер сіз жұмыс кезінде музыка тыңдауды ұнатсаңыз, онда мұнда біраз өнертапқыштық көрсету керек. Жүйе негізінде mp3 форматына есептелмеген, бірақ ogg урада оқиды. Бұл патенттік құқықтармен байланысты, бірақ қалыптасқан жағдайдан тамаша шығу бар, файлдарды қайта кодтау жеткілікті және сүйікті музыканы ләззат аласыз.

2.1 Ubuntu

Ubuntu-жеке компьютерлерде, ноутбуктер мен серверлерде пайдалану үшін өте қолайлы Linux ядросына негізделген операциялық жүйе. Ол сізге қажет барлық қажетті бағдарламаларды қамтиды: Интернетті қарау

бағдарламасы, мәтіндермен, электрондық кестелермен және презентациялармен жұмыс істеуге арналған кеңселік пакет, ғаламторда қарым-қатынас жасауға арналған бағдарламалар және т.б.

Shotcut танымал және тиімді FFmpeg кітапхана арқасында көптеген танымал аудио және бейне форматтар мен кодекстердің қолдауына ие. Импорт қажет емес, бұл өзінің редакциялануын білдіреді, сондай-ақ жобада көп форматты уақыт шкаласы, рұқсат және кадрлардың жиілігі бар. Кадрларды нақты іздеу көптеген бейнефильмдер үшін Қолдау бар.

Мультимедиалық файлдардың толық сапасын, соңғы файлдарды іздеуді, миниатюраларды ұсынатын ойнату тізімін, сүзгілер панелін, тарихты, кодтау панелін, тапсырмалар кезегін, сондай-ақ балқытылған сервер мен ойнату тізімін қоса алғанда, бірнеше бекітілген және ажыратылатын панельдер бар. Сондай-ақ, файл менеджерінен активтерді сүйреуді қолдайды.

Сіз Shotcut өңдегішін сіздің қалауыңыз бойынша пішімге айналдырудан бұрын көрсетілген ұзындықтағы бейнені қиып алу үшін пайдалануға болады. Сіз сондай-ақ сүзгілерді және әсерлерді таңдау арқылы жобаларыңызды өңдеуге болады. Shotcut сондай-ақ веб-камерадан алынған материалды сақтауға және өңдеуге мүмкіндік беретін жазу функциясын қамтиды, сондай-ақ HTTP, HLS, RTMP, RTSP, MMS және UDP форматтарында ағын беруді қолдайды.

Енгізу және алдын ала қарау үшін Blackmagic Design SDI және HDMI. Экран, веб-камера және аудио басып алу. Желі ағынын ойнату. 4K ажыратымдылығы және SDI, HDMI, веб-камера, Jack & Pulse аудио, IP ағыны, X11 экраны және Windows DirectShow құрылғылары сияқты әртүрлі құрылғылардан түсіріледі.

2.3 Debian

Debian философиясының және әдіснамасының комбинациясы, GNU құралдары, Linux ядросы және басқа да маңызды бағдарламалар Debian GNU/Linux деп аталатын бірегей дистрибутивті құрайды. Бұл дистрибутив көптеген бағдарламалар пакеттерінен жиналған. Дистрибутивтегі әрбір пакетте орындалатын файлдар, сценарийлер, құжаттама, конфигурациялық ақпарат бар және пакетті өзекті күйде ұстау үшін жауап беретін сүйемелдеуші бар, қателер туралы хабарламаларды (bug reports) қадағалайды және бағдарламаның негізгі авторларымен байланысады. Біздің қате туралы хабарламаларды қадағалау жүйесімен үйлескен пайдаланушыларымыздың үлкен базасы проблемалардың тез табылатындығына және жойылатындығына кепілдік береді.

Debian егжей-тегжейлі назар жоғары сапалы, тұрақты және кеңейтілген дистрибутив құруға мүмкіндік берді. Орнатылған жүйелер әртүрлі міндеттерді орындауға оңай бапталуы мүмкін: қарапайым желіаралық экраннан (firewall), ғалымның жұмыс станциясынан, жоғары өнімді желілік серверге дейін.

Debian оның техникалық жетілуі және Linux қоғамдастықтың қажеттіліктері мен күтулерін терең түсіну үшін тәжірибелі пайдаланушылар

арасында әсіресе танымал. Debian сондай-ақ қазір барлық жерде пайдаланылатын Linux көптеген жаңа қасиеттерін қосты.

Мысалы, Debian оңай орнату және бағдарламаларды жою үшін пакеттерді басқару жүйесі болды Linux бірінші дистрибутив болды. Сондай-ақ, ол қайта орнатусыз соңғы нұсқаға дейін жаңартуға болатын Linux-тың бірінші дистрибутиві болды.

Debian Linux әзірлеу көшбасшы болып табылады. Оның даму процесі, мысалы, тұтас операциялық жүйені құру және сүйемелдеу сияқты өте күрделі есептер үшін де ашық бастаулар моделі (Open Source) қалай жақсы жұмыс істей алатынының мысалы болып табылады.

Debian басқа Linux дистрибутивтерінен ерекшеленетін ерекшелігі оның пакеттерді басқару жүйесі болып табылады. Ол Debian жүйесінің әкімшісіне жүйеде орнатылған пакеттерге толық бақылау береді, бұл бір пакетті орнату немесе барлық операциялық жүйені автоматты түрде жаңарту. Сондай-ақ, жеке пакеттер жаңартудан қорғалуы мүмкін. Сіз тіпті өзіңіз жинаған бағдарлама пакеттерін басқару жүйесін және олар қандай бағдарламаларға байланысты екенін көрсете аласыз.

Сіздің жүйеңізді "троян аттарынан" және басқа да зиянды бағдарламалардан қорғау үшін Debian серверлерінде келіп түсетін пакеттер тек тіркелген Debian еріп жүрушілерінен алынғанын тексеру жүргізіледі. Сондай-ақ, Debian әзірлеушілері өз пакеттеріндегі бағдарламалар қауіпсіздігін реттеуге қамқорлық. Шығарылған пакеттегі қауіпсіздік мәселелері болған кезде, әдетте өте тез түзетулер шығады. Қарапайым Debian жаңартулары жүйесі арқылы қауіпсіздік түзетулерін жүктеу және Интернет арқылы автоматты түрде орнатуға болады [12].

3 Windows Server 2012

Windows Server – көптеген ірі деректер орталықтары жұмыс істейтін серверлік операциялық жүйе – бүкіл әлем бойынша кез келген көлемдегі кәсіпорындарға кең мүмкіндіктер ұсынады. Көптеген дәстүрлерді жалғастыра отырып, Windows Server 2012 АТ шығындарын азайту және бизнес құндылығын арттыру үшін АТ виртуализациясы мен бұлтты есептеу орталарын өзгертуге мүмкіндік беретін жүздеген жаңа және жақсартылған мүмкіндіктерді қамтиды. Windows Server 2012 виртуалдандыру, желіге қосылу, сақтау және қолжетімділік саласындағы таңғажайып инновацияларды ұсынады.

3.1 Radius Server

Заманауи виртуалдау платформасы. Windows Server 2012 дәстүрлі виртуалдан тыс шығуға мүмкіндік беретін және жеке ДӨО, жеке бұлт болсын, қызмет көрсету үшін серверлік инфрақұрылымды құруда таңдау еркіндігін немесе ашық бұлтты сервистермен өзара іс-қимылды ұйымдастыруды қамтамасыз ететін бөлінетін архитектурасы бар динамикалық платформаны ұсынады. Көптеген серверлердің қуаты, бір құралдың қарапайымдылығы. Windows Server 2012 бағдарламасын пайдалана отырып, жоғары дәрежелі автоматтандырумен және айтарлықтай қаржы салымынсыз қарапайым басқарумен жоғары қол жетімді мультисерверлік платформа жасай аласыз. Кез келген платформадағы кез келген қосымша. Windows Server 2012-web және қосымшалар үшін ең әмбебап, масштабталатын және икемді платформа. Сіз жеке ресурстарда, сондай-ақ бұлтты сервистерде немесе олардың кез келген комбинациясында, құралдардың бірыңғай жиынтығын пайдалана отырып, қосымшаларды құру және өрістетудің икемді мүмкіндіктерін аласыз. Жұмыстың заманауи стилі. Пайдаланушыларды қолданыстағы құрылғыға және орналасқан жеріне қарамастан әдеттегі жұмыс ортасына оңай, ыңғайлы және қауіпсіз кіруге мүмкіндік береді.

RADIUS-түрлі желілік қызметтерге қосылатын пайдаланушылардың орталықтандырылған аутентификациясын, авторизациясын және есебін қамтамасыз етуге арналған желілік хаттама. Мысалы, WiFi, VPN пайдаланушыларын аутентификациялау кезінде, өткен, dialup-қосылымдар және басқа да осындай жағдайларда қолданылады**.**

Сонымен қатар, Интернет желісіне қатынау серверлері үшін Livingston Enterprises фирмасында РИГНИ Карлы (Carl Rigney) әзірленген. Қазіргі уақытта бірнеше коммерциялық және еркін таратылатын RADIUS серверлері бар. Олар өздерінің мүмкіндіктері бойынша бір-бірінен ерекшеленеді, бірақ көпшілігі мәтіндік файлдарда және әр түрлі деректер базасында пайдаланушылар тізімін қолдайды. Пайдаланушылардың есептік жазбалары мәтіндік файлдарда, әртүрлі деректер қорында немесе сыртқы серверлерде сақталуы мүмкін. RADIUS үшін прокси-серверлер бар, Орталықтандырылған әкімшілендіруді жеңілдетедіжәне/немесе интернет-роуминг тұжырымдамасын

іске асыруды қадағалайды. RADIUS-протоколдың танымалдығы көп жағдайда түсіндіріледі: ескірген жабдықпен жұмыс істеу қабілетін сақтай отырып, жаңа функционалдылықты толтыруға ашықтық, UDP пакеттерді тасымалдау ретінде пайдалануға байланысты сұраныстарды өңдеу кезінде өте жоғары реактивті, сондай-ақ сұраныстарды өңдеудің жақсы параллельдік алгоритмі; кластерлік, архитектуралар мен мультипроцессорлық платформаларда – өнімділікті арттыру мақсатында де, бас тартуға төзімділікті іске асыру үшін де жұмыс істеу қабілеті.

Тікелей аутентификациядан, авторландырудан және есепке алудан басқа, RADIUS-серверлер бірқатар өзге функцияларды орындай алады:

а) пайдаланушылардың немесе абоненттердің тіркелгілерін жасау және сақтау;

ә) жеке интерфейстен, мысалы, веб-кабинеттен пайдаланушының есептік жазбасын басқару;

б) кейбір әрекет ету лимиті бар (интернетке және карточкалық IP-телефонияға қатынау Dial-Up) қызметтерді ұсыну үшін қол жеткізу карточкаларын (логин/PIN-код) жасау);

в) берілген өлшемге немесе лимитке қол жеткізу бойынша абоненттің есептік жазбасын қолмен және автоматты түрде бұғаттау;

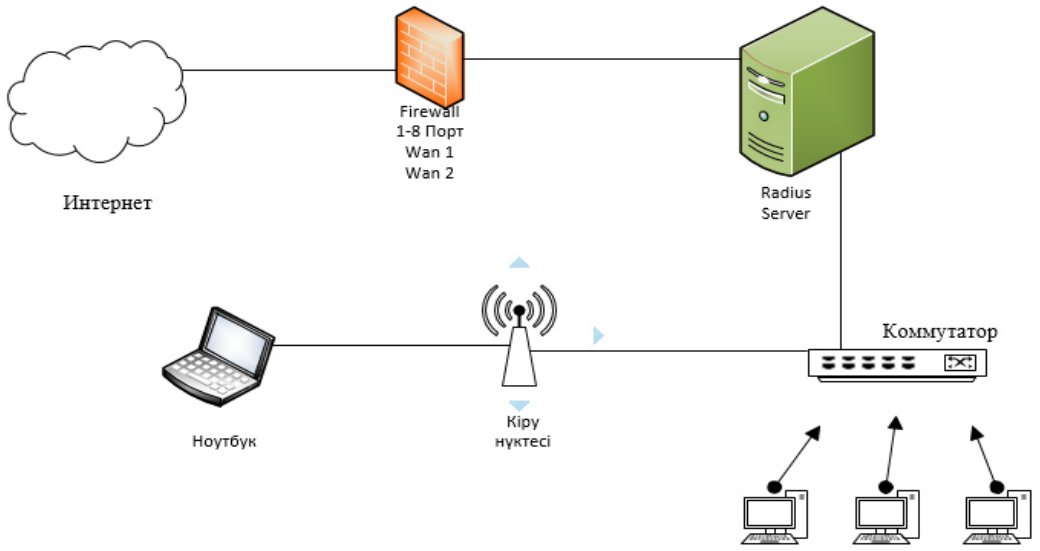
г) пайдаланушының және барлық қызмет көрсетілетін жүйенің сессиялары туралы статистикалық ақпаратты жинау және талдау;

д) дртүрлі статистикалық параметрлер бойынша есептер жасау;

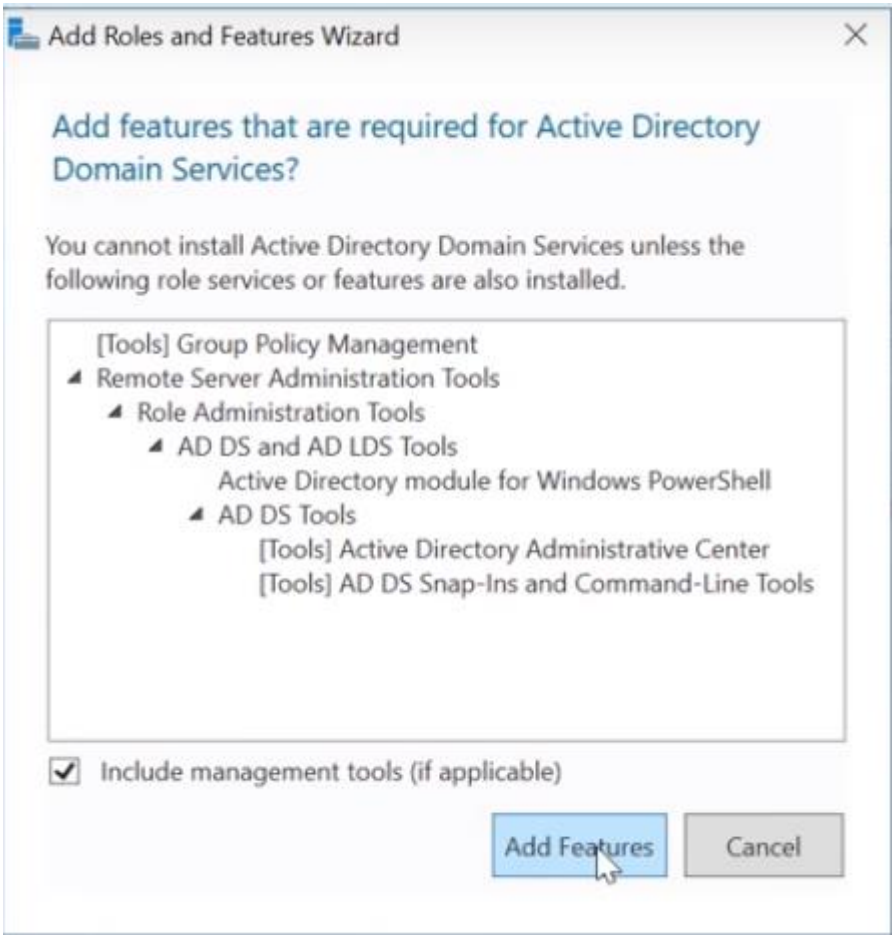
е) төлем шоттарын жасау, басып шығару және жіберу;

ж) қызмет көрсетілетін жүйеден RADIUS-серверге барлық сұраныстарды аутентификациялау.

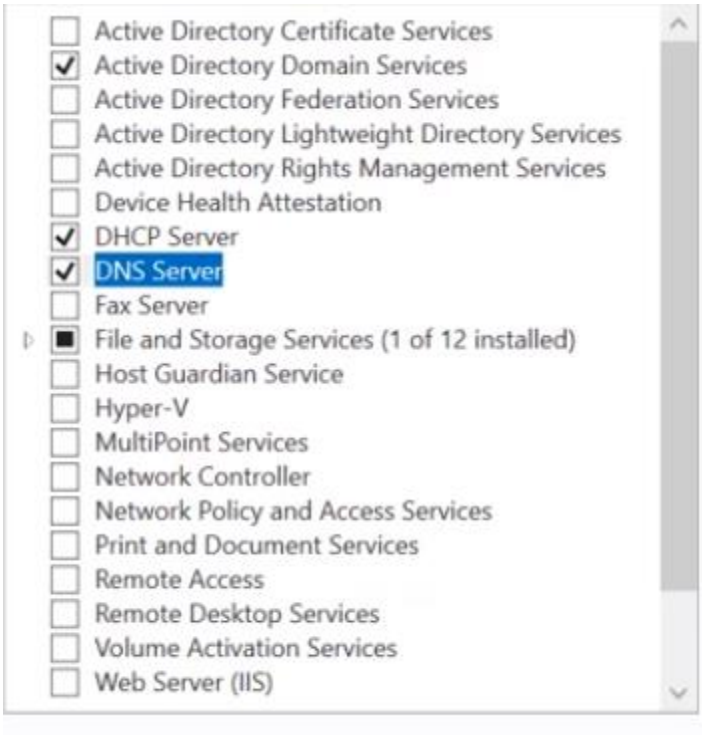
Жоғарыда аталған интернет-қызмет провайдерлері белсенді пайдаланады, олардың ортасында RADIUS кең таралған. 3.1 – 3.21 суреттерде екі жақты қорғаныс көрсетілген [13].



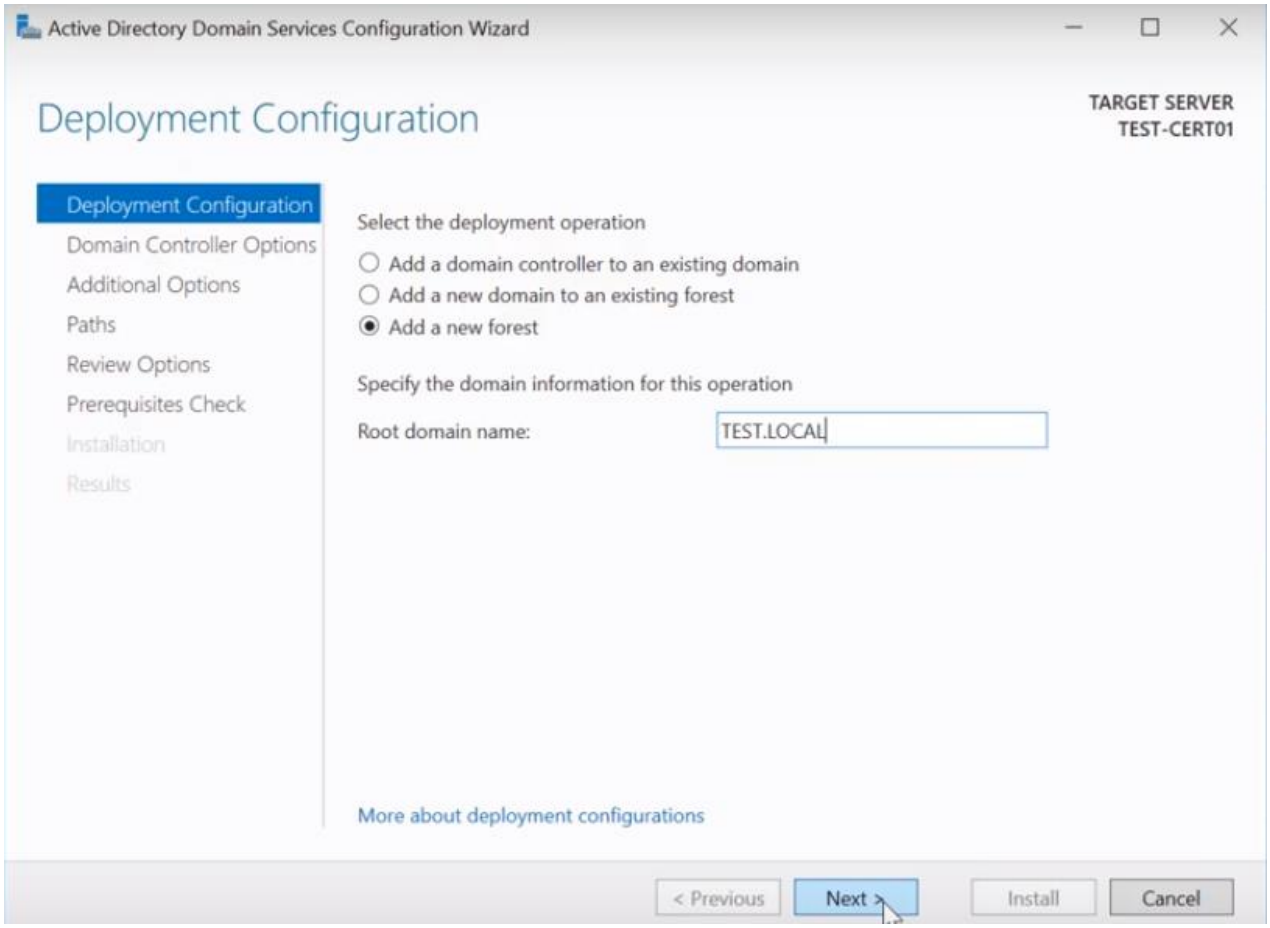
Сурет 3.1 – Radius Server-дің схемасы



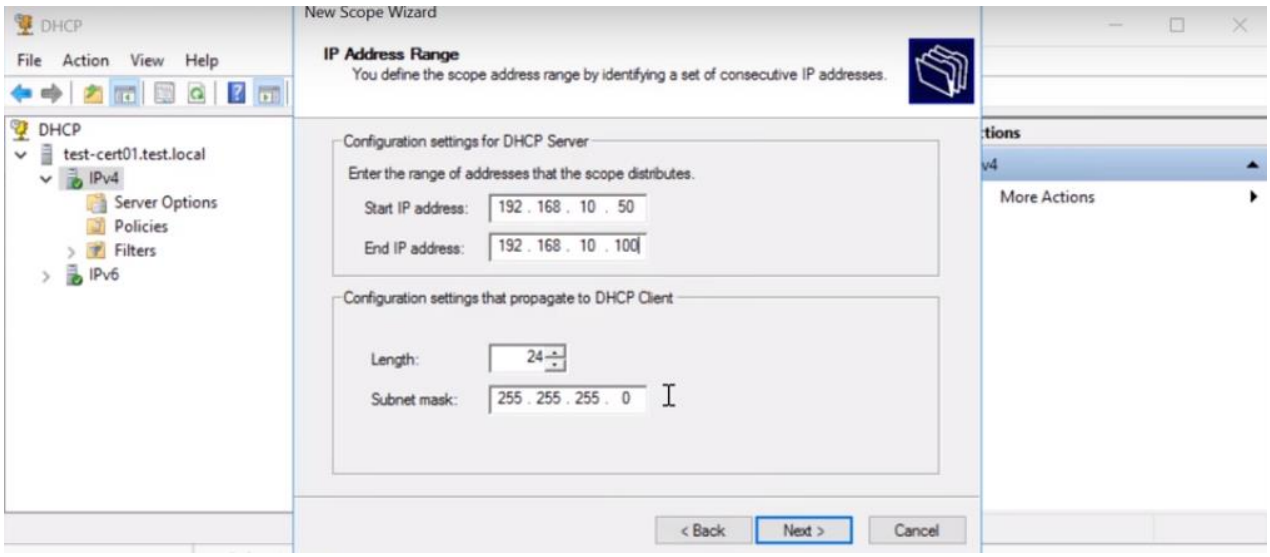
Сурет 3.2 – Домен орнату



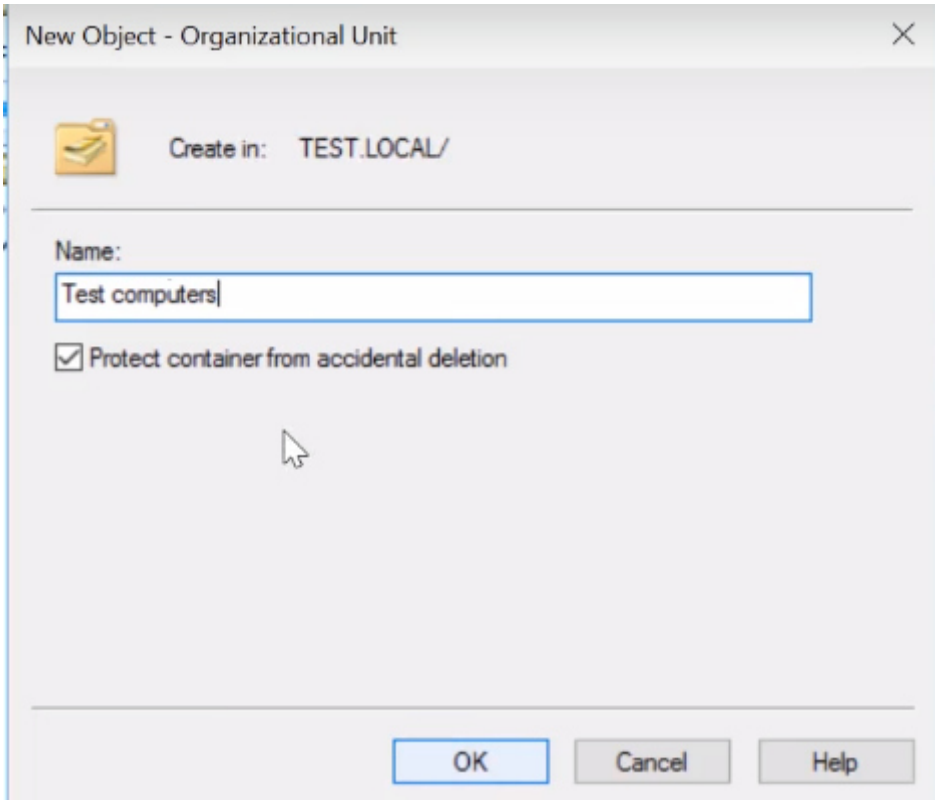
Сурет 3.3 – DHCP Server, DNS Server орнату



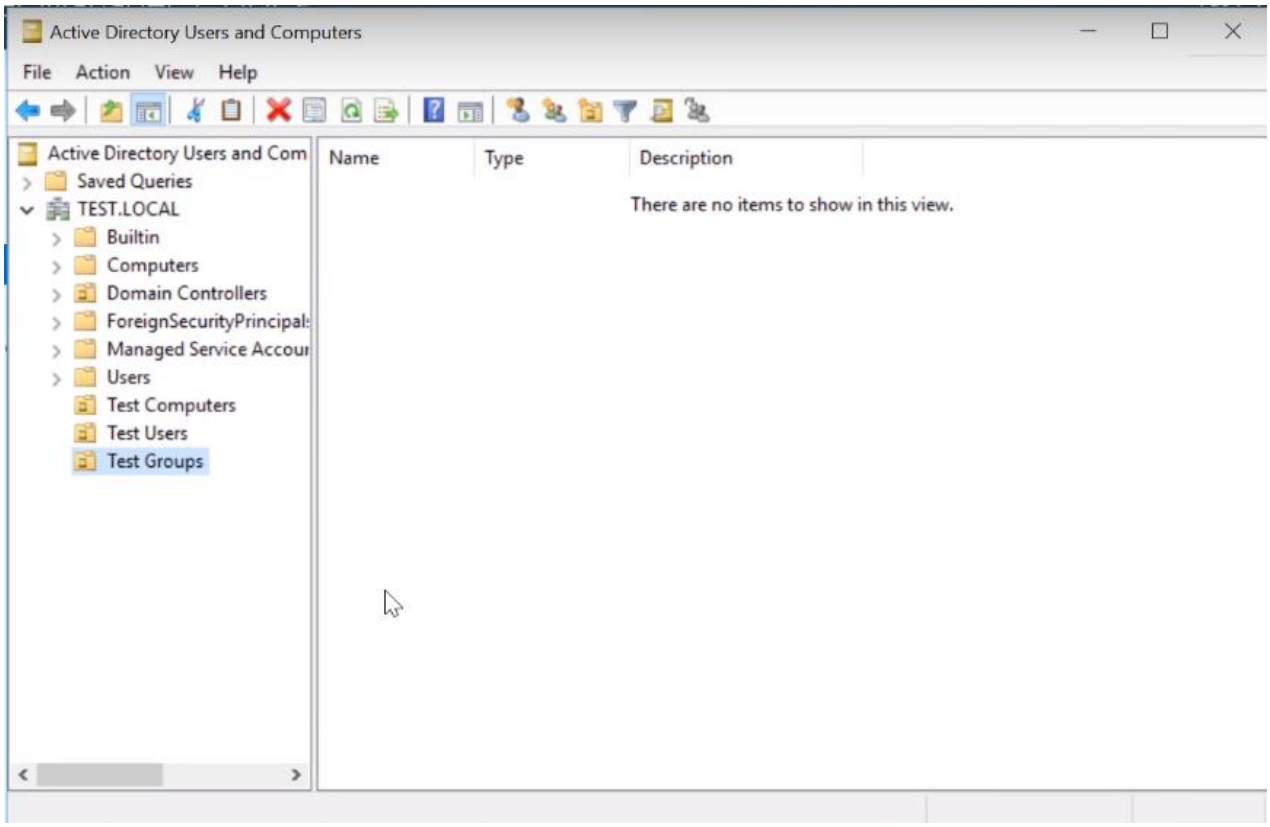
Сурет 3.4 – Домаенге ат беру



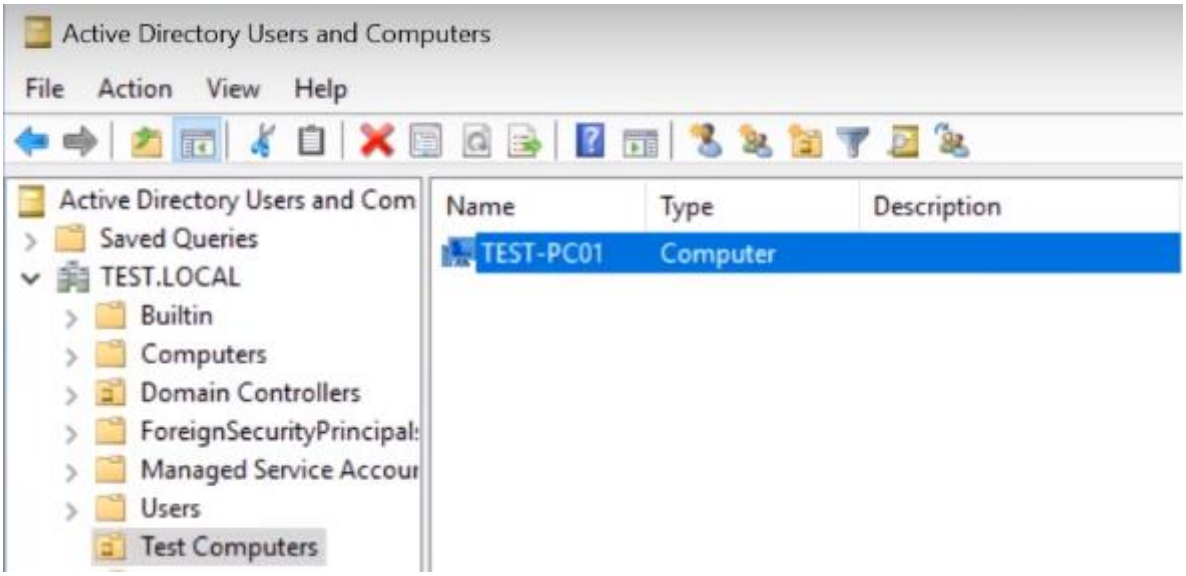
Сурет 3.5 – DHCP ip мекен жайын түзейміз



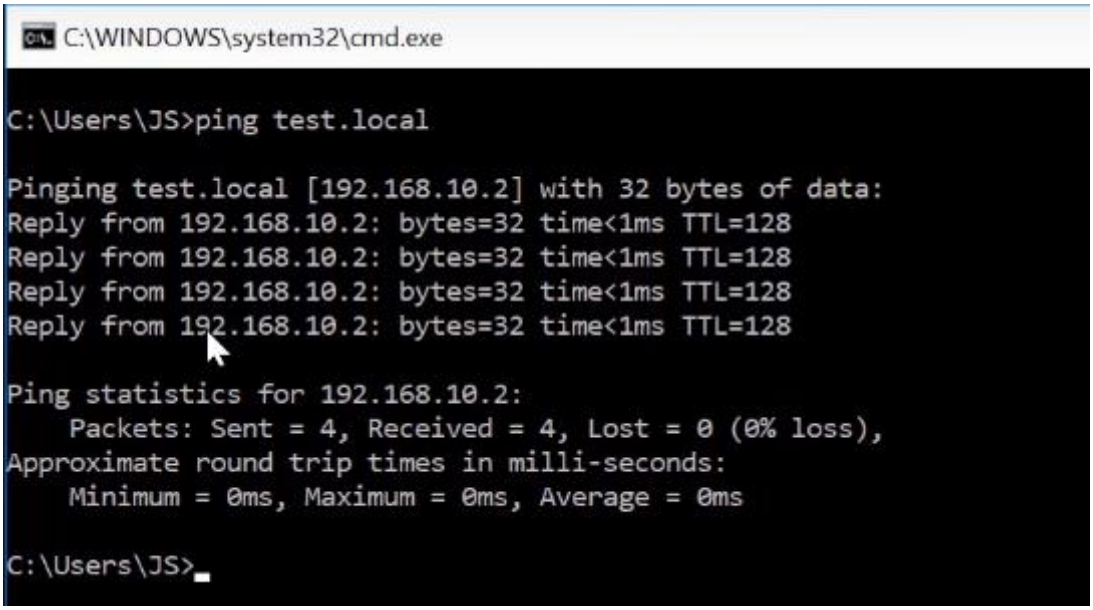
Сурет 3.6 – Топ құру



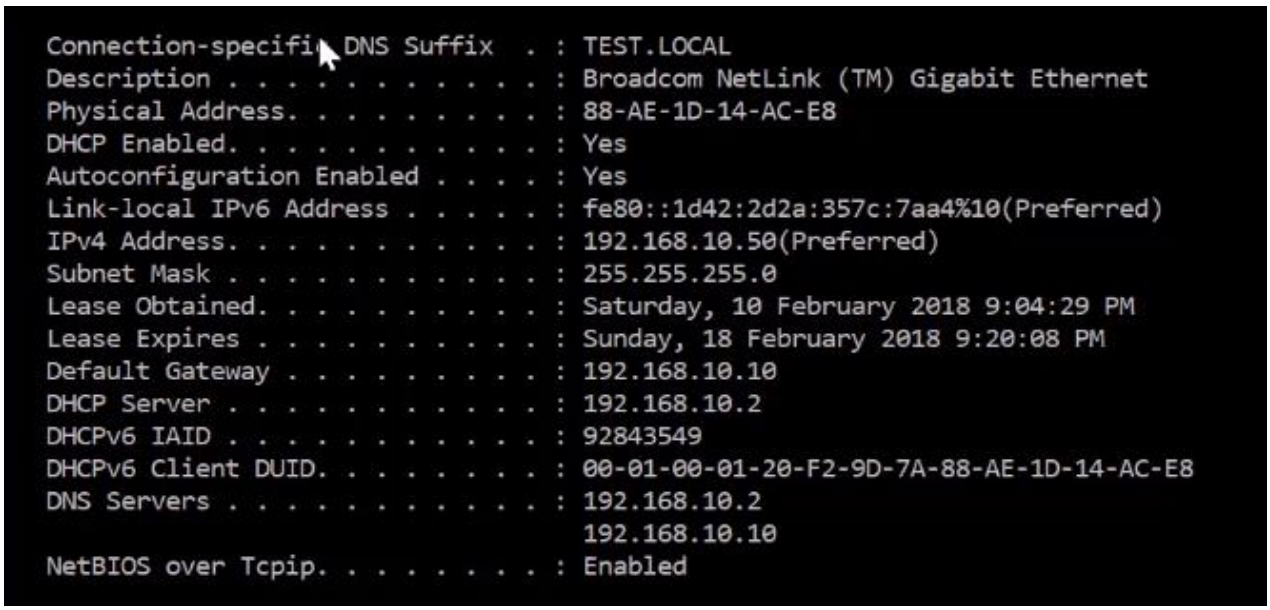
Сурет 3.7 – Active Directory да топпен пайдаланушы құрдым



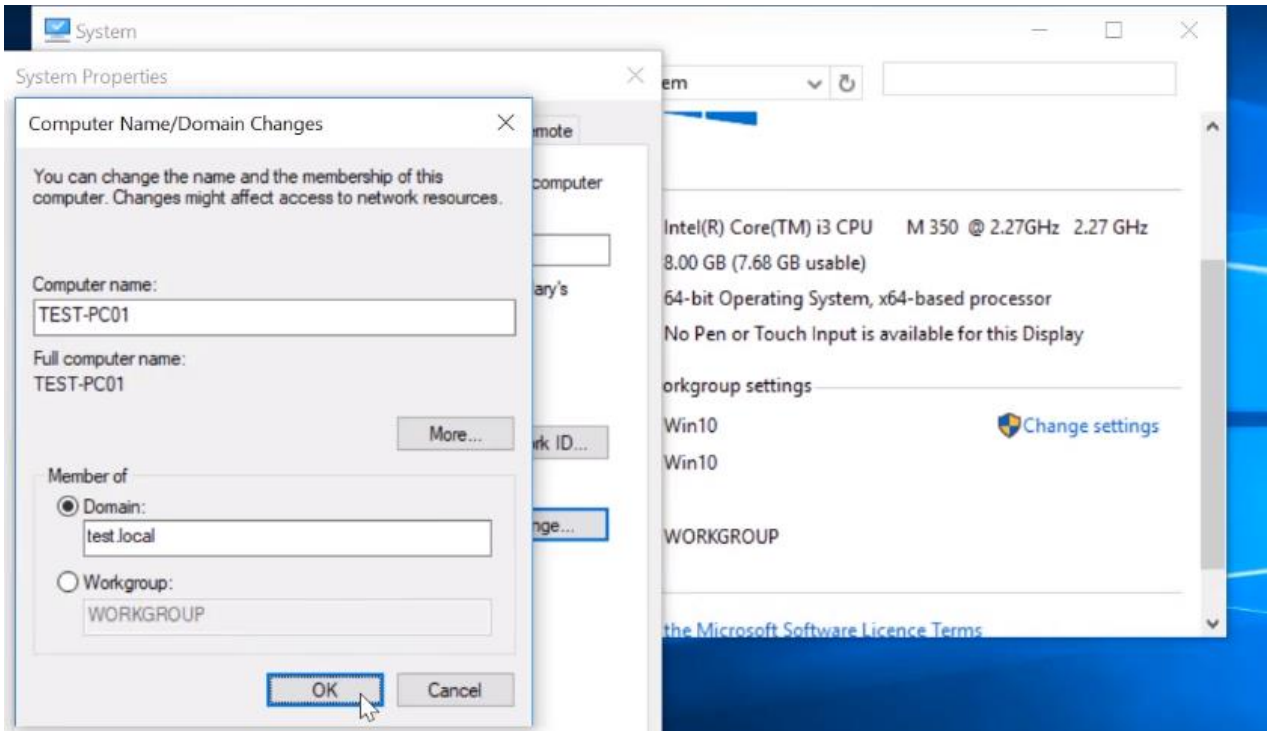
Сурет 3.8 – Пайдаланушы



Сурет 3.9 – Доменнің жұмыс жасауын тексердім



Сурет 3.10 – Доменді көру

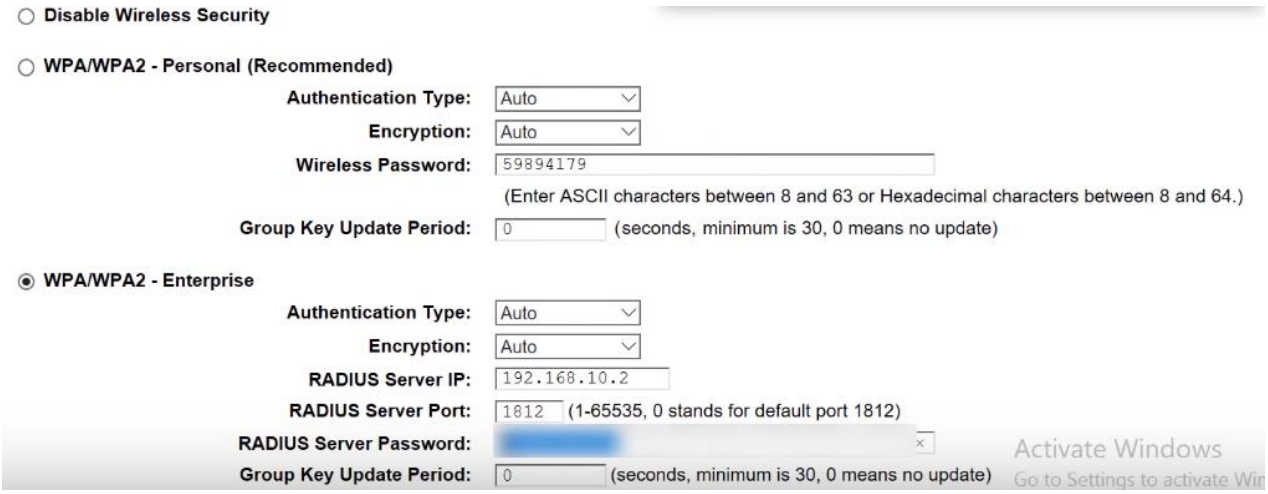


Сурет 3.11 – Доменге кіру

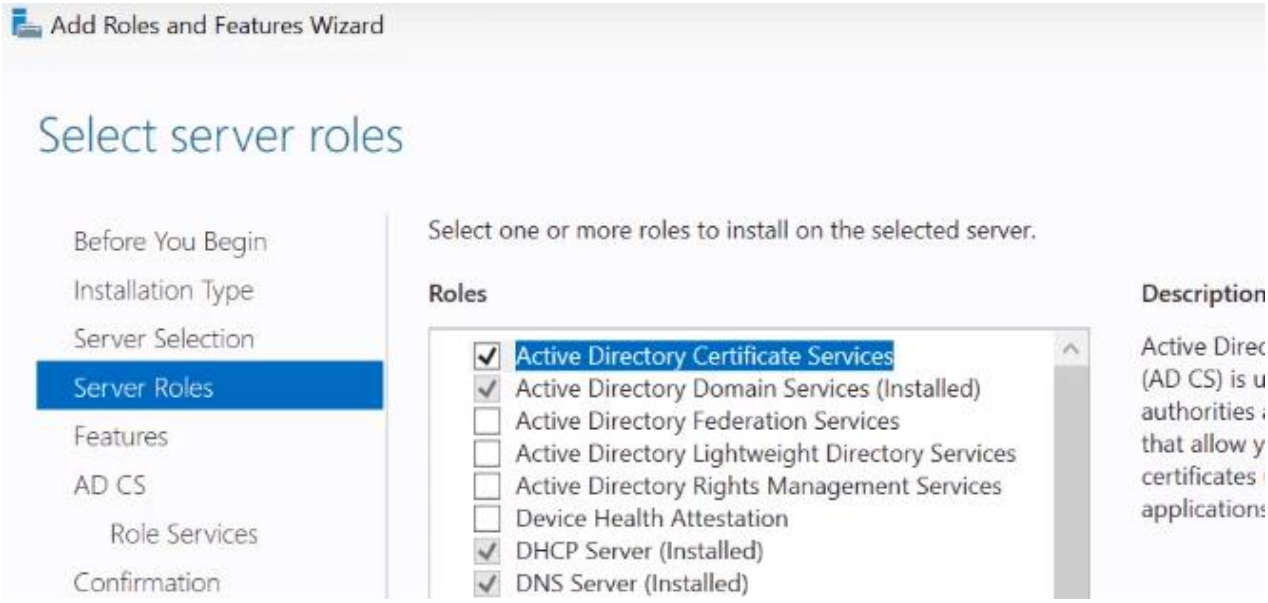
Сурет 3.12 – Ip адрес жазу

Name	Connection Type	VPI/VCI	IP/Mask	Gateway	DNS	Status
ipoe_eth1_d	Dynamic IP	N/A	192.168.10.51 /24	192.168.10.10	192.168.10.2 192.168.10.10	Connected

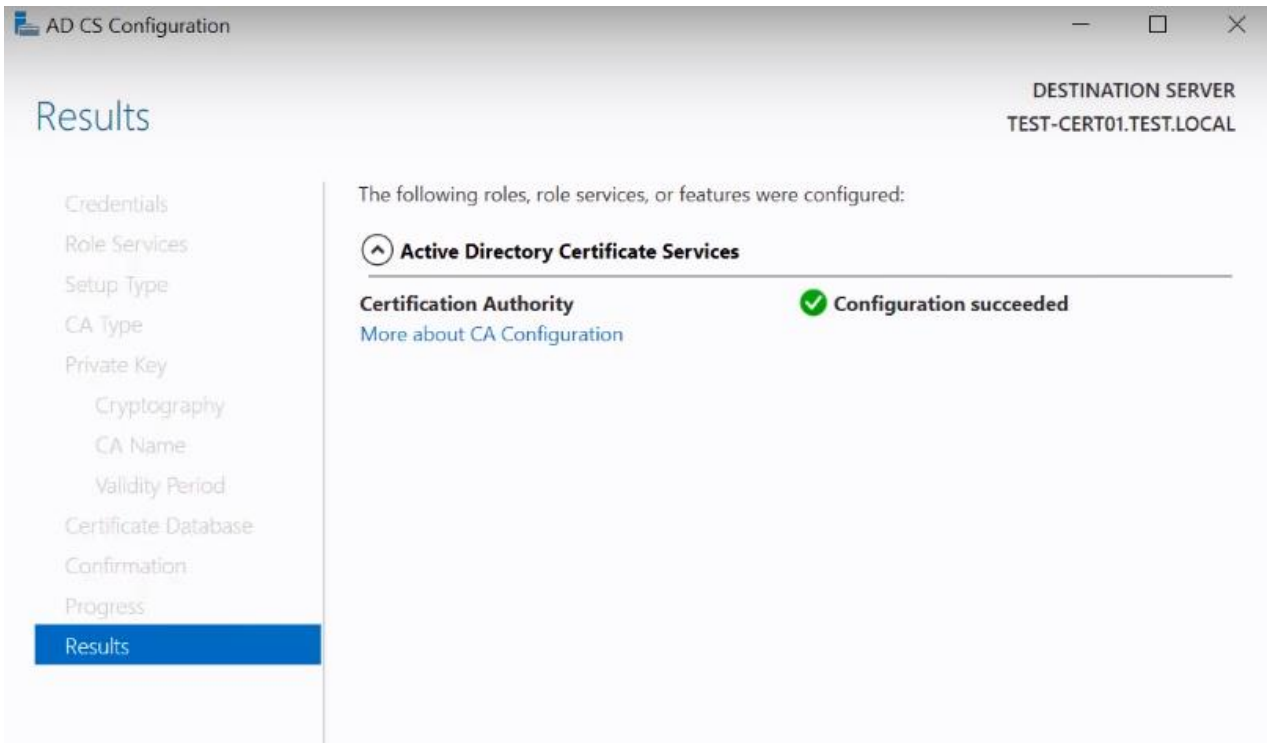
Сурет 3.13 – Radius Server ді баптау



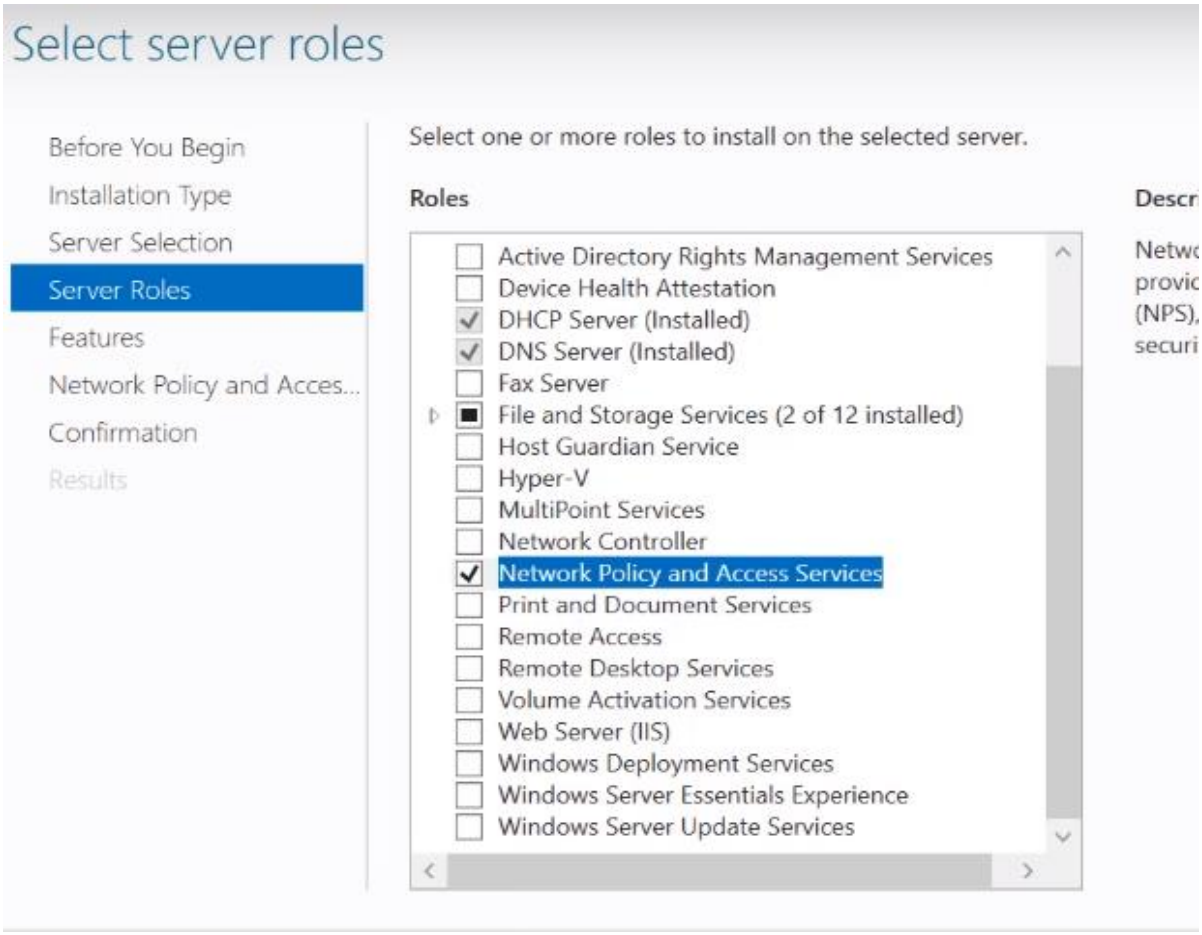
Сурет 3.14 – Radius Server дегі ip мекен жайын дурыстаймыз



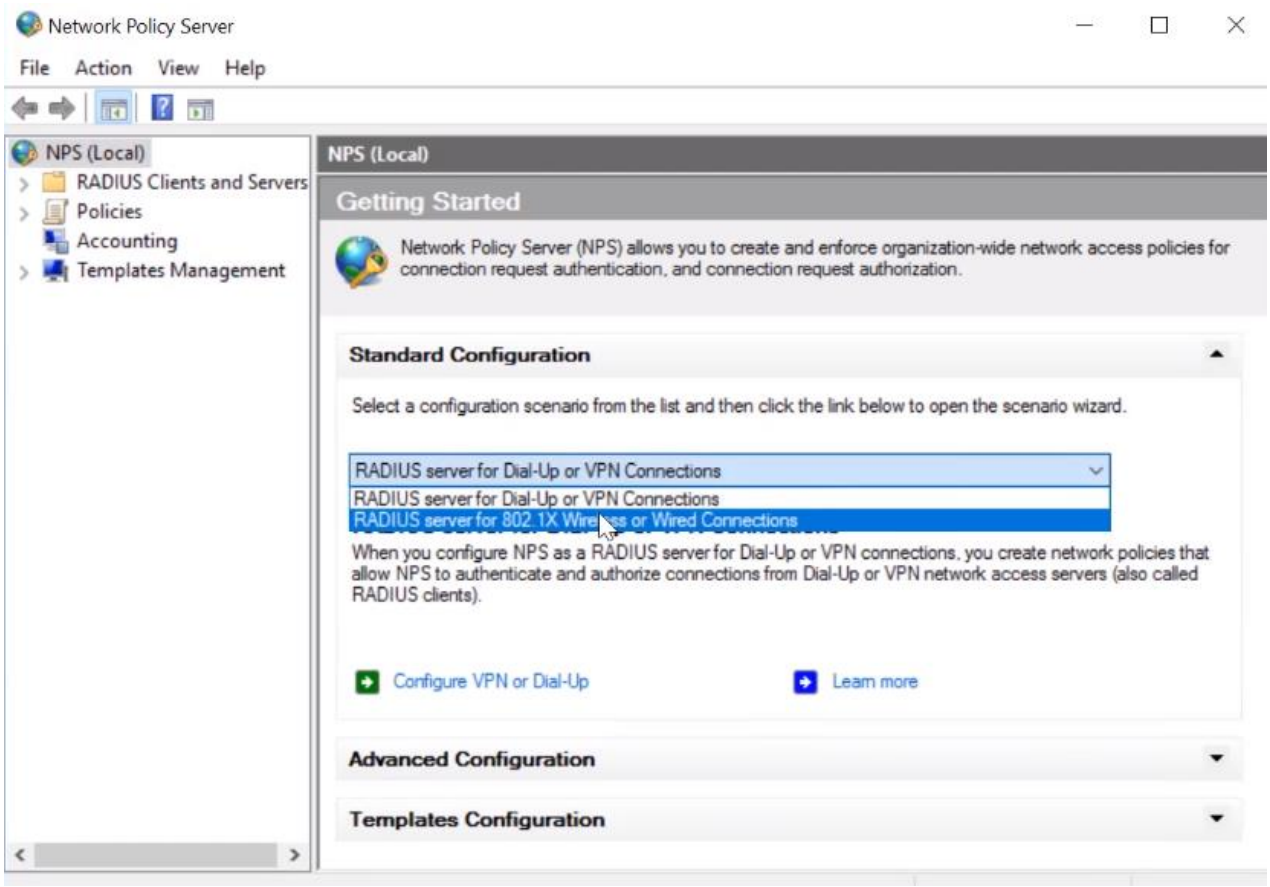
Сурет 3.15 – Active Directory сертификатының қызметтері



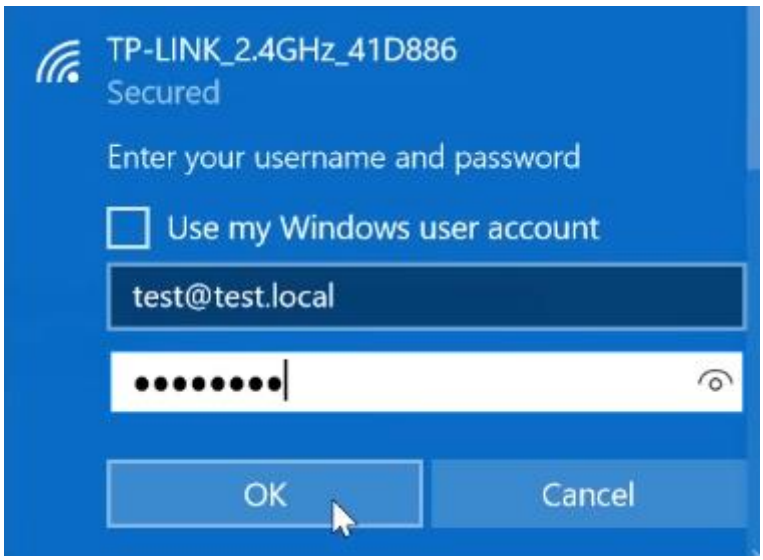
Сурет 3.16 – Active Directory сертификатының қызметтерің орнаттым



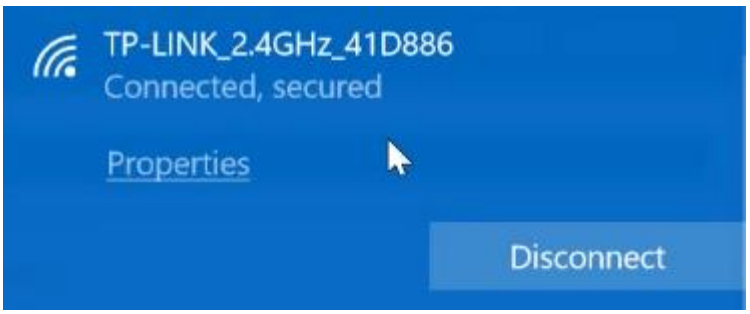
Сурет 3.17 – Желілік саясат және кірі қызметтерін орнаттым



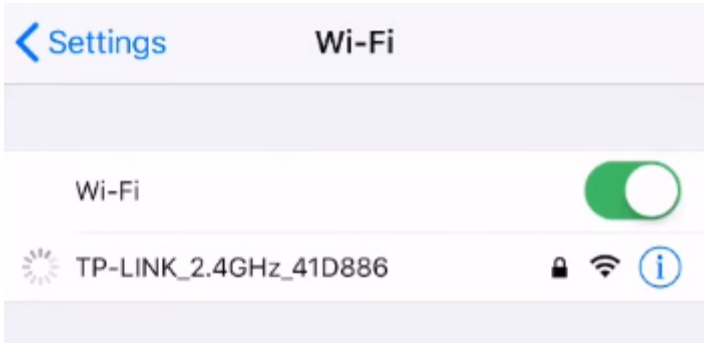
Сурет 3.18 – Radius Server



Сурет 3.19 – Тіркелген пайдаланушы атынан желіге кіріп көреміз



Сурет 3.20 – Желіге кірді



Сурет 3.21 – Желіге кіріп тур

4 Техникалық-экономикалық негіздері

4.1 Жобаның сипаттамасы

Бұл дипломдық жобаның мақсаты жергілікті желілерде ақпаратты қорғауды жобалау болып табылады.

Бұл жобаны мамандар тобы жүзеге асыру жоспарлануда. Топқа жоба жетекшісі, жүйелік әкімші кіруі тиіс.

Жоба жетекшісі жұмысты орындаудың толық күнтізбелік кестесін жобалауға және оның сақталуын бақылауға көмек көрсету, бітіру біліктілік жұмысының жоспарын жасауға көмек көрсету, әңгімелесу мен консультациялар өткізу, орындалған бітіру біліктілік жұмыстарын бөліп, сондай-ақ тұтастай тексеруге тиіс. Жүйелік администратор-әзірлеуші теориялық негіздемені дайындап, жобаны жасап, алгоритмді және интерфейсті идеологияны әзірлеуі тиіс. Осылайша, жүйелік администратор-жобалауға жоспарлау жауапкершілігі және жобаны іске асыру үшін жалпы жауапкершілік жүктеледі жүйе администратор-жоба жүйенің бағдарламалық модульдерін іске асыруға, жобаға жұмыс тестілеуін жүргізуге міндетті.

Жобаның техникалық-экономикалық негіздемесі мен менің жұмысымның орындалуы келесідей:

- жобаның күрделілігін анықтау;
- есептеу есептеуді есептейді;
- әзірленген жобаның ықтимал бағасын анықтау
- жұмыс істеудің әлеуметтік-экономикалық нәтижелерін бағалау.(4.1 – кесте).

4.2 Еңбек сыйымдылығы жобалау

4.1-кесте – Еңбек сыйымдылығының қорытынды көрсеткіштері

Жобалау кезеңдері	Осы кезеңдегі жұмыс түрі	Жобалаудың еңбек сыйымдылығы, адам. х ч.
1	Міндеттер қою	12
2	Техникалық тапсырманы жобалау және бекіту	13
3	Жобаның қазіргі әдістерімен танысу	14
4	Әдебиетті таңдау және зерттеу	22
5	Кешенді қорғау жобасының әртүрлі әдістеріне талдау жүргізу	18
6	Тестілеу	15
7	Бағдарламалық жобаның теориялық бөлігін рәсімдеу	19

4.1 кестенің жалғасы

8	Бағдарламалық жобаның эксперименттік бөлігін әзірлеу	32
9	Жоба ортасын таңдау	13
10	Математикалық есептеулерді жобалау	15
11	Жобаны іске асыру	49
12	Қолданбаны баптау	17
13	Есепті ресімдеу және атқарылған жұмыс туралы қорытынды жасау	15
ЖИЫНЫ	Жобалық жұмысты орындаудың еңбек сыйымдылығы	256

Нәтижесінде бағдарламалық қамтамасыз етуді іске асыру үшін 32 жұмыс күні қажет. (256:8)

4.3 Жобалау шығындарын есептеу

Өзіндік құнды есептеу ЛЖ жобалау кезінде жұмсалған шығыстар бойынша жүргізіледі. Жобалау жұмыстарын жүргізуге кететін шығындар өндіріс алдындағы шығындарға жатады-бұл жобалауды орындайтын барлық жұмыстарға арналған бір реттік шығындар.

Шығындар өзіндік құн калькуляциясының баптарын қосу жолымен анықталады:

- материалдар;
- ғылыми және тәжірибелік жұмыстарға арналған арнайы жабдықтар;
- заработная плата
- еңбекақы төлеу қорына есептеу
- басқа да тікелей шығындар
- үстеме шығыстар.

Материалдық шығындарды есептеу 4.2 кестеде берілген нысан бойынша жүргізілед

4.2-кесте – Материалдық ресурстарға шығындар

Материалдың атауы	Бірлік өлшеу	Саны	Бағасы теңгемен бірлік	Сомасы теңгемен
Кеңсе қағазы	Буып-түю	1	1 200	1200,00
Дәптер (80 бет)	Дана	2	150	300,00

4.2 кестенің жалғасы

Қалам	Дана	2	135	300,00
Компьютерлік тышқан	Дана	1	4000	4000,00
Жиыны:				5800,00

Материалдық құралдарға ($З_м$) қажетті жалпы соманы мынадай формула бойынша есептеуге болады:

$$З_м = \sum P_i * Ц_i, \quad (4.1)$$

мұнда Р_і-материалдық ресурстың і түрінің шығысы, заттай бірліктер;

$Ц_i$ - материалдық ресурстың і түрінің бірлігінің бағасы, тг;

і-материалдық Ресурстың түрі;

n-материалдық ресурстар түрлерінің саны.

Бағдарламалық қамтамасыз етуді жобалау үшін Lenovo IdeaPad Legion Y720 ноутбук қолданылады . Өнім бағдарламасын тестілеу үшін орнатылған операциялық жүйесі бар ДК қажет болады. Windows 7/8/10 нұсқалары. Ноутбукке сым арқылы қосылу үшін смартфон қажет.

Қажетті жабдықтар мен бағдарламалық қамтамасыз ету шығындарын есептеу 4.3-кестеде келтірілген нысан бойынша жүргізіледі [14].

4.3-кесте – Жоба үшін қажетті жабдық пен БҚ шығындарын есептеу

Материалдық ресурстың атауы	Бірлік өлшеу	Осы материалдан шығыстар саны	Бірлік бағасы, тг	Жиыны, тг
MS Windows 10 операциялық жүйесі бар дербес компьютер	дана	1	130 000	130 000,00
Ноутбук Lenovo IdeaPad Legion Y720	дана	1	340 000	340 000,00
POE коммутатор, 8 порт	дана	1	28000	28000,00
Ұялы телефон (iPhone 5s)	дана	1	80000	80000,00
ЖИЫНЫ				578 000,00

Осы кестеге сәйкес жобаға материалдық шығындар 578 000,00 теңгені құрайды.

Электр энергиясын тұтынусыз Жергілікті желілерді жобалау кезінде электр энергиясына жұмсалатын шығындарды есептеу мәні бар.

4.1-кестеге сәйкес, жергілікті желілерді қорғауды жобалау үшін жүйелік администраторға 256 сағат қажет. Енді 256 сағат ішінде жұмсалатын электр энергиясының құнын есептеу қажет.

$$Э = З_{эл.эн.обор.} + З_{доп.нужды.}, \quad (4.2)$$

мұнда $З_{эл.эн.обор.}$ – жабдықтың электр энергиясына арналған шығындар;

$З_{доп.нужды.}$ – қосымша мұқтаждықтарға электр энергиясының шығындары.

Жабдық үшін қажетті электр энергиясын есептеу мынадай формула бойынша анықталады:

$$З_{эл.эн.обор.} = \sum \boldsymbol{W} * К_{исц} * \boldsymbol{S} * \boldsymbol{T}, \quad (4.3)$$

мұнда W-тұтынылатын қуат, Вт;

$К_{исц}$ -пайдалану коэффициенті ($К_{исц}$ **= 0,7..0,9);**

4.4-кесте – Электр энергиясына шығындар

Аспаптардың атауы	Паспорттық қуаты, кВт	Қуат коэффициенті	Жабдықтың жұмыс уақыты, сағ	Баға ЭЭ тг/кВтч	Сомасы, тг.
Ноутбук	0,5	0,7	256	23,85	2136,96
Жұмыс станциясы	0,4	0,9	256	23,85	2198,02
Ұялы телефон	0,5	0,9	15	23,85	160,99
Дербес компьютер	0,9	0,9	140	23,85	2704,59
POE коммутатор, 8 портов	0,5	0,9	256	23,85	2747,52
Жарықтандыру	0,35	0,7	256	23,85	1495,87
Жиыны:					11443,95

$$З_{эл.эн.обор.} = 11443{,}95(\text{тенге})$$

Қосымша қажеттіліктерге шығыстар электр энергиясына арналған шығыстардың 5% көлемінде жоғары көрсеткіш негізінде есептеледі:

$$З_{доп.нужды} = 5\% * З_{эл.эн.обор.}, \quad (4.4)$$

(4.4) формулаға сәйкес қосымша қажеттіліктерге жұмсалатын шығындарды анықтаймыз.

$$З_{доп.нужды} = 0.05 * 11443 = 572,15(тенге)$$

Барлық есептеулерге сүйене отырып, электр энергиясына толық шығындар құрайды:

$$Э = 572,15 + 11443 = 12015,15\ (тенге)$$

4.4 Еңбекақы төлеу шығындарын есептеу

Жергілікті желілерді қорғауды жобалау үшін, бұрын көрсетілгендей, екі қызметкер қажет:

- жоба жетекшісі – жұмыс уақытын басқару, жұмыс процестерін түзету, үйлестіру, пәндік облысты зерттеу;
- Жүйелік администратор-желінің жұмыс қабілеттілігі мен қауіпсіздігін қамтамасыз ету, тестілеу және сүйемелдеу.

Еңбекақы төлеу шығындарының сомасын келесі формула бойынша есептеуге болады:

$$З_{тр} = \sum ЧС_i * T_i \quad (4.5)$$

мұндағы $ЧС_i$ – қызметкердің сағаттық мөлшерлемесі, тг;

T_i – модельді әзірлеудің еңбек сыйымдылығы, адам×сағ; і-қызметкердің санаты;

n – ПҚ әзірлеумен айналысатын қызметкерлердің саны.

Жобаны іске асыру кезінде жұмыс уақыты

қатысушылардың біркелкі, сондықтан мағынасы белгіленсін часовую ставку әрбір қызметкердің және жалпы көлемі жалақы.

Часовую ставку қызметкерінің есептеуге болады мынадай формула бойынша:

$$ЧС_i = \frac{ЗП_i}{ФРВ_i} \quad (4.6)$$

онда $ЗП_i$ – месячная заработная плата і-ші қызметкердің тг;

$ФРВ_i$ – і жұмыс уақытының айлық қоры, сағат.

Басшының айлық жалақысы 190 000 теңгеге тең және СИС администің айлық жалақысы 140 000 теңгеге тең. Әр қызметкердің сағаттық ставкасын формулаға сәйкес есептейміз (4.6):

$$ЧС_{руководитель} = \frac{190\,000}{22 * 8} = 1\,079{,}54\ тг/ч$$

$$ЧС_{разработчик} = \frac{140\,000}{22 * 8} = 795{,}45тг/ч$$

Басшының сағаттық ставкасы 1 079,54 (тг/сағ) құрайды, еңбек сыйымдылығы 120 сағатқа тең. Жүйелік администратордың сағаттық ставкасы 795,45 (тг/сағ), жобаның еңбек сыйымдылығы 256 сағатқа тең. (4.5) формулаға сәйкес қызметкерлердің еңбекақысына арналған шығындар сомасын есептеуге болады:

$$З_{тр} = 1\,079{,}54 * 120 + 795{,}45 * 256 = 130\,000 + 203\,635 = 333\,635{,}00$$

Еңбек ақы төлеу бойынша шығындарды есептеу (4.5) кестеде көрсетілген.

4.5-кесте. – Жалақыны есептеу

Қызметкердің санаты	Біліктілігі	Еңбек сыйымдылығы жобалау, сағ.	Сағаттық тарифтг/ч	Бағасы, тг.
Басшы	Инженер жобалаушы	120	1 079,54	130 000,00
Жүйелік әкімші	Жүйелік әкімші	256	795,45	203 635,00
Жиыны:				333 635,00

4.5 Әлеуметтік салық бойынша шығындарды есептеу

Қазақстан Республикасының Салық кодексіне сәйкес әлеуметтік салық еңбекақы төлеу қорының 9,5% - ын құрайды. Әлеуметтік салықты келесі формула бойынша есептеуге болады: [5]

$$С_н = (ФОТ - ПО) * 0{,}095 \qquad (4.7)$$

бұл жерде зейнетақы қорына аударымдар ФОТ-дан 10% құрайды.

$$ПО = 333\,635 * 0{,}1 = 333\,63{,}50\ тенге$$

$$С_н = (333\,635 - 333\,63{,}5) * 0{,}095 = 28\,525{,}80\ тенге$$

Есептеу нәтижелері кестеде берілген (4,6):

4.6-кесте – Әлеуметтік салықты есептеу

Қызметкердің санаты	Адамдар саны	Еңбекақы,тг	Зейнетақылардан босату, тг	Әлеуметтік салық, тг
Басшы	1	130 000	13 000	11 115,00
Жүйелік әкімші	1	203 635	20 363,5	17 410,80
Жиыны:				28 525,80

4.6 Негізгі қорлардың амортизациясы және өзге де шығындар

Амортизация нормалары ҚҚ анықтау қажет салық кодексіне сәйкес. ОФ амортизациясын келесі формула бойынша анықтауға болады:

$$A_{\text{г}} = \frac{\text{С}_{\text{об}} * \text{Н}_{\text{а}}}{100} \quad (4.8)$$

мұндағы, $\text{С}_{\text{об}}$ – жабдықтың құны;

$\text{Н}_{\text{а}}$ – амортизация нормасы (амортизация нормасы = 25).

Формула (4.8) ноутбук үшін бір жыл ішінде амортизациялық аударымдар үшін қажетті соманы есептеуге мүмкіндік береді:

$$A_{\text{г}} = \frac{340\,000 * 25}{100} = 85\,000 \text{ тенге}$$

Енді әзірлеу кезеңі үшін амортизация нормасын есептеу қажет:

$$A_{\text{г}} = \frac{85\,000 * 32}{365} = 7452{,}05 \text{ тенге}$$

Осылайша, барлық жабдық үшін амортизация нормасын есептеу қажет. Есептеу нәтижелері кестеде келтірілген (4.7).

4.7 – кесте – ОФ амортизациясы

Наименование оборудования и ПО	Жабдықтармен БҚ құны, тг	Жылдық амортизация нормасы, %	Жыл ішіндегі амортизация сомасы, тг	Жобалау кезіндегі амортизация сомасы, тг
Ноутбук	340 000	25	85 000	7452,05
Ұялы ттелефон	80000	15	12 000	1052,05
Дк	130 000	20	26 000	2279,45
POE коммутатор, 8 портов	28 000	20	7000	613,69

4.7 – кестенің жалғасы

Жұмыс станциясы	40000	20	8000	701,36
Жиыны:			136 000	12098,57

Жергілікті желілердегі қорғауды жобалауға арналған шығындар сметасы.

Барлық берілген есеп-қисаптардың негізінде (4.8) кестеде келтірілген нысанға сәйкес жобалау шығындары сметасын ресімдеу қажет.

4.8-кесте – Жобалауға арналған шығындар сметасы

Шығындар баптары	Сумма, тг
Жабдыққа арналған шығындар	578 000
Электр энергиясына арналған шығындар	12015,15
Еңбекақы төлеу шығындары	333 635,00
Әлеуметтік салықтар	28 525,80
Негізгіқорлардың амортизациясы	12098,57
Мат шығындары. ресурстар	5600,00
Смета бойынша жиыны:	969 874,52

4.7 Жобаның ықтимал (шарттық) бағасын анықтау

Жобаның ықтимал (шарттық) бағасының шамасы. Тапсырыс берушінің (тұтынушының) және Орындаушының экономикалық мүдделеріне жауап беретін деңгейде оның орындалу тиімділігін, сапасын және мерзімдерін ескере отырып. Қолданбалы жобаға арналған шарт бағасы (Цд) мынадай формула бойынша есептеледі:

$$Цд = Знир(1+Р/100), \quad (4.9)$$

(4.8 - кестеден)

Р-жоба рентабельділігінің орташа деңгейі, бұл параметр 25% тең деп қабылдаймыз.

$$Цд = 969\ 874{,}52 * 0{,}25 = 242\ 468{,}63 \text{ тенге}$$

Бұдан әрі қосылған құн салығын (ҚҚС) есепке ала отырып, өткізу құнын анықтау қажет, ҚҚС ставкасы ҚР заңнамалық Салық кодексімен белгіленеді. 2019 жылға ҚҚС ставкасы 12% - ға размерде орнатылған.

Іске асыру құны ҚҚС-ты ескере отырып есептеуге болады мынадай формула бойынша:

$$Ц_р = Ц_д + Ц_д * НДС, \quad (4.10)$$

$$Ц_р = 1\ 212\ 343{,}15\ + 1\ 212\ 343{,}15\ * 0{,}12 = 1\ 357\ 824{,}33 \text{ тенге}$$

4.8 Жобаның жұмыс істеуінің әлеуметтік-экономикалық нәтижелері

Бұл жобаның экономикалық мақсаттылығы сандық және сапалы құрамдастардан құралатын болады. Жобалау үшін экономикалық тиімділік дербес жүйелік администратордың да, жобаны іске асырумен айналысатын кәсіпорынның да қаржылық жағдайын жақсартудан тұрады. Осы жобаны сәтті іске асыру кезінде: тікелей жүйелік администратор құрылғы үшін құрылғы алады, қазандық құралы 203 635 теңгені құрайды. Жүйелік администратор үшін сапалы әсер-бұл жобаны нарыққа шығарудың бірінші тәжірибесі, онда әзірлеушілер жобаны әрі қарай жобалау мәселелерін қарастырады, мысалы, жобаның тиімділігі, одан әрі жұмыс негіздерін жобалау. Сондай-ақ жобаны іске асыру барысында жарнама маркетингі, бағдарламалық қамтамасыз ету нарығын игеру мәселелері шешілетін болады.

Бұл жобаның өзіндік құны 969 874,52 теңгені құрады, пайда 242 468,63 теңгеге тең.Осы жобаның Хдсс есебімен іске асырудың ықтимал бағасы 1 357 825

5 Өмір тіршілік қауіпсіздігі

5.1 Жұмыс жағдайларының кодтарын талдау

Өндірістік тәуекелдердің шаңын талдау – бұл әрбір адамның қалыпты жұмыс жағдайын анықтауға бағытталған шаралар кешенінің бағасы, сондай-ақ адам денсаулығына зиян келтіретін және еңбек жағдайында адамның күндізгі кодексінің өміріне әсер ететін осы факторлардың екеуін анықтау.

Бұл жобаның жобасы жергілікті желідегі ақпараттық қауіпсіздікті жобалауға арналған. Дизайн бағасы жоғары жабдықтың және электронды жабдықтардың компьютерлік түрлерін пайдалану арқылы жүзеге асырылады. Қаралып отырған бөлмеде бір қызметкер болған кезде жұмыс орныңыз.

Жұмыс істеген кезде, әзірлеуші оған қауіп төніп тұрса да, бірнеше қауіпті фактор бар:

- электрмагниттік өрістердің әсер етуі;
- бөлменің екі жарықтылығы жеткіліксіз;
- қанағаттанарлықсыз, бірақ бұл бөлмедегі микроклимат.

Қауіпсіздік кодының және санитарияның өндірістік желісінің инженерлік кодексінің ережелерін сақтамау, қауіпсіздік техникасын дұрыс іске асыру авариярға немесе өндірістік жарақатқа әкелуі мүмкін.

Компьютермен жұмыс істегенде, мен бағдарламашыға қауіпті кодтардың және екі зиянды фактордың ықпалымен кодқа ұшырауын қалаймын. Бұл компьютерлік бағдарламашы жұмыс істеу процесі

Бағдарламашы досының жұмыс қабілетін көрсетудің барлық маңызды түрі. Басқа бір жағдайда, персоналға визуалды кілттің қажетті қабілетіне ие бір маңызды кернеу пайда болады. Ең бастысы, жұмыссыздық, бас ауруы, кодтық шаршау және тітіркену қаупіне наразылық тудырады.

Тиісті түрде жасалынған туын және жұмыс өрісіндегі барлық жарықтандыруды жүзеге асырады, ол көрнекілік тиімділігін арттырады, шаршауды азайтады, жұмыс идеясының жұмысын жақсартады, қызметкерлердің тиімділігіне әсер етеді, бұл қызметкерге оң психологиялық көңіл-күй береді, төменгі қауіпсіздік қауіпсіздігін арттырады жұмыс істейді және ядро жарақаттарын азайтады.

Шабуылдардың жеткіліксіз күндізгі қамтуы жеңіл көрнекі қабілетке әкеледі, қызығушылықты әлсіретіп, ерте басталған шаршаудың пайда болуына әкелді. Тым көп

Ашық қауіпті жарық көзі соқырлықты, шағылыстырумен және ауырсынуды тудырады. Осы бөлімнің жұмыс істеуіне жарық бағасының бүкіл бағыты дұрыс емес болуы мүмкін өткір көлеңкелерге, шағылыс түрлерінің пайда болуына, жұмысшыны шатастыруға. Кодекстің аталған барлық коэффициенттері кодекстердің жоғары немесе кәсіптік аурулардың коэффициенттеріне әкелуі мүмкін, сондықтан сәтте шамдар жарықтың дұрыс есептелуі болып табылады.

Бұл қауіпсіздік талаптарын бұзу дербес компьютерлік базада жұмыс істегенде, ядро қызметкері қолайсыздықты сезінуі мүмкін: көздің барлық ауырсынуын және ауырсынуын, сыртқы көріністің және нервоздың шаршауының басы бар. Белгілі бір адамдарда сахналық снаряд, аппетит, көрнекі қабілеті нашарлайды, бұл ауру аурудың, мойынның, төменгі артқы мәзір мен дене мүшелерінің басқа да органдарынан басталады. Ақаулы шаммен жұмыс жасағанда, бұл жүйкедегі сарқылудың пайда болу қажеттілігі бар.

Жақсы жарықтандырылған жұмыс үстелінде тұрған кезде, осы компьютерлерде отыратын қызметкердің кеңсе көрінісі маңызды. Ең бастысы, сіздің жұмысыңыздың жарықтылығы, тіпті егер сайт жыл бойы болса да, шабуылдардың орнына желінің көзқарастарына зиян келтірсе де, компьютерде болу фактісі шабуыл болды.

5.2 Компьютерден бөлінген сәулелердің адамға әсері

Компьютерден бөлінетін сәулелердің адам ағзасына неге зиянды екенін анықтайық.

Адам ағзасы да электрлік импульстерді шығарады. Олардың көмегімен ми мен жұлынға жүйке үштары арқылы сигналдар келіп түседі, қаңқа бұлшықеті мен жүрек бұлшықеттері азаяды. Жүйке үштары арқылы секундына мыңдаған сигналдар беріледі, сондықтан компьютерден қандай зиян келетінін оңай түсінуге болады, сәулелер электрлік импульс жіберудің қиын жүйесіне әсер етіп, олардың өзара байланысына бөгет келтіруі мүмкін. Оның әсері бір сәтте сезілмейді,ол ағзада жинақталып, мүшелер мен жүйелердің жұмысын біртіндеп нашарлатады.

Екі маңызды жүйе ең осал болып табылады:

а) жүйке жүйесі

ә) жүрек-қан тамырлар жүйесі.

Бұның әсерінен ми сигналдары патологиялық түрде өзгеруі мүмкін. Бұл мидың және жүрек-тамыр жүйесі органдарының бұзылуына себеп болады. Жүрек-қантамыр жүйесінің қалыпты жұмыс істеуі импульстердің когеренттігіне және беріктігіне байланысты. Үйдегі бір немесе одан да көп құрылғылар жүрек жұмысын елеулі бұзылуға алып келмейді, бірақ үнемі сәулелену аритмия мен жүрек-тамыр қабілетінің бұзылуына әкелуі мүмкін. Ұзақ уақыт бойы әсер етуі бас ауруы, мигреньдер, иммунитеттің төмендеуі, депрессия, гормоналды теңгерімсіздік және ұйқының бұзылуына әкелуі мүмкін. Компьютерде көп жұмыс істеу Альцгеймер ауруы, Паркинсон ауруы, қатерлі ісік ауруы және ұрпақты болу жүйесінің бұзылу қаупін арттырады. Сонымен қатар миокард және перикард ауруларына, ағзаның жалпы гормональды фонының бұзылуына, су-тұз алмасуының нашарлауына, гомеостаздың бұзылуына алып келуі мүмкін.

Үй компьютері, ноутбук немесе смартфон зиянды сәуле көзі болып табылады. Компьютерден қанша сәуле алатынымыз түрлі факторларға байланысты: құралдың түрі, пайдалану уақыты, орналасуы.

Кондиционер, егер жұмысшы біреудің бөлмесіне ие болса, онда қызметкердің жақсы микроклиматының бір жылын ұстап тұру керек еді, ол жұмыс уақытының барлық ауыртпалығы кезінде жұмыс үшін қажетті бөлмені оңтайлы күйде орналастырады. Үш адам бөлмені шаңнан шығаруды қажет етеді екі зиянды заттарды білдіретін басқа файл. Шабуылдарды орындау үшін бұл аз мөлшерде, үшеуі өте таза, біреуі таза бөлмеде жүргізіледі. Мұның бәрі, қоспағанда, ластаушы ауа арқылы бөлме шабуылының ауырсынуын болдырмауға мүмкіндік береді. Жабдықта болса да, бұл функциялар әуе файлын бөлу туралы ереже бойынша жекелендірілген болса да назарға алынады. Үш қызметкердің бөлмесінде жұмыс істейтін ең төменгі ауа температурасы кемінде 18 ° С кем емес

Оңтайлы жағдайлардың кодтарын қалыптастыру үшін бірқатар жұмысшылардың еңбек нормалары осы өндіріс микроклиматының барлық нормалары ретінде анықталады. Дербес компьютердің шабуыл шотымен жұмыс жасағанда, SanPin 2.2.2 / 2.4.1340-03:

Жоғарыда суық мезгілде:

- 22-24 ° С температура файлын қалыпқа келтірді;
- рұқсат етілген ядролар - 18-26 ° С;
- ауаның салыстырмалы ылғалдылығы 40-60%;
- рұқсат етілген желі 75%.

Жылы кезеңде:

- температура 23-25 ° С-ге дейін қалыпты;
- рұқсат етілген дос 20-30 ° С;
- ауаның салыстырмалы ылғалдылығы 40-60%;
- қабырғалардың рұқсат етілген ылғалдылығы 55% құрайды.

Олардың кэшті орналасуы қарастырылған (5.1 суретте) сипаттамалары:

- екі қабатты ғимараттың бірінші қабатында орналасқан;
- бір қызметкердің көлемі бір бөлме: ядро ұзындығы 4 м, ені 3 м, биіктігі 3 м;
- жасанды жарықтандыру - шамдар: әрқайсысында 2 шам

Әрқайсысының 2 люминесцентті лампасы (PVLM - 1 × 40);

- визуалды жағдайларға ауыр жұмыстардың ауырлығы жоғары IV санатына жатқызу, ең кішкентай нысан нысанды 1-ден 5 мм-ге дейін бөлетіндіктен;
- жұмыс орындарының саны [15].

5.3 Жасанды жарықтандыруды есептеу

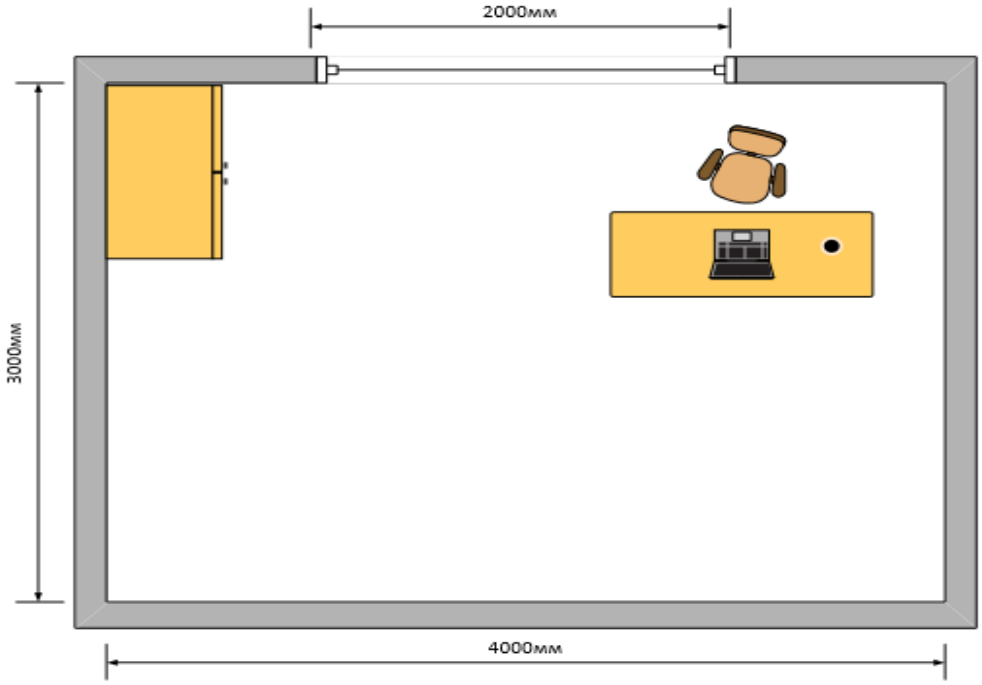
Жасанды жарықтандырудың кілтін жасаған кезде маған бөлме керек, шинаның аумағын, оның тесіктерін анықтау қажет, шамдардың шамасын төменде келтірілген талаптарға сәйкес қалыпқа келтіреді.

Шығару визуалды жұмыс болып табылады - iv.

Қалаған қалыпты жарықтандыру - 400 лкс.

Біз оны өзіміздің флуоресцентті лампалармен бірге жалпы жарықтандыру жүйесін пайдаланамы [15].

Кесте 5.1-де болды. Газ тәріздес лампалардың техникалық сипаттамалары LB болды.



Сурет 5.1 – Операторлық бөлме

Кесте 5.1-газразрядты шамдардың техникалық сипаттамалары ЛБ

Номиналды қуаты, Вт	Номиналды бұл жарық ағыны типті шам ЛБ-40. лм Номиналды қуаты, Вт	Оның шамдардың өлшемдері, мм	
		Диаметр	Ұзындығы үш қаңқаға
40	3000	40	1213.6

Жұмыс бетінің үстінде шамды ілу биіктігін есептейміз:

$$H = h - hp - hc, \quad (5.1)$$

мұнда hc шамдан циклге дейінгі қабырғалардың қашықтығы, hc = 0,05 м;

hp – бұл кеңістіктің үстіңгі қабатының үстіңгі қабатының биіктігінің биіктігі, hp = 0,7 м;

h – осы бөлменің биіктігі, h = 3 м.

$$H = 3 - 0,7 - 0,05 = 2,25$$

Барлығы үшін ең тиімдісі - барлық шамдардың арасындағы айырмашылық:

$$L = \times H \qquad (5.2)$$

мұнда $\lambda = 1,2 \div 1,4$.

$$L = 1,3 \times 2,25 = 2,925.$$

Бір бөлмнің негізгі индексін анықтаймыз:

$$i = (a \times b) / (H \times (a + b \qquad (5.3)$$

мұнда a – бөлменің ұзындығы;
b – ені.

$$i =. (4 \times 3) / (2.25 \times (4 + 3)) = 0.8$$

Бір қабырға мен еден төбесінен әрбір көрінісін коэффициенттері тиісінше тең:

- ρpot = 70%;
- рст = 50%;
- Р қабат = 30%.

Негізгі коэффициентінің мәні - бұл үйдің геометриялық файлдық параметрлері формасын (осы үй-жайдың индексі) бір-бірінің оптикалық сипаттамалары бар ŋ = 40% байланыстыратын кестелер. Барлық қорлардың коэффициенті, егер мәзірге тең болса, k3 = 1,2.

Флуоресцентті лампалардың санын төменде анықтаймыз:

$$N = (E \times k\_3 \times S\_oc \times Z) / (n \times F\_l \times), \qquad (5.4)$$

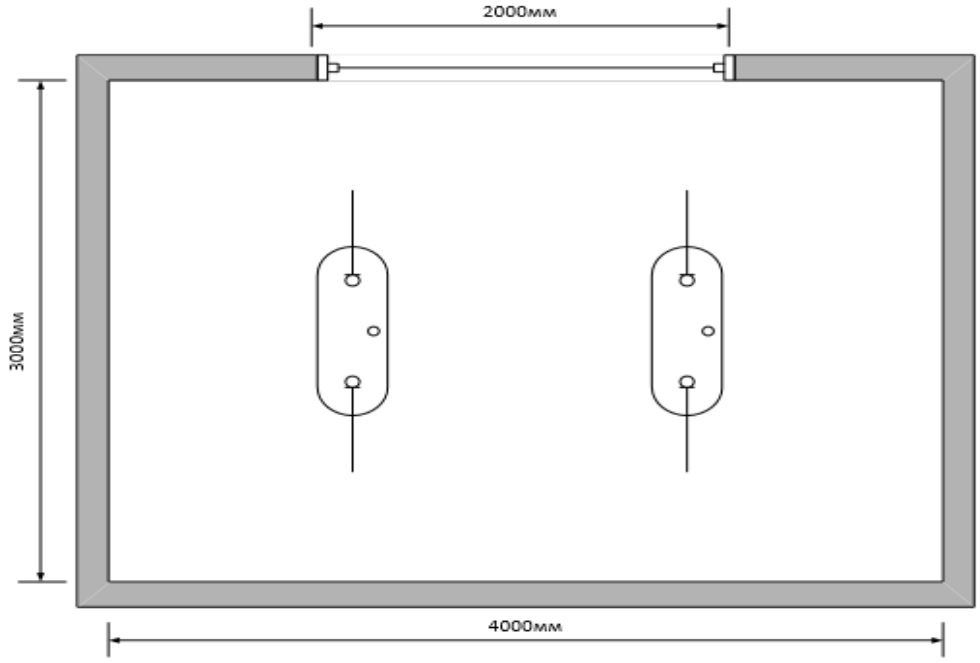
мұнда SOS – бұл үй-жайдың ауданы;
kz – фактор маржа болды, kz = 1,2;
E – барлығына арналған ең төменгі жарықтандыру, E = 200 люкс. ;
Z – бұл біркелкі емес коэффициент жарықтандыру болды, Z = 1.1;
n – шамдағы шам шамдарының саны;
FL – таңдалған лампа файлы болды, FL = 3000 лм;
п – пайдалану коэффициенті, п = 40%.

$$N = (200 \times 1.2 \times 12 \times 1.1) / (2 \times 3000 \times 0.4) = 1.55 \approx 2$$

Бұл 200 люкс қалыпты жарықтандыруды жасау үшін шамдарға арналған 1 ламинамен ПВЛМ сериялары болуы үшін 2 люменің коды қажет, барлығы 2 люминесцентті лампалар, қуат немесе тіпті әрбір лампа файлы кем дегенде 40 Вт болуы керек, бұл шындыққа сәйкес келмейді яғни санитарлық жыл стандарттарына сәйкес келетін барлық жарық жеткіліксіз. Бөлмеде тек 1 люстра орнатылған, бұл санитарлық жылы бұзылған, төменде тағы бір шамды

орнату қажет. Осы идеялардың арқасында жасанды жарықтандыру кем дегенде қайта қалпына келтірілді, соның салдарынан санитарлық нормаларға сәйкес келетін шамдарда 2 лампамен толық ПВЛМ сериясындағы 1 шам ғана болды.

Схема, егер оларда орын берілсе, орналасу орны қажет болған жағдайда 5.2-сурет (үстіңгі көрінісі).



Сурет 5.2 – жарықтық кезіндегі опереторлық бөлмедегі лампа

5.3 Кондиционерлерді есептеу жүйесі

Барлық үй-жайларды кондиционерлеу жабдықтардың барлығында жұмыс істеу үшін ең қолайлы жағдайлар болған жағдайда қамтамасыз етеді.

Біз бұл ғимараттың ішінен алынып тасталатын ауа көлемін анықтаймыз жылу аймағын ұлғайту:

$$L = Q\_izb / (s \times (t\_cut-t\_pr)\ \gamma\_uh), \qquad (5.5)$$

мұнда W – қызыл жылудың артық бағасы,;

c = 0.278 W • h / (kg • -) – ауаның термиялық көздің сыйымдылық тәуекелдігі;

γу = 1.19 кг / м3 – шығыс ауа тығыздығы.

Жылытылған:

$$Qя = Q1 + Q2 + Q3 + Q4, \qquad (5.6)$$

мұнда Q1 – жылу пайдаланылған жабдықтан алынған болса, босату;

Q2 – ЕТҰ-дан жылу кодының түрін шығару;

Q3 – қызметкерлердің жылуы;

Q4 – күн терезесінен жылу ағыны код терезесінен.

Пайдаланылатын жабдықтан жылуды шығару:

$$Q1 = \psi1 * \psi2 * \psi3 * \psi4 * Nn, \quad (5.7)$$

мұндағы ψ1 – екі қолдануға арналған қуат файлдық қатынасы;

ψ2 – жүктеме коэффициенті;

ψ3 – бір мезгілде барлық жабдықтардың жұмыс істеу коэффициенті;

ψ4 – бөлме түріндегі ауаның жылу ассимиляция коэффициенті;

Nnom – барлық жабдықтардың күші номиналды.

Лампалардың коэффициенттерін таңдаған барлық төрт ағынның өнімі 0,25-ке тең болады.

$$Q1 = 0,25 • 1000 = 250 \text{ Вт.}$$

EUT-дан шыққан жылу шығыны:

$$Q2 = \varphi • Nosv, \quad (5.8)$$

мұнда φ – өтпелі энергияның жылу коэффициенті. Барлық флуоресцентті лампалар үшін (LL) φ = 0.6;

Nosv – оператордың барлық бөлмесінің шамының күші - әрқайсысы 40 Вт 2 шам.

$$Q2 = 0.6 • (2 • 40) = 48 \text{ Вт.}$$

Қызметкерлерден жылу бөлінген:

$$Q3 = n • q \quad (5.9)$$

мұнда n – негізгі жұмысшылардың саны;

q – біреудің бұл жылу жоғалуы 116 ваттға тең болды.

$$Q3 = 1 • 116 = 116 \text{ Вт.}$$

Қыздыру шарасының келуі терезеден күн шығып тұрады:

$$Q4 = Fost • q • m \cdot k \quad (5.10)$$

Фост – үш терезенің ауданы, м2;

m – мәзір терезелері бар орындардың саны;

k – түзету коэффициентін береді, барлық металлды байланыстыру үшін өзімізді пайдаланамыз, k = 1.25;

q – 1 м2 терезе, q = 224 Вт / м2 көлемінде жылу беру.

$$Q4 = 3 • 224 • 1 • 1.25 = 840 \text{ Вт.}$$

Ашық өріс арқылы шығарылатын жылу коды формуласымен анықталды.

$$Qя = Q1 + Q2 + Q3 + Q4 \quad (5.11)$$

$$Qя = 250 +48 +116 +840 = 1254 \text{ Вт.}$$

Файл әрбір бөлмеден шығатын жылу формула бойынша анықталады:

$$Quh = \lambda \bullet S \bullet (tvn - tn) / \delta, \quad (5.12)$$

λ = 1 Вт / м • ℃ – барлық негізгі қабырғалардың жылу өткізгіштік қасиеті;

S = 4 • (6 + 4) = 40 м2 – бұл досдың беті жылу шығысынан жоғары.

tвн - оператор ішіндегі қабырғалардың температурасы:

- жазғы формада 24 ℃;
- Қысқы файл 21 ℃.

tн - ғимараттың сыртындағы температура торабы:

- жазда 28 0С желісінде;
- қыс мезгілінде 10 0С.

δ = 0,4 м – барлық қабырғалардың қалыңдығы.

Бір формуланы барлық адамдар үшін пайдаланып, жазғы кезеңде, сондай-ақ қысқы кезеңде жылы болғанын анықтадық.

Жазғы шаң кезеңіне арналған файлды анықтаңыз:

$$Қызба = Қя – Кух \quad (5.13)$$

мұнда Q uh = 0.

$$Q \text{ гардерлері} = 1254 - 0 = 1254 \text{ ватт.}$$

Біз қысқы кезеңдегі желіні анықтаймыз:

$$Қызба = Қя – Кух \quad (5.14)$$

$$Q \text{ yf} = 1 \bullet 40 \bullet (21 - 10) / 0.4 = 660 \text{ Вт;}$$

$$Q \text{ huts} = 1254 - 660 = 594 \text{ Вт.}$$

Бөлмедегі жұмыс кэшінен тазаланған ауа көлемі анықталған кілт болып табылады.

Есептеулер тек формулаға сәйкес жасалады (6.5).

Жазда:

$$L = 1254 / (0,278 \times (28 - 24) \times 1,19) = 947,7 \text{ м3 / сағ.}$$

Қыста:

$$L = 594 / (0,278 \times (21 - 10) \times 1,19) = 163,2 \text{ м3 / сағ.}$$

Сондықтан ауа алмасу тең:

$$n = L \bullet / V \qquad (5.15)$$

мұндағы V – кеңістіктің көлемі, м3.

$$V = 4 \bullet 3 \bullet 3 = 45 \text{ м3}.$$

Жазда:

$$n = 947.7 / 45 = 21 \text{ рет}.$$

Қыста:

$$n = 163.2 / 45 = 3.63 \text{ есе}.$$

Оның санына сай, менің бөлмем үшін кем дегенде жылу алудың ең жоғары коды, салқындатқыштың нысаны осы суық өнімділіктің ең жақын көрінісі арқылы таңдалады. Көптеген максималды құнды файлдар үшін, біз осы санның жазылуын жазғы кодекс кезеңінде жылу болатынбыз. Суықтың екі қорын ескере отырып, кондиционеріңізді таңдаңыз.

Барлық сипаттамаларға сай, біздің «Tcl-TCH-07CHS / XA21» кондиционерлеріміз біздің қабырғамыздан жоғары. Суық ауа баптағышының кодтық кодының жұмысы осы маусымда әр мезгілде біздің бөлмелерде де өндірілетін артық ыстықтың мөлшерінен асып түседі.

Біз ауаны баптау құрылғыларының қажетті шабуылдарының саны боламыз деп үміттенеміз.

Формула бойынша:

$$n = Lnorm / Lqsh. \qquad (5.16)$$

мұнда Lq – таңдалған кондиционерден жоғары нәтиже.

$$n = 947.7 / 2100 = 0.45\text{-}1.$$

Ішкі блок қабырғаға биіктігі 2,5 метр биіктікте, яғни жұмыс аймағынан жоғары орналасқан.

«TCL TAC-07CHS / XA21» бір кондиционерінің техникалық сипаттамалары 5.2-кестеде келтірілген.

Оның сыртында, терезе терезенің астына орнатылады, одан ішкі бөлікке фреонды типті түтікшені, барлық тесіктерді жүргіземіз, одан кейін құбырларды кабельдер мөрленеді. Егер кәрізге қосылған болса, құрылғының ішінен конденсатты ағызу үшін дренаж кодын орнатамыз

5.2-кесте – кондиционер параметрлері

Параметрлер атауы	Нормалары
Эл. Тамақтану,×ф×Гц	230×1×50

Суық бойынша өнімділігі, Вт	2100
Тұтыну ток болуы, А	3,6
Ылғалды жою (max), л/4	1,5
Жылу өнімділігі, Вт	2200
Ішкі коды блок	
Ауа кэшінің шығыны (max), м3/ч	1345
Өлшемдері д×в×г, мм	750×270×175
Сыртқы блок	

5.2-кестенің жалғасы

Шығын ауа кодтары (max), м3/ч	950
Өлшемдері д×в×г, мм	660×500×230

Нәтижесінде, мен жасаған барлық есептеулердің түйінін, қажетті желілік параметрлерді есептедім, бір кондиционерді таңдадым.

Қорытынды

Бұл шарада осы жұмыс үшін оңтайлы жағдайларды талдау, бағдарламаны әзірлеу үшін немесе қажетті қауіпсіздік шаралары карталарының идеялары келтірілген [15].

Сондай-ақ, бөлмеде ауа жинағы үшін қажетті отыру параметрлері қарастырылды. Сондай-ақ, бұл жарықтандыру бір жыл бойы талданды, егер бағдарламаның дамуы, яғни жасанды жарықтандыру есептеуі бойынша, кілтінің нәтижесі бойынша шамдар 200 люкс стандартты жарықтандыру жасау үшін жасалуы мүмкін болса, сізге 2 жарық Шамда 1 лампа файлы бар ПВЛМ түрі, барлығы 2 люминесцентті лампалар, әрбір шамға арналған қуат кемінде 40 Вт болуы керек. Сондай-ақ, бөлмеде нормаланған температураны ұстап тұру үшін, ауа баптағышында бағаның қажеттілігі есептелді, ол файл 12 метрлік негізгі қызмет үшін есептелетін файл болып есептелді, ал TCL TAC-07CHS / XA21 кондиционері қолайлы ауа ағыны ретінде таңдалды. Нәтижесінде, бұл ауыртпалықты қызметкерлердің еңбегі үшін жақсы жағдайға ие файлдық файлы бар екеніне сенімді бола аласыз.

Қорытынды

Жақын арада есептеуіш техника құралдары, бағдарламалық жабдықтау және желілік құрылғының даму аумағындағы прогресс қауіпсіздікті қамтамасыз ету құрылғыларының дамуына түрткі беріп, ақпараттық қауіпсіздігінің бар ғылыми парадигмасын қайта қарауын талап етеді. Қауіпсіздікті жаңадан қараудың негізгі ережелері:

- компьютер жүйелері қауіпсіздігінің бұзылу себептерін талдау мен зерттеу;
- бағдарламалық және аппараттық құралдардың қазіргі даму деңгейіне сонымен қатар, зиянкестер мен бағдарламалық құралдарды бұзушылардың мүмкіндіктеріне сай, нәтижелі қауіпсіздік модельдерін құрастыру;
- икемді басқару мүмкіндігі, қойылатын талаптарға, мүмкін болатын тәуекел мен ресурс шығындарына сай қауіпсіздігі бар қазіргі есептеуіш жүйелеріне қауіпсіздік модельдерін дұрыс ендіру тәсілдері мен құралдарын құрастыру.

Тестілік әсер етуді (шабуылдарды) жүзеге асыру көмегімен компьютерлік жүйе қауіпсіздігін талдау құралдарын құрастыру қажеттілігі.

Мемлекеттерді және ҚР субъектерін қазіргі егемендендіруі, әскери жанжалдың жалғасуы, мемлекеттерді бір біріне территориялық, экономикалық және т.б. ниеттену әрекеті, жеке азаматтар мен мемлекеттік құрылымдарға қатысты терроризм қаупінің өсуі жағдайында есептеуіш жүйелерді қосатын маңызды мелекеттік тұлпатерді басқару мерзімінде ақпаратты сенімді қорғау мәселелері алда тұр. Бұл кәсіпорынның жергілікті желісінде ақпараттық қауіпсіздікті қамтамасыз етудің теориясы мен тәжірибесінің ары қарай дамуын, ақпараттық соғыс (күрес) жағдайы өскен кезде құпиялы ақпаратты өңдеудің заманауи жүйелерін қолдану сенімділігін арттыру қажеттілігін талап етеді.

Қоғамды кеңінен ақпараттандыру, мемлекетік маңызды тұлпаерді басқару саласына компьютерлік құрылғыны ендіру, ақпараттық құрылғыларда оң жетістікпен қатар ғылыми-техникалық прогресс қарқынының өсуі құпиялы ақпараттың жайылып кетуінің алғышарттарын тудырады.

Мақсаты жергілікті желідегі ақпаратты қорғау бойынша жалпы ұсыныстарды құрастыру және ақпараттың қауіпсіздігін қамтамасыз ететін басқару құжаттар пакетін жасау болып табылатын дипломдық жұмыста, келесідей нәтижелер алынды:

- деректерді өңдеу жүйелеріндегі ақпаратқа рұқсатсыз кіруден қорғаудың негізгі жолдары қарастырылған;
- ақпаратты қорғау тәсілдері мен құралдарының дәреже иденфикациясы жасалынды;
- Локальді желілерде ақпаратты қорғау тәсілдерінің толық талдауы жүргізілді;
- ЛЖ-дегі ақпаратты қорғаудың негізгі бағыттары қарастырылған.

Әдебиеттер тізімі

1. Золотов, С.Н. Протоколы Internet / С.Н. Золо-тов. - СПб.: BHV-Санкт-Петербург, 2002. - 212 с.

2. Олифер, В.Г. Компьютерные сети. Принципы, технологии, протоколы / В.Г. Олифер, Н.А. Олифер. –СПб.: Питер, 2000. - 672 с.

3. Таненбаум, Э. Распределенные системы. Принципы и парадигмы / Э. Таненбаум. - СПб.: Питер, 2003. - 877 с.

4. Кулаков, В.Г. Модели процессов реализации угроз и противодействий им в информационно-телекоммуникационных системах (региональный аспект) - Воронеж, 2003. - 136 с.

5. Питерсон, Дж. Теория сетей петри и моделирование систем: Пер. с англ. / Дж. Питерсон - М.: Мир, 1984. - 244 с.

6. Зыбарев, Ю.М. Спецификация и моделирование распределенных информационных систем на основе сетей проблемы информатики. - 2008. - № 1. С. 17-21.

7. Аманжолова К. Б., Алибаева С. А. Экономика предприятии телекоммуникации: Учебно пособие. – Алматы: АИЭС, 2003.

8. Дюсебаева М. К. «Безопасность жизнедеятельности. Методические указания к выполнению раздела в дипломных проектах». – Алматы: АИЭС, 2005г.

9. Щербаков, А.Ю. Современная компьютерная безопасность. Теоретические основы. –М.: Вильямс, 2007

10. Ярочкин, В.И. Информационная безопасность. Учебник для вузов. Фонд "Информационная безопасность: - СПб.: БЧИ-Петербург, 2002.

11. Герасименко В.А., Малюк А.А. Основы защиты информации. – М.: Вильямс 2007.

12. Раторгуев С.П. Программные методы защиты инфоормации в компьютерах и сетях. -М.: Яхтсмен, 1995.

13. Соколов А.В., Степанюк О.М., Защита от компьютерного терроризма. –СПб.: БЧИ-Петербург, 2002.

14. Спесивцев А.В., Защита информации в персональных ЭВМ. - М.:Мир, 1995.

15.Мафтик С. Механизмы защиты в сетях ЭВМ. -М.:Мир, 1995.