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

«ҚОРҒАУҒА ЖІБЕРІЛДІ»
Кафедра меңгерушісі т.ғ.к., доцент Бердібаев Р.Ш.
(ғылыми дәрежесі, атағы, аты-жөні)
_____ «_____» _____ 2020 ж.
(қолы)

ДИПЛОМДЫҚ ЖОБА

Тақырыбы: Microsoft Windows Server құралдары арқылы қауіпсіздік профилін құру

Мамандығы: 5В100200 – «Ақпараттық қауіпсіздік жүйелері»
Орындаған: Мухамедкулов Исламбек Адилович Тобы: СИБк-16-1
(аты-жөні)
Ғылыми жетекші: т. ғ. к. профессор Маргаров Геворг Иванович
(ғылыми дәрежесі, атағы, аты-жөні)
Кеңесшілер:
Мамандығы бойынша:
аға оқытушы Дмитриева Маргарита Валерьевна
(ғылыми дәрежесі, атағы, аты-жөні)
_____«_____»_____ 2020 ж.
(қолы)
Тіршілік қауіпсіздігі бөлімі бойынша:
доцент Жандаулетова Фарида Рустембековна
(ғылыми дәрежесі, атағы, аты-жөні)
_____«_____»_____ 2020 ж.
(қолы)
Мөлшер бақылаушы:
аға оқытушы Альмуратова Камшат Бимуратовна
(ғылыми дәрежесі, атағы, аты-жөні)
_____«_____»_____ 2020 ж.
(қолы)
Пікір беруші:
Төлеулиев Сырым Бимуратович
(ғылыми дәрежесі, атағы, аты-жөні)
_____«_____»_____ 2020 ж.
(қолы)

Алматы 2020

ҚАЗАҚСТАН РЕСПУБЛИКАСЫ БІЛІМ ЖӘНЕ ҒЫЛЫМ МИНИСТРЛІГІ
«ҒҰМАРБЕК ДӘУКЕЕВ АТЫНДАҒЫ 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: Мухамедкулов Исламбек Адилович
(аты-жөні)

Жобаның тақырыбы: Microsoft Windows Server құралдары арқылы қауіпсіздік профилін құру

2019 ж. «11» қараша № 56 университет бұйрығымен бекітілді.

Аяқталған жұмысты тапсыру мерзімі: « 1 » маусым 2020 ж.

Жобаға алғашқы деректер (талап етілетін зерттеу (жоба) нәтижелерінің параметрлері және зерттеу нысанының алғашқы деректері):

1. BitLocker шифрлау бағдарламасы
2. Microsoft Windows Server VPN қызметі
3. Microsoft Windows 10 операциядық жүйесі
4. Microsoft Windows Server 2012 R2 оперциялық жүйесі

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

Кіріспе
1.Профиль ұғымы
2. Қауіпсіз байланыс және деректерді шифрлау туралы түсінік
3. Практикалық бөлім
4. Техникалық және физикалық қорғау
5. Өміртіршілік қауіпсіздігі бөлім
6.Ақпараттық қауіпсіздіктің тәуекелдерін есептеу
Қорытынды
Әдебиеттер тізім

Графикалық материалдардың (міндетті түрде дайындалатын сызбаларды көрсету) тізімі:

1. Виртуалды қорғалған VPN желісі
2. Туннельге дайындалған пакеттің мысалы
3. Виртуалды қауіпсіз тіннельдің схемасы
4. Қауіпсіздікті ықтимал бұзушының моделін әзірлеу
5. «Server Roles» қойындысына «Remote Access» ролын таңдау
6. Маршруттауды және қашықтан қатынауды баптау және қосу
7. Тор және жалпы қатынауды басқару орталығы
8. Қосылу немесе желі тұнбалары
9. Шифрлеу үшін дискінің көлемін таңдау
10. Тарау бойынша қорытындылар

Негізгі ұсынылатын әдебиеттер:

1. Станек, Уильям Р. Microsoft Windows Server 2012. Справочник администратора. - М.: БХВ-Петербург, 2014. - 843 с.

2. Девянин, П.Н. Анализ безопасности управления доступом и информационными потоками в компьютерных системах / П.Н. Девянин. - М.: Радио и связь, 2006. - 176 с.

3. Рэнд, Моримото Microsoft Windows Server 2012. Полное руководство / Моримото Рэнд. - М.: Диалектика / Вильямс, 2013. - 791 с. Станек, У. Microsoft Windows Server 2012 R2. Хранение, безопасность, сетевые компоненты. Справочник администратора / У. Станек. - М.: БХВ-Петербург, 2015. - 445 с.

4. Защита компьютерной информации от несанкционированного доступа. А. Ю. Щеглов. – СПб.: Издательство «Наука и Техника», 2014. – 384 с.

Жоба бойынша жобаның бөлімдеріне қатысты белгіленген кеңесшілер

Бөлімдері	Кеңесшілері	Мерзімі	Қолы
Негізгі бөлім	Маргаров Г.И.	03.03.2020ж	
А.Қ.Т.Е.	Дмитриева М.В.	20.04.2020ж	
Нормабақылаушы	Альмуратова К.Б.	02.06.2020ж	
Ө.Т.Қ.Н.	Жандаулетова Ф.Р.	13.04.2020ж	

Диплом жобасын дайындау
КЕСТЕСІ

Бөлімдердің атауы, әзірленетін мәселелердің тізімі	Ғылыми жетекшіге ұсыну мерзімдері	Ескерту
1. Профиль ұғымын талдау	25.02. 2020ж.	
2. Қауіпсіз байланыс және деректерді шифрлау түсінігін талдау	25.02. 2020ж.	
3. VPN технологиясының ақпараттық қауіпсіздігін талдау шаралары	25.02. 2020ж.	
4. Құпия ақпараты қорғау үшін шифрлауды қолдану шаралары	30.04. 2020ж.	
5. Тарау бойынша қорытындылар	30.04. 2020ж.	
6. Ұйымдастыру шаралары	30.04. 2020ж.	
7. Виртуалды қорғалған VPN желілерін құру	30.04. 2020ж.	
8. BitLocker арқылы деректерді шифрлау шаралары	30.04. 2020ж.	
9. Өміртіршілік қауіпсіздігі бөлімі	10.05. 2020ж.	
10. Есептеу бөлімі	10.05. 2020ж.	
11.А.Қ.Т.Е.	10.05. 2020ж.	
12. Қорытынды	20.05.2020ж.	

Тапсырманың берілген уақыты «12» ақпан 2020 ж.

Кафедра меңгерушісі: _____ (Бердібаев Р.Ш.)
(қолы) (аты-жөні)

Жобаның
ғылыми жетекшісі: _____ (Маргаров Г. И.)
(қолы) (аты-жөні)

Орындалатын тапсырманы
қабылдаған студент: _____ (Мухамедкулов И. А.)
(қолы) (аты-жөні)

Аңдатпа

Бұл дипломдық жобада Microsoft Windows Server көмегімен қауіпсіздік профилін құру және VPN-байланысы арқылы құнды деректерді беру кезінде шифрлау мен құпиялылықтың көмегімен мәліметтерді қорғауды қамтамасыз ету қарастырылады.

Өміртіршілік қауіпсіздігі бөлімінде еңбек шарттары талданды және анықталды, электромагниттік өрістің жоғары және өте жоғары жиіліктерінің әсерлерін қалыпқа келтіру, сонымен қатар жерге тұйықтау есептеулері жүргізілді.

Тәуекелдерді бағалау бөлімінде барлық анықталған ресурстар бойынша тәуекелдерге талдау жүргізілді және ақпараттық жүйені қорғау шаралары анықталды.

Анотация

В данном дипломном проекте рассматривается построение профиля безопасности средствами Microsoft Windows Server и обеспечение защиты данных с помощью шифрования и конфиденциальности при передаче ценных данных через VPN-соединение.

В разделе Безопасность жизнедеятельности были проанализированы и определены условия труда, проведена нормализация воздействия высоко-и высоких частот электромагнитного поля, а также расчет заземления.

В разделе оценки рисков проведен анализ рисков по всем выявленным ресурсам и определены меры защиты информационной системы.

Annotation

This thesis project focuses on building a security profile using Microsoft Windows Server and ensuring data protection with encryption and privacy when transferring valuable data over a VPN connection.

In the section life Safety, working conditions were analyzed and defined, the impact of high-and high-frequency electromagnetic fields was normalized, as well as the calculation of grounding.

In the risk assessment section, a risk analysis was performed for all identified resources and information system security measures were defined.

Мазмұны

Кіріспе

Қазіргі таңда IT-индустрия қарқынды дамып келеді. Компания басшылығы шешетін маңызды мәселелердің бірі деректер қауіпсіздігі болып табылады. Деректер қауіпсіздігі деп жеке және корпоративтік ақпараттың сыртқа шығуын болдырмау, ұйымның компьютерлік жүйесіне шабуылдарды көрсету ғана емес, сонымен қатар жүйенің жұмысын тұтастай оңтайландыру да түсініледі. Бір міндетті шешуге орасан зор ресурстар жұмсалған уақыт өтті, ілгерілеу орнында тұрмайды және ең аз ықтимал шығындар кезінде барынша нәтиже алу қажет. Ұйымның қызмет салалары мен құрылымдарының біртектілігі бір әмбебап шешімді таңдау іс жүзінде мүмкін емес. Мұнда ауқымды және кешенді ойлау керек.

Қандай да бір қорғау жүйесін әзірлеуге кіріспес бұрын күзетілетін объектіге жалпы шолу және талдау жүргізілуі тиіс. Шолу және талдау осы объектінің қандай қатерлер мен осалдықтарының бар екендігі, сондай-ақ қандай қорғау әдістерін қолдану қажеттігі туралы мәліметтерді қамтиды.

Дипломдық жобада қорғаныс объектісі ретінде корпоративтік желі қарастырылады. Корпоративтік желі — кез келген ұйым үшін деректерді берудің негізгі ортасы. Бұл желі-кез келген инфрақұрылымның өмір сүру негізі, ол ұйымның барлық құрылымдық бөлімшелерін бірыңғай ақпараттық кеңістікке біріктіреді.

Корпоративтік желіде деректерді қорғау туралы мәселені қарастыра отырып, негізгі проблемалар: деректерді өңдеу, сақтау және беру кезінде қорғау, коммуникация құралдарын қорғау, сондай-ақ ішкі және сыртқы түрлі қауіп-қатерлер болып табылады. Ақпаратты қорғаудың кешенді жүйесі ұйымдық, техникалық, бағдарламалық, аппараттық және бағдарламалық-аппараттық қорғау құралдарын біріктіреді. Дипломдық жобаның мақсаты VPN виртуалды қорғалған желіні құру және құнды деректерді беру үшін BitLocker арқылы деректерді шифрлеу.

1 Профиль ұғымы

1.1 Пайдаланушы профильдері және оларды басқару

Кез келген компанияда, ұйымның негізгі бөлігі IT-инфрақұрылымында пайдаланушылар деп аталатын қызметкерлер болып саналады. Әрбір пайдаланушы жұмыс үстелінің фонын, экрандық заставканы және басқа элементтерді жекелендіру үшін пайдаланушы профильдері қолданылады. Шын мәнінде, пайдаланушылардың профильдері пайдаланушылардың есептік жазбаларынан ерекшеленеді, пайдаланушы профильдері пайдаланушының операциялық жүйеге әрбір кіруінде дербес параметрлерді қолдануға мүмкіндік береді, ал пайдаланушылардың есептік жазбалары сияқты жүйеге кіру үшін пайдаланылмайды. Профильдер жүйелік әкімшілер үшін де, соңғы пайдаланушылар үшін де бірқатар артықшылықтарды ұсынады. Мысалы, әкімші өз міндеттеріне сәйкес келетін әдепкі пайдаланушы параметрлерін орната алады, жұмыс ортасында жасалған өзгерістерді сақтамайды, сондай-ақ барлық параметрлерді жүйеге кіргенде жергілікті компьютерге жүктейді. Бір компьютер бірнеше пайдаланушыға қызмет ете алады, яғни кіруді орындайтын нақты пайдаланушы оған сақталған толық бапталған жұмыс ортасын алады, және де бір пайдаланушының жұмыс ортасын баптауы басқа пайдаланушының жұмыс ортасының параметрлеріне әсер етпейді. Назар аудару керек, бұл әрбір пайдаланушы тіркелгісінде кем дегенде бір профиль болуы мүмкін.

Көптеген жүйелік әкімшілер өздерінің пайдаланушылары үшін клиенттік сайттарды орналастыру және басқару кезінде пайдаланушылар жұмыс үстелдеріндегі орталықтандырылған басқару сияқты ұсақ бөлшектерді елемейді. Бір жағынан, оларды түсінуге болады, өйткені қолданушылар мұндай әрекеттерді өздерінің жұмыс орындарындағы тек қана бос кеңістікті толығымен бақылау әрекеті ретінде қарастырады, бұл жанжалды жағдайларға әкеледі. Бірақ егер сіз бұл фактіні екінші жағынан қарастыратын болсаңыз, онда пайдаланушыға кез-келген параметрлерді өзгерту мүмкіндігін беру әрекеттері дұрыс емес конфигурацияға әкелуі мүмкін, бұл қандай да бір жолмен жүйелік әкімші ретінде сіздің өміріңізді қиындатуы мүмкін. Пайдаланушының профилін және пайдаланушылық үстелді орталықтандырылған басқаруды теңдестірумен байланысты көптеген нюанстар сіздің ұйымыңыздың корпоративтік ережелеріне байланысты және бұл параметрлерді топтық саясатты қолдана отырып анықтауға болады. Бірақ бәрі корпоративті ережелерде айтылған болса да, пайдаланушылар сізбен үнемі ант береді, өйткені ерте ме, кеш пе олар жұмыс үстеліне әдемі пейзаждың суретін салғысы келеді, сол себепті сіз үнемі мәлімдеме аласыз. Қызметкердің өмірін жеңілдету және жұмыс үстелін жекелендіруге мүмкіндік беру туралы бөлім басшыларының қолы қойылған. Топтық саясатты қолдану, әрине, сіздің өміріңізді жеңілдетеді, сондықтан осы мәселеге қатысты негізгі

міндет пайдаланушыларға жұмыс үстелдерін басқару келесі жұмыс үшін ыңғайлылық беретініне сендіру процесін қамтуы керек [1].

Windows операциялық жүйелерінде профильдердің төрт түрі бар, олардың параметрлерін жүйелік әкімшілер де, соңғы пайдаланушылар да өзгерте алады:

- уақытша пайдаланушының профилі. Егер пайдаланушы жүйелік қатеге байланысты операциялық жүйе кіру кезінде жүктеме алмаса және сәйкесінше пайдаланушы жүйеден шықса, бұл профиль жойылады;
- жергілікті пайдаланушының профилі. Пайдаланушы жүйеге бірінші рет кіретін және жергілікті қатты дискіде сақталатын профиль;
- роуминг пайдаланушысының профилі. Жүйелік әкімші соңғы пайдаланушы үшін арнайы жасайтын және серверде сақталатын профиль. Бұл профильдер пайдаланушының ұйымдағы кез-келген компьютерге кіру арқылы өзінің жұмыс ортасына қол жеткізе алатындығына ыңғайлы;
- пайдаланушының міндетті профилі. Белгілі бір пайдаланушыларға немесе өзгертулерді тек әкімшілер енгізетін пайдаланушы топтарына арналған нақты параметрлерден тұратын роуминг профилі.

Соңғы пайдаланушылар сізден ең алдымен нені қалайды? Олар үшін ұйымның кез-келген компьютерінен жүйеге кірудің ең маңызды сәті - бұл жұмыс үстелінде жеке компьютердегі параметрлермен бірдей сәт, және олар үшін олардың орналасқан жеріне қарамастан, өз деректеріне қол жеткізу өте маңызды. Осы себепті, соңғы пайдаланушыға үшін пайдаланушы профильдерін дұрыс басқару әлдеқайда маңызды әкімшіге арналған қарағанда. Сіз осы функцияның барлығын роумингтегі пайдаланушы профильдерін қолдана аласыз. Бұл мақалада сіз пайдаланушы профильдері туралы мәліметтер, жергілікті және роуминг профильдерінің айырмашылығы, сондай-ақ роуминг профильдері мен топтық саясатты басқару туралы білесіз.

1.2 Пайдаланушы профильдерінің мазмұны

Пайдаланушы профилінің өмірлік циклі әдепкі пайдаланушы профилінің папкасын, яғни Windows жұмыс істейтін кез-келген компьютерде сақталатын Әдепкі пайдаланушы папкасын көшіруден басталады. Пайдаланушы профиліндегі ақпарат HKEY_CURRENT_USER тіркеу тізбегіне сәйкес келеді, оны сіз профиль папкасының түбірінен, атап айтқанда Ntuser.dat файлынан таба аласыз. Бұл файлда операциялық жүйенің конфигурациясының параметрлері, бағдарлама параметрлері, сонымен қатар ағымдағы пайдаланушының жұмыс үстелі бар. Пайдаланушы профилінде сонымен қатар жұмыс үстелінің параметрлері мен бастау мәзірі, қосымшаның конфигурациясы және тағы басқалар сияқты мәліметтерді қамтитын жасырын папкалар, сондай-ақ бастапқыда пайдаланушыға қол жетімді және құжаттарды, музыкалық және бейне файлдарды, Интернеттен жүктелген файлдарды және файлдарды сақтауға арналған папкалары бар.

Сіздердің көпшілігіңіз Windows XP операциялық жүйесіндегі пайдаланушы профильдерінде қандай папкалар орналасқанын және олардың барлығы құжаттар мен параметрлер папкасында екенін білесіз. Бірақ Windows Vista және Windows Server 2008-тен бастап жұмыс істейтін жүйелерде мұндай папка жоқ, бұл осы операциялық жүйелермен алғаш рет жұмыс істейтін адамдар үшін аздап адастырады. Енді барлық қолданушы профильдері Пайдаланушылар папкасында орналасқан және бұрын болмаған пайдаланушыларға қол жетімді көптеген папкалар пайда болды. Мысалы, бәрі бірдей Windows XP операциялық жүйесінде, қолданушы профильдерінде «Менің құжаттарым», «Менің музыкам», «Менің суреттерім» және т.б. сияқты папкалар болғанын есте сақтайды, бұл пайдаланушылар арасында көптеген қызықты қақтығыстар тудырды. және әкімшілер [2]. Енді бұл папкалардың бәрі басқа атауға ие, бұл соңғы пайдаланушылармен кейбір қақтығыстарды болдырмайды. Барлық осы папкалар келесі кестеде берілген.

1.1-кесте – Пайдаланушының стандартты папкалары

Windows Vista/7/Server 2008/2008 R2	Windows XP/Server 2003	Қысқаша сипаттамасы
Contacts (Байланыстар)	Жоқ	Әдепкі бойынша пайдаланушы контактілерін сақтауға арналған папка
Desktop (Жұмыс үстелі)	Desktop	Жұмыс үстелі элементтері бар папка
Documents (Жұмыс үстелі)	My Documents	Әдепкі бойынша барлық қолданушы жасаған құжаттарды сақтауға арналған папка
Downloads (Жүктеулер)	Жоқ	Әдепкі бойынша Интернеттен пайдаланушы жүктеген барлық файлдарды сақтауға арналған папка
Favorites (Таңдаулы)	Жоқ	Internet Explorer таңдаулылары бар папка
Links (Сілтемелер)	Жоқ	Internet Explorer-дің сүйікті сілтемелері сақталған папка
Music (Менің музыкам)	My Music	Пайдаланушының әдепкі музыка файлдарын сақтауға арналған папка
Pictures (Суреттер)	My Pictures	Әдепкі бойынша пайдаланушының сурет файлдарын сақтауға арналған папка
Saved Games (Сақталған ойындар)	Жоқ	Сақталатын папка пайдаланушының әдепкі ойындарына арналған

1.1-кестетің жалғасы

Searches (Іздеу)	Жоқ	Пайдаланушы іздеулерін сақтауға арналған папка
Videos (Менің бейнелерім)	My Videos	Пайдаланушының әдепкі бейне файлдарын сақтауға арналған папка
Virtual Machines (Виртуалды машиналар)*	Жоқ	Әдепкі бойынша пайдаланушының виртуалды машиналарын сақтауға арналған папка (Windows Vista жүйесінде бұл қапшық жоқ)
Қосылу нүктелері		
AppData	Жоқ	Бұл папка жасырылған және ол әдепкі бойынша қолданушы туралы мәліметтерді қамтиды. Бұл қапшықта мазмұны төменде көрсетілген Жергілікті және Роуминг ішкі папкалары, сондай-ақ қорғалған процестерге арналған бағдарлама параметрлерін сақтайтын және роуминг профильдерін қолданған кезде қозғалмайтын LocalLow папкасы бар
AppData\Roaming	Application Data	Осы қосылу нүктесінде қосымшаны жасаушылар анықтайтын бағдарлама деректері сақталады
AppData\Roaming\Microsoft\Windows\Cookies	Cookies	Пайдаланушы туралы ақпарат пен параметрлерді қамтиды
AppData\Local	Local Settings	Осы қосылу нүктелерінде сіз қолданбалы деректер, журнал файлдарын, сондай-ақ роуминг профилінің құрамына кіретін уақытша файлдарды таба аласыз
AppData\Local\Microsoft\Windows\History		
AppData\Local\Temp		
AppData\Local\Microsoft\Windows\Temporary Internet Files		
AppData\Roaming\Microsoft\Windows\Network Shortcuts	NetHood	Бұл қосылу нүктесінде желілік орта элементтеріне арналған сілтемелер бар.

1.1-кестетің жалғасы

AppData\Roaming\Microsoft\Windows\Printer Shortcuts	PrintHood	Бұл түйіспеде принтер папкасындағы элементтер үшін сілтемелер бар
AppData\Roaming\Microsoft\Windows\Recent	Recent	Бұл түйіспеде жақында қолданылған құжаттар мен папкаларға арналған сілтемелер бар
AppData\Roaming\Microsoft\Windows\Send To	SendTo	Бұл түйіспе құжаттама утилиталарына сілтемелерден тұрады
AppData\Roaming\Microsoft\Windows\Start Menu	Start Menu	Бұл қосылу нүктесінде «Бастау» мәзіріндегі бағдарламалар үшін сілтемелер бар.
AppData\Roaming\Microsoft\Windows\Templates	Templates	Бұл қосылу нүктесінде пайдаланушы үлгілері бар.
\Documents	My Documents	Пайдаланушы құжаттары мен ішкі папкаларын қамтиды

Алдыңғы кестеден байқағаныңыздай, пайдаланушының профильдерінде стандартты папкалардан басқа, қосылу нүктелері бар - ортақ папкаларға кіруге мүмкіндік беретін папкалар. Байланыс нүктелері, бір қарағанда, папкаларға ұқсас, бірақ іс жүзінде олар файл сұрауын дискідегі басқа орынға бағыттайтын сілтемені ғана қамтиды. Windows-тың алдыңғы нұсқаларындағы қосымшаларды пайдалану кезінде қосылу нүктелері қосымшаларға Windows Vista және одан жоғары операциялық жүйелердегі пайдаланушы профильдерінде жаңа атауларды қолданатын папкаларға ақпарат жазуға мүмкіндік береді (2-нұсқа).

1.3 Жергілікті және жылжытылатын профильдер арасындағы негізгі айырмашылықтар

Бұрын мен жергілікті және орны ауыстырылатын профильдердің анықтамасын қысқаша сипаттадым. Енді мен егжей-тегжейлі мәнін сипаттаймын, қолдану және осы екі түрі таңдамалы профильдер кейбір айырмашылықтар.

1.3.1 Жергілікті пайдаланушы профильдер

Бұрын айтылғандай, жергілікті пайдаланушы профилі пайдаланушы жүйеге кіргенде әрбір компьютерде жасалады. Бұл профиль %SystemDrive%\User папкасында орналасқан, жаңа пайдаланушының профилі папкасына көшірілетін жасырын Default пайдаланушы профиліне негізделген. Сонымен қатар, пайдаланушының жұмыс үстелінің параметрлерінің кейбір параметрлері оның профильімен ғана емес, сонымен қатар All Users папкасындағы бағдарламалардың жалпы топтарымен анықталады. Пайдаланушы жүйеден шыққан кезде, пайдаланушы орындаған барлық параметрлер профиль папкасында сақталады, ал

Default User папкасындағы профиль өзгеріссіз қалады. Пайдаланушы профильдері SID қауіпсіздік идентификаторларымен байланысты. Сондықтан, пайдаланушы жергілікті компьютерге қайта кіргенде, осы профиль алынады және пайдаланушыға сол жұмыс үстелін береді, ол шығу кезінде сақталған. Егер жергілікті компьютерде пайдаланушыда домендегі есептік жазбадан басқа жеке есептік жазба болса, онда осы есептік жазбалардың жергілікті профильдері өзгеше. Егер компьютер доменге қосылған болса, онда ең алдымен доменді контроллерде NETLOGON жалпы ресурсында орналасқан әдепкі пайдаланушы профилінің желілік нұсқасы тексеріледі [3].

Жергілікті пайдаланушы профильдерінің негізгі артықшылығына жергілікті компьютерге кіретін кез келген пайдаланушы бірегей жеке параметрлерді қолдайды. Мұндай профильдерді үй компьютерлерінде немесе барлық пайдаланушылар жұмыс топтарына кіретін шағын кеңселерде ұстау керек. Бірақ ұйым ішінде пайдаланушылар көптеген компьютерлер арасында орын ауыстырған жағдайда, әрбір компьютердегі профильдердің үлкен санын қолдау сәтті шешім болып саналмайды. Мұндай тапсырманы шешу үшін жылжытылатын пайдаланушы профильдері сияқты шешімді пайдалану мағынасы бар.

1.3.2 Жылжытылатын пайдаланушы профильдер

Орын ауыстыратын пайдаланушы профильдері ұйымда көптеген компьютерлер арасында орын ауыстыратын пайдаланушылар өз профиліне тікелей қол жеткізе алатындай, олардың профильдерінің параметрлерін сақтай отырып, Домен компьютерлеріндегі жүйеге кіруге мүмкіндік береді. Бұл жағдайда барлық пайдаланушы профильдері әкімші белгілеген серверде тікелей орналастырылады. Пайдаланушы жүйеге кіргенде және Active Directory жүйесінде түпнұсқалығын тексергенде, пайдаланушы профилі жергілікті компьютерге көшіріледі. Пайдаланушы өз профиліне енгізетін барлық өзгерістер жергілікті жазылады, сондай-ақ серверде сақталатын пайдаланушы профиліне көшіріледі және жүйеге келесі кіргенде пайдаланылады. Егер домен пайдаланушының есептік жазбасы үшін профилге жол дұрыс көрсетілсе және сервер қол жетімді болса, пайдаланушы жүйеден шыққан кезде оның жергілікті профилінің көшірмесі серверде жергілікті және көрсетілген қалтада сақталады. Тиісінше, пайдаланушының барлық параметрлері мен құжаттары жүйеге кіруіне қарамастан қол жетімді болады. Әдепкі бойынша, профиль көшірмесі жергілікті компьютерде де кэштеледі. Егер пайдаланушы ағымдағы компьютерден кірген болса, онда жергілікті компьютердегі Профильді уақытша белгі NETLOGON жалпы ресурсындағы Профильді уақытша белгімен салыстырылады. Бұл уақытша белгі профильдегі ең жаңа файлдарды анықтау үшін қолданылады. Серверде профилі жергілікті компьютерге қарағанда жаңа болса, бүкіл профиль серверден көшіріледі. Егер сервер қол жетімсіз болса, пайдаланушы жергілікті буферде сақталған жылжытылатын профильдің көшірмесін алады. Ал егер Пайдаланушы

осы компьютерден жүйеге бір рет кірмесе, онда ол үшін жергілікті пайдаланушының жаңа профилі жасалады. Бірінші және екінші жағдайда, бұл профиль уақытша деп аталады, өйткені пайдаланушы жүйеден шыққан кезде бұл профиль жойылады. Windows Vista операциялық жүйесінен бастап, профильдер қалталарының құрылымы қатты өзгерді, сондықтан аралас ортада, сіз пайдаланушы профильдерін іске асыруды мұқият жоспарлауыңыз керек.

Мұндай жолмен пайдаланушының міндетті профилдерімен жұмыс ұйымдастырылған. Міндетті және орын ауыстыратын профильдер пайдаланушылар тобы үшін функционалдығы шектеулі жұмыс үстелінің стандартталған конфигурациясын жасау мақсатында бірге пайдаланылады. Міндетті профильдер келесі сценарийде пайдалану керек. Мысалы, ұйымыңызда жұмыс үстелін дербестендіру мүмкіндігін шектейтін топтық саясатты таратумен бірдей операцияларды орындайтын бөлім бар. Бұл жағдайда пайдаланушылар конфигурациясын өзгерте алмайтын осы пайдаланушылар тобы үшін жалғыз міндетті пайдаланушы профилін жасау керек. NETLOGON құру және ортақ ресурсына бөлгеннен кейін мұндай бейінге алынған NTUSER атын өзгерту керек. NTUSER-де DAT.MAN және тек оқу үшін рұқсаттарды тағайындау, содан кейін жылжитын профиль ретінде оны баптау қажет. Нәтижесінде, пайдаланушы профильді серверде профиль өзгерістерін енгізбейді.

Орын ауыстыратын профильдерді жоспарлау кезінде сізге міндетті профильдермен қатар уақытша пайдаланушы профильдерін қолдану жағдайын талдау қажет. Егер Профильді сервер қол жетімсіз болса, міндетті профильдері бар топқа кіретін пайдаланушылар жүйеге кіре алмайды. Арнайы осы жағдайлар үшін сізге қосымша, жақсартылған қауіпсіздік деңгейін қамтамасыз етуге мүмкіндік беретін орны ауыстырылатын профильдер қолжетімсіз болған жағдайда пайдаланушыларға компьютерлерге кіруге тыйым салатын мәжбүрлеу профильдерін жасау қажет [4].

1.4 Топтық қауіпсіздік саясаты

Топтық саясат – бұл қабылдау және жіберу жұмыс ортасын (Windows, X-unix және желіні қолдайтын басқа операциялық жүйелер) баптау жүргізілетін ережелер мен параметрлер жиынтығы. Топтық саясат доменде құрылады және домен шеңберінде репликацияланады. Топтық саясат объектісі (Group Policy Object, GPO) екі физикалық бөлек құрамнан тұрады: топтық саясат контейнері (Топ Policy Container, GPC) және топтық саясат үлгісі (Group Policy Template, GPT). Бұл екі компонент топтық саясат объектісінің құрамына енгізілетін жұмыс ортасының параметрлері туралы барлық деректерді қамтиды. GPO нысандарын Active Directory каталогындағы объектілерге ойластырылған қолдану Windows операциялық жүйе базасында тиімді және оңай басқарылатын Компьютерлік жұмыс ортасын құруға мүмкіндік береді. Саясат Active Directory каталогының иерархиясы бойынша жоғарыдан төмен қарай қолданылады.

1. Топтық саясат жасау. Әдепкі бойынша, Active Directory каталогы иерархиясында екі топтық саясат жасалады: Default Domain Policy (домен саясаты әдепкі) және Default Domain Controller ' s Policy (Домен контроллерінің саясаты әдепкі). Олардың біріншісі Домен, екіншісі - домен контроллері кіретін контейнерге тағайындалады. Егер сіз өз GPO нысанын жасау керек болса, сіз қажетті өкілеттіктерге ие болу керек. Әдепкі бойынша жаңа GPO құру құқығына Enterprise Administrators (кәсіпорын әкімшісі) және Domain Administrators (Домен әкімшілері) топтары ие.

2. Топтық саясатты қолдану. Топтық саясаткерлермен жұмыс істей отырып, бұл:

- GPO нысандары тұйықтаушы емес, контейнерлерге қатысты қолданылады;
- бір контейнер бірнеше GPO нысандарымен байланысты болуы мүмкін;
- бір контейнермен байланысты GPO объектілері осы контейнерге қатысты олар тағайындалған тәртіппен қолданылады;
- GPO нысаны екі компонентті қамтиды: компьютерге қатысты параметрлер және пайдаланушыға қатысты параметрлер;
- осы құрауыштардың кез келгенін өңдеуді өшіруге болады;
- GPO нысандарын мұраға қалдыру мүмкін;
- GPO нысандарын мұраға қалдыруға болады;
- GPO нысандарын ACL тізімдері арқылы сүзгілеуге болады.

3. Екі саясаттың қайшылықтарын шешу. Кейбір параметр (мысалы, logon banner — қосылған кезде графикалық құрылғы) P3 саясатында да, P1 саясатында да анықталған. P3 саясатында берілген параметрдің мәні P1 саясатында берілген мәннен ерекшеленеді. Осы екі саясаттарды қолдану нәтижесінде параметрге қандай мән беріледі? Мұндай жағдайда объект параметріне GPO-дан алынған мән беріледі, ол объектіге жақын. Осылайша, қаралған жағдайда logon banner параметріне P1 саясатынан алынған мән беріледі.

4. Саяси мұрагерлік. P3 саясаты logon banner параметрінің мәнін қамтиды, ал P1 саясаты осы параметрді анықтамайды. Бұл жағдайда, егер объектіге қатысты осы екі саясат қолданылса, қарастырылып отырған объектінің параметріне P3 саясатынан мән беріледі. Алайда sa контейнері үшін бірде-бір саясат анықталмаған. Дегенмен, бұл контейнердің logon banner параметріне P3 саясатынан мән беріледі. Сонымен қатар, бұл контейнерге қатысты P3 және P1 саясаты толық көлемде қолданылатын болады, өйткені sa контейнері бұл өзінің мұрагерлік саясаттынан іздейді.

5. Бір контейнерге қатысты бірнеше саясатты қолдану. Әр түрлі параметрлердің мәндерін анықтайтын P4 және P5 саясаттары Acct контейнеріне қолданылады деп елестетіп көріңіз. P4 саясатындағы компьютердің конфигурация бөлімінде жаһандық есеп тобының мүшелеріне Acct контейнеріндегі кез-келген компьютерге, сондай-ақ осы контейнердің барлық ішкі контейнерлеріне жергілікті қосылуға рұқсат етілген. P5 саясатының компьютерді конфигурациялау

бөлімінде Есеп тобына құқықтар берілмеген. Домен контроллері қасиеттері терезесінде Топтық саясат бетінде көрсетілген саясаттар тізімінде, P5 саясаты тізімнің ең жоғарғы жағында - P4 саясатының үстінде орналасқан. Осы тізімде көрсетілген ережелер объектіге төменнен жоғарыға қарай қолданылады. Басқаша айтқанда, алдымен тізімнің төменгі жағындағы саясат, содан кейін тізімнің жоғарғы жағындағы саясат қолданылады. Осылайша, Acct контейнеріне қатысты қарастырылған саясат жиынтығын өңдеген кезде алдымен P4, содан кейін P5 саясаты қолданылады. Сондықтан саясат жиынтығын өңдегеннен кейін жүйеге жергілікті қосылуға құқықтар параметрінде P5 саясатының мәні болады. Осылайша, жаһандық Бухгалтерлік есеп (бухгалтерлік есеп) тобының мүшелері локальды түрде Acct контейнерінің компьютеріне және оның қосалқы контейнерлеріне қосылуға құқылы емес. Саясаттардың өңделу тәртібін өзгерту үшін Топтық саясат қойындысының төменгі оң жақ бұрышындағы Жоғары және Төмен батырмаларын пайдаланыңыз.

Windows 2000 сізге GPO-ның кейбір бөлімдерін пайдалануға тыйым салуға мүмкіндік береді. Егер саясат контейнерге толығымен емес, ішінара қолданылса, пайдаланушының жүйеге қосылуының жалпы уақыты қысқарады. Нысанға қолданылатын GPO параметрлері неғұрлым аз болса, тиісті саясат жылдамырақ өңделеді. Саясаттың кейбір бөлімдерін өңдеуді ажырату әр ЖПО үшін бөлек орындалуы мүмкін. Ол үшін келесі әрекеттерді орындаймыз:

Белсенді каталог пайдаланушылары мен компьютерлердің қосымшасын ашамыз (Active Directory пайдаланушылары мен компьютерлер). Бізді қызықтыратын контейнерге апарып, осы контейнердің қасиеттері терезесін ашып, Топтық саясат қойындысына өтеміз. Өзгерткіңіз келетін GPO таңдаймыз. Сипаттар түймесін басамыз. Мұнда сіз компьютер конфигурациясына немесе пайдаланушы конфигурациясына қатысты контейнерге арналған саясат параметрлерін бұғаттай аласыз.

GPO бөлімдерінің қайсысы бұғатталуы керек екенін көрсеткеннен кейін, экранда осы саясатқа байланысты өзгертілген параметрлердің бастапқы қалпына келтірілетіні туралы хабарлама пайда болады. Мысалы, егер сіз пайдаланушы конфигурациясына байланысты GPO параметрлерін пайдалануды бұғаттасаңыз, онда осы саясат әсер еткен барлық пайдаланушылардың конфигурациясы осы саясат қолданылғанға дейін қалпына келтіріледі. Windows 2000-дан айырмашылығы, NT 4.0 операциялық жүйесі саясатты дұрыс тазаламады. Осыған байланысты, NT 4.0-де, саясат жойылғаннан кейін де, объект параметрлері жойылған саясатты қолдану барысында оларға берілген мәндерді сақтап қалды.

Саясат бөлімдерінің бірінің қолданбасын блоктау нақты GPO үшін бапталып және осы GPO тағайындалған барлық контейнерлер үшін жарамды.

6. Топтық саясатты басқару жөніндегі делегация. GPO нысандарын басқару мүмкіндігін басқа жауапты тұлғаларға беруге болады. Жіберу ACL тізімдерінің көмегімен жүзеге асырылады. GPO нысанның ACL тізімі осы нысанға қатысты

GPO түрлендіруге немесе кейбір контейнерге қатысты GPO тағайындауға рұқсат беруге мүмкіндік береді. Осылайша, авторланбаған GPO нысандарын құруға тыйым салуға болады. Мысалы, GPO құру және модификациялау Домен әкімшілерінің тобына сенуге болады,ал осы GPO тағайындауды OU жеке контейнерлерінің әкімшілері жүзеге асыра алады. OU контейнерінің әкімшісі ең қолайлы GPO нысанын таңдап, осы GPO-ны өзінің бақылауындағы OU-ға қатысты қолдана алады. Дегенмен, бұл GPO мазмұнын өзгерте алмайды немесе жаңа GPO жасай алмайды.

7. Клиент жағында пайдаланушы құжаттарын және кэширлеуді басқару. Топтық саясат кейбір пайдаланушылар каталогтарын оларға қол жеткізу кезінде желілік каталогтарға немесе жергілікті файлдық жүйенің нақты орындарына қол жеткізетін етіп бағыттауға мүмкіндік береді. Осы жолмен қайта бағыттауға болатын папкалар жиынтығы мыналарды қамтиды:

- Application data;
- Desktop (Жұмыс үстелі);
- My Documents (Менің құжаттарым);
- My Pictures (Менің суреттерім);
- Start Menu (Бас мәзір).

Пайдаланушы қалтасын қайта бағыттау тетігі IntelliMirror технологиясының бөлігі болып табылады, оның мақсаты жұмыс файлына және қолданушы жұмыс жасайтын станцияға қарамастан конфигурация туралы ақпаратқа қол жеткізу болып табылады. Нәтижесінде, Intellimirror технологиясы пайдаланушының жұмыс бекеті істен шыққан жағдайда файлдардың және конфигурация деректерінің қауіпсіздігін қамтамасыз етеді. Каталогты қайта бағыттау Windows параметрлер қалтасын қайта бағыттау тобының саясат объектісінің Пайдаланушыны конфигурациялау бөлімінде конфигурацияланған. Бұл бөлімде бұрын тізімделген барлық қалталар көрсетілген. Осы қалталардың біреуін жаңа орынға бағыттау үшін, оның атын тінтуірдің оң жақ түймешігімен нұқып, пайда болатын мәзірден Қасиеттерді таңдаңыз.

- Target қойындысында(Мақсат) пайдаланушы папкасын қайта бағыттаудың үш нұсқасының біреуін таңдауға болады;
- No administrative policy specified (Әкімшілік саясат көрсетілмеген);
- Basic (базалық). Пайдаланушы қай топқа жататынына қарамастан, қалтаны жаңа орынға бағыттайды. Жаңа орын UNC форматын қолдану арқылы көрсетілуі керек. Жаңа орынды анықтау кезінде% username% сияқты айнымалыларды қолдануға болады. Осылайша, әр түрлі пайдаланушылар үшін қалтаны әртүрлі каталогтарға бағыттауға болады, алайда бұл каталогтардың барлығы бірдей желілік ортақ қалтада орналасуы керек [5];
- Advanced (қиын). Әр түрлі пайдаланушы топтары үшін әр түрлі қалталардың орнын көрсетуге болады. Әр түрлі топтар үшін әр түрлі UNC

атауларын көрсетуге болады. Тиісті папкаларды әртүрлі серверлерде орналастыруға болады.

Бөлім бойынша қорытынды: бұл бөлімде топтық саясат және профиль жайлы теориялық мәлімет бар. Сонымен қатар жергілікті және жылжытылатын профильдер арасындағы айырмашылықтары туралы жазылған.

2 Қауіпсіз байланыс және деректерді шифрлау туралы түсінік

2.1 VPN технологиясының ақпараттық қауіпсіздік негіздері

Vpn виртуалды желілерін құру тұжырымдамасының негізінде жеткілікті қарапайым идея жатыр: егер жаһандық желіде ақпаратпен алмасу қажет екі торап болса, онда осы екі торап арасында ашық желілер арқылы берілетін ақпараттың құпиялылығы мен тұтастығын қамтамасыз ету үшін виртуалды қорғалған туннель салу қажет; осы виртуалды туннельге қолжетімділік барлық мүмкін болатын белсенді және пассивті сыртқы бақылаушыларға өте қиын болуы тиіс.

Мұндай виртуалды туннельдерді құрудан компания алатын артықшылықтар ең алдымен қаржы қаражатын айтарлықтай үнемдеуден тұрады, өйткені бұл жағдайда компания өзінің intranet/extranet желілерін құру үшін қымбат бөлінген байланыс арналарын құрудан немесе жалға беруден бас тарта алады және бұл үшін сенімділік пен беру жылдамдығы көп жағдайда бөлінген желілерден кем түспейтін арзан Интернет-арналарды пайдалана алады. VPN-технологияларын енгізуден экономикалық тиімділік кәсіпорынды оларды белсенді енгізуге ынталандырады.

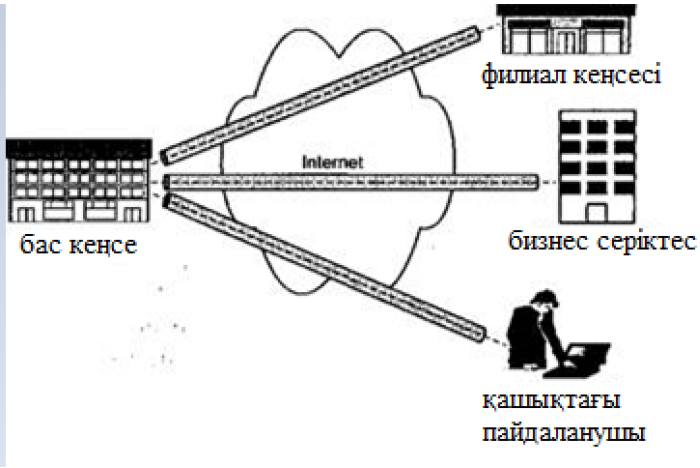
VPN желісінің негізгі ұғымдары мен функциялары:

- корпоративтік жергілікті желіні ашық желіге қосу кезінде екі негізгі типтегі қауіпсіздік қатері туындайды;
- осы желіге рұқсатсыз кіру нәтижесінде қаскүнем алатын корпоративтік жергілікті желінің ішкі ресурстарына ЖТӘ;
- ашық желі арқылы беру процесінде корпоративтік деректерге МТЖ;
- ашық желілер арқылы, атап айтқанда интернет желісі арқылы жергілікті желілер мен жекелеген компьютерлердің ақпараттық өзара іс-қимылының қауіпсіздігін қамтамасыз ету келесі міндеттерді тиімді шешу жолымен мүмкін болады;
- ашық байланыс арналарына қосылған жергілікті желілер мен жеке компьютерлерді сыртқы орта тарапынан рұқсат етілмеген әрекеттерден қорғау;
- ақпаратты ашық байланыс арналары арқылы беру процесінде қорғау.

Жоғарыда айтылғандай, жергілікті желілерді және жеке компьютерлерді сыртқы ортадан рұқсат етілмеген әрекеттерден қорғау үшін олар әдетте екі жақты хабарлама ағынын сүзгілеу арқылы ақпараттық өзара әрекеттестіктің қауіпсіздігін қамтамасыз ететін, сондай-ақ ақпарат алмасу кезінде делдалдық функцияларды орындайтын МЭ пайдаланады. МЭ жергілікті және ашық желілердің түйіскен жерінде орналасқан. Ашық желіге қосылған бөлек қашықтағы компьютерді қорғау үшін бұл компьютерде брандмауэр бағдарламалық жасақтамасы орнатылған және мұндай брандмауэр жеке деп аталады.

Ашық арналар арқылы берілу кезіндегі ақпаратты қорғау виртуалды қауіпсіз VPN желілерін пайдалануға негізделген. Виртуалды жеке желі VPN (Virtual Private Network) - бұл ақпараттың бірыңғай виртуалды корпоративті

желіге берілуі үшін ашық сыртқы орта арқылы жергілікті желілер мен жеке компьютерлердің жиынтығы, бұл мәліметтердің қауіпсіздігін қамтамасыз етеді. Виртуалды қауіпсіз VPN желісі жалпыға қол жетімді желінің ашық байланыс арналары негізінде құрылған виртуалды қауіпсіз байланыс арналарын құру арқылы құрылады. Бұл виртуалды қауіпсіз арналар VPN туннельдері деп аталады. VPN VPN-ге орталық кеңсені, филиалдарды, іскери серіктестер мен қашықтағы пайдаланушыларды қосуға және ақпаратты Интернет арқылы қауіпсіз жеткізуге мүмкіндік береді [6].



2.1 сурет – Виртуалды қорғалған VPN желісі

VPN туннелі - бұл виртуалды желінің криптографиялық қауіпсіз пакеттері жіберілетін ашық желі арқылы қосылыс. VPN туннелі арқылы беру кезіндегі ақпаратты қорғау мыналарға негізделген:

- өзара әрекеттесетін тараптарды аутентификациялау туралы;
- берілетін деректерді криптографиялық жабу (шифрлау);
- жеткізілген ақпараттың шынайылығын және тұтастығын тексеру.

Бұл функциялар бір-бірімен өзара байланысты сипатталады. Іске асырылған кезде ақпаратты қорғаудың криптографиялық әдістері қолданылады. Мұндай қорғаудың тиімділігі симметриялық және асимметриялық криптографиялық жүйелерді бірлесіп қолдану арқылы қамтамасыз етіледі. VPN құрылғыларымен құрылған VPN туннелі Интернет сияқты жалпыға ортақ желіде орналастырылған қауіпсіз жалға берілген желінің қасиеттеріне ие. VPN құрылғылары виртуалды жеке желілерде VPN клиенті, VPN сервері немесе VPN қауіпсіздік шлюзі рөлін атқара алады.

VPN-клиент – бұл әдетте дербес компьютер негізінде орындалатын бағдарламалық немесе аппараттық-бағдарламалық кешен. Оның желілік бағдарламалық жасақтамасы осы құрылғы басқа VPN клиенттерімен, VPN серверлерімен немесе VPN қауіпсіздік шлюздерімен алмасатын трафикті шифрлау және аутентификациялау үшін өзгертілген. Әдетте, VPN клиентін енгізу – бұл

стандартты ОС Windows NT/2000/XP немесе Unix-ті толықтыратын бағдарламалық шешім.

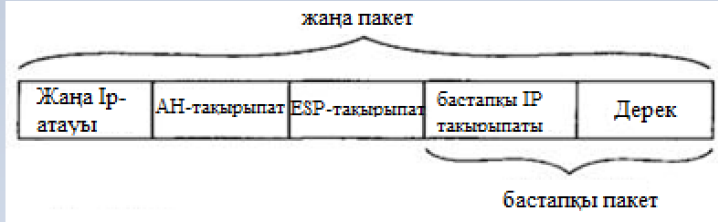
VPN сервері – бұл сервер ретінде әрекет ететін компьютерде орнатылған бағдарламалық жасақтама немесе аппараттық-бағдарламалық кешен.VPN сервері серверлерді сыртқы желілерден рұқсатсыз кіруден қорғайды, сонымен қатар жеке компьютерлермен және жергілікті желілік сегменттердегі компьютерлермен қауіпсіз қосылыстарды (ассоциацияларды) ұйымдастырады. тиісті VPN өнімдерімен қорғалған. VPN сервері - бұл серверлік платформаларға арналған VPN клиент өнімінің функционалды аналогы. Ол ең алдымен VPN клиенттерімен бірнеше қосылыстарды қолдау үшін кеңейтілген ресурстарымен ерекшеленеді. VPN сервері ұялы пайдаланушылармен қауіпсіз қосылысты қолдай алады.

Security Gateway VPN – бұл екі желіге қосылатын және оның артында орналасқан көптеген хосттарға шифрлау және аутентификация функцияларын қамтамасыз ететін желілік құрылғы. VPN қауіпсіздік шлюзі ішкі корпоративтік желіге арналған барлық трафик сол арқылы өтетін етіп орналасқан. VPN шлюзінің желілік қосылымы шлюздің артындағы пайдаланушылар үшін ашық болады және олар арнайы желі ретінде көрінеді, дегенмен іс жүзінде ол пакеттік коммутацияланған желі арқылы жіберіледі. VPN қауіпсіздік шлюзінің мекен-жайы кіретін туннель пакетінің сыртқы мекен-жайы ретінде көрсетілген, пакеттің ішкі мекенжайы шлюздің артындағы нақты хост мекен-жайы болып табылады. VPN қауіпсіздік шлюзі бөлек бағдарламалық шешім, бөлек аппараттық құрал, сонымен қатар VPN функцияларымен толықтырылған маршрутизатор немесе МЕ ретінде жүзеге асырылуы мүмкін [6].

Ашық сыртқы ақпарат беру ортасы Интернет пайдаланылатын жоғары жылдамдықты деректер арналарын және баяу қоғамдық байланыс арналарын қамтиды, олар әдетте телефон желісінің арналары болып табылады. VPN виртуалды жеке желісінің тиімділігі ашық байланыс арналары арқылы таратылатын ақпараттың қауіпсіздігімен анықталады. Инкапсуляция және туннельдеу ашық желілер арқылы мәліметтерді қауіпсіз беру үшін кеңінен қолданылады. Туннельдеу техникасын қолдана отырып, деректер пакеттері кәдімгі «нүкте-нүкте» қосылымы сияқты жалпы желі арқылы беріледі. «Жіберуші - деректерді қабылдаушы» жұбының арасында ерекше туннель орнатылған - бұл бір хаттаманың деректерін екіншісінің пакеттеріне инкапсулациялауға мүмкіндік беретін логикалық байланыс.

Туннельдеудің мәні қызмет көрсету өрістерімен бірге жаңа «конвертке» жинақталған деректердің бөлігін, яғни «орау». Бұл жағдайда төменгі деңгейдегі протокол пакеті жоғары немесе бірдей деңгейдегі протокол пакетінің деректер өрісіне орналастырылады. Айта кету керек, туннельдің өзі деректерді рұқсатсыз кіруден немесе бұрмаланудан қорғамайды, бірақ туннельдің арқасында қоршалған бастапқы пакеттерді толық шифрлауға болады. Берілген деректердің құпиялығын

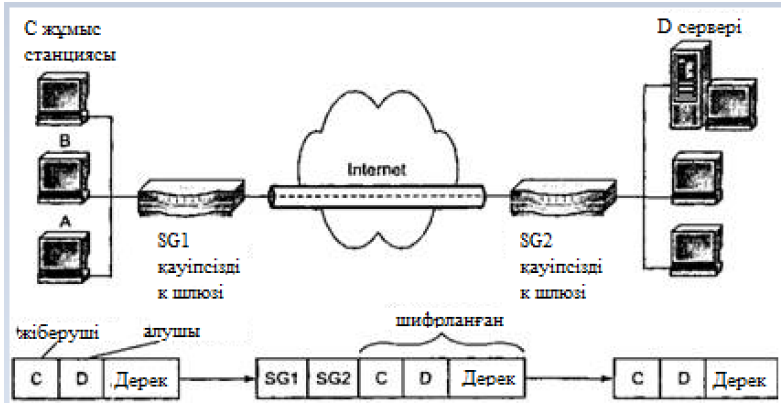
қамтамасыз ету үшін жіберуші бастапқы пакеттерді шифрлайды, жаңа IP тақырыппен сыртқы пакетке салады және транзиттік желі арқылы жібереді.



2.2 сурет - Туннельге дайындалған пакеттің мысалы

Туннельдеу технологиясының ерекшелігі - бұл тек деректер өрісін ғана емес, сонымен бірге тақырыптамамен қатар, бастапқы пакетті де шифрлауға мүмкіндік береді. Бұл маңызды, өйткені кейбір тақырып өрістерінде шабуылдаушы қолдануы мүмкін ақпарат бар. Атап айтқанда, желінің ішкі құрылымы туралы ақпаратты - ішкі желілер мен түйіндер саны туралы мәліметтер және олардың IP мекенжайлары - бастапқы пакеттің тақырыбынан алуға болады. Бұл ақпаратты корпоративті желіге шабуыл жасау үшін шабуылдаушы қолдана алады. Шифрланған тақырыптары бар түпнұсқа пакетті желі арқылы тасымалдауды ұйымдастыру үшін пайдалануға болмайды. Сондықтан бастапқы пакетті қорғау үшін инкапсуляция және туннельдеу қолданылады. Бастапқы пакет тақырыппен бірге толық шифрланған, содан кейін бұл шифрланған пакет басқа ашық сыртқы бумаға орналастырылады. Деректерді ашық желі арқылы тасымалдау үшін сыртқы пакеттің ашық тақырыптары қолданылады.

Қорғалған арнаның соңғы нүктесіне жеткенде ішкі пакет сыртқы пакеттен алынады, шифрланған және қалпына келтірілген тақырып ішкі желі арқылы әрі қарай беру үшін қолданылады.



2.3 сурет - Виртуалды қауіпсіз туннельдің схемасы

Туннельдеуді пакет мазмұнының құпиялығын ғана емес, сонымен қатар оның тұтастығы мен түпнұсқалығын қорғау үшін де қолдануға болады, сонымен қатар электрондық цифрлық қолтаңбаны пакеттің барлық өрістеріне таратуға болады.

Желі құрылымын екі нүктенің арасында жасырумен қатар, туннельдеу екі жергілікті желі арасындағы мүмкін болатын қақтығыстардың алдын алады. Интернетке қосылмаған жергілікті желіні құру кезінде компания өзінің желілік құрылғылары мен компьютерлері үшін кез-келген IP мекенжайын қолдана алады. Бұрын оқшауланған желілерді біріктірген кезде бұл мекен-жайлар бір-біріне және Интернетте бұрыннан бар мекенжайларға қайшы келуі мүмкін. Пакеттерді инкапсуляциялау бұл мәселені шешеді, өйткені ол бастапқы мекен-жайларды жасыруға және Интернет желісіндегі IP мекенжайлар кеңістігінде жаңа, қайталанбас қосуға мүмкіндік береді, оларды кейіннен ортақ желі арқылы деректерді жіберуге пайдаланады. Мұнда сонымен қатар жергілікті желіге қосылатын мобильді пайдаланушылар үшін IP мекенжайын және басқа параметрлерді конфигурациялау тапсырмасы бар.

Туннельдік механизм қауіпсіз арнаны қалыптастыру үшін әртүрлі хаттамаларда кеңінен қолданылады. Әдетте, туннель ашық желінің бөлігі ғана жасалады, онда құпиялылық пен деректердің тұтастығын бұзу қаупі бар, мысалы, ашық Интернетке кіру нүктесі мен корпоративтік желіге кіру нүктесі арасында. Бұл жағдайда осы екі нүктеде орнатылған шекаралық маршрутизаторлардың мекенжайлары сыртқы пакеттер үшін пайдаланылады, ал соңғы түйіндердің ішкі мекенжайлары ішкі көз пакеттерінде қорғалған түрде болады. Айта кету керек, туннельдік механизмнің өзі туннельдеу мақсатына тәуелсіз. Туннельдеуді тек берілетін деректердің бүкіл бөлігінің құпиялылығы мен тұтастығын қамтамасыз ету үшін ғана емес, сонымен қатар әртүрлі протоколдармен (мысалы, IPv4 және IPv6) желілер арасында ауысуды ұйымдастыру үшін де қолдануға болады. Туннельдеу басқа протоколды қолдана отырып, бір хаттаманың пакеттерін логикалық ортада беруді ұйымдастыруға мүмкіндік береді. Нәтижесінде, әр түрлі типтегі бірнеше желілердің өзара әрекеттесу мәселелерін, берілетін деректердің тұтастығы мен құпиялылығын қамтамасыз ету қажеттілігінен бастап, сыртқы хаттамалардың немесе адресаттар схемаларының сәйкессіздіктерін жеңумен аяқталатын мәселелерді шешуге болады.

Туннельдік механизмнің іске асырылуы үш типті хаттаманың нәтижесі ретінде ұсынылуы мүмкін: «жолаушы» хаттамасы, өткізу протоколы және туннельдік хаттама. Мысалы, IPX көліктік хаттамасын «жолаушылар» протоколы ретінде бір кәсіпорынның филиалдарының жергілікті желілерінде деректерді бере отырып пайдалануға болады. Интернеттегі IP протоколы оператордың ең кең таралған нұсқасы болып табылады. Туннельдеу протоколдары ретінде PPTP және L2TP байланыс қабаттарының протоколдарын, сонымен қатар IPSec желілік қабат протоколдарын пайдалануға болады. Туннель арқылы Интернет инфрақұрылымын VPN қосымшаларынан жасыруға болады.

VPN туннельдерін әр түрлі түпкі пайдаланушылар үшін жасауға болады - бұл қауіпсіздік шлюзі бар жергілікті желі (LAN) немесе қашықтағы және мобильді пайдаланушылардың бөлек компьютерлері. Ірі кәсіпорынның виртуалды жеке

желісін құру үшін сізге VPN шлюздері, VPN серверлері және VPN клиенттері қажет. Кәсіпорынның локальді желілерін қорғау үшін VPN шлюздерін қолданған жөн, VPN серверлері мен VPN клиенттері Интернет арқылы корпоративтік желіге қашықтан және мобильді пайдаланушылар арасындағы қауіпсіз қосылыстарды ұйымдастыру үшін қолданылады.

VPN қауіпсіздік құралдары:

- қауіпсіз виртуалды VPN желісін құру кезінде ақпараттық қауіпсіздікті қамтамасыз ету міндеті өте маңызды. Жалпы қабылданған анықтамаға сәйкес деректердің қауіпсіздігі олардың құпиялылығы, тұтастығы және қол жетімділігі ретінде түсініледі. VPN қосымшалары үшін деректер қауіпсіздігі критерийлерін келесідей анықтауға болады;
- құпиялылық - деректерді қауіпсіз VPN арналары арқылы беру кезінде бұл мәліметтер заңды жіберуші мен алушыға ғана белгілі болатынына кепілдік;
- тұтастық - қауіпсіз VPN арнасы арқылы берілетін мәліметтердің қауіпсіздігінің кепілі. Жаңа деректерді өзгертуге, өзгертуге, жоюға немесе жасауға кез келген әрекет табылып, заңды пайдаланушыларға белгілі болады;
- қол жетімділік - VPN функцияларын орындайтын құралдар заңды қолданушыларға үнемі қол жетімді болатындығының кепілі. VPN құралдарының қол жетімділігі - бұл іске асырудың сенімділігіне, қызмет көрсету сапасына және құралдың өзін сыртқы шабуылдардан қорғау дәрежесіне байланысты жан-жақты индикатор.

Құпиялылық симметриялы және асимметриялық шифрлаудың әртүрлі әдістері мен алгоритмдері арқылы қамтамасыз етіледі. Берілетін деректердің тұтастығына, әдетте, асимметриялық шифрлау әдістері мен бір жақты функцияларға негізделген электрондық қолтаңба технологиясының әртүрлі нұсқаларын қолдану арқылы қол жеткізіледі.

Аутентификация қайта пайдалануға болатын және бір реттік парольдерге, сандық сертификаттарға, смарт-карталарға, күшті түпнұсқалық растама хаттамаларына негізделген, VPN байланысын тек заңды пайдаланушылар арасында орнатуды қамтамасыз етеді және VPN құралдарына қалаусыз адамдардың кіруіне жол бермейді.

Авторизация дегеніміз әр түрлі қызмет түрлерінің заңдылығын (шынайылығын) дәлелдеген абоненттерге, атап айтқанда, олардың трафиктерін шифрлаудың әр түрлі тәсілдерін ұсынуды білдіреді. Авторизация мен қол жеткізуді басқару көбінесе бірдей әдістермен жүзеге асырылады.

Виртуалды қауіпсіз желілерде берілетін деректердің қауіпсіздігін қамтамасыз ету үшін желілік қауіпсіздіктің келесі негізгі міндеттері шешілуі керек:

- қосылымды орнатқан кезде абоненттердің өзара аутентификациясы;
- берілетін ақпараттың құпиялығын, тұтастығын және шынайылығын қамтамасыз ету;

- авторизация және қол жеткізуді басқару;
- желінің периметрі бойынша қауіпсіздік және шабуылды анықтау;
- желілік қауіпсіздікті басқару.

Абоненттердің аутентификациясы. Аутентификация процедурасы (аутентификация) заңды пайдаланушыларға кіруге мүмкіндік береді және қалаусыз адамдардың желісіне кіруге жол бермейді.

Ақпараттың құпиялығын, тұтастығы мен шынайылығын қамтамасыз ету. Ақпараттың құпиялығын қамтамасыз ету міндеті - берілген деректерді рұқсатсыз оқудан және көшіруден қорғау. Ақпараттың құпиялығын қамтамасыз етудің негізгі құралы - шифрлау.

Авторизация және қол жеткізуді басқару. VPN қауіпсіздігінің негізгі компоненті желі авторластырылмаған пайдаланушылар үшін желі толығымен жабылған кезде авторланған пайдаланушылардың компьютерлік ресурстарға қол жеткізуді қамтамасыз ету болып табылады.

Авторизация бағдарламалық жасақтамасын құру кезінде келесілер пайдаланылады:

- орталықтандырылған авторизация схемасы;
- орталықтандырылмаған авторизация схемасы;
- орталықтандырылған авторизация жүйесінің негізгі мақсаты - бірыңғай кіру қағидатын іске асыру. Пайдаланушыны ресурстармен қамтамасыз ету процесі сервермен басқарылады. Керберос, RADIUS және TACACS жүйелерінде авторизациялау процесіне орталықтандырылған тәсіл енгізілген.

Жақында рөлге негізделген қол жетімділікті басқару белсенді дамып келеді. Бұл қауіпсіздік мәселелерін шешпейді, өйткені ол жүйенің басқарылуын жақсартады. Рөлдік қол жеткізуді басқарудың мәні аралық субъектілер - рөлдер - пайдаланушылар мен олардың артықшылықтары арасында орналасуында. Әр пайдаланушы үшін бір уақытта бірнеше рөлдер белсенді бола алады, олардың әрқайсысы оған нақты анықталған құқықтар береді.

Пайдаланушылар мен артықшылықтарға қарағанда рөлдер аз болғандықтан, рөлдерді қолдану күрделілікті азайтуға және, демек, жүйенің басқарылуын жақсартуға көмектеседі. Сонымен қатар, қол жеткізуді басқарудың рөлдік моделіне сүйене отырып, міндеттерді бөлу сияқты маңызды қағиданы іске асыруға болады (мысалы, сыни процесті жалғыз өзі жасай алмау).

Желінің периметрі бойынша қауіпсіздік және шабуылды анықтау. Қорғалған желінің қосымшаларына, қызметтері мен ресурстарына қол жеткізуді қатаң бақылау дұрыс құрылған желінің маңызды функциясы болып табылады. Қауіпсіздік функцияларын МЕ, интрузияны анықтау жүйелері, қауіпсіздік аудиті жүйелері, антивирустық жүйелер пайдалану желі арқылы тасымалданатын мәліметтерді жүйелік қорғауды қамтамасыз етеді.

Желілік қауіпсіздіктің жалпы шешімінің маңызды бөлігі қорғалған желінің периметрін кесіп өтетін трафикті басқаратын және ұйымның қауіпсіздік саясатына сәйкес трафиктің өтуіне шектеулер қоятын ЭЕМ болып табылады.

Желінің периметрі бойынша қауіпсіздік кепілдігінің қосымша элементі Интрузияны анықтау жүйесі (IDS) болып табылады, ол нақты уақыт режимінде жұмыс істейді және сыртқы және ішкі көздерден рұқсат етілмеген желілік әрекеттерді анықтауға, тіркеуге және тоқтатуға арналған.

Қауіпсіздікті талдау жүйелері қауіпсіздіктің әлсіз жақтарын анықтау үшін корпоративтік желіні қарап шығады, бұл желіні басқарушыларға желіні шабуылдардан жақсы қорғауға мүмкіндік береді.

Желілік қауіпсіздікті басқару. VPN желілік құрылғылардың өзін де, қауіпсіздік пен өткізу қабілеттілігін басқарудың көптеген қызметтерін де біріктіреді. Компанияларға осы құрылғылар мен қызметтерді VPN инфрақұрылымы, соның ішінде қашықтан қол жеткізетін пайдаланушылар мен экстражелі құралдар арқылы кешенді басқару қажет. Осыған байланысты VPN құралдарын басқару VPN-нің тиімді жұмысын қамтамасыз етудегі маңызды міндеттердің бірі болып табылады. Корпоративтік желіні басқару жүйесі кез-келген масштабтағы қауіпсіздік саясатын, құрылғылар мен VPN қызметтерін басқаруға қажетті құралдар жиынтығын қамтуы керек [7].

Желілік қауіпсіздікті басқару VPN-дің түпкілікті өнімдері тобының негізі болып табылады. VPN қауіпсіздігінің және басқарудың жоғары деңгейін, әсіресе криптографиялық кілт пен сертификатты тарату жүйесін қамтамасыз ету үшін бүкіл қорғалған корпоративтік желінің қауіпсіздігін орталықтандырылған үйлестіруді қамтамасыз ету қажет.

2.2 Құпия ақпаратты қорғау үшін шифрлауды қолдану

Дискіні шифрлау дегеніміз - заңсыз қолданушы оңай шеше алмайтын, дискідегі мәліметтерді оқылмайтын кодқа ауыстыратын ақпаратты қорғау технологиясы. Дискіні шифрлау үшін сақтаудың әр битін шифрлайтын арнайы бағдарламалық немесе аппараттық құрал қолданылады.

Дискіні толық шифрлау (FDE) өрнегі, әдетте, дискідегі барлық нәрсе, оның ішінде жүктеу жүйесінің бөліктері де шифрланғанын білдіреді.

Файлдық жүйенің деңгей шифрлау (FLE) - бұл әр файлды қоймада шифрлау процесі. Шифрланған деректерге қол жеткізуді тек сәтті түпнұсқалық растамадан кейін алуға болады. Кейбір операциялық жүйелерде FLE-ге арналған қосымшалар бар, алайда көптеген үшінші тараптардың қол жетімділігі бар. FLE ашық, яғни файлдық жүйеге қолы жететіндердің бәрі шабуылдаушы пайдалана алатын шифрланған файлдардың атаулары мен метадеректерін көре алады.

Файлдық жүйе деңгейінің шифрлануы дискіні толық шифрлаудан өзгеше. FDE деректерді пайдаланушы жүктеу аяқталғанға дейін қорғайды, сондықтан егер диск жоғалған немесе ұрланған болса, шабуылдаушыға қол жетімді болмайды,

бірақ егер жұмыс кезінде диск шифрланған болса және шабуылдаушы компьютерге қол жеткізсе, онда ол барлық файлдарға қол жеткізе алады. қойма. FLE, екінші жағынан, қолданушы белгілі бір файлға сәйкестендірілгенге дейін қорғайды, бір файлмен жұмыс істегенде, қалғаны әлі де шифрланған, сондықтан FLE қауіпсіздігін жоғарылату үшін толық шифрлаумен бірге қолдануға болады.

Тағы бір маңызды айырмашылық - FDE дискідегі барлық деректерді автоматты түрде шифрлайды, ал FLE шифрланған файлдар мен қалталардан тыс деректерді қорғамайды, сондықтан уақытша және своп файлдарында шифрланбаған ақпарат болуы мүмкін.

Сенімді платформа модулі (TPM) - бұл аналық платаға ендірілген, қауіпсіздікті қамтамасыз ететін аппараттық құрылғылардың аутентификациясы үшін қолданылатын қауіпсіз криптографиялық процессор. Ол сонымен қатар үлкен екілік деректерді сақтай алады, мысалы, құпия кілттерді және оларды мақсатты жүйенің конфигурациясымен байланыстырады, нәтижесінде шифрланады және оларды тек таңдалған құрылғыда шешуге болады [8].

TPM қолданатын FDE бар, мысалы, BitLocker және онымен жұмыс істеуді қолдамайтындар, мысалы TrueCrypt.

2.2.1 BitLocker шифрлау

BitLocker шифрлау - бұл Windows операциялық жүйелерінің бөлігі болып табылатын меншікті дискіні шифрлау технологиясы.

BitLocker дискіні толықтай шифрлау арқылы деректерді қорғауға мүмкіндік береді (логикалық, Windows 7 және SD карталары мен USB флэш-дискілері) (Microsoft терминологиясында – томдар). Келесі шифрлау алгоритмдеріне қолдау көрсетіледі:

- AES 128;
- AES 128 с Elephant diffuser (әдепкі бойынша қолданылады);
- AES 256;
- AES 256 с Elephant diffuser.

Кілттің өзін TPM-де немесе USB құрылғысында немесе компьютерде сақтауға болады. TPM жағдайында компьютер іске қосылған кезде, кілт оны дереу немесе USB кілтін пайдаланып немесе қолданушы PIN-кодты енгізгеннен кейін алынады. Осылайша қол жетімділік үшін келесі комбинациялар қол жетімді:

- TPM;
- TPM + PIN коды;
- TPM + PIN + USB пернесі;
- TPM + USB қосқышы;
- USB пернесі (бұл режим топтық саясат арқылы іске қосылуды қажет етеді);
- Пароль (бұл режим Windows 8 жүйесінен бастап қол жетімді және топтық саясат арқылы активацияны қажет етеді).

BitLocker физикалық дискіні емес, көлемді шифрлайды. Көлемі дисктің бір бөлігін алуы немесе бірнеше дискілерден тұратын болуы мүмкін. BitLocker жұмысы үшін, жүйелік диск шифрланған жағдайда, NTFS екі көлемі қажет болады, біреуі ОС үшін, ал екіншісі - жүктеу бөлігі үшін. Соңғысы кемінде 1,5 ГБ болуы керек және шифрланбауы керек. Windows Vista SP1 бастап, енді жүйелік емес көлемдерді шифрлай аласыз. Бөлімдерді жасағаннан кейін, компьютерде TPM модулін қай жерде, қай жерде орнатып, BitLocker-ді іске қосу керек. Windows 7-де BitLocker To Go пайда болды, ол алынбалы медианы шифрлауға мүмкіндік береді, сонымен қатар жүктеу бөлігіне қойылатын талаптарды төмендетеді, оған 100 Мбайт жеткілікті. Windows 7 жүйесін бос дискіге орнатқан кезде жүктеу бөлімі автоматты түрде жасалады.

Bitlocker шифрлауын қолдану үшін аутентификацияның үш механизмі бар:

Ашық жұмыс режимі. Бұл режим пайдаланушының мөлдір тәжірибесін қамтамасыз ету үшін сенімді платформа модулінің аппараттық мүмкіндіктерін қолданады. Пайдаланушылар Windows компьютеріне әдеттегідей кіреді. Дискіні шифрлау үшін пайдаланылатын кілт TPM чипінде кодталады және оны тек ОЖ-нің жүктеу кодымен шығаруға болады (егер жүктеу файлдары өзгеріссіз көрсетілсе). Бұл режим суық жүктеу кезінде шабуылға осал келеді, өйткені бұл шабуылдаушыға компьютерді және жүктеуді өшіруге мүмкіндік береді.

Пайдаланушының аутентификация режимі. Бұл режим пайдаланушы алдын-ала жүктеу ортасында PIN-кодты алдын-ала енгізу түрінде кейбір аутентификацияны өтті деп болжайды. Бұл режим жүктеу шабуылына осал.

USB қосқыш режимі. Қауіпсіз амалдық жүйеге жүктеу үшін пайдаланушы компьютерге бастау кілті бар USB құрылғысын салыуы керек. Бұл режим үшін компьютердегі BIOS жүктелетін ортада USB құрылғыларын оқуды қолдауы керек екенін ескеріңіз. Бұл режим, сонымен қатар, жүктеу шабуылдарына осал.

2.2.2 TrueCrypt шифрлау

TrueCrypt - Microsoft Windows NT 5 және жаңа отбасы (GUI-интерфейсі), Linux және Mac OS X-нің 32-биттік және 64-биттік операциялық жүйелеріне арналған жедел шифрлауға арналған компьютерлік бағдарлама, сізге сақталған шифрланған логикалық (виртуалды) дискіні жасауға мүмкіндік береді. файл. TrueCrypt көмегімен сіз қатты диск бөлімін немесе USB флэш-дискісі сияқты басқа сақтау ортасын толық шифрлай аласыз. TrueCrypt көлеміндегі барлық сақталған деректер толықтай шифрланған, оның ішінде файлдар мен каталог атаулары. Орнатылған TrueCrypt кәдімгі логикалық дискке ұқсас, сондықтан сіз онымен қарапайым файлдық жүйені тексеріп, дефрагментациялау бағдарламаларын пайдаланып жұмыс жасай аласыз.

Бағдарламаның лицензиясы тегін деп саналды, бірақ 2008 жылдың қазан айында Федора дистрибьюторына TrueCrypt қосылғаны тексерілген кезде қауіпті

және тегін емес түсініксіздіктер ашылды. Қарашаға дейін лицензияға түзетулер енгізілді.

2014 жылғы 28 мамырда жоба жабылды, игеру кезең-кезеңімен аяқталды. Барлық ескі нұсқалар жойылды, репозиторий жойылды. Жобаның жабылуына байланысты жағдайлар IT қауымдастығында көптеген алып-сатарлықтар мен пікірталастар тудырды.

TrueCrypt көмегімен сіз шифрланған виртуалды дискіні жасай аласыз:

- онымен жұмыс істеуді жеңілдететін контейнер файлында - беру, көшіру (оның ішінде кез келген басқа қарапайым файл сияқты сыртқы құрылғыларға), атын өзгерту немесе жою;
- жұмысты тиімдірек және ыңғайлы ететін шифрланған диск бөлімі түрінде, 5.0 нұсқасында жүйелік бөлімді шифрлауға мүмкіндік туды;
- USB флэш-дискісі сияқты құрылғының мазмұнын толық шифрлау арқылы (7.0 нұсқасынан бастап дискеталарға қолдау көрсетілмейді);
- TrueCrypt 6.2 қолдайтын шифрлау алгоритмдеріне AES, Serpent және Twofish кіреді.
- бағдарлама үш хэш функцияның біреуін таңдауға мүмкіндік береді: HMAC-RIPEMD-160, HMAC-Whirlpool, HMAC-SHA-512 шифрлау кілттерін, тұзды және тақырып кілтін құруға.

Шифрланған деректерге қол жеткізу үшін сіз парольді (фразалық фразаны), негізгі файлдарды (бір немесе бірнеше) немесе олардың тіркесімдерін пайдалана аласыз. Кілт файлдары ретінде сіз жергілікті, желілік, алынбалы дискілердегі кез келген қол жетімді файлдарды қолдана аласыз (алғашқы 1,048,576 байт пайдаланылады) және өзіңіздің негізгі файлдарыңызды жасай аласыз [9].

TrueCrypt-тің назар аударарлық ерекшеліктерінің бірі - қолданушы парольді мәжбүрлеп тапқан жағдайда қажет болатын, шифрланған мәліметтердің болуын екі деңгеймен қамтамасыз ету:

Жасырын көлем кез-келген файлдық жүйеге ие бола алады және негізгі көлемнің пайдаланылмаған кеңістігінде орналасуы мүмкін, ал негізгі парольмен қол жеткізуге болмайтын мәліметтерге қол жеткізу үшін тұрақты көлемде екінші құпия сөзді (және кілт файлдарының жиынтығын) орнатуға мүмкіндік береді.

TrueCrypt көлемін анықтау мүмкін емес (TrueCrypt көлемін кездейсоқ мәліметтер жиынтығынан бөліп алуға болмайды, яғни файл TrueCrypt-пен, оны құрған бағдарламамен, кез-келген түрде немесе шеңберде байланыстырыла алмайды).

2.2.3 VeraCrypt шифрлау

VeraCrypt – бұл шұғыл шифрлау үшін қолданылатын бағдарламалық жасақтама. VeraCrypt ақысыз және ашық бастапқы жоба, 2013 жылдың 22 маусымында TrueCrypt шанышқысы ретінде іске қосылды. Іске қосылған және

қазіргі уақытта IDRIX негізін қалаушы Mounir Idrassi қолдайды, TrueCrypt қолдауы тоқтатылғаннан кейін 2014 жылдың 28 мамырында.

VeraCrypt келесі шифрлау алгоритмдерін қолдана алады: AES, Serpent, Twofish, Camellia, Grasshopper, сонымен қатар осы алгоритмдердің комбинациясы.

Пайдаланылған криптографиялық хэш функциялары: RIPEMD-160, SHA-256, SHA-512, Stribog және Whirlpool.

Әзірлеушілердің айтуынша, VeraCrypt TrueCrypt-ке қатысты бірқатар жақсартуларды жүзеге асырды.

TrueCrypt кілтті құру кезінде 1000 итерацияны пайдаланады, ол PBKDF2-RIPEMD-160 алгоритмін пайдаланып жүйелік бөлімді шифрлайды, VeraCrypt 327,661 итерацияны қолданады. Шифрланған дискідегі стандартты бөлімдер мен файл контейнерлері үшін VeraCrypt RIPEMD-160 хэш функциясы үшін 655 331 итерацияны және SHA-2 және Whirlpool үшін 500,000 итерацияны қолданады. Бұл шифрланған диск бөлімдерін оларды орнату кезінде ашқан кезде VeraCrypt-ті едәуір баяулатады, бірақ оны тікұшақ шабуылына 10 (және 300-ден көп емес) есе төзімді етеді [10].

Windows үшін жүктеу құралының осалдығы. Шифрланған бөлімнен жүктеу режимі үшін SHA-256 алгоритміне қолдау қосылды және Windows үшін ShellExecute осалдығы туралы мәселелер шешілді.

2.2.4 Symantec Endpoint Encryption шифрлау

Symantec Endpoint шифрлау дискіні, жүйелік файлдарды және ауыстыру файлдарын қоса алғанда, қатты дискідегі (файлдар, қалталар) және флэш-медиадағы (USB, SD жад карталары) ақпаратты шифрлау арқылы деректердің ұрлануынан немесе жоғалуынан қорғайды.

Шифрлау жылдамдығын арттыру үшін AES-NI жабдықты оңтайландыру мүмкіндіктерін қолдана отырып, PGP гибридтік криптографиялық оптимизаторы (HCO) технологиясы негізінде шифрлау.

Алынатын медиа тізімдерін және жеке пайдаланушылар топтарын құру арқылы деректерді автоматты түрде шифрлау.

Пайдаланушы аутентификациясының екі факторлы мүмкіндігімен құжаттар мен файлдарға қол жеткізу (пароль және смарт карта немесе токен). Жеке және топтық кілттерді басқару саясатына арналған Active Directory интеграциясы. Шифрланған қатты дискіде орналасқан құжаттармен жұмыс істеу үшін пайдаланушыларды бірнеше пайдаланушының аутентификациясы мүмкіндігі.

Бумада қамтылған бір басқару серверін (Encryption Management Server) қолдана отырып, ұйымдағы қауіпсіздік саясатының, кілттерді басқарудың және клиенттік қосымшалардың орталықтандырылған конфигурациясы.

Symantec дискісін шифрлауды Symantec шифрлаудың басқа құралдарымен бірге бірнеше қауіпсіздіктің деңгейлерін қамтамасыз ету үшін пайдалануға

болады: Файлдарды ортақ пайдалану шифрлау, жұмыс үстеліндегі электрондық поштаны шифрлау, сонымен қатар мобильді шифрлау [11].

2.2.5 Деректерді шифрлау құралдарын салыстыру

2.1-кесте – Анықтама ақпарат

Атауы	Әзірлеуші	Қашан шығарылды	Лицензиялау	Қолдау
BitLocker	Microsoft	2006	патенттелген	да
TrueCrypt	Фонд TrueCrypt	2004-02-02	TrueCrypt Лицензия 3.1	нет
VeraCrypt	IDRIX	2013-06-22	Лицензия Apache 2.0 TrueCrypt нұсқасы 3.0 (тек ескірген код)	да
Symantec Endpoint Encryption	Symantec Corporation	2008	патенттелген	да

2.2-кесте – Операциялық жүйелер

Атауы	Windows	Linux	Mac OS
BitLocker	иә	Жартылай	Жартылай
TrueCrypt	иә	иә	иә
VeraCrypt	иә	иә	иә
Symantec Endpoint Encryption	иә	жоқ	иә

2.3-кесте –Ерекшеліктері

Атауы	Жасырын контейнерлер	Жүктеу алдында аутентификация	Бір кіру нүктесі	Пайдаланушы аутентификация	Бірнеше кілттер	Құпия фразаның күшеюі	TPM аппараттық жеделдету	Файлдық	Екі факторлы аутентификация
BitLocker	жоқ	иә	жоқ	иә	иә	иә	иә	Негізінен NTFS	иә
TrueCrypt	Иә (бір сыртқы контейнерге шектелген)	тек Windows	?	жоқ	иә бірнеше кілт файлдары бар	иә	жоқ	Тек Windows MBR томы; UEFI GPT жетектері емес, динамикалық жетектер ұсынылмайды	иә
VeraCrypt	Иә (бір сыртқы контейнерге шектелген)	тек Windows	жоқ	жоқ	иә бірнеше кілт файлдары бар	иә	жоқ	Windows MBR және UEFI GPT дискілерінде; динамикалық дискілер ұсынылмайды	иә
Symantec Endpoint Encryption	жоқ	иә	иә	иә	иә	жоқ	жоқ	NTFS, FAT32	иә

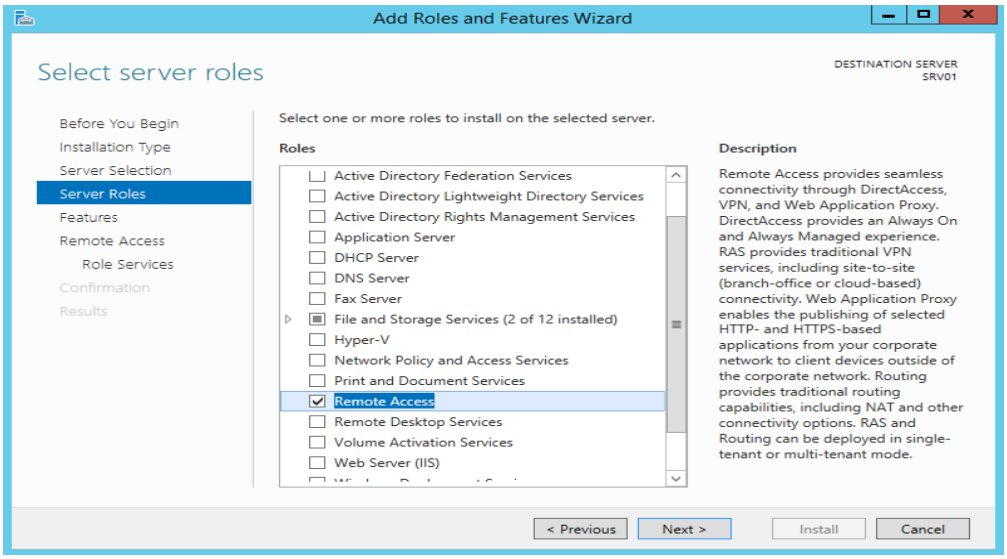
Бөлім бойынша қорытынды: дипломның бұл бөлігі VPN технологиясының ақпараттық қауіпсіздік негіздері туралы. Оған қоса құпия ақпартты қорғау үшін шифрлауды қолдану туралы теориялық мәлімет жазылған.

3 Практикалық бөлім

3.1 Виртуалды қорғалған VPN желілерін құру

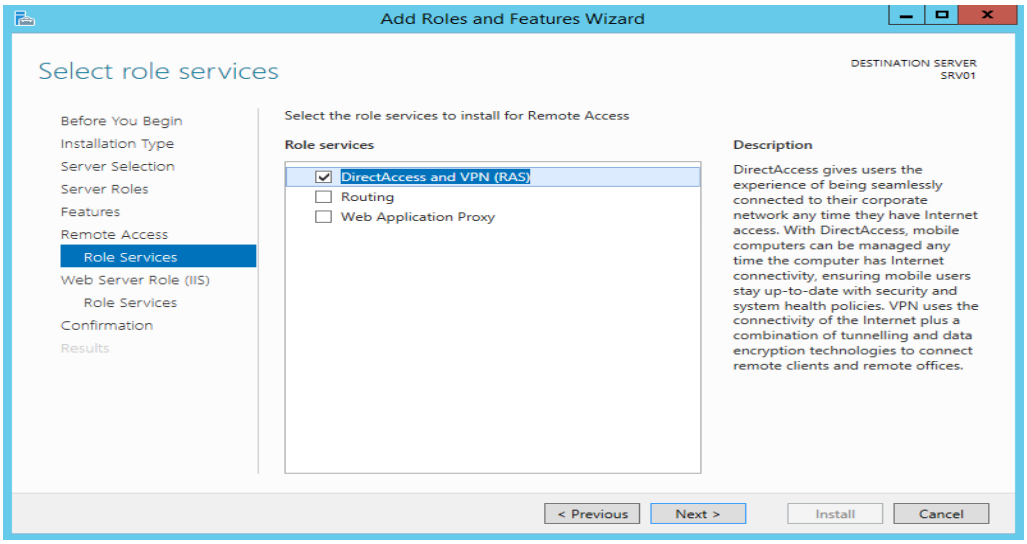
Жұмыста сипатталған барлық әрекеттер Windows Server 2012 R2-де жасалған, бірақ Нұсқаулық Windows Server 2008 R2-ден бастап Windows Server 2016-ке дейін кез келген өзекті серверлік операциялық жүйе үшін жарамды.

Сондықтан бастайық. Біріншіден, бізге қашықтан кіру рөлін орнату қажет. Бұл үшін Server Manager құрылғысында рөлдерді қосу шеберін іске қосып, барлық қосымша фичтармен "Remote Access" рөлін таңдаймыз.



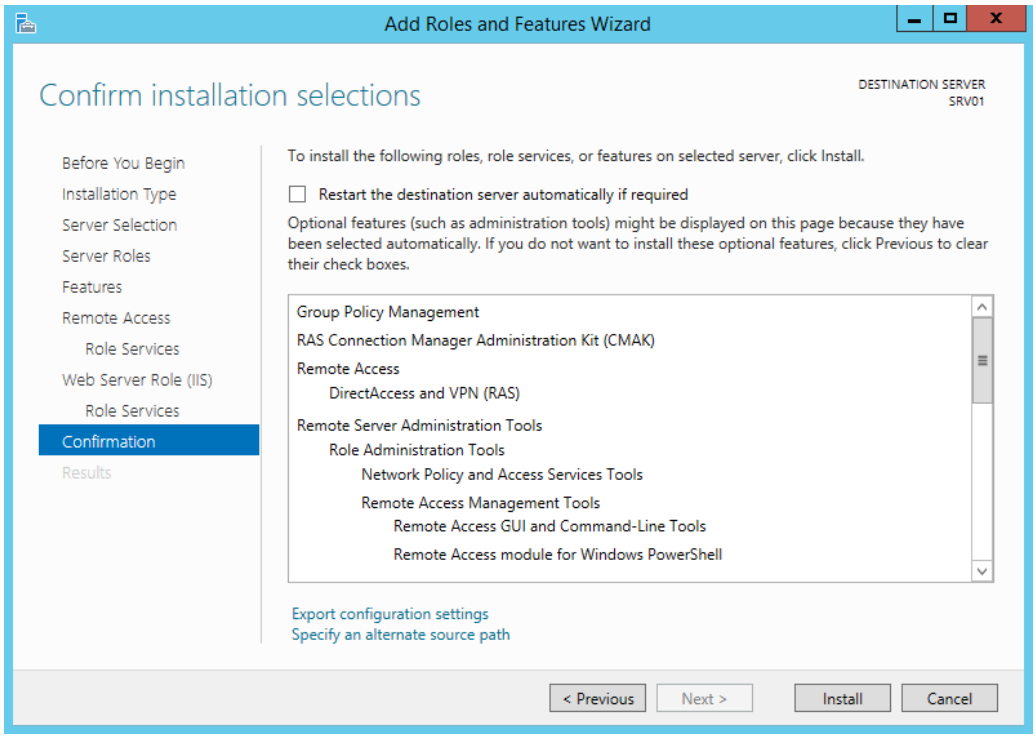
3.1 сурет – «Server Roles» қойындысына «Remote Access» ролын таңдау

Содан кейін осы рөл үшін сервистер тізімінде «DirectAccess and VPN (RAS)» таңдаймыз.



3.2 сурет – «Server Roles» қойындысына «Remote Access» сервисін таңдау

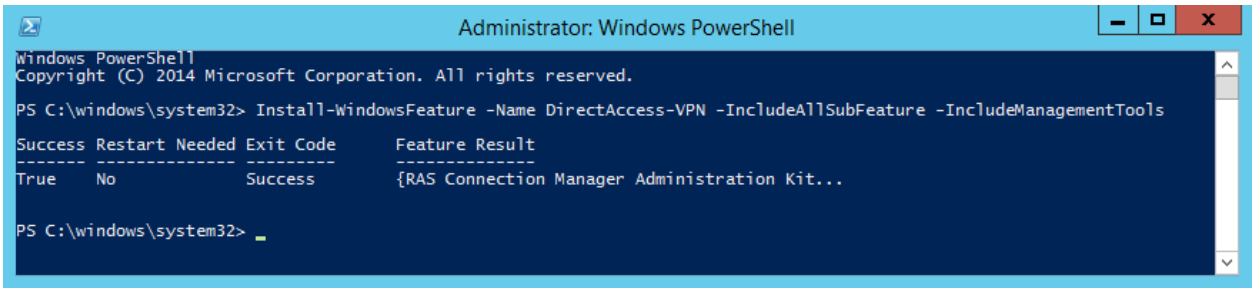
Қашықтан кіру және басқару құралдарының рөлінен басқа, қосымша IIS web-сервері және Windows Ішкі деректер қоры орнатылады. Орнатылған компоненттердің толық тізімін орнатуды бастамас бұрын шебердің соңғы терезесінде көруге болады.



3.3 сурет – Орнатылатын компоненттер

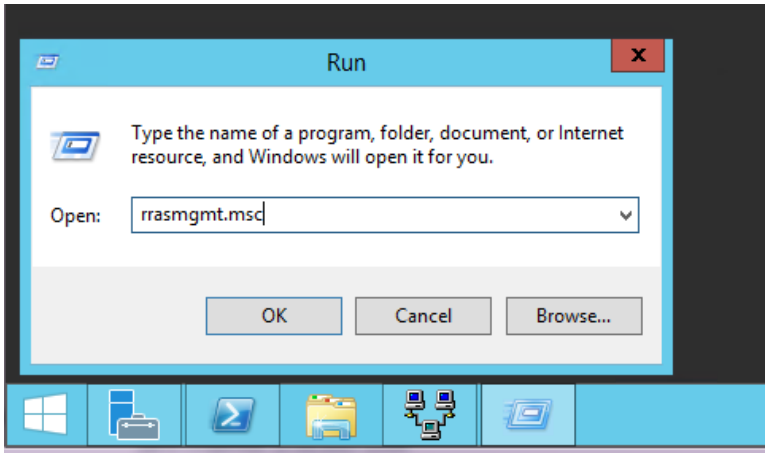
Бірдей, тек әлдеқайда жылдам, PowerShell арқылы жасауға болады. Ол үшін консоль ашып, команданы орындау керек:

Install-WindowsFeature -Name Direct-Access-VPN -IncludeAllSubFeature -IncludeManagementTools



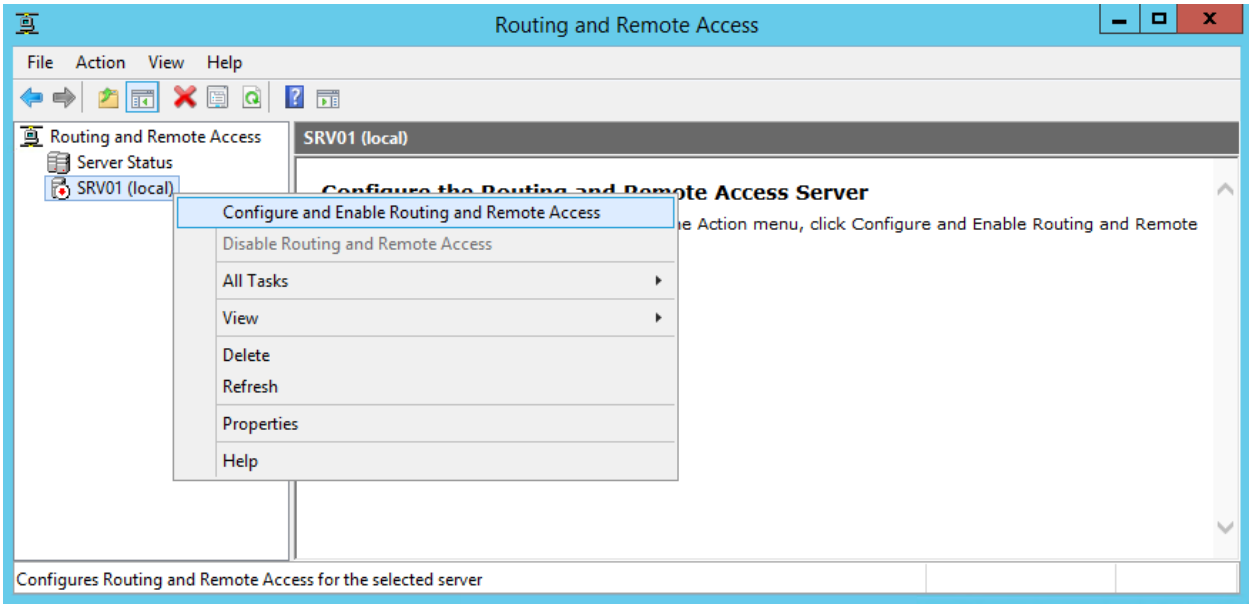
3.4 сурет – Консольде команданы орындау

Рөлді орнатқаннан кейін, "Routing and Remote Access" құралы арқылы қызметті қосу және теңшеу қажет болады. Оны ашу үшін Win+R жуамыз және rrasmgmt командасын енгіземіз.msc.



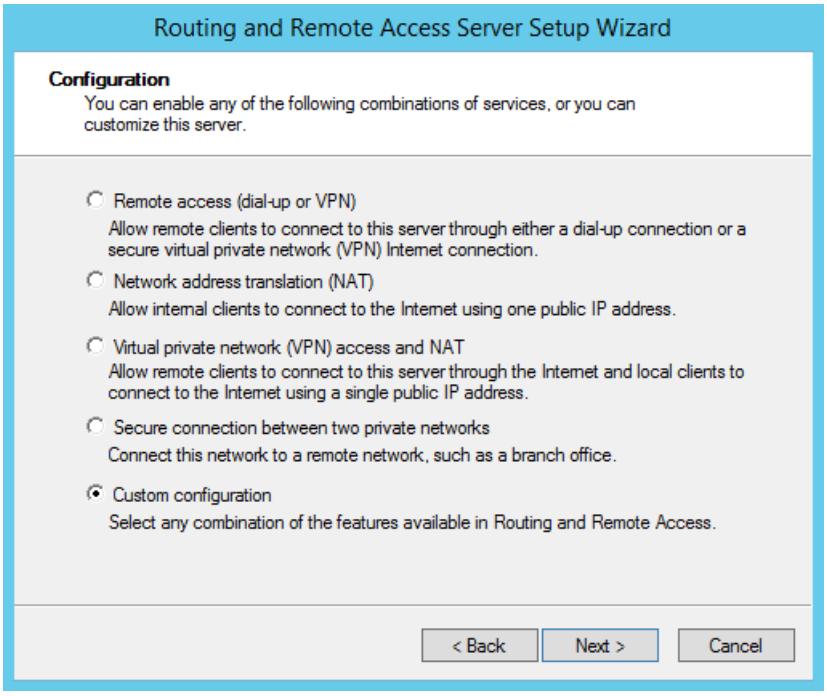
3.5 сурет – rrasmgmt.msc командасын орындау

Сонымен қатар, «Configure and Enable Routing and Remote Access» тармағын таңдаймыз.

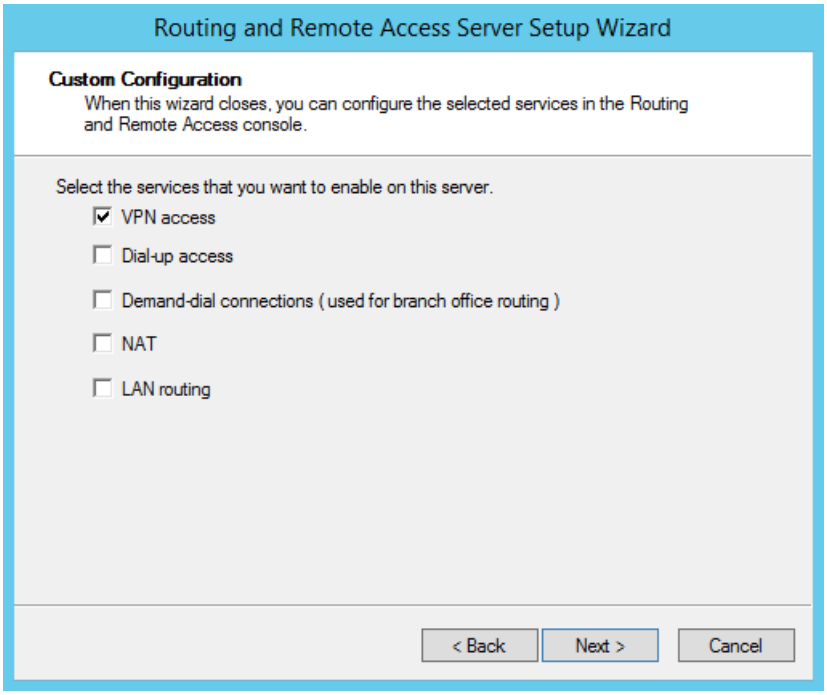


3.6 сурет – Маршруттауды және қашықтан қатынауды баптау және қосу

Орнату шебері терезесінде «Custom configuration» тармағын таңдаймыз және «VPN access» қызметін атап өтеміз.

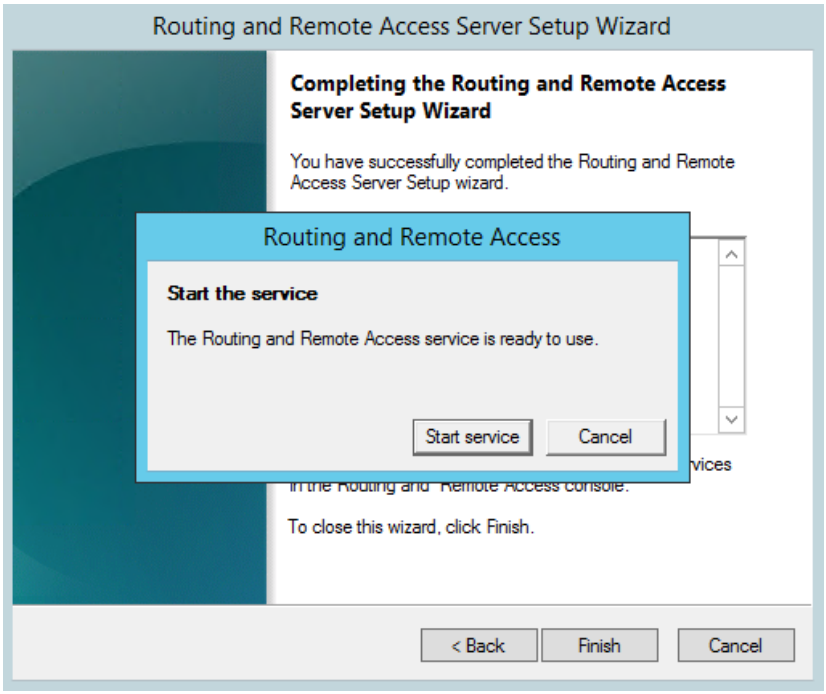


3.7 сурет – «Custom configuration» тармағын таңдау



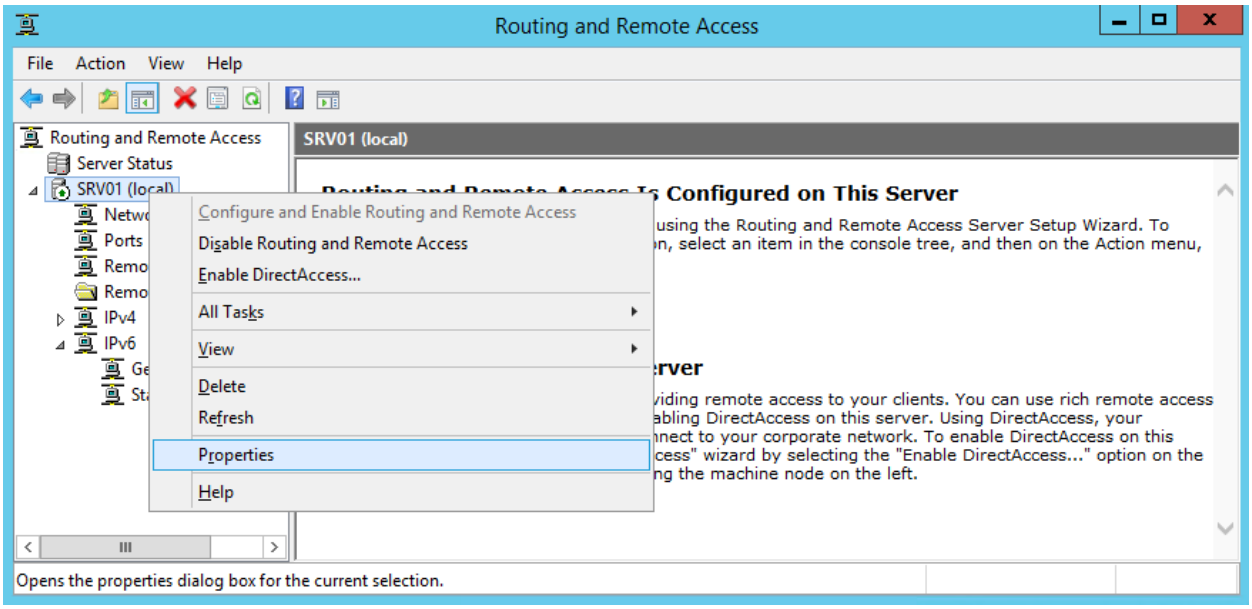
3.8 сурет – «VPN access» сервисін таңдау

Соңында параметрлер бастаймыз сервис қашықтықтан қол жеткізу.



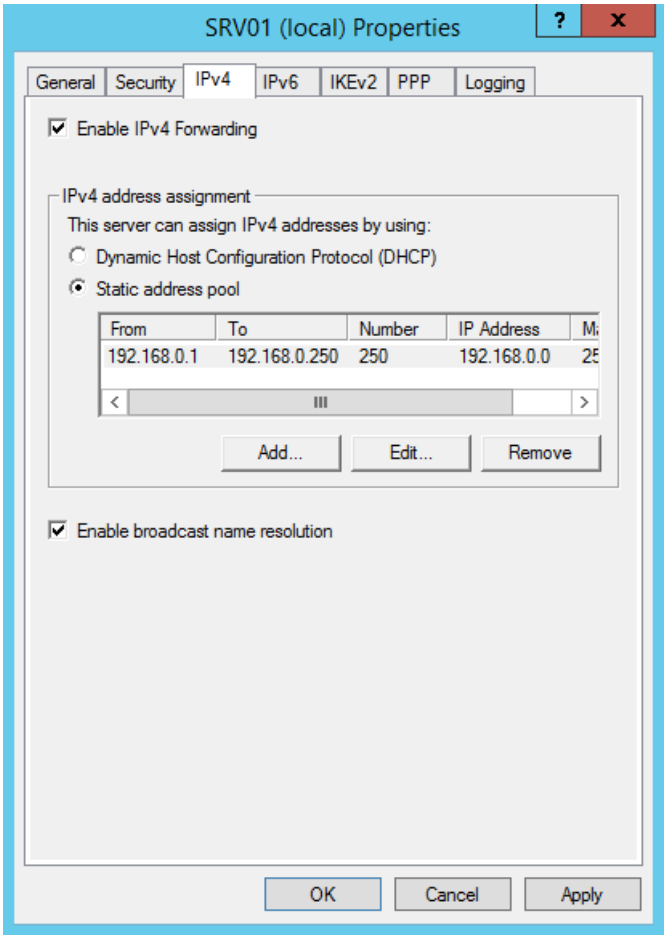
3.9 сурет – Сервис бастау терезесі

VPN сервисі орнатылған және қосылған, енді оны бізге қажетті түрде баптау керек. Мәзірді қайта ашып «Properties» тармағын таңдаңыз.



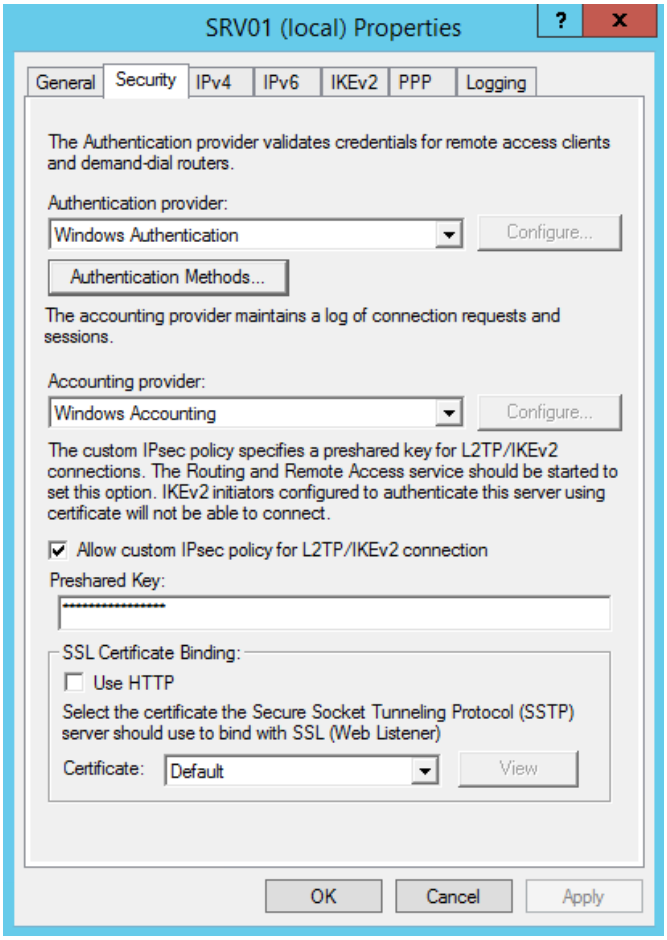
3.10 сурет – Properties пунктін таңдау

IPv4 қойындысына өтіңіз. Егер желіде DHCP сервері болмаса, онда серверге қосылған кезде клиенттер алатын IP адрестерінің ауқымын орнату қажет.



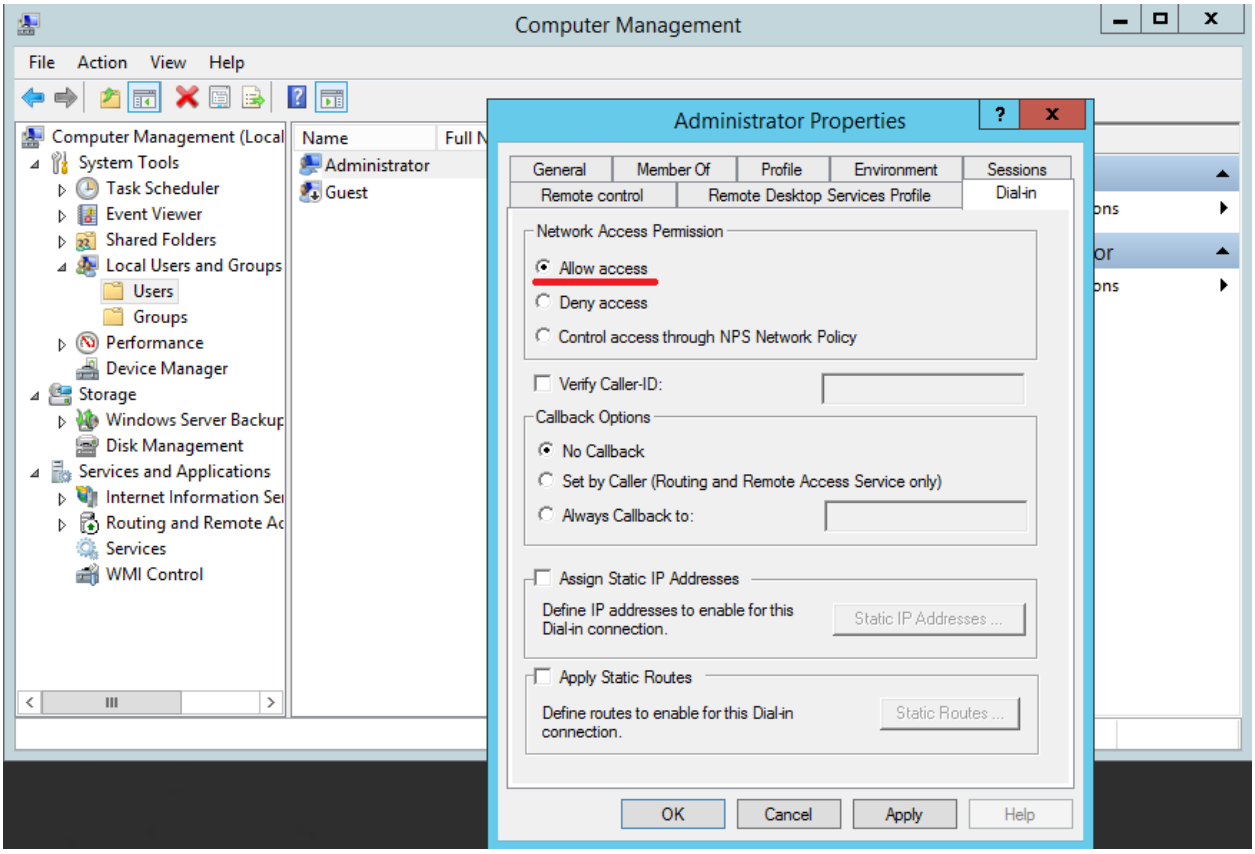
3.11 сурет – IPv4 қойындысы

Қосымша «Security» қосымша бетінде қауіпсіздік параметрлерін орнатуға болады — аутентификация түрін таңдау, L2TP үшін алдын ала кілт (preshared key) орнату немесе SSTP үшін сертификат таңдау.



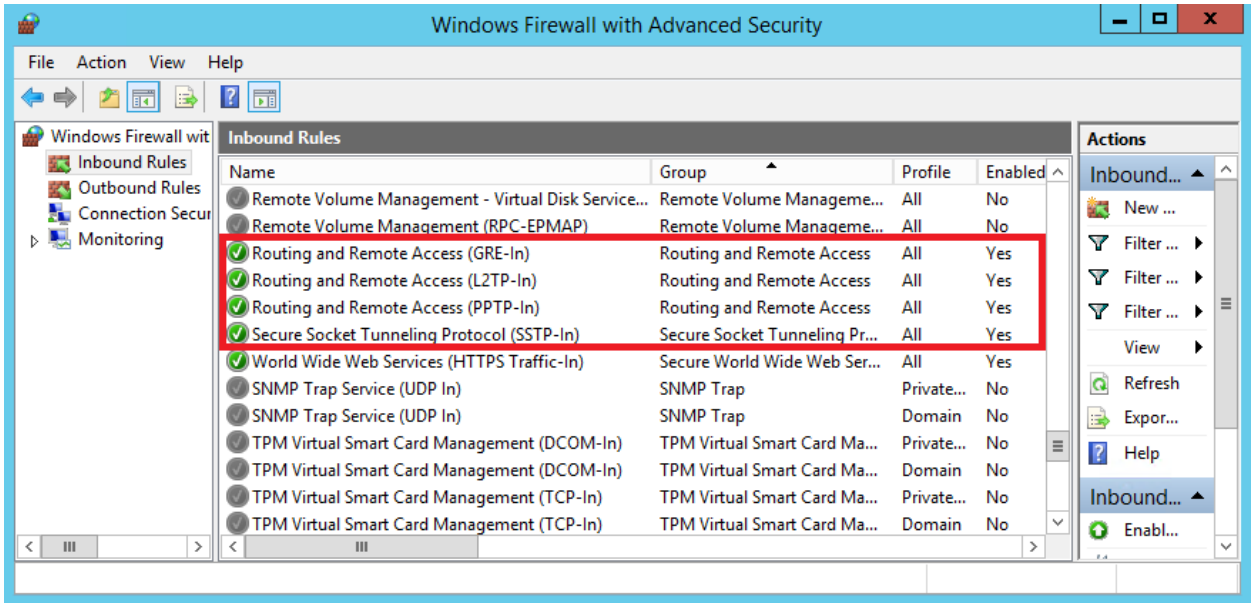
3.12 сурет – Security қойындысы

Сонымен қатар, VPN қосылымынсыз қосылым бола алмайды. Біріншіден, осы серверге қосылуға рұқсаты бар пайдаланушыларды таңдау қажет. Жеке тұрған сервер үшін теңшеу жергілікті, «Computer Management» жабдығында жүргізіледі. Жабдықты іске қосу үшін compmgmt командасын орындау керек.msc, содан кейін «Local Users and Groups» бөліміне өтіңіз. Содан кейін пайдаланушыны таңдап, оның сипаттарын ашып, «Dial-In» қойындысында «Allow access» тармағын белгілеу керек. Егер компьютер Active Directory доменінің мүшесі болса, онда осы параметрлерді «Active Directory Users and Computers» консолынан жасауға болады.



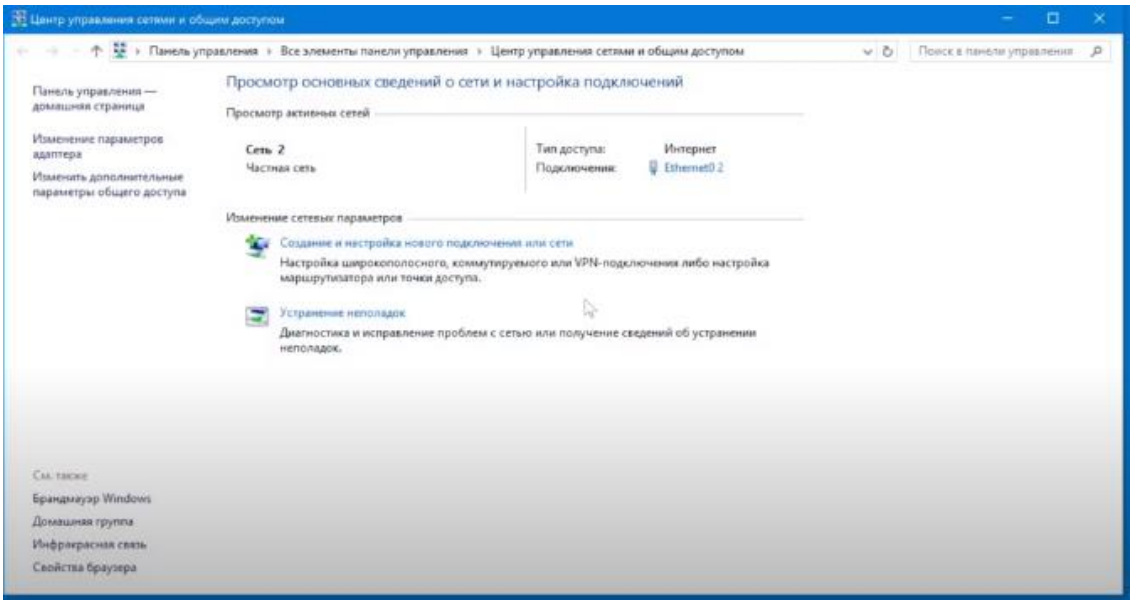
3.13 сурет – Administrator Properties қойындысы

Екіншіден, файлерволлда қажетті порттардың ашылғанын тексеру қажет. Теориялық рөлді қосу кезінде тиісті ережелер автоматты түрде қосылады, бірақ тексеру артық кедергі болмайды.



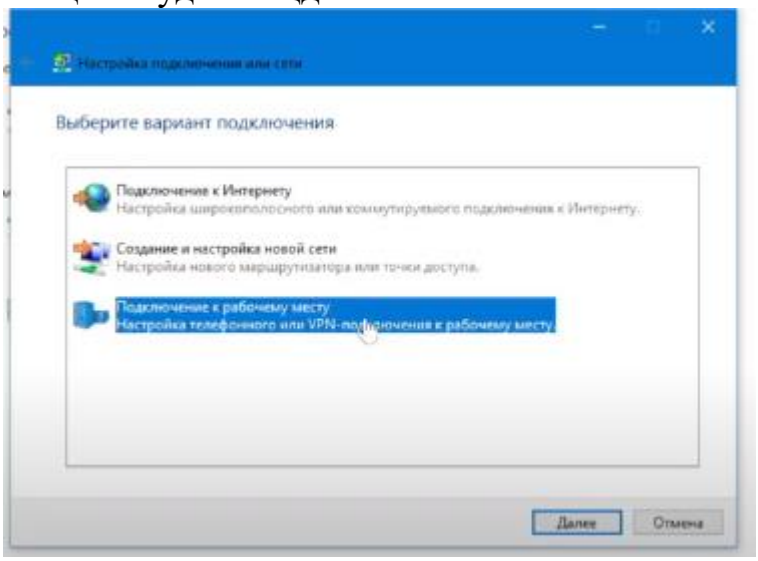
3.14 сурет – Windows Firewall with Advanced Security терезесі

Енді VPN сервері теңшелген және оған қосылуға болады. Келесі әрекеттер клиенттік компьютерден кіріп, баптауды орындаңыз. Бірінші іс-әрекет желілерді басқару орталығына және жалпы қолжетімділікке кіреміз.



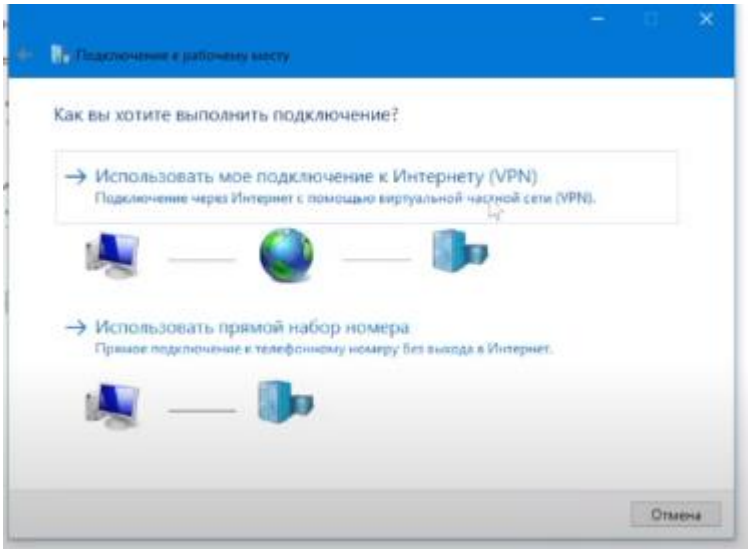
3.15 сурет – Тор және жалпы қатынауды басқару орталығы терезесі

Одан әрі «жаңа қосылуды немесе желіні жасау және баптау» түймесін басып, «жұмыс орнына қосылуды» таңдаймыз.



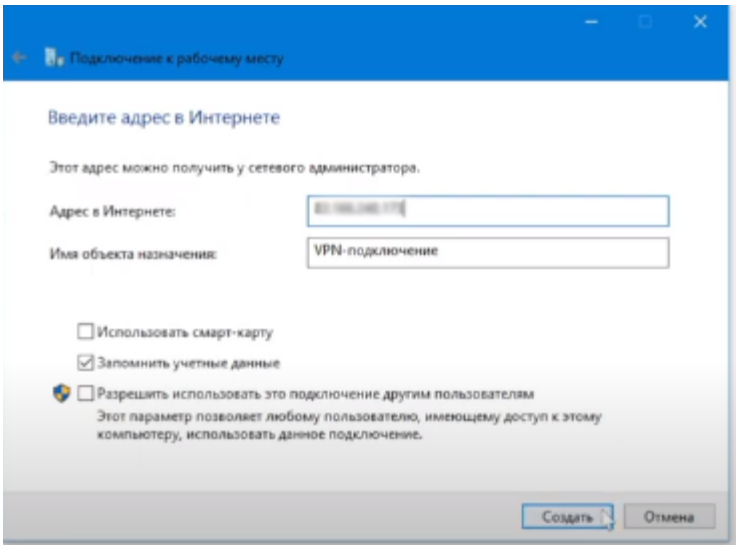
3.16 сурет – Қосылу немесе желі тұнбалары

Келесі әрекет «Менің интернет қосылымымды пайдалану (VPN)»



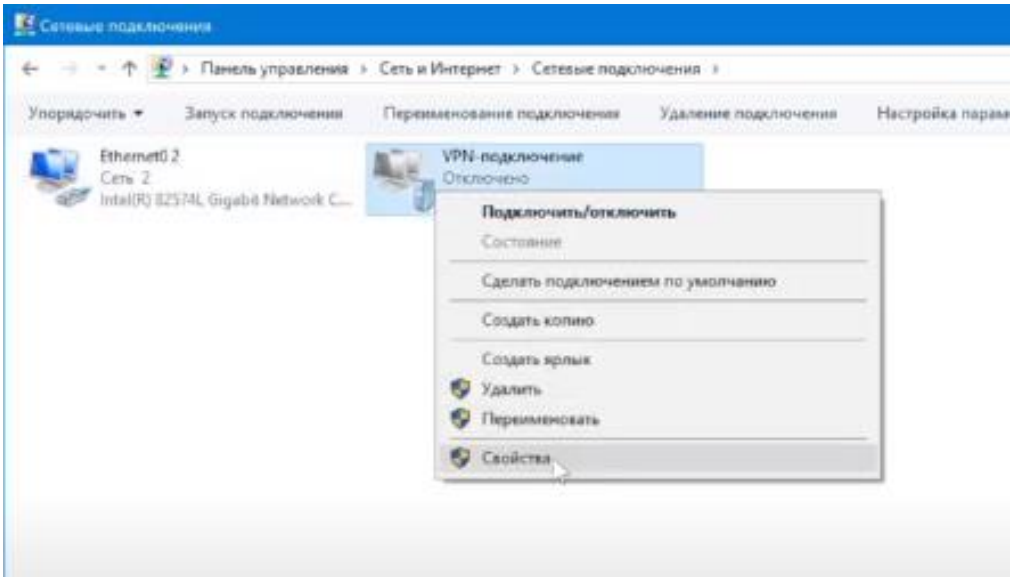
3.17 сурет – Жұмыс үстеліне қосу

Содан кейін пайда болған терезеде біз Ip мекен-жайын және мақсатты нысанның атауын енгізуіміз керек.



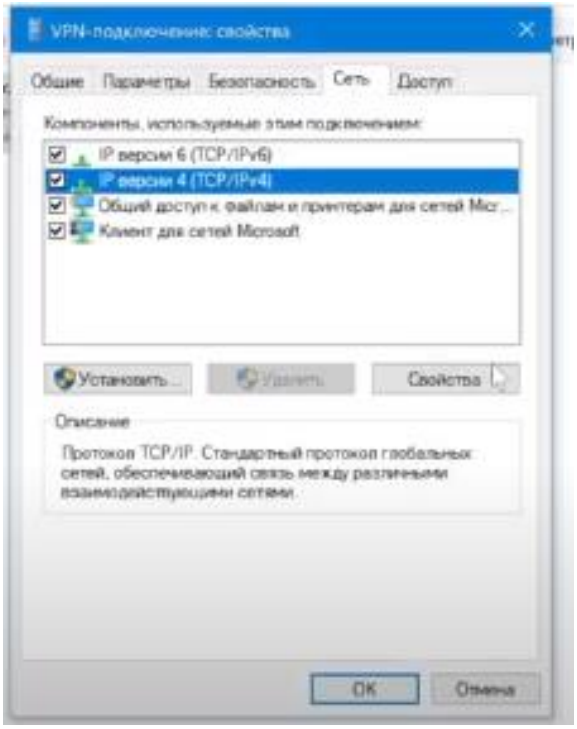
3.18 сурет – IP-адрес енгізу

Енді бізде VPN байланыс құрылды. Одан әрі біздің әрекетіміз желілік қосылымдарға кіріп, vpn-қосылым қасиеттеріне көшеміз.



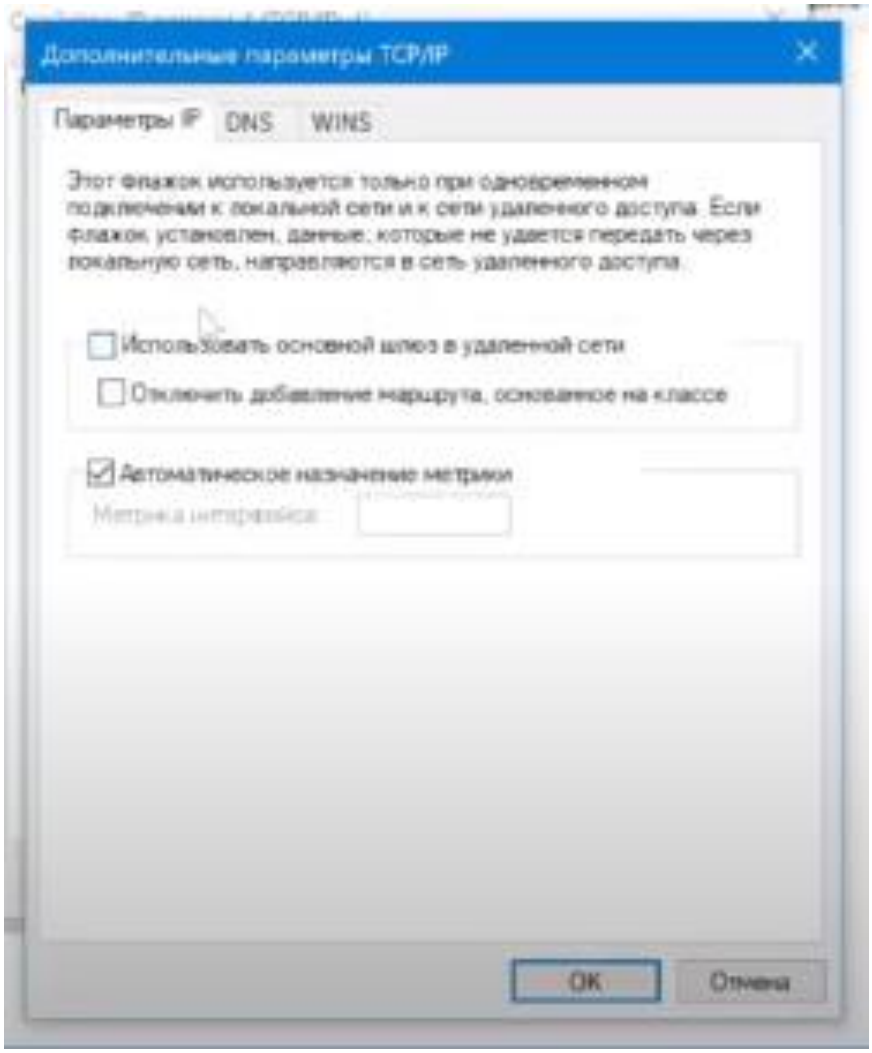
3.19 сурет – Желілік қосылымдар

Содан кейін IP нұсқа 4 (TCP/IPv4).



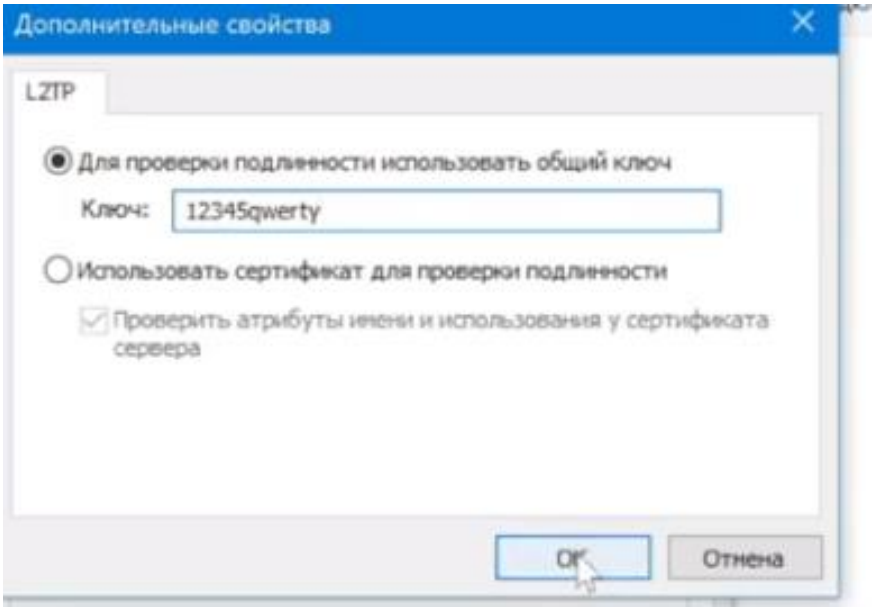
3.20 сурет – VPN-қосылу, қасиеттері

Орнатудың осы кезеңінде сақ болу керек. «IP параметрлері” қойындысында «негізгі шлюзді қашықтағы желіде пайдалану» құсбелгісін алып тастау керек. Бұл жергілікті байланыс жұмысын тоқтатты.



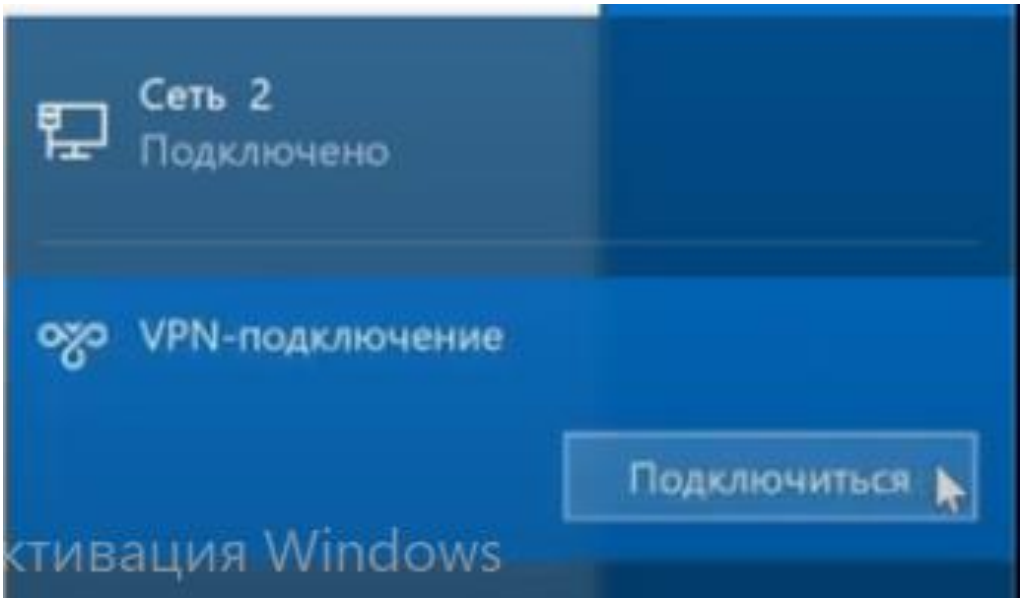
3.21сурет – Қосымша TCP/IP параметрлері

Енді біз vpn теңшеу кезінде орнатылған құпия сөзді енгізуіміз керек.



3.22 сурет – Қосымша қасиеттері

Енді біз корпоративтік желіге қосылған, сондықтан біз оның барлық ресурстарын пайдалана аламыз.



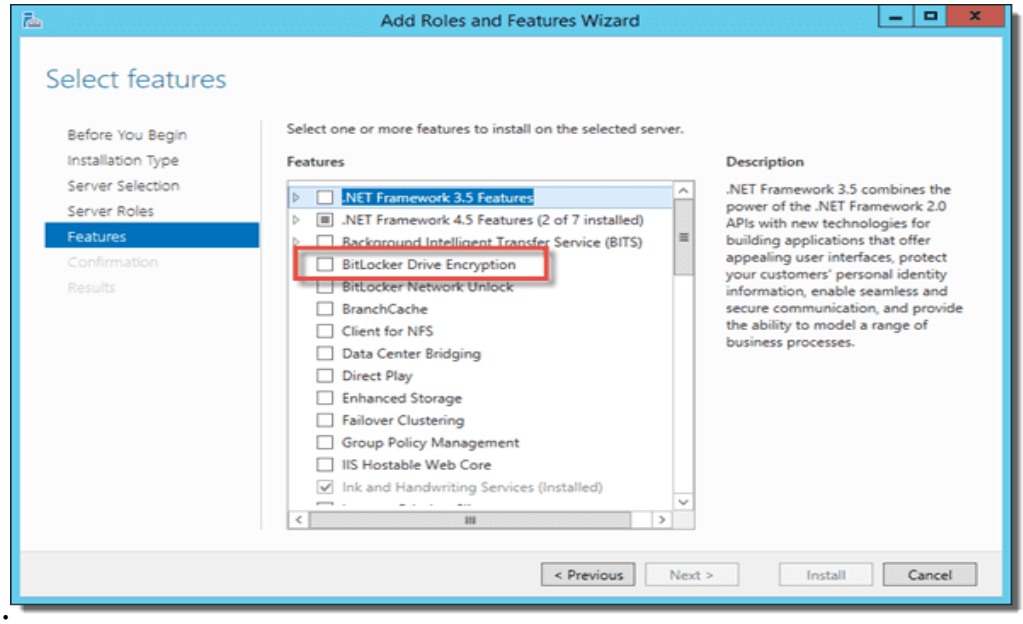
3.23 сурет – Жұмыстың нәтижесі

3.2 BitLocker арқылы деректерді шифрлау

Әдепкі бойынша BitLocker дискісін шифрлау Windows Server орнатылмаған. Оны орнату үшін графикалық интерфейсті пайдалану керек немесе PowerShell командасын іске қосу керек.

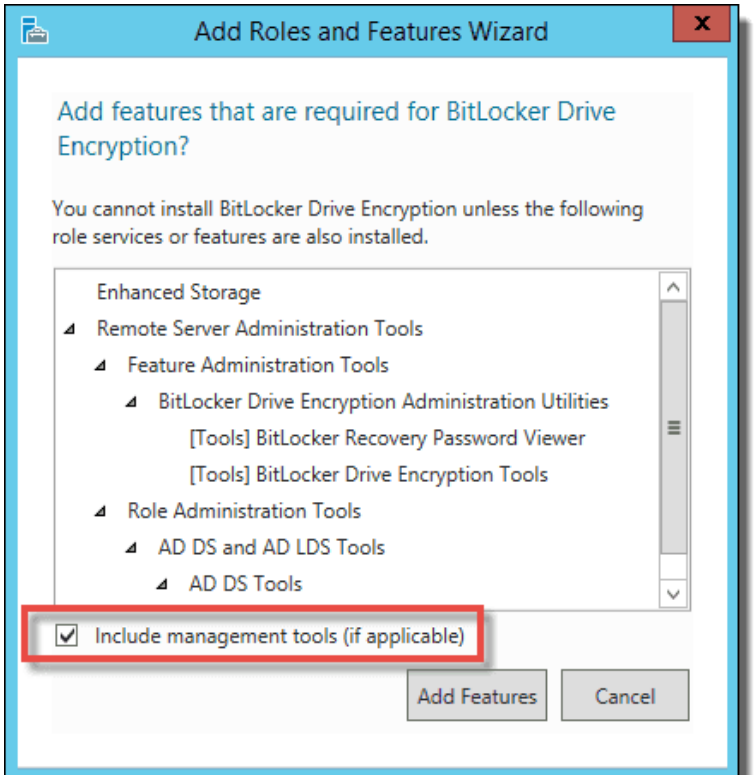
Серверлер реттеушісінде Add roles and features түймесін басыңыз. Экранды бастамас бұрын Бетте Next басыңыз және одан әрі орнату түріне қайтадан, нәтижесінде role-based or feature-based installation әдепкі. Серверіңізді таңдап,

«Next» түймесін қайта басыңыз. Next түймесін басу арқылы сервер рөлін жіберіп алыңыз. Функциялар терезесінде «BitLocker Drive Encryption».



3.24 сурет – Рөлдер мен компоненттерді қосу шеберінде BitLocker дискісін шифрлауды орнату

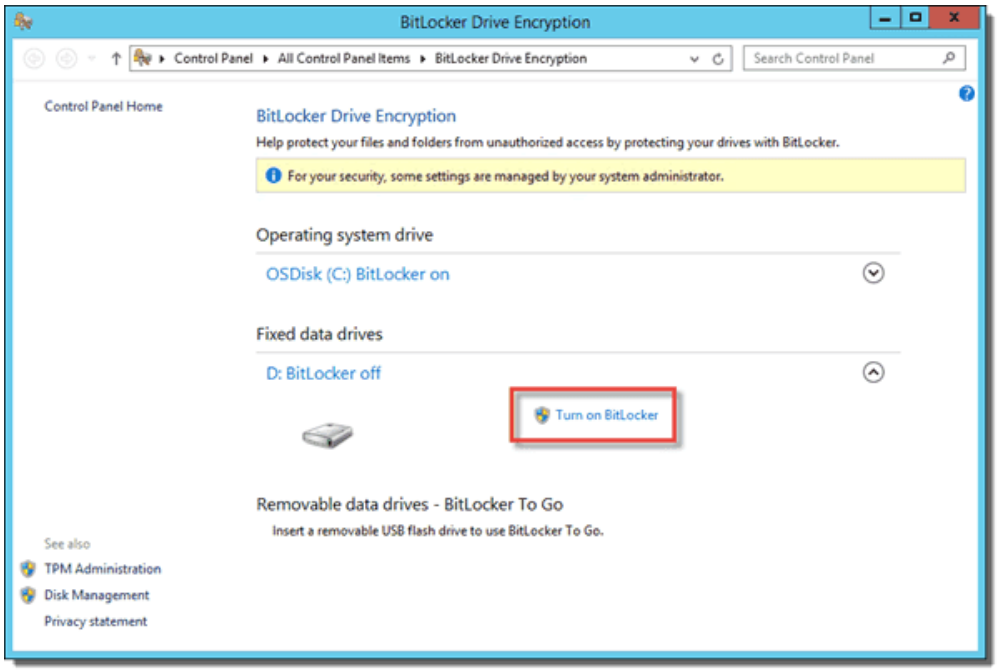
Сұрау пайда болған кезде Include management tools (if applicable) құсбелгісін қойып, Add Features түймесін басыңыз.



3.25 сурет – BitLocker дискісін шифрлау үшін басқару құралын қосу

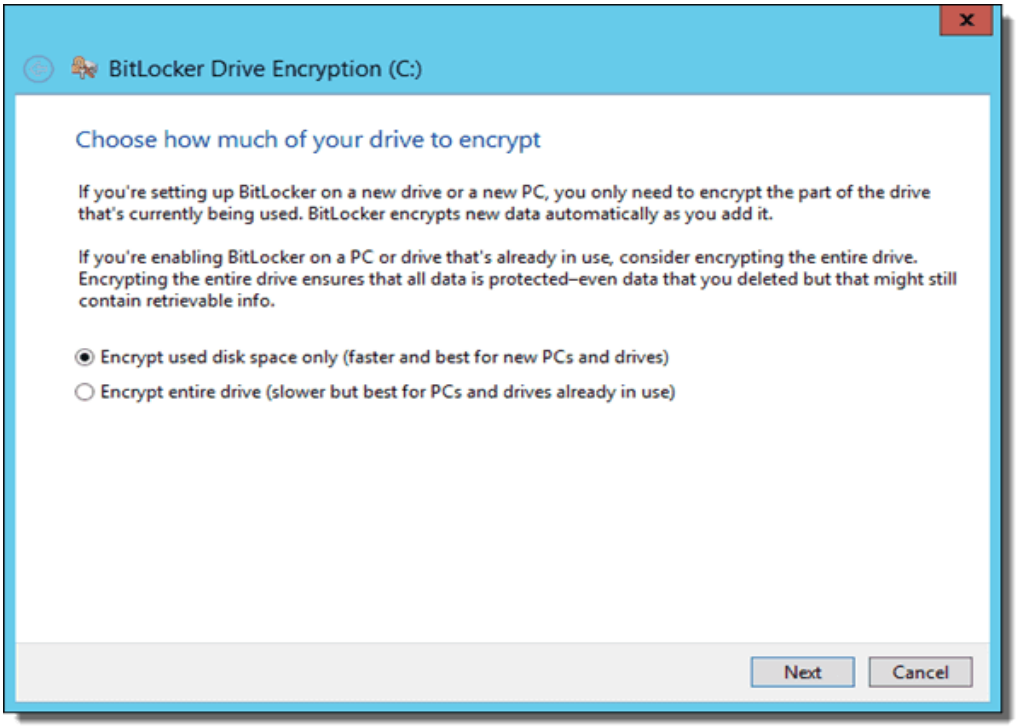
Select Features терезесіне оралғанда Next басыңыз. Орнату процесі қайта жүктеуді талап етеді; Restart the destination server automatically if required таңдап, Install түймесін басыңыз. Yes түймесін басып, қайта жүктеу туралы ескертуді қабылдаңыз, содан кейін Install түймесін соңғы рет басыңыз.

Деректер қатты дискісін графикалық интерфейсте шифрлау үшін басқару панеліне өтіп, BitLocker дискісін шифрлауға өтіңіз. Деректер дискілері бөлімінде BitLocker Turn on BitLocker түймесін басыңыз.



3.26 сурет – Қатты дискілер үшін графикалық интерфейсті пайдаланып BitLocker қосу

Содан кейін сіз Encrypt useddiskspace only or Encrypt entire drive қалайсыз ба таңдау керек. Егер сіз жаңа сервермен жұмыс істесеңіз, қолданылатын диск кеңістігі дискіні жылдам шифрлайды. Егер сіз пайдаланылған сервермен жұмыс істесе, барлық кеңістік (бос кеңістікті қоса алғанда) шифрлануы үшін барлық дискінің опциясы қолайлы опция болып табылады. Сіз таңдау жасағаннан кейін Next басыңыз.



3.27 сурет – Шифрлеу үшін дискіңіздің көлемін таңдау: пайдаланылатын кеңістік немесе бүкіл диск

Соңғы экранда «Run BitLocker system check» белгісін орнату арқылы жабдықты тексеруді таңдай аласыз. Егер сіз осы өрісті таңдасаңыз, компьютерді қайта іске қосу керек. Шифрлау процесін бастау үшін «Start encrypting» түймесін басыңыз.

3.28 сурет – Шифрлеу таңдағаннан кейін BitLocker жүйесін тексеруді іске қосу»

Бөлім бойынша қорытынды: бұл бөлімде виртуалды қорғалған VPN желісін құру жәнеде BitLocker арқылы деректерді шифрлау іс жүзінде көрсетілген.

4 Өміртіршілігінің қауіпсіздігі

4.1 Еңбек жағдайларын талдау

Бұл бөлімінде дипломдық жобаның "Microsoft Windows Server құралдарымен қауіпсіздік профилін құру" өндірістік тәуекелдерді зерттеу Қалыпты еңбек жағдайларын анықтауға, сонымен қатар адамның денсаулығы мен өміріне жұмыс ортасында зиян келтіретін факторларды анықтауға бағытталған қырлар кешені. Жұмыс орнында программисттерге екі ноутбук және модем орнатылған. Ноутбуктар ғаламторға Wi-fi арқылы немесе RJ-45 кабелі арқылы модемге байланысады.

Бағдарламалық жасақтаманы құру кезінде әзірлеуші компьютермен ұзақ уақыт жұмыс істеуге мәжбүр. Осы бөлімде адамға кері әсер ететін кейбір факторларға тексеру жүргізілді. Санитарлық-эпидемиологиялық нұсқауларға сәйкес қондырғы көздерімен жұмыс істеу жағдайларына қойылатын физикалық факторлар (ДК) әсер ететін адамдарға жеңіл 1б санатта қолайлы микроклиматтық көрсеткіштер мынадай шарттар болып табылады:

- қыста температура 23-21ºС, жылдың ыстық мезгілінде 22-24ºС, мұндағы ауа ылғалдылығы 40 - 60%;

- жылдың ыстық мезгілінде ауа айналымының жылдамдығы 0,2 м/с, қыста 0,1 м/с.

Бұл көрсеткіштер жұмыс орнында іске асырылуы тиіс. Барлық электроника өрттің әлеуетті көзі болып табылады. Өрт туындауының алдын алу үшін электрондық техника қауіпсіздік шаралары сақталынды: техника мен электр кабельдерінің дұрыс орналастырылды. Сондай-ақ инциденттердің туындауын болдырмау үшін физикалық әсерден қорғалған электр желісі, электрмен қоректендіруге қосудың сапалы нүктелерін, өрт қауіпсіздігі шараларын қатаң сақтауды, электр желісіне жүктемені сауатты есептеуді, жабдықты шаңмен немесе басқа заттармен ластанудан тұрақты тазалау жүзеге асырылды, электр қоректендіруге қосу нүктелерінде тұйықталуды болдырмау үшін физикалық әсер мөлшерін азайтылды. Электротехниканың жұмысы барысында электр өрісі пайда болады, ол әртүрлі жақын тұрған заттарға әсер етеді. Мысалы, компьютер кулерінің жұмысы кезінде электрлендірілген шаңның шығуы орын алады, ол адамға кері әсер етеді. Компьютерлік мониторлар статикалық электрдің күшті жинақтаушысы болып табылады. Бүгінгі таңда адамға статикалық электрдің қандай әсер ететіні туралы толыққанды деректер жоқ. Зерттеулерге сәйкес, статикалық электрдің әсерінен адамның терісінің жүйке бітеулерінің тітіркенуі болады, сондай-ақ бұл әсер матаның иондық құрамының өзгеруін тудырады.

Бұл әсерлердің барлығы шаршауға, толыққанды болмаған ұйқыға және тітіркенуге әкеледі. Статикалық электрдің адамға кері әсерін болдырмау үшін ұсыныстар мынадай: жұмыс кеңістігі шегінде ауаны ылғалдандыру, ылғалды жинау (ылғалдылығы 50% - дан артық емес), электротехниканы жерге тұйықтау,

бөлмені тұрақты желдетілуін ұйымдастыру. Сонымен қатар ДК-мен ұзақ жұмыс кезінде адамға электромагниттік әсердің пайда болуы ықтималдығы үлкен. Бұл әсерді болдырмау үшін бөлмені тұрақты желдету, физикалық жүктеме, жұмыс орнына тек барлық қауіпсіздік шаралары мен санитарлық нормаларға жауап беретін ғана сапалы жабдықты орнату ұсынылады.

Компьютермен жұмыс істеу кезінде маңызды аспектілердің бірі бөлменің жарықтандырылуы болып саналады. Табиғи жарықтандыру өте маңызды, сондықтан компьютердің терезеге қатысты орналасуы өте маңызды. Компьютерді терезеден жарық тікелей түспейтіндей орналастырылды. Әйтпесе, бұл жұмыс кезінде көздің шаршауына себеп болады. Шешім - күн сәулесінен қорғайтын жалюзи немесе тығыз перделерді қолдану.

Жұмыс кезінде компьютерді пайдаланушыға әсер ететін жоғарыда айтылған зиянды және қауіпті жағдайлардан басқа, компьютерде жұмысты дұрыс ұйымдастырмаудан туындаған басқа да зиянды жағдайларды да бөліп көрсетілді. Осылайша, ұзақ отырып жұмыс істеу адамға зиян болып саналады, жұмыс орнын ұйымдастыруға көп көңіл бөлінді. Ұзақ уақыт бойы бір қалыпта болуы бұлшықетті үнемі демалыссыз жұмыс істеуге мәжбүр етеді. Аз қозғалу - компьютерлерді пайдаланушылардың және бағдарламалық қамтамасыз етуді әзірлеушілердің басты проблемасы. Ұзақ отырудан туындаған физиологиялық қызметтің азаюы кезінде семіздік, геморрой, остеохондроз сияқты ауру қаупі артады. Дұрыс емес қалыпта отырғандағы бүкірлік арқылы дискілерді деформациялап, жарақаттап, омыртқаға теріс әсер етеді.

Бұрын сипатталған психофизиологиялық қауіпті және зиянды жағдайлар әсер ету сипаты бойынша мынадай бөлінеді:

- физикалық (статикалық және динамикалық);
- жүйке-психикалық (ақыл-ойдың артық тырысуы, талдағыштардың артық тырысуы, еңбектің монотондылығы және эмоциялық артық жүктеме);
- компьютерде жұмысты ұйымдастыру шарттары;
- жұмыс бөлмесінде табиғи және жасанды жарықтандырудың болуы;
- бөлмені кондиционерлеу жүйелерімен немесе тиімді желдеткішпен жабдықталуы; бөлме сағат сайын желдетіледі;
- бөлменің күнделікті ылғалды тазалау;
- күн сәулесінің тікелей түсуінен аулақ болу үшін перделерден немесе жалюздерден пайдалану;
- біркелкі жасанды жарықтандыру. Барлық еңбек нормаларын сақтау үшін қажет қосалқы есептеулер бұдан әрі келтірілген.

4.1.1 Жұмыс орнының сипаттамасы

Ғимаратты жобалау және құру кезінде ҚР ҚНжЕ 3.02-04-2009 [12] нормасымен анықталды.

Жұмыс бөлмесі бір жұмыс орнына жабдықталған. Жұмыс бөлмесі Қазақ Тамақтану Академиясының ғимаратында, 2 қабатта орналасқан. Бөлме жолдан алыс ғимараттың соңында орналасқандықтан әр түрлі шу көздері жұмыс барысына әсер ете алмайды.

Бағдарламалық қамтамасыз етуді әзірлеу жүргізілетін бөлмені қарастырайық (5.1-сурет). Бөлме өлшемдері: ұзындығы (L) = 4 метр, ені (B) = 3,5 метр, биіктігі (H) = 2,8 метр. 01.12.2011 жылғы санитарлық талаптарға сәйкес ДК және сұйық кристалды дисплейді пайдаланушылардың бір жұмыс орны ауданы 4,5 шаршы метрден кем болмауы тиіс. Жұмыс орнының жалпы ауданы 14 ш. м. болғандықтан санитарлық талаптарды қанағаттандырады.

4.1 сурет - Жұмыс бөлмесінің жоспары

4.1.2 Өрт қауіпсіздігі

Өрт қауіпсіздігі персоналдың жұмыс ортасының қауіпсіздігін қамтамасыз етудегі ҚР ҚНжЕ 2.02-05-2009 [13] құрылыс проект нормасымен анықталады. Өрт қауіпсіздігі-өрт мүмкіндігін толық жоққа шығаратын, ал ол туындаған жағдайда адамдарға өрттің жағымсыз факторларының әсерін болдырмайтын және жұмыс ортасы мен материалдарын қорғау қамтамасыз етілетін объектінің жай-күйі.

Өрт қауіпсіздігі өрттің алдын алу жүйесімен және өрттен қорғау жүйесімен қамтамасыз етілді.

Жұмыс орнындағы өрттер аса қауіпті, себебі үлкен материалдық шығындармен байланысты. Жұмыс орнының ерекшелігі - бөлменің шағын аудандары. Өрт жанғыш заттардың, тотығу мен тұтану көздерінің өзара әрекеттесуі кезінде туындайды. Жұмыс орнында өрт пайда болу үшін қажетті барлық үш негізгі фактор бар.

Жанғыш компоненттерге бөлмені әрлеуге арналған материалдар, қалқалар, есіктер, едендер, кабельдерді оқшаулау және т. б. жатады.

Өртке қарсы қорғаныс – бұл адамдардың қауіпсіздігін қамтамасыз етуге, өрттің алдын алуға, оның таралуын шектеуге, сондай-ақ өртті сәтті сөндіру үшін жағдай жасауға бағытталған ұйымдастырушылық және техникалық іс-шаралар кешені.

От алдыру көздері ЭЕМ-нің электрондық схемалары, техникалық қызмет көрсету үшін қолданылатын аспаптар, жануға қабілетті электрмен қоректендіру құрылғылары болып саналады. Сондай-ақ оларды ӨҚ талаптарына сәйкес келмейтін жағдайда сақтау немесе пайдалану.

Жұмыс орнындағы өрт өте қолайсыз салдары: құнды ақпараттың жоғалуы, мүліктің бүлінуі, адамдардың қаза болуы және т. б.

Өрттің шығу себептері:

- электр сымдарының, розеткалар мен ажыратқыштардың қысқа тұйықталуына немесе оқшаулау сынамасына әкелу ақаулары;
- ақаулы электр құралдарын пайдалану;
- бөлмені ашық қыздыру элементтері бар электр қыздыру аспаптарын пайдалану;
- ғимаратқа найзағайдың түсуі салдарынан;
- ғимараттың жануына ықпал ететін сыртқы әсерлер;
- отты ұқыпсыз қолдану және өрт қауіпсіздігі шараларын сақтамау.

Өрт алдын алу адамдардың қауіпсіздігін қамтамасыз етуге, өрттің алдын алуға, оның таралуын шектеуге, сондай-ақ өртті сәтті сөндіру үшін 81 жағдай жасауға бағытталған ұйымдастырушылық және техникалық іс-шаралар кешені болып табылады. Өрттің алдын алу үшін ғимараттың өрт қауіптілігін дұрыс бағалау, қауіпті факторларды анықтау және өрт алдын алу және қорғау тәсілдері мен құралдарын негіздеу өте маңызды.

Өрт қауіпсіздігін қамтамасыз ету шарттарының бірі-тұтанудың ықтимал көздерін жою.

Жұмыс ортасында тұтану көзідері:

- электр жабдықтарының ақаулары, сымдардағы, электр розеткалары мен ажыратқыштардағы ақаулар. Сондықтан, ақауларды уақтылы анықтау және жою, жоспарлы тексеріс жүргізу және барлық ақауларды уақтылы жою үшін өрттің алдын-алу өте маңызды;
- электр құрылғыларының ақаулығы. Өртті болдырмауға қажетті шараларға электр құрылғыларын уақтылы жөндеу, бұзылған электр құрылғыларын сапалы емес жөндеу кіреді;
- бөлмені ашық жылыту элементтері бар электр жылытқыштарымен жылыту. Қыздырылған беттердің шығуы өртке әкеледі, өйткені бөлмеде кітаптар, нұсқаулықтар және қағаз түріндегі қағаз құжаттары мен анықтамалықтар бар.

- жанғыш зат. Өрттің алдын алу үшін зертханада ашық жылыту құрылғыларын пайдаланбауды ұсынамыз;
- сымдағы қысқа тұйықталу. Қысқа тұйықталу салдарынан өрт шығу ықтималдығын азайту үшін сымды жасырын істедік.

Өрт қауіпсіздігі шараларын сақтамау және бөлмеде темекі шегу өрттің шығуына әкеледі. Лабораторияда темекі шегудің салдарынан болатын өртті жою үшін мен темекі шегуге үзілді-кесілді тыйым салуды және оған тек белгіленген жерде рұқсат етуді ұсынамын [14].

Өрт туындаған кезде алдымен электр қуатын өшіріп, өрт сөндіру бригадасын шақырып, эвакуация жоспарына сәйкес адамдарды бөлмеден шығарып, өрт сөндірушілермен өртті сөндіруге кірісу керек. Егер кішкене жалын болса, ауаны тұтату қондырғысына жетпеу үшін қолдағы құралдарды пайдаланылады.

4.1.3 Электр қауіпсіздігі

Қоғамдық ғимараттардың электротехникалық құрылғылары Қазақстан Республикасының электр қондырғыларын орнату ережесіне, ҚР ҚНжЕ 2.04-01-2001 [14] талаптарына сәйкес жобаланады.

Электр қауіпсіздігі — адамдарды электр тогының, электр доғасының, электрлі магнит өрісінің және статикалық электрдің зиянды және қауіпті әсерінен қорғанысын қамтамасыз ететін ұйымдастыру-техникалық шаралардың және құралдардың жүйесі.

Жергілікті электр жарақаттары электр тогының дене ұлпалары мен мүшелерін зақымауы: күюлер, электр таңбалары, терінің электр металдануы және электроофтальмия (көздің қарығуы) болып табылады.

Токтың келесі шектік мәндерін бөліп атауға болады:
- токты сезу шегі –ең аз сезілетін ток (0,5 -1,5мА);
- босатпайтын ток шегі –адам өз бетімен бұлшық еттері электродтармен
- қамтылған әрекеттен босана алмайтын ең аз ток мөлшері (6-10мА). Бұдан аз токтар босататын болып есептеледі;
- қаза ететін (100 мА және одан астам) ток.

Изоляцияның бүлінуінің әсерінен кернеу астында қалған металды құрылымдарды немесе электр құрылғылардың корпусын ұстау нәтижесінде алынатын электрлік жарақаттарды болдырмау және аппаратураларды қорғау үшін қорғанысты жерлендіру орналастырылады. Ол электр қондырғылардың метал бөліктерін жермен әдейі жалғау арқылы жасалынады.

Жерлендіру құрылғыларын (ЖҚ) жобалау кезінде адамның электр тоғымен жарақат алу ықтималдылығы ескеріледі. Алайда, бірде-бір салада және жалпы өмірде адамдардың толық қауіпсіздігін қамтамасыз ете алмайды.

Сондықтан, ЖҚ-ның аймағында қауіпсіздікті қамтамасыз ету мәселесін адам электр тоғымен жарақат алу қаупі жағдайының болу ықтималдылығын азайтады.

Тиімді жерлендірген желілерде электр қауіпсіздігі қамтамасыз етілген деп жерлендіргіштегі φж потенциалы 10 кВ-тан аспайтын, ал жерлендіргіштің нәтижелі кедергісі жылдың кез-келген мерзімінде 0,5 Ом-нан аспайтын болып саналады.

4.1.4 Жерлендіру

Жасанды қорғаныстық жерлендіру құрылғыларын орнату кезінде ЭҚО ережелері сақталды, бұл ережелер мен талаптар ҚР ҚНжЕ 4.04-10-2002 [15] талаптарына сәйкес жобаланады. Әкімшілік ғимараттың электр қондырғыларындағы потенциалды теңестіру үшін келесі өткізгіш бөліктерді қосатын Негізгі потенциалды теңестіру жүйесі енгізілді:

- жеткізу желісінің қорғаныс өткізгіші (PE немесе PEN);
- жерге тұйықталу электродына қосылған жерлендіргіш;
- ғимаратқа кіретін инженерлік желілердің металл құбырлары;
- ғимараттың металл қаңқасы;
- орталықтандырылған желдету және ауа баптау жүйелерінің металл бөліктері. Сондай-ақ, кондиционерлер мен желдеткіштерге арналған электр шкафтарының PE шинасына қосылған осы жүйелердің автономды металл ауа каналдары бар;
- найзағайдан қорғау жүйесі;
- функционалды (жұмыс істейтін) жерге тұйықтаушы өткізгіш.

Бұл бөліктердің бір-бірімен байланысы негізгі жерге қосу шинасы (қысқыш) көмегімен жасалады.

Ғимараттар мен құрылыстар үшін негізгі жерге қосу шинасы (қысқыш) ВУ (ВРУ) кіріс құрылғысының ішінде жасалады. ВУ ішінде PE шинасы негізгі жерге қосу шинасы ретінде қолданылды.

Жеке орнату үшін негізгі жерге қосу шинасы ғимараттың электр қондырғысын басқару блогының жанында қол жетімді, техникалық қызмет көрсетуге ыңғайлы жерде орналастырылды.

Жеткізу желісінің PE - өткізгіші (PEN - өткізгіш) өткізгіштігі өткізгіштік PE (PEN) - жеткізу желісінің өткізгішінен кем емес өткізгішті қолдана отырып, негізгі жерге қосу шинасына қосылған PE VU шинасына қосылған.

ВУ ішіндегі негізгі жерге тұйықтау шинасын орындау кезінде оның өткізгіштік қабілеті PEN - өткізгіш өткізгіштің өткізгіштігінен кем емес.

Жерге қосу құрылғыларын орнату тиісті ГОСТ-тың техникалық талаптарына сәйкес келетін монтаж өнімдерін қолдану арқылы жүзеге асырылды.

Жерге қосылатын электр қондырғысының әр бөлігі жеке тармақты қолданып жерге қосу желісіне қосылған.

4.2 Есептеу бөлімі

4.2.1 Жерлендіру есебі

Есеп әдістемелік нұсқауларымен жүргізілді [16]. Жұмысты электр қондырғыларын техникалық пайдалану ережелеріне сәйкес жүргізеді. Сонымен қатар электр құралдарымен жұмыс істеу кезінде қауіпсіздік техникасы бойынша кіріспе және мерзімді нұсқамалар сақталды, еңбек тәртібін орындалды , жұмыс орнын дұрыс ұйымдастыралды. Жерлендіру шиналары қол жетімді жерлерде орналасқан. Қорғау үшін жабдық пен аспаптардың ток өткізгіш бөліктеріне жанасу оқшаулауды, ток өткізгіш бөліктерінің орналасуы мен қоршауын пайдаланады. Жабдықтың металл бөліктеріне жанасу кезінде кездейсоқ кернеу астында болуы мүмкін электр тогының зақымдануынан қорғау үшін, қондырғы корпусын қорғағыш жерге қосылды.

4.1 кесте – Жерлендіруді есептеу үшін бастапқы деректер

Топырақтың меншікті кедергісі, Ом*м	Жерлендіруді диаметрі, d, м	Жерлендіруді ұзындығы, L, м	Жерлендіруді орналасу тереңдігі, h, м	Жерлендіруді арасындағы қашықтық,	Жолақтың ені, b, м
300	0,05	2,0	0,7	6,0	0,02

Бір жерлендірудің кедергісі мына формула бойынша анықталады:

$$R\text{тк} = \text{p} * (\lg (2 * \text{L} / \text{d}) + 0{,}5 * \lg ((2 * 4 * \text{t} + \text{L}) / (4\text{t} * \text{L}))) / 2 * \text{п} * \text{L} \quad (4.1)$$

мұндағы, Rтк - жерлендірудің кедергісі;

ρ – топырақтың меншікті кедергісі;

L – жерлендірудің ұзындығы;

t – жерлендірудің орналасу тереңдігі;

d – жерлендірудің диаметрі.

$$\text{Rтк} = 300 * (\lg (2 * 3 / 0{,}05) + 0{,}5 * \lg ((4 * 2{,}2 + 3) / (4 * 2{,}2 * 3))) / 2 * 3{,}14 * 3 = 15{,}57 \text{ Ом}.$$

Жерлендірудің саны мына формуламен есептеледі:

$$n = R\text{тк} / R\text{нк} \quad (4.2)$$

мұндағы, n - жерлендірудің саны;

Rтк - жерлендірудің кедергісі;

Rнк - нормалар бойынша жерлендірудің кедергісі (4 Ом).

Жерлендірудің арасындағы қашықтық мынадай формула бойынша есептеледі:

$$a = 2 * L \quad (4.3)$$

мұндағы, а - жерлендірудің арақашықтық;

L - жерлендірудің ұзындығы.

$$a = 2 * 3 = 6 \text{ м}$$

Олардың өзара экрандалуын ескере отырып, жерлендірудің саны мынадай формула бойынша анықталады:

$$\text{nЭ} = n/\eta\text{жс} \quad (4.4)$$

мұндағы, $n_Э$ - өзара экрандалуын ескергендегі жерлендірудің саны;

n - өзара экрандалуын ескермегендегі жерлендірудің саны;

$\eta_{жс}$ - жерлендіргіштерді өзара экрандалуын ескеретін пайдалану коэффициенті.

$$n_э = 4/0{,}88 = 5$$

Жерлендірудің өткізгіштерінің ұзындығы мынадай формула бойынша анықталады:

$$Ln = 1{,}05 * a * n_э \quad (4.5)$$

мұндағы, Ln – жерлендіру өткізгіштердің ұзындығы;

а - жерлендірудің арақашықтығы;

$n_э$ - өзара экрандалуын ескергендегі жерлендірудің саны;

$$Ln = 1{,}05 * 6 * 5 = 31{,}5 \text{ м}$$

Жерлендірудің өткізгішінің кедергісі мынадай формула бойынша болады:

$$R\text{п} = \rho * (lg (2 * Ln / b * t)) / 2 * \text{п} * L \quad (4.6)$$

мұндағы, Rж - жолақтық болаттан жасалған жерлендірудің өткізгішінің кедергісі;

Ln - жерлендірудің өткізгіштердің ұзындығы;

b - жерлендірудің өткізгіш жолағының ені;

t - жерлендірудің орналасу тереңдігі.

$$R\text{ж} = 300 * (lg (2 * 31{,}5 / 0{,}02 * 0{,}7)) / 2{,}5 * 3{,}14 * 2 = 30{,}03 \text{ Ом}$$

Барлық токтың ағуына кедергі жерлендірудің құрылғысының мынадай формула бойынша есептеледі:

$$R\text{жт} = R\text{тк} * R\text{ж} / (R\text{тк} * \eta * n + R\text{ж} * \eta_{жс} * n) \quad (4.7)$$

мұндағы Rжт - барлық жерлендірудің токқа ағу кедергісі.

$$R\text{жт} = 30{,}03 * 15{,}57/(5 * 30{,}03 * 0{,}8 + 15{,}57 * 1{,}1) = 3{,}41 \text{ Ом}$$

Жерлендірудің нақты саны мынадай формула бойынша анықтадым:

$$n = Rж / \eta жс * Rжт \quad (4.8)$$

мұндағы, n - жерлендірудің нақты саны.

$$n = 15{,}57 / (0{,}88 * 3{,}41) = 5$$

4.2.2 Жоғары, ультра жоғары және аса жоғары жиіліктегі ЭМӨ әсерін нормалау есебі

ГОСТ 12.1.006-84 [16] сәйкес, 60 кГц-ден 300 МГц-ке дейінгі жиілік диапазонында (ЖЖ және УЖЖ) ЭМӨ-нің электрлік және магниттік компоненттері, сонымен қатар адамға шаққандағы энергия жүктемесі қалыпқа келтіріледі.Онда $Е_{пд}$, $Н_{пд}$, $Э_{Епд}$ и $Э_{Нпд}$ максималды мәндері 2 кестеде келтірілген.

300 МГц - 300 ГГц (ӨЖЖ) жиілік диапазонында ГОСТ 12.1.006-84 [16] бойынша энергия ағынының тығыздығы $П_{пд}$ және энергетикалық жүктеме адамға жұмыс күні $Э_{пд}$ қалыпқа келтіріледі.

Энергия ағынының тығыздығының мәні П – 10 Вт/м2 аспауы керек, тіпті адамдар бұл аймақта аз уақыт болса да. Ал 10 Вт/м2-ден астам ағынмен бұл аймақта қорғаныс құралдары жоқ адамдарға болуға тыйым салынады.

Егер энергия ағынының тығыздығы П – 10 Вт/м2-ден аз болса, онда сіз осы аймақта адамдар өткізетін рұқсат етілген уақытты есептей аламыз (немесе белгілі уақытта энергия ағынының тығыздығының шекті мәнін есептей аламыз):

$$Т_{ПД} = \frac{Э_{ПД}}{П}, \text{ егер } П £ 10 \text{ Вт/м}^2 \quad (5.9)$$

$$П_{ПД} = \frac{Э_{ПД}}{Т}, \text{ егер } ППД £ 10 \text{ Вт/м}^2 \quad (5.10)$$

мұндағы, $ТП_{я}$-адамдардың электромагниттік өрісте болуына рұқсат етілетін ең көп уақыт, с;

ЭПД-жұмыс күніндегі энергия жүктемесінің стандартты мәні, Вт . сағ/м2;

П-адамдардың ауданындағы энергия ағынының тығыздығының мәні, Вт/м^2;

$П_{ПД}$-энергия ағынының тығыздығының шекті рұқсат етілген мәні, Вт/м^2;

Т-сәулелену аймағында бір ауысымда өткізілген уақыт, сағ.

Э энергетикалық жүктемесі Т әсер ету уақытында сәулеленетін беттің бірлігі арқылы өтетін П энергияның жиынтық ағыны болып табылады:

$$Э = П \cdot Т \quad (5.11)$$

Жұмыс күніндегі энергетикалық жүктеменің нормативтік шамасы:

$Э_{пд}$ =2Вт· сағ/м^2 – айналмалы және сканерлейтін антенналардан сәулелену қоспағанда, барлық сәулелену жағдайлары үшін.

$Э_{пд}$ =20Вт · саг/м^2 – айналмалы және сканерлейтін антенналардан айналу жиілігі немесе сканерлеу 1 Гц аспайтын және 50-ден кем емес болған жағдайда.

Бұл есептеуде 2 мысал қарастырамыз:

Мысал 1. 100 ГГц жиіліктегі ЭҚК көзі - 5 айн/мин айналатын антенна. Оператордың жұмыс орнында энергия ағынының тығыздығы 4 Вт/м^2 құрайды. Бір ауысымда жұмыс орнында оператор өткізетін қолайлы уақытты анықтау.

Шешім:

Бір адамға бір күндегі рұқсат етілетін энергетикалық жүктеме ГОСТ 12.1.006-84 бойынша 20 Вт · с/м^2 құрайды. (5.12) формула бойынша:

$$Т_{ПД} = \frac{Э_{ПД}}{П} = \frac{20}{4} = 5 \text{ сағ.} \qquad (5.12)$$

яғни, $Т_{ПД}$ рұқсат етілген уақыты 5 сағаттан аспайды.

2-мысал. АЖЖ-қондырғы операторының жұмыс орнындағы энергия ағыны тығыздығының шекті рұқсат етілген мәнін есептеу. Оператордың жұмыс уақыты 8 сағ.

Шешім:

ГОСТ 12.1.006-84 сәйкес қабылданған қуат жүктемесінің стандартты мәні $Э_{пд}$ = 2 Вт · саг/м^2. (5.13) формуласы бойынша:

$$П_{ПД} = \frac{Э_{ПД}}{Т} = \frac{2}{8} = 0{,}25 \qquad (5.13)$$

$П_{пд}$ = 0,25 Вт/м^2 < 10 Вт/м^2 екендігін тексердім.

Осылайша, $П_{пд}$ шекті рұқсат етілген мәні 0,25 Вт/м^2 тең.

2-мысалдан ең нашар жағдайлар үшін және бір жұмыс күн ішінде микротолқынды сәулеленуден келетін энергия ағынының тығыздығының шекті мәні 0,25 Вт /м^2 болатындығы көрінеді.

Бөлім бойынша қорытынды: бұл бөлімде жұмыс орнындағы еңбек жағдайына талдау жасалды, атап айтқанда табиғи және жасанды жарықтандыру есебі. Есептеу көрсеткендей, үшін бөлме аумағы 14м^2 жеткіліксіз табиғи жарықтандыру терезе өлшемі 2х2м, пайдалану қажет қосымша жасанды жарықтандыру. Жұмыс орнында жасанды жарықтандыру жеткілікті болды. Сонымен, жасанды жарықтандыру жүйесі 3120 Лк жарық ағыны бар 3 шамнан тұрады, сондықтан бұл бөлмеде тәуліктің қараңғы уақытында да жұмыс істеуге болады.

5 Ақпараттық қауіпсіздік тәуекелдерді бағалау

5.1 тәуекелді талдау және бағалау

Дипломдық жұмыстың осы бөлімінде біз Windows Server қауіпсіздік профилі үшін тәуекелдерді бағалаймыз.

АҚ саясатын іске асырудың маңызды аспектілерінің бірі қауіптерді талдау, олардың шынайылығы мен ықтимал салдардың маңыздылығын бағалау болып табылады. Нақты тәуекел қауіпті жүзеге асыру ықтималдығы бар жерде пайда болады, бұл ретте тәуекелдің шамасы осы ықтималдықтың шамасына тікелей пропорционалды.

Тәуекелдерді басқарудың мәні олардың мөлшерін бағалау, азайту шараларын әзірлеу және қалдық тәуекелдер рұқсат етілген деңгейден аспайтындығын бақылау тетігін құру болып табылады. Осылайша, тәуекелдерді басқару екі қызметтің түрін қамтиды: тәуекелдерді бағалау және тиімді және экономикалық қорғаныс және реттеу тетіктерін таңдау.

Тәуекелдерді басқару процесін келесі кезеңдерге бөлуге болады:

- қорғауға мұқтаж активтер мен ресурстардың құндылықтарын анықтау;
- талданатын объектілерді таңдау және оларды қарастырудың егжей-тегжейлі дәрежесі;
- қауіптер мен олардың салдарын талдау, қорғаудағы әлсіз жақтарын анықтау;
- тәуекелдерді жіктеу, тәуекелдерді бағалау әдістемесі мен бағалауды таңдау;
- қорғау шараларын таңдау, енгізу және тексеру;
- қалдық тәуекелді бағалау.

Тәуекелді бағалау оның деңгейін (сапалық немесе сандық шамасын) айқындаудан және осы деңгейді ең жоғарғы рұқсат етілген (қолайлы) деңгеймен, сондай-ақ басқа тәуекелдердің деңгейімен салыстырудан тұрады. Басқаша айтқанда, АҚ бұзу тәуекелін бағалау-бұл ақпараттық активтерді олардың өмірлік циклінің барлық сатыларында пайдаланумен байланысты АҚ тәуекелдерін бағалауды жүргізуге мүмкіндік беретін ақпаратты анықтаудың, жинаудың, пайдаланудың және талдаудың жүйелі және құжатталған процесі.

Маңызды объектілердің қауіп-қатерін есептеу үшін екі фактор бойынша тәуекелдерді бағалау әдісі қолданылды [21].

Бірінші қадамда қауіп төнген әрбір ресурс үшін алдын ала белгіленген шкала бойынша теріс әсер (ресурс көрсеткіші) бағаланады.

Үшінші қадамда тәуекел көрсеткіші есептеледі. Әдістеменің қарапайым нұсқасында бұл көбейту арқылы жасалады. Алайда, көбейту операциясы сандық шкалаларға белгіленгенін есте сақтау қажет. Рангтік (сапалық) параметрлер үшін теріс әсер ету көрсеткіші және қауіп-қатерді іске асыру ықтималдығы сияқты

болып табылады. Тиісінше нақты ұйымға қатысты тәуекелдер көрсеткіштерін бағалау әдістемесі әзірленуі тиіс.

Ақпараттық активтің қауіпсіздігіне ақпараттың құпиялылығы (рұқсатсыз қол жеткізуден қорғау), тұтастық (ақпараттың өзектілігі мен дәйектілігі, оның жойылуынан және рұқсат етілмеген өзгертулерден қорғалуы) және қол жетімділік (қажетті уақыт кезеңінде қажетті ақпараттық қызметті алу мүмкіндігі) сияқты қасиеттері жатады [22].

Қауіпті іске асыру ықтималдығы сараптамалық бағалау, болжау жолымен, сондай-ақ статистикалық деректер негізінде айқындалады. Белгілі бір уақыт кезеңінде қауіп-қатерді іске асыру әрекеттерінің күтілетін санын анықтайтын оң сан болып табылады.

Әрбір жобалық тәуекелді сипаттайтын келесі маңызды компонент шығын мөлшері болып табылады.

Ақпаратты ашуға, рұқсатсыз модификациялауға, уақытша қолжетімділікке немесе бұзуға байланысты қауіпсіздік инциденттері нәтижесінде ұйымға келтірілген залалдың мөлшері ақпараттық активтердің құндылығымен айқындалады. Мұндай инциденттердің салдарлары жіберілген пайдада, бәсекелік артықшылықтардың жоғалуында, ұйым имиджінің нашарлауында, үшінші тараптың мүдделеріне зиян келтіруде, айыппұлдарда, тікелей қаржы шығындарында немесе қызметті іріткісіздендіруде көрініс табуы мүмкін. Бұл ретте әрбір актив үшін оқиғаларды дамытудың ең нашар сценарийін қарау керек.

5.1-кесте – Қауіптің туындау ықтималдығы шкаласы

Қауіптің туындау ықтималдығы шкаласы	
Ықтималдылық деңгейі	Қауіптің туындау ықтималдығы
1 – Өте төмен	Шамамен 2-3 рет 10 жылда
2 - Төмен	Шамамен 5 жылда бірнеше рет және сирек
3 - Орташа	Шамамен жылына бірнеше рет
4 - Жоғары	Айына шамамен 1 рет
5 – Өте жоғары	Шамамен айына бірнеше рет

Келесі кестеде деңгейлер бойынша тәуекел салдарының шамасы көрсетілген.

5.2-кесте – Залал шамасының шкаласы

Залал шамасының шкаласы	
Мәні	Сипаттамасы
1 – Өте төмен	құны 50 000 теңгеге дейін
2 - Төмен	құны 200 000 теңгеге дейін

5.2-кестенің жалғасы

3 - Орташа	құны 500 000 теңгеге дейін
4 - Жоғары	бағасы 1 000 000 теңгеге дейін
5 – Өте жоғары	құны 1 000 000 теңгеден жоғары

Дипломдық жұмысты әзірлеу кезінде қолданылатын маңызды объектілерді анықтау арқылы қорғауды талап ететін активтер тізімі жасалды:

- жұмыс станциясы;
- Windows Server 2012 R2;
- сервер.

5.3-кесте бойынша қорытынды: нәтижесінде тәуекелдердің ең жоғары деңгейі 5.1 және 5.2-кестелерде келтірілген шкалаларды пайдалана отырып есептілінді. Осылайша, қызметкерлердің іс-әрекетінен туындайтын тәуекелдер, SQL-кодты енгізу және қызмет көрсетуден бас тарту (DDoS шабуылдар) ең қауіпті болып табылды. Тәуекелдер деңгейі қолайсыз болып шықты, сондықтан барлық тәуекелдер үшін қорғау шаралары ұсынылды. Кейін қолайсыз тәуекелдерге арналған қорғау шаралары анықталып, тәуекелдерді қайта есептеу жүргізілді.

5.3 кесте – Тәуекелдерді бағалаудың қорытынды кестесі

№	Қауіптер	Осалдықтар	Жоғарғы мәні	Қорғаныс шаралары	Қалдық мәні
1 Жұмыс станциясы					
1.1	Құжаттарды, тасымалдаушылардың ұрлануы	Рұқсатсыз көшіру	6	Құпия ақпараттың ақпараттық жүйеден ағып кетуінің алдын алу	3
1.2	Бағдарламалық бұзылуы	DDOS шабуылдар немесе техниканы істен шығаруға бағытталған басқа да шабуылдар	2	Басып кіруді анықтау жүйесі, жүйені резервтік қалпына ке	1
1.3	Деректерді өзгерту	Ақпараттық жүйемен жұмыс істеу кезінде белгіленген ережелерді білмеу немесе сақтамау және деректерді өзгерту	4	Рұқсат етілмеген қолжетімділікті жүзеге асыру мүмкіндігін болдырмау	2
1.4	Дұшпандық апплеттер мен вирустар	Зиянды бағдарламаны орнату, қауіпті сайттарға кіру	8	Дұрыс антивирустық бағдарламаны таңдау. Вирусты анықтау процедуралары	4

5.3-кестенің жалғасы

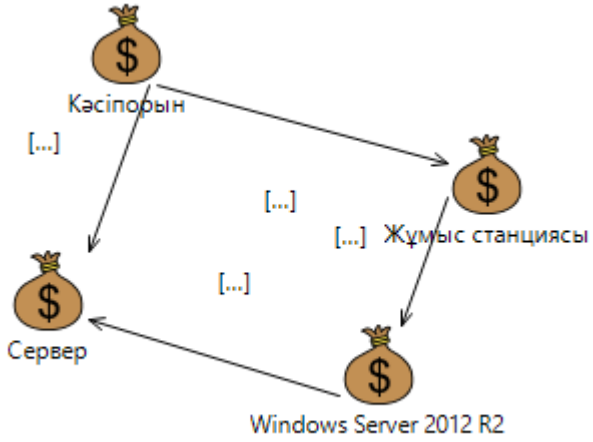
2 Windows Server 2012 R2					
2.1	Қызмет көрсетуден бас тарту	DDoS-ге әкелетін белгісіз осалдықты пайдалану векторы	8	Басып кіруді анықтау жүйесі, жүйенің резервтік көшірмесі	4
2.2	Ақпараттың құпиялығын бұзу	Қашықтан кіру қызметтерін дұрыс пайдаланбау	4	Қашықтан қол жеткізу кезінде құқықтардың тағайындалуы. Қашықтықтан қол жеткізу қауіпсіздігі тұжырымдамасын әзірлеу	2
2.3	Белсенді желілік компоненттердің дұрыс емес конфигурациялары	Бастапқы және ресурстық IP адрестерін алмастыру мүмкіндігі	4	Операциялық жүйе басқарумен TCP / IP желілік сервистерін баптау	2
2.4	Бақылаусыз көшіру	Файл жүйесін бірлесіп қолданғанда ұқыпсыздық	7	Қорғауды талап ететін ақпараттық ресурстардың дұрыс орналасуы. Жүйені басқаруды қамтамасыз ету	3
3 Сервер					
3.1	Серверді басқаруға рұқсатсыз кіру	Қол жеткізу құқықтарын дұрыс бөлмеу	8	Рұқсат етілмеген қолжетімділікті жүзеге асыру мүмкіндігін болдырмау	4
3.2	Жабдықтың істен шығуы	Кемшіліктері бар үздіксіздік жоспарлары	5	Басып кіруді анықтау жүйесі, жүйені резервтік қалпына келтіру	3
3.3	SQL инъекциясы	SQL сұраныстары үшін сүзгілеу ережелерінің жеткіліксіздігі	9	Желі аралық экран үшін АҚ саясаты, сүзгілерді пайдалану	4
3.4	Сервер кеңейтімдерін енгізу	Пайдаланушы берген деректерді сервермен түсіндірілген файлға сақтамас бұрын тексерудің болмауы.	8	Рұқсат етілмеген қолжетімділікті жүзеге асыру мүмкіндігін болдырмау	4

5.2 CORAS құралы арқылы тәуекелдерді талдау

Coras құралы бағдарламалық жасақтаманы әзірлеу саласында объектілі модельдеу үшін UML – графикалық сипаттау тілін қолданады.

Тәуекелдерді талдаудың көрнекілігі үшін Coras бағдарламалық құралын пайдаландық. Жоғарыда сипатталған активтер диаграммасынан кейін және олардың арасындағы байланысы 5.1-суретте көрсетілген.

Бағдарламада қорғауға жататын құндылықты (ақпаратты) білдіретін Asset элементі пайдаланамыз.

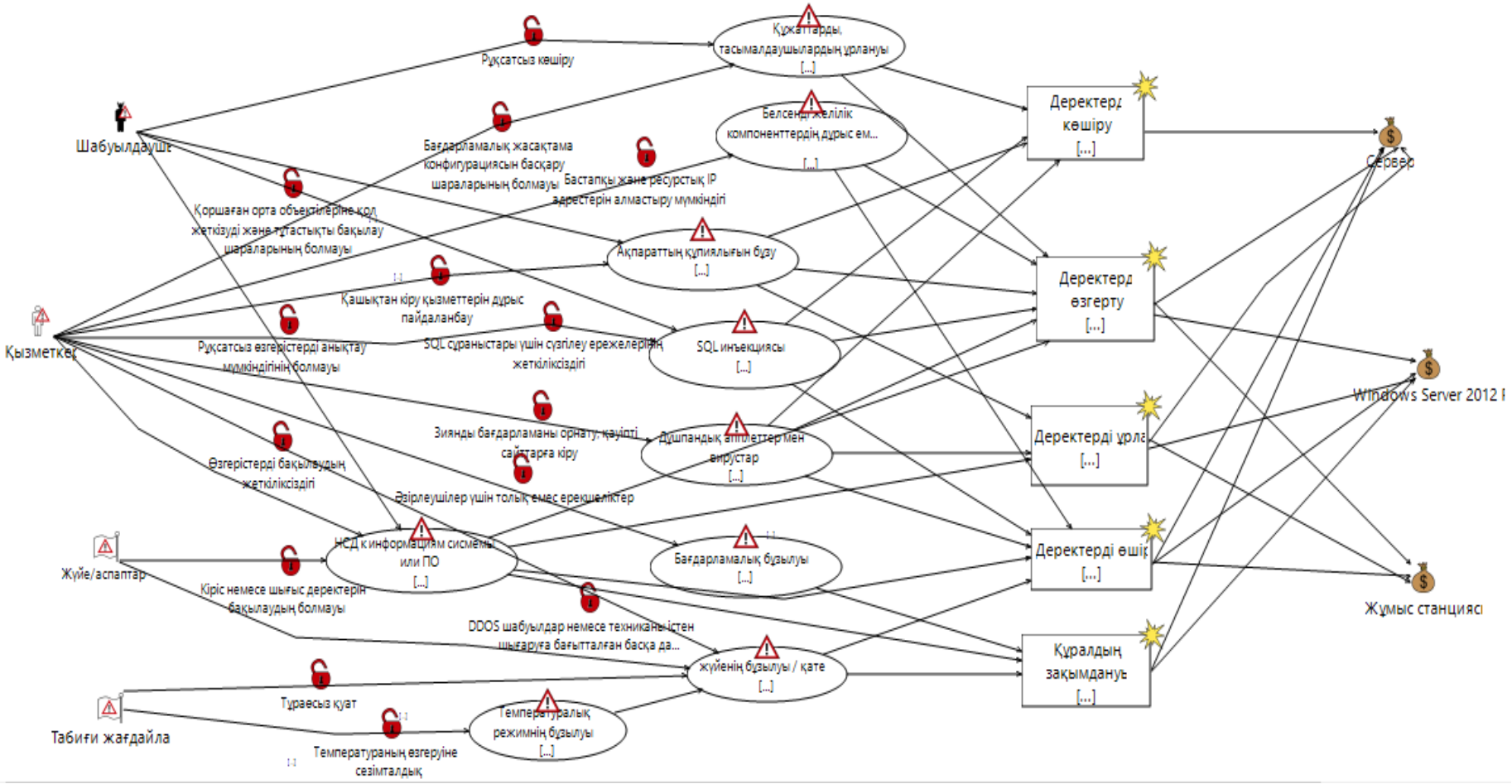


5.1сурет – Активтер диаграммасы

5.4-кестені пайдалана отырып, тәуекелдерді үлгілейміз, яғни әуекелдер диаграммасын генерациялаймыз, бұдан әрі әрбір актив үшін әрбір тәуекел бойынша осы тәуекел жүзеге асырылған жағдайда салдарларды анықтаймыз. Алынған диаграмма 5.4- суретте көрсетілген

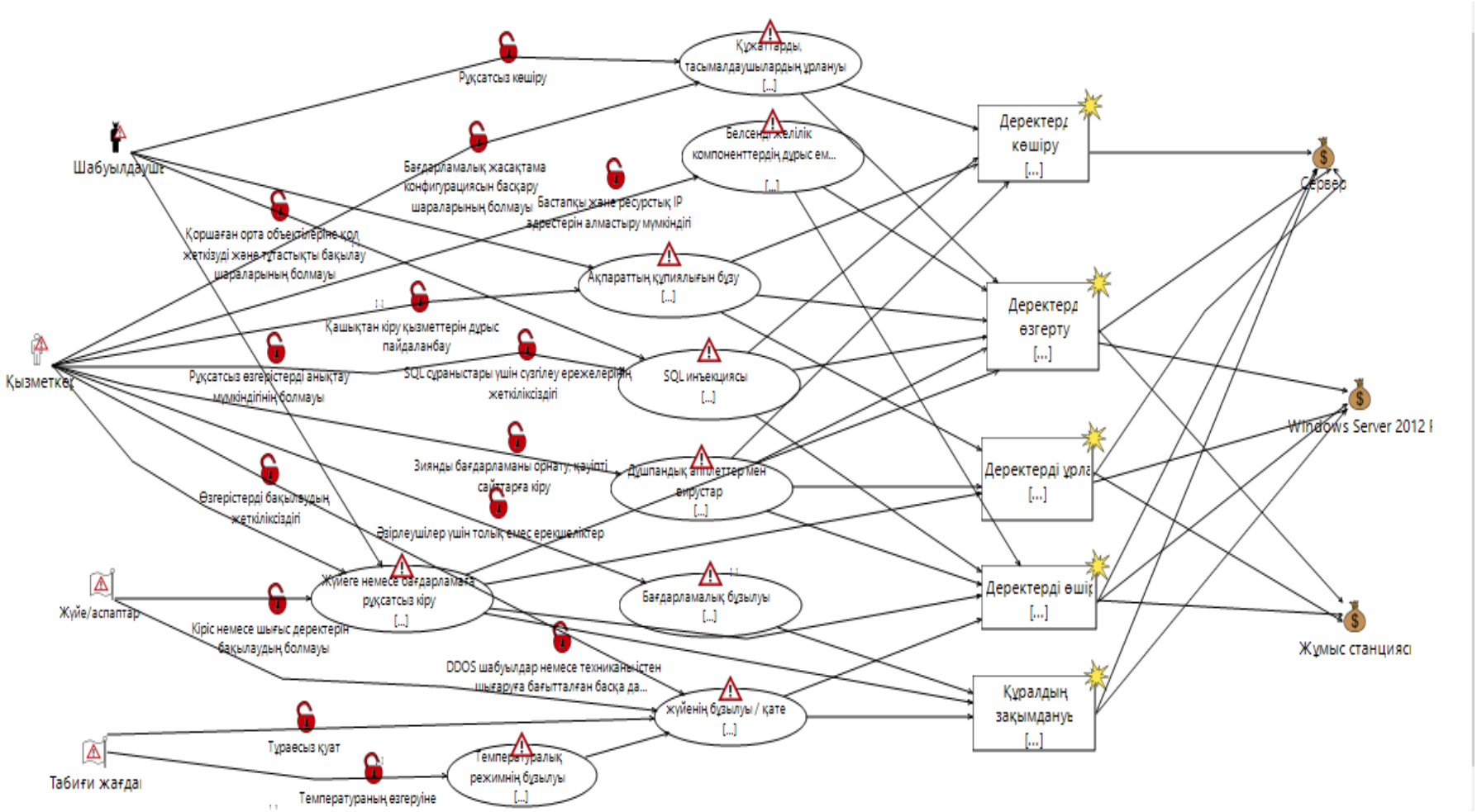
Бағдарлмада келесі элементтер пайдаланылады:

- Threat Human Accident - адам факторымен байланысты қасақана емес қауіп-қатерлерді белгілеу үшін
- Threat Human Deliberate - адам факторына байланысты қасақана қауіп-қатерлерді белгілеу үшін
- Threat Non Human адам факторымен байланысты емес қауіптерді белгілеу үшін;
- Threat Scenario - қатерлерді сипаттау үшін;
- Vulneravility - осалдықтарды сипаттау үшін;
- Unwanted Incident - жағымсыз оқиғаларды белгілеу үшін [23].



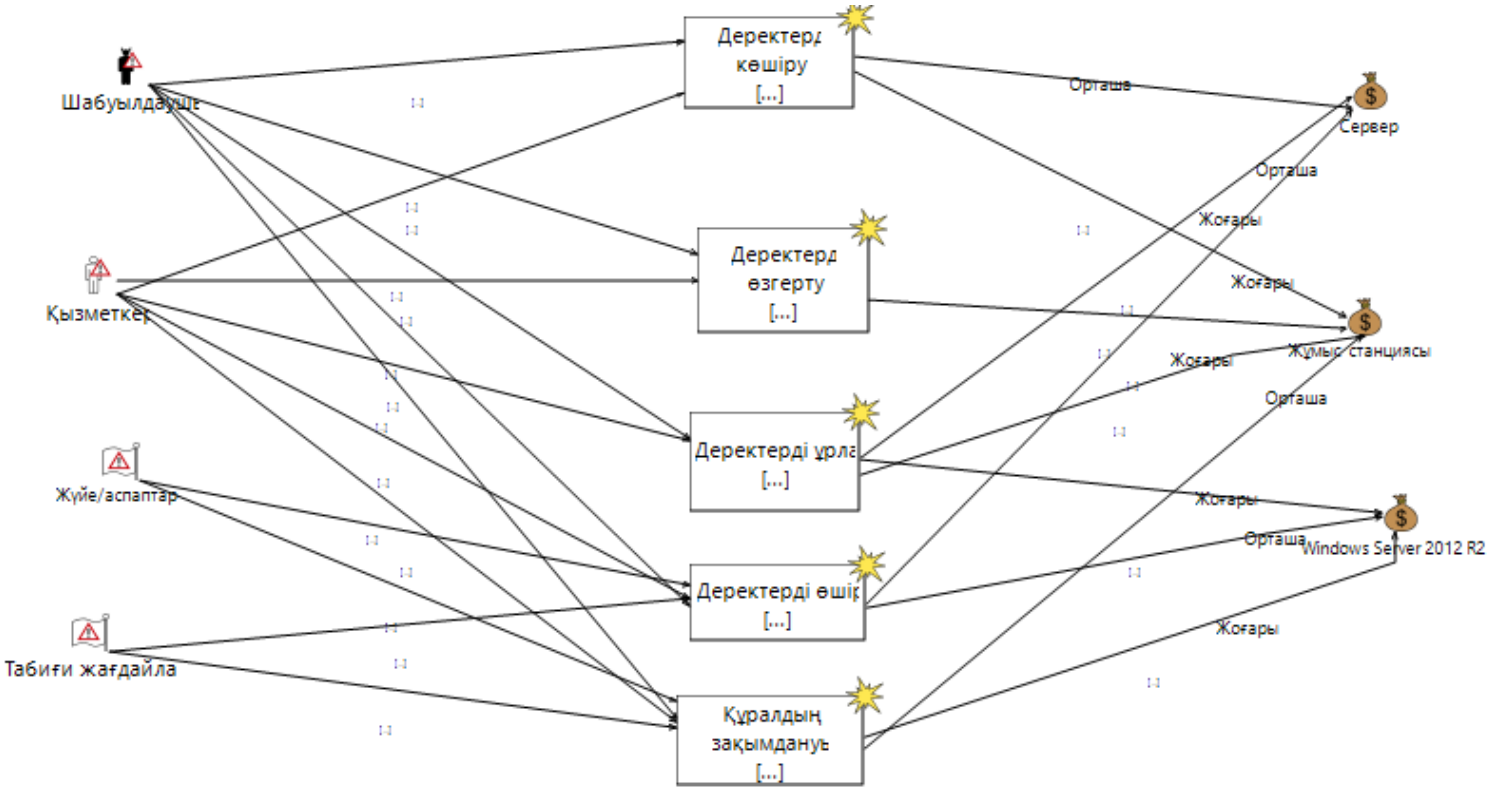
5.2-сурет–Қауіптер моделі

Бұдан әрі пайда болған тәуекелдерді іске асыру жиілігін анықтаймыз (белгілі бір уақыт кезеңінде қауіп-қатерді іске асырудың күтілетін саны).



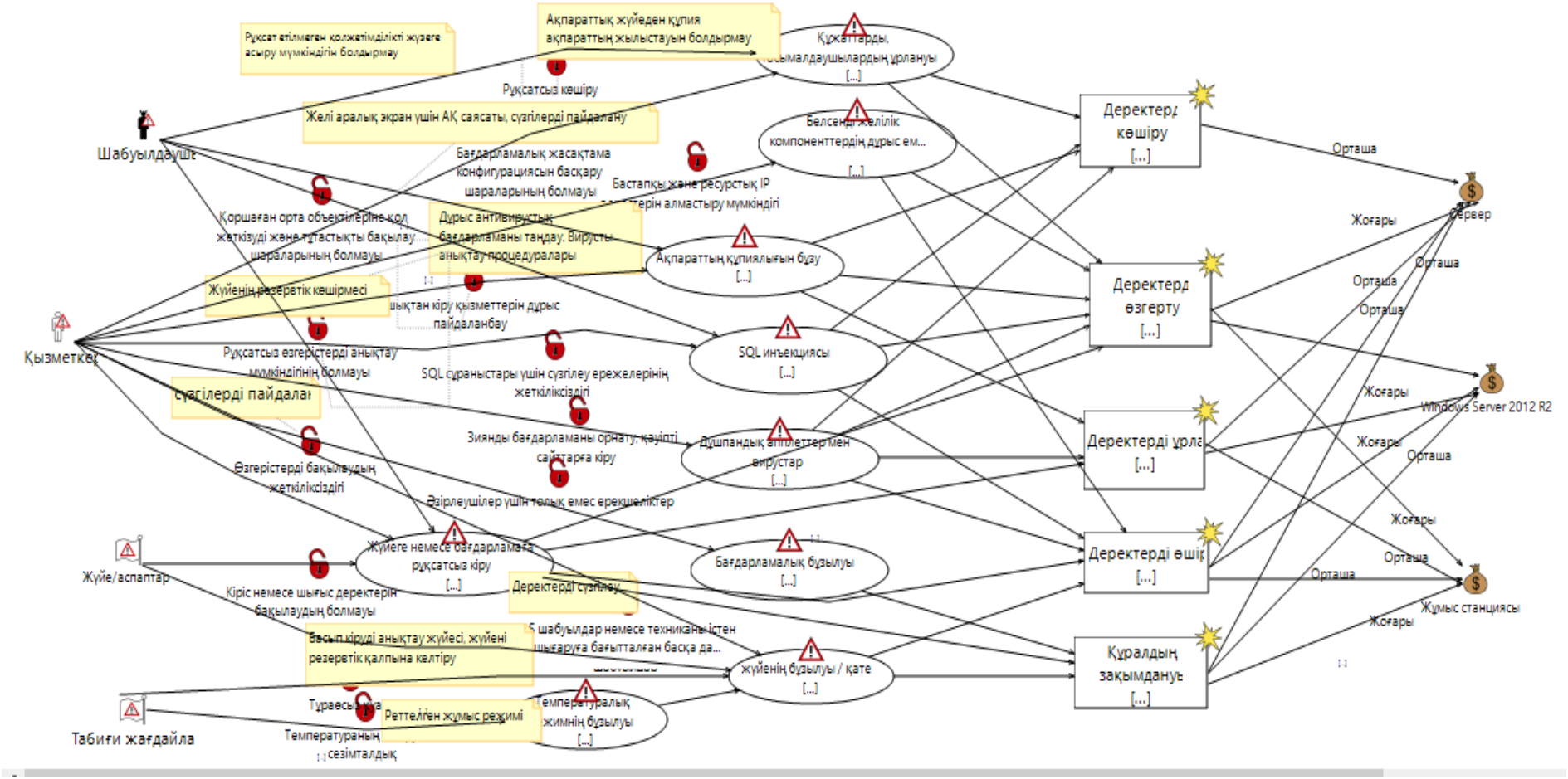
5.3-сурет – Ықтимал сипаттамалары бар қауіптер моделі

Ақпараттық қауіпсіздік инциденті бірнеше активтерге немесе активтің бір бөлігіне әсер етуі мүмкін. Әсер ету оқиғаның сәттілік деңгейімен байланысты. Әсер қаржылық немесе нарықтық салдарды қамтитын жедел әсердің немесе болашақ (іскерлік) әсердің болуы деп саналады. Әрі қарай әрбір актив үшін тәуекелге ұшырау дәрежесін бағалаймыз (5.4 сурет)



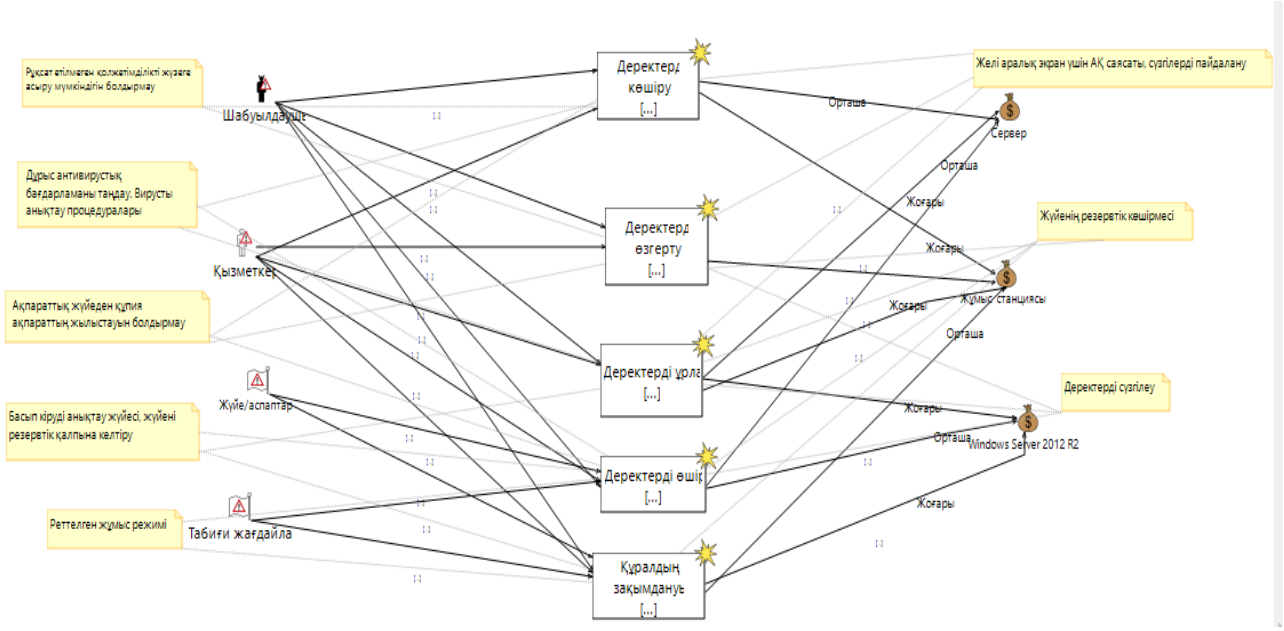
5.4-сурет – Қауіпті жүзеге асыру салдарларының сипаттамасы бар тәуекелдер диаграммасы

Іс-шараларды таңдау және нақтылау ақпараттық қауіпсіздікке төнетін қатерді талдау нәтижелеріне негізделуі керек. Біз олардың өмірлік циклі процестерінде бағдарламалық осалдықтардың пайда болуын және жойылуын болдырмау мақсатында қауіп-қатерді жүзеге асыратын қорғау шараларының тізбесін анықтаймыз (5.5 сурет).



5.5-сурет – Қорғаныс шараларын қосқаннан кейінгі қауіптер диаграммасы

Қорғау шараларын қосқаннан кейін қабылданбайтын тәуекелдер қалуы мүмкін. Мұндай жағдайларда шешім қабылдайтын тұлғаларға қалыпты қабылдау критерийлерін қабылдамайтын тәуекелдерді сақтауға тура келуі мүмкін. Егер бұл қажет болса, шешім қабылдайтын тұлға тәуекелдерге нақты түсінік беріп, шешім үшін ақтауды енгізуге тиіс тәуекелдің қалыпты қабылдау критерийлерін жою (5.6 сурет).



5.6 –сурет – Қолайсыз тәуекелдер диаграммасы

Бөлім бойынша қорытынды: дипломдық жұмыстың осы бөлімінде компания шабуылдаушы активтерінің тәуекелдері анықталды.

Барлық анықталған ресурстар бойынша тәуекелдерге талдау жүргізілді және ақпараттық жүйені қорғау шаралары анықталды. Тәуекелдерді бағалау үдерісіне арналған негізгі жұмыстар қаралды. Таңдалған активтердің негізгі қауіптері мен осалдықтары қаралды. Тәуекелдерді бағалау екі фактор бойынша есептеу әдісін қолдана отырып жүргізілді. Тәуекелдердің жоғары деңгейі анықталды, осыған байланысты қорғау шараларын пайдалану туралы шешім қабылданды. Ұсынылған қорғау шараларын ескере отырып, тәуекелдерге қайта есептеу жүргізілді.

Қорғаныс шараларын қолдану нәтижесінде тәуекелдің орташа көрсеткіші 2 есе төмендеді және активтер үшін қолайлы болды.

Екінші бөлікте CORAS көмегімен ақпараттық тәуекелдерге талдау жүргізілді және активтерді сәйкестендіруден бастап, қауіп-қатер мен осалдықтар моделінен бастап, қарсы өлшемдерді енгізумен аяқталатын UML диаграммалары салынды.

Қорытынды

Бұл дипломдық жобада профиль түсінігі қарастырылды, талдау барысында ақпаратты шифрлау үшін бағдарламалық жасақтама таңдалды. Қауіпсіз байланыс және деректерді шифрлау ұғымы зерттелген. Microsoft Windows Server 2012 R2 операциялық жүйесінде қауіпсіз VPN қосылымын құру жұмыстары жүргізілді және BitLocker шифрлау бағдарламалық жасақтамасы сыналды.

Өміртіршілік қауіпсіздігі бөлімде жұмыс орнындағы еңбек жағдайына талдау жасалды, атап айтқанда жоғары, ультра жоғары және аса жоғары жиіліктегі ЭМӨ әсерін нормалау және электр қауіпсіздігі бойынша жерлердіру есебі жасалды.

Ақпараттық қауіпсіздік тәуекелдерін бағалау бөлімінде Windows Server қауіпсіздік профилі үшін туындайтын тәуекелдер бағаланып, қорғау шешімдері ұсынылды.

Әдебиеттер тізімі

5. Комплексная защита информации в компьютерных системах: Учебное пособие. Завгородний В. И. – М.: Логос; ПБОЮЛ Н. А. Егоров, 2016. – 269 с.

6. Знакомство с Microsoft Windows Server 2012 / Пер. с англ. / Дж. Ханикат – М.: Издательско-торговый дом “Русская редакция”, 2014. – 464 с.

7. Станек, Уильям Р. Microsoft Windows Server 2012. Справочник администратора. - М.: БХВ-Петербург, 2014. - 843 с.

8. Девянин, П.Н. Анализ безопасности управления доступом и информационными потоками в компьютерных системах / П.Н. Девянин. - М.: Радио и связь, 2006. - 176 с.

9. Рэнд, Моримото Microsoft Windows Server 2012. Полное руководство / Моримото Рэнд. - М.: Диалектика / Вильямс, 2013. - 791 с. Станек, У. Microsoft Windows Server 2012 R2. Хранение, безопасность, сетевые компоненты. Справочник администратора / У. Станек. - М.: БХВ-Петербург, 2015. - 445 с.

10. Защита компьютерной информации от несанкционированного доступа. А. Ю. Щеглов. – СПб.: Издательство «Наука и Техника», 2014. – 384 с.

11. Ботуз, С. П. Интеллектуальные интерактивные системы и технологии управления удаленным доступом. Учебное пособие: моногр. / С.П. Ботуз. - М.: Солон-Пресс, 2014. - 340 с.

12. Гатчин Ю.А., Коробейников А.Г. Основы криптографических алгоритмов. Учебное пособие. - СПб.: СПбГИТМО(ТУ), 2002.

13. Баричев С.Г., Серов Р.Е. Основы современной криптографии. - Горячая Линия - Телеком, 2002 - 153 с.

14. ExamREVIEW MCSE Windows Server & SQL Server 2012 Exam 70-410, 461, 462 & 465 ExamFOCUS Study Notes & Review Questions; Pimlico - Москва, 2012. - 440 с.

15. Craig Zacker Exam Ref 70-410: Installing and Configuring Windows Server 2012; Microsoft Press - Москва, 2013. - 400 с.

16. ҚР ҚНжЕ 3.02-04-2009 – «Әкімшілік және тұрмыстық ғимараттар» - Сәулет, қала құрылысы және құрылыс саласындағы мемлекеттік нормативтер, Астана, 2010.

17. ҚР ҚНжЕ 2.02-05-2009 – «Ғимараттар мен имараттардың өрт қауіпсіздігі» - Сәулет, қала құрылысы және құрылыс саласындағы мемлекеттік нормативтер, Астана, 2010.

18. Ж.С. Абдимуратов. Охрана труда. Методические указания к выполнению расчетно-графических работ для студентов - бакалавров специальности 5В071800 - «Электроэнергетика» - Алматы: АУЭС, 2013 - 22с.

19. ҚР ҚНжЕ 4.04-10-2002 Қазақстан Республикасы Индустрия және сауда министрлігінің Құрылыс комитеті Астана, 2002.

20. ГОСТ 12.1.006-84. ССБТ. Электромагнитные поля радиочастот. Допустимые уровни на рабочих местах и требования к проведению контроля. - М.: Издательство стандартов. 1984.

21. ҚР ҚНжЕ 2.04-01-2001. «Құрылыстық климатология» - Сәулет, қала құрылысы және құрылыс саласындағы мемлекеттік нормативтер, Астана, 2002.

22. Н.Г. Приходько, Ф.Р. Жандаулетова. Основы пожарной безопасности. Методические указания к выполнению курсовой работы для студентов специальности 5В073100 – Безопасность жизнедеятельности и защита окружающей среды. - Алматы: АУЭС, 2013 - 31 с.

23. Абикенова А.А., Санатова Т.С. Безопасность жизнедеятельности. Методические указания к выполнению раздела «Пожарная профилактика» в выпускных работах для всех специальностей. Бакалавриат - Алматы: АИЭС, 2009. - 32 с.

24. Ж.С. Абдимуратов. Охрана труда. Методические указания к выполнению расчетно-графических работ для студентов - бакалавров специальности 5В071800 - «Электроэнергетики» - Алматы: АУЭС, 2013 - 22с.

25. ISO/IEC 27005 Информационная технология. Методы и средства обеспечения безопасности. Менеджмент риска информационной безопасности. М: Стандартинформ. 2008 – 40 с.

26. Глатенко. В.А. Основы информационной безопасности: учебное пособие для вузов / В.А. Глатенко. – М.: ИНТУИТ, 2012 – 205 с.

27. ГОСТ Р ИСО/МЭК 15408-1-2012. Информационная технология. Методы и средства обеспечения безопасности. Критерии оценки безопасности информационных технологий. Часть 1. Введение и общая модель. — М.: Изд-во стандартов, 2012. — 50 с.