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

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

ДИПЛОМДЫҚ ЖОБА

Тақырыбы: «Кәсіпорынның қауіпсіз ұжымдық желісін жобалау»

Мамандығы: 5В100200 – «Ақпараттық қауіпсіздік жүйелері»
Орындаған: Бейсенбек Ернар Әмірбекұлы Тобы СИБк-16-1
(аты-жөні)
Ғылыми жетекші: т.ғ.қ., доцент Шайкулова А. А.
(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:
ҚР БҒМ ҒК «Ақпараттық және есептеуіш технологиялар институты» РМК, ғылыми қызметкері, PhD Бегимова Енлик Ериковна
(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: Бейсенбек Ернар Әмірбекұлы
(аты-жөні)

Жобаның тақырыбы: «Кәсіпорынның қауіпсіз ұжымдық желісін жобалау»

2019 ж. «11» қараша №146 университет бұйрығымен бекітілді.

Аяқталған жұмысты тапсыру мерзімі: «____»_____20___ ж.

Жобаға алғашқы деректер (талап етілетін зерттеу (жоба) нәтижелерінің параметрлері және зерттеу нысанының алғашқы деректері): _____
Кәсіпорынның қауіпсіз ұжымдық желісін жобалаудың қорғалған жергілікті желі модулінің түрлері тәжірибе жүзінде іске асырылып, алынған деректерге сүйене отырып, қорғану немесе шабуылдың алдын алу жолдары ұсынылды. Атап. айтқанда, кәсіпорынның ұжымдық қауіпсіз желісін жобалау жүйесін жетілдіріп. қорғалған жергілікті желі моделі eve-ng виртуалды бағдарламсын қолдана отырып, әзірленді.

Диплом жобасындағы әзірленуі тиіс мәселелер тізімі немесе диплом жобасының қысқаша мазмұны:
1. Ұжымдық қауіпсіздік желісінің өзектілігі.
2. Қорғау түрлері және қорғану әдістері.
3. Ұжымдық желіні модельдеу үдерісі.
4. Жергілікті желіні eve-ng виртуалды бағдарламасымен модельдеу.
5. Жұмыс жағдайында табиғи жарықтандыруды, өрт қауіпсіздігін және хабарлағаш санын есептеу.
6. Ақпараттық қауіпсіздік тәуекелдерін екі параметр бойынша бағалау.

Графикалық материалдардың (міндетті түрде дайындалатын сызбаларды көрсету) тізімі:

2.7 сурет – Есептеу желісінің моделін құру

2.11 сурет – Дамушы кәсіпорынның компьютерлік желісі туралы түсінік

2.14 сурет – №1 компьютерлік желінің құрастырылған моделі

2.16 сурет – R маршрутизатордағы орналасқан DHCP-пулдар

2.23 сурет – DHCP серверінен IP мекенжайын сәтті жалға алу нәтижесі

2.27 сурет – R1 маршрутизаторындағы IP-мекен-жайды аудару кестесі

3.1 кесте – Жерге тұйықтау есебі үшін бастапқы деректер

3.2 кесте – Түтін датчиктерінің санын есептеу кестесі

4.6 кесте – Қолайсыз тәуекелдер диаграммасы

Негізгі ұсынылатын әдебиеттер:

1. В.П.Корячко Д.А.Перепелкин. Корпоративные сети: технологии, протоколы, алгоритмы– М.: Горячая Линия - Телеком, 2011 - с. 220.

2. Биячуев Т.А. Безопасность корпоративных сетей – СПБ.: ГУ ИТМО, 2004. -161 с.

3. Оливер В.Г., Олифер Н.А. – Компьютерные сети. Принципы, технологии, протоколы: Учебник для вузов. СПБ.: Питер, 2003. – 847 с.

4. 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.

Жоба бойынша жобаның бөлімдеріне қатысты белгіленген кеңесшілер

Бөлімдері	Кеңесшілері	Мерзімі	Қолы
Негізгі бөлім	Шайкулова А. А.		
Өміртішілік қауіпсіздігі	Жандаулетова Ф.Р.		
Тәуекелдерді есептеу бөлімі	Дмитриева М.В.		

Диплом жобасын дайындау
КЕСТЕСІ

Бөлімдердің атауы, әзірленетін мәселелердің тізімі	Ғылыми жетекшіге ұсыну мерзімдері	Ескерту
Кіріспе	12.02.20 – 14.02.20	орындалды
1.1 Ұжымдық қауіпсіздік желісінің өзектілігі	18.02.20 – 10.03.20	орындалды
1.2 Қорғау түрлері және қорғану әдістері.	18.02.20 – 10.02.20	орындалды
2 Ұжымдық желіні модельдеу үдерісі.	12.03.20 – 24.03.20	орындалды
2.1 Жергілікті желіні eve-ng виртуалды бағдарламасымен модельдеу.	26.03.20 – 15.04.20	орындалды
3 Өміртіршілік қауіпсіздігі	19.04.20 – 15.05.20	орындалды
3.1 Кәсіпорындағы еңбек жағдайларын талдау	19.04.20 – 02.05.20	орындалды
3.2 Есептеу бөлімі	02.05.20 – 15.05.20	орындалды
4 Ақпараттық қауіпсіздіктің тәуекелдерін есептеу	08.05.20 – 28.05.20	орындалды
4.1 Ақпараттық қауіпсіздік тәуекелдері	08.05.20 – 15.05.20	орындалды
4.2 Екі параметр бойынша есептеу	15.05.20 – 28.05.20	орындалды

Тапсырманың берілген уақыты «12 » қаңтар 2020 ж.

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

Жобаның
ғылыми жетекшісі _____ (Шайкулова А. А.)

(қолы) (аты-жөні)

Орындалатын тапсырманы
қабылдаған студент _____ (Бейсенбек Е.Ә.)
(қолы) (аты-жөні)

Аңдатпа

Бұл дипломдық жобада кәсіпорынның ұжымдық қауіпсіз желісін жобалау бойынша eve-ng виртуалды модельдеу бағдарламасын пайдалана отырып, әр түрлі шаралар арқылы кәсіпорынның қауіпсіз желі үлгісін құрылды. Жобада кәсіпорын желісінің туннельдік әсері, құрылғылардың ақауға төзімділігі және желі жабдықтарының қол жетімділігі қарастырылды.

Өмір-тіршілік қауіпсіздігі бөлімінде өрт сөндіру құралдарына қажеттілікті және жерге тұйықтауға есептеу нәтижелері жүргізілді.

Тәуекелдерді бағалау қажеттілігі бірінші кезекте олардың кәсіпорынның бизнес процестеріне әсер ету дәрежесін анықтаумен, оларды іске асырудан болған қандай да бір шығындардың (залалдың) мөлшерін бағалаумен және оларды барынша азайту немесе болдырмау тетіктерін әзірлеумен байланыстырды.

Аннотация

В данном дипломном проекте разработана модель безопасной сети предприятия с использованием программы виртуального моделирования eve-ng по проектированию корпоративной безопасной сети предприятия посредством различных мер. В проекте предусмотрены туннельные эффекты сети предприятия, дефектостойкость оборудования и доступность сетевого оборудования.

В части безопасности жизнедеятельности были проведены результаты расчета потребности в средствах пожаротушения и заземления.

Необходимость оценки рисков в первую очередь связана с определением степени их влияния на бизнес процессы предприятия, оценкой размеров каких-либо убытков (убытков) от их реализации и разработкой механизмов их минимизации или предотвращения.

Abstract

In this graduate, a model of a secure enterprise network was developed using the eve-ng virtual simulation program for designing a corporate secure enterprise network through various measures. The project provides for tunnel effects of the enterprise network, fault tolerance of equipment and availability of network equipment.

In terms of life safety, the results of calculating the need for fire extinguishing and grounding facilities were carried out.

The need to assess risks is primarily related to determining the extent of their impact on the business processes of the enterprise, assessing the size of any losses (losses) from their implementation and developing mechanisms to minimize or prevent them.

Мазмұны

Кіріспе

Қазіргі уақытта жаңа жергілікті желілер саны ұлғаюда, қолданыстағы желілер кеңеюде, осы желілерді пайдаланушылар саны ұлғаюы, желілерді әзірлеу мен өрістету сапасына қойылатын талаптар да өсуде, сонымен бірге кәсіпорын желісінің қауіпсіздігін жобалау ақпараттың қауіпсіздігі мен жергілікті желінің құны оны құру кезіндегі басты факторлардың бірі болып табылады.

Еліміздегі кез келген мемлекеттік немесе коммерциялық кәсіпорын ақпаратты қорғау мәселесінің маңыздылығын тудыратын обьективті үдерістер-бұл кәсіпорын ақпаратының қауіпсіздігі әдетте бұл ақпаратты және бүкіл ұжымды қауіпсіз желісін қасақана, кездейсоқ әрекеттерден немесе қызметкердің тәжірибесіздігі мен немқұрайлығынан зиян әкеп соғуынан қорғау деп түсініледі.

Қауіпсіздік талаптарын сақтау қорғанудың бірден-бір жолы болып табылады. ‘Қандай ақпарат қорғануды қажет етеді және зиянкестен назарын тудырады?’ деген сауалға келер болсақ. Бұл, әдетте, маңызды шарттар, клиенттер тізімі, бухгалтерлік бағдарламалардың деректер базасы, парольдер мен “клиент-сервер” жүйесінің кілттері, бөлімшелермен байланыс арналары және т.б. Қауіпсіздікті жеткілікті түрде бағалаудың екі амалы бар, біріншісі құндылық жақындығы жөнінді қаскүнем ақпаратқа қол жеткізу үшін кең көлемде шығындалса, сонша ол ұтады деген пікірге негізделген, ал екіншісі уақыт жақындығы ақпаратты жою ісі дәлеліне негізделген. Дегенмен, ақпараттың таралып кетуі және олардан болатын зақымдардың саны әрдайым артып келеді. Оның себебі кәсіпорынның ішіндегі – ұжымдық желінің қауіпсіз болмауы және қауіпсіз құжат айналымын дұрыс жолға қойылмауынан ақпаратты қасақана ұрлау, байқаусызда жоғалту − кездейсоқ ағып кету фактілері орын алуы мүмкін.

Мұндайда дәстүрлі қорғаныс құралдары көмегіне жүгіне айтарлықтай нәтиже бермейді.Кәсіпорынның ұжымдық қауіпсіз желісін жобалау жүйесін жетілдіру іс-әрекетінің мониторингі кәсіпорынға қауіп-қатерлерді жою және азайту бойынша шараларды талдап, қабылдауға мүмкіндік береді.

Дипломдық жобаның мақсаты – кәсіпорынның қауіпсіз ұжымдық желісін жобалау жүйесін жетілдіріп. қорғалған жергілікті желі моделі eve-ng виртуалды бағдарламсын қолдана отырып, әзірлеу.

Осы міндеттерді шешудің жолдары мынадай:

Қазақстан нарығында ұсынылған жабдықтарды талдау, атап айтқанда: еліміздің нарығында отандық және шетелдік өндірушілер ұсынған жабдықтардың барлық түрлеріне салыстырмалы талдау жүргізу және ақпаратты қорғауды қамтамасыз етуді ескере отырып, жабдықтардың бір түрін пайдаланудың артықшылықтары туралы қорытынды жасау.

Бұл дипломдық жұмыстың тақырыбы бойынша берілген кәсіпорын желісінің қауіпсіздігін қамтамасыз ететін кешенді талдау жүргізіп, ақпаратты

қорғау жөніндегі тиімді жобасын жасауды әзірлеу бойынша осы өзекті мәселелерді шешуге арналған.

Сонымен қатар, дипломдық жұмыс тақырыбының өзектілігі қазіргі уақытта қалыптасқан объективті қарама-қайшылықты шешуге бағытталған, бір жағынан, кәсіпорын желілері қауіпсіздігін нығайту болса, екінші жағынан жергілікті желілер мен олардың пайдаланушыларының санын көбейту қажеттілігінің өсуі мен байланыс арналарының шектеулі мүмкіндіктері арасында, ақпараттық қауіпсіздікті және осы технологияларды қолдану мақсаттылығын тәуекелге негіздеу.

Кәсіпорын қауіпсіздігін қорғауды ұйымдастыру ақпараттық қауіпсіздік туралы қолданыстағы заңдар мен ережелерді толығымен сақтауға тиіс. Заманауи кәсіпорындардың басым бөлігі өздерінің меншік нысаны мен қызмет түріне қарамастан, өздерінің қызметін автоматтандырылған жүйелерде өңдеу, сақтау және алмасу кезінде ақпараттық қауіпсіздікті ұйымдастырушылық, реттеуші және техникалық құралдарын қоса алғанда, ақпаратты қорғау жүйесін қамтамасыз ете алмай сәтті жүзеге асыра алмайды.

1. Ақпараттық бөлім

1.1 Ұжымдық қауіпсіздік желісінің өзектілігі

Ұжымдық қауіпсіздікті қамтамасыз ету - заңнамалық, әкімшілік, процедуралық және бағдарламалық-техникалық деңгейде үйлестірілген әрекеттерді талап ететін күрделі мәселе. Әкімшілік деңгейдегі негізгі құжатты ұйымның қауіпсіздік саясаты құрылып және іске асырылған кезде интернет қоғамдастығының ұсыныстарын «Кәсіпорынның ақпараттық қауіпсіздік жөніндегі нұсқаулығын» пайдалануға болады. Мұнда қауіпсіздік саясаты мен процедураларын қалыптастырудың практикалық аспектілерін айқындайды, әкімшілік және іс жүргізу деңгейлерінің негізгі ұғымдарын түсіндіреді, өткізілуге қажет іс-әрекеттерге уәждеме беріледі, тәуекелдерді талдау мәселелеріне, құқық бұзушылықты жауап беруге, ақпараттық қауіпсіздік қажет деңгейге келтіру әрекеттеріне қөңіл бөлінген.

Қауіпсіздік саясаты, қорғауды ұйымдастырудың жалпы қағидалары, ресурстарды топтастыру және басқару, қызметкерлердің қауіпсіздігі, физикалық қауіпсіздік, жүйе мен желіні басқару қағидаттары, қол жеткізуді бақылау, ақпараттық жүйелерді құру және сүйемелдеу, сондай-ақ ұйымның үздіксіз жұмыс жасауын жоспарлау сияқты түсініктер мен рәсімдер келтірілген БАҚ-та интернет арқылы ақпараттар мен қаржылардың ұрланғандығын жиі хабарлайды, әдетте хакерді қолға түсіру оңайға соқтырмайды. Ал кәсіпорындардың көпшілігі өздерінің іскерлік беделін сақтау үшін өз желілерінің бұзылғандығын, деректердің ұрланғандығын жасырады.

Зиянкестердің құрбаны болмас үшін, ұжымдық компьютерлер мен желілерді интернет қауіптен қорғау қажет. Кәсіпорынның ақпараттық қауіпсіздігін қамтамасыз ету қажеттілігі туындаған кезде басшылық әдетте жүйелік интеграторларға жүгінеді. Олар кешенді талдау жүргізіп, ақпаратты қорғау жөніндегі жобаны әзірлейді. Соңына келе, осының бәрі Cisco , Microsoft ISA, Checkpoint секілді қымбат бағдарламалық және ақпараттық құралдарды сатып алуға алып келеді. Мұндай үлкен кешенді жобалар 15 мың астам АҚШ долларынан тұрады және тұрақты қызмет көрсетілуін талап етеді және ірі кәсіпорындар үшін ғана орынды қолданады.

Шағын және орта кәсіпорындар үшін барлық қорғау жобасын екі пунктке жеткізуге болады:

Дербес компьютерлерді қорғау;

Интернет-шлюзден және фаерволдан алынған кешен, кәсіпорын желісін бүкіләлемдік желіден және пайдаланушы компьютерін сырттан енуден қорғайтын;

Ақпараттық қауіпсіздікті қамтамасыз ету жүйесі ақпараттық ортаны қорғауға бағытталған ұйымдастырушылық, әкімшілік-құқықтық, бағдарламалық-

техникалық және өзге де іс-шаралар кешенін білдіреді. Кәсіпорынның ақпараттық қауіпсіздігін қамтамасыз етудің кешенді интеграцияланған жүйесінің (АҚЖ) объектілеріне:

Ақпараттық жүйелер (пайдаланушылардың сұраулары бойынша ақпаратты сақтауға, іздеуге және беруге арналған жүйелер);

Ақпараттық процестер (ақпараттық жүйелер мен деректерді беру құралдарымен қамтамасыз етілетін ақпаратты қабылдау, жинақтау, өңдеу және беру процестері);

Ақпараттық ресурстар – кәсіпорын үшін құнды және материалдық ресурстар ретінде әрекет ететін деректер жиынтығы: сыртқы жадыда сақталатын негізгі және қосалқы деректер массивтері және кіріс құжаттары.

Өкінішке орай, күрделі желілік технологиялар мақсатты шабуылдар үшін осал. Бұл ретте бағытталған шабуылдар сырттан, оның ішінде желіден тыс орындалуы мүмкін. Осының барлығы ақпараттық инфрақұрылым әзірлеуші алдында жаңа мәселелерді қояды. Кейбір қазіргі заманғы бизнестің нысандары желілік технологияларға толығымен негізделген (электрондық сауда, IP-телефония, желілік провайдерлер және т.б.) осы себепті осалды. Бұл тұста заңнама саласында халықаралық ынтымақтастық және желілік зиянкестер үшін кедергілер орнату қажет. Қауіпсіздік талаптарын ескере отырып, уақыт өте келе кейбір хаттамалар мен бағдарламаларды түрлендіруге тура келеді.

Қауіпсіздік комплекстік ұғым болғандықтан, оған жабдықтардың сенімділігінің техникалық аспектілері, электр желісінің сапасы, бағдарламалық қамтамасыздықтың осалдылығы және т.б. кіреді.

Желіні интернеттен ажыратуға, дискілік қорғауды қамтамасыз ету үшін RAID жүйесін орнатуға, сенімді UPS жүйесімен қамтасыз етуге болады, алайда өрт туындаған жағдайда бірнеше жыл жасаған деректер базасын жоғалтуға болады. Желіні жобалау барысында, бастысы объективті, субъективті барлық ықтимал қатерлерді ескеру қажет.

1.2 Желілік қауіпсіздіктің негізгі мақсаттары

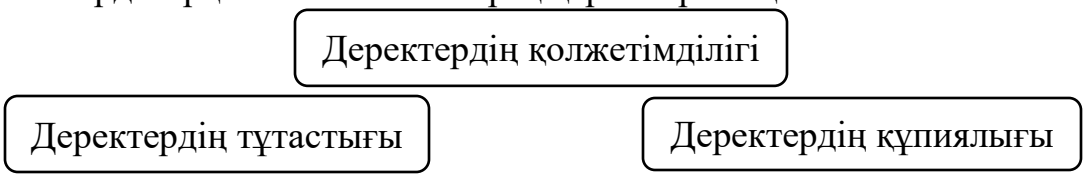
Желілік қауіпсіздік мақсаттары жағдайларға байланысты өзгеруі мүмкін, бірақ негізгі мақсаттары әдетте үшеу:

Деректердің тұтастығы.

Деректердің құпиялығы.

Деректердің қолжетімділігі.

Оларды әрқайсысын толығырақ қарастырайық.



Деректердің тұтастығы

Желілік қауіпсіздіктің негізгі мақсаттарының бірі – деректердің өзгермеуіне, ауыстырылуы немесе жойылмауына кепілдік беру. Деректер тұтастығы кездейсоқ және зұлымдық әрекеттерден сақталуына кепілдік беруі тиіс. Деректер тұтастығын қамтамасыз ету әдетте желілік қауіпсіздіктің ең күрделі міндеттерінің бірі болып табылады.

Деректердің құпиялығы

Желілік қауіпсіздіктің екінші басты мақсаты деректердің құпиялылығын қамтамасыз ету болып табылады. Барлық деректерді құпия ақпаратқа жатқызуға болмайды. Құпия ақпаратқа келесі деректерді жатқызуға болады.

- пайдаланушылардың жеке мәліметтері.
- тіркелуші жазбалары(есімдер және құпия сөз)
- кредит карта туралы деректер.
- әзірлемелер туралы деректер және әртүрлі ішкі құжаттар.
- бухгалтерлік ақпарат.

Деректердің қолжетімділігі

Деректер қауіпсіздігінің үшінші мақсаты олардың қол жетімділігі болып табылады. Пайдаланушы деректердің қол жетімсіздігінен жұмыс жасай алмаса, деректер қауіпсіздігі жайлы айту пайдасыз. Әдетте жергілікті желіде “қол жетімді” болуы тиіс ресурстардың тізіміне принтерлер, серверлер және жұмыс станциялары жатады.

Желі қауіпсіздігі жолында тұрған қауіп-қатерлер мен кедергілерді қарастырып көрейік. Олардың барлығын екі үлкен топқа бөлуге болады:

1.Техникалық қауіптер

2.Адами факторлар.

Техникалық қауіптер:

- бағдарламалық қамтамасыз етудегі қателер.
- түрлі DoS және DDoS- шабуылдар.
- компьютерлік вирустар, трояндар.
- хаттама талдағыштар және тыңдауыш бағдарламалар(снифферлер).
- ақпарат алудың техникалық құралдары.

Кез келген желінің осал жері – сервер, маршрутизатор және жұмыс орындардың бағдарламалық қамтамасыздығы. Мұндай бағдарлама жүйесінің күрделігі жоғары болған сайын, онда қатер табу ықтималдығы соғұрлым көп болады. Олардың көпшілігі ешқандай қауіп төндірмейді, кейбіреуі зиянкестердің серверді бақылауына алуы, сервердің істен шығуы, ресурстарды рұқсатсыз пайдалану сияқты салдарға әкелуі мүмкін. Мұндай осалдылықтардың көпшілігі бағдарлама қамтамасыздығының өндірушісі үнемі шығаратын жаңартулар

пакеттерінің көмегімен жойылады. Мұндай жаңартуларды уақытылы орнату желі қауіпсіздігінің қажетті шарты болып табылады.

DoS және DDoS-шабуылдар

Denial Of Service(қызмет көрсетуден бас тарту) – желіні немесе серверді жұмысқа қабілетті күйден шығаруға бағытталған шабуылдардың ерекше түрі. DoS-шабуылдарда бағдарламалық қамтамадағы қателер немесе үлкен ауқымдағы операциялар қолданылуы мүмкін. DDoS (Distributed Denial Of Service)шабуылдардың жаңа түрі алдыңғыдан әр түрлі аймақта орналасқанбірнеше компьютерлердің тұтастығымен ерекшелінеді. Мұндай шабуылдар каналды трафикпен шамадан тыс жүктейді, пайдалы ақпарат өтімділігіне кедергі жасайды.

Компьютерлік вирустар, трояндар.

Вирустар – қауіптің соңғы кездердегі таза күйде кездеспейтін ескі санаты болып табылады. Желілік технологияларды белсенді пайдаланудың әсерінен вирустар бағдарламалық компененттерге біріктіріледі. Қазіргі таңда вирустардың таралуының көп жолдары бар: электрондық пошта, ақпарат тасушы құрылғылары. Жиі жағдайларда залалданған машина DDos – шабуылшысы болады. Қорғану шаралары көп, олардың бірі жаңартуларды уақытылы орнату болып табылады.

Снифферлер және хаттама талдағыштар.

Бұл топқа желі арқылы берілетін деректерді ұстап қалу құралдары кіреді. Мұндай құралдар аппараттық және бағдарламалық болуы мүмкін. Әдетте деректер желі бойынша ашық түрде беріледі, бұл қаскүнемге жергілікті желі ішінде оларды ұстап алуға мүмкіндік береді. Желі жұмысының кейбір хаттамалары (FTP,POP) парольдерді шифрлауды қолданбайды, бұл қаскүнемге оларды ұстап, өзіне пайдалануға мүмкіндік береді. Мүмкіндігінше авторланбаған пайдаланушылар мен кездейсоқ адамдарға желіге кіруді шектеу қажет.

Ақпарат алудың техникалық құралдары.

Бұл топқа мини камералар, дыбыс жазушы құралдар, пернетақта тыңшысын жатқыздыруға болады. Бұл топ жоғарыда айтылғандардан сирек кездеседі, себебі арнайы желіге және оның құрамдас бөліктеріне қолжетімділікті талап етеді.

Адами факторлар:

- жұмыстан босатылған немесе наразы қызметкерлер.
- өнеркәсіптік тыңшылық.
- немқұрайлық
- төмен біліктілік.

Жұмыстан босатылған және наразы қызметкерлер

Адамдардың бұл тобы аса қауіпті, себебі жұмыс істейтін қызметкерлердің көпшілігі құпия ақпаратқа рұқсат етілген болуы мүмкін. Бұл топты жүйелік администраторлар құрайды, көбінесе өзінің материалдық жағдайына көңілі

толмайтын немесе жұмыстан босатумен келіспейтіндер, олар ресурстарды одан әрі зиянды пайдалану, құпия ақпаратты ұрлау және т.б. әрекеттерге баруы мүмкін.

Өнеркәсіптік тыңшылық

Бұл ең қиын факторлардың бірі. Егер сіздің деректеріңіз біреуге қызықты болса, онда бұл адам оны алу жолдарын табады. Жақсы қорғалған желіні бұзу оңай емес. Мүмкін, қарапайым тазалау жұмыстарымен айналысытын үстелдің астын жуып, қораптағы сымдарға ашуланып, үнемі бір нәрсеге наразы болып жүретін кіші қызметкерлердің өзі өте жоғары деңгейдегі хакер болып шығуы мүмкін.

Немқұрайлылық

Бұзушылықтардың өте кең тараған болып табылады. Бұл уақытылы орнатылмаған жаңартулардан бастап, өзгермеген «әдепкі» параметрлерден Internet, кіру үшін рұқсат етілмеген модемдерге дейін болуы мүмкін, нәтижесінде шабуылдаушылар жақсы қорғалған желіге қол жеткізе алады.

Төмен біліктілік

Көбінесе білімнің жеткіліксіз болуы пайдаланушыға не істеп жатқанын түсінуге мүмкіндік бермейді; осыған байланысты, тіпті жақсы қорғаныс бағдарламалары жүйелік әкімші үшін нағыз мәселеге айналады және ол тек периметрді қорғауға сенуге мәжбүр болады. Көптеген қолданушылар орындалатын файлдар мен сценарийлердің нақты қауіпін түсінбейді және орындалатын файлдар тек «exe» кеңейтімі бар файлдар деп санайды. Төмен біліктілік сонымен қатар қай ақпарат шынымен құпия және қайсысы ашылатындығын анықтай алмайды. Ірі компанияларда сіз пайдаланушыға жиі қоңырау шалып, өзіңізді әкімші ретінде таныстыра аласыз, одан желіге кіру туралы мәліметтерді біле аласыз. Шығудың бір ғана жолы бар - пайдаланушыларды оқыту, тиісті құжаттарды құру және біліктілікті арттыру.

1.3. Қорғау түрлері және қорғану әдістері

Кәсіпорынның жалпы инфрақұрылымындағы әрбір АТ қызметі немесе объектісі белгілі бір қауіп факторына ие, сондықтан кез-келген мекеме үшін қауіпсіздік тұжырымдамасын әзірлеу оларды жан-жақты талдаудан басталуы керек.

Қауіпсіздік тұжырымдамасын жоспарлаудың тағы бір маңызды факторы әрбір АТ-инфрақұрылымдық қызметке әр түрлі қауіптерді қарастыру керек. Бұл аспектілер объектілерді бағалау факторларымен тікелей байланысты және қорғаныс шаралары бойынша кейінгі әрекеттер туралы ақпарат береді. Іс-шаралар тиімділігінің маңызды ережесі - қорғау артық болмауы керек.

Қатерлердің түрлеріне жан-жақты талдаудың нәтижелері және АТ-инфрақұрылымының әр объектісін бағалау қауіпсіздік саясатын әзірлеу және іске асыру үшін негіз болып табылады. Ол басқару саясатын, мониторинг және аудит жүйелерін баптау және жаңарту және басқа да жүйелік саясат пен рәсімдердің

алдын-алу шараларын қамтиды. Кәсіпорынның типтік IT ортасының аналогы аз сынақ зертханасының болуы міндетті шарт болып табылады. Жүйелердің қауіптері мен осал тұстарын талдауда жинақталған білім мен тәжірибе, шын мәнінде, бірегей білім базасы болып табылады және сенімді және қауіпсіз инфрақұрылым құруға және қызметкерлерді кейінгі оқытуға негіз болады. Алайда, инфрақұрылымды өзгерту (модернизациялау), жаңа қондырғылар қосу кезінде қауіпсіздік саясатын қайта бағалау, талдау және кейіннен өзгерту қажет екенін атап өткен жөн.

Осы тұста мынадай қауіп-қатерлер кездесуі мүмкін.

Артықшылықтың өсуі - буферлік толып кету, заңсыз әкімшілік құқықтарды алу арқылы шабуыл жасау арқылы жүйелік артықшылықтарды алу.

Фальсификация - желі арқылы берілетін мәліметтерді өзгерту, файлдарды өзгерту.

Симуляция - электрондық хабарламаларды қолдан жасау, аутентификация кезінде жауап пакеттерін жасау.

Ашу - құпия ақпаратқа рұқсатсыз қол жеткізу немесе заңсыз жариялау.

Қабылдамау - сыни файлды немесе сатып алуды жою, содан кейін олардың әрекеттерін мойындаудан бас тарту.

Сервистен бас тарту - жалған пакеттердің көптігі бар желілік ресурстарды жүктеу.

Барлық деңгейде қорғану әдістері.

Кәсіпорынның IT-ортасына сәтті кіру мүмкіндігін азайту үшін барлық деңгейлерде қауіпсіздік шараларын жасау қажет. Бұл ақпараттық қауіпсіздік тұжырымдамасы қорғаудың бір деңгейінің бұзылуы бүкіл жүйеге нұқсан келтірмейді дегенді білдіреді.

Әр қауіпсіздік деңгейінің дизайны мен құрылысы кез-келген деңгей шабуылдаушы тарапынан бұзылуы мүмкін деп болжауы керек. Сонымен қатар, деңгейлердің әрқайсысының өзіндік ерекше және тиімді қорғау әдістері бар. Көптеген танымал сатушылар жасаған және қол жетімді технологиялар тізімінен техникалық және экономикалық факторларға ең қолайлы нұсқаны таңдауға болады. Мысалы:

Деректерді қорғау - қол жеткізуді басқару тізімдері, шифрлау.

Қосымшалар - қорғалған қосымшалар, антивирустық жүйелер.

Компьютерлер - операциялық жүйені қорғау, жаңартуды басқару, аутентификация, хост деңгейіндегі кіруді анықтау жүйесі.

Ішкі желі - желіні сегментациялау, IP қауіпсіздігі, желіні басып кіруді анықтау жүйелері.

Периметр - бағдарламалық және аппараттық-бағдарламалық брандмауэр, карантиндік функциялары бар виртуалды жеке желілерді құру.

Физикалық қорғаныс - қауіпсіздік, қол жетімділікті бақылау және бақылау құралдары.

Саясаттар мен процедуралар - пайдаланушылар мен техникалық қызметкерлерді оқыту.

Осылайша, барлық деңгейлердегі кешенді қорғаныс шараларының нәтижесінде интрузияны анықтау процесі жеңілдетіліп, шабуылдаушының жетістікке жету мүмкіндігі азаяды.

Адам факторы

Көптеген қорғаныс деңгейлері аппараттық және бағдарламалық жасақтамаға негізделген, алайда «адам факторының» әсері жалпы көріністі елеулі түрде өзгертеді.

Физикалық қорғаныс деңгейі

Физикалық қорғауға қойылатын талаптар негізгі және негізгі болып табылады.

Жабдыққа физикалық қол жеткізе отырып, шабуылдаушы келесі қорғаныс деңгейлерінен оңай өтіп кетеді. Қол жеткізу үшін компанияның телефондарын немесе телефон құрылғыларын пайдалануға болады. Маңызды ақпараттың ағып кетуіне әсіресе корпорациядан тыс жерде болуы мүмкін ноутбуктер жатады.

Кейбір жағдайларда қол жеткізу факторы зиян келтіруге бағытталған. Алайда, егер сізде физикалық қол жетімділік болса, маңызды корпоративтік ақпаратты бақылау және бақылау үшін бағдарламалық жасақтама құралдарын орнатуға болады, ол оны ұзақ уақыт жинақтайды.

Физикалық қорғаныс деңгейінің қауіпсіздігін қамтамасыз ету үшін кәсіпорын қаражатына мүмкіндік беретін кез-келген құралдарды пайдалануға болады. Қауіпсіздік мүмкіндіктері АТ инфрақұрылымының барлық компоненттерін қамтуы керек. Мысалы, сервистік инженер мекеме пайдаланушыларының маңызды деректері бар RAID1 деңгейінің сәтсіз массивін ауыстырды. Осыдан кейін дискіні қызмет көрсету орталығына жіберуге болады, онда оны қалпына келтіруге және деректерге қол жеткізуге болады. Бұл жағдайда кәсіпорынның физикалық қорғау деңгейіне нұқсан келтірілген деп санауға болады.

Қорғаныштың сенімді деңгейін қамтамасыз етудегі алғашқы қадам сервер мен пайдаланушының инфрақұрылымын физикалық бөлу болып табылады. Сонымен бірге, кіруді қатаң бақылау және бақылау процедуралары бар жеке, қауіпсіз қоршалған бөлме болуы міндетті болып табылады. Магниттік карталар немесе биометриялық құрылғылар негізінде жеке қол жетімділіктің болуы шабуылдаушының мүмкіндігін айтарлықтай төмендетеді. Сервер бөлмесі автоматты өрт сөндіру және климаттық бақылау жүйелерімен жабдықталған болуы керек.

Оқиғаларды жазу мүмкіндігі бар бейнебақылау жүйесін пайдалану арқылы қол жеткізуді қосымша басқаруға болады.

Сервер консольдеріне қашықтан қол жетімділік те қатаң бақылауда болады. Әкімшілік топты басқарылатын коммутаторлар мен хосттардың желілік деңгейінде де, жеке сәйкестендірудің логикалық деңгейінде де тұрақты қол жетімділікпен жеке физикалық сегментке бөлу мағынасы бар.

Физикалық қорғаудың толық спектрін қамтамасыз етудің кейінгі шаралары кіріс құрылғыларын (дискета және CD дискілері) қажет емес жерлерде оларды компьютерлерден шығаруға және жоюға бағытталуы керек. Егер бұл мүмкін болмаса, тасымалдаушы құралға кіруді бұғаттау үшін міндетті түрде бағдарламалық жасақтаманы пайдалану керек. Сайып келгенде, қол жетімділігі бар арнайы шкафтардағы белсенді желілік жабдықтардың (коммутаторлар, маршрутизаторлар) физикалық қорғалуының кепілдігі қамтамасыз етілуі керек. Сонымен қатар, шынымен қажет құрылғылар мен тоқ көздерінің ауысуын ғана қамтамасыз ету керек.

Физикалық қол жетімділіктің әсері

Файлдарды қарау, өзгерту, жою

Зиянды кодты орнату

Жабдықтың зақымдануы

Жабдықты бөлшектеу

Периметр қауіпсіздігі

Ақпараттық жүйенің периметрі - бұл сыртқы шабуылдарға барынша ашық желілік инфрақұрылым бөлігі. Периметрге интернет, бұтақтар, серіктес желілер, мобильді пайдаланушылар, сымсыз желілер кіреді.

Интернетке қосымшалар.

Бұл деңгейдің қауіпсіздігін нақты бағыт үшін ғана емес, тұтастай қарастыру маңызды. Периметр бойынша шабуылдың мүмкін бағыттары:

• ұйым желісіне

• мобильді пайдаланушылар үшін

• серіктестерден

Әдеттегідей, интернеттің бағыты ең осал болып табылады, алайда басқа бағыттағы қауіп те маңызды емес. Сіздің желіге кіретін және шығаратын барлық құрылғылардың қауіпсіздігі маңызды. Іскери серіктестердің немесе филиалдардың желілік инфрақұрылымындағы қорғаныс шаралары туралы сенімсіз болу мүмкін, сондықтан бұл бағытқа да назар аудару қажет.

Периметр қауіпсіздігі ең алдымен брандмауэрді қолдану арқылы қамтамасыз етіледі. Олардың конфигурациясы, әдетте, техникалық жағынан өте күрделі және жоғары білікті қызметкерлерді, сондай-ақ параметрлерді мұқият құжаттауды қажет етеді. Қазіргі операциялық жүйелер шабуылдың ықтималдығын азайту үшін пайдаланылмаған порттарды оқшаулауды жеңілдетеді.

Желілік мекен-жайларды аудару (NAT) ұйымға ішкі порттарды жабуға мүмкіндік береді. Ақпаратты қауіпті арналар арқылы беру кезінде шифрлау мен туннельдерге негізделген виртуалды жеке желілерді (VPN) құру әдістерін қолдану қажет.

Қауіптер мен LAN қорғанысы

Шабуыл тек сыртқы көздерден ғана жасалуы мүмкін. Статистикаға сәйкес, сәтті шабуылдардың өте үлкен пайызы желілік ортадағы шабуылдарға жатады. Зиянды және кездейсоқ қатерлерді тоқтату үшін ішкі желінің қауіпсіздігін құру өте маңызды. Желінің ішкі инфрақұрылымына бақылаусыз қол сұғушыға маңызды корпоративтік мәліметтерге қол жеткізуге және желілік трафикті басқаруға мүмкіндік береді. Толық реттелетін желілер шабуылдаушыға кез-келген желі сегментіндегі кез-келген ресурстарға қол жеткізуге мүмкіндік береді. Желілік операциялық жүйелерде көптеген орнатылған желілік қызметтер бар, олардың әрқайсысы шабуылдың объектісі бола алады.

Желінің ішкі ортасын қорғау үшін, ғаламдық каталог қызметінде (бірыңғай кіру орталығы) пайдаланушыларды сенімді аутентификациялау тетіктерін қамтамасыз ету қажет. Сервер мен желілік жұмыс станциясы деңгейіндегі өзара аутентификация желілік қауіпсіздіктің сапасын айтарлықтай арттырады. Ағымдағы талаптар басқарылатын коммутацияланатын орта мен логикалық сегментацияны (VLAN) білдіреді. Қашықтағы құрылғыларды басқару үшін сіз әрдайым қауіпсіз хаттама байланысын пайдалануыңыз керек (мысалы, SSH). Телнет байланысының трафигін оңай ұстап алуға болады, ал атаулар мен парольдер нақты мәтінмен беріледі. Желілік құрылғы конфигурациясының резервтік көшірмелерін қорғауға барынша назар аудару арқылы олар шабуылдаушыға желілік топология туралы көп нәрсе айта алады.

Сурет 1.1 - LAN қауіптері

Желілік сегменттен кейін де желілік трафик қорғалуы керек. Сымды және сымсыз қосылымдардың екеуінде де шифрланған және аутентификацияланған

қатынасты қамтамасыз ету үшін 802.1X протоколын пайдалануға болады. Бұл шешім ғаламдық каталог қызметінде (Microsoft Active Directory, Novell e-Directory және т.б.) немесе сандық сертификаттардағы есептік жазбалар мен парольдерді қолдана алады. Куәліктердің сандық технологиясы желілік тасымалдауда өте жоғары қорғанысты қамтамасыз етеді, бірақ ол сервер мен сертификаттар дүкені түрінде ашық кілт инфрақұрылымын орналастыруды талап етеді.

Шифрлау технологияларын және IPSec немесе Server Message Block (SMB) қол қою сияқты цифрлық қолтаңбаларды енгізу желілік трафикті ұстап қалуға және оны талдауға жол бермейді.

LAN қорғанысы

Пайдаланушылар мен желілік ресурстардың өзара аутентификациясы

LAN сегментациясы

Желілік трафикті шифрлау

Пайдаланылмаған порттарды бұғаттау

Желілік құрылғыларға қол жеткізуді басқару

Сандық түрде желілік пакеттерге қол қою

Компромисс және компьютерді қорғау

Желілік ортадағы компьютерлік жүйелер қорғаныс талаптарын анықтайтын бірнеше тапсырмаларды орындайды. Желі хосттарына көпшілік қол жетімді болғандықтан шабуыл жасауы мүмкін. Шабуылдаушылар шабуыл жасау үшін зиянды кодты (вирустарды) тарата алады. Жұмыс станцияларында және серверлерде орнатылған бағдарламалық жасақтамада бағдарламалық кодтың осал тұстары болуы мүмкін, сондықтан жаңартуларды уақытында орнату жалпы қорғаудың тұжырымдамасындағы маңызды қадамдардың бірі болып табылады.

Компьютер деңгейіндегі қауіпсіздік саясатының параметрлерін орталық бақылау қажет, мысалы, Group Policy қолдана отырып. Бұл деңгейдегі серверлік жүйелерді қорғау файлдық жүйелер үшін қауіпсіздік атрибуттарын орнатуды, аудит саясаттарын, портты сүзгілеуді және сервердің рөлі мен мақсатына байланысты басқа шараларды қамтиды.

Амалдық жүйенің және бағдарламалық жасақтаманың барлық қол жетімді жаңартуларының болуы қауіпсіздіктің жалпы деңгейін айтарлықтай жақсартады. Сіз автоматты түрде орнатудың және жаңартуларды бақылаудың кез келген құралдарын пайдалана аласыз, ең қарапайымынан - Windows жаңарту, бағдарламалық жасақтаманы жаңарту қызметі (SUS), Windows жаңарту қызметі (WUS) бастап ең күрделі және қуатты - жүйелерді басқару сервері (SMS).

Ағымдағы жаңартулары бар антивирустық пакетті пайдалану арқылы портты сүзгіленген жеке брандмауэр шабуыл жасау мүмкіндігін азайтады.

Компьютерді қорғау үшін:

Пайдаланушылардың, серверлердің және жұмыс станцияларының өзара аутентификациясы

ОЖ қорғанысы

Қауіпсіздік жаңартуларын орнатыңыз
Сәтті және сәтсіз оқиғаларды тексеріңіз
Пайдаланылмаған қызметтерді өшіру
Антивирустық жүйелерді орнату және жаңарту
Қолданбаны қорғау

Желілік қосымшалар пайдаланушыларға деректерге қол жеткізуге және басқаруға мүмкіндік береді. Желілік қосымша - бұл бағдарлама жұмыс істейтін серверге кіру нүктесі. Бұл жағдайда қосымша зиянды пайдаланушылардың шабуылына төзімді болуы керек желілік қызметтің белгілі бір деңгейін қамтамасыз етеді. Өзіміздің әзірлемелерімізді де, осалдықтар үшін пайдаланылатын коммерциялық өнімдерді де мұқият зерттеу қажет. Шабуылдың мақсаты қолданбалы кодты жою (нәтижесінде - қол жетімсіздігі) және зиянды кодты орындау болуы мүмкін. Сондай-ақ, шабуылдаушы қолданбалы жұмыстың шамадан тыс жүктелуіне бағытталған таратылған шабуыл тактикасын қолдана алады. Нәтижесінде қызмет көрсетуден бас тарту мүмкін (қызмет көрсетуден бас тарту).

Қосымшаны пошта хабарламаларын бағыттау (ашық поштаның релесі) сияқты күтпеген тапсырмаларда қолдануға болады. Қосымшаларды қажетті функционалдылық пен қызмет көрсету деңгейімен ғана орнату және конфигурациялау керек, ал бағдарламалық кодты бақылау жүйелерімен және антивирустық пакеттермен басқаруға болады. Қатерлерді азайту үшін қосымшалардың орындалуы желінің ең төменгі артықшылықтарымен шектелуі керек.

1.5 Ұжымдық желіні ұйымдастыру және оны қорғау

Желіні ұйымдастыру үшін желілік жабдықты пайдаланады.

Тор немесе роутер маршрутизасы (ағылш. router) - кемінде бір желілік интерфейсі бар мамандандырылған желілік компьютер;

Желі сегменттері арасындағы деректер пакеттерін қайта жіберетін, әр түрлі құрылымды желілерді байланыстыратын, қабылдаушы топология туралы ақпарат негізінде жіберу туралы шешім желі әкімші берген белгілі бір ережелердің болуы.

Маршрутизатор жоғары "желілік" үш деңгейде жұмыс істейді.

OSI модельдері,коммутатор (немесе желіліккөпір)және концентратор (хаб),олар 2 деңгейінде және 1 OSI деңгейінде жұмыс істейді.

Желілік коммутатор (ағылш. Switch-қосқыш)-құрылғы, бірнеше тораптық компьютерлерді қосуға арналған желі бір немесе бірнеше сегменттер шегінде жұмыс атқарады.

Коммутатор OSI моделінің арналық (екінші) деңгейінде жұмыс жасайды. Көппортты көпірлерді коммутаторлар көпірлерді пайдалану технологияларын жиі

қарастырылады. Қосу үшін бірнеше желілерді негізінде маршрутизаторлар желілік деңгейдің қызмет етеді.

Бір қосылған құрылғыдан басқаларына трафикті тарататын концентратор В В коммутатор деректерді береді, тек тікелей алушыға ғана айырмашылық (барлық желі тораптарына кең тарату трафигін және коммутатордың шығыс порты белгісіз құрылғыларға арналған трафикті қоспағанда). Бұл желінің басқа сегменттерін оларға арналмаған деректерді өңдеу қажеттілігінен (және мүмкіндіктерінен) босата отырып, желінің өнімділігі мен қауіпсіздігін арттырады.

Желілік экранның негізгі міндеті компьютерлік желілерді немесе жекелеген тораптарды рұқсатсыз кіруден қорғау болып табылады. Сонымен қатар, желілік экрандар жиі сүзгілер деп аталады, себебі олардың негізгі міндеті - конфигурацияда анықталған критерийлерге сәйкес келмейтін пакеттерді өткізбеу (сүзу).

Кейбір желілік экрандар, сондай - ақ адрестердің трансляциясын жүзеге асыруға мүмкіндік береді-желіішілік (сұр) адрестердің немесе порттардың жергілікті есептеуші желі шегінен тыс пайдаланылатын сыртқы мекен-жайларының қозғалысының ауыстырылуын жүзеге асырады.

1.6 Ұжымдық желіні құру

Ұжымдық желілер туралы айтпас бұрын, бұл сөздердің нені білдіретінін анықтау керек. Соңғы уақытта бұл сөздің танымалдығы артуда. Біздің түсінуімізде ұжымдық желі - мекеме жүйесінде қолданылатын әртүрлі қосымшалар арасында ақпаратты беруді қамтамасыз ететін жүйе. Осыған байланысты, біз осындай жүйелерді құрудың түрлі тәсілдерін қарастырамыз және ұжымдық желі ұғымын нақты мазмұнмен толтыруға тырысамыз. Сонымен қатар, біз желі барынша әмбебап болуы керек деп есептейміз, яғни қолда бар және болашақ қосымшаларды ең аз ықтимал шығындар мен шектеулермен біріктіруге жол береміз.

Ұжымдық желі, әдетте, аумақтық бөлінген, яғни бір-бірінен едәуір алшақ орналасқан кеңселерді, бөлімшелерді және басқа да құрылымдарды біріктіретін болып табылады. Ұжымдық желі тораптары жиі әртүрлі қалаларда, кейде елдерде орналасқан. Мұндай желі салынатын принциптер бірнеше ғимаратты қамтитын жергілікті желіні құру кезінде пайдаланылатындардан айтарлықтай ерекшеленеді. Негізгі айырмашылық аумақтық бөлінген желілер жеткілікті баяу (бүгінгі күні - секундына ондаған және жүздеген килобит, кейде 2 Мбит/с дейін) байланыс желілерін пайдаланады. Егер жергілікті желіні құру кезінде негізгі шығындар жабдықты сатып алуға және кәбілді төсеуге тура келсе, онда аумақтық-бөлінген желілерде құнның ең маңызды элементі деректерді беру сапасы мен жылдамдығының артуымен жылдам өсетін арналарды пайдалану үшін жалдау ақысы көрсетіледі. Бұлшектеу принципті болып табылады және корпоративтік желіні жобалау кезінде берілетін деректердің көлемін азайту үшін барлық

шараларды қолдану керек. Сонымен қатар, бұл жүйе бойынша ақпаратты өңдеу үшін қандай да бір қосымшалар мен қандай жолмен өңделетін ақпаратқа шектеу енгізбеуі тиіс.

Қосымшаларды біз мұнда жүйелік бағдарламалық қамтамасыз етуді - деректер базасын, пошта жүйелерін, есептеу ресурстарын, файлдық сервисті және басқаларды - соңғы пайдаланушы жұмыс істейтін құралдарды түсінеміз. Ұжымдық желінің негізгі міндеттері әртүрлі тораптарда орналасқан жүйелік қосымшалардың өзара іс-қимылы және оларға қашықтағы пайдаланушылардың қол жетімділігі болып табылады.

Ұжымдық желіні құру кезінде шешуге тура келетін бірінші мәселе-байланыс арналарын ұйымдастыру. Егер бір қала шегінде бөлінген желілерді, соның ішінде жоғары жылдамдықты желілерді жалға алуға болатынына сене алатын болсақ, алыс- шалғай қашықтағы тораптарға көшу кезінде арналарды жалға алу құны жай астрономиялық болып табылады, ал олардың сапасы мен сенімділігі төмен болуы мүмкін.

Бұл проблеманың табиғи шешімі қазіргі бар жаһандық желілерді пайдалану болып табылады. Бұл жағдайда кеңселерден желінің жақын тораптарына дейін арналарды қамтамасыз ету жеткілікті. Ақпарат жеткізу тораптары арасындағы міндетін ғаламдық желі бұл ретте өз мойнына алады. Бір қала шегінде шағын желіні құру кезінде де қазіргі бар жаһандық желілермен үйлесімді технологияларды одан әрі кеңейту және пайдалану мүмкіндігін ескеру қажет.

1.7 Internet-ті ұжымдық желілерде пайдалану

Internet шешілетін тапсырмаларға байланысты әр түрлі деңгейлерде қарастыруға болады. Соңғы пайдаланушы үшін бұл ең алдымен дүниежүзілік ақпараттық және пошта қызметтерін ұсыну жүйесі. WorldWideWeb ұғымымен біріктірілетін ақпаратқа қол жеткізудің жаңа технологияларын Internet компьютерлік байланысының арзан және жалпыға қолжетімді Ғаламдық жүйесімен ұштастыру іс жүзінде тек theNet - желі деп аталатын жаңа бұқаралық ақпарат құралын тудырды. Осы жүйеге қосылған адам оны белгілі бір қызметтерге қол жеткізу тетігі ретінде қабылдайды. Осы механизмді жүзеге асыру мүлдем маңызды емес.

Соңғы уақытта кеңінен талқыланатын Internet-тің тағы бір мәселесі қауіпсіздік мәселесі. Егер біз жеке желі туралы айтатын болсақ, берілетін ақпаратты бөтен көзқарастан қорғау әбден табиғи болып табылады. Жиын арасындағы ақпарат жолдарының болжамсыздығы.

Internet тәуелсіз тораптары кез келген желінің қызықты операторы сіздің мәліметтеріңізді дискіге қоса алады (техникалық жағынан бұл қиын емес), сонымен қатар ақпараттың таралып кету орнын анықтау мүмкін емес. Шифрлеу құралдары мәселені тек ішінара шешеді, себебі негізінен поштаға, файлдарды

беруге және т. б. шешімдер қолданылады, бұл ақпаратты нақты уақытта қолайлы жылдамдықпен шифрлауға мүмкіндік береді (мысалы, қашықтағы деректер базасымен немесе файл-сервермен тікелей жұмыс істеу кезінде), жолдар да қол жетімсіз.

Қауіпсіздік проблемасының тағы бір аспектісі Internet орталықсыздығымен байланысты. Сіздің жеке желі ресурстарына қолжетімділікті шектей алатын ешкім жоқ. Бұл ашық жүйе болғандықтан, барлық адамдар кеңселік желіге кіріп, деректер мен бағдарламаларға қол жеткізе алады. Әрине, қорғаныс құралдары бар (олар үшін Firewall - дәлірек айтқанда "брандмауэр"- шабуылға қарсы қабырға деп аталады). Алайда, оларды панацея деп санауға болмайды, вирустар мен антивирустық бағдарламалар туралы есте сақтаңыз. Кез келген қорғауды бұзуға болады, тек бұл бұзу құнын төлейді.

Сондай-ақ, интернетке қосылған жүйені жұмыс істемейтін және сіздің желіге кірмей-ақ жасауға болатынын атап өту қажет. Internet-ті бұзу үшін қолжетімділікті сол немесе басқа серверге басқару тораптары желісі, немесе жай ғана пайдалану ерекшеліктерін құрылымы белгілі рұқсат етілмеген жағдайларда қол жеткізуге болады.

Осылайша, Internet-ті сенімділік пен жабықтықты талап ететін жүйелердің негізі ретінде ұсынуға болмайды. Ұжымдық желіні пайдаланудың негізгі мәні Internet-ке қосылу бізге желі деп аталатын үлкен ақпараттық кеңістікке қиындықсыз қол жеткізу болып табылады.

1.8 Ұжымдық желілердің жабдықтары

Ұжымдық желі- бұл әртүрлі байланыс түрлерін, коммуникация хаттамаларын ресурстарды қосу тәсілдерін пайдаланатын күрделі құрылым.

Барлық құрал-жабдықтар, компьютерлік желілерді екіге бөлуге болады: перифериялық пайдаланылады желісіне қосылу үшін хосттардың және магистральное немесе тіреу, оны іске асыратын негізгі функциялары желісі (арналар коммутациясын, бағдарлауды және т. б.). Бұл түрлердің арасындағы нақты шек жоқ-бір құрылғылар әртүрлі сапада немесе басқа функцияларды біріктіре алады. Атап өту керек, магистральдық жабдыққа әдетте сенімділік, өнімділік, порттар саны және одан әрі кеңейту бөлігінде жоғары талаптар қойылады. Перифериялық жабдық кез келген ұжымдық желінің қажетті компоненті болып табылады. Сонымен қатар, магистральды тораптардың функциялары деректерді берудің ғаламдық желісін өзіне ала алады ресурстар қосылады. Әдетте, ұжымдық желі құрамындағы магистральды тораптар жалға алынған байланыс арналары пайдаланылғанда немесе жеке қатынау тораптары құрылғанда ғана пайда болады.

Сондай-ақ, ұжымдық желілердің перифериялық жабдықтарын орындалатын функциялар тұрғысынан да екі топқа бөлуге болады. Біріншіден, бұл

маршрутизаторлар (routers), қызметшілер біріктіру үшін біртекті LAN (әдетте, IP немесе IPX) арқылы ғаламдық желісінде деректерді беру. IP немесе IPX негізгі хаттама ретінде пайдаланатын желілерде-атап айтқанда, сол Internet-маршрутизаторлар әртүрлі арналар мен байланыс хаттамаларының түйісуін қамтамасыз ететін магистральды жабдық ретінде де пайдаланылады. Маршрутизаторлар дербес құрылғылар түрінде де, компьютерлер мен арнайы коммуникациялық адаптерлер базасында бағдарламалық құралдармен да орындалуы мүмкін.

Екінші кең қолданылатын перифериялық жабдық түрі - әр түрлі желілерде жұмыс істейтін қосымшалардың өзара әрекеттесуін іске асыратын шлюздер (gateways). Ұжымдық желілерде негізінен OSI шлюздері пайдаланылады.

IBM желілеріне қосылуды қамтамасыз ететін SNA шлюздері. Толық функционалды шлюз әрдайым бағдарламалық-аппараттық кешен болып табылады, өйткені қосымшалар үшін қажетті бағдарламалық интерфейстерді қамтамасыз етуі тиіс.

Арасында маршрутизаторлар ең белгілі жабдық Cisco Systems мекеменің іске асыратын үлкен жинағы хаттамалар мен құралдар, жұмыс барысында қолданылатын жергілікті желілер. Cisco жабдығы X. 25, Frame Relay және ISDN сияқты әртүрлі байланыс әдістерін қолдайды, айтарлықтай күрделі жүйелерді құруға мүмкіндік береді. Сонымен қатар, Cisco маршрутизаторлар тобының арасында жергілікті желілерге қашықтағы қатынау серверлері бар, ал олардың кейбірінде шлюздер (Protocol Translation) функциялары ішінара іске асырылған.

Cisco маршрутизаторларын қолданудың негізгі мақсаты-IP немесе IPX хаттамасын пайдаланатын кең желі Cisco жабдығы жиі Internet тірек тораптарында қолданылады. Егер ұжымдық желі алыстағы жергілікті желілерді біріктіруге арналып және IP-дің әртүрлі байланыс арналары мен деректер беру желілері арқылы күрделі бағытталуын талап ететін болса, Cisco жабдығын пайдалану оңтайлы таңдау болады. Ұжымдық желілерде қолдану үшін ең танымал Cisco 2509, Cisco 2511 қатынау серверлері және Cisco 2520 сериялы жаңа құрылғылар болып табылады. Олардың негізгі байланыс аймағы- қашықтағы пайдаланушылардың телефон желілері арқылы жергілікті желілерге немесе IP-адрестердің динамикалық арналуымен (DHCP) ISDN қатынауы болып табылады.

1.9 Ақпараттық қауіпсіздік саясатын жергілікті желіде жобалау

Ақпараттық жүйенің қауіпсіздігін қамтамасыз ету сияқты маңыздылығы жоғары мәселеде толық дайын шешім жоқ және болмақ емес. Бұл әрбір ұйымның құрылымы, оның бөлімшелері мен жекелеген қызметкерлері арасындағы функционалдық байланыстар ешқашан толығымен қайталанбауына байланысты. Тек ұйым басшылығы ақпараттық жүйенің компоненті үшін қауіпсіздіктің

қаншалықты сыни бұзылғанын, кім, қашан және қандай міндеттерді шешу үшін қандай да бір ақпараттық сервистерді пайдалана алатынын анықтай алады.

Сенімді ақпараттық жүйені құру үшін негізгі кезең қауіпсіздік саясатын әзірлеу болып табылады.

Қауіпсіздік саясаты деп біз ақпаратты және онымен байланысты ресурстарды қорғауға бағытталған құжатталған басқару шешімдерінің жиынтығы екені бізге бұрыннан белгілі.

Практикалық тұрғыдан алғанда, қауіпсіздік саясатын үш деңгейге бөлу орынды:

Бірінші деңгей жалпы ұйымға қатысты шешімдер. Олар жалпы сипатқа ие және әдетте ұйым басшылығынан шығады.

Екінші деңгейде ақпараттық қауіпсіздіктің жекелеген аспектілеріне қатысты, бірақ ұйым пайдаланатын әр түрлі жүйелер үшін маңызды мәселелер. Ақпараттық жүйенің нақты сервистері.

Үшінші деңгей екі аспектіден тұрады - мақсаттар (қауіпсіздік саясаты) және оларға қол жеткізу ережелері, сондықтан оны іске асыру мәселелерінен ажырату қиын. Екі жоғарғы деңгейден айырмашылығы, үшіншісі әлдеқайда егжей-тегжейлі болуы керек. Жеке сервистерде барлық ұйым шеңберінде бірыңғай түрде регламенттеуге болмайтын қасиеттер көп. Сонымен қатар, бұл қасиеттер қауіпсіздік режимін қамтамасыз ету үшін өте маңызды, бұл оларға қатысты шешімдер техникалық деңгейде емес, басқару деңгейінде қабылдануы тиіс.[1]

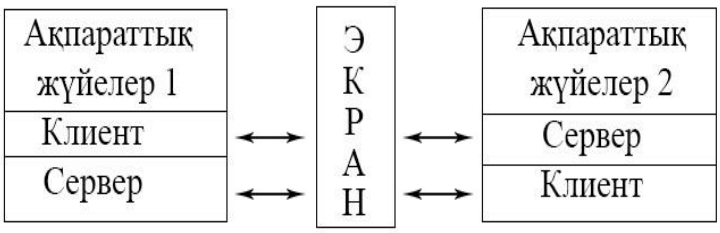
Қарастырылып отырған жағдайда төменгі екі деңгейде қалыптасатын қауіпсіздік саясаты маңызды. Оны нақты қарастыру үшін желіаралық экранның мәні мен негізгі функционалдық қасиеттерін - осы саясатты жүргізу құралын анықтау қажет.

Кәсіпорынның (ұйымның) ақпараттық жүйесінің құрылымын қарастырайық. Жалпы жағдайда ол әртүрлі операциялық жүйелермен басқарылатын әртүрлі компьютерлерден және компьютерлер арасындағы өзара әрекеттесуді жүзеге асыратын желілік құралдардан біртекті емес жиынтық (кешен) болып табылады. Осы жүйе әр түрлі болғандықтан (тіпті бір үлгідегі және бір ОС бар компьютерлер олардың мақсатына сәйкес мүлдем әр түрлі конфигурациялары болуы мүмкін), әрбір элементті жеке –жеке қорғауды қамтамасыз етуді жүзеге асырудың қажеті жоқ. Осыған байланысты жалпы жергілікті желі үшін ақпараттық қауіпсіздікті қамтамасыз ету мәселелерін қарастыру ұсынылады. Бұл желіаралық экранды (firewall) пайдалану кезінде мүмкін болады.

Желіаралық экрандау тұжырымдамасы былайша тұжырымдалады.

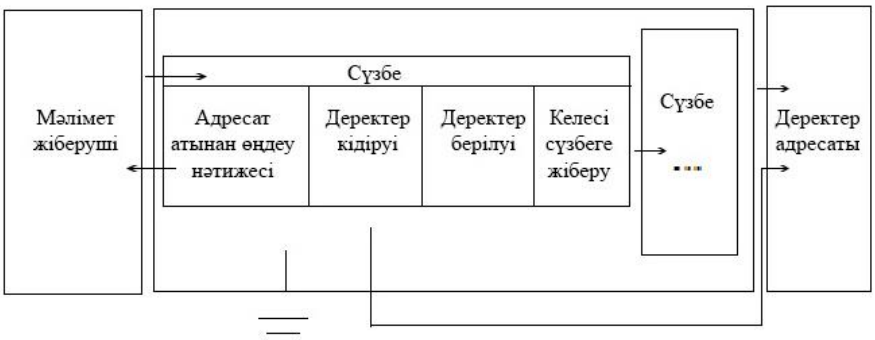
[1] Есептеуіш техника құралдары. Рұқсатсыз қол жеткізуден қорғау және ақпарат. Ақпаратқа рұқсатсыз қол жеткізуден қорғау көрсеткіштері. Басшылық құжат. Ресей Мемтехкомиссиясы. Мәскеу, әскери баспа, 1999.

Мәселен, ақпараттық жүйенің екі жиыны бар делік. Экран-бұл пайдаланушының бір жиыннан басқа жиындардан серверге кіруін шектейтін құрал. Экран екі жүйе арасындағы барлық ақпараттық ағындарды бақылай отырып, өз қызметін орындап отырады.



Сурет. 1.2 - Экран кіруді шектеу құралы ретінде.

Бұл жағдайда, экранда екі механизмнен тұрады, олардың біреуі деректерді жылжытуды шектейді, ал екіншісі керісінше оған ықпал етеді(яғни деректерді жылжытуды жүзеге асырады). Жалпы жағдайда экран (жартылай өткізбейтін қабық) сүзгілер тізбегі ретінде ыңғайлы. Олардың әрқайсысы деректерді кідіртуі (жіберіп алмауы) мүмкін, ал бірден "оларды" басқа жаққа "лақтыруы мүмкін". Бұдан басқа, талдауды жалғастыру үшін келесі сүзгішке деректер порциясын беруге немесе адресаттың атынан деректерді өңдеуге және нәтижені жіберушіге қайтаруға жол беріледі.



Сурет. 1.3 - Экран сүзгілер тізбегі ретінде.

Қол жетімділікті шектеу функцияларынан басқа, экрандар да ақпараттық алмасуларды хаттамалауды жүзеге асырады.

Әдетте экран симметриялы емес, ол үшін "ішкі" және "сыртқы"ұғымдары анықталған. Бұл ретте экрандау міндеті ішкі аймақты әлеуетті дұшпандық сыртқы қорғау ретінде тұжырымдалады. Мысалы, желіаралық экрандар Internet сияқты ашық ортаға шығатын ұйымның жергілікті желісін қорғау үшін орнатылады. Экранның басқа мысалы-барлық басқа жүйелік қорғаныс құралдарына дейін және

тәуелсіз компьютердің коммуникациялық портына кіруді бақылайтын портты қорғау құрылғысы. Экрандау сыртқы белсенділікпен индукцияланған жүктемені азайту немесе жалпы жою арқылы ішкі облыстың сервистеріне қолжетімділікті қолдауға мүмкіндік береді. Ішкі қауіпсіздік сервистерінің осалдығы азаяды, өйткені бастапқыда бөгде қаскүнем қорғаныш тетіктері әсіресе, мұқият және қатаң құрастырылған экранды еңсеруі тиіс. Сонымен қатар, экрандау жүйесі, әмбебап қарағанда, қарапайым демек, қауіпсіз түрде жасалуы мүмкін.

Экрандау сондай-ақ сыртқы аймаққа бағытталған ақпараттық ағындарды бақылап қана қоймай, бұл құпиялылық режимін сақтауға мүмкіндік береді.

Көбінесе экранды үшінші (желілік), төртінші (көліктік) немесе жетінші (қолданбалы) деңгейлерде OSI жеті деңгейлі эталондық моделінің желілік сервисі ретінде іске асырады. Бірінші жағдайда біз экрандаушы маршрутизатор, екінші жағдайда - экрандаушы көлік, үшінші жағдайда - экрандаушы шлюз бар. Әрбір тәсілдің өз артықшылықтары мен кемшіліктері бар; сондай-ақ аталған тәсілдердің үздік сапасын біріктіруге әрекет жасайтын гибридті экрандар да белгілі.

Экрандалған маршрутизатор жеке деректер пакеттерімен айналысады, сондықтан кейде оны пакеттік сүзгі деп атайды. Деректерді жіберіп немесе кідірту туралы шешімдер әрбір пакет үшін желілік және көлік деңгейлерінің тақырыптарының өрістерін талдау негізінде алдын ала берілген Ереже жүйесін қолдану жолымен қабылданады. Талданатын ақпараттың тағы бір маңызды компоненті-пакет маршрутизаторға келіп түскен порт.

Қазіргі заманғы маршрутизаторлар (Bay Networks немесе Cisco компанияларының өнімдері сияқты) әрбір портпен бірнеше ондаған ережелерді байланыстыруға және пакеттерді кіруде (маршрутизаторға түскен кезде) және шығуда сүзгілеуге мүмкіндік береді. Негізінде, пакеттік сүзгі ретінде бірнеше желілік карталармен жабдықталған әмбебап компьютер де қолданылуы мүмкін. Негізгі қадір-қасиетін экрандау маршрутизаторов - арзандығы (шекарадағы желілерін маршрутизатор қажет іс жүзінде әрқашан, тек оның іске қосу, оны экрандау мүмкіндігі) және ашықтығы үшін жоғары деңгейдегі OSI моделінің. Негізгі кемшілік - талданатын ақпараттың шектелуі және салдары ретінде. қамтамасыз етілген қорғаудың салыстырмалы әлсіздігі болып табылады.

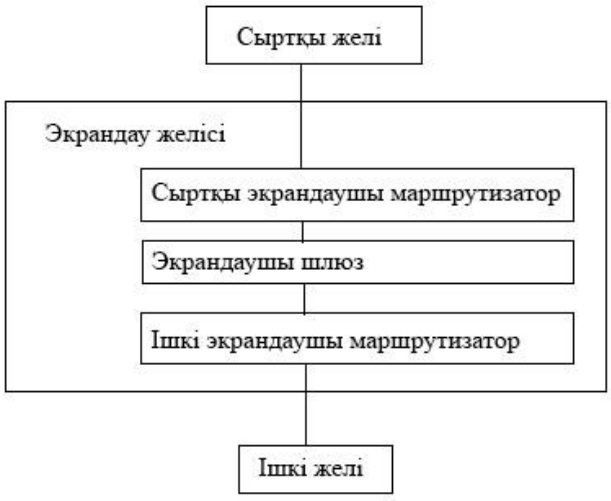
Экрандаушы көлік виртуалды қосылыстарды орнату процесін және олар бойынша ақпарат беруді бақылауға мүмкіндік береді. Іске асыру тұрғысынан экрандаушы көлік өте қарапайым, яғни сенімді бағдарлама болып табылады. Экрандау көлігінің үлгісі-TCP wrapper өнімі.

Пакеттік сүзгілермен салыстырғанда, экрандаушы көлік үлкен ақпаратқа ие, сондықтан ол виртуалды қосылыстарға неғұрлым жұқа бақылауды жүзеге асыра алады (мысалы, ол берілетін ақпараттың санын қадағалауға және белгілі бір шектен асып кеткен соң, ақпараттың рұқсатсыз экспортына кедергі жасай отырып, қосылыстарды бұзуға қабілетті). Осыған ұқсас, неғұрлым мазмұнды тіркеу ақпараты жинақталуы мүмкін. Басты кемшілік-қолдану аймағының тарылуы,

өйткені бақылаудан тыс датаграммдық хаттамалар қалады. Әдетте, экрандаушы шлюз әмбебап компьютер болып табылады, онда бағдарламалық агенттер бір-бірден әрбір қызмет көрсетілетін қолданбалы хаттама үшін жұмыс жасайды. Мұндай тәсілде сүзуден басқа экрандаудың тағы бір маңызды аспектісі іске асырылады. Сыртқы желі субъектілері тек шлюздік компьютерді ғана көреді; тиісінше оларға шлюз экспорттауды қажет деп санайтын ішкі желі туралы ақпарат ғана қол жетімді. Шлюз шын мәнінде сыртқы әлемнің ішкі желісін қорғайды. Сонымен қатар, ішкі желі субъектілеріне олар сыртқы әлем объектілерімен тікелей қарым-қатынас жасайды. Экрандаушы шлюздердің жетіспеушілігі - әрбір қолданбалы хаттаманы қолдау үшін арнайы іс-әрекеттерді талап ететін толық ашықтықтың болмауы.

Экрандық шлюздерді құру үшін құралдардың мысалы Trusted Information Systems компаниясының TIS Firewall Toolkit болып табылады.Sun Microsystems компаниясының Firewall-1 сияқты гибридті жүйелерде экрандық жүйелердің ең жақсы сапасын біріктіре алады, яғни сенімді қорғаныс алу, қосымшалар үшін мөлдірлікті сақтау және үстеме шығындарды ақылға қонымды шектерде ұстап тұру. Сонымен қатар, датаграммдық хаттамалар шеңберінде ақпарат беруді қадағалау сияқты өте құнды жаңа мүмкіндіктер де пайда болады.

Экрандаудың маңызды түсінігі экранды немесе оның қандай да бір компоненттерін еңсергеннен кейін қаскүнемге қол жетімді болатын көптеген жүйелер ретінде анықталатын тәуекел аймағы болып табылады. Әдетте, қорғаныс сенімділігін арттыру үшін экран элементтер жиынтығы ретінде іске асырылады, өйткені олардың бірінің "бұзу" барлық ішкі желіге қатынауды ашпайды. Көп компонентті экранның ықтимал конфигурациясының мысалы,мына 1.4.суретте көрсетілген.



Сурет. 1.4 - Көп компонентті экран.

Желіаралық экрандауды жүзеге асыратын нақты жүйеге қойылатын талаптарды қарастырайық.

Көп жағдайларда экрандау жүйесі:

Ішкі (қорғалатын) желінің қауіпсіздігін және сыртқы байланыстар мен байланыс сеанстарын толық бақылауды қамтамасыз етуі тиіс;

Ұйымның қауіпсіздік саясатын толық және мүмкіндігінше қарапайым іске асыру үшін қуатты және икемді басқару құралдарына ие болу. Бұдан басқа, экрандау жүйесі желі құрылымы өзгерген кезде жүйенің қарапайым қайта жаңартылуын қамтамасыз етуі тиіс;

Тиімді жұмыс істеу және барлық кіріс және шығыс трафиктерді "ең жоғары" режимдерде өңдеуге үлгеру. Бұл firewall жұмысты бұзуға әкелетін көптеген шақыруларды "лақтыруға" болмайды;

Кез келген рұқсатсыз әсерлерден өзін-өзі қорғау қасиеттеріне ие болу, өйткені желіаралық экран ұйымдағы құпия ақпараттың кілті болып табылады;

Егер ұйымда бірнеше сыртқы қосулар бар болса, оның ішінде алыс филиалдарда да экрандарды басқару жүйесі олар үшін бірыңғай қауіпсіздік саясатын жүргізуді орталықтандырып қамтамасыз етуге мүмкіндігі болуы тиіс;

Сыртқы қосылыстар арқылы пайдаланушылардың қол жетімділігін авторландыру құралдары болуы тиіс. Ұйым қызметкерлерінің бір бөлігі, мысалы, іссапарларға шығуы тиіс және жұмыс процесінде оларға кем дегенде, ұйымның ішкі компьютерлік желісінің кейбір ресурстарына қол жеткізу талап етілетін жағдай типтік болып табылады. Жүйе осындай пайдаланушыларды сенімді түрде тануы және оларға қол жеткізудің қажетті түрлерін ұсынуы тиіс.

Экрандау сыртқы белсенділікпен бастамашылық еткен жүктемені азайту немесе жалпы жою арқылы ақпараттық жүйенің ішінде сервистерге қол жетімділікті қолдауға мүмкіндік береді. Ішкі қауіпсіздік сервистерінің осалдығы азаяды, өйткені алғашында зиянкестер қорғаныс тетіктері әсіресе мұқият және қатаң құрастырылған экранды еңсеруі тиіс. Сонымен қатар, экрандау жүйесі, әмбебап қарағанда, қарапайым және, демек, неғұрлым сенімді түрде жасалуы мүмкін. Экрандау құпиялылық режимін қамтамасыз ете отырып, сыртқы облысқа бағытталған ақпараттық ағындарды бақылауға мүмкіндік береді.

Осылайша, экрандау басқа қауіпсіздік шараларымен бірге көп деңгейлі қорғаныс идеясын пайдаланады. Осының есебінен ішкі желі бірнеше, әртүрлі ұйымдастырылған қорғаныс шептерін еңсерген жағдайда ғана тәуекелге ұшырайды.

Желіаралық экрандау құралының болуы оны және байланыстың коммутацияланатын арналары бойынша ұйымның ақпараттық ресурстарына қолжетімділікті бақылау үшін пайдалануға мүмкіндік береді. Ол үшін терминал сервері деп аталатын құрылғыны пайдалану қажет. Терминалдық сервер келесі бөлімде қарастырылған бағдарламалық-аппараттық конфигурацияны білдіреді. Коммутацияланатын байланыс арналарымен жұмыс істеу құралы ретінде "Bay Networks" компаниясының "Annex"терминалдық сервері ұсынылады.

Экранды желісі бар желіаралық экран конфигурациясы бүгінгі күні ең сенімді болып табылады. Мұның себебі кем дегенде үш қорғау деңгейінің болуы:

Сыртқы экрандау маршрутизаторы;

Экрандау шлюзі;

Ішкі экрандау маршрутизаторы.

Осы жүйелердің әрқайсысының әлсіз орындары әр түрлі. Экрандау желісі сондай-ақ коммутацияланатын байланыс арналарын қауіпсіздікті қамтамасыз етудің жалпы контурына оңай қосуға мүмкіндік береді. Ұсынылған шешім жағдайында экрандау шлюзінің жұмыс тиімділігі, оның экран арқылы өтетін ақпаратты тиімді өңдеу қабілеті сыни болады. Бұл, өз кезегінде, жүйе өнімділігінің аз шығыны бар бағдарламалық қамтамасыз етуді экрандаушы компьютер-шлюзге орнатуды талап етеді, ол өзі кіріктірілген ОЖ құралдарымен жеткілікті сенімді қорғалған - мысалы, Firewall-1 желіаралық экрандау бағдарламасы бар Solaris ОЖ басқаруындағы SUN фирмасының компьютері.

Желілік пакеттерді сүзу деңгейінде де, қосымшалар деңгейінде де жұмыспен қамтамасыз етілетін жоғары сенімділік;

Бірнеше сүзгіш модульдердің жұмысын орталықтандырылған басқару;

Стандартты және белгілі бір пайдаланушымен кез келген желілік сервиспен жұмыс істеу мүмкіндігі;

Жоғары жұмыс тиімділігі: Firewall-1 пайдалану ақпараттық арнаның өткізу қабілетін 10% артық емес азайтады;

Пайдаланушыларға арналған сервистер мен қосымшалар жұмысының толық ашықтығы;

Көптеген сервистер үшін қосымша аутентификация;

Қауіпсіздік саясаты терминдерінде сипаттай отырып, сүзу ережелерін оңай қайта құруға мүмкіндік беретін достық интерфейсі;

Әрбір ереже (қол жеткізу саясаты) үшін хаттамалау, әкімшіге хабарлау немесе жүйенің өзге реакциясы шарттары айқындалуы мүмкін;

Сүзгінің ішкі қарама-қайшы еместігіне жұмыс істеу ережелерін тексеру құралдары;

Оған шабуыл жасау әрекетін уақтылы анықтауға мүмкіндік беретін жүйе компонентінің жай-күйін мониторингілеу құралдары;

Есептерді егжей-тегжейлі хаттамалау және генерациялау құралдары;

Жергілікті желі компьютерлерін қосымша қорғауды, сондай-ақ IP-адрестердің ресми жиынтығын тиімді пайдалануды іске асыруға мүмкіндік беретін жергілікті желі адрестерін трансляциялау;

Орнату және басқару оңай.

Алыстағы пайдаланушыларды аутентификациялаудың ең көп таралған құралдарының бірі Bellcore компаниясының S/key бағдарламасы болып табылады. Бұл бағдарлама бір реттік парольдермен алмасу құралы болып табылады, бұл жүйеге рұқсатсыз кіруге мүмкіндік бермейді, тіпті бұл ақпарат біреу ұстап қалған

болса да. S/key бағдарламасы Firewall-1 жүйесін аутентификациялау құралдарымен үйлесімді.

Желіаралық экрандарды конфигурациялау кезінде негізгі конструктивтік шешімдер ұйымда қабылданған қауіпсіздік саясатымен алдын ала белгіленеді. Сипатталған жағдайда қауіпсіздік саясатының екі аспектісін қарастыру қажет: желілік сервистерге қол жеткізу саясаты және желіаралық экран саясаты.

Желілік сервистерге қол жеткізу саясатын қалыптастыру кезінде ұйымда пайдаланылатын әртүрлі сервистерге пайдаланушылардың қол жеткізу ережелері қалыптастырылуы тиіс. Бұл аспект екі компоненттен тұрады.

Пайдаланушыларға арналған ережелер базасы қандай пайдаланушы (пайдаланушылар тобы) қандай сервисті және қандай компьютерде пайдалана алатынын сипаттайды. Ұйымның жергілікті желісінен тыс пайдаланушылардың жұмыс шарттары олардың аутентификация шарттары сияқты жеке анықталады.

Сервистерге арналған ережелер базасы желілік экран арқылы өтетін сервистер жиынтығын, сондай-ақ әрбір сервис (сервис топтары) үшін серверлер клиенттерінің рұқсат етілген мекенжайын сипаттайды.

Желіаралық экранның жұмысын регламенттейтін саясатта шешімдер пайдалану жеңілдігіне нұқсан келтіретін қауіпсіздік пайдасына де, керісінше да қабылдануы мүмкін. Мынадай екі негізгі бар:

«Барлығы, бұған жол берілмейді, яғни тыйым салынған.

Егер тыйым салынбаса, бәріне рұқсат етіледі ».

Бірінші жағдайда желіаралық экран барлығын бұғаттайтындай етіп конфигурациялануы тиіс, ал оның жұмысы қауіптілік пен тәуекелді мұқият талдау негізінде реттелуі тиіс. Бұл пайдаланушыларға тікелей әсер етеді және олар жалпы айтқанда, экранды бөгеуіл ретінде қарастыра алады. Мұндай жағдай экрандау жүйелерінің өнімділігіне жоғары талаптар қоюға мәжбүр етеді және пайдаланушылар тұрғысынан желіаралық экран жұмысының "мөлдірлігі" сияқты қасиеттің өзектілігін арттырады. Бірінші тәсіл неғұрлым қауіпсіз болып табылады, өйткені әкімші қандай сервистер немесе порттар қауіпсіз екенін және бағдарламалық қамтамасыз етуді әзірлеушінің ядросында немесе қосымшасында қандай "тесіктер" болуы мүмкін екенін білмейді. Бағдарламалық қамтамасыз етудің көптеген өндірушілері ақпараттық қауіпсіздік үшін маңызды анықталған кемшіліктерді жариялауға асықпайды (бұл "жабық" бағдарламалық қамтамасыз етудің өндірушілеріне тән, олардың ең ірісі Microsoft болып табылады), бұл тәсіл, сөзсіз, неғұрлым консервативті болып табылады. Шын мәнінде, ол білмеу зиян келтіруі мүмкін фактіні мойындау болып табылады.

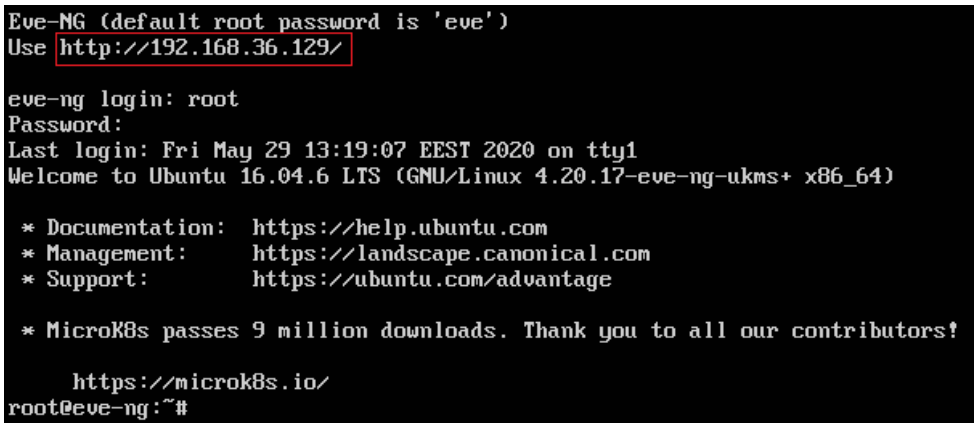
Екінші жағдайда жүйелік әкімші әрекет ету режимінде жұмыс істейді, қауіпсіздікке теріс әсер ететін қандай іс-әрекеттерді пайдаланушылар не тәртіп бұзушылар жасай алады және осындай іс-әрекеттерге қарсы қорғауды дайындайды. Бұл өте қызықты болуы мүмкін шексіз "қару-жарақ жарыстарында" пайдаланушыларға қарсы firewall әкімшісін айтарлықтай қалпына келтіреді. Егер

қауіпсіздікті қамтамасыз етуге бағытталған шаралардың қажеттілігіне сенімді болмаса, пайдаланушы ақпараттық жүйенің қауіпсіздігін бұзуы мүмкін.

2. Техникалық бөлім

2.1 Ұжымдық желіні модельдеу процесі.

Eve-ng бағдарламасын іске қосу үшін виртуалды машинаны құру қажет. Виртуалды машинаны құру барысында VMware Workstation 15 бағдарламасы қолданылған болатын. Бұл бағдарламалық қамтама компьютерге бір немесе одан көп виртуалды машиналарды орнатуға мүмкіндік береді. Eve-ng бағдарламасының орнатылуы құрылған виртуалды машинада бастапқы файлдарды орнатылумен жүзеге асады. Орнатылғаннан кейін Eve-ng жұмыс жасауға дайын, кіру үшін берілген Ip-адресті қолданамыз.

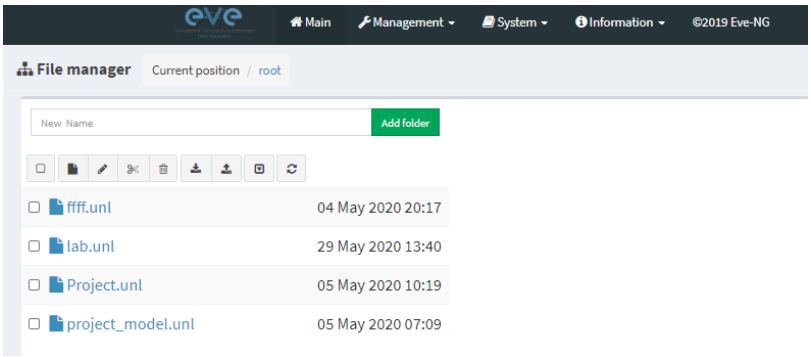


Сурет 2.1 – ip адресс

Eve-ng модельдеу процесі веб-браузер арқылы кіруге болатын графикалық интерфейс түрінде болады.

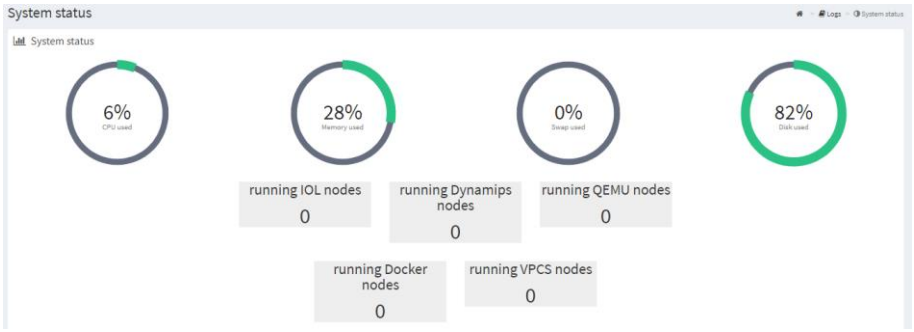
Сурет 2.2 – Кіру интерфейсі

Сәтті аутентификациядан кейін қолданушы келесі мәзірге көшеді. Басқару панелі арқылы қолданушы жобаларды басқаруына мүмкіндік алады(жою, көшіру, қиып алу, жасау).



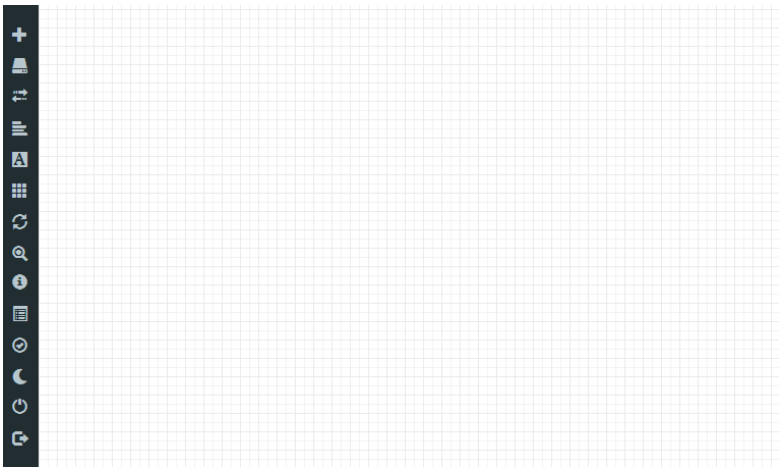
Сурет 2.3 – Басқару интерфейсі

Status мәзірі қазіргі уақытта бағдарламаның қолданылып отырған ресурстарының тізімін көруге мүмкіндік береді.



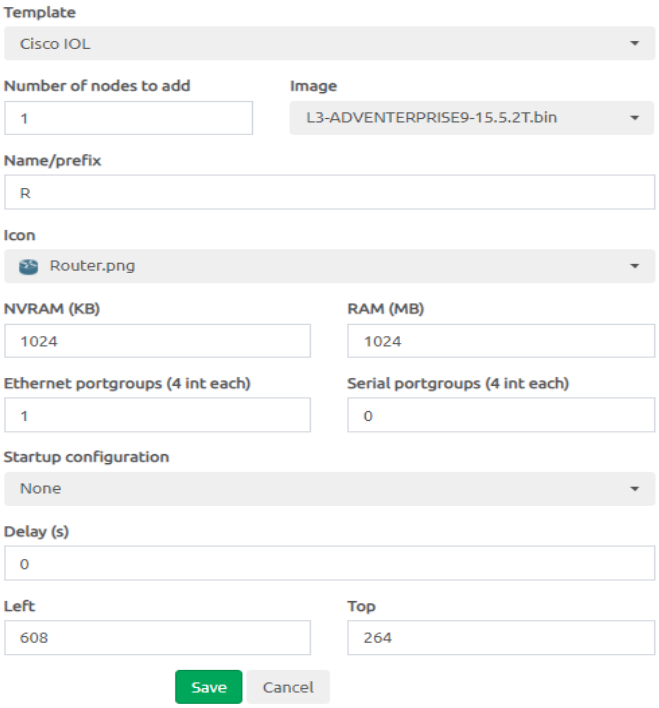
Сурет 2.4 – Қолданылған ресурстар туралы ақпарат

Жаңа жоба даярлай отырып қолданушы жұмыс терезесіне түседі.



Сурет 2.5 – Жұмыс терезесі

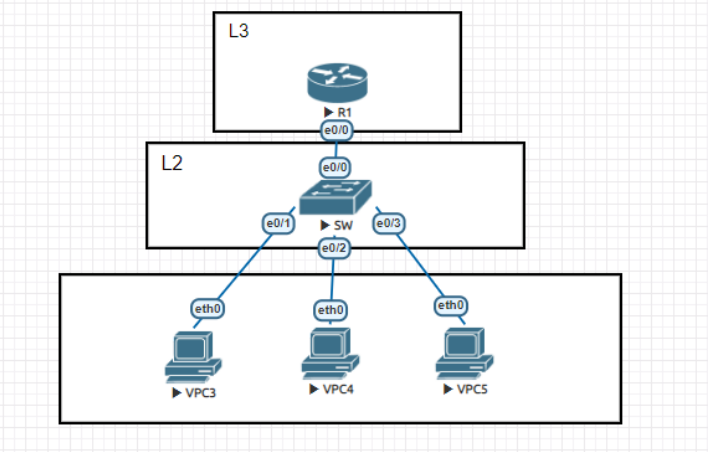
Add an object батырмасы қолданушыға желі құрылғыларының әртүрлі өнімдерін пайдалануға мүмкіндік береді. Белгілі құрылғыны таңдағаннан кейін сипаттама беруге мүмкіндік ашылады: ат қою, жедел жады мөлшері және т.б. Бағдарлама қолданушыға берілген желі құрылғысын өздігінен баптауына мүмкіндік береді. Cisco компаниясының құрылғылары мысалында, пайдаланушы құрылғының бағдарламалық қабығын (Cisco IOS) эмуляциялайтын желілік құрылғының бейнесін таңдайды және параметрлерді орнату арқылы болашақ физикалық құрылғыны баптайды. Осылайша, өлшемдер өзгере отырып, пайдаланушы әр түрлі, нақты құрылғылардың жұмысын еліктей алады.



Сурет 2.6 – Желі құрылғысын баптау

Құрылғы сипаттамалары берілгеннен кейін жұмыс терезесінде пайда болады. Осылайша қолданушы жаңа құрылғаларды қосу арқылы болашақ желі архитектурасын құрады.

Құрылғыларды өзара жалғау үшін Connect node батырмасын басып, керекті құрылғыларды таңдау керек.



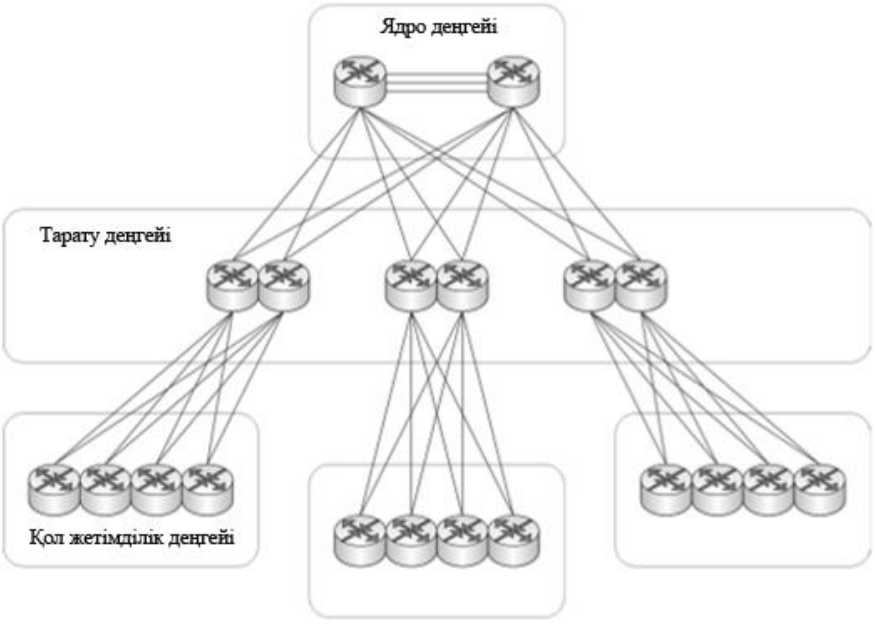
Сурет 2.7 – Есептеу желісінің моделін құру

2.2 Есептеу желісі архитектурасына талдау

Есептеу желілерінің архитектурасындағы басты принциптердің бірі-модульдік принцип. Модульдік принцип есептеуіш желінің барлық архитектурасын жеке модульдерге бөлуге болатынын білдіреді, өз кезегінде, әрбір модульдің атқаратын қызметіне жеке көңіл бөлуге мүмкіндік береді, бұл ретте мұндай тәсіл оны жүзеге асыру мен басқаруды жеңілдетеді.

Ірі желіні кіші модульдерге бөлу, ең алдымен, желінің тұрақтылығына ықпал етеді, өйткені желіде ақаулар немесе сәтсіздіктер туындаса, сіз бар мәселені реттей аласыз. Дегенмен, тұрақты жұмыс жасайтын басқа желілік модульдерге әсер етпейді. Желінің модульділігінің тағы бір артықшылығы - компьютерлік желіні кеңейту қажеттілігі туындаған кезде қосымша модульдерді енгізу арқылы қол жетімді жеңілдетілген және ауыртпалықсыз масштабтау мүмкіндігі бар.

Есептеу желі архитектурасында желінің иерархиялық моделі қолданылады. Осы модельге орай есептеуіш желі үш иерархиялық деңгейге бөлінеді. Әр қайсысы өз міндетін атқарады оларға: қолжетімділік деңгейі, тарату деңгейі және желі ядросының деңгейі жатады.



Сурет 2.8 – Үш деңгейлі есептеуіш желі деңгейі

Қол жетімділік деңгейінде пайдаланушыларға немесе құрылғыларға (сканер, принтер, ip телефондар және т.б.) қол жетімділік ұсынылады. Бұл деңгейдің басты міндеті – біріктірілген желіге кіру нүктелерін құру. Қолжетімділік деңгейі желіде OSI моделі желілерінің екінші деңгейдегі коммутаторларын(L2) ұсынады.

Келесі - тарату деңгейі, оның негізгі міндеті кіру деңгейлерін жинақтау және маршруттау мәселерін шешу болып табылады. Бұл деңгейде үшінші деңгейдегі құрылғылар – бұл әртүрлі желілік сегменттер арасындағы әртүрлі трафикті бағыттайтын L3-коммутаторлар(маршрутизаторлар). Сондай-ақ тарату деңгейінде сүзгілеу және ғаламдық желілердің функцияларына қол жеткізу жүзеге асырылады. Коммутаторларды бір желіге біріктіру байланыстарды азайтуға мүмкіндік береді.

Ядро деңгейі – бірнеше кеңселер мен ғимараттарды біріктіретін үлкен желілерде қолданылады. Бұл деңгей үлкен көлемдегі трафиктің жылдам және уақытылы берілінуіне жауап береді. Сонымен қатар, ядролық деңгей тарату деңгейлерін біріктіретінін атап кеткен жөн, сондықтан осы деңгейдің ақаулыққа төзімділігі маңызды. Ядро деңгейіндегі қате барлық желі пайдаланушыларына әсер етеді. Желінің өзегі – қуатты қосқыштар мен маршрутизаторлар жиынтығы.

Есептеу желісін жобалау барысында иерархиялық құрылыммен қатар келесі негізгі қағидаларды басшылыққа алу қажет:

- желі мультисервистік қызметке ие болу керек, ол трафиктің барлық түрлерін жеке арналар арқылы беруді қамтиды.

- желіні кеңейту және оны басқа желілермен біріктіру мүмкіндігін қамтамасыз ету үшін компьютерлік желіні ашық стандарттар мен интерфейстер негізінде құру қажет.

Компьютерлік желіні құруға және пайдалануға байланысты барлық шығындарды азайту принципі. Бұл принцип экономикалық тұрғыдан алғанда, байланыс арналарын тиімді пайдалануға мүмкіндік беретін пакеттік коммутацияны қолданатын желі болады.

Аталған есептеу желінің модульділігі әртүрлі функциялар үшін жеке модульдер құруды қарастырады. Есептеу желінің негізгі модульдеріне интернет модулі, аумақтық желілік модуль және серверлік модуль және серверлік модуль кіреді.

2.3 Құрылған есептеуіш желінің сипаттамасы

Eve-ng виртуалды жобалау бағдарламасының негізінде күрделі есептеу желілерінің бірнеше модельдері жасалды. Әзірленген компьютерлік желілер Cisco желілік жабдықтарын қолдануға негіздерген, ол желілік жабдықтар нарығында үздік болып табылады және шағын кеңседен ірі құрылымдарға дейін компьютерлік желілерді құруға арналған құрылғыларды ұсынады.

Барлық жұмыс бірнеше кезеңдерге бөлінеді, олардың әрқайсының компанияның дамуын және жаңа міндеттерді шешетін есептеу желісі жасалады.

Бірінші деңгейде шағын деңгейдегі кәсіпорындар үшін бастапқы деңгейдегі компьютерлік желілердің модельдері жасалады. Мұндай кәсіпорынның кеңселері бір немесе бірнеше көршілес ғимараттарда орналасуы мүмкін. Компьютерлік

желінің бұл моделі кәсіпорындағы жұмыс станцияларын желімен біріктірудің сызбасын көрсетеді, олардың арасындағы өзара әрекеттесу мүмкіндігін қамтамасыз етеді, сонымен қатар осы қосылулардың әртүрлі нұсқаларын көрсетеді.

Кәсіпорындардың жұмыс станцияларын бір ғимаратта орналасқан (әр түрлі қабаттарда) бір желіге біріктірудің екі жолын да, сонымен қатар бір-біріне жақын орналасқан әр түрлі ғимараттарда орналасқан жұмыс станцияларын желіде біріктіру мүмкіндігі қарастырылады.

Келесі кезеңде кәсіпорынның дамуын көрсететін компьютерлік желілердің моделі жасалады. Әзірлеу мысалында желіге қосылған жұмыс станциялары санының ұлғаюы көрсетіледі, сонымен қатар олар алдыңғы модельде көрсетілген жұмыс станцияларын желіге қосудың түрлі әдістерін қосқанда әртүрлі қондырғыларға бөлінеді. Сонымен қатар, кәсіпорынның барлық жұмыс станциялары үшін интернетке қол жетімділік қамтамасыз етіледі. Интернетке қол жеткізу үшін кәсіпорын «ақ» IP-мекен-жайын және провайдерден тек біреуін жалдай алатындай жағдай жасалады. Кәсіпорынның барлық жұмыс станциялары үшін ғаламдық желіге қол жеткізу тек арнайы IP-адрес провайдері арқылы жүзеге асырылады, бұл кәсіпорынның қаржылық шығындарын айтарлықтай төмендетеді. Ғаламдық желіге қосылудың бұл тәсілі де жақсы, өйткені ол компьютерлік желіні ұйымдастырудың ішкі құрылымын бөтен адамдардан жасырады.

Соңғы кезеңде кәсіпорынның өсуін және географиялық тұрғыдан алыс филиалдарға бөлінуін көрсететін компьютерлік желінің модельдері жасалады. Филиалдарды біріктіруге арналған туннелін құрудың әртүрлі нұсқалары қарастырылады. Егер филиалдар арасында желілік өзара әрекеттесу қажет болса, барлық ақпараттық трафик осы туннель арқылы өтеді. Филиалдар арасындағы ақпаратты беру компьютерлік желінің ішкі құрылымынан тыс жүретіндіктен, бұл ақпаратты рұқсатсыз кіруден қорғау керек. Сондықтан, туннелде «оралған» барлық таралып жатқан трафикті шифрлауды баптау қажет.

Кәсіпорынның өсуімен оның логикалық дамуы серверлік жабдықтың пайда болуы болып табылады. Бұл файл, пошта немесе веб-сервер болсын. Құрылған модельде ұйымның сервері рұқсат етілмеген пайдаланушылардан жасырылған, компьютерлік желінің ішкі құрылымында орналасқан ашық қол жетімді болатын жағдай қарастырылады. Кез-келген пайдаланушы, тіпті кәсіпорынның желісінен тыс жерде, кәсіпорынның серверіне кіре алады.

Сондай-ақ, модель кәсіпорынның филиалдар желісінің қателіктеріне төзімділік мәселесін қарастырады. Серверлік жабдық орналасқан компьютерлік желінің топологиясы егер қосылыстың физикалық тұтастығының бұзылуы (тарату ортасындағы, кабельдегі үзіліс) орын алса, бүкіл желі тоқтамайтындай етіп жасалады. Компьютерлік желінің моделі, ақаулық анықталған кезде, оның функционалдығы бұзылмайтын етіп автоматты түрде қалпына келтіріледі, осылайша кәсіпорынның жұмысын үзбейді.

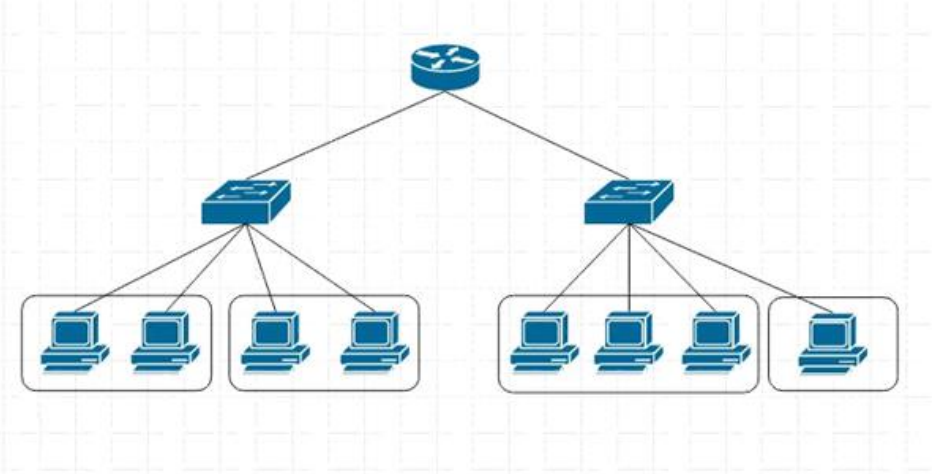
2.4 Есептеу желісінің ұғымын құру

Eve-ng компьютерлік желілердің модельдерін әзірлемес бұрын, алдымен болашақ модельдер тұжырымдамасын жасау керек.

Әзірленген тұжырымдамада компьютерлік желілердің болашақ топологиясы көрініс табады. Осылайша, болашақ есептеу желісінің барлық түйіндері жобаланатын болады. Сегменттер ішкі желілерге бөлініп, олар үшін мекенжайлар бөлініп, құрылғылар арасындағы барлық қосылыстар жобаланатын болады.

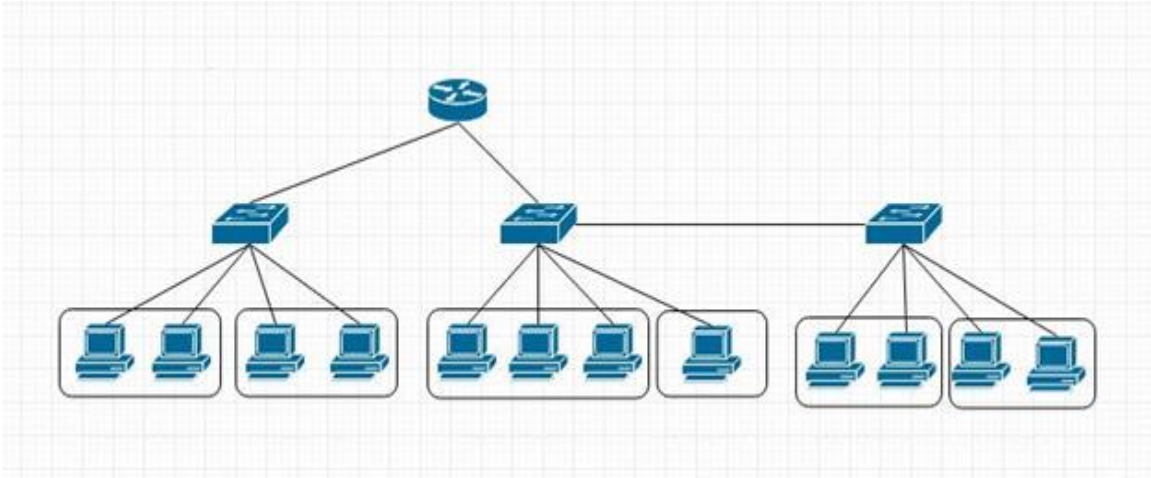
Мұндай тұжырымдаманың дамуы болашақ желілердің барлық мәселерін ескеруге, сонымен қатар эмулятордағы желіні модельдеу сатысында қателіктерге жол бермеуге мүмкіндік береді.

2.9-суретте көрсетілген бірінші тұжырымдамада қарапайым компьютерлік желі пайда болады, оның негізгі мақсаты кәсіпорынның компьютерлерін бір желіге біріктіру және олардың арасындағы желілік өзара әрекеттесу мүмкіндігін құру болып табылады. Бұл желі компьютерлер тобын әр түрлі жергілікті желілерге бөлуге арналған бірнеше қосқыштардан тұрады, бөлу кез-келген қағидаға сәйкес болуы мүмкін (мысалы, компанияның белгілі бір бөлімшесіне арналған компьютерлерге қатысты) және әр түрлі орналасқан компаниялардың жұмыс станциялары арасында желілік байланысты қамтамасыз ететін роутер. жергілікті желілер. Осылайша құрылған компьютерлік желі бір локальды желіде орналасқан компьютерлерді әр түрлі алып тастауды қамтуы мүмкін. Мысалы, бір ғимараттың әртүрлі қабаттарында. Осылайша, компьютерлерді ішкі желіде логикалық түрде біріктіруге болады, бұл болашақта мұндай желіні басқаруды айтарлықтай жеңілдетеді және оны логикалық құрылымдайды.



Сурет 2.9 - Қарапайым есептеу желісін көрсететін тұжырымдама

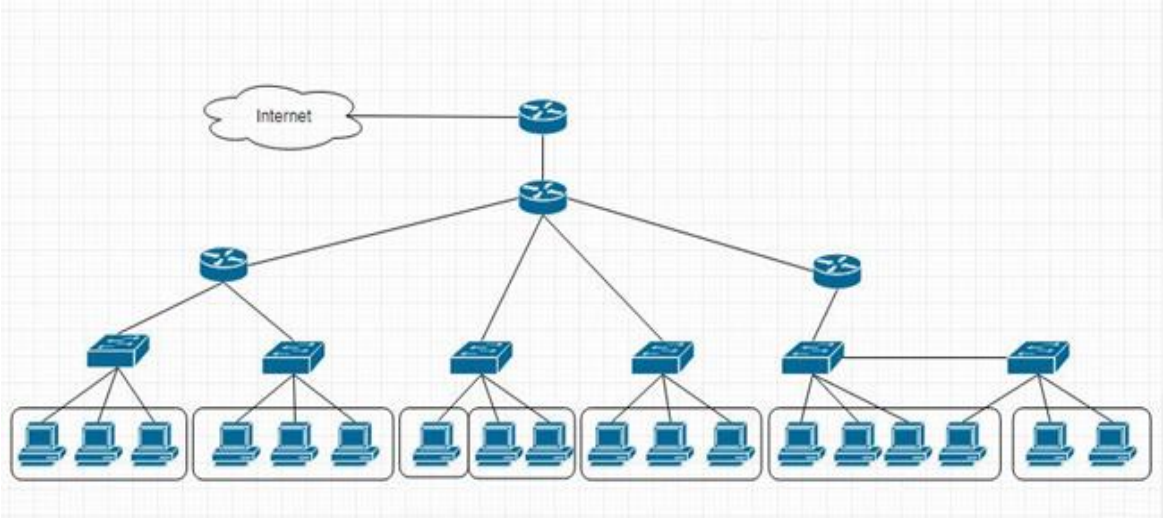
Келесі 2.10-суретте көрсетілген тұжырымдама алдыңғы тұжырымдаманың логикалық жалғасы болып табылады. Бұл компьютерлерді бірыңғай локальды желіде логикалық түрде біріктіру, бірақ түрлі қосқыштарға физикалық тұрғыдан жалғанған жағдайды көрсетеді. Бұл жағдайда логикалық түрде төртінші жергілікті желіде орналасқан, бірақ әртүрлі қосқыштарға физикалық түрде қосылған компьютерлер маршрутизаторды ескерусіз де желілік өзара әрекеттесуге мүмкіндік алады. Алайда, бірінші жергілікті желіде орналасқан компьютерлермен жағдай керісінше, тек қана маршрутизатормен өзара әрекеттесу мүмкін.



Сурет 2.10 - Тұжырымдаманың логикалық жалғасы

Әрі қарай, 2.11-суретте көрсетілген кәсіпорынның өсуін көрсететін есептеу желісінің тұжырымдамасын жобалаймыз. Жұмыс станцияларының саны да, есептеу желісін құру үшін желілік құрылғылардың саны да артады.

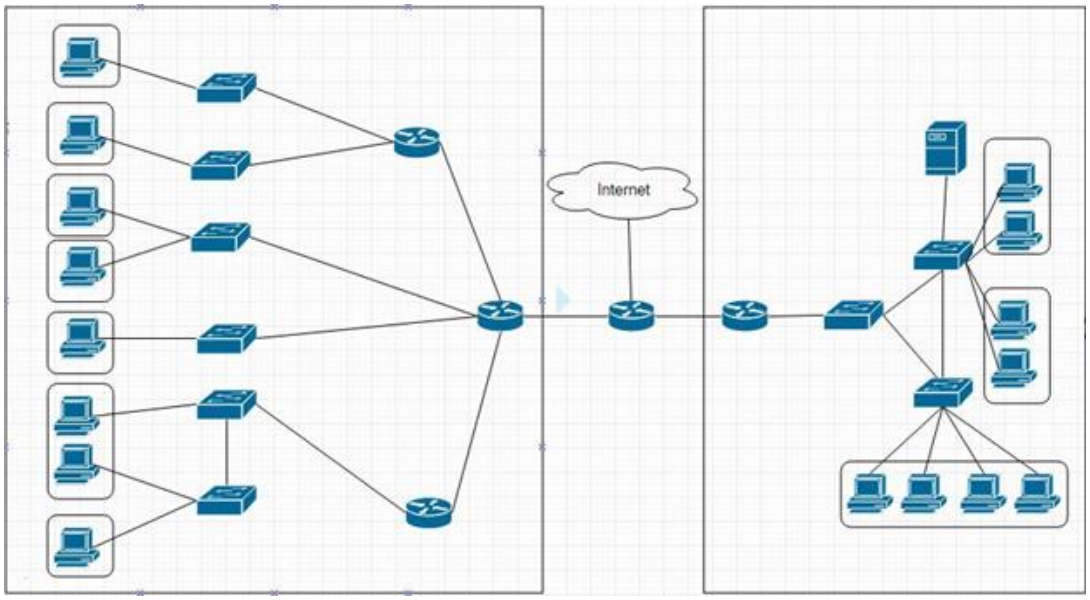
Бұл тұжырымдама алдыңғы тұжырымдамалардан жұмыс станцияларын қосудың екі әдісін де қамтиды. Сондай-ақ, тұжырымдамада компьютерлерді жергілікті желілерге кәсіпорындағы бөлімшелерге қатысты логикалық бөлу көрсетілген. Мысалы, жергілікті кеңсе желісі әртүрлі қосқыштарға физикалық түрде қосылған компьютерлерден тұрады. Сондай – ақ, тұжырымдамада "ақ" IP-мекенжайдың провайдері көрініс бере бастады. Яғни, кәсіпорынның барлық жұмыс станциялары үшін жаһандық желіге қатынау провайдер бөлген бір ғана IP-мекен-жай арқылы қол жеткізуге болады. Бұл өз кезегінде тек бір IP-мекенжайды жалға алған кезде кәсіпорынның қаржылық ресурстарын үнемдеуге әкеледі.



Сурет 2.11 - Дамушы кәсіпорынның компьютерлік желісі туралы түсінік

2.12-суретте көрсетілген келесі тұжырымдама аумақтық салаларға бөлуді көрсетеді. Бұл іс компанияның географиялық жағынан алыстағы филиалы болған кезде қарастырылады және әр түрлі филиалдардың объектілері арасында желілік өзара әрекеттесу мүмкіндігі үшін ортақ компьютерлік желі құру қажеттілігі туындайды. Әрбір филиалда осы IP арасында провайдердің арнайы IP мекенжайы бойынша Интернетке қол жетімді мекен-жайлар филиалдар арасында барлық ақпарат болатын арнайы туннель жасайды.

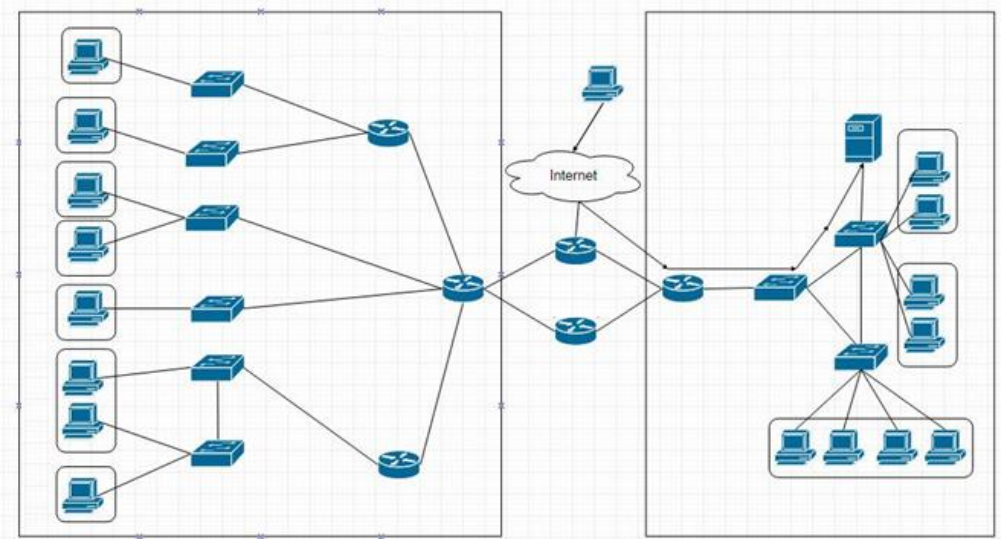
Тұжырымдамада кәсіпорынның жаңа нысаны-сервері пайда болды. Кез келген кәсіпорын үшін серверлік жабдық оның инфрақұрылымындағы маңызды нысан болып табылады. Бұл жабдықтың құны ғана емес, сонымен қатар онда сақталатын ақпараттың көлемі мен маңыздылығына да қол жеткізіледі. Мұндай жабдықтың істен шығуы бүкіл кәсіпорынның жұмыс істеуін толық тоқтатуға алып келуі мүмкін, сондықтан оған тоқтауға тұрақты қол жеткізуді қамтамасыз ету өте маңызды мақсат болып табылады. Бұл үшін филиалдар желісінің топологиясы коммутациялық құрылғылар арасындағы қосылыстардың біреуінің физикалық үзілуі орын алған кезде, сервермен байланыс бұзылмайды, осылайша кәсіпорынның жұмысына кедергі жасамайтын етіп құрылды.



Сурет 2.12 - Географиялық тұрғыдан алыс филиалдарға бөлінген компьютерлік желі туралы түсінік

2.13-суретте көрсетілген соңғы тұжырымдамада кәсіпорын филиалдары арасында байланыс туннелін салудың тағы бір нұсқасы қарастырылады. Бұл опция әрбір филиал провайдерлерден кем дегенде екі "ақ" IP мекен-жайды жалдауды білдіреді. Әрбір жұп IP- мекен-жай арқылы бір негізгі және бір резервтік есептік туннель жүргізіледі.

Негізгі провайдер арасында екі жағынан байланыс үзілген жағдайда, желілік топология автоматты түрде қалпына келтіріліп, резервтік провайдер арқылы екінші байланыс туннелі іске. Осылайша, филиалдар арасындағы байланыстың бұзылуына төзімділікке қол жеткізіледі, бұл өз кезегінде бүкіл кәсіпорынның жұмысы істеу сенімділігіне әкеледі. Сонымен қатар, тұжырымдамада кәсіпорынның компьютерлік желісінің ішкі құрылымынан тыс орналасқан интернет желісінен пайдаланушылардың кәсіпорын серверіне қол жеткізу мүмкіндігі көрсетілген. Яғни, серверге қол жеткізу ашық болады және кәсіпорынға тиесілігіне қарамастан кез- келген қолданушыға қол жетімді болады.



Сурет 2.13 - Аумақтық тұрғыдан шалғайдағы филиалдарға бөлініп, қателіктерге төзімді компьютерлік желісінің тұжырымдамасы

Осылайша компьютерлік желілердің болашақ модельдер туралы тұжырымдамасы қалыптасты. Келесі, таңдалған онлайн-платформа негізінде eve-ng виртуализациялау, осы тұжырымдамалар негізінде күрделі есептеу желілерінің модельдері әзірленеді және олардың тиімділігіне зерттеулер жүргізіледі.

2.5 Қолданылатын технологиялардың сипаттамасы

Бұрын жасалған тұжырымдамаларда кіші желілерде жұмыс істеуге, байланыс туннельдерін құруға және кәсіпорынның жұмыс станцияларына Интернетке кіруге мүмкіндік беретін логикалық талданудан бастап, IP адрестерін құрудан бастап көптеген түрлі міндеттер тұжырымдалды. Сонымен қатар, компьютерлік желінің дұрыс жұмыс істеуі үшін кәсіпорын компьютерлері арасындағы желілік өзара әрекеттесу мүмкіндігі үшін желі ішіндегі барлық ағып жатқан трафикті бағыттау қажет. Осы міндеттердің бәріне қол жеткізу үшін, сонымен қатар қателіктерге төзімділікті арттыру және байланыс туннельдері арқылы ағып жатқан ақпаратты қорғау үшін әртүрлі желілік хаттамаларды қолдану қажет, олардың көмегімен есептеу желісі ішіндегі барлық жұмыс ұйымдастырылатын болады.

Бұл технологияларды толығырақ қарастырайық.

VLAN

Желіні логикалық құрылымдау мәселесін шешу үшін VLAN технологиясы (VirtualLocalAreaNetwork, виртуалды локальдық желі) қолданылады - бұл бірдей физикалық желілік интерфейсте бірнеше виртуалды локальді желілерді құруға

мүмкіндік беретін, желіні логикалық ішкі желіге бөлуге мүмкіндік беретін технология. Технология құрылғыларға бір-бірімен деректерді беру қабатында тікелей байланыс орнатуға мүмкіндік береді, бірақ физикалық түрде оларды әртүрлі желілік қосқыштарға қосуға болады. Керісінше, әр түрлі VLAN құрылғыларында орналасқан құрылғылар бір-біріне тікелей арналық деңгейінде көрінбейді, тіпті егер олар бір коммутаторға қосылған болса да, бұл құрылғылар арасындағы байланыс тек желіде және одан жоғары деңгейлерде яғни маршрутизаторларды пайдаланумен мүмкін болады.

Осы технологияның негізгі артықшылықтарына назар аударайық:

Құрылғыларды икемділігі әдетте, бір VLAN бір торға сәйкес келеді. Компьютерлер, әртүрлі VLAN-да орналасқан, бір-бірінен оқшауланады;

Хабар таратудың трафигінің төмендеуі. Әрбір VLAN-жеке кең таратылатын домен болып табылғандықтан, әр түрлі VLAN хабар тарату трафигі арасында таратылмайды.

Виртуалды ішкі желіге бөлінген желідегі қауіпсіздік пен басқарылуын арттыру. Әрбір VLAN үшін қауіпсіздік саясаты мен ережелерін қолдану ыңғайлы. Қауіпсіздік саясат бір құрылғыға емес, бүкіл ішкі, тұтас желіге қолданылады.

Аппараттық және желілік кабельдің қысқаруы жаңа виртуалды жергілікті желіні құру үшін коммутаторды сатып алу және желілік кабель төсеу қажет емес.

DHCP

Компьютер желісінде жұмыс істеу үшін оған IP-мекен-жайы қажет. IP-адресті компьютерге беру статикалық әдіспен (қолданушының IP-адресін қолмен тағайындау), сондай-ақ динамикалық түрде (IP-адресті автоматты түрде тағындау) жүргізілуі мүмкін. Біздің желіде жұмыс станцияларының саны ондаған болуы мүмкін болғандықтан, онда нақты екінші әдісті қолдану қажет.

DHCP (DynamicHostConfigurationProtocol - хостты динамикалық торап құру хаттамасы) - бұл компьютерлерге IP мекенжайын және желіде жұмыс істеуге қажетті басқа параметрлерді автоматты түрде алуға мүмкіндік беретін желілік хаттама. Бұл хаттама «тұтынушы-сервер» үлгісіне сәйкес жұмыс істейді, онда компьютер клиент ретінде әрекет етеді, желіде жұмыс істеу үшін DHCP серверінен конфигурацияны сұрайды. Автоматты конфигурациялау үшін клиенттік компьютер желілік құрылғының конфигурация сатысында деп аталатын серверге жүгінеді. DHCP сонымен қатар, одан қажетті параметрлерді алады. Желілік әкімші сервер арасында компьютерлер арасында таратылатын мекен-жайлардың ауқымын көрсете алады. Бұл компьютер желісін қолмен реттеп, қателерді азайтады.

EIGRP

Компьютерлік желінің дұрыс жұмыс істеуі үшін компьютерлер арасындағы желілік өзара әрекеттесу мүмкіндігі үшін желі ішіндегі барлық ағып жатқан

трафикті бағыттау қажет. Маршруттау - бұл желідегі бағыттауды анықтау үдерісі. Бағыттау статикалық бағыттау және динамикалық бағыттау болып екіге бөлінеді.

Статикалық маршруттау кезінде маршруттарды желінің әкімшісі орнатады. Маршрутизацияның бұл түрі шағын желіні іске асыру үшін өте ыңғайлы, бірақ ол үлкен желіде мүмкін емес, өйткені барлық бағыттар маршрутизатордың конфигурациясы кезінде көрсетілген. Статикалық бағыттауларға негізделген желі тұрақсыз және нашар таралған. Бағыттаудың бұл түрі дамып келе жатқан кәсіпорын үшін компьютерлік желіні енгізу үшін тиімсіз.

Динамикалық маршруттауды қолдана отырып, конфигурацияланған желіде маршруттау кестесі бағдарламалық жасақтамамен өңделеді, яғни динамикалық маршруттауды орындау маршруттау хаттамаларына байланысты жүреді.

NAT

Кәсіпорынның құрылғыларына интернетке қосылу мәселесін шешу үшін провайдер бөлген IP-мекенжай арқылы NAT технологиясы қолданылады.

NAT (NetworkAddressTranslation— "желілік мекен- жайды түрлендіру») — бұл TCP / IP желілеріндегі технология, оның көмегімен бірнеше компьютер немесе жеке желі құрылғылары (мұндай диапазондардан жеке мекенжайлар мен 192.168.x.x, 172.X. x) бір IPv4 адресін бірге пайдалана алады. NAT-тың өсіп келе жатқандығының басты себебі IPv4 хаттамасы мекен-жайларының қазіргі интернет-протоколдардың неғұрлым шиеленіскен, тапшылығымен күрт жетіспеуімен байланысты.

Осы технологияның негізгі артықшылықтарына назар аударсақ:

• Жалпыға қол жетімді IP мекенжайларын үнемдеу бір мекен-жай арқылы сіз 65000-нан астам сұр мекен-жайлар шығара аласыз.

• Сыртқы қосылымдардың соңғы компьютерлерге кедергі жетуіне жол бермейді. Егер NAT технологиясы қосылған құрылғыға сырттан рұқсат етілмеген пакет келсе, ол жай ғана жойылады.

Сыртқы маршрутты трассалау кезінде желінің ішкі құрылымын бөгде көздерден жасырады, NAT қосылған құрылғы бұдан әрі ештеңе қол жетімді болмайды. Жабдық пен желі кабелінің санын азайту жаңа виртуалды жергілікті желіні құру үшін сатып алу және желілік кабель салу қажет емес.

STP

Соңғы тұжырымдамада көрсетілген серверге бас тартуға тұрақты қатынау мәселесін шешу үшін STP желілік хаттамасы, атап айтқанда оның rstp жақсартылған нұсқасы, топологияның жедел қайта жаңғыртуы бар STP хаттамасының нұсқасы қолданылады.

STP (SpanningTreeProtocol,қалған хаттамасы) — STP негізгі міндеті арна деңгейінде ілмектердің пайда болуын болдырмау. Хаттама жұмысы қайталанатын маршрутты бұғаттаудан тұрады, осылайша ілмектердің пайда болуын

болдырмайды. Біздің тұжырымдамада хаттама жұмысы бір маршрутты серверге дейін "резервте қалдыру" болып табылады.

Егер серверге апаратын қолданыстағы бағыттардың бірінде ақаулық орын алса, оны резервтелген маршрут қайталайды, басқа уақытта топологияда ілмектер болмас үшін «сақталған» бағыт бұғатталады.

VPN/GRE/IPsec

Желілік өзара іс-қимыл жасау мүмкіндігі үшін аумақтық шалғай филиалдар арасында байланыс туннель құру міндеті қиын емес және әртүрлі шешім нұсқалары бар. Ұсынылған 2.5-тарауда, тұжырымдамаларда осы есептің әртүрлі шешімі ұсынылды. Бірінші, филиалдардың маршрутизаторлары арасында байланыс туннель құру, екінші – бұл екі байланыс туннель құру, олардың біреуі резервтік күйде болады және тек негізгі ақаулықтар пайда болған кезде ғана пайдаланылатын болады. Сонымен қатар, бұл байланыс туннельдері ішкі желінің шегінен шығып, интернет арқылы өтетіндіктен, мұндай туннельдер арқылы ағымдық ақпаратты рұқсат етілмеген пайдаланушылардан қорғау қажет.Бірінші тапсырманы шешу үшін VPN технологиясы қолданылады. VPN (VirtualPrivateNetwork-виртуалды жеке желі) - офистің аралық екі жақты тұрақты арнасын ұйымдастыру үшін пайдаланылады және ол қосымша бағдарламалық қамтамасыз етуді орнатуды талап етпейді.

Негізгі филиалдар арасындағы байланыс арнасы ретінде интернетті пайдалану қымбат жалға алынатын жеке желілердің экономикалық тиімді баламасы болып табылады. VPN технологиясы қауіпсіздікті қамтамасыз ету және оларды ұстап қалуды болдырмау үшін туннель бойынша берілетін деректерді күрделі шифрлауды қолдануды білдіреді.

VPN туннель бойынша өтетін шифрлау IPSec қорғалған қатынау желілік хаттамасы бойынша жүргізіледі.

IPsec— (IP Security-тен қысқарту) IP желіаралық хаттамасы бойынша берілетін деректерді қорғауды қамтамасыз ету үшін хаттамалар жиынтығы.Ол IP пакеттерін аутентификациялау, туннелдеу және шифрлау үшін арналған. IPSec ашық және барлық желілерде жұмыс істей алатындай өте ыңғайлы. IPSec туннельді іске қосу кезінде пайдаланушыларды немесе компьютерлерді сәйкестендірудің стандартты әдістерін, туннельдің соңғы нүктелері үшін шифрлауды қолданудың стандартты әдістерін және соңғы нүктелер арасындағы шифрлау кілттерін алмасудың және басқарудың стандартты әдістерін ұсынады.

Осылайша, есеп берудің қауіпсіз туннелін құрудың бірінші міндетін шешу үшін IPSec көмегімен деректерді шифрлаумен VPN туннелі құрылады.

Екінші міндет екі байланыс туннелінің болуын және олардың біреуі істен шыққан жағдайда олардың автоматты конфигурациясының болуын білдіретіндіктен, онда бас тартуға төзімді туннельдің есебін шешу үшін бұрын сипатталған EIGRP хаттамасы қолданылады. Алайда, EIGRP хаттамасының

жұмысы жақын көршілерді табу сатысында эфирлік пакеттерге негізделгендіктен, VPN байланыс туннелін салуға бұрын сипатталған хаттама бұл мақсатқа жарамайды, VPN хаттамасының бір ерекшелігі - эфирлік трафиктің берілуі. Сондықтан екінші есепті шешу үшін есеп беру туннелін құру үшін GRE хаттамасы қолданылады.

GRE – Cisco Systems әзірлеген желілік пакеттің туннельдік хаттамасы. Бұл хаттама пакеттерді бір желіден екінші желіге беру үшін қолданылады. GRE туннелі - нүкте-нүкте байланысы және жоқ деректерді шифрлайтын VPN туннелінің бір түрі деп санауға болады.

GRE-дің басты артықшылығы - таратылатын трафикті беру мүмкіндігі, ол оны пайдаланатын маршруттық хаттамаларды құрылған туннель арқылы өтуге мүмкіндік береді.

Осылайша, екінші мәселені шешу үшін, ақауларға төзімді есеп туннельдерін құру үшін EIGRP динамикалық бағыттау хаттамасымен GRE протоколы пайдаланылады. GRE протоколы VPN қарағанда, әдепкі бойынша туннель бойынша өтетін деректерді шифрлауды талап етпейді, оны қосымша баптау қажет. Бұл үшін IPSec мәліметтерін қорғауды қамтамасыз ету үшін бұрын аталған хаттамалар жиынтығы пайдаланылатын болады. Нәтижесінде GRE-мен динамикалық EIGRP маршрутизациясы бар және IPSec көмегімен қорғалған 2 туннель құрылады.

2.6 Eve-ng-тағы компьютерлік желіні модельдеу

Eve-ng желілік жабдықтарын виртуалдау үшін таңдалған заманауи онлайн платформаның негізінде күрделі компьютерлік желілердің бірнеше модельдері жасалды. Әзірленген модельдер кішігірім кеңседен аумақтық алыс шалғайда филиалдары бар, жоғары есептеу ресурстарын және оларды қорғауды қажет ететін үлкен кәсіпорынға айналу жолын көрсетеді.

Cisco Systems жабдығын қолдана отырып, компьютерлік желілерді модельдеу үдерісіі Cisco IOS коммутациялық және бағыттау жабдығының операциялық жүйесін эмуляциялау арқылы жүзеге асырылды. Эмуляцияланған құрылғылардың параметрлері орнатылды: коммутаторлар үшін - кездейсоқ қол жетімді жад (RAM) және флэш-жад (NVRAM) үшін 128 Мбайт; роутерлер үшін - флэш-жады үшін 128 Мбайт (NVRAM) және кездейсоқ қол жетімді жад (RAM) үшін 256 Мбайт.

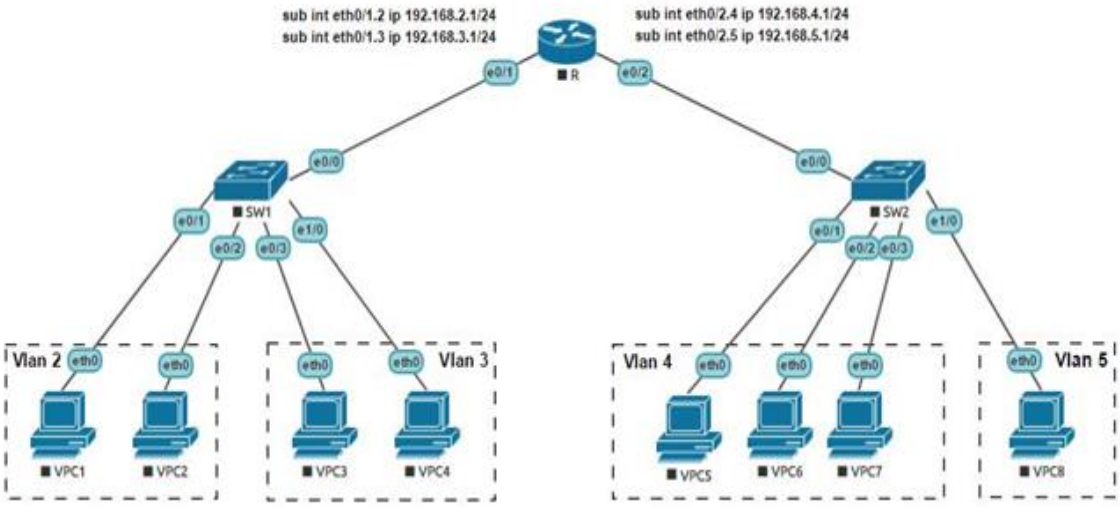
NAT – желілік адрестерді түрлендіру технологиясын және маршрутталатын құрылғыда бапталған VPN/GRE хабарлаушы туннельдерді құру технологияларын пайдалана отырып, есептеу желілерінің модельдерін құру кезінде жедел жады (RAM) саны 512 Mbyte-ге дейін артты. Жедел жады санының көбеюі жоғарыда аталған хаттамалардың жұмысына байланысты.

Серверлік жабдықтың жұмысын модельдеу үшін eve-ng платформасында веб-сервер ашылды. Осылайша, жобаланған модельдерді физикалық қалпына келтіру кезінде eve-ng-де жабдықтың типі мен сериясын таңдау сипатталған сипаттамаларға және қосылатын жабдық үшін қажетті порттардың санына байланысты болуы мүмкін.

Нәтижесінде, eve-ng платформасында, компьютерлік желілердің тұжырымдамаларына негізделген және таңдалған желілік технологияларды қолдана отырып, компьютерлік желінің модельдері жасалды.

2.7 Компьютерлік желілердің сипаттамасы

2.14-суретте көрсетілген №1 модель SW1 және SW2 екі қосқыштардан және R маршрутизаторынан тұратын модель болып табылады және қарапайым компьютерлік желіні көрсетеді, оның негізгі мақсаты кәсіпорынның компьютерлерін біріктіру және олардың арасындағы желілік өзара әрекеттесу мүмкіндігін құру болып табылады.



Сурет 2.14 - №1 компьютерлік желінің құрастырылған моделі

Әрбір коммутаторда виртуалды жергілікті желілер (VLAN) орнатылған. VLAN2 және VLAN3 LAN қосқышы SW1 қосқышында бапталған, ал VLAN4 және VLAN5 SW2 қосқышында бапталған. Жұмыс станциясының байланысын анықтау жергілікті желілерге қосқыш интерфейстерін тарату жолымен жүреді. SW1 коммутаторының жергілікті желілері бойынша интерфейстердің бұл таралуы 2.15 суретте көрсетілген.

```
VLAN Name                              Status    Ports
---- --------------------------------- --------- -------------------------------
1    default                           active    Et1/1, Et1/2, Et1/3
2    VLAN0002                          active    Et0/1, Et0/2
3    VLAN0003                          active    Et0/3, Et1/0
1002 fddi-default                      act/unsup
1003 token-ring-default                act/unsup
1004 fddinet-default                   act/unsup
1005 trnet-default                     act/unsup
```

Сурет 2.15 - SW1 коммутаторындағы жергілікті желілер бойынша қосылу интерфейстерінің таралуы

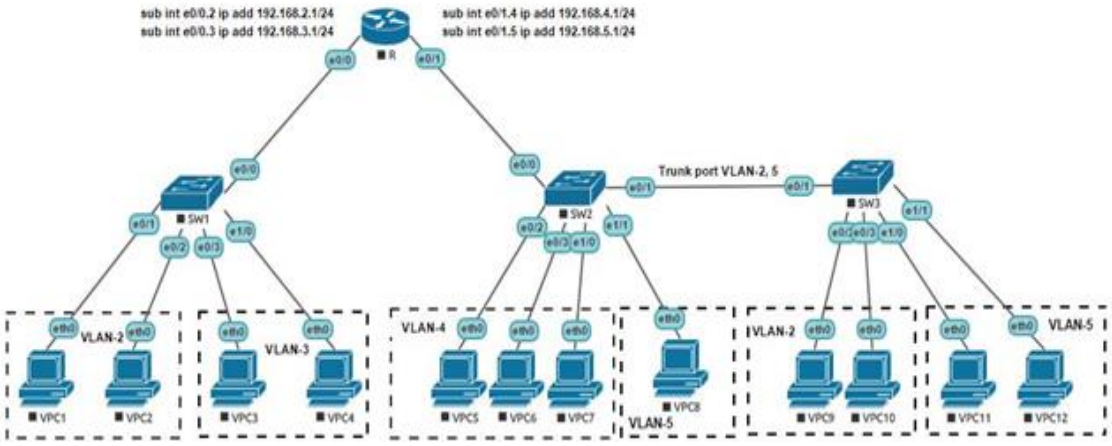
Осылайша, кәсіпорынның қарамағындағы жұмыс станциялары әр түрлі жергілікті желілерде логикалық түрде таратылды. Мұндай жұмыс станцияларын жергілікті желілерге бөлу болашақта осындай желіні басқаруды жеңілдетуге және оны логикалық құрылымдауға мүмкіндік береді. Бұл модельде R маршрутизаторы бар, оның міндеті әртүрлі жергілікті желілерде орналасқан жұмыс станциялары арасында желілік өзара әрекеттесу мүмкіндігін ұйымдастыру болып табылады.

Сонымен қатар маршрутизаторда DHCP-сервері орнатылған, оның міндеті желідегі жұмыс станцияларының жұмысы үшін қажетті компьютер-агенттерге IP-адрестерді автоматты түрде беру болып табылады. Ол үшін маршрутизаторда әрбір жергілікті желі үшін берілетін параметрлермен DHCP-пулдары жасалды. R маршрутизаторына теңшелген мұндай DHCP пулдарының мысалы 2.16 суретте көрсетілген.

```
ip dhcp pool DHCP-VLAN2
 network 192.168.2.0 255.255.255.0
 default-router 192.168.2.1
 dns-server 8.8.8.8
!
ip dhcp pool DHCP-VLAN3
 network 192.168.3.0 255.255.255.0
 default-router 192.168.3.1
 dns-server 8.8.8.8
!
ip dhcp pool DHCP-VLAN4
 network 192.168.4.0 255.255.255.0
 default-router 192.168.4.1
 dns-server 8.8.8.8
!
ip dhcp pool DHCP-VLAN5
 network 192.168.5.0 255.255.255.0
 default-router 192.168.5.1
 dns-server 8.8.8.8
```

Сурет 2.16 - R маршрутизатордағы орналасқан DHCP-пулдар

№2 модель, 2.17 суретте көрсетілген, есептеу моделінің құрылымы №1 модельге ұқсас, өйткені ол алдыңғы модельдің логикалық жалғасы болып табылады.

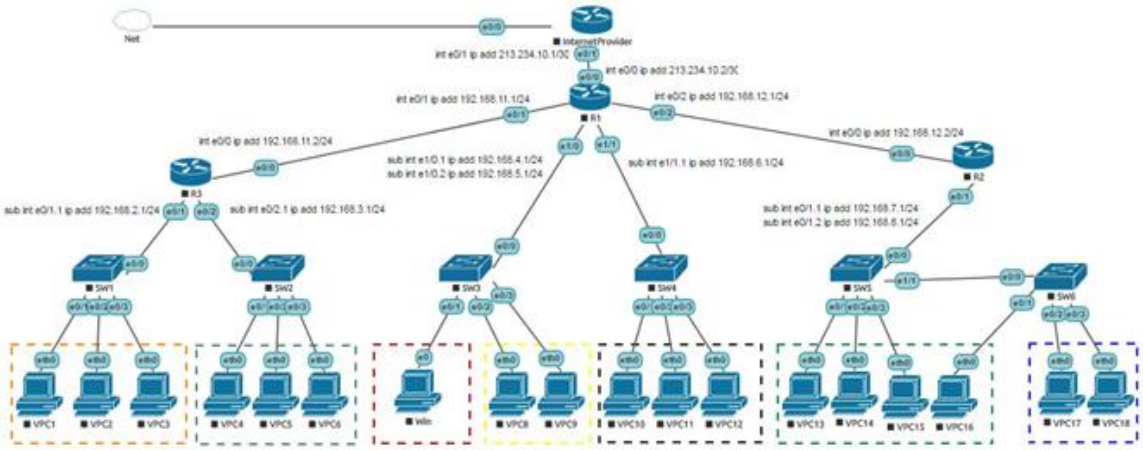


Сурет 2.17 - № 2 компьютерлік желінің жобаланған моделі

Бұл компьютерлерді бір жергілікті желіде логикалық түрде біріктіру міндеті туындайтын, бірақ физикалық түрде әртүрлі қосқыштарға қосылған жағдайды көрсетті. Бұл жағдайда логикалық түрде бесінші жергілікті желіде орналасқан, бірақ әр түрлі қосқыштарға (SW2 және SW3) қосылған компьютерлер R маршрутизаторын ескерусіз де желілік өзара әрекеттесуге мүмкіндік алады.

Алайда, екінші жергілікті желіде логикалық орналасқан компьютерлермен жағдай керісінше, тек қана маршрутизатормен өзара әрекеттесу мүмкін. Мұндай логикалық бірлестік SW2 және SW3 коммутаторларын магистральды портпен (Trunkport) қосу жолымен мүмкін болды. Бұл магистральды порт құрылғылар арасында жергілікті желілердің (VLAN) трафигін құрылғылар арасында тасымалдау үшін қызмет етеді.

2.18-суретте көрсетілген №3 үлгі кәсіпорынның өсуін көрсетеді. Компьютерлік желіні құруға арналған желілік құрылғылардың саны сияқты жұмыс станцияларының саны да артып келеді. Бұл тұжырымдама алдыңғы модельдерден жұмыс станцияларын қосудың екі әдісін де қамтиды. Сондай-ақ модельде компьютерлердің кәсіпорындағы бөлімшелерге қатысты жергілікті желілерге логикалық бөлінуін көрсетеді.



Сурет 2.18 - №3 есептеу желісінің жобаланған үлгісі

Бұл модельде үш маршрутизатор (R1, R2 және R3) болғандықтан, желіде өтетін трафикті бағыттау қажеттілігі пайда болады. Бұл үшін көрші маршрутизаторларды өздері білетін желілер туралы ақпаратпен алмасуды көздейтін EIGRP динамикалық бағыттау хаттамасы қолданылды. Бұл протоколды R1 маршрутизаторында баптау 2.19-суретте көрсетілген.

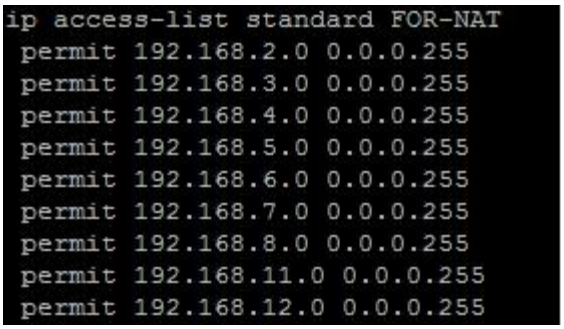
```
router eigrp 1
 network 192.168.4.0
 network 192.168.5.0
 network 192.168.6.0
 network 192.168.11.0
 network 192.168.12.0
 network 213.234.10.0
```

Сурет 2.19 - R1 маршрутизаторында eigrp динамикалық бағыттау хаттамасын баптау

NAT хаттамасының көмегімен провайдер бөлінген IP-мекен-жайы арқылы интернет желісіне қатынау желісінің барлық тораптарына қатынау ашылды. Ол үшін, R1 маршрутизаторында провайдер бөлген IP-адрестерге түрлендіруге қажетті жергілікті желілердің IP-адрестерінің тізімі бар қатынау парағы жасалды. Яғни, интернет желісіне жергілікті желіден қатынау пайда болған кезде, оның "сұр" IP-адресін "ақ"-қа трансляциялау жүргізілді. R1 маршрутизаторында жасалған кіру парағы 2.20-суретте көрсетілген.

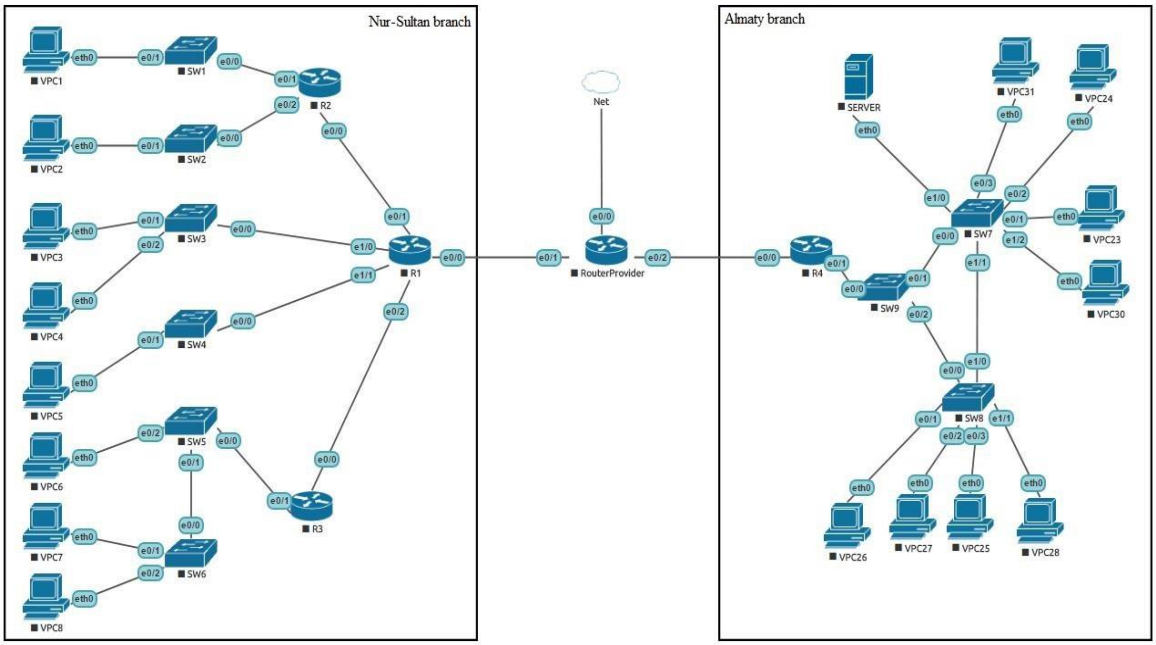
Модельдік провайдерге (InternetProvider) – жеткізуші "ақ" IP-мекенжай кіреді. NAT-ты арнайы IP-мекен-жайы арқылы пайдалану провайдер барлық интернет желісіне қол жеткізе алды. Ол үшін арнайы IP мекен-жайға түрлендірілуі

керек жергілікті желілердің IP мекенжайларының тізімі бар R1 маршрутизаторында қол жетімділіктің тізімі жасалды. Яғни, желіге қол жеткізген кезде, қол жеткізу тізіміндегі жергілікті желідегі интернет түйіні өзінің «сұр» IP мекенжайын «ақ»-қа ауыстырады. R1 маршрутизаторына арналған кіру парағы 2.20 - суретте көрсетілген.



Сурет 2.20 - R1 маршрутизаторында NAT хаттамасымен жергілікті желілердің таратылып отырған IP- мекен-жайларының тізімі бар кіру парағы

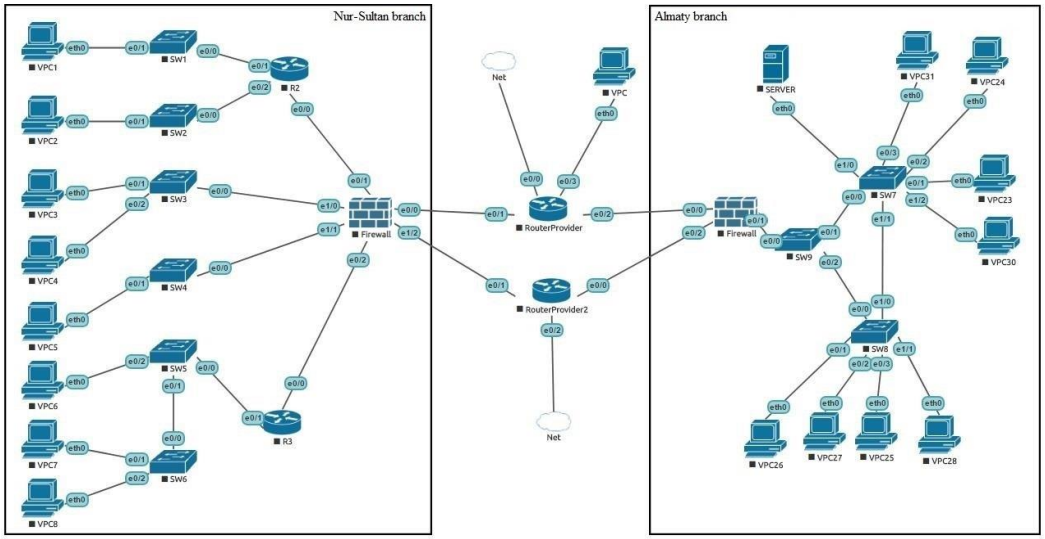
2.21-суретте №4 үлгіде кәсіпорынның құрылымдық бөлімшесі аумақтық филиалдарға бөлінуі көрсетілген. Бұл жағдай кәсіпорынның аумақтық шалғай филиалы пайда болған кезде жасалады және әртүрлі филиалдар объектілері арасында желілік өзара әрекеттесу мүмкіндігі үшін ортақ компьютерлік желіні құру қажеттілігі туындайды. Әрбір филиал өзінің провайдерімен бөлінген IP-мекен-жайы арқылы интернетке қатынау мүмкіндігіне ие болғандықтан, осы IP-мекен-жайлар арасында хабарлаушы VPN туннель құрылды. Яғни, R1 және R4 маршрутизаторларының сыртқы интерфейстері арасында нүкте-нүкте түріндегі айқын байланыс құрылды. Содан кейін құрылған VPN туннелінде IPSec хаттамасынан шифрлау саясаты қолданылды.



Сурет 2.21 - №4 компьютерлік желісінің жобаланған моделі

Алайда, жергілікті желіден тыс шығатын трафикті бағыттау қажеттілігі пайда болады. Трафикті сұрыптау керек. Филиалдың жергілікті желісіне өтетін трафик VPN туннелі бойынша өткізілуі керек, ал қалған трафик провайдер бөлген IP мекен-жайға ауыстырылуы керек. Бұл мәселені шешу үшін VPN туннелі арқылы қандай трафикті бағыттауға болатындығын және оны «ақ» IP мекен-жайға аудару керек екендігі туралы кеңейтілген қол жеткізу тізімі қолданылды. Серверлік жабдықтардың ақауларға төзімді болуын қамтамасыз ету үшін STW желілік хаттамасы SW7, SW8 және SW9 коммутаторларындағы филиалдық компьютерлік желінің топологиясында, дәлірек айтсақ оның жетілдірілген RSTP нұсқасы жасалды, ол бұзылған жағдайда топологияны қалпына келтіруге аз уақытты алады.

2.22-суретте №5 қорытынды үлгіде компания филиалдары арасында байланыс туннель құрудың тағы бір нұсқасы көрсетілген.



Сурет 2.22 - № 5 компьютерлік желінің жобаланған моделі

Бұл нұсқада әрбір филиал провайдерлерден кем дегенде екі "ақ" IP-адресін жалға алады. IP-адрестердің әрбір жұбы арқылы хабарлаушы GRE тоннельдер, бір негізгі және бір резервтік жүргізілген. Туннельдердің ақаулыққа төзімділігін жүзеге асыру үшін R1 және R4 тармақтарының маршрутизаторларында бұрын пайдаланылған EIGRP динамикалық бағыттау протоколы құрылды. Негізгі GRE туннелінде ақау пайда болған жағдайда, топология автоматты түрде қалпына келтіріліп, резервтік GRE туннелі іске қосылады. Сондай-ақ, модельде кәсіпорынның серверіне қол жетімділік интернеттен, кәсіпорынның компьютерлік желісінің ішкі құрылымынан тыс пайдаланушылар үшін бапталған. Пайдаланушы NAT технологиясын қолдана отырып, R4 маршрутизаторында провайдер бөлген IP-мекен-жайға қол жеткізген кезде сервердің көмегімен IP-мекен-жайы трансляция жүргізіледі.. Осылайша, серверге қол жетімділік жалпыға қол жетімді осылайша, серверге қол жеткізу ашық болады және интернеттегі барлық пайдаланушылар үшін қол жетімді болады.

Компьютерлік желілердің жобаланған модельдерінің тиімділігі туралы зерттеу жүргізу үшін осы желінің жұмысын модельдеу қажет. Eve-ng-та жасалған әр модель үшін олардың тұжырымдамаларын әзірлеу кезінде қойылған міндеттерді орындау тиімділігі туралы зерттеулер жүргізілді. Егер зерттеу нәтижесінде қойылған мақсаттарға қол жеткізілсе, онда модель тиімді деп саналды.

2.8 Компьютерлер арасындағы желілік әрекеттесу мүмкіндігін зерттеу

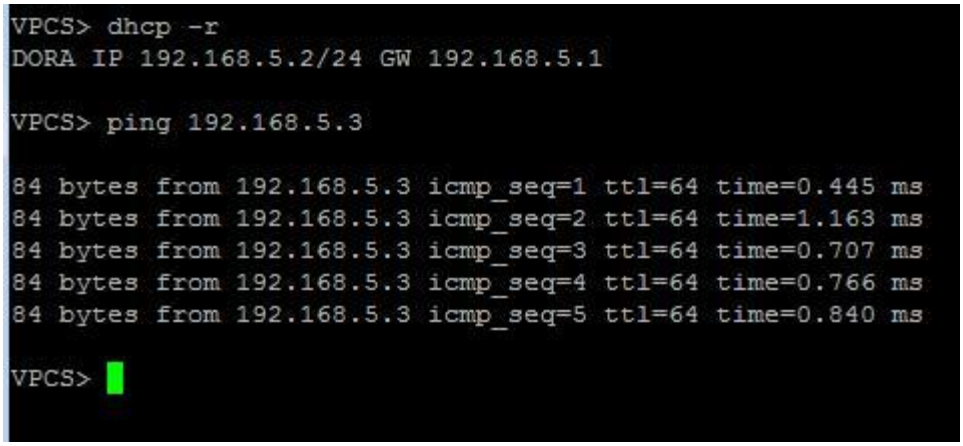
Негізгі міндеті кәсіпорынның есептеуіш машиналарын бірыңғай желіге біріктіру және олардың арасындағы желілік өзара іс-қимыл мүмкіндігін құру

болып табылатын №1 және №2 модельдер үшін осы өзара іс-қимыл мүмкіндіктерін зерттеу жүргізілді. Желілік өзара іс – қимыл мүмкіндігі "ping" бір жергілікті желі компьютерлері мен әртүрлі жергілікті желілерде орналасқан компьютерлер арасындағы желілік қосылыстың бүтіндігі мен сапасын тексеру үшін желілік қызметтің сәтті орындалуымен анықталды. Алдымен, жұмыс станциясындағы «dhcp -r» пәрменін пайдаланып, DHCP серверінен IP мекенжайын жалға алуды бастай отырып, №1 модельдегі R маршрутизаторында бапталған DHCP серверінің сәтті жұмыс істейтіндігін тексереміз. Жұмыс станциясындағы dhcp -r командасының нәтижесі 2.23-суретте көрсетілген.

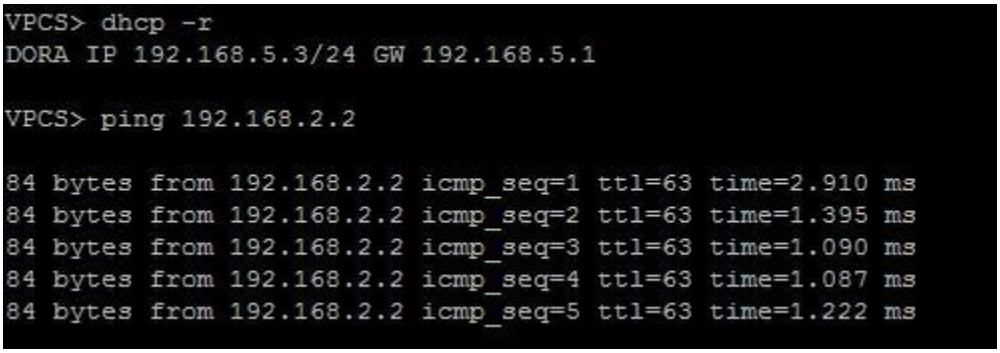
```
VPCS> dhcp -r
DDORA IP 192.168.2.2/24 GW 192.168.2.1

VPCS> show ip

NAME        : VPCS[1]
IP/MASK     : 192.168.2.2/24
GATEWAY     : 192.168.2.1
DNS         : 8.8.8.8
DHCP SERVER : 192.168.2.1
DHCP LEASE  : 86386, 86400/43200/75600
MAC         : 00:50:79:66:68:05
LPORT       : 20000
RHOST:PORT  : 127.0.0.1:30000
MTU         : 1500
```

Сурет 2.23 - DHCP серверінен IP мекенжайын сәтті жалға алу нәтижесі

Алынған нәтижелерден жұмыс станциясы DHCP серверінен жауап ретінде желіде жұмыс істеуге арналған параметрлер конфигурациясын сәтті қабылдағанын көруге болады. Одан әрі, №2 үлгінің мысалында, бір жергілікті желіде, бесінші және әр түрлі, бесінші және екіншісінде орналасқан компьютерлердің желілік өзара әрекеттесу мүмкіндігін тексереміз. Бір жергілікті желіде және әр түрлі желілерде орналасқан компьютерлердің желілік өзара әрекетін сәтті жүзеге асырудың нәтижелері сәйкесінше 2.24 және 2.25-суреттерде көрсетілген.



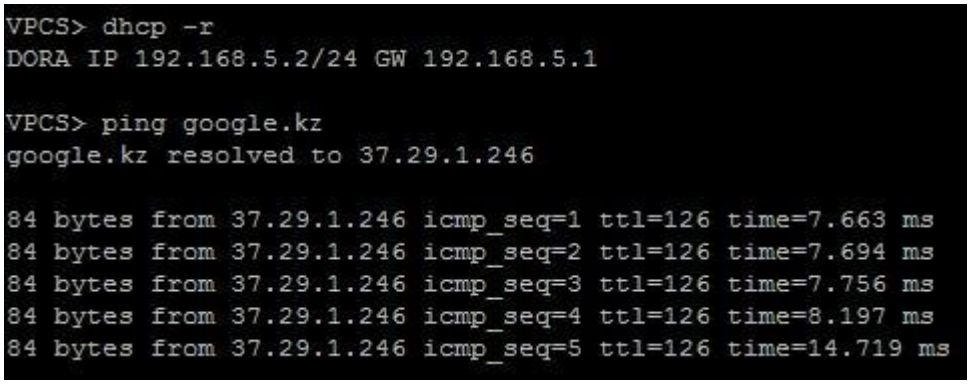
Сурет 2.24 - Бесінші жергілікті желіде орналасқан компьютерлердің табысты желілік өзара әрекеттесуінің нәтижесі



Сурет 2.25 - Әр түрлі жергілікті желілерде орналасқан компьютерлер арасындағы сәтті желілік өзара іс-қимылының нәтижесі

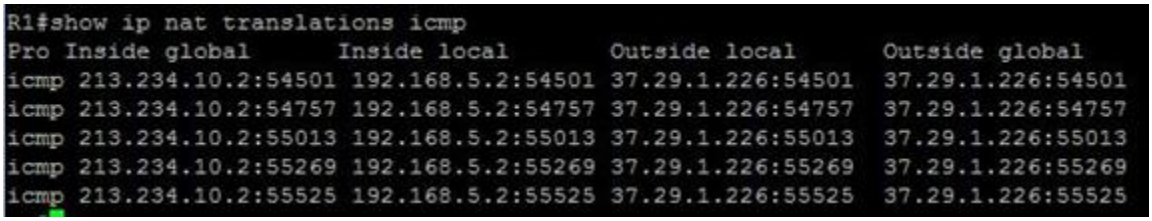
2.9 Интернет желісіне кіру мүмкіндігі туралы зерттеу жүргізу

№ 3 модель үшін басты міндет провайдер бөлген IP мекен-жайы арқылы барлық жұмыс станцияларына Интернет желісіне кіруге қол жетімділікті ашу болды. Провайдер компанияға 213.234.10.2 түріндегі «ақ» IP мекен-жайды тағайындады, ол арқылы интернет желісіне қол жеткізуге болады. Біз R1 маршрутизаторында бапталған NAT технологиясының жұмысын тексеріп, кәсіпорынның жұмыс станциясымен және Google.kz сайтымен желілік өзара әрекеттесуге тырысамыз. Нәтижесі 2.26 - суретте көрсетілген.



Сурет 2.26 - «Google.kz» тораптармен табысты желілік өзара іс-қимыл нәтижесі

R1 маршрутизаторындағы «Google.ru» торабымен желінің сәтті өзара әрекеттесуінің нәтижесін NAT технологиясын қолдана отырып IP адресін аудару кестесіне қарап тексерейік.



Сурет 2.27 - R1 маршрутизаторындағы IP-мекен-жайды аудару кестесі

2.27 суретте көрсетілгендей, «Google.kz» торабымен 192.168.5.2 IP мекенжайы бар кәсіпорынды компьютерге қосуға тырысқанда, адрес NAT технологиясымен 213.234.10.2 IP адресіне аударылған. Бұл модель дұрыс орнатылған білдіреді.

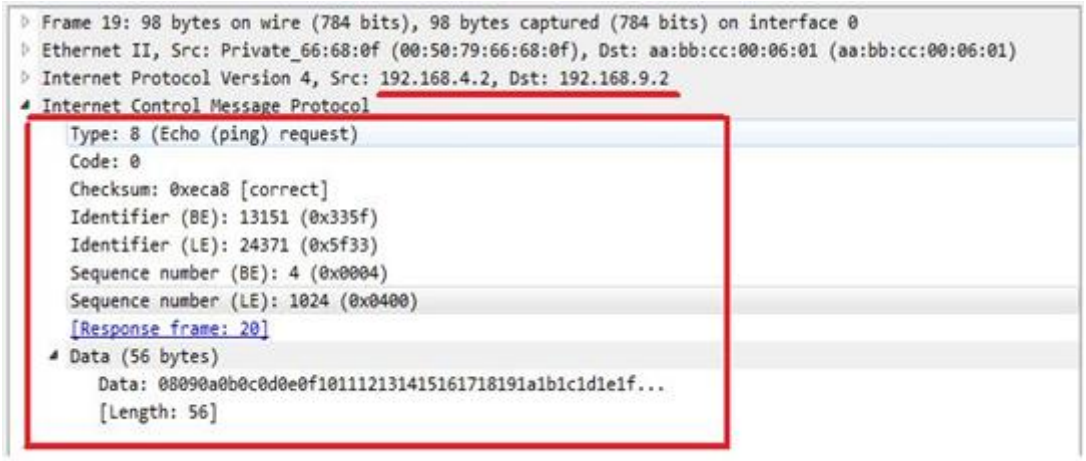
2.10 Қауіпсіз байланыс туннелінің тиімділігіне және серверлік жабдықтың ақауларының төзімділікке қол жеткізуге зерттеу жүргізу

№ 4 модельде филиалдар арасында VPN туннелін қосатын құру, сондай-ақ ол арқылы өтетін трафикті шифрлеу міндеті қойылды. Төртінші жергілікті желіде, Нұр-Сұлтан филиалында және 9 жергілікті желіде, Алматы филиалында орналасқан компьютерлер арасындағы желілік өзара әрекеттестік мысалын қолдана отырып, филиалдардың компьютерлерінің өзара әрекеттесуін тексерейік. Желілік өзара әрекеттесудің нәтижесі 2.28 - суретте көрсетілген.

```
VPCS> dhcp -r
DORA IP 192.168.4.2/24 GW 192.168.4.1

VPCS> ping 192.168.9.2

84 bytes from 192.168.9.2 icmp_seq=1 ttl=62 time=3.367 ms
84 bytes from 192.168.9.2 icmp_seq=2 ttl=62 time=2.061 ms
84 bytes from 192.168.9.2 icmp_seq=3 ttl=62 time=1.989 ms
84 bytes from 192.168.9.2 icmp_seq=4 ttl=62 time=2.102 ms
84 bytes from 192.168.9.2 icmp_seq=5 ttl=62 time=1.958 ms
```

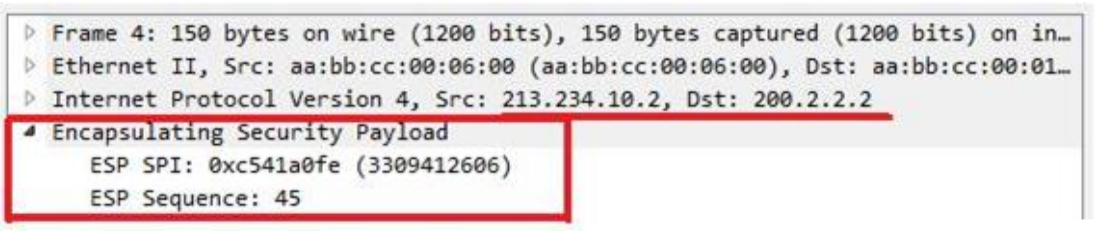
Сурет 2.28 - Салалық компьютерлер арасындағы табысты желілік өзара іс-қимыл байланыстың нәтижесі

VPN туннелі арқылы өтетін шифрды тексеру үшін трафикті қосымша трафик анализаторы болып табылатын WireShark бағдарламалық жасақтамасы пайдаланды. Алдымен филиалдардың компьютерлері арасындағы Алматы филиалының жергілікті желісінің ішінен өтетін трафикке кедергі келтірейік, 2.29-сурет.



Сурет 2.29 - Шифрланбаған түрде филиалдар компьютерлері арасында берілетін ақпараттың мазмұны

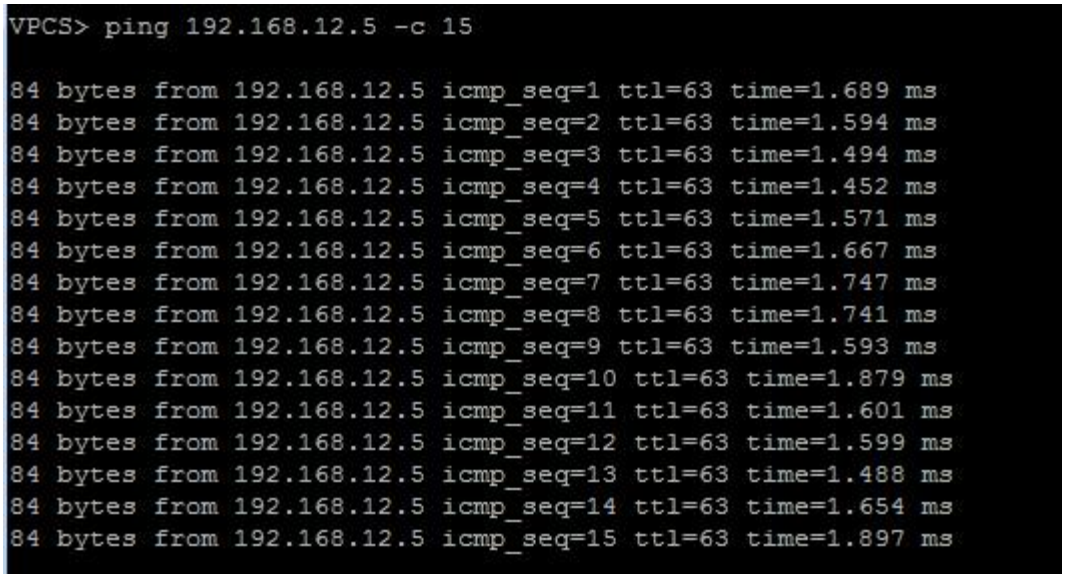
Сонымен, филиалдар компьютерлері арасындағы Алматы филиалының жергілікті желісінің сыртынан, VPN туннелінің ішіндегі трафикке кедергі келтірейік, 2.30-сурет.



Сурет 2.30 - Салалық компьютерлер арасында шифрланған түрде берілетін ақпараттың мазмұны

Нәтижелерден шифрлау туралы хаттаманың түрі мен оның мазмұны туралы ақпарат болған кезде, шифрлаудан кейін тек шифрлау алгоритмінің атауы болғанын көруге болады.

Филиалдың жұмыс станциясында «ping –c 15» пәрменін іске қосу арқылы және SW8 және SW9 қосқыштары арасындағы тарату ортасын қолмен бұзу арқылы серверлік жабдыққа ақаулыққа төзімді қатынасты тексереміз.



Сурет 2.31 - SW8 және SW9 қосқыштарын мәжбүрлеп ажырату кезінде серверлік жабдықтармен желілік өзара әрекеттесудің нәтижесі

2.32-суретте көрсетілген нәтижелерден, трансмиссиялық ортада ақаулық болған кезде, серверлік жабдықпен желілік өзара әрекеттесу кезінде бірде-бір пакет жоғалмағанын көруге болады.

2.11 Өнімділікті зерттеу ақаулыққа төзімді туннелі және интернеттен сервердің қол жетімділігі

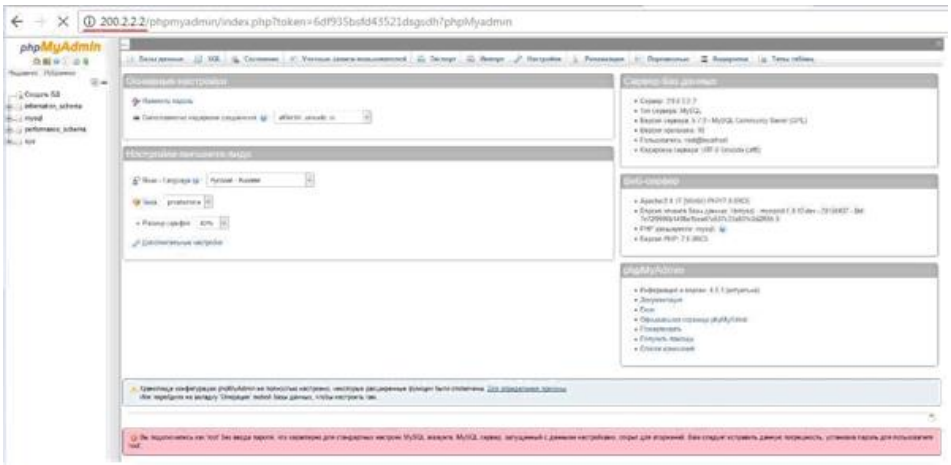
№ 5 модельде бұтақтар арасында ақауларға төзімді байланыс туннелін салу міндеті қойылды. «ping-100 100» пәрменін қолдана отырып, филиалдардағы

компьютерлер арасындағы ұзақ уақыттық өзара әрекеттесуді және R1 және R4 маршрутизаторлары арасындағы туннельді беру ортасын қолмен бұзып, туннельдің ақаулыққа төзімділігін тексереміз.

```
VPCS> ping 192.168.4.2 -c 100

84 bytes from 192.168.4.2 icmp_seq=1 ttl=62 time=1.935 ms
84 bytes from 192.168.4.2 icmp_seq=2 ttl=62 time=1.758 ms
84 bytes from 192.168.4.2 icmp_seq=3 ttl=62 time=1.937 ms
84 bytes from 192.168.4.2 icmp_seq=4 ttl=62 time=1.717 ms
192.168.4.2 icmp_seq=5 timeout
192.168.4.2 icmp_seq=6 timeout
192.168.4.2 icmp_seq=7 timeout
192.168.4.2 icmp_seq=8 timeout
192.168.4.2 icmp_seq=9 timeout
192.168.4.2 icmp_seq=10 timeout
192.168.4.2 icmp_seq=11 timeout
192.168.4.2 icmp_seq=12 timeout
192.168.4.2 icmp_seq=13 timeout
192.168.4.2 icmp_seq=14 timeout
192.168.4.2 icmp_seq=15 timeout
192.168.4.2 icmp_seq=16 timeout
192.168.4.2 icmp_seq=17 timeout
192.168.4.2 icmp_seq=18 timeout
192.168.4.2 icmp_seq=19 timeout
84 bytes from 192.168.4.2 icmp_seq=20 ttl=62 time=2.450 ms
84 bytes from 192.168.4.2 icmp_seq=21 ttl=62 time=2.170 ms
84 bytes from 192.168.4.2 icmp_seq=22 ttl=62 time=2.078 ms
84 bytes from 192.168.4.2 icmp_seq=23 ttl=62 time=2.525 ms
84 bytes from 192.168.4.2 icmp_seq=24 ttl=62 time=2.211 ms
84 bytes from 192.168.4.2 icmp_seq=25 ttl=62 time=2.106 ms
84 bytes from 192.168.4.2 icmp_seq=26 ttl=62 time=2.050 ms
```

Сурет 2.32 - Байланыс туннелінде үзіліс болған жағдайда филиалдық компьютерлер арасындағы желілік өзара әрекеттесудің нәтижесі

2.32-суретте көрсетілген нәтижелерден, ақаулар болған жағдайда байланыс туннелін қалпына келтіру процесі шамамен 15 секундты алатындығын көруге болады. Осы уақыттан кейін филиалдармен байланыс қалпына келтіріледі. Содан кейін интернеттегі пайдаланушылар үшін сервер қол жетімділігін тексеріңіз. Ол үшін Windows-та жұмыс істейтін компьютерде мекенжай қатары арқылы 200.2.2.2 IP-мекен-жайына өтіңіз.



Сурет 2.33 - Интернеттен пайдаланушыға серверге қол жеткізудің нәтижесі

Нәтижелерден көрініп отырғандай, 2.33-сурет, интернет пайдаланушылар үшін кәсіпорынның сервері қол жетімді. NAT технологиясын қолдана отырып, провайдер бөлген 200.2.2.2 IP-мекен-жайына қол жеткізу кезінде веб-сервер орналастырылған сервердің IP-мекен-жайына аударма жасалды.

3. Өмір тіршілігінің қауіпсіздігі

3.1 Еңбек жағдайларын талдау

Желі қауіпсіздігін қамтамасыз ету компьютерлік технологиялар мен серверлік жабдықтардың көмегімен жүзеге асырылады. Қарастырылып отырған офис он екі жұмысшыны құрайды, әр қайсының өзінің жеке жұмыс орны бар.

Бағдарламашы жұмыс істеу барысында қауіпті және зиянды факторлар келесідей:

- электромагниттік өрістерге әсер ету;
- бөлмені жарықтандыру жеткіліксіз;
- бөлменің микроклиматы қанағаттанарлықсыз.

Қауіпсіздік ережелерін және өндірістік гигиенаны сақтамау, қауіпсіздік шараларын дұрыс орындамау апатқа немесе адам жарақатына әкелуі мүмкін.

Сондай – ақ, жұмыс орындары өте маңызды орын алады. Нақтырақ айтқанда, ұйымдастыру кезінде, бағдарламашы жұмыс орны келесі негізгі шарттарға сай болу керек:

-жұмыс орнының бөлігі болып табылатын жабдықтарды оптималды орналастыру;

-барлық қажетті қозғалыстар мен қозғалыстарды жүзеге асыруға мүмкіндік беретін жеткілікті жұмыс кеңістігі;

- берілген таапсырмаларды орындау кезінде қажет болатын табиғи және жасанды жарықтандыру;

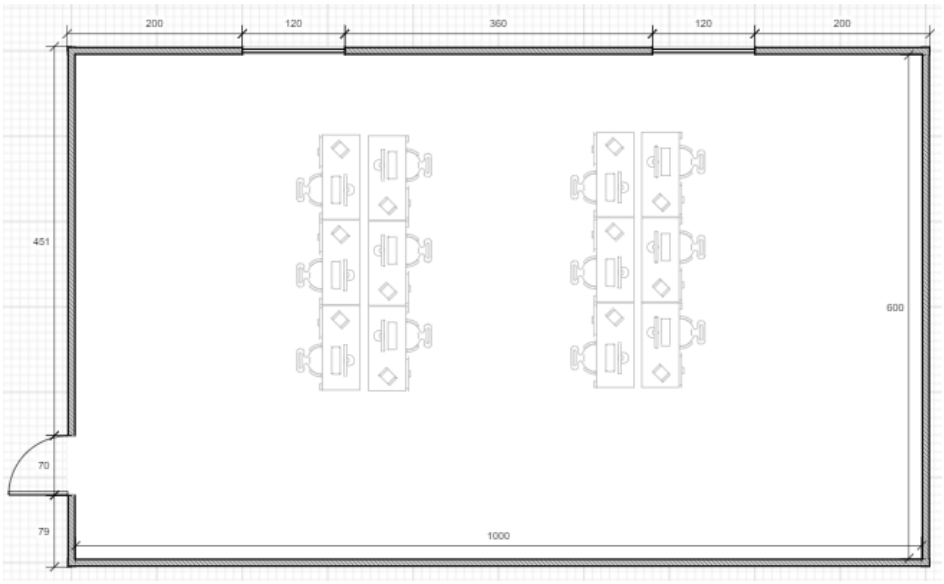
Компьютермен жұмыс кезінде бағдарламашы қауіпті және зиянды факторларға ұшырайды. Бағдарламалаушының компьютермен жұмыс істеу процесі бағдарламашының өнімділігі үшін өте маңызды. Басқа жағдайда, қызметкерлер айтарлықтай визуалды стрессті сезінеді. Болашақта жұмысқа қанағаттанбауға, бас ауруына, шаршағыштыққа және тітіркенуге әкеледі.

3.1.1 Жұмыс орнының сипаттамасы

Кеңсені жобалау және құру кезінде ҚР ҚНжЕ 3.02-04-2009 ережелеріне сүйене отырып жасалған.

Кеңсе бір жұмыс орнына жабдықталған. Кеңсе Жібек жолы, 142/2 ғимаратының 3-ші қабатында орналасқан.

Бағдарламалық қамтамасыз етуді әзірлеу жүргізілетін бөлмені қарастырайық (3.1-сурет). Бөлме өлшемдері: ұзындығы (L) = 10 метр, ені (B) = 6 метр, биіктігі (H) = 3,2 метр. Жұмыс орнының жалпы ауданы 60 ш. м. болғандықтан санитарлық талаптарды қанағаттандырады.



Сурет 3.1 - Жұмыс бөлмесінің жоспары

3.1.2 Жерге тұйықтау есебі

Есеп әдістемелік нұсқауларымен жүргізілді. 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.

Топырақтың меншікті	Жерге тұйықтауд	Жерге тұйықтауұз	Жерге тұйықтауо	Жерге тұйықтауара	Жолақтың ені, b, м

кедергісі, Ом*м	иаметрі, d, м	ындығы, L, м	рналасу тереңдігі, h, м	сындағы қашықтық,	
300	0,05	2,0	0,7	6,0	0,02

Кесте 3.1 - Жерге тұйықтау есебі үшін бастапқы деректер

Бір жерге тұйықтаукедергісі мына формула бойынша анықталады:

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

мұндағы Rтк - жерге тұйықтаукедергісі;

ρ – топырақтың меншікті кедергісі;

L – жерге тұйықтауұзындығы;

t – жерге тұйықтауорналасу тереңдігі;

d – жерге тұйықтаудиаметрі.

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

Жерге тұйықтаусаны мына формуламен есептеледі:

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

мұндағы, n - жерге тұйықтаусаны;

Rтк - жерге тұйықтаукедергісі;

Rнк - нормалар бойынша жерге тұйықтаукедергісі (4 Ом).

Жерге тұйықтауарасындағы қашықтық мынадай формула бойынша есептеледі:

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

мұндағы, а - жерге тұйықтауарақашықтық;

L - жерге тұйықтауұзындығы.

$$a = 2 * 3 = 6 \text{ м}$$

Олардың өзара экрандалуын ескере отырып, жерге тұйықтаусаны мынадай формула бойынша анықталады:

$$\text{n}_\text{Э} = n/\eta_{\text{жс}} \quad (4.4)$$

мұндағы, $\text{n}_\text{Э}$ - өзара экрандалуын ескергендегі жерге тұйықтаусаны;

n - өзара экрандалуын ескермегендегі жерге тұйықтаусаны;

$\eta_{\text{жс}}$ - жерге тұйықтауөзара экрандалуын ескеретін пайдалану коэффициенті.

$n\text{э} = 4/0{,}88 = 5$

жерге тұйықтауөткізгіштерінің ұзындығы мынадай формула бойынша анықталады:

$$Ln = 1{,}05 * a * n_э \qquad (4.5)$$

мұндағы, Ln – жерге тұйықтауөткізгіштердің ұзындығы;
a - жерге тұйықтауарақашықтығы;
$n_э$ - өзара экрандалуын ескергендегі жерге тұйықтаусаны;

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

жерге тұйықтауөткізгішінің кедергісі мынадай формула бойынша болады:

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

мұндағы, Rж -жолақтық болаттан жасалған жерге тұйықтауөткізгішінің кедергісі;
Ln - жерге тұйықтауөткізгіштердің ұзындығы;
b - жерге тұйықтауөткізгіш жолағының ені;
t - жерге тұйықтауорналасу тереңдігі.

Rж = 300 * (lg (2 * 31,5 / 0,02 * 0,7)) / 2,5 * 3,14 * 2 = 30,03 Ом

Барлық токтың ағуына кедергі жерге тұйықтауқұрылғысының мынадай формула бойынша есептеледі:

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

мұндағы Rжт - барлық жерге тұйықтаутокқа ағу кедергісі.

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

жерге тұйықтаунақты саны мынадай формула бойынша анықтадым:

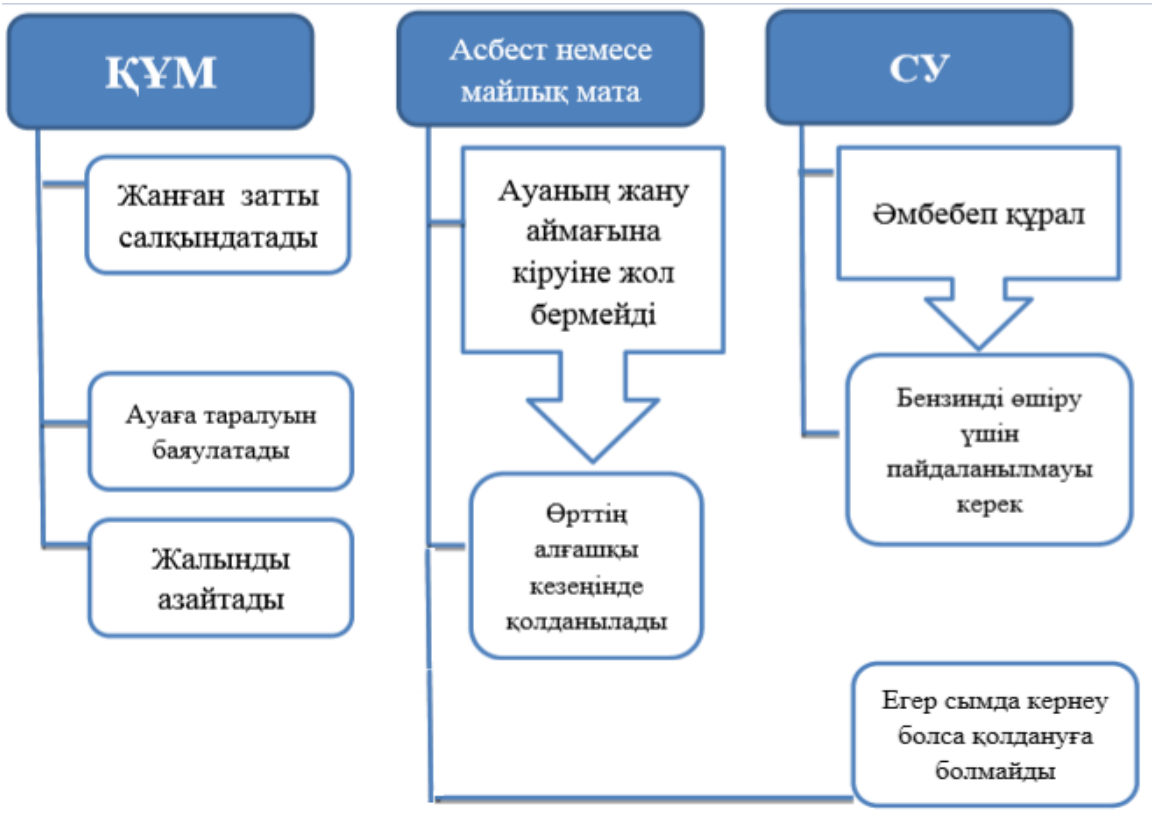
$$n = R\text{ж} / \eta\text{жс} * R\text{жт} \qquad (4.8)$$

мұндағы, n - жерге тұйықтау нақты саны.

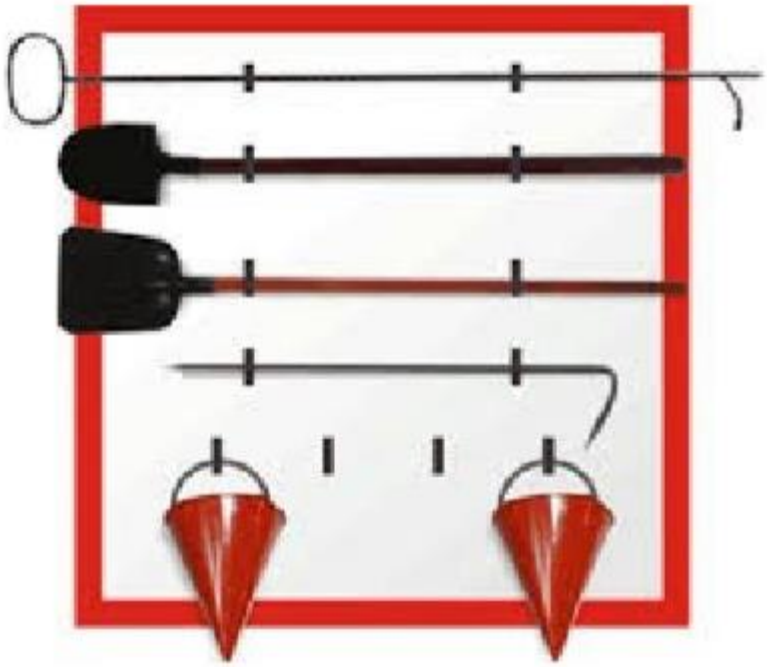
$$n = 15{,}57 / (0{,}88 * 3{,}41) = 5$$

3.1.3 Алғашқы өрт сөндіру құралдарына қажеттілікті есептеу

Өртке қарсы құралдарды міндетті түрде қолдану қажеттілігін анықтайтын күрделі технологиялық жабдықтармен және өртке қауіпті материалдармен және ғимараттар мен ғимараттардың өрт қаупі бар материалдарымен толтыру кезінде бастапқы өрт сөндіру қондырғыларын білу және оларды пайдалану тәртібі, сондай-ақ оларды пайдалану тәртібі газ өрт сөндіруде ерекше маңызды болып табылады. Өндірістік, әкімшілік, көмекші және қоймалық ғимараттар, ғимараттар мен үй-жайлар, сондай-ақ ашық өндірістік алаңдар немесе аудандар өнеркәсіп өрт қауіпсіздігі ережелерімен белгіленген қолданыстағы ережелерге сәйкес бастапқы өрт сөндіру жабдықтарымен қамтамасыз етілуге тиіс. Алғашқы өрт сөндіру жабдықтары портативті және жылжымалы өрт сөндіргіштері, өрт гидранттарының жабдықтары, ұнтақ композициялары бар қораптар (құм, перлит және т.б.), сондай-ақ отқа төзімді маталар (асбест матасы, киіз матасы, киіз және т.б.) қамтиды. Егер өрт отпен күресу үшін осы құралдардың көмегімен өздігінен өрт алмайтын болса; әрдайым, өрт сөндіру бригадаларының жауынгерлік экипаждары өрт сөндіру және адамдарды босату үшін жылжымалы құралдармен қаруланған құтқаруға келеді; жабдықтарды, қорғаныс құралдарын және кең ауқымды тәжірибені қамтиды.



Сурет 3.2 – Өрт сөндірудің қарапайым құралдары



Сурет 3.3 – Өрттен қорғану құралдары

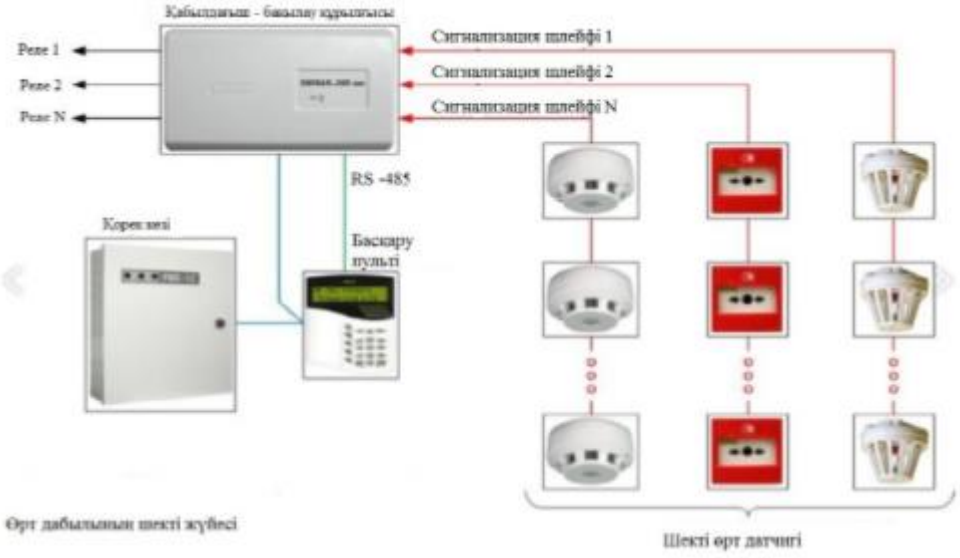
Қазіргі заманғы Қазақтандық нарықта өрт сөндіру жүйелері көпшілікпен ұсынылған. Сондай-ақ, сапа, функционалдылық және бағалар бойынша өртке қарсы дабыл жүйелерін құруға қабілетті ұйымдардың саны жеткілікті. Бұл қызмет тұтынушылар арасында жоғары сұранысқа ие. Өрттің пайда болуы туралы иелеріне ескерту жасау үшін, қазірдің өзінде көптеген құрылғылар қолданылуы мүмкін. Бұл түтін детекторлары, ашық жалын детекторлары және жылу детекторлары. Ықтимал өрттен мүмкіндігінше өздерін қорғау үшін жеке үйлердің иелеріне барлық осы құрылғыларды орнату ұсынылады. Түтін датчигі - жану өнімдеріне (түтінге) жауап береді және моделіне байланысты инфрақызыл, ультракүлгін немесе көрінетін спектрлерде жұмыс істейді. Айтпақшы, мұндай сенсорлармен жабдықталған детекторлар әкімшілік және тұрмыстық объектілерді қорғау үшін қолданылуы тиіс.

Кесте 3.2 - Түтін датчиктерінің санын есептеу келесі кесте негізінде жүргізілуі тиіс деректер

Бөлменің биіктігі, м	Сәуленің биіктігі, D,м	Датчиктер арасындағы максималды Егер сымда кернеу болса қолдануға болмайды арақашықтық, М, м
3 м-ге дейін	0,1 – ден астам	2,3

4 м-ге дейін	0,1 – ден астам	2,8
5 м-ге дейін	0,1 – ден астам	3
6 м – ге дейін	0,1 – ден астам	3,3
12 м- ге дейін	0,1 – ден астам	5

Біз сенсорларды шамамен 3м биіктікте орнатамыз, бір датчикке қызмет көрсететін алаң шамамен 18 шаршы метрді құрайды. Тек 2 датчикті орнатуға болады, бірақ содан кейін қабырғаларға дейінгі қашықтық тым үлкен болады. Біз кестеге сәйкес қажетті орындарды таңдаймыз. Біздің жағдайда бұл құрылғылар арасындағы қашықтық 2,3 метрден аз болады. Белгілі бір объектіге қандай да бір датчиктерді орнату керек, ол 1кестеде «қорғалатын үй-жайдың мақсаттарына және өрттің түріне байланысты өрт хабарлағыштарының түрлерін таңдау» кестесінде жеткілікті түрде сипатталған. Және бұл, әдетте, ешқандай проблемалар жоқ. Бірақ нүкте детекторларын дұрыс орнату үшін, барлық талаптарды сақтай отырып, қажетті қашықтықты ұстап тұру - жиі бірқатар сұрақтар туындайды. Биіктігі неғұрлым жоғары болса, бақыланатын аймақ соғұрлым аз болады және датчиктердің бір-біріне жақын қашықтығы - 13-тармақты қарап «Өрт қауіпсіздігі жүйесі» SP 5.13.130.2009. Орнатылған өрт хабарлағыштары жарылғыш нүктені жылдам анықтауға және тұрғындарға және өрт бөліміне қауіп төндіреді. Құрылғының тиімді жұмыс істеуі үшін алдымен қажетті есептеулерді дұрыс жасап, диаграмманы құрастырыңыз, ол бүкіл жүйені орнату үшін пайдаланылады. Детекторларды орнату бойынша дайындалған жобаға ие бола отырып, пәтерде болашақ өрт хабарлағышы үшін тиісті бағалауды жасап, тиісті жабдықты таңдауға болады. Сигналдың ерекшеліктеріне қарай ол үш түрге бөлінеді: - шекті мән; - мекен-жайы; - аналогтық адрес. Өрт сигнализациясының жүйесі бөлменің сипаттамаларына байланысты.



Сурет 3.4 – Өрт сигнализациясының жүйесі

Шекті дабылдың жұмыс істеу принципі кез-келген сенсордан сигнал алынған кезде бүкіл жүйенің жалпы жауапына негізделген. Сондықтан, тұтану көзінің оқшауланuын дәл анықтау үшін бұл сәтті болмайды. Бірақ кішігірім ауданы бар пәтерге арналған бұл құрылғы жақсы таңдау болып табылады және оны қолдану оңай. Өрт сөндіргіш - сақтандырылған өрт сөндіру агентінің шығарылуына байланысты өртті сөндіруге арналған портативті немесе мобильді құрылғы. Қолмен өрт сөндіргіш, әдетте, шашатын немесе түтікшесі бар қызыл цилиндр цилиндр болып табылады. Өрт сөндіргіші іске қосылған кезде, өрт сөндіруге қабілетті зат жоғары қысымда оның саптамасынан пайда болады. Мұндай зат көбік, су, ұнтақ түріндегі кез келген химиялық қосылыс, сондай-ақ көміртегі диоксиді, азот және басқа да химиялық инертті газдар болуы мүмкін.

Сурет 3.5 – Оп-5 оттегі өрт сөндіргіш

Бізге офиске ұнтақты өрт сөндіргішті таңдадық. Кез келген үй-жайда, соның ішінде кеңселерде, кеңсе ғимараттарында, қоймаларда және өндірістік цехтарда ұнтақты өрт сөндіргіш -40-тан +50 ° С-қа дейін қолдануға болады. Қорғалатын аумақтың көлемі ұнтақты өртсөндіргіш көлеміне байланысты. Егер өрт сөндіргіш ОП-2 деп белгіленсе, онда орта есеппен қорғалатын аумақ 20 м2 болады, ОП-5 болса, тиісінше 50 м^2. Ұнтақты өртсөндіргіш заряд массасы 0,5-тен 100 кг-ға дейін, ұнтақты шығарудың ұзындығы 2-6 метр, жұмыс уақыты 6-30 секунд болуы мүмкін.

3.1.4 Қорытынды

Бұл бөлімде жұмыс орнындағы еңбек жағдайына талдау жасалды, атап айтқанда жерге тұйықтау және алғашқы өрт сөндіру құралдарына қажеттіліктіесебі. Біздің жағдайымызда 60 м^2 болғандықтан ОП-5 ұнтақты өрт сөндіргішін таңдап алдық. Бөлме толықтай жерлендірілген. Енді құрылғылар зақымдалған жағдайда электр тогы адамның бойына емес, жерге соғады.

4. Жобалық тәуекелдерді бағалау

4.1 Тәуекелді талдау және бағалау

Дипломдық жұмыстың осы бөлігінде біз кәсіпорынның ақпараттық қауіпсіздік шараларын бағалаймыз. Ақпараттық қауіпсіздікте "тәуекел" ұғымы "қауіп" және "осалдық"ұғымдарымен тікелей байланысты. Осалдық-бұл ақпараттық жүйенің жұмысындағы, оның архитектурасындағы немесе жүйеге/процеске әсер ететін немесе тәуелді және қауіп-қатерлермен пайдаланылуы мүмкін үдерістегі кемшілікті атайды. Қауіпті осалдықтарды іске асыру көзі ретінде анықтауға болады.

АҚ тәуекелдерін бағалау оларды іске асыру кезінде келтірілген сәйкестендірілген қауіптердің, осалдықтар мен залалдың негізінде жүргізіледі. Тәуекелдерді бағалау қажеттілігі бірінші кезекте олардың компанияның бизнес процестеріне әсер ету дәрежесін анықтаумен, оларды іске асырудан болған қандай да бір шығындардың (залалдың) мөлшерін бағалаумен және оларды барынша азайту немесе болдырмау тетіктерін әзірлеумен байланысты.

Ақпараттық ресурстар — активтер)-компания процестері шеңберінде оның өмірлік циклінің барлық кезеңдерінде ақпаратты өңдеу үшін қолданылатын ақпарат және оны өңдеу құралдары (бағдарламалық-аппараттық кешендер). Тәуекелдерді бағалау үшін біз компаниядағы ақпараттық ресурстарды анықтаймыз, содан кейін оларды түгендеу мен жіктеуді жүргіземіз. Компанияның негізгі қызметін жүзеге асыруға қатысатын барлық ақпараттық ресурстары түгендеуге жататынын атап өту қажет.

Ақпараттық ресурстарға түгендеу кезінде олардың иелеріне, тағайындалуына, бірегей қасиеттеріне, орналасуына және т. б. қатысты ақпаратты қамтитын атрибуттар жиынтығы беріледі. Тұтастық пен қол жетімділікті жіктеу мәндерінің бірыңғай шкаласы компанияның барлық ақпараттық ресурстары үшін енгізіледі. Ақпараттық ресурстар санаттарын беру қажетті жеткіліктілік қағидаттарына сүйене отырып жүргізілуі тиіс, өйткені ақпараттық ресурстарды түгендеу және санаттау процесі циклді және ақпаратты өңдеу, беру, сақтау жүйесінің қоршаған/мазмұнының кез келген маңызды өзгеруіне байланысты. Ақпараттық ресурстарды түгендеу және жіктеу нәтижесінде біз оларға қойылатын

ресурстар мен талаптар туралы ақпарат бар тізілімді аламыз. Маңызды объектілердің тәуекелдерін есептеу үшін бағалау әдістемесі қолданылды.

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

Екіншісінде-сол шкала бойынша әр қауіптің іске асырылу ықтималдығы 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.

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.

Қауіптің туындау ықтималдығы шкаласы	
Ықтималдылық деңгейі	Қауіптің туындау ықтималдығы
1 – өте төмен	10 жылда 2-3 рет
2 - төмен	5 жылда бірнеше рет
3 - орташа	Жылына бірнеше рет
4 - жоғары	Айына 1 рет
5 – өте жоғары	Айына бірнеше рет

4.1 кесте – Қауіптің туындау ықтималдығы шкаласы

Келесі кестеде деңгейлер бойынша тәуекел салдарының шамасы көрсетілген.

Шығын көлемінің шкаласы	
Мәні	Сипаттамасы
1 – өте төмен	50000тг дейінгі баға
2 - төмен	200000тг дейінгі баға
3 - орта	500000тг дейінгі баға
4 - жоғары	1000000тг дейінгі баға
5 – өте жоғары	1000000тг жоғары баға

4.2 кесте – Шығын көлемінің шкаласы

Дипломдық жұмысты орындау барысында активтер тізімі жинақталды оларға:

- Жұмыс машиналары
- Коммутатор
- Маршрутизатор
- Желіаралық экран
- Сервер

4.3 кесте – Тәуекелдерді бағалаудың қорытынды кестесі

	Қауіптер	Осалдылықтар	Тәуекелдің ең жоғары деңгейі	Сипаттамасы	Тәуекелдің қалдық деңгейі
	1 Жұмыс машиналары				
.1	Құжаттар немесе ақпараттың жоғалуы	Көшіруге бағынушылық		Ақпаратты көшіруден қорғау	
.2	Жүйелік қателіктер	Істен шығаруға бағытталған шабуылдар		Шабуылдарды анықтау жүйесі	
.3	Деректерді бұрмалау	Ақпаратпен жұмыс жасағанда ережелердің сақталмауы, немқұрайлылық		Рұқсатсызқол жеткізуден қорғау	
.4	Дұшпандық апплеттер мен вирустар	Қауіпті бағдарламалардыңорнатылуы		Вирусқа қарсы бағдарламалық жасақты пайдаланылу	
	2 Маршрутизатор				
.1	Қызмет көрсетуден бастарату	Желілік жабдықтарды нормаланбаған ұйымдастыру, алыстан ажырату		Кіруді анықтау жүйесі, жүйені резервтік қалпына келтіру	

.2	Деректерді бұрмалау	Қайтарылатын деректерді тексерудің болмауы, қолжетімділікті шектеудің дұрыс болмауы		Конфигурация элементтеріне рұқсатсыз кіруден қорғау; жүйені резервтік қалпына келтіру	
.3	Белсенді желілік компоненттердің дұрыс емес конфигурациялары.	IP-мекенжайын ауыстыру мүмкіндігі		OS басқаруымен TCP / IP желілік сервистерін теңшеу	
.4	Бақыланбайтын көшіру	Зиянды бағдарламалар мен сайттарды өткізу үшін сүзу параметрлері		Зиянды бағдарламалар мен сайттарды өткізу үшін сүзу параметрлері	
	3 Сервер				
.1	Серверді басқаруға рұқсат етілмеген алу	Дұрыс үлестіріомеген қол жеткізу құқығы		Рұқсатсыз кіруді жүзеге асыру мүмкіндігін болдырмайды	
.2	Жабдықтың істен шығуы	Үздіксіздік жоспарлары алынды		Басып кіруді анықтау жүйесі, жүйені резервтік қалпына келтіру	
.3	Деректер қорына бағытталған шабуыл	Жүйелік кодтың осалдылығы		АҚ саясаты желі экраныны сүзгілеу.	
.4	Серверлік кеңейтулерді енгізу	Пайдаланушы ұсынған деректерді сервер түсіндіретін файлда сақтамас бұрын тексерудің болмауы.		Рұқсат етілмеген кіру мүмкіндігін болдырмайды	
	4 Желіаралық қалқан				
.1	Брандмауэрге рұқсатсыз кіру	Қауіпсіздік саясатын дұрыс орнатпау, жүйе әкімшісінің қателері		Деректер конфигурациясы және жүйелік қауіпсіздік саясаты	

.2	Зиянды БҚ (вирустар)	Құрылғыға арнайы құрылған қосымшаларды жіберу және еркін кодты қашықтан орындау мүмкіндігі.		Желіаралық экрандарды туннелдеуді орнату, ОЖ жаңартуын орнату.	
.3	Зиянды орындалатын командаларады ендіру осалдылығы.	Басқару деңгейіндегі ақпараттарды өшіру.		АҚЖ саясатын орнату, ақпараттарды сүзгілеу.	
.4	Бағытталған шабуылдар	Жүйенің осалдылығын пайдалану.		Жаңартулар орнату, осалдылықтарды алдын алу.	
	5 Коммутатор				
.1	Қызмет көрсетуден бастарату	Желілік жабдықтарды нормаланбаған ұйымдастыру, алыстан ажырату.		Кіруді анықтау жүйесі, жүйені резервтік қалпына келтіру.	
.2	Жүйелік қателіктер	Істен шығаруға бағытталған шабуылдар.		Шабуылдарды анықтау жүйесі.	
.3	Құрылғы жүйесіне зиянды қосымшалар орнату	Жүйе осалдылығын пайдаланып, зиянды қосымшалар орнату.		Реттелген жаңарту жабдықтамалары ұжымдастыру.	
.4	Белсенді желілік компоненттердің дұрыс емес конфигурациялары.	IP-мекенжайын ауыстыру мүмкіндігі.		OS басқаруымен TCP / IP желілік сервистерін теңшеу.	

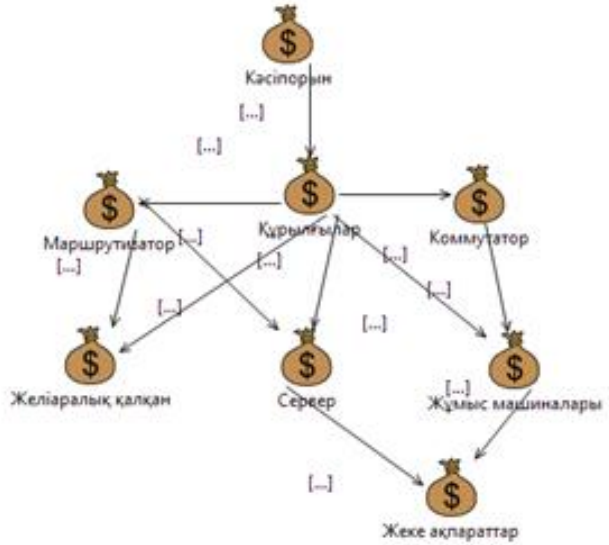
Бастапқы бағалау кезінде тәуекелдер қолайсыз болып шықты (7-ден 9-ға дейін 10 балдық шкала бойынша), сондықтан барлық тәуекелдер үшін қорғау шаралары сипатталған. Тәуекелдерді өңдеу үшін шаралар енгізілгеннен кейін тәуекелдер қайта есептелді, қалдық тәуекелдер алынды. Қорғау шараларын ескере отырып, қайта есептеуден кейін қалған барлық тәуекелдер қолайлы болды (1-ден 6-ға дейін 10 балдық шкала бойынша).

Бұдан әрі CORAS бағдарламасында іске асырылған тәуекелдерді талдау компоненттерінің өзара байланысының әртүрлі диаграммалары ұсынылған (тәуекелдерді талдаудың жоғарыда көрсетілген кестесі негізінде).

4.2 CORAS құралымен тәуекелдерді талдау

CORAS – бұл тәуекелді модельдеу арқылы талдау нәтижелері туралы есептерді жасауға мүмкіндік беретін компьютерлік құрал.

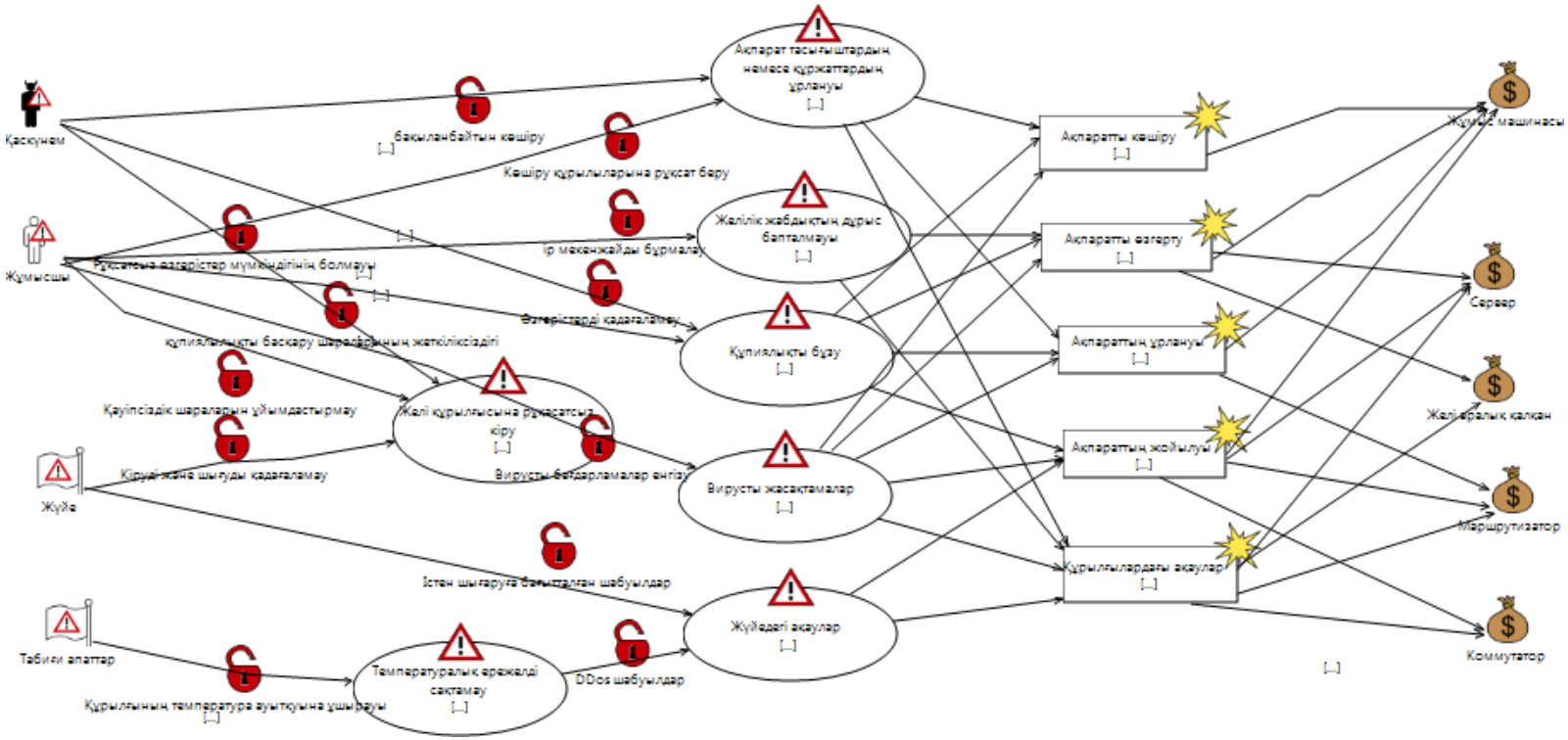
Тәуекелдерді талдаудың үшін Coras бағдарламалық құралдарын пайдаланылды. Жоғарыда сипатталған активтер диаграммасын және олардың арасындағы байланысты жасады (5.1 сурет). Бағдарламалық жасақтамада қорғауға жататын құндылықты (ақпаратты) білдіретін Asset элементі пайдаланылады.



4.1 сурет – Акттивтер диаграммасы

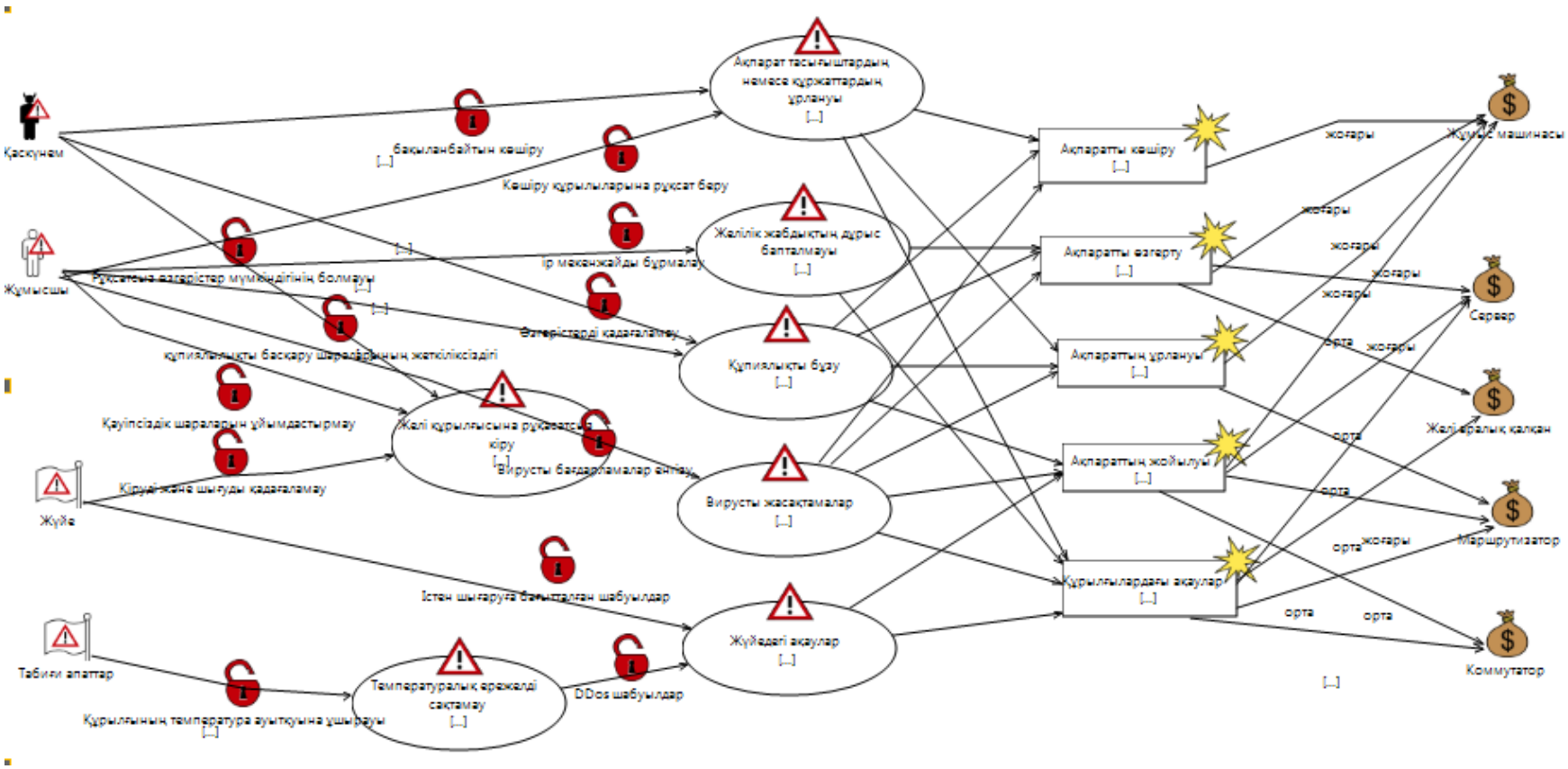
- 4.3 кестені қолданып, тәуекелдер диаграммасын құрамыз,бұдан әрі әрбір актив үшін әрбір тәуекел бойынша осы тәуекел жүзеге асырылған жағдайда салдарларды анықтаймыз. Алынған диаграмма 4.2 суретте көрсетілген.

- Адам факторымен байланысты қасақана қауіп-қатерлерді белгілеу үшін Threat Human Accident;
- Адам факторына байланысты қасақана қауіп-қатерлерді белгілеу үшін Threat Human Deliberate;
- Адам факторымен байланысты емес қауіп-қатерлерді белгілеу үшін Threat Non Human;
- Қатерлерді сипаттау үшін Threat Scenario;
- Осалдықтарды сипаттау үшін Vulneravility;
- Жағымсыз оқиғаларды белгілеу үшін Unwanted Incident.



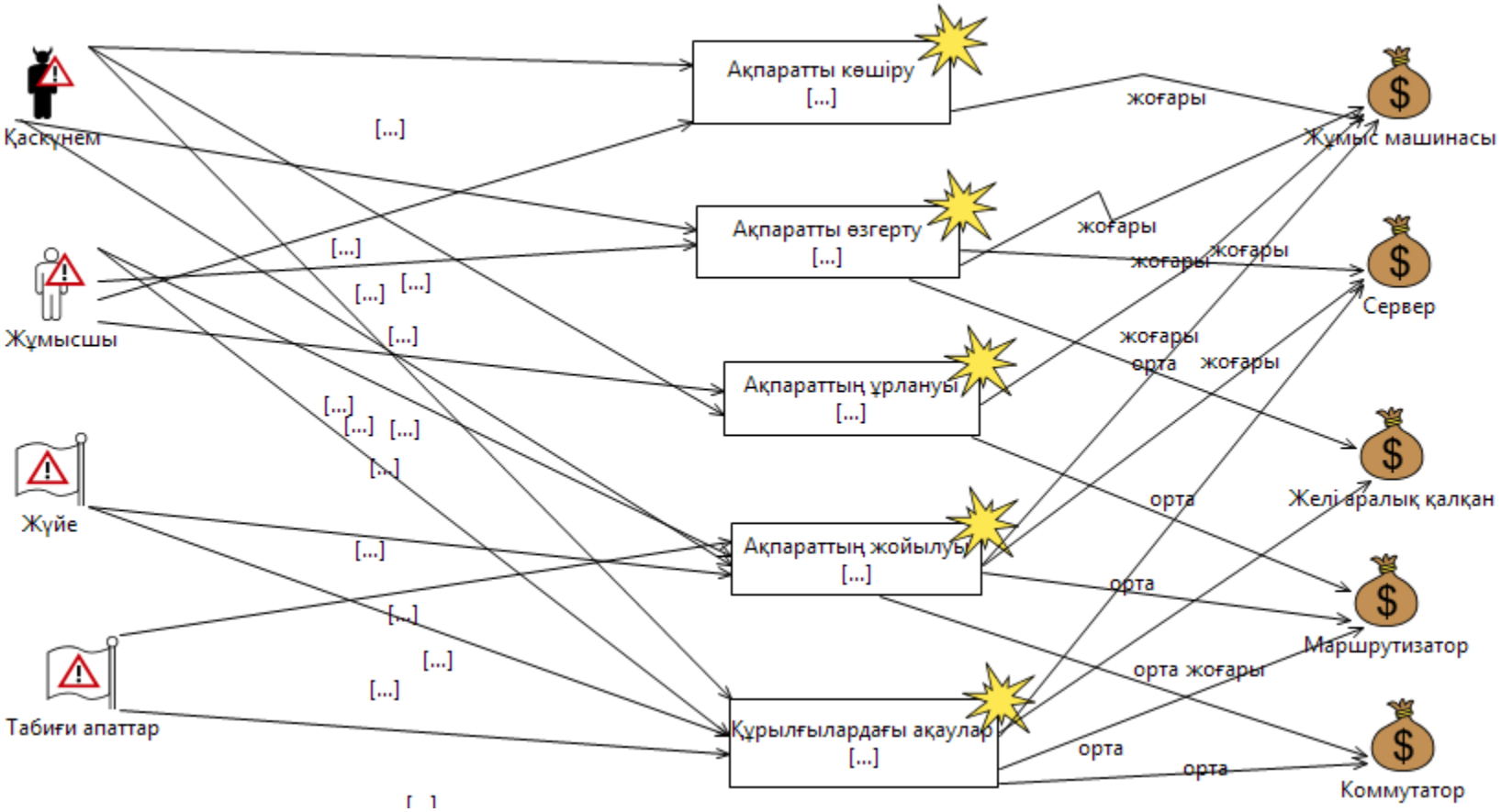
4.2 сурет – Қауіптер моделі

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



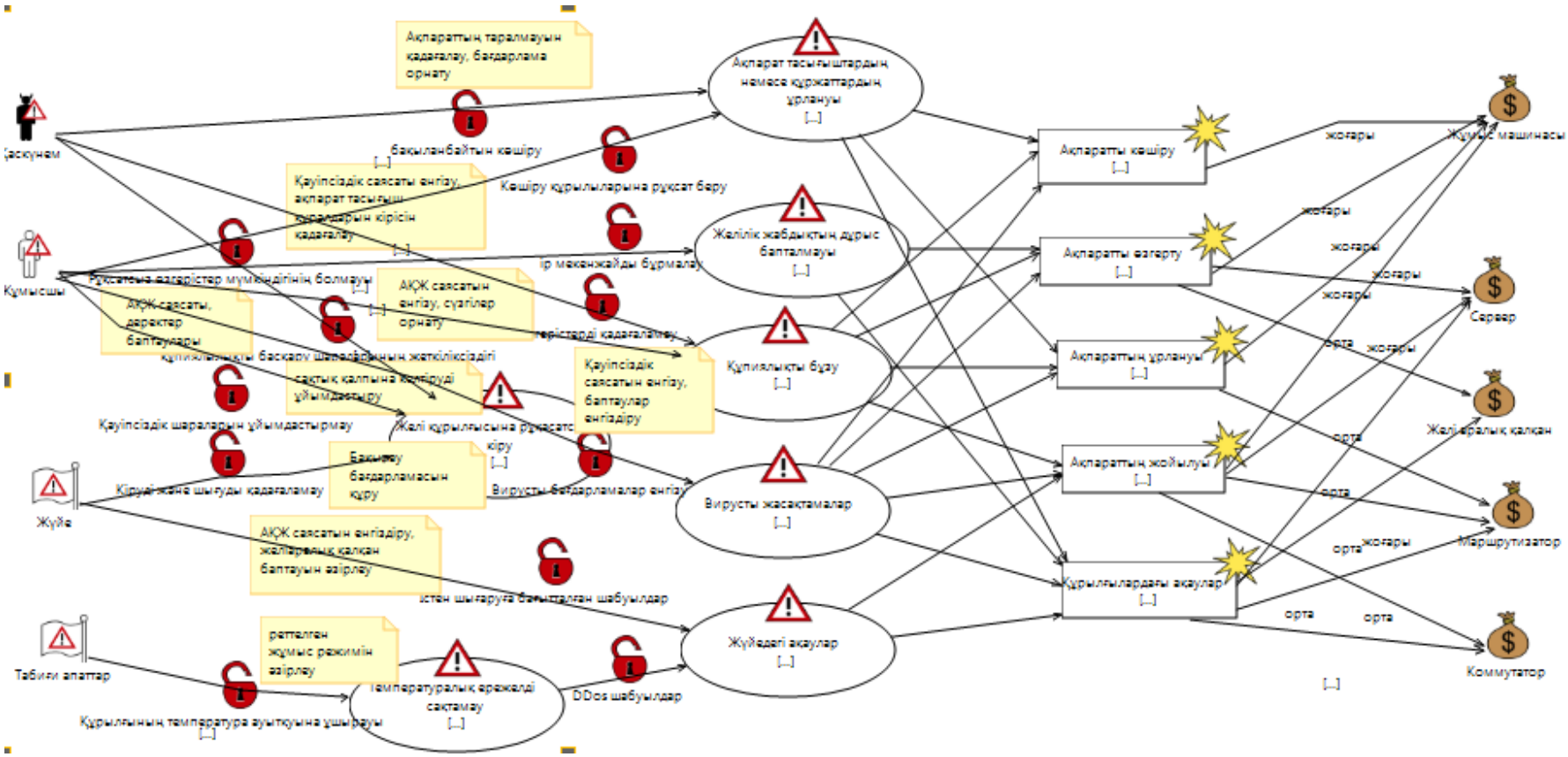
4.3 сурет – Ықтимал сипаттамалары бар қауіптер моделі

Ақпараттық қауіпсіздік инциденті көп чемодин активке немесе активтің бір бөлігіне әсер етуі мүмкін. Әсер инциденттің табысқа байланысты. Ықпал деп қаржылық және нарықтық қорытындыларды қамтитын тікелей (пайдалану)әсері немесе болашақ (бизнес) әсері есептеледі.Бұдан әрі әрбір актив үшін тәуекелдердің әсер ету дәрежесін бағалаймыз (сурет. 4.3)



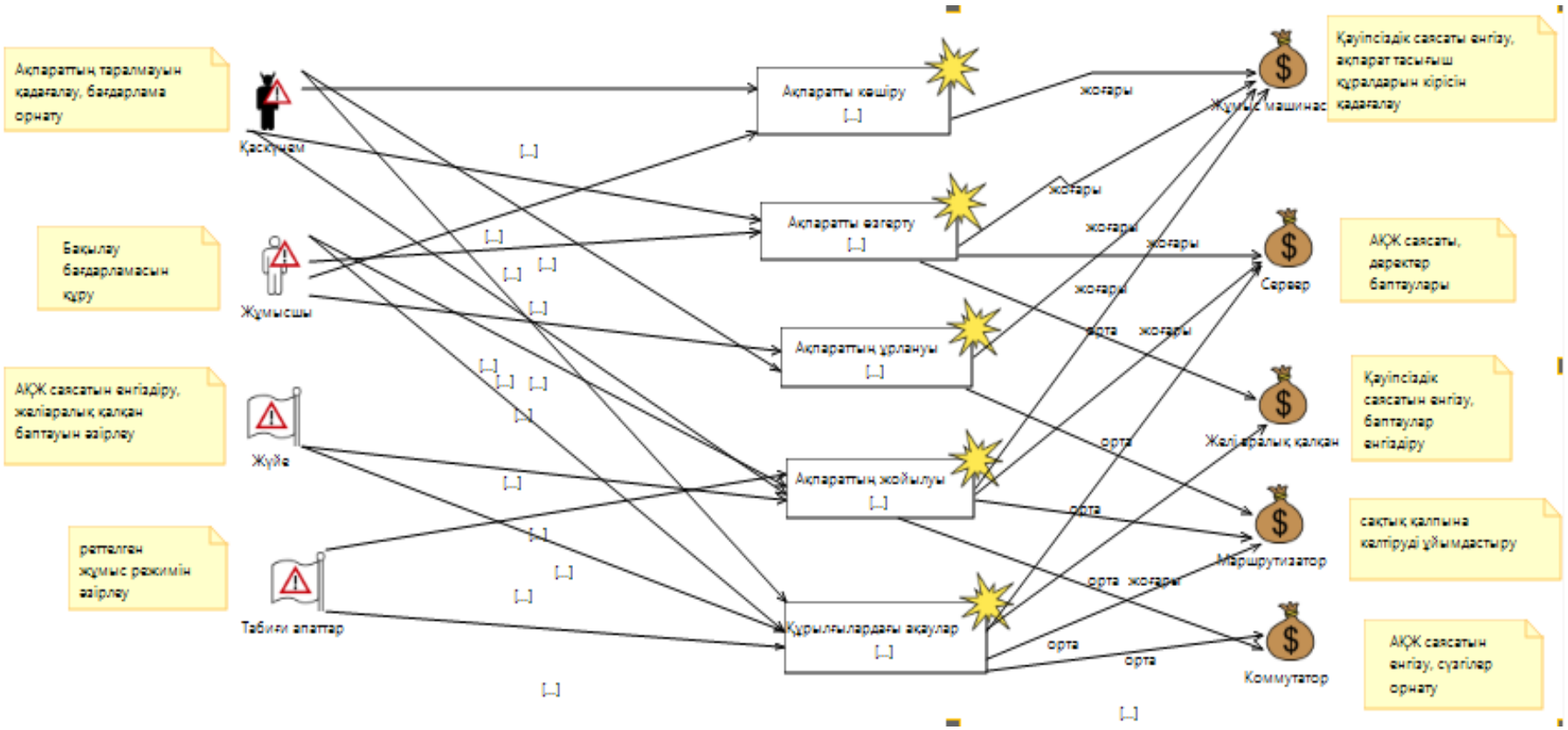
4.4 сурет – Қауіпті жүзеге асыру салдарының сипаттамасы бар тәуекелдер диаграммасы

Шараларды таңдау және нақтылау ақпарат қауіпсіздігіне төнетін қауіп-қатерлерге жүргізілген талдау нәтижелеріне негізделуі тиіс. Бағдарламаның тіршілік циклінің процестерінде осалдықтарының пайда болуын болдырмау және жою мақсатында қауіптерді іске асыруға жататын қорғау шараларының тізбесін анықтаймыз (сурет. 4.4).



4.5 сурет – Қорғау 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 (сурет. 4.5).



4.6 сурет – Қолайсыз тәуекелдер диаграммасы

4.3 Қорытынды

Дипломдық жұмыстың осы бөлігінің мақсаты (тәуекелдерді бағалау) объектіні қорғаудың әзірленетін жүйесі үшін тәуекелдер сипаттамаларын анықтаудан тұрады.

Барлық анықталған ресурстар бойынша тәуекелдерге талдау жүргізілді және ақпараттық жүйені қорғау шаралары анықталды. Тәуекелдерді бағалау үдерісіне арналған негізгі жұмыстар қаралды. Таңдалған активтердің негізгі қатерлері мен осалдықтары қаралды. Тәуекелдерді бағалау екі фактор бойынша есептеу әдісін қолдана отырып жүргізілді.Қорғау шараларын қолдану туралы шешім қабылданды. Содан кейін ұсынылған қорғау шараларын ескере отырып, тәуекелдерге қайта есептеу жүргізілді.Қорғау шараларын енгізгеннен кейін активтердің тәуекелдері (орташа) 2 есе азайтылды.

Қорытынды

Бұл дипломдық жоба жұмысында кәсіпорынның байланыс желісін ұйымдастыру мүмкіндігін eve-ng эмуляторын қолдана отырып жасау қарастырылды. Бүгінгі күні кез-келген кәсіпорынның жетістігі оның бизнес-үдерістеріне тікелей әсер ететін ақпараттың қол жетімділігі мен маңыздылығына байланысты. Маңызды құжаттардың, деректердің уақтылы берілуін және алынуын қамтамасыз ету ұжымдық желінің басты міндеті болып табылады. Дипломдық жұмыстың бірінші бөлімі заманауи ұжымдық желілерді, сондай-ақ оларды қауіп- қатерден қорғау және қорғану шараларының негізгі ерекшеліктерін талдауға арналған. Бүгінгі таңда ұжымды байланыс желісі ақпараттық қызметтердің кең спектрін ұсынуы керек: телефония, бейнеконференция, деректерді беру, кәсіпорынның ортақ ресурстарына қашықтықтан қол жеткізу мүмкіндігі, интернетке қол жеткізу. Сонымен қатар, ұжымдық желі географиялық жағынан бір-бірінен алшақ орналасқан филиалдарды біріктіру мәселесін шешуі керек.

Дипломдық жұмыстың екінші бөлімінде желі eve-ng эмуляторының функционалдығы қарастырылып модельденді, коммуникацияның оңтайлы арнасы өткізілді. Бүгінгі күні бұл бағдарлама әртүрлі коммуникациялық желілерді модельдеуге және модельдеуге арналған қуатты өнім болып табылады. Қолдау көрсетілетін жабдықтардың кең спектрі эмуляторды тек оқу құралы ретінде ғана емес, сонымен қатар бастапқы кезеңде дизайнға арналған бағдарламалық өнім ретінде де пайдалануға мүмкіндік береді. Ұжымдық байланыс желісі үшін ең қолайлы жабдық таңдалды және IP жоспары бар желінің толық құжаттары ұсынылды. Сонымен қатар барлық VLAN тізімдері бапталды.

«Өмір тіршілігінің қауіпсіздігі» бөлімі ұжымды байланыс желісіне қызмет ететін бағдарламашының серверлік бөлмесіндегі жұмыс жағдайларын талдауға арналған. Сонымен қатар, серверлік бөлмелерді ұйымдастырудың барлық негізгі талаптары ескерілді.

Диплом жобасының төртінші бөлімінде тәуекелдерді бағалау үдерісіне арналған негізгі жұмыстар жүргізілді. Таңдалған активтердің негізгі қатерлері мен осалдықтары қарастырылып, тәуекелдерді бағалау екі фактор бойынша есептеу әдісін қолдана отырып жүргізілде келе қорғау шараларын қолдану туралы шешім қабылданды.

Пайдаланылған әдебиеттер

1. В.П.Корячко Д.А.Перепелкин. Корпоративные сети: технологии, протоколы, алгоритмы– М.: Горячая Линия - Телеком, 2011 - б. 220.

2. Олифер В.Г., Олифер Н.А. – Компьютерные сети. Принципы, технологии, протоколы: Учебник для вузов. 2-е изд. СПБ.: Питер, 2003 - б. 958.

3. Особенности создания корпоративной сети. Сазонов И.В., журнал TComm - Телекоммуникации и Транспорт, 2011. С. 106-107.

4. Биячуев Т. А. Безопасность корпоративных сетей — СПБ.: ГУ ИТМО, 2004 - 161 б.

5. 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 б.

6. 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 б.

7. А. Астахов. Искусство управления рисками. GlobalTrust. 2009.

8. R. L. Winkler, Uncertainty in probabilistic risk assessment, Reliability Engineering and System Safety 54 (2–3) (1996), б. 127–132.

9. Методологии управления ИТ-рисками. // www.osp.ru URL: https://www.osp.ru/os/2006/08/3584582/.

10. Bjorn, A.G. (January 2002). CORAS, A Platform for Risk Analysis on Security Critical Systems — Model-based Risk Analysis Targeting Security (www.nr.no/coras).