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

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

ДИПЛОМДЫҚ ЖОБА

Тақырыбы: Компанияның ақпараттық қауіпсіздігіне қатер төндіру мүмкіндігін азайтуды әзірлеу.

Мамандығы: 5В100200 – «Ақпараттық қауіпсіздік жүйелері»
Орындаған: Акуов Ернар Рахатович Тобы: СИБк-16-1
(аты-жөні)
Ғылыми жетекші: т.ғ.д., профессор Якубова Мубарак Захидовна
(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 Бегимбаева 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 жүйелері және ақпараттық технологиялар институты
Ақпараттық қауіпсіздік жүйелері кафедрасы
5В100200 – «Ақпараттық қауіпсіздік жүйелері» мамандығы

Дипломдық жобаны орындауға берілген

ТАПСЫРМА

Студент: Акуов Ернар Рахатович
(аты-жөні)

Жобаның тақырыбы: Компанияның ақпараттық қауіпсіздігіне қатер төндіру мүмкіндігін азайтуды әзірлеу.

2020 ж. «30» сәуір №56 университет бұйрығымен бекітілді.

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

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

Жобада ақпараттық қауіпсіздік жүйесінің талдауы жасалды және VipNet кешені, антивирустық қорғау сияқты компанияның ақпараттық ресурстарын қорғаудың қазіргі заманғы құралдарын қолдану түсіндірілді. Ерекшілігі бұл жобада ақпараттық қауіпсіздіктің күн сайын артып келе жатқан қаупі жаңа шаралар мен қорғау кешендерінің пайда болуына және жасалуына алып келеді.

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

1. Ақпараттық қауіпсіздік қатерлерінің негізгі түрлері.
2. Ақпараттық қауіпсіздік қатерден қорғау әдістері мен құралдары.
3. АҚ қауіп-қатерін төмендету жөніндегі шаралар кешенін әзірлеу.
4. VPN шешімдері.
5. Өмір тіршілігінің қауіпсіздігі.
6. Жобаның тәуекелін бағалау.

Графикалық материалдардың (міндетті түрде дайындалатын сызбаларды көрсету) тізімі:

2.1 сурет – Firewall сұлбасы.

2.2 сурет – Ernst&Young компаниясының зерттеу қорытындысы бойынша бизнеске қауіп-қатерлерді жіктеу.

2.3 сурет – Корпоративтік желінің функционалдық моделі.

2.4 сурет – VPN технологиясына негізделген аумақтық-бөлінген ақпараттық жүйе.

2.5 сурет – Желі-желі сұлбасының қосылуы.

2.6 сурет – VPN желісіне екі стационарлық компьютерді қосу.

2.7 сурет – Қашықтағы пайдаланушыны VPN желісіне қосу.

2.8 сурет – Компания желісінің схемасы.

Негізгі ұсынылатын әдебиеттер:

1. Фратто М. Секреты виртуальных частных сетей// Сети и системы связи. – 1998. - №3 (25).

2. Развертывание сети ViPNet. Руководство администратора. – М.: ОАО «Инфотекс, 2011. URL: http://www.infotecs.ru.

3. 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	Якубова М.З.		
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. Ақпараттық қауіпсіздік қатерлерінің негізгі түрлері	18.02.20 – 10.03.20	орындалды
1.1. Құпиялықты бұзу қаупі	18.02.20 – 10.02.20	орындалды
2. Ақпараттық қауіпсіздік қатерден қорғау әдістері мен құралдарын талдау	12.03.20 – 24.03.20	орындалды
3. АҚ қауіп-қатерін төмендету жөніндегі шаралар кешенін әзірлеу	26.03.20 – 15.04.20	орындалды
4. Өмір тіршілігінің қауіпсіздігі	19.04.20 – 15.05.20	орындалды
4.1. Еңбек жағдайларын талдау	19.04.20 – 15.05.20	орындалды
4.1.1. Жұмыс орнының сипаттамасы	19.04.20 – 02.05.20	орындалды
4.2. Есептеу бөлімі	02.05.20 – 15.05.20	орындалды
5. Ақпараттық қауіпсіздіктің		
тәуекелдерін есептеу	08.05.20 – 28.05.20	орындалды
5.1 Тәуекелдерді талдау және бағалау	08.05.20 – 15.05.20	орындалды
5.2 CORAS құралы арқылы тәуекелдерді талдау	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 _____ (Якубова М.З.)
(қолы) (аты-жөні)

Орындалатын тапсырманы
қабылдаған студент _____ (Акуов Е.Р.)
(қолы) (аты-жөні)

Аңдатпа

Бұл дипломдық жобада компанияның ақпараттық қауіпсіздігіне қатер төндіру мүмкіндігін азайтуды әзірлеу бойынша VipNet бағдарламасы орнатылды және PacketTracer бағдарламасында VPN желілерінің моделі жасалды, сондай-ақ әртүрлі шаралар арқылы компанияның ақпараттық қауіпсіздігін қамтамасыз ету негізгі мақсат болды. Жобада ақпараттық қауіпсіздік жүйесінің талдауы жасалды және VipNet кешені, антивирустық қорғау сияқты компанияның ақпараттық ресурстарын қорғаудың қазіргі заманғы құралдарын қолдану түсіндірілді.

Дипломдық жоба тақырыбының өзектілігі - ақпараттық қауіпсіздіктің күн сайын артып келе жатқан қаупі жаңа шаралар мен қорғау кешендерінің пайда болуына және жасалуына алып келеді.

Аннотация

В данном дипломном проекте установлена программа VipNet по разработке снижения возможности угрозы информационной безопасности компании и разработана модель VPN сетей в программе PacketTracer, а также основной целью стало обеспечение информационной безопасности компании посредством различных мероприятий. В проекте проведен анализ системы информационной безопасности и разъяснено применение современных средств защиты информационных ресурсов компании, таких как комплекс VipNet, антивирусная защита.

Актуальность темы дипломного проекта - ежедневный возрастающий риск информационной безопасности приводит к появлению и созданию новых мер и защитных комплексов.

Annotation

In this diploma project, the VipNet program was installed to reduce the possibility of a threat to the company's information security, and a model of VPN networks was developed in the PacketTracer program, as well as the main goal was to ensure the company's information security through various activities. The project analyzes the information security system and explains the use of modern means of protecting the company's information resources, such as the VipNet complex and antivirus protection.

The relevance of the topic of the diploma project - the daily increasing risk of information security leads to the emergence and creation of new measures and protective complexes.

Мазмұны

Кіріспе

Бүгінгі күні ақпаратты қорғау саласындағы маңызды мәселелердің бірі ақпараттық қауіпсіздікті қамтамасыз етудің тиімді әдістері мен құралдарын құру болып табылады.

Дипломдық жоба тақырыбының өзектілігі-ақпараттық қауіпсіздіктің күн сайын артып келе жатқан қаупі жаңа шаралар мен қорғау кешендерінің пайда болуына және жасалуына алып келеді.

Дипломдық жобаның жаңалығы VipNet кешені, антивирустық қорғау сияқты компанияның ақпараттық ресурстарын қорғаудың қазіргі заманғы құралдарын қолдану болып табылады.

Дипломдық жобаның мақсаты VipNet бағдарламалық кешенін, сондай-ақ компанияның ақпараттық қауіпсіздік қатерін азайту үшін виртуалды жеке желілер технологияларын енгізу және конфигурациялау болып табылады.

Осы мақсатқа жету үшін келесі міндеттерді шешу қажет:

- ақпараттық қауіпсіздік қатерлері туралы түсінік беру;
- желіде қауіп-қатерлерге қарсы күрес әдістерін зерттеу;
- желідегі қауіптерден қорғаудың қолданыстағы бағдарламалық құралдарына талдау жүргізу;
- виртуалды жеке желілер технологиясын пайдаланудың артықшылықтары мен кемшіліктерін анықтау;
- VipNet бағдарламалық кешенін конфигурациялауды жүргізу;
- Packet Tracer ортасында VPN технологиясы бойынша желіні қорғауды модельдеу жүргізу;
- санитарлық-гигиеналық шаралар мен өмір тіршілігінің қауіпсіздігіне талдау жүргізу;
- жобаның ақпараттық қауіпсіздік тәуекелдердің есебін жасау.

1 Ақпараттық қауіпсіздік қатерлерінің негізгі түрлері

Қауіпсіздіктің негізгі қатерлі түрлері болып мыналар бөлінеді [1]:

– құпиялылықтың бұзылуы;
– тұтастықтың бұзылуы;
– қолжетімділіктің бұзылуы;
– қадағалаудың бұзылуы;
– дәлме-дәлдігін бұзу.

Қауіпсіздікке қатысты кез-келген қатер қауіпсіз жүйенің қызметімен байланысты болуы мүмкін, яғни ол құпиялылық, тұтастық, қол жетімділік қызметі болады немесе сәйкесінше қол жетімділік және түпнұсқалық қызметі болады. Сонымен қатар, егер жоғарыда аталған барлық қызмет түрлері ұсынылса, жүйе қорғалған немесе қауіпсіз [2].

Корпоративтік желілерді пайдалану кезінде кездесетін қауіптердің барлық түрлері екі санатқа бөлінеді [2]:

– зиянкес шыққан қауіп;
– ақпараттық жүйенің жұмыс істеу ортасын бұзуды іске асыруға немесе қолдауға байланысты қауіптер.

Шабуыл жасаушы тарапынан болатын қауіптерге мыналар жатады:

– құпия ақпаратты ұстау/жария ету - құпиялылықты бұзу қаупі;
– заңсыз көздерден, олар қалыптастыратын ақпараттан түрлендіру немесе басқаның атынан жалған ақпарат жасау - тұтастықты бұзу қаупі;
– берілген уақытта белгілі бір алушыға ақпаратты қалыптастыру және тарату көзіне қызмет көрсетуден жалған бас тарту - түпнұсқалықтың бұзылу қаупі;
– алушының белгіленген уақытта белгілі бір көзден ақпарат алу/беру фактісін жалған растауы - түпнұсқалықтың бұзылу қаупі;
– ақпараттық жүйеде жұмыс істеу алгоритмдерін рұқсатсыз өзгерту - кез келген базалық қауіп болуы мүмкін.
– ақпараттық жүйенің жұмыс қабілеттілігін бұғаттау - қолжетімділіктің бұзылу қаупі.

Ақпараттық жүйелердің жұмыс істеуінің ішкі ортасын іске асырумен, қолдаумен немесе бұзумен байланысты қатерлерге мыналар жатады:

– қауіпсіздік тұрғысынан дұрыс емес өнімді өткізу және орналастыру;
– өнімді дұрыс емес қолдау және басқару;
– өнімнің жұмыс істеу ортасының бұзылуы.

Егер өнімнің дұрыс іске асырылуының өлшемдері туралы айтатын болсақ, онда ол сенімді аутентификация және авторизация қолданушының болуымен, сондай-ақ осы арнамен және осы жүйенің қалған бөліктері арасында қорғалған байланыс арналарының болуымен қамтамасыз етіледі. Бұл өлшемдер бұзушымен байланысты келтірілген қауіптерді төмендетеді. Сонымен қатар, бастапқы өнімді дұрыс іске асыру оның құрамдас бөліктерін және олар пайдаланатын технологияларды белгілі бір күйге келтіруді білдіреді, бұл осы өнімді дұрыс емес қолдау және әкімшілендіру тәуекелін

төмендетеді. Ең аз артықшылықтармен, сондай-ақ жүйе құрауыштарының арасындағы қорғалған байланыс арналарымен жұмыс істеу принципін пайдалануды шешкенде, сондай-ақ өнімнің жұмыс істеу ортасының бұзылу тәуекелін төмендетуге мүмкіндік береді.

1.1 Құпиялықты бұзу қаупі

Құпиялылық дегеніміз - ақпараттың мұндай қасиеті, егер пайдаланушы санкцияланбаған болса, ақпарат алу мүмкін еместігінен тұрады, яғни, дәл осы қолданушы осы ақпаратты пайдалануға ешқандай артықшылықтары жоқ [1]. Мұндай бағалы ақпаратты сақтау, түрлендіру және қарау тек өзінің қызметтік міндеттері мен өкілеттіктері бойынша оны пайдалана алатын пайдаланушыларға ғана мүмкін болады. Құпиялылық қасиеті ақпаратты пассивті шабуылдардан қорғауды қамтамасыз етуге мүмкіндік береді, олар беретін деректер ағыны аналитикалық зерттеуден тұрады. Бұл сипат ақпарат көзі мен оның мазмұнын анықтауға мүмкіндік бермейді. Құпиялылықты қамтамасыз етудің негізгі тәсіліне пайдаланушының кілттерін пайдалана отырып, ақпаратты шифрлау жатады. Мұндай тәсілмен берілетін ақпараттың мазмұнымен тек осы кілттердің иелері болып табылатын, осы ақпарат көмегімен шифрланған пайдаланушылар ғана таныса алады. Бұл сипатты қамтамасыз ету маңызды құрамдас болып табылады, өйткені ақпараттың тұтастығы мен қол жетімділігінің қасиеттері бұзылғанда, бүліну, ұрлану немесе модификациялау нәтижесінде оны сақталған мұрағаттардан қалпына келтіру оңай болады, ал егер құпиялылықтың бұзылуы орын алса, онда ақпарат жалпыға қол жетімді болады, бұл компания үшін үлкен шығынға әкеп соғады.

Егер ақпараттың құпиялылығын бұзу қаупі туралы айтатын болсақ, онда оларға ұрлауды/көшіруді, сондай-ақ ақпараттың ағып кетуін жатқызуға болады. Құпиялылықты бұзуға бағытталған шабуылдардың негізгі түрлеріне байланыс арналарында пассивті тыңдау және ұстап қалу, сондай-ақ кілттерді ұрлау құқықтарын заңсыз пайдалану жатады. Байланыс желісінде арнаны тыңдау ұстап алудың мысалы болып табылады. Шабуылдың мұндай түрі пассивті әсер болып табылады және берілетін ақпараттың құпиялылығын бұзуға әкелуі мүмкін. Қаскүнемде кілт туралы ақпараттың болуы шифрланған хабарламалардың құпиялылығын бұзуға алып келеді және олардың құпиялылығын бұзады. Қауіпсіздік қатерлерін азайту үшін криптоанализ әдістерін қолдануға болады, бірақ олар әдетте үлкен шығындарды талап етеді. Шығындарды азайту үшін қарапайым схемаларды пайдалануға болады, себебі компания қызметкерлері қауіп-қатерге ұшырайды деп күдіктенбейді. Оларға әлеуметтік инженерия әдістері қолданылуы мүмкін, олар қазіргі уақытта ақпараттық қызметтің барлық салалары үшін үлкен қауіп төндіреді.

1.2 Тұтастықтың бұзылу қаупі

Тұтастық - бұл авторланбаған пайдаланушылардың ақпаратты модификациялаудан тұратын ақпараттың қасиеті [1]. Бұл дұрыс деп кепілдік

беретін кезде ғана құндылығы бар ақпарат түрлерінің көп саны бар. Тұтастықтың қасиеттерін қамтамасыз ету жөніндегі іс-шаралардың негізгі міндеті ақпараттың бүлінбеуі, бүлінбеуі немесе кез келген тәсілмен өзгертілуі туралы хабарламаның модификациясы орын алған фактіні анықтау мүмкіндігі болып табылады. Ақпаратты модификациялау жүйенің ішіндегі ақпараттық ағындарды толық бақылауды немесе басқа объектінің атынан басқа жүйе объектілеріне хабар беру мүмкіндігін білдіреді. Тұтастық қасиеттерін іске асыру үшін электрондық-цифрлық қолтаңбаның әр түрлі түрлерін немесе бір бағыттағы хэш-функцияларды пайдаланады. Тұтастық қасиеттерінің бұзылуының мысалы ретінде ақпарат электрондық пошта хаттарын немесе құжаттарды қолдан жасау, немесе қандай да бір басқа пайдаланушы үшін алдау және өзін беру мақсатында ақпаратты әдейі түрлендіру бола алады, бұл үлкен шығынға әкеп соғады.

1.3 Қол жетімділікті бұзу қаупі

Қол жетімділік - бұл берілген уақыт аралығынан артық күтпей, қауіпсіздік саясаты ережелеріне сәйкес тиісті өкілеттілігі бар, пайдаланушының және/немесе процестің пайдалануынан тұратын ақпараттық жүйе ресурсының қасиеті. Мысалы, ресурс пайдаланушыға қажетті күйде болғанда, пайдаланушыға қажетті жерде және ол оған қажет болған кезде [1]. Яғни, ақпарат пен ақпараттық жүйенің талап бойынша пайдалануға қолжетімділігі мен дайындығын қамтамасыз етуге мүмкіндік береді. Мұндай жағдайда ақпараттың тұрақты қол жетімділігіне және жарамды күйде қолдауға кепілдік берілуі тиіс. Бұзушының мақсаты-шабуыл жасалған объектіде операциялық жүйенің істен шығуына қол жеткізу, демек, жүйенің қалған барлық объектілері үшін осы объектінің ресурстарына қол жеткізу мүмкін емес.

Ақпараттың қолжетімділігіне әкелетін шабуылдардың негізгі түрлері DoS типті шабуылдар (қызмет көрсетуден бас тарту) болып табылады. Олар заңды пайдаланушылар үшін қажетті сәтте ақпаратты пайдалана алмайды. Dos типті шабуылдардың бір түрі DDoS-шабуыл болып табылады. Ол барлық Internet желісі бойынша таратылуымен ерекшеленеді: оны іске асыру рұқсатсыз орталықтандырылған басқарумен зиянды бағдарламалық қызмет көрсету орнатылған тораптардан басталады, ол желі бойынша командамен іске асырылады және зиянды машиналар зардап шегушінің пакеттерімен тастай бастайды. Бүгінгі күні шабуылдардың осы түрінен тиімді қорғаныс жоқ. Мұндай шабуылдардың мысалдары көпшілік WEB-серверге жасалған шабуылдар болып табылады, олар әртүрлі деректерді сақтайды және нәтижесінде оларды істен шығару және сервисті сапалы ұсыну мүмкін емес. Сондай-ақ шабуыл кез келген компанияның WEB-серверіне немесе пошта қызметіне немесе корпоративтік желі шлюзіне оны істен шығару және желіден ажырату мақсатында жіберілуі мүмкін.

1.4 Түпнұсқалықтың бұзылу қаупі

Аутентификация - аутентификация процедурасының көмегімен қамтамасыз етілетін қасиет. Аутентификация - телекоммуникациялық жүйе объектісінің ұсынылған сәйкестендіргішінің осы объектіге тиесілілігі мәніне сәйкестігін тексеруді жүзеге асыратын рәсім [1]. Аутентификация қасиеттерінің бұзылу қаупі ақпаратты жалғау және оның нәтижесін немесе пайдаланушының кейбір іс-әрекеттерін және процесті басқа пайдаланушы үшін беру болып табылады, бұл бөтен құқықтар мен артықшылықтарды пайдалануға мүмкіндік береді. Осы іске асырудың мысалдары мынадай:

– адам типті шабуыл ортасында (Maninthemiddle), қаскүнем екі абонент арасындағы байланыс арнасына байқаусыз енгізілгенде және қатысушы тараптар алмасатын ақпаратқа толық бақылау (модификация, жою, дезинформация жасау) алған кезде. Бұл ретте ол абоненттер үшін мүлдем көрінбейтін болып қалады. Бұл шабуыл желіні қорғаудың барлық құралдары жоқ болуы мүмкін;

– жалған желілік мекен-жайларды (ARP-spoofing) және домендік атауларды (DNS-spoofing) таңу, сонымен қатар веб-серверлерді заңды (фишинг) болып көрінетін жергілікті көшірмелерімен ауыстыру.

Бақылау - бұл ақпараттық жүйенің қасиеті пассивті объектілерді пайдаланатын пайдаланушылар мен үдерістердің қызметін тіркеуге мүмкіндік береді, сондай-ақ қауіпсіздік саясатын бұзу немесе орын алған белгілі бір оқиғалар үшін жауапкершілік фактісін жасыру мақсатында нақты оқиғаларға қатысы бар пайдаланушылар мен үдерістердің сәйкестендіргіштерін бір мәнді белгілеуге мүмкіндік береді [1]. Осы шабуылдарды іске асырудың мысалдары:

– жүйе аудит журналдарын тазалау;

– аудит жүйесін істен шығару;

– аса маңызды деректерді өшіру үшін жасанды жасалған ақпарат ағынымен аудиттер журналын қайта жазу;

– зиянды бағдарламаны енгізу.

2 Ақпараттық қауіпсіздікті қатерден қорғау әдістері мен құралдарын талдау

2.1 Желіаралық экрандар

Бүгінгі күні кез келген компанияның қызметі көбінесе интернет желісіне қосылуына және онда пайдаланылатын сервистердің болуына байланысты. Сонымен қатар, желі пайдаланушыларының интернет желісінің барлық артықшылықтары мен пайдаларын, сондай-ақ компанияның қызметі үшін ең аз тәуекелдермен пайдалану мүмкіндігі болуы мәселесі қарастырылады. Сондықтан бүгінгі күні ақпараттық жүйелердің қауіпсіздігін қамтамасыз ету мәселесі өте өзекті.

Бұл сегмент үнемі дамып келеді және айтарлықтай серпінді. Ақпараттық жүйелерді қорғаудың негізгі құралдарына желіаралық экрандарды жатқызуға болады. Әдебиетте олардың синонимдері кездеседі, олардың арасында: брандмауэр, firewall, сүзгіш маршрутизатор және т. б. бар. [3]. Бұл синонимдердің барлығы бірдей терминді білдіреді және бір функционалдық міндеті бар, тек әртүрлі қорғаныс құралдарын қамтуы мүмкін.

Желіаралық экрандар жалпы қауіпсіздік жүйесінің бөлігі болып табылады. Олар белгілі бір қауіпсіздік деңгейін қамтамасыз етеді және желілік деңгейде қорғау саясатын іске асыру құралы болып табылады. Желілік экранды ұсынатын қауіпсіздік деңгейі жүйенің қауіпсіздік талаптарына байланысты өзгереді. Қазір экран элементтері арасында дәстүрлі келісім бар, олардың арасында қауіпсіздік, пайдалану қарапайымдылығы, құны, күрделілігі және т.б. Желілік экран қорғаныс мақсатында желіге және желіге қатынауды басқару және бақылау үшін пайдаланылатын кейбір тетіктердің бірі.

Желіаралық экран жүйесі маршрутизаторды немесе желінің сыртқы шлюзін ауыстырады. Сондықтан ол қорғалған желі бөлігі оның артында орналасады. Желіаралық экранға бағытталған пакеттер жергілікті өңделеді, жай ғана емес. Желіаралық экранда орналасқан басқа объектілерге арналған пакеттер жеткізілмейді. Экранның кез келген жергілікті желімен және сыртқы интернет желісімен өзара әрекеттесу схемасы 2.1-суретте көрсетілген.

2.1 сурет – Firewall сұлбасы

Бұл схема өте қарапайым және сенімді, өйткені көп емес, тек бір машинаны қорғауды қамтамасыз етеді. Жиі экран екі және одан да көп желілік интерфейстермен желілік станция ретінде қолданылады [4]. Оның бір интерфейсі Интернет желісімен, ал екіншісі қорғалған желімен байланысты жүзеге асырады. Желіаралық экран маршрутизатор-шлюздің функцияларын да, тікелей экранды да және оны басқаруды да қамтиды.

Олардың артықшылықтарынан туындайтын экрандардың кемшіліктері бар, мысалы, жүйе сыртқа қатынауды қиындатқан кезде сырттан күрделі қол жеткізу. Стандартты емес порттарда жұмыс істейтін және прокси-серверді қолдайтын кейбір бағдарламалар үшін, қосылуды орнату үшін арнайы порттар ашылады немесе осы бағдарламалармен мүлдем пайдаланылмайды. Мұндай жүйеде FTP файлдық алмасу қызметі болмауы мүмкін, бірақ ол бар болса, қатынау тек желіаралық экран серверіне ғана және одан ғана жүзеге асырылады. Ішкі пайдаланушылар сыртқы әлемнің кез келген басқа пайдаланушысымен тікелей FTP-байланысты орната алмайды. Telnet және rlogin сияқты процедуралар тек серверге кіру арқылы ғана мүмкін. Сонымен қатар, көптеген экрандар ICMP трафигін ішкі желіге өткізуге тыйым салады.

Қауіпсіздікті қамтамасыз ету мақсатында мұндай қорғалған желі желіаралық экран жүйесінен басқа, оның ішінде модемдік құрылғылар арқылы сыртқы әлемге шыға алмайды. Экран әдетте маршрут әдебі бойынша қорғалған желіге көрсетіледі. Мұндай қорғалған желіні пайдаланушылар үшін FTP, telnet және басқа да қызметтер порттары үшін қажетті кірулер жасайды. Мұндай есептеулерде, осы қорғалған желіге файлдарды тасымалдау бойынша ешқандай шектеулер енгізілмейді және әдетте, FTP-сессияның бастамашысы осы қорғалған желінің клиенті болып табылса да, осындай желіден келе жатқан барлық файлдарды жіберу бұғатталады. Интернет желісінің сыртқы клиенттері бірде-бір қорғалған компьютерлерге хаттама арқылы қол жеткізе алмайды.

Желіаралық экрандарға қойылатын талаптар:

– желілік деңгейде пакеттерді сүзу;
– пакеттерді қолданбалы деңгейде сүзу;
– сүзгілеу және басқару ережелерін теңшеу;
– қорғалған желі бойынша аутентификация үшін тұрақты хаттамаларды пайдалану;
– аудит журналын жүргізу.

Желіаралық экранның алғашқы үш талаптарын орындау кезінде келесі компоненттерді пайдаланады:

– сүзгі маршрутизаторлар;
– желілік деңгейдегі шлюздер;
– қолданбалы деңгейдегі шлюздер (прокси-сервер).

2.1.1 Сүзгі маршрутизаторлары брандмауэрдің қарапайым компоненті болып табылады. Екі (немесе одан да көп) әртүрлі желілер арасында екі бағытта да деректерді беретін маршрутизатор. Қалыпты маршрутизатор пакетті бір желіден алады және оны осы желі ішінде немесе басқа желіде орналасатын жерге бағыттайды. Сүзу маршрутизаторы бірдей функцияларды орындайды, бірақ бұл пакеттерді қалай және қайда жіберу керектігін ғана емес, тұтастай пакетті бір жерге жіберу-жібермеу туралы шешім қабылдауға мүмкіндік береді. Бұл маршрутизаторға осы бумамен нақты не істеу керектігін шешуге мүмкіндік беретін бірнеше сүзгілерді орнату арқылы болады.

Пакетті сүзу процесінде маршрутизаторды дайындау үшін іріктеу саясатының кейбір мынадай критерийлер қажет: жіберушінің және алушының IP-адрестері, жіберушінің және алушының TCP-порттарының нөмірлері, TCP-«ack» растау бит жағдайы, жіберушінің және алушының UDP-порттарының нөмірлері және пакетті жіберу бағыты. Қауіпсіз сүзу сұлбаларын қалыптастыру үшін қажетті ақпараттың тағы бір өлшемі болып табылады, біздің маршрутизаторымыз сүзу нұсқауларының тәртібін өзгертеді ме және қолданылатын интерфейстердің әрқайсысында кіріс және шығыс пакеттерге арналған осы сүзгілерді пайдалануға бола ма. Егер маршрутизатор тек шығу пакеттерін сүзсе, онда ол өз сүзгілеріне қатысты сыртқы болып табылады және ықтимал шабуылдар үшін неғұрлым осал болады. Маршрутизатордың осалдықтарынан басқа, кіріс және шығыс пакеттері үшін пайдаланылатын сүзгілер арасындағы айырмашылық 2 интерфейстен астам маршрутизаторлар үшін аса маңызды өлшем болып табылады. Басқа маңызды сәттерге IP-тақырып опцияларына және буманың фрагменттерінің жағдайына негізделген сүзгілер жасау мүмкіндігі жатады. Жақсы сүзгіні қалыптастыру өте қиын жұмыс және сүзілетін қызметтер (хаттамалар) түрін жақсы түсінуді талап етеді.

2.1.2 Желілік деңгейдегі шлюздер. Желілік деңгейдегі шлюздер - бұл транзиттік пакеттердің IP-адресін түрлендіруге мүмкіндік беретін TCP/IP желілеріндегі NAT технологиясын іске асыратын құрылғылар немесе бағдарламалық қамтамасыз ету. NAT әдісін пайдалана отырып, адрестердегі мұндай түрлендіруді әрбір маршрутизатор, не қол жеткізу сервері, не желіаралық экран жүргізеді. Бұл механизмнің мәні пакеттен бір жаққа өту кезінде кері адресті ауыстыру және кері пакеттегі тағайындау адресін қайта ауыстыру болып табылады. Көз/алушының мекенжайларымен қатар көз/алушы порттарының нөмірлері өзгеруі мүмкін. NAT тетігі бірегей IP-адрестердің санын едәуір қысқартады, бұл деректерді Ғаламдық маршрутталатын мекенжай кеңістігіне трансляциялау арқылы жергілікті бірегей адрестері бар интернет-компания желісіне қосылуға мүмкіндік береді. Сондай-ақ, NAT механизмі жергілікті желіде IP-адрестерді жасыру үшін қолданылады.

NAT технологиясының артықшылықтары келесідей [5]:

а) IP-адрестердің санын бірнеше ішкі жеке IP-адрестерді бір сыртқы ашық IP-адрестерге немесе керісінше тарату арқылы үнемдеуге мүмкіндік береді;

б) ішкі хостарға сырттан келуді болдырмауға мүмкіндік береді,бұл ретте ішінен сыртқа шығу мүмкіндігін қалдырады. Желі ішінде болатын қосылысты инициалдау процесінде қандай да бір трансляция жасалады. Сырттан келіп түсетін жауап пакеттері құрылған трансляцияға сәйкес келеді және өткізіледі. Сырттан келіп түсетін басқа пакеттер үшін тиісті трансляция жоқ, сондықтан олар жіберілмейді.

NAT технологиясының кемшіліктеріне мыналар жатады [5]:

а) барлық хаттамалар NAT механизмін «еңсере алмайды». Кейбірі (мысалы, IPSec) жұмыс істемейді, егер олардың жолында өзара әрекеттес хостер арасында адрестердің трансляциясы бар болса. IP-адрестерді таратуды жүзеге асыратын кейбір желіаралық экрандар IP-адрестерді тек IP тақырыптарында ғана емес, сонымен қатар басқа да жоғары деңгейлерде (мысалы, FTP немесе h. 323 хаттамаларының командаларында) тиісті түрде ауыстыру арқылы осы кемшіліктерді түзетеді);

б) «көптің біреуі» мекенжайларын аударуға байланысты пайдаланушыларды анықтауда қосымша қиындықтар туындайды, бұл аудармалардың аудиторлық жазбаларының толық деректерін сақтау қажеттілігіне әкеледі.

2.1.3 Прокси-сервер - бұл қолданбалы қызметтерді тек бір ғана машина арқылы бағыттауға мүмкіндік беретін құрал. Әдетте, прокси-сервер ретінде жұмыс істейтін бір машина (қорғалған желілік машина, ДК) бар, хаттамалар тізімін қолданатын, SMTP, FTP, HTTP, және т. б. Бірақ белгілі бір қызмет түрлері үшін арнайы қолданылатын жеке машиналар да болуы мүмкін. Сыртқы сервермен тікелей қосылудың орнына, клиент алдымен сұралған сыртқы сервермен қосылуды бастамашы прокси-серверге қосылады. Пайдаланылатын прокси-серверге байланысты ішкі клиент автоматты түрде қайта бағыттау жүзеге асырылатындай етіп конфигурацияланады, яғни пайдаланушыны хабардар етпестен, ал басқа пайдаланушылар прокси-серверге қосуды және содан кейін ғана арнайы формат шеңберінде қосылуға бастамашы болуды талап ете алады.

Прокси-сервер құрылғыларын қолдану ақпараттық қауіпсіздікті қамтамасыз ету саласында елеулі артықшылықтарды қамтамасыз етеді. Пайдаланушыдан немесе қол жеткізу алдында аутентификацияның белгілі бір деңгейін қамтамасыз ету жүйесінен талап ететін хаттамалар үшін қол жеткізу тізімін қосу мүмкіндігі жүзеге асырылады. Сондай-ақ, кейде ALG (Application Layer Gateways) деп аталатын, хаттамалардың белгілі бір түрлеріне бағытталған жетілдірілген прокси серверлер бағдарламалануы мүмкін. Мысалы, FTP протоколы үшін ALG үшін «get»-тен «put» командасымен ерекшеленеді; компания пайдаланушыларға интернет желісінен түскен файлдар үшін «get» командасын орындауға рұқсат бере алады, бірақ қашықтағы сервердегі жергілікті файлдар үшін «put» командасына тыйым сала алады. Керісінше, фильтрлеу маршрутизаторы

мұндай FTP-қолжетімділікті бұғаттайды немесе жоқ, бірақ ішінара тыйым салуларды іске асырмайды. Прокси-серверлер әртүрлі параметрлердің негізінде деректер ағындарын шифрлау үшін теңшейді. Компания осы ерекшелікті екі торап арасындағы криптографиялық қосылыстарды шешу үшін пайдаланады, олардың біреуі Интернет желісінде орналастырылуы мүмкін. Желілік экрандар көбіне қаскүнемдер үшін қолжетімділікті бұғаттау құралдарының бірі ретінде қарастырылады, сонымен қатар заңды пайдаланушылардың кейбір торапқа қол жеткізу мүмкіндігі. Заңды пайдаланушыға тұрақты кіру қажет болған жағдайда, мысалы, презентациялар немесе конференция кезінде негізгі бетке көп мысалдар бар. Интернет желісіне қолжетімділікті мұндай жағдайда сенімсіз машина немесе желі арқылы жүзеге асыруға болады. Дұрыс бапталған прокси сервері дұрыс пайдаланушыларды кез келген торапқа жібереді және барлық қалған тораптардың кіруін бұғаттайды.

Қазіргі таңда желіаралық экранның ең жақсы нұсқасы екі экранды маршрутизатордан және маршрутизаторлар арасындағы желіде бір немесе одан да көп прокси-серверден тұратын комбинация болып табылады. Бұл схема сыртқы маршрутизаторға ақпараттық қауіпсіздікті бұзу үшін төменгі IP-деңгейді пайдаланудың барлық әрекеттерін бұғаттауға мүмкіндік береді, ал прокси-сервер осалдықтарды жоғарғы хаттамалар деңгейінде қорғайды. Ішкі маршрутизатордың мақсаты - барлық трафикті бұғатту, сонымен қатар прокси-сервердің кіруіне бағытталған. Егер осы схеманы іске асырса, онда ақпараттық қауіпсіздіктің жоғары дәрежесі қамтамасыз етілетін болады.

Әкімшіге кез келген қатерлерді дер кезінде сәйкестендіруге және оларды жою бойынша шаралар қабылдауға мүмкіндік беретін кез келген желілік сұраныстарды тіркеудің жақсы теңшелген жүйесі үлкен маңызға ие.

Желіаралық экрандардың көпшілігі желі қауіпсіздігін басқару үшін теңшелетін журналдар жүйесі бар. Мұндай мониторинг жүйесі әдетте орталықтандырылып, стандартты емес жағдайдың кез келген туындауында ескертулерді жіберетіндей етіп теңшелген. Кез келген басып кіру белгісі немесе бұзу әрекеті кезінде журнал файлдарын үнемі қарау қажет. Кейбір зиянкестер журнал файлдарын редакциялау арқылы өз іздерін жасыра алады, мұндай файлдарды әрдайым қорғау қажет. Бұл үшін көптеген жолдар бар, соның ішінде: WORM драйвері (write once, read many) және «syslog» утилитасы арқылы ұйымдастырылған орталықтандырылған журнал файлдары [5].

FireWall типті жүйелер корпоративтік желілерді құруда және қорғауда жиі қолданылады, онда желінің жекелеген бөліктері бір-бірінен жеткілікті түрде жойылған. Мұндай жағдайда қосымша ақпараттық қауіпсіздік шаралары ретінде пакеттерді шифрлау қолданылады. FireWall типті жүйе арнайы бағдарламалық қамтамасыз етуді қажет етеді. Жүйенің өте күрделі әрі қымбат екендігін және бұл ретте «ішкі» зиянкестерден қорғамайтынын ескеру қажет. Қосымша қорғау дәрежесі қажет болған жағдайда пайдаланушылардың желінің қорғалған бөлігінде авторизациялануын,

сондай-ақ атаулар мен парольдерді сәйкестендірудің аппараттық құралдарын немесе шифрлауды пайдаланады.

Firewall жүйесін таңдау кезінде бірқатар талаптарды ескеру қажет:

– операциялық жүйе. UNIX iwindows NT ОЖ-мен жұмыс істейтін Firewall түрлі нұсқалары бар. Кейбір өндірушілер қауіпсіздікті күшейту үшін ОЖ түрлендіреді. Сондықтан өзіңіз жақсы білетін ОЖ таңдау қажет;

– хаттамалар. Барлық экрандар SNMP жедел хабарламаларды жіберу протоколынан басқа FTP файлдарын жіберу хаттамасымен (21 порт), e-mail электрондық поштасымен (25 порт), HTTP (80 порт), NNTP (119 порт), Telnet (23 порт), Gopher (70 порт), SSL (443 порт) және басқа да белгілі хаттамалармен жұмыс істейді;

– сүзгілер түрлері. Прокси-сервердің қолданбалы деңгейінде жұмыс істейтін желілік сүзгіштер желі әкімшісіне Firewall экраны арқылы өтетін ақпараттық ағындарды бақылауға мүмкіндік береді, бірақ жоғары жылдамдыққа ие емес. Аппараттық шешімдерді пайдалану кезінде көп ағындар жіберіледі. «Схемалық» прокси деңгейі бар, желі пакеттерін қара жәшіктер ретінде қарайтын және оларды өткізетін. Пакеттерді іріктеу жіберушінің, алушының мекен-жай параметрлері, порттар нөмірі, интерфейстер түрі және пакет тақырыбының кейбір өрістері бойынша жүзеге асырылады;

– операцияларды тіркеу жүйесі. Firewall экрандарының барлық дерлік жүйелері барлық операцияларды тіркеудің кірістірілген жүйесіне ие. Мұнда мұндай жазбалары бар файлдарды өңдеу құралдарының болуына ерекше назар аудару қажет;

– басқару. Тек кейбір Firewall экран жүйелері пайдаланушының графикалық интерфейстерімен жабдықталған. Қалғандары мәтіндік конфигурациялық файлдарды пайдаланады және қашықтан басқаруға рұқсат етеді;

– қарапайымдылығы. Прокси сервері түсінікті құрылымы мен ыңғайлы тексеру жүйесі бар. Осы бөлімнің бағдарламалар мәтіндерінің болуы қажет, бұл бағдарламалық қамтамасыз етудегі осалдықтардан қорғау деңгейін арттырады;

– туннельдеу. Firewall экрандарының кейбір жүйелері компанияның немесе ұйымның қашықтағы филиалдарымен (интранет жүйелері) байланыс үшін интернет желісі арқылы туннелдерді ұйымдастырады. Мұндай туннельдер бойынша ақпарат әдетте шифрланған түрде беріледі.

Бүгінгі күні желілік экрандар бағалар мен өнімділіктің кең ауқымында бар. Коммерциялық опция бағасы $ 1000 USD басталады және $ 25000 USD жетеді. Тегін БҚ базасындағы желілік экрандар аз сомаға салынады. Экран үшін тегін бағдарламалық қамтамасыз етуді пайдалану кезінде шығын бөлігі аппараттық бөлікті сатып алуға және білікті әкімшіні іздеуге жұмсалуы мүмкін. Желілік экранның дұрыс конфигурациясы үшін (коммерциялық немесе жоқ) TCP/IP стегінің белгілі бір шеберлігі мен білімі қажет. Экранның екі түрі де тұрақты қызмет көрсетуді, жаңарту пакеттерін орнатуды және

бағдарламаларды түзетуді, сондай-ақ үздіксіз бақылауды талап етеді. Желіаралық экранның бюджетін бағалау кезінде мұндай қосымша шығындар желіаралық экранның аппараттық бөлігімен бірге ескерілуі тиіс.

Желі экрандары желінің ақпараттық қауіпсіздігін қамтамасыз ету кезінде үлкен көмек көрсетеді, көптеген шабуылдардан қорғайды. Желіаралық экранның кемшілігі-бұл қауіпсіздік шешімінің бір бөлігі ғана.

2.2 IDS жүйелері

IDS типті шабуылдарды анықтауға арналған жүйелер желілік, сондай-ақ жүйелік және қолданбалы деңгейлерде ақпараттық жүйенің мониторингі бойынша міндеттерді шеше алады және қауіпсіздіктің бұзылуын анықтауды қамтамасыз етеді және оларға жедел ден қояды. IDS желілік жүйелері желілік пакеттерді талдау үшін Деректер көзі болып табылады, А IDS жүйесі жүйелік деңгейде (хосты - hostbased) операциялық жүйенің қауіпсіздік аудит журналдарының жазбаларын және кез келген қосымшаларды талдауға мүмкіндік береді. Бұл ретте талдау әдістері (шабуылдарды анықтау) IDS жүйесінің барлық сыныптары үшін ортақ болып қалады.

Бүгінгі күні шабуылдарды анықтау мәселесін шешуде көптеген тәсілдер ұсынылды. Алайда қолданыстағы IDS жүйелері екі негізгі класқа бөлінеді: статистикалық талдауды қолданатын жүйелер, сигналатуралық талдауды қолданатын жүйелер.

Статистикалық әдіс зиянкестің белсенділігі қандай да бір ауытқулармен, пайдаланушылардың мінез-құлық бейінінің өзгеруімен немесе бағдарламалар мен аппаратурамен бірге жүреді деген болжамға негізделеді.

Көптеген заманауи коммерциялық өнімдерде қабылданған шабуылдарды анықтау үшін негізгі әдіс-сигналдық талдау. Мұндай әдістің қарапайымдылығы оны тәжірибеде енгізуге мүмкіндік береді. Сигналатуралық талдауды қолданатын IDS жүйелері желіаралық экранды іске асыратын қауіпсіздік саясатының ережелері туралы «білмейді», сондықтан бұл жағдайда әңгіме әдейі белсенділік туралы емес, тек шабуылдар туралы болып отыр. Олардың жұмыс істеуінің негізгі принципі-жүйеде/желіде болып жатқан оқиғаларды белгілі шабуылдармен салыстыру.

Ақпараттық технологиялардың қауіпсіздігін бағалауға арналған жалпы өлшемдерге «қауіпсіздік аудитінің деректерін талдау» (Securityauditanalysis) [3]. Бұл талаптар статистикалық және сигналдық талдау сияқты әдістермен қаскүнемдік белсенділікті іздейтін IDS жүйелерінің функционалдығын айқын анықтай алады.

«Профильдерді қолдануға негізделген аномальды белсенділікті анықтау» (Profilebasedanomalydetection) деп аталатын FAU_SAA2 типті Компонент жүйе профилдерінің көмегімен аномальды белсенділікті анықтауды анықтайды, олар қауіпсіздік тұрғысынан жүйенің пайдаланушыларының қауіпті әрекеттерін анықтайды және осы әрекеттерді анықтайды. Мұндай әрекеттердің қауіптілік дәрежесін анықтау үшін сол немесе басқа пайдаланушы үшін осы пайдаланушыларға тиісті «сенімсіздік

рейтингтері» есептеледі. Пайдаланушының әрекет ету қаупі неғұрлым көп болған сайын, оның «сенімсіздік рейтингі» соғұрлым жоғары болады. Мұндай «сенімсіздік рейтингі» белгіленген сыни мәнге жеткенде, онда қаскүнемдік белсенділікке әрекет ету бойынша қауіпсіздік саясатында көзделген әрекеттер қолданылады.

Қазіргі таңда желілік шабуылдарды анықтау бойынша екі негізгі тәсіл бар: желілік трафикті талдау және контентті талдау. Желі трафигін талдауда тек желілік пакеттердің тақырыптары, контентті талдауда – олардың мазмұны зерттеледі. Ақпараттық өзара іс-қимылдарды барынша толық және дәл бақылауды олардың тақырыптары мен деректер саласы қосылатын желілік пакеттердің барлық мазмұнын талдау жолымен ғана қамтамасыз етуге болады. Бірақ практикалық тұрғыдан бұл міндет өңдеу қажет болатын деректердің көп көлеміне байланысты қиындайды. Қазіргі заманғы IDS жүйелері желілерде 100 Мб / с жылдамдыққа жеткен кезде өнімділікпен күрделі проблемаларды бастан өткеруде. Сондықтан шабуылдарды анықтау үшін желілік трафикті талдауды қолданған жөн, тек кейбір жағдайларда оны контентті талдаумен бірге қолданған жөн.

Сонымен қатар IDS жүйесін желі базасында және хост базасында салынатын өнімдерге бөлуге болады. Мұндай екі жүйе де басып кіруді анықтайды, бірақ әртүрлі деректерді өңдейді. Желі базасында құрылатын IDS жүйесі шабуылдар анықталған кезде талдағышқа ұқсас деректер ағынын оқиды. Ол интерфейсі коммутатор портын талдауға немесе көшіруге арналған портқа қосылған барлық желілік Сенсорлардан тұрады. Жүйе желісіне осындай қосылу үшін балама ретінде концентраторлар немесе тармақтағыштар қолданылады [16].

Хост негізінде жұмыс істейтін IDS жүйесі агенттер принципін қолданады [16]. Олардың жұмысы - қауіпті оқиғалар белгілерін іздеуде тіркеу немесе аудит журналдарының деректері негізінде белсенділікті талдайтын бақыланатын серверлерде немесе жұмыс орындарында қосымша бағдарламалық қамтамасыз ету.

Шабуылдарды анықтаудың ең тиімді және кең таралған әдісі – кейбір үлгімен салыстыру. Вирустарды сканерлегенде, тик әдіс шаблондардың немесе сигналдардың бұрыннан бар тізіміне сүйеніп отырады, соның негізінде шабуылдың болуы туралы қорытынды жасалады. Бұл жүйелер тек әрбір деректер пакетін барлық үлгілермен салыстырады және олар сәйкес келген жағдайда басып кіру анықталды деп есептеледі. Мұндай әдістің жеткіліксіздігі өте үлкен шығындар мен нашар масштабталу болып табылады [4]. Әлдеқайда тиімдірек пайдалануға талдау әдісі хаттамалар, өйткені ол емес жүреді дәйекті салыстыру шаблонмен, ал алдымен декодируются кезінде пайдаланылатын өзара іс-қимыл хаттамалары. Мұндай рұқсат етілген стандарттан ауытқулар шабуылдың бірінші ықтимал белгісі болып табылады. Қосымша белгілі бір шаблондар пайдаланылуы мүмкін, бірақ деректер трафигі тиісті Хаттамаға қатысты шаблондармен ғана салыстырылады. Бұл әдіс өнімділігін айтарлықтай арттырады, бірақ іс жүзінде хаттамаларды

талдау әдісі мен хаттамаларды ескере отырып, оңтайландырылған үлгілермен салыстыру арасындағы айырмашылық анық қалады.

Теорияда шабуылдарды анықтаудың тағы бір әдісі бар - статистикалық әдіс [6]. Бұл әдіске сәйкес IDS жүйесі алдымен желілік трафиктің көптеген параметрлеріне негізделген «эталондық мәнді» анықтай алады, содан кейін одан ауытқуларды әлеуетті қауіп ретінде қарастыра алады. Алайда, бұл әдіс бүгінгі күні практикалық тануды алған жоқ және барлық қолданыстағы коммерциялық жүйелер шаблонмен салыстыруды немесе шаблонмен салыстырумен бірге хаттамаларды талдау әдісін қолданады.

Желі базасында негізделген IDS жүйелеріне қатысты, ал вирустардан қорғау жүйелерінің тиімділігі шаблондардың өзектілігіне байланысты. Күн сайын жаңа осал жерлер пайда болады және зиянкестер оларды пайдалану жағдайын жіберіп алмайды, IDS жүйесі әрқашан өзекті және оларды жеңуге дайын болуы тиіс. Егер осы жүйенің шаблондары жаңа қатерлерді айына бір рет жаңартса, онда жаңартулар арасындағы аралықта жаңа, жүйемен танылмайтын шабуылдар пайда болуы мүмкін екенін ескеру қажет. Егер жаңа шабуылдар хаттамадан ауытқумен іске асырылса, хаттаманы талдау әдісінің негізінде жүйелер осындай проблеманы ішінара ғана шеше алады. Бүгінгі күні шабуылдарды анықтау кезінде ең үлкен проблема жалған дабыл сигналдарының көп болуына байланысты жоғары операциялық шығындар болып табылады. Олар, егер тізімдегі үлгі әдеттегі деректер ағымында, тіпті қандай да бір шабуыл болмаған кезде немесе әдеттегі қосымшалар стандартты хаттамалардың елеусіз модификацияларын пайдаланған кезде пайда болады, бұл ақыр соңында IDS жүйесімен дабыл сигналын беруге әкеледі. Кейде себеп кейбір желілік қателер немесе сервердің немесе жұмыс орнының дұрыс теңшелген параметрлері болып жатады.

Дабылдың жалған сигналдарының түсуін азайту үшін әртүрлі тәсілдер қолданылады. Шешімдердің бірі кешенді үлгілер болып табылады: қарапайым трафикте пайда болу ықтималдығы өте аз. Бірақ кемшіліктер бар – бұл кешенді үлгілер сенсордың өнімділігін төмендетеді.

Шешімнің басқа нұсқасы ақпараттық жүйенің нақты бар инфрақұрылымы туралы ақпаратпен әлеуетті белгілі шабуылдарды корреляциялаудан тұрады. Windows операциялық жүйесі үшін ерекше UNIX жұмыс станциясына қарсы бағытталған зұлымдық әрекет толық қате, не, кем дегенде, мағынасыз болып табылады, өйткені соңғы жүйеде жоқ осал орынға бағытталған. Сондықтан, дабыл сигналы сүзіледі немесе оның басымдығын айтарлықтай төмендетеді. Инфрақұрылым бойынша осындай ақпарат көзі ретінде желі ТК сканерлеу нәтижелері немесе арнайы сенсорлар қызмет етеді. Мұндай талдау кезінде жүйе жалпы желілік трафикті оқи алады және деректер пакеттеріндегі ақпараттың негізінде қандай операциялық жүйе немесе қандай қосымшалар бақыланатын желідегі белгілі бір соңғы мекен-жай бойынша орналасқанын анықтай алады. Бұл үшін ең оңтайлы нұсқа-бұл шабуылдарды анықтау жүйесінің келіп түсетін дабыл сигналдарын тіркей отырып, нақты уақыт режимінде осы ақпаратты түзету.

Әдетте әкімшілер шабуыл туралы жалған сигналдарды болдырмауға тырысады және IDS жүйесінің сенсорларын қолмен реттейді. Бұл жағдайда сенсорлардың немесе IP-адрестердің нақты топтары үшін белгілі бір шаблондарды белсендіреді. Мұндай жұмыс қаржы жағынан да, қаражат жағынан да шығын болып табылады, бірақ сенсорлар соқыр бола алады, бұл IDS жүйесін енгізу бойынша жобаның барлық мағынасына күмән келтіреді.

Шабуылдарды анықтаудың сапалы жүйесінің маңызды белгілерінің бірі бақыланатын трафик көлемінің саны, анықтау дәлдігі, қосымша бақылау және қолмен талдау үшін әкімшідегі пайдаланылатын құралдар болып табылады. Мұндай жағдайда сол бастапқы немесе соңғы мекен-жай бойынша басқа хаттамалық қызмет туралы ақпаратты қарапайым және тез алу тек жұмыстың басталуы.

Ең жақсы анықтау жылдамдығы, егер әкімші осы жүйеден туындайтын ақпарат ағынын жеңе алмаса, ештеңе бермейді. Қысқа уақыт аралығында IDS жүйесі үшін шабуылдар туралы дабыл сигналдары бар барлық жады қиын болмайды. IDS жүйелерін қолдана отырып, ақпаратты қорғау жүйелерін жобалау кезінде қолданыстағы жүйелердің шектеулері ескеріледі. Әдетте өндірушілер белгілі үлгілердің саны немесе ең көп талданатын өткізу қабілеті сияқты шекті мәндерді көрсетеді. Бірақ IDS жүйесі қалай көп немесе дәл қандай басып кіруді анықтай алмайды. Мәселе анықтау технологиясына тамырмен кетеді, себебі хаттамаларды талдау кезінде ол жиі бар үлгілерге негізделеді. Мұндай деректер ағынында үлгінің белгілі бір түрі бар болса, онда шабуылдар танылады. Бірақ егер бар шабуыл орын алса, бұл жағдайда үлгі көрмесе, онда мұндай шабуыл жүйесі таппайды. Жиі жүйелер эксплоит деп аталатын белгілі автоматтандырылған басып кіру құралының көмегімен осы шабуыл кезінде байтқа тән реттілігі бойынша басып кіруді анықтайды. Егер зиянкестер осы вопроскада үлкен тәжірибеге ие болса, онда оның өз бетінше құрал жасауға және шабуыл жасауға үлкен мүмкіндігі бар, ол шаблондар базасында негізделген IDS жүйесі жағынан байқалмаған болып қалады.

Олар жеке болып табылатын жалпы негізгі қағиданы пайдаланғанына қарамастан, қосымша деңгейінде де басып кіру мүмкін. Желілік деңгейде танылатын ешқандай үлгілер жоқ. IDS жүйелері үшін мұндай шабуылдарды анықтау қабілеті жеке қосымшалардың логикасына ие және олардың ағымдағы мәртебесін қадағалайды. Он таңбалы санды енгізу Web формасының бір өрісіне рұқсат етіледі, ал басқа өріске немесе басқа URL мекен-жайына рұқсат етілмеген командаларды орындауға келтіріледі. Шабуылдарды анықтаудың көптеген заманауи жүйелері осы функцияға ие емес.

Жаһандық таратылған сенсорлар негізінде негізделген IDS жүйесін бағалау жүргізілетін статистикалық деректер мен зерттеулерді абайлап пайдалану қажет. Көбінесе 80 порты арқылы өтетін шабуыл олардың кейбіріне қатысты – дайын эксплоиттер базасында ғана жарамды, бірақ қосымшалар үшін ерекше жиі кездесетін жеке шабуылдарға қатысты емес. Бұл шабуылдар IDS жүйесінің сенсорлары ерекшелік ретінде анықталады.

Желілік шабуылдардың сигналдары вирустар үшін сигналдардан іс жүзінде айырмашылығы жоқ. Олар желілік шабуылдарды желілік трафиктің басқа түрлерінен ажыратуға мүмкіндік беретін белгілер жиынтығы болып табылады. Трафикті талдау кезінде (желілік пакеттердің тақырыптары) қолданылатын шабуылдар сигнатурасы ретінде қарастырылатын белгілерді атайық [5]:

– TCP пакетінің атауында 139 нөмірі бар порт және os жалауы (OutofBand) қолданылады, бұл WinNuke үшін шабуыл белгісі болып табылады;

– бір мезгілде бір-біріне қайшы келетін TCP-пакеттің тулары орнатылған: SYN және FIN. Осы жалаулар комбинациясы арқылы көптеген шабуылдаушы бағдарламаларда тек жалғыз SYN-жалаудың орнатылуын тексеретін сүзгілер мен мониторларды айналып өтуге болады.

Контент үшін талдау әдістері де кемшіліктер бар. Олар жұмыс істемейді, процесс кезінде DDoS, trojans типті бағдарламалар пакеттері, ал трафикті шифрлеуге жүгінеді. Шабуылдардың осы түрін анықтау әдістері желілік пакеттердің тақырыбын талдаумен шектейді.

Бүгінгі күні IDS жүйелері корпоративтік желілердің қауіпсіздігін қамтамасыз ету тәжірибесіне енгізілуде. Бірақ мұның бәрі проблемалардың көбеюіне ие және шабуылдарды анықтау жүйесін өрістететін компания үшін сними қақтығысы сөзсіз. Кейбір енгізу мәселелерін келтіреміз:

– IDS коммерциялық жүйелерінің үлкен құны;

– қазіргі заманғы IDS жүйелерінің төмен тиімділігі, ол жалған іске қосылулар мен іске қосылулардың көп санымен сипатталады (falsepositivesandfalsenegatives);

– ресурстарды талап ету және кейде желілерде 100 Мбит/с жылдамдықпен IDS жүйелерінің төмен өнімділігі;

– желілік шабуылдармен байланысты жоғары тәуекелдер;

– компанияда тәуекелдерді талдау және оларды басқару әдістемелерінің болмауы, ол басшылыққа тәуекелдердің шамасын барабар бағалауға және қарсы өлшемдерді іске асыру үшін олардың құнын негіздеуге мүмкіндік береді;

– IDS жүйесін енгізу және өрістету мүмкін емес шабуылдарды анықтау бойынша сарапшылардың жоғары біліктілігі қажеттілігі.

Аппараттық орындаудағы заманауи IDS жүйелерінің құны 5000 USD-нан 50000-ға дейін және одан жоғары болады [7]. Құны компанияның масштабы және оның өткізу қабілетіне қойылатын талаптары, сондай-ақ шабуылдарға арналған сигналдар жиынтығы есебінен анықталады. Бүгінгі нарықта бағдарламалық өнімдер бар, айтарлықтай аз құны және қол жетімді. Желіаралық экрандар сияқты, ал IDS жүйелеріне қатысты осы құралмен 80 пайызға қамтамасыз етілетін қорғаныс деңгейі әкімшілердің құзыреттілігіне және сигналдар жаңартуларының шығуына байланысты. Баспасөзде IDS осы жүйелері нақты қолданыстағы жүйеге жұқа күйге келтірудің болмауына

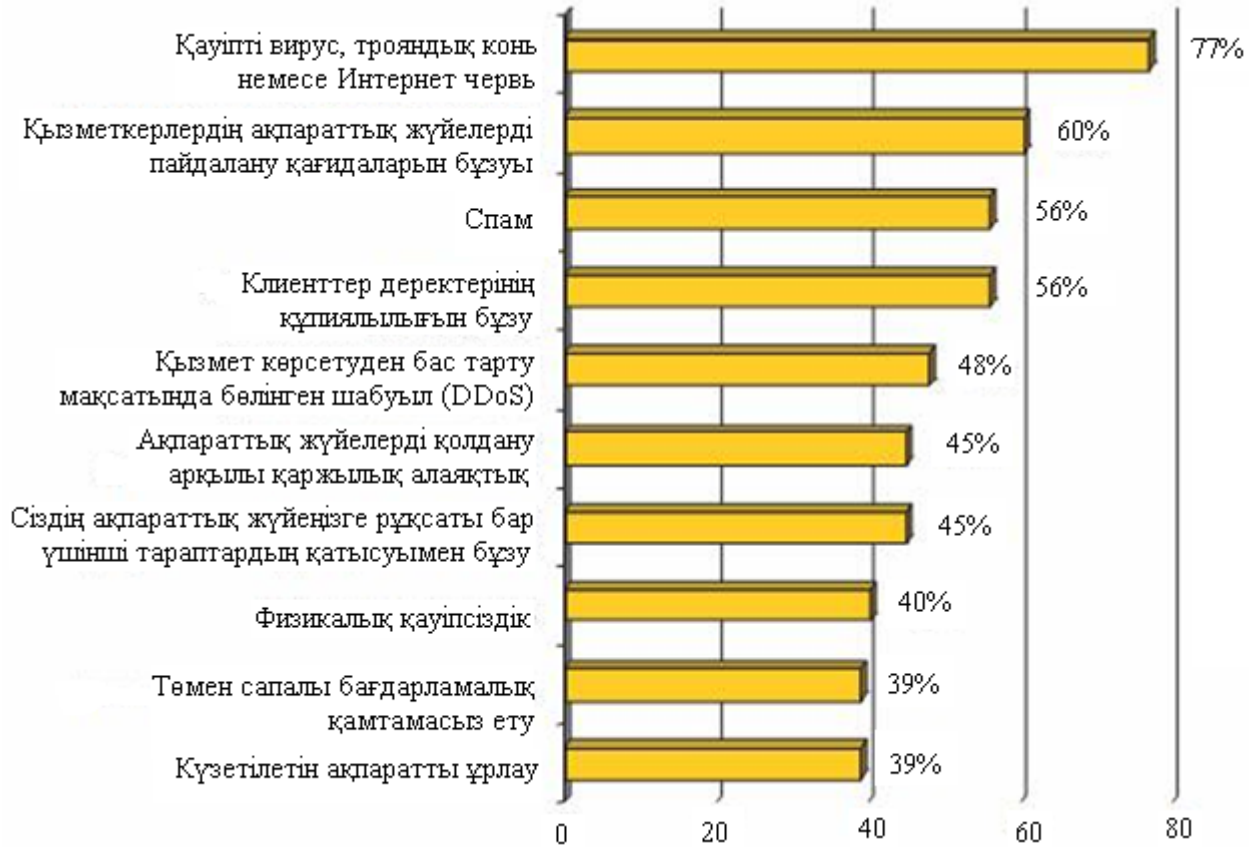
байланысты ғана әрекет етпеген көптеген мысалдар бар, осылайша, оларды қолдану практикасы іс жүзінде нөлге дейін төмендейді.

2.3 Вирусқа қарсы қорғаныс

Қазіргі уақытта кәсіпорында антивирустық қауіпсіздік жүйесі - бұл қорғаудың маңызды элементі және көп жағдайда ақпараттық қауіпсіздікті қамтамасыз етудің барлық қолданыстағы жүйелерінің ішіндегі ең өзекті жүйе. Заттардың бұл ережесі түрлі беделді компаниялардың бірнеше рет зерттеуін растайды. Мысалы, Ernst&Young компаниясының 2.2-суретінде келтірілген 2004 жылдың қорытындысы бойынша есепте сұралған мамандардың көпшілігі вирусқа қарсы қорғау мәселесін және вирусты жұқтыру қаупін тікелей бірінші орынға қояды [8].

Тұрақты дамудағы компаниялар желілері корпоративтік желілерге қазіргі заманғы вирустардың ену нүктелерінің санын кеңейтеді. Бір кездері зиянды код компьютерге тек ақпаратты тасымалдағыш арқылы ғана пайдаланушы кіре алатын болады. Қазіргі уақытта, енудің негізгі нүктелеріне электрондық пошта, сондай-ақ шлюздер (корпоративтік желіге кірудің Орталық нүктесі) және Интернет желісінің сервері (webbrowsing түрлі CGI сценарийлер және пайдаланушы жүктейтін басқа да зиянды код жатады).

Корпоративтік желіні дамытумен қатар, вирусқа қарсы қорғау жүйесін де дамыту қажет, тіпті оның дамуы бір қадамға басып озуы немесе бір мезгілде және осы желіні пайдаланушыларға ұсынатын сервистер саны мен сапасының кеңеюіне сәйкес өзгеруі қажет [9]. 2.2 суретте вирустардың жіктелуі келтірілген, әрі қарай ақпараттық жүйелерге зиян келтіретін кейбір қауіптерді сипаттаймыз.



2.2 сурет – Ernst&Young компаниясының зерттеу қорытындысы бойынша бизнеске қауіп-қатерлерді жіктеу

2.3.1 «Трояндық конь» типті вирусты қауіп. «Трояндық конь» - бұл пайдалы, көрінетін бағдарлама немесе жасырын кодты қамтитын командалық рәсім, оны іске қосқаннан кейін тасымалдаушы бағдарлама жағымсыз немесе жойғыш әрекеттерді орындайды.

Бұл түрдегі бағдарламалар рұқсатсыз пайдаланушы өз бетінше орындай алмайтын кейбір операцияларды ортақ орындау үшін қызмет етуі мүмкін. Мысалы, бірнеше адамның ортақ пайдалануындағы өз компьютеріндегі басқа пайдаланушының қандай да бір файлдарына қатынауды алу үшін, қаскүнем осы пайдаланушының файлдарына қатынауды бақылауды орындау барысында параметрлерді өзгертетін «троянский конь» типті бағдарламаны жасайды және осы файлдарды барлық пайдаланушылар үшін ашық етіп жасайды. Осы бағдарламаны ұйымдастыра отырып, зиянкестер оны іске қосу үшін басқа да пайдаланушыларды жалпыға қолжетімді каталогқа орналастыру арқылы және оған көптеген пайдаланушыларға қандай да бір пайдалы бағдарламаның немесе одан да көп утилитаның атымен көрінетіндей атау бере отырып, итермелеуі мүмкін. Мысалы, бізге қажетті форматта пайдаланушы үшін файлдар тізімін жасайтын бағдарлама. Кейбір пайдаланушы осы бағдарламаны іске қосқаннан кейін, осы бағдарламаның авторы осы пайдаланушының файлдарында қамтылған кез келген ақпаратқа қол жеткізеді. Тану қиын «троянский конь» вирусының мысалы - белгілі бір түрдегі компилятор бағдарламаларға қосымша кодты енгізу мақсатында модификацияланған компилятор, мысалы, жүйеге кіру бағдарламаларында [10]. Бұл код бағдарлама авторына осы жүйеге арнайы пароль арқылы кіруге мүмкіндік беретін тіркеу модуліндегі өрмекші болып табылады. Жүйеге кіру бағдарламасының бастапқы коды бойынша «троянский конь» типті осындай вирус табу мүмкін емес.

«Трояндық жылқы» типті вирусты жазу үшін ынталандырудың тағы бір көзі-деректерді бұзу. Бұл жағдайда қандай да бір пайдалы функцияларды орындайтын бұл бағдарлама кез келген сыртқы көріністерсіз біздің пайдаланушымыздың файлдарын жояды.

2.3.2 Вирустар. Вирус - бұл басқа бағдарламаларды түрлендіру арқылы «зақымдайтын» бағдарлама. Модификацияланған кодқа вирустың осындай коды енгізіледі, соның нәтижесінде біздің вирустың коды басқа пайдаланылатын бағдарламаларға жұқтыруды жалғастырады.

Компьютер жүйесіне енгізілген мұндай вирус уақытша компьютердің операциялық жүйесін басқара алады. Содан кейін, бағдарламалық қамтамасыз ету жұқтырылмаған жұқтырған компьютермен әрбір байланыста болған кезде вирустың кезекті көшірмесі жаңа бағдарламаға салынады. Осылайша, мұндай жұқпа бір компьютерден басқа компьютерге ішкі жинақтағыштарды алмасатын немесе корпоративтік желі бойынша бағдарламаларды жіберетін ештеңе күдікті емес пайдаланушылармен

беріледі. Басқа компьютерлердің қосымшалары мен жүйелік қызметтеріне қол жеткізу мүмкіндігі бар мұндай желі кез келген вирустың таралуы үшін тамаша орта болып табылады.

2.3.3 «Құрттар» (черви). Желілік бағдарламалар – «құрттар» - бұл бір жүйеден екіншісіне тарату үшін желілік қосылыстарды қолданатын бағдарламалар. Олардың қандай да бір жеке дербес компьютерінде жұмыс істеу кезінде желілік «құрт» өзін компьютерлік вирус ретінде ұстайды немесе «троян атын» енгізеді, немесе қандай да бір басқа қирату немесе бүлдіру функцияларын орындайды. Желілік «құрт» көбею үшін ақпаратты жеткізудің желілік құралдарының бірін пайдаланады. Мысалдар құралдарының қызмет мынадай қызмет:

– электрондық пошта, "құрт" көшірмесін пошта арқылы басқа жүйеге жібергенде;

– «құрт» кез келген басқа жүйеде көшірмені іске қосқан кезде бағдарламаларды қашықтан шақыру;

– «құрт» қашықтағы жүйеге авторизацияланған пайдаланушы ретінде кіргенде, содан кейін жүйенің бірінен екіншісіне өзін көшіру командасын пайдаланады.

Бағдарламаның жаңа көшірмесі – «құрт», соның нәтижесінде жойылған жүйеде іске қосылған болып табылады, онда қалған барлық толықтыруларға «құрт» операциялары жоғарыда көрсетілген тәсілмен көбейтіле береді.

Желілік «құрт» көп жағдайда компьютерлік вирусқа ұқсас: оның инкубациялық кезеңі, сондай-ақ таралу фазасы, активтендіру фазасы және орындау фазасы бар. Тарату кезеңі келесі міндеттерді орындайды:

– тек осы компьютерге белгілі тораптардың немесе осы қашықтағы жүйелердің мекен-жайлары туралы ақпаратты сақтайтын басқа да ұқсас нысандардың тізімін тексеру арқылы жұқтыруға болатын жаңа жүйелерді іздеу;

– қашықтағы жүйемен байланыс орнату;

– кодыңызды қашықтағы жүйеге көшіру және оны іске қосуды бастау.

Жаңа жүйеге өзін көшірмес бұрын, желілік «құрт» бұл жүйе бұрын жұқтырмағанын тексеруге тырысады. Көп пайдалы ортада ол қандай да бір жүйелік процеске сәйкес келетін қандай да бір атауды тағайындау арқылы немесе жүйелік әкімшіде күдік тудырмайтын қандай да бір басқа атауды пайдалану арқылы өзінің қатысуын жасырады.

Желілік «құрттармен» күресу қиын. Бірақ, жеке компьютерлік жүйелерді қорғау шараларымен бірге, оларды дұрыс әзірлеу және қолдану шартымен, «құрттар» болып табылатын қауіпті айтарлықтай азайтатын желілік қорғаныс шаралары бар.

Вирустарды табу проблемалары үшін тамаша шешім жұқтырудың алдын алу, яғни вирустың компьютерлік жүйеге бастапқы енуіне тыйым салу болып табылады. Бұл мақсатқа жету мүмкін емес, бірақ кейбір шаралар вирустармен табысты аяқталған шабуылдардың санын азайтуы мүмкін. Вирустарды анықтауға қойылатын талаптар**:**

– табу. Егер жұқтыру орын алса, онда ол вирустың мекендеу орны анықталса;

– сәйкестендіру. Вирусты жұқтырғаннан кейін бағдарламаны жұқтырған вирустың осы түрін анықтау қажет;

– жою. Вирус сәйкестендірілген соң, осы вирустың барлық іздерін жұқтырған бағдарламалардан алып тастау қажет және бағдарламаны олардың бастапқы түріне қалпына келтіру қажет. Ауру одан әрі таралмауы үшін барлық жұқпалы жүйелерден вирустың жойылуы өте маңызды.

Егер вирус байқалса, бірақ оны жүйеден анықтау немесе жою мүмкін болмаса, онда іс-әрекеттің баламасы инфекцияланған бағдарламаны жою болып табылады.

2.3.4 Ақпараттық жүйелерді вирусқа қарсы қорғауға қойылатын талаптар. Қарапайым корпоративтік желі жүздеген жұмыс станцияларынан, он серверден, белсенді және пассивті телекоммуникациялық құрал-жабдықтардан тұрады және айтарлықтай күрделі құрылымы бар. Бірақ бұл желіге қызмет көрсету құны оған қосылатын объектілер санының ұлғаюымен бірге қарқынды өсуде. Антивирустық қорғау шығындары жалпы шығындар тізімінде соңғы емес пункт болып табылады. Алайда осы корпоративтік желіні қорғаудың барлық антивирустық кешенімен орталықтандырылған орнатуды, басқаруды және жаңартуды іске асыру жолымен оларды азайту мүмкіндігі бар.

Вирусқа қарсы қауіпсіздік жүйесін бастапқы жобалау кезінде қорғалған барлық нүктелерді анықтау қажет және корпоративтік желінің үлкен архитектурасын нақты функционалды модельге келтіру қажет.

Қарапайым функционалды модельдің мысалы 2.3 суретте келтірілген.

2.3 сурет – Корпоративтік желінің функционалдық моделі

Бұл модельде сервистік және желілік деңгей көрсетілмеген, егер жүйенің осы деңгейлерінде антивирустық бақылауды қамтамасыз ету қажеттілігі болса, онда оларды функционалдық үлгіге қосу қажет.

Осы корпоративтік желіде антивирустық қауіпсіздік жұмыс станциялары мен серверлерде орнатылған антивирустар есебінен ғана қамтамасыз етілмейді. Бірақ бүгін корпоративтік желінің барлық учаскелерін бақылайтын бір өнім жоқ [11]. Бұл жағдайда кәсіпорында қолданылатын барлық вирусқа қарсы өнімдерді орталықтандырылған бақылау және басқару туралы ұмытпау қажет.

Желі әкімшісі бірыңғай консольден вирустардың ену нүктелерін қадағалап, оларды кәсіпорын желісінде бар вирусқа қарсы қорғау нүктелерін тиімді басқаруы қажет. Бүгінгі күні вирусты индустрияның дамуы, әкімшіде осындай тұтқаның болмауы компанияның осындай желісінің бірнеше объектілерін бақылауды жоғалтуға алып келеді, ал нашар жағдайда – антивирустық қорғау жүйесінің барлық бөлігіне жалпы бақылауды жоғалтуға алып келеді. Бұл жаңа осалдықты және осы осалдықты пайдаланатын құрт пайда болған кезде – «Zero-day» орын алады [11].

Кешенді орталықтандырылған басқаруды құрудың күрделілігі антивирустық қорғау үшін тиімді осындай корпоративтік жүйелерді табысты құрудың күрделі міндеттерін шешу болып табылады, бұл осы компьютерлік вирустардың біздің корпоративтік желілерге енуінің ықтимал қаупіне алып келеді.

Ақпараттық жүйені антивирустық қорғау жүйесінің құрылымын түпкілікті анықтау үшін оның функционалдығына тағы не енгізу қажет деп ойлану қажет. Мұндай жүйелерге қойылатын талаптар бар, ақпараттық қауіпсіздікті басқарудың осы саласындағы халықаралық, ең беделді, стандарт – ISO 17799 стандарты [5].

Талаптар антивирустық шешімдерді пайдалану өнімділігі мен ыңғайлылығы туралы ұғымдарды қамтиды. Құны сондай-ақ антивирустық шешімді таңдауда маңызды рөл атқарады, себебі бұл Компанияның барлық корпоративтік желісінің сенімді жұмыс істеуін қамтамасыз ететін тікелей шығындар.

Өндірушінің лицензиялық саясатына назар аудару маңызды. Кәсіпорындардың корпоративтік желілерінің сегментіне арналған өнімдерді кейбір өндірушілер «LicenseForceCheck» әлі күнге дейін қамтиды.

Вирустарды анықтаудың тиімділігі өте маңызды, өйткені осы антивирустық БҚ сатып алу мен пайдалануға біздің қаржылық шығынымызды тікелей ақтайды.

Осы антивирустық бағдарламалық қамтамасыз етуді орталықтандырылған басқару мүмкіндігі жеткілікті өзекті, өйткені соңғы пайдаланушылар жұмыс істеу қабілеттілігін және өзінің жұмыс станцияларында антивирустық қорғауды жаңартуды үнемі қолдайды. Бұл ретте жүйелік іркіліс нәтижесінде жаңылыс және жаңарту жүйесінің өзі орын алады. Ал бұл бүкіл жүйенің осалдығы болады.

Бүгінгі таңда өз жұмысын қашықтан орындайтын, корпоративтік желі ресурстарына қашықтан қосылатын, вирустардың енуіне жаңа қауіп төндіре отырып, осындай пайдаланушылардың көп саны бар. Сондықтан әкімші оларды жергілікті пайдаланушылар сияқты вирусқа қарсы қорғау деңгейінде қолдау қажет.

Ұжымдық пайдалану үшін антивирустық бағдарламалық қамтамасыз етудің, үйде пайдалану үшін бағдарламалық қамтамасыз етуден басты айырмашылығы – бұл баптауларды көбірек нақтылаудың қажеттілігі. Корпоративтік желінің әр түрлі объектілері үшін талаптар түбегейлі ерекшеленеді. Вирусқа қарсы бағдарламалардың көптеген өндірушілері бүкіл қауіпсіздік кешенін баптау бойынша мүмкіндіктерді кеңейтуді қажет деп санамайды.

Осылайша, вирустық қауіптер қазіргі заманғы ақпараттық жүйелер үшін үлкен қауіп төндіреді. Бұл бұзушылықтар статистикасының зерттеулері мен осы саладағы сарапшылардың пікірі. Бұдан қазіргі заманғы жүйелердегі вирусқа қарсы қорғаудың тиісті деңгейін қамтамасыз ету қорғаудың жалпы бағдарламасының ажырамас бөлігі болып табылады және вирустық белсенділік мәселелері бірінші кезекте қауіпсіздік кепілдігінің тиісті деңгейін қамтамасыз ету үшін шешіледі деген қорытынды жасауға болады.

2.4 VPN шешімдері

Деректерді беру үшін ғаламдық компьютерлік желілерді кеңінен қолдану компаниялардың жергілікті желілерін біріктіруге және аумақтық таратуға және жеке виртуалды желілерді (VPN) құруға мүмкіндік береді. Ғаламдық желі бірыңғай ақпараттық-есептеу кешені ретінде қызмет етеді. VPN желілерін құру тұрақты жалғасуда:

– бөлінген байланыс арналарын жалға алудың жоғары құнына;
– орынға қатты байланыстыру.

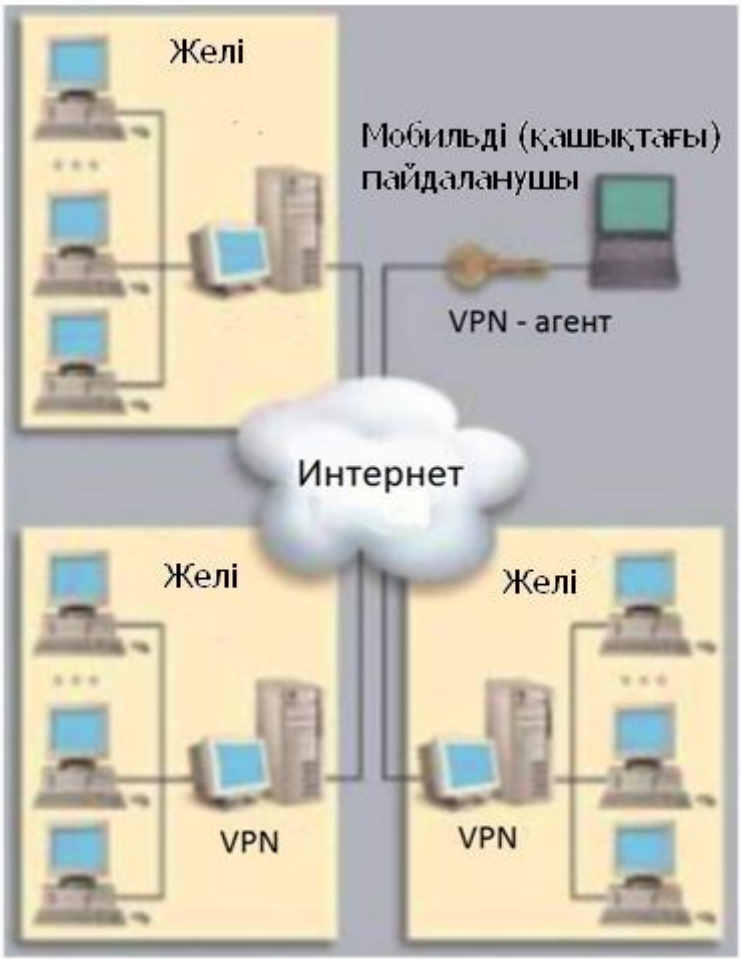
Деректерді берудің жаһандық желілерінің коммутацияланатын арналарын пайдалану енді VPN желілерін құру кезінде икемділікке, масштабталуға және әмбебаптыққа қол жеткізуге мүмкіндік береді. Интернет желісін кеңейту көптеген компанияларға өз қызметкерлерінің бір бөлігін үй жұмыс режиміне – алыстан аударуға мүмкіндік береді. Бұл жағдайда қызметкер әрдайым электронды құжат айналымы сияқты жүйелер аясында компаниямен тұрақты байланыста болады және оны компанияның желісіне қосу проблемалары провайдермен байланысты.

IP хаттамасы негізінде салынған желілердің қауіпсіздігін қамтамасыз ету қажеттілігі үнемі өсіп келеді. Интернет желісіне, интрасет, еншілес бөлімшелерге қол жеткізу немесе алыстан қол жеткізу болған жағдайда өте маңызды ақпарат осы желілердің шекаралары арқылы үнемі қозғалады. Желілік әкімшілердің және басқа да ақпараттық қызмет мамандарының міндеті осы трафик жол бермеуі:

– арналар арқылы жіберу кезінде деректерді түрлендіру;
– құрылғыны ұстап қалу, көру немесе көшіру;
– авторланбаған пайдаланушылар тарапынан деректерге қол жеткізу.

Көрсетілген мәселелер әлі де деректер тұтастығын, құпиялылықты және аутентификацияны қамтамасыз ету ретінде белгілі. Сонымен қатар, ақпаратты ойнаудан қорғау қажет.

Интернет желісінің ашық арналары арқылы ақпаратты берудің осы проблемасын шешу үшін виртуалды VPN шешімдерін қолданады. VPN - бұл ортақ пайдалану желісіне, бірыңғай виртуалды (логикалық бөлінген) желіге қосылған бірқатар жергілікті желілерді біріктіру. VPN құралдары криптография арқылы екі нүкте арасында қорғалған туннель ұйымдастырады. Бұл ретте аутентификация алгоритмдерін, шифрлеу және деректер ағынының тұтастығын тексеру әдістерін таңдау бойынша кең мүмкіндіктер беріледі [7].



2.4 сурет – VPN технологиясына негізделген аумақтық-бөлінген ақпараттық жүйе

VPN желісін пайдалану кезінде біздің компанияның ресурстары оңай біріктіріледі және үлкен тиімділікпен пайдаланылады. VPN желісі қолданыстағы интернет желісінің архитектурасы базасында жұмыс істейтіндіктен және компанияда қосымша жабдықты сатып алу мен байланыс желілерін жалға алумен байланысты қосымша шығындар туындамайды. Бөлінген (жалға алынған) байланыс желілерін пайдалану шығындарды жүз

мың долларға дейін арттыруға алып келеді, ал мұндай шығындарды ақтау өте қиын.

VPN желісін құрудың басты артықшылығы бір тетікті пайдалана отырып, көптеген коммуникациялық ағындардың қауіпсіздігін қамтамасыз ету болып табылады. VPN - web, e-mail, ftp, интернет-бейнеконференция және кез келген басқа деректер ағындары қосылған кезде TCP/IP протоколын пайдаланады, қызықты көздерден қорғалады.

VPN көмегімен көптеген қауіптердің алдын алуға болады. VPN желісі арнайы протоколдар мен аутентификация схемаларын қолданып шифрлау, аутентификация арқылы деректердің тұтастығы мен құпиялығын қамтамасыз етеді. Сонымен қатар, VPN желісі құралдары IP-spoofing және Hijacking сияқты желілік шабуылдардың қатарынан IP пакеттерін тасымалдауға қатысты ақпаратты жасыру есебінен қорғалған, сондай-ақ олар Man-in-the-Middle типті шабуылдардан қорғалған [28]. VPN желісін құру немесе оны аппараттық іске асыру үшін БҚ іске асыру осал болуы мүмкін, бірақ әдетте тәжірибеде өз өнімдері үшін тұрақты жаңартуларды және төлетуді шығаратын белгілі әзірлеушілердің уақытпен тексерілген шешімдерін қолданады.

VPN шешімдеріне қойылатын негізгі талаптар:

– пайдаланушы аутентификациясы. Құрал қашықтағы VPN-Клиентті аутентификациялайды және тек авторизацияланған пайдаланушыларға рұқсат береді. Пайдаланушылардың белсенділігін көру үшін аудит саясатын қамтамасыз ету керек: кім, қашан және қанша қосылған;

– IP-мекен-жайларды басқару. VPN құралы ішкі желінің мекен-жайларын шығарады және бұл мекенжайлар табылмайтынына кепілдік береді;

– мәліметтерді шифрлау. Жалпыға қол жетімді желілер арқылы берілетін мәліметтер оқылмауы керек;

– негізгі ақпаратты басқару. VPN құралы шифрлау үшін кілттерді қалыптастырады және оларды жүйелі түрде жаңартады.

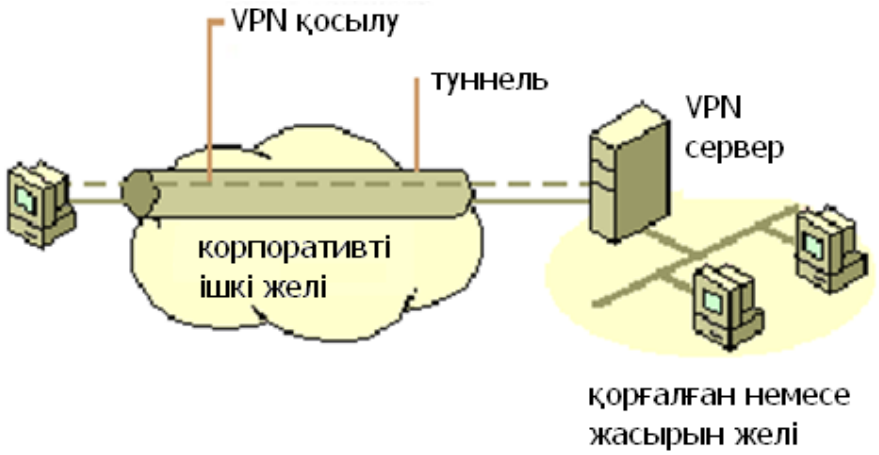
Корпоративтік VPN желілерін құру кезінде қолданылатын VPN желісін құрудың төрт негізгі нұсқасын бөліп көрсетуге болады:

а) ашық байланыс арналары арқылы өзара іс-қимыл жасайтын бір компанияның бірнеше таратылған филиалдарын бірыңғай қорғалған желіге біріктіруге мүмкіндік беретін «Intranet VPN» нұсқасы (2.5 сурет). Шешімнің бұл нұсқасы бүкіл әлемде кең таралған. Бұл нұсқа «желі-желі» типті топологиясын білдіреді. Бұл конфигурацияда әрбір шлюздер осы желінің соңында орналасқан және екі желі арасындағы байланыс арнасының қауіпсіздігін қамтамасыз етеді. Конфигурацияның бұл түрі аумақтық жағынан бөлінген жергілікті желілерді қосу үшін ең қолайлы. Бұл жергілікті желі конфигурациясының басты артықшылығы - VPN конфигурациясындағы қашықтағы жергілікті желілер соңғы пайдаланушы үшін мөлдір болып табылады. VPN шлюздері пайдаланушы үшін маршрутизатор болып табылады. VPN «желі-желі» типінің құрылымы ішкі желілердің байланысы үшін де, аралас арналар үшін де қолданылады. Интранет желілері арасында

берілетін деректер осындай беру кезінде құпиялылықты сақтай алады. Бұл схема бірнеше компанияның сыртқы желілері (extranet) үшін қолданылады, онда әрбір компанияның бизнес бойынша серіктестермен ғана бөлісетін бір ресурсы бар;

2.5 сурет – Желі-желі сұлбасының қосылуы

б) корпоративті желінің екі торабы (желілері емес) арасындағы берілетін деректердің қорғалуын қамтамасыз ететін «Клиент/Сервер VPN» типті қосылу мүмкіндігі (2.6 сурет). Мұндай нұсқаның ерекшелігі, әдетте, осы желінің бір сегментінде орналасқан тораптар арасында VPN құрылысында, мысалы, жұмыс станциясы мен сервер арасында. Бұл қажеттілік бір физикалық желіде бірнеше логикалық жасау қажет болған жағдайларда туындайды. Қажет болған жағдайда маршрутизаторлармен бір физикалық сегменттегі серверлерге жүгінетін бухгалтериялар мен кадрлар бөлімі арасында трафикті бөлу. Бұл опция арнадан жоғары деңгейде болатын VLAN технологиясына өте ұқсас;

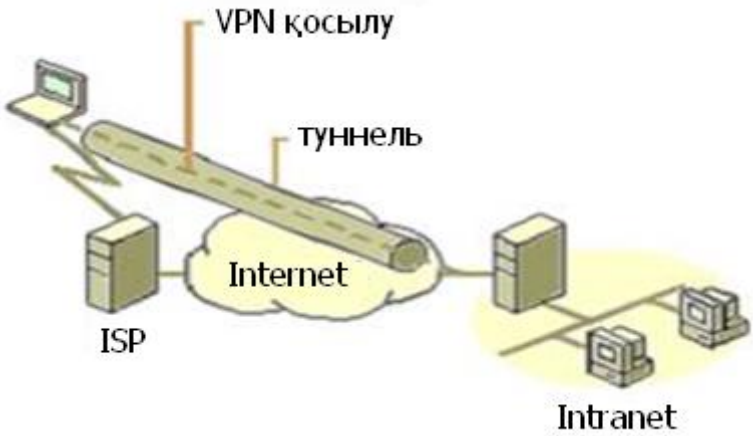


2.6 сурет – VPN желісіне екі стационарлық компьютерді қосу

в) "Extranet VPN" типінің нұсқасы, ол өз қызметкерлеріне қарағанда сенім деңгейі айтарлықтай төмен бөгде пайдаланушылар қосылатын желілерге арналған. Мұндай Extranet VPN шешімінің мысалы-бірлескен жұмыс жүргізу үшін түрлі компаниялардың желілерін біріктіру;

г) "RemoteAccess VPN" типінің нұсқасы, ол осы корпоративтік желі сегменті (орталық офис немесе филиал) мен үйден корпоративтік ресурстарға (үй пайдаланушысы) немесе notebook (мобильді пайдаланушы) арқылы қосылатын жалғыз пайдаланушылар арасында қорғалған өзара іс-қимылды жүзеге асыруға мүмкіндік береді. Бұл опция қашықтағы пайдаланушының мекен-жайларымен ерекшеленеді, әдетте ол "статикалық" мекен-жайы жоқ және қорғалатын ресурсқа қосылу бөлінген VPN құрылғысы арқылы емес, VPN технологиясын іске асыратын бағдарламалық жасақтама орнатылған өз компьютерінен тікелей алады. Бұл әдіс мобильді пайдаланушыларға осы корпоративтік желімен байланысты қамтамасыз етуге мүмкіндік береді және желіні виртуалды қорғауға, немесе құрылымға, vpn хост-желісіне мүмкіндік береді. Бұл конфигурацияда әрбір хост бір-біріне қарамастан VPN шлюзі арқылы жергілікті желімен байланысады. Әрбір хост аутентификацияны жүзеге асырады және ол үшін арнайы қорғалған VPN-туннель ұйымдастырылады. Ұялы хост кез келген тәсілдермен қосылады, олардың ішінде коммутацияланатын желі (dial-up), жергілікті желіге қосылу немесе сымсыз байланыс.

"Хост-желі"типінің құрылымы алыстан қол жеткізу орнатылған жағдайда ұтады. Ұялы пайдаланушы өзінің портативті компьютерінде VPN бағдарламалық жасақтамасы бар VPN шлюзі арқылы ішкі есептеу желісімен қосыла алады. VPN желісінің осы схемасы үйде жұмыс істейтін қызметкерлер үшін (өз компьютерінен) қолданылады. Сандық және кабельдік модем желілерін ұйымдастыру үшін пайдаланудың өсуі үйден алыс жұмыс істеу үшін тартымды мүмкіндік береді. VPN технологиясы VPN корпоративтік шлюзіне түскен кезге дейін құпия және оқылмайтын ақпараттық алмасу ағынын жасайды.



2.7 сурет – Қашықтағы пайдаланушыны VPN желісіне қосу

Деректерді берудің жаһандық желілері негізінде құрылған VPN шешімдерінің кең таралуы оларды потенциалды бұзушының қолда бар шабуылдарына қатысты жеткілікті әлсіретеді, өйткені мұндай конфигурация хаттамалар стегінің барлық осалдығын иеленеді. Сонымен қатар, IP және/немесе IPX протоколдары бойынша ақпараттық пакеттер түрінде жіберілетін құпия деректерді беру үшін Internet желісін жиі пайдаланатындықтан, көліктік хаттама ретінде TCP/IP стегі қолданылады. Ақпараттық қауіпсіздікті қамтамасыз етуге арналған құралдар IP-пакеттерге ауыстырылады, басқа пакеттердің ішіне салынады, одан кейін Internet желісі арқылы маршрутталады. Ақпараттық ағын басқа ақпараттық ағынға өзгеруі мүмкін, осылайша туннелдеу процесі жүреді. Мұндай жағдайда берілетін IP-пакетіндегі деректер өрістері ғана емес, сонымен қатар оның адрестік бөлігі, сондай-ақ осы деректердің қызметтік өрістері шифрланады.

Сонымен қатар, VPN желісі бойынша ақпаратты тарату үшін қолданылатын негізгі хаттамаларға бағыттаудың төрт хаттамасын жатқызуға болады: Layer 2 ForwardingProtocol (арналық деңгейді тарату ХАТТАМАСЫ), Layer 2 TunnelingProtocol (арналық деңгейді туннелдеу ХАТТАМАСЫ), Point-to-PointTunnelingProtocol (нүкте-нүкте түріндегі туннелдеу хаттамасы), сондай-ақ IETFC комитетімен ұсынылған IP Security (IPSec) хаттамасы.

Қазіргі уақытта SSL/TLS протоколы негізінде VPN үшін SSL технологиясын пайдалану өсуде, ол WEB-браузерлерде қосылыстарды қорғау үшін қолданылады.

SSL (SecureSocketsLayer) қорғалған хаттамасының негізіндегі виртуалды жеке желі Интернет желісі және стандартты веб-браузер бар әлемнің кез келген нүктесінен корпоративтік ресурстарға қашықтан қол жеткізу мүмкіндігін алатын әрбір авторизацияланған пайдаланушыға корпоративтік желілік қызметтерді қауіпсіз ұсынуға арналған. SSL протоколы бойынша веб-браузерді және кіріктірілген шифрлау жүйелерін пайдалану корпоративтік желіге үй жеке компьютерлері, Интернет дүңгіршектері немесе Wi-Fi сымсыз құрылғылары сияқты кез келген қашықтағы құрылғылардан, яғни VPN желісінің клиенттік бағдарламалық жасақтамасын орнату және IPSec протоколымен VPN байланысын құру үлкен қиындықтармен ұштасқан кез келген нүктеден қатынауды қамтамасыз етеді. Әкімшілер кез келген пайдаланушы үшін жеке веб-сайттарға және корпоративтік бағдарламаларға кіру параметрлерін реттейді. Корпоративтік желіаралық экрандар SSL протоколы бойынша қосылуды қолдайтын болғандықтан, желіні қосымша күйге келтіру қажет емес. Нәтижесінде SSL/VPN технологиясы желіаралық экранды пайдалануды айналып өтіп, желінің кез келген нүктесінен қатынауды қамтамасыз етеді.

VPN желісін құру үшін барлық өнімдер екі санатқа бөлінеді: бағдарламалық және аппараттық. VPN желісіне арналған бағдарламалық шешім желіге қосылған жеке компьютерге орнатылған дайын қолданбадан тұрады. Axent Technologies, Check Point Software Technologies және NetGuard сияқты бірқатар өндірушілер бағдарламалық желіаралық экрандармен оңай

интеграцияланатын және Windows NT/2000, SunSolaris және Linux сияқты әртүрлі операциялық жүйелерде жұмыс істейтін VPN-пакеттерді жеткізеді. Сонымен қатар, VPN желісін құру үшін, арнайы бағдарламалық қамтамасыз етуге негізделген жеке компьютерлік жүйені құру қажет және бұл шешімдер аппараттық қамтамасыз етумен салыстырғанда өрістету үшін қиын. Мұндай жүйені құру осы компьютерді және оның операциялық жүйесін тану үшін серверді конфигурациялауды, VPN -пакетті, кез келген қосылу үшін желілік платаларды және шифрлау операцияларын жеделдету үшін арнайы платаларды қарастыруы мүмкін. Бұл жұмыс тәжірибелі мамандар үшін де қиын. VPN-дің бағдарламалық аппараттарынан айырмашылығы қосылу үшін қажетті элементтерден тұрады-бұл компьютер, жеке операциялық жүйе және арнайы бағдарламалық қамтамасыз ету. Аппараттық шешімдерді қолдану әлдеқайда оңай. Өйткені олар нақты шарттар үшін қажет, сондықтан оларды іске қосуға болатын уақыт минутпен немесе сағаттармен есептеледі. Vpn аппараттық шешімдердің тағы бір маңызды артықшылығы жоғары өнімділік болып табылады. VPN аппараттық шешімдердің кемшіліктері арасында олардың жоғары құнын атап өтуге болады. Шешімдердің тағы бір кемшілігі қауіпсіздік жөніндегі басқа шешімдерден бөлек басқару болып табылады, бұл әсіресе ақпаратты қорғау бөлімінің қызметкерлері жетіспеген жағдайда, қауіпсіздік инфрақұрылымын әкімшілендіру міндетін қиындатады.

Сонымен қатар, VPN желісі мен бүкіл компания ауқымындағы желіаралық экрандар үшін келісілген қауіпсіздік ережелерін қолдау және vpn құрылғыларын басқару проблемасына тап болу керек. Егер қызметкерлердің осы салада жеткілікті дағдылары болмаса, онда виртуалды жеке желіні құру үшін тиісті қызметтер көрсететін тәуелсіз компанияға жүгінуге болады.

VPN шешімдерін пайдалану арнайы қауіпсіздік құралдарынан бас тартуға себеп емес. Қазіргі статистика бойынша бүгінгі күні ақпараттық қауіпсіздікке байланысты барлық проблемалардың шамамен 80% - ы осы корпоративтік желіге рұқсат етілген рұқсаты бар авторландырылған пайдаланушылардың кінәсінен болды, бұл мұндай пайдаланушыдан шабуыл немесе вирус шифрланады және зиянсыз трафикпен тең беріледі [30]. Осы технологияны пайдалану желінің өнімділігін төмендетеді, бұл VPN-құрылғылар арасында қорғалған қосылуды орнатудың кідірістерімен, деректерді шифрлаудың кідірістерімен, олардың тұтастығын бақылаудың кідірістерімен және пакеттердің ұзын тақырыптарын пайдаланудың артынан ұлғайған трафиктермен байланысты.

VPN құралдары деректерді ашық байланыс арналары арқылы қауіпсіз беруді жүзеге асырады және деректерді әр түрлі қауіптерден сенімді криптографиялық қорғауды қамтамасыз етеді. VPN шешімдерін пайдалану кезіндегі қорғаныс деңгейі оларды теңшеу дұрыстығына байланысты, бұл жүйелік әкімшінің белгілі бір біліктілік деңгейін және VPN технологиясын және пайдаланылатын хаттамаларды білуді талап етеді.

2.5 Парольдік қорғауды ұйымдастыру

2.1-кестеде паролді қорғауды ұйымдастыру жөніндегі ұсынымдар келтірілген.

Кесте 2.1 – Құпия қорғау саясаты

Саясат	Ұсынылатын баптаулар
Құпия сөз тарихы сақталады	24 құпия сөз
Парольдің ең ұзақ әрекет ету мерзімі	24 күн
Парольдің ең аз әрекет ету мерзімі	4 күн
Парольдің минималды ұзындығы	8 таңба
Құпия сөз күрделілік талаптарын қанағаттандыруы тиіс	Қосылған
Құпия сөз домендегі барлық пайдаланушылар үшін кері кодтау арқылы сақталады	Ажыратылған

Күрделілік талаптары:

Топтық саясаттың баптаулары қосылған кезде «пароль күрделілік талаптарын қанағаттандырады», онда парольдің ұзындығы кем дегенде 6 символды құрайды. Талаптарға сәйкес, пароль кемінде үш түрдегі символдарды қамтуы тиіс:

Ағылшын бас әріптері A, B, C, …, Z

Ағылшын жазбаша әріптері a, b, c, …, z

Араб сандары 0, 1, 2, …, 9

Алфавитті емес символдар – мысалы, тыныс белгілері.

Ескерту: құпия сөз саясаты Windows 2000 серверлерінде ғана емес, тіркеу үшін құпия сөзді талап ететін әрбір құрылғыларда да орнатылады. Маршрутизаторлар мен коммутаторлар арасында желілік құрылғылар, егер құпия сөзді қолданса, кез келген бұзу үшін осал. Зиянкестер осындай желілік құрылғыларға оңай бақылау орната алады және брандмауэрлерді айналып өтеді.

Сондай-ақ компанияда резервтік көшіруді ұйымдастыру және штаттан тыс жағдайларда іс-қимыл тәртібі жөніндегі нұсқаулықты міндетті түрде әзірлеу қажет.

2.6 Тапсырманы қою

Компанияның ақпараттық қауіпсіздігіне төнетін қатерлерді төмендету және құпиялылықтың, тұтастықтың, қолжетімділіктің, қадағалаудың және дәлме-дәлдіктің бұзылу қатерлерін азайту жөніндегі іс-шараларды іске асыру үшін желіаралық экрандар негізінде шешімдер таңдап алынды, сондай-ақ компанияның желісі VPN-шешімдер негізінде құрылады. Бұл іс-шаралар ViPNet бағдарламалық өнімі базасында жақсы жүзеге асырылады, ол:

– жергілікті желілер арасындағы байланыс арналарын шифрлау;

– желілік шабуылдардан жергілікті желілерді қорғау, трафикті сүзу, NAT;

– VPN бойынша корпоративтік ресурстарға (серверлерге, порталдарға, деректер қорына, IP-телефония және т. б.) қорғалған қашықтан қол жеткізуді ұйымдастыру.

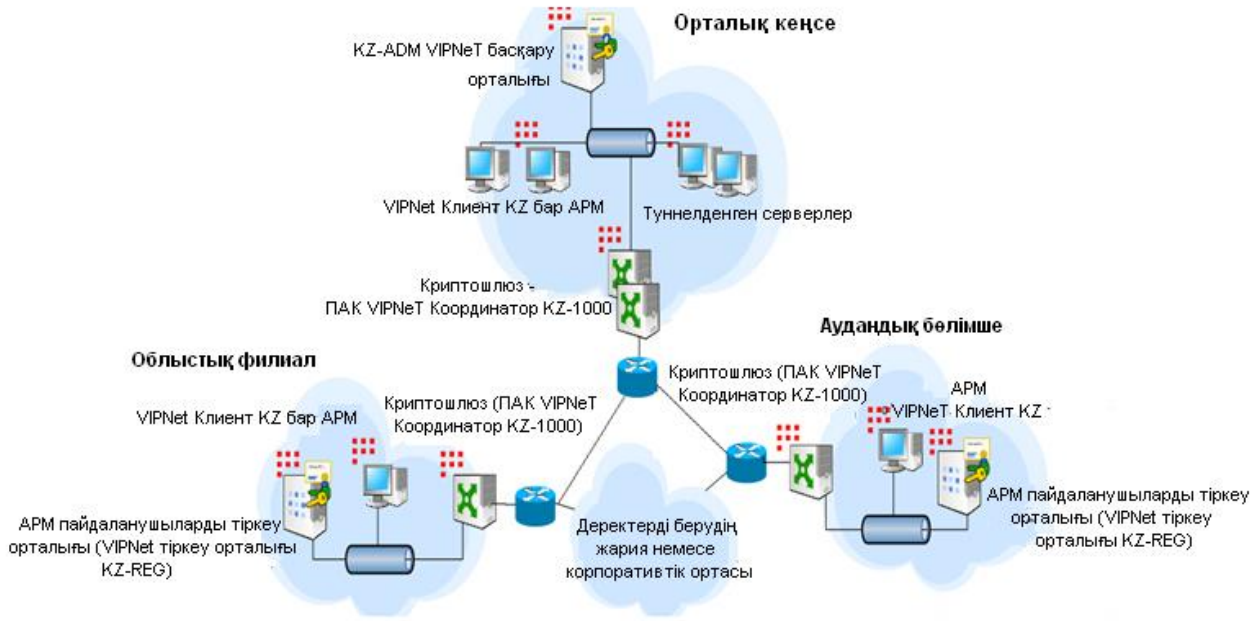
Жұмыс станциялары мен серверлердің операциялық жүйесін қорғау үшін Касперский зертханасының базасында антивирустық қорғаныс таңдалды.

Сонымен қатар, пайдаланушының жұмыс станциялары мен құрылғыларында жүйеге кіру үшін парольдік қорғанысты орнату жүзеге асырылды және Windows ОЖ стандартты қосымшаларының негізінде іске асырылды.

Компанияда виртуалды жеке желінің барлық функциялары бар желі құрылған, ол компания кеңсесін филиалдармен және еелиенттермен байланыстыратын. Желі сұлбасы 2.8 суретте көрсетілген.

Жобада жаңа клиентті осы желіге қосу мүмкіндігін және оның клиенттік қосымшасын баптауды, сондай-ақ оның дербес деректерін қорғауды қарастырамыз.

Ол үшін Компанияның корпоративтік желісімен байланыс үшін ViPNet Client бағдарламалық қамтамасыз етуі және клиенттің жеке деректерін қорғау үшін VipNetSafeDisk пайдаланылды.



2.8 сурет – Компания желісінің схемасы

3 АҚ қауіп-қатерін төмендету жөніндегі шаралар кешенін әзірлеу

Клиенттің компания кеңселерімен байланысын ұйымдастыру кезінде ақпаратты қорғауды қамтамасыз ету үшін шаралар кешені әзірленді, онда:

– клиент пен компания филиалдары арасында ViPNet виртуалды жеке желісін құру;

– антивирус пайдаланып клиенттің ДК қорғау;

– VipNetSafeDisk арқылы клиентті жеке қорғау.

3.1 ViPNet ортасында пайдаланушыны орнату

Жобада ViPNet бағдарламалық кешені пайдаланылады, ол әртүрлі түрдегі байланыстың жалпыға бірдей қолжетімді арналары бойынша қауіпсіз ақпарат алмасу ортасын қалыптастыруға мүмкіндік береді. Бұл әрекет жоғары сенімділіктің криптографиялық құралдарымен қорғалған желінің логикалық контурларын құру кезінде қол жеткізіледі. Желінің мұндай контурлары екі түрге бөлінеді:

– жеке нұсқа ретінде электрондық құжат айналымын ұйымдастыру үшін ViPNet желісі;

– VPN технологиясының барлық функциялары бар ViPNet желісі.

Бұл ретте қамтамасыз ету қажет:

– интернет желісінің ашық арналары арқылы өту кезінде ақпараттық алмасуды қорғау;

– жергілікті желі ішіндегі ақпарат алмасуды қорғау;

– виртуалды қорғалған желінің сыртқы пайдаланушылардан құпиялылығы;

– мобильді пайдаланушылардың еркін санына қол жеткізу;

– осы виртуалды қорғалған желіге кіретін ресурстарды қоспағанда, ашық интернет ресурстарына виртуалды қорғалған желіні пайдаланушыларға қол жеткізуді шектеу.

Осы қорғауды ұйымдастыру үшін желінің келесі базалық элементтері қолданылады:

– ViPNet басқару орталығы (Administrator) – бұл осы желіні баптау және басқаруды қамтамасыз ететін базалық бағдарламалық немесе бағдарламалық-аппараттық кешен;

– ViPNet тіркеу пункті - бұл желіде пайдаланушыларды тіркеуді қамтамасыз ететін бағдарламалық немесе бағдарламалық-аппараттық кешен;

– ViPNet Publication Service – электрондық цифрлық қолтаңба сертификаттарын жариялауға арналған қызмет;

– Бұл жүйе желінің орталықтандырылған мониторингін қамтамасыз етеді;

– ViPNet Клиент - бұл бағдарламалық VPN-клиент, жеке экран, немесе қорғалған пошта жүйесінің клиенті;

– Pack ViPNet терминалы - пайдаланушының толық қорғалған жұмыс орнын ұйымдастыру үшін қызмет ететін терминалдық «жұқа» клиент.

ViPNet Клиент сондай-ақ желілік қорғауды және оны VPN желісіне жеке компьютерлерді қосуды қамтамасыз етеді. ViPNet Coordinator бағдарламалық қамтамасыз етуі бар Компьютер қолда бар жергілікті желілер мен сегменттердің шекарасында орнатылады, бұл қамтамасыз етуге мүмкіндік береді:

– бұл жергілікті желілерде немесе олардың сегменттерінде орналасқан ашық және қорғалған компьютерлерді мекен-жай түріне тәуелсіз VPN желісіне қосу;

– желілік шабуылдардан желілерді бөлу және қорғау, сондай-ақ ViPNet-пен компьютерді клиентпен онымен байланысты барлық желілік тораптардың жай-күйі туралы құлақтандыру.

ViPNet желісіндегі компьютерлер IP протоколын қолдайтын кез келген түрдегі жергілікті желілердің ішінде орналасады. Осы желіге қосылудың кез келген түрі таңдалады: Ethernet, ADSL арқылы Ppppoe хаттамасы бойынша, кәдімгі Dial UP немесе ISDN арқылы PPP, GPRS немесе Wireless ұялы байланыс желісі-құрылғылар, MPLS немесе VLAN желілері. ViPNet бойынша арналық деңгейдің әртүрлі хаттамаларына автоматты қолдау көрсетеді.

ViPNet желісінің компьютерлері желіде және желіаралық қорғаныс құрылғыларын пайдаланбастан және кез келген желіаралық экрандар мен мекенжайларды түрлендіру функцияларын орындайтын басқа да құрылғылар арқылы жұмыс істейді (NAT)

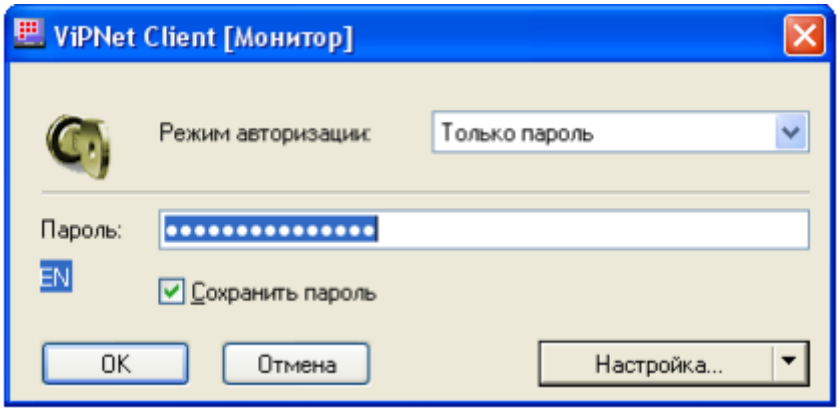
Виртуалды желінің бағдарламалық құралдарын пайдаланатын қолданыстағы жергілікті желілердің ішінде ақпараттық тәуелсіз, өзара қолжетімсіз немесе ішінара қиылысатын жабық (тәуелсіз) компьютерлер топтары құрылады.

Осы виртуалды желінің бағдарламалық құралдары VPN желісін құруға қатысатын жергілікті желінің компьютерлерін Интернет желісіне оңай қосуға мүмкіндік береді. Сонымен қатар, қорғалған қосылыстар үшін, мұндай жағдайда интернет желісінен берілген компьютерлерге (қорғалған және ашық) қолжетімділікке толық жол берілмейді, сондай-ақ олардың интернет желісінің қорғалмаған бос ресурстарына шығуын ұйымдастыру.

Мұндай виртуалды желінің қатысушысына қорғалған қосылыспен бір уақытта жергілікті немесе жаһандық желінің ашық ақпараттық ресурстарына біржақты қолжетімділікті қамтамасыз етуге, сондай-ақ осындай ашық трафикті сүзудің кез келген басқа типтеріне ие болуға мүмкіндік беретін арнайы технологиялар біздің берген қауіпсіздік саясатына сәйкес жүзеге асырылады.

Қорғалған трафик үшін жүргізілген күйге келтірулерге сәйкес оны сүзу қамтамасыз етіледі.

3.1.1 ViPNet клиентті орнату. Компьютерге жүктеп алған кезде парольді енгізу ұсынысымен пайдаланушыны анықтауға мүмкіндік беретін терезе пайда болады (3.2 сурет).



3.2 сурет – Пайдаланушыларды сәйкестендіру терезесі

Егер ViPNet клиент бірінші рет іске қосылған болса, онда пароль енгізу терезесінде «Настройка» кнопкасының оң жағындағы және пайда болған шыққан тізімдегі «Первичная инициализация» пунктін басу арқылы анықтамалық-кілттік ақпаратты бастапқы инициализациялау рәсімін орындау қажет (3.2 Сурет). Содан кейін инициализация шеберінің кеңестерін орындау қажет.

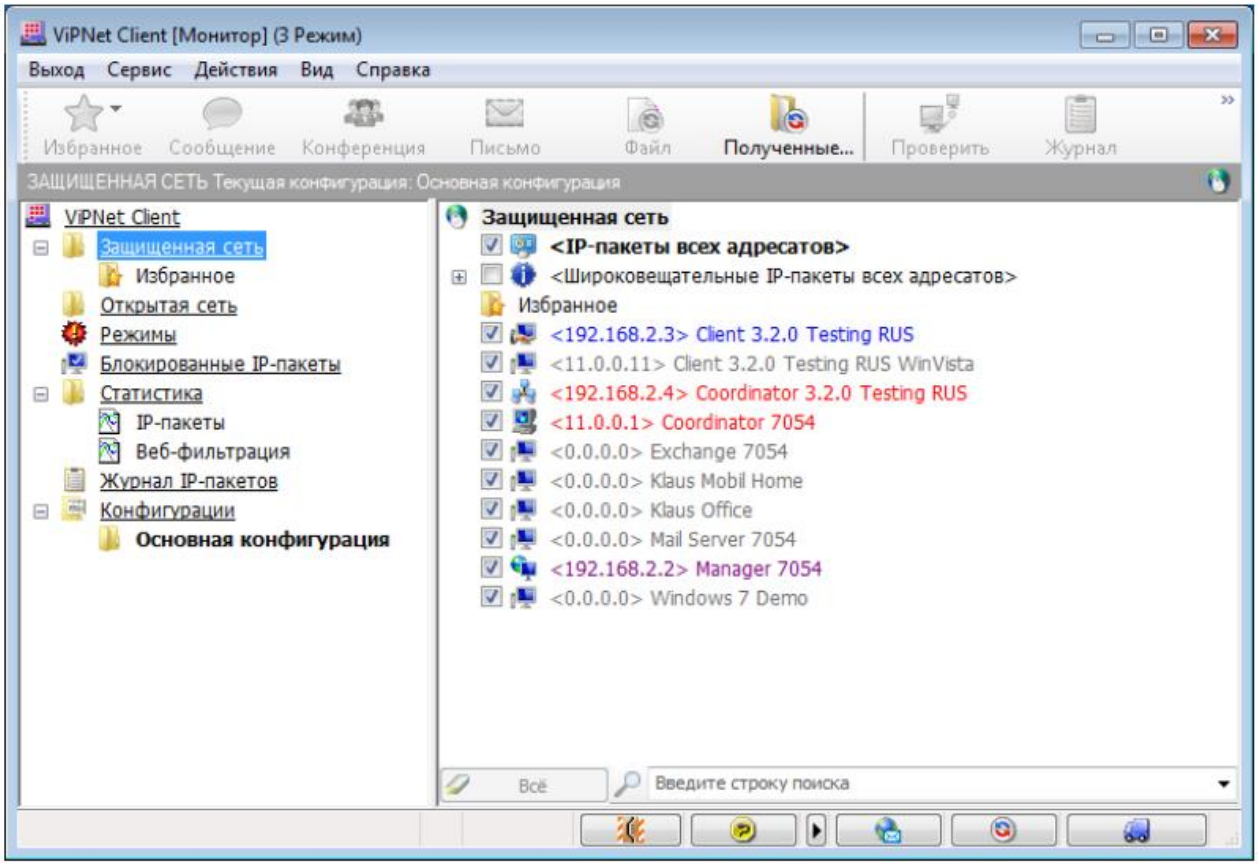
Клиентті бірнеше рет қосқан кезде құпия сөзді енгізу және/немесе деректерді сақтаудың сыртқы құрылғысымен байланысты қамтамасыз ету (авторландыру режиміне байланысты) және «ОК» батырмасын басу қажет.

Іске қосу және енгізілген парольдің дұрыстығын тексеру процесінен кейін, ViPNet бағдарламасының басты терезесі экранға шығады (3.3 сурет).

Құпия сөзді енгізгеннен кейін келесі тексерулерді жүзеге асыру қажет:

– егер компьютерде Клиент мониторының біреуден артық конфигурациясы жасалса, онда сақталған конфигурациялар тізімінен қажетті конфигурацияны таңдау қажет. Мұндай конфигурацияларды таңдау терезесі пайда болу үшін осы бағдарламаның «теңшеу\іске қосу» жалпы баптауларында және теңшеу терезесін «шақыру» флажогымен апатты аяқтауды жүзеге асыру қажет. Егер бұл флажок алынып тасталса, конфигурацияның ең соңғы нұсқасы жүктелген;

– электрондық қолтаңба кілті сертификатының қолданылу мерзімін тексеру қажет. Егер сертификаттың қолданылу мерзімі аяқталса, онда бұл туралы хабарлама пайда болады және жаңа кілт сертификатына сұраныс жасау ұсынылады. Бұл жағдайда «қауіпсіздік параметрлерін теңшеу» бағдарламасының ескертуі (егер қауіпсіздік параметрлерінің теңшелімдерінде осы сертификаттың әрекет ету мерзімінің аяқталғаны туралы хабарламаны көрсету флажогы алынбаса).



3.3 сурет – ViPNet Клиент бағдарламасының басты терезесі

Орталық басқару құрылғысында (немесе ViPNet Manager) орнатылған параметрлерге байланысты, клиент кез келген желіаралық экран арқылы жұмыс істеу үшін теңшеуге болады. Бағдарламаны алғаш іске қосқаннан кейін ViPNet арқылы жұмыс істеуге тілек білдіру туралы сұрақ қойылады. Бұл жағдайда сұраққа оң жауапты таңдау қажет.

Егер бағдарламаны жүктеу кезінде жергілікті желі байланысы үзілген болса, ол туралы хабар пайда болады. Бұл хабар пайда болған жағдайда, алдымен желі сымының қосылуын немесе модемнің қосылуын тексеру ұсынылады.

Осы терезенің пайда болуын өшіру үшін «орнату/ескерту» бағдарламасының жалпы параметрлерінде жергілікті желі мен қашықтағы қосылымдардың қол жетімсіздігі туралы хабарлар беру «флажогын алып тастау немесе хабар терезесінде» бұл хабарды одан әрі көрсетпеу флажогын орнату қажет.

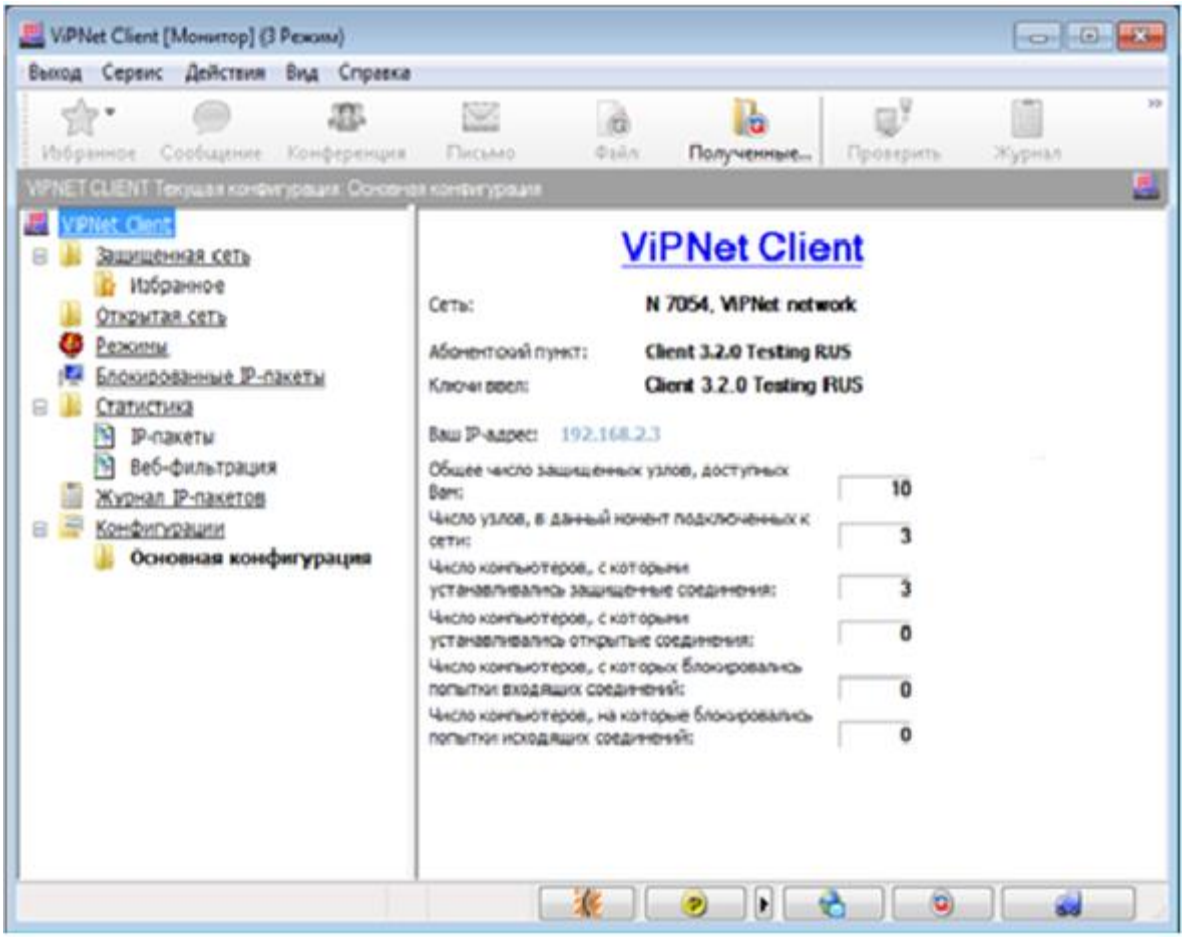
Бағдарлама тапсырмалар тақтасында хабарландыру аймағында іске қосылғаннан кейін ViPNet клиенттің іске қосылғанын білдіретін белгі пайда болады. Бұдан әрі шифрланған пакеттерді жіберу және жұмыс істеу кезінде бұл белгіше ақ түспен жарқырайды. Жұмыс барысында, бағдарламалық қамтамасыздандырумен тораптар арасында пошта ақпаратымен алмасу үшін ViPNet MFTP транспорттық модулі мезгіл-мезгіл жүктелді және хабарламалар саласында тапсырмалар панелінде белгіше пайда болады ( ).

Бағдарлама іске қосылғаннан кейін, сондай-ақ, әдепкі пайдаланушы тағайындаған қауіпсіздік режимі орнатылады, мысалы, тыйым салынғандардан басқа барлық шығыс байланыстарын босататын 3 режимі.

Бағдарлама жұмысын аяқтау үшін «шығу» басты мәзірінің тармағын таңдаңыз.

3.1.2 Бағдарлама параметрлерін баптау. «Теңшеу» терезесі бағдарлама параметрлерін баптауды қамтамасыз етеді, «Сервис/теңшеу» басты мәзірі арқылы ашылады. «Орнату» терезесі «Ctrl+Alt+S» ыстық пернелер комбинациясы арқылы да шақырылады.

Орнату терезесінде екі панель бар. Терезенің сол жағында панель теңшеу бөлімдерінің құрылымын көрсетеді. Панельдің оң жағында сол жақ панельде таңдалған теңшеу параметрлерінің тізімі көрсетіледі (3.4 сурет).



3.4 сурет – «Теңшеу» терезесі

Орнату терезесі келесі бөлімдерді қамтиды (3.5 сурет):

– жалпы бағдарлама параметрлерін теңшеу;

– әр түрлі оқиғалар туралы ескертулерді теңшеу жүзеге асырылатын ескерту;

– іске қосу және авариялық аяқтау, іске қосу және апатты аяқтау параметрлерін баптауға мүмкіндік береді;

– қорғалған желі, ұйымдастырушы желіге қосылу параметрлерін баптайды;

– SQL сүзгілердің жалпы параметрлері үшін Microsoft SQL сүзгісі;

– біздің қорғалған желі үшін қосымша параметрлерді баптауды қамтамасыз ететін қосымша параметрлер;

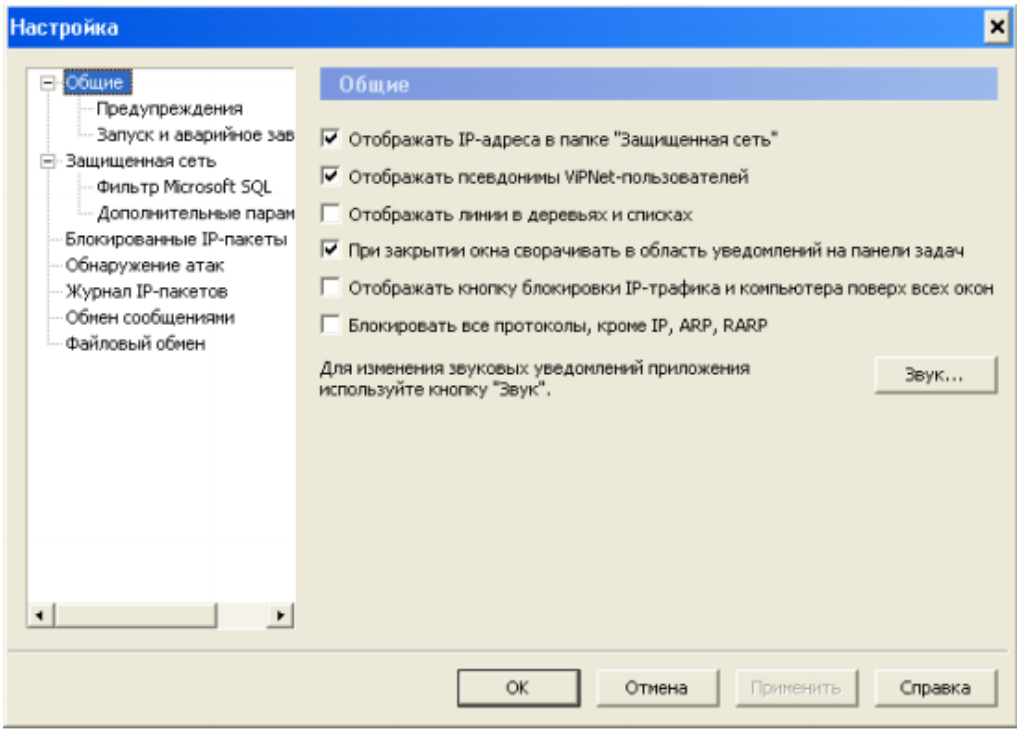
– блокталған IP-пакеттер IP-пакеттерді бұғаттау туралы пайдаланушыны хабардар етуді теңшеуге мүмкіндік береді;

– шабуылдарды анықтау әр түрлі басып кіруді анықтау жүйесін баптау үшін қолданылады;

– IP-пакеттер журналы IP-пакеттер туралы ақпарат журналда тіркелетін параметрлерді баптауды қамтамасыз етеді;

– хабар алмасу - хабар алмасу қызметінің параметрлері;

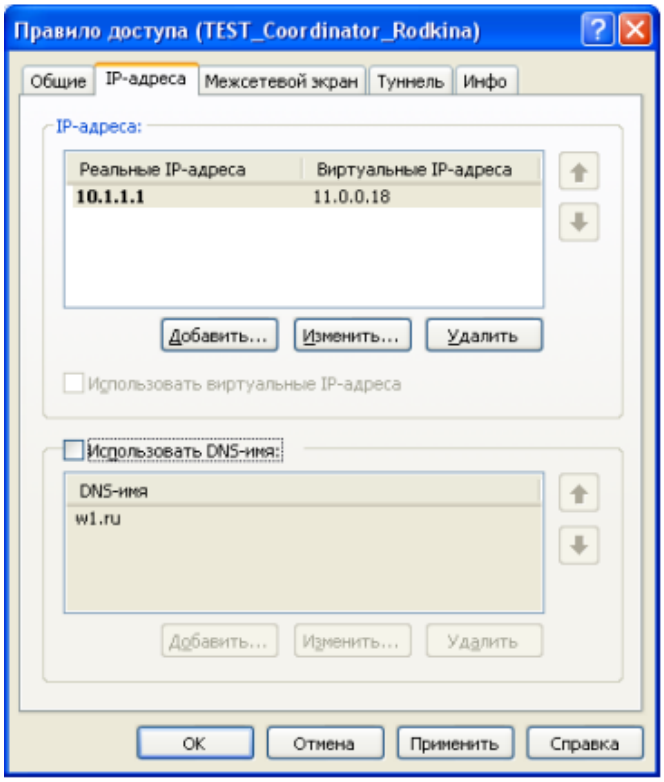
– файл алмасу құралы файл алмасу қызметін баптауды қамтамасыз етеді.



3.5 сурет – «Орнату» терезесі

3.1.3 IP адрестерінің серверін баптау. Басқа тораптарды желіге қосу әдістері мен белсенділігі туралы пайдаланушыға хабарлауды олардың өзара іс-қимылы үшін IP-адрестер сервері жүзеге асырады. IP-адрестер серверінде пайдаланушымен байланысты осы желідегі әрбір торап туралы ақпараттың толық көлемі бар. Сондықтан пайдаланушы өзінің IP - адрестерін (немесе DNS-атауын) біледі. Бұл мекенжай координатордың өзінің мекен-жайы немесе желіаралық экран/NAT - біздің желі шекарасында орнатылған құрылғы арқылы жүзеге асырылатын қатынау мекен-жайы.

IP-адресті немесе IP-адрестер серверінің DNS-атауын баптау үшін «қорғалған желі» терезесінде қажетті үйлестірушінің атына тінтуірдің сол жақ батырмасын екі рет басу қажет. Кейін «кіру ережесі» терезесі ашылады (3.6 сурет).



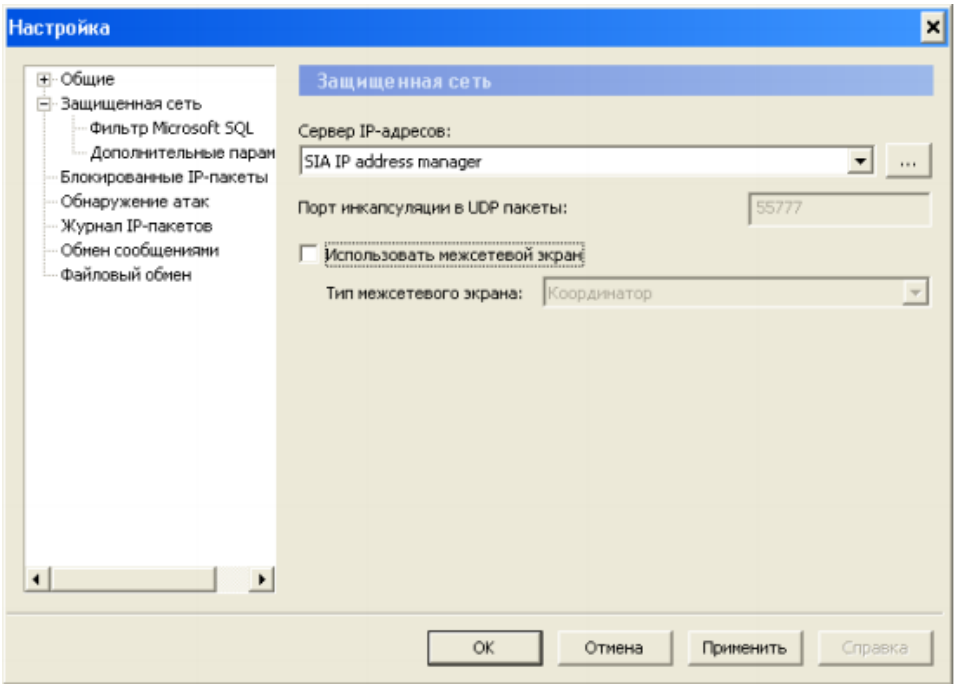
3.6 сурет – «Кіру ережесі» терезесі

IP-мекенжай бетінде «Қосу» батырмасын пайдаланғанда кез келген қол жетімді IP-мекенжайды (нақты) таңдаңыз немесе «DNS-атын пайдалану» флажогын орнатқанда «Қосу» батырмасын басамыз - қажетті координатордың DNS-атауын көрсете аламыз. Осы әрекеттер аяқталғаннан кейін "OK" басыңыз. Одан әрі «кіру ережесі» терезесінде «қолдану/OK» басыңыз.

Егер желіаралық экран/NAT-құрылғы арқылы IP-адрестердің серверіне қатынау мекенжайы мен порты бұрыннан белгілі болса, онда біз желі шекарасында орнатылған немесе IP-адрестердің тікелей серверінің IP-адрестерінің сырттан қол жетімді IP-адрестері, онда өз IP-адресін немесе DNS-атын теңшеу орнына «желіаралық экран» қойындысында қатынау және порттың IP-адрестерін баптауды жүргізуге болады, алдын ала «желіаралық экран арқылы торап жұмысының баптауларын пайдалану» құсбелгісін қою арқылы болады.

Одан әрі IP-адрестердің сервері ретінде координаторды таңдаймыз. Бұл үшін «Сервис/ Теңшеу» бас мәзірін пайдаланамыз. «Теңшеу» терезесінде «қорғалған желі» бөлімін таңдаймыз (3.7 сурет) және «IP-адрестердің сервері» тізімінде IP-адрестердің сервері болып табылатын координаторды

таңдаймыз. Бұл бұрын IP мекен-жайын реттеу жүргізілген координатор. "OK"батырмасын басу арқылы баптау процесін аяқтаймыз.



3.7 сурет – Теңшеу терезесі

3.1.3 Желіге қосылу параметрлерін баптау. ViPNet желісінің тораптары сыртқы желіге тікелей қосылған немесе желіаралық экрандар арқылы жұмыс істейді**.**

ViPNet желісінің тораптары IP протоколын қолдайтын кез келген түрдегі жергілікті желілердің ішінде орналасады. Ethernet желісіне қосылу тәсілі. ViPNet арқылы арналық деңгейдің әртүрлі хаттамаларын автоматты түрде қолдайды. IP - протоколдар арасында қорғалған VPN-туннелдерді құру үшін кез келген басқа IP хаттамаларын буып-түйетін екі типті IP-протоколдарды (IP/241 және IP/UDP) қолданамыз.

Барлық желілік тораптардың өзара әрекеттесуі кезінде, егер олардың арасында адресті түрлендірумен желіаралық экрандар болмаса, неғұрлым үнемді IP/241 хаттамасы қолданылады.

Бұл хаттама UDP протоколына қарағанда 8 байт көлеміндегі қосымша тақырыптары жоқ. Шифрлаудан кейін бастапқы пакет хаттаманың 241 нөмірі бар IP-пакетке оралады.

Барлық қалған жағдайларда UDP тасымалдау хаттамасы қолданылады. Шифрлаудан кейін бастапқы пакет белгіленген портпен UDP-пакеттерге оралады (әдепкі бойынша 55777 порты тағайындалады).

2.6 кесте - желілік тораптардың кез келген нүктелерінен басқа желілік тораптармен кепілді қосылу сапасын қамтамасыз ету үшін ViPNet клиент бағдарламасында сыртқы желіге қосылу тәсіліне байланысты қосудың төрт түрінің бірі таңдалады. Қосылу түрін таңдау үшін «Сервис/теңшеу» негізгі

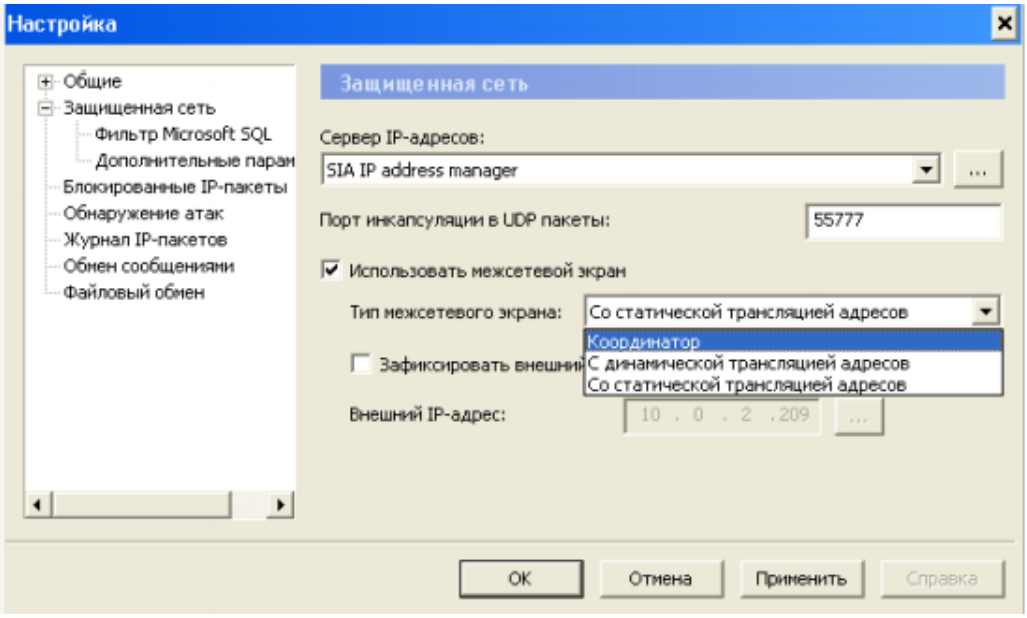
мәзірін қолданамыз. «Теңшеу» терезесінде «қорғалған желі» бөлімін таңдаймыз (3.8 сурет) және келесі параметрлердің бірін шығарамыз:

а) сыртқы желіге тікелей қосылу (МЭ пайдаланбай) – бұл жағдайда «желіаралық экранды пайдалану» деген флажокты алып тастау қажет;

Б) ViPNet арқылы қосылу - бұл жағдайда «желіаралық экранды пайдалану» флажогын орнатамыз және «желіаралық экранның түрі» тізімінде «Координатор» мәнін таңдаймыз;

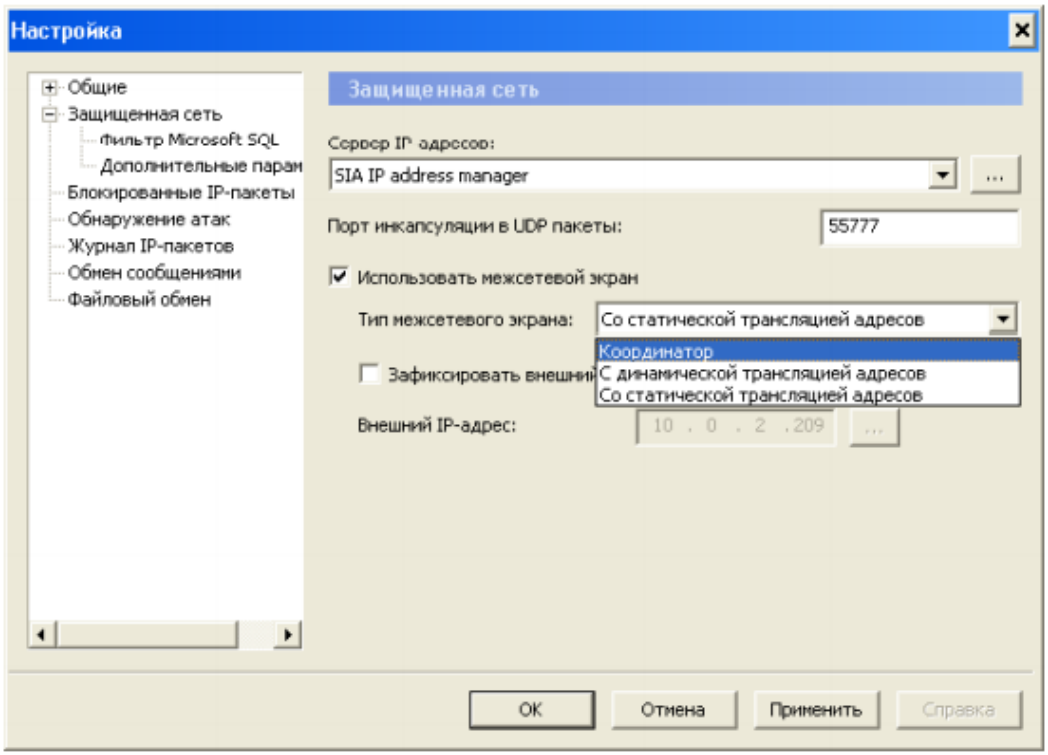
в) МЭ арқылы (NAT-құрылғы) қосылу, онда адрестерді трансляциялаудың статикалық ережелерін теңшеуге болады – бұл жағдайда «желіаралық экранды пайдалану» жалаушасы орнатылады, ал «желіаралық экранның түрі» тізімінде «адрестерді статикалық трансляциямен» мәнін таңдаймыз;

г) МЭ арқылы қосылу (NAT-құрылғы), адрестерді таратудың статикалық ережелерін теңшеу кезінде қиын немесе мүмкін емес – бұл жағдайда «желіаралық экранды пайдалану» жалаушасын орнатамыз, ал «желіаралық экранның түрі» тізімінде «адрестерді динамикалық трансляциямен» мәнін таңдаймыз.



3.8 сурет – «Қорғалған желі» терезесі

Егер желі конфигурациясы туралы ең аз мәлімет болса, сыртқы желімен жұмыс істеуді қамтамасыз ету үшін байланыс түрінің жылдам баптауын жүргізу қажет. Қосылу түрін таңдау үшін "Сервис/теңшеу"негізгі мәзірін қолданамыз. «Теңшеу» терезесінде «Қорғалған желі» тарауын таңдаймыз, «Пайдалану желіаралық экран пайдалану» жалаушасын орнатамыз.



3.9 сурет – «Қорғалған желі» терезесі

Келесі баптауларды жүргіземіз:

а) Егер ViPNet-координатор пайдаланушы сияқты сол жергілікті желіде орнатылса, онда жұмысты ViPNet-координатор арқылы теңшеу қажет, яғни «желіаралық экранның түрі» тізімінде «Координаторды» таңдау керек;

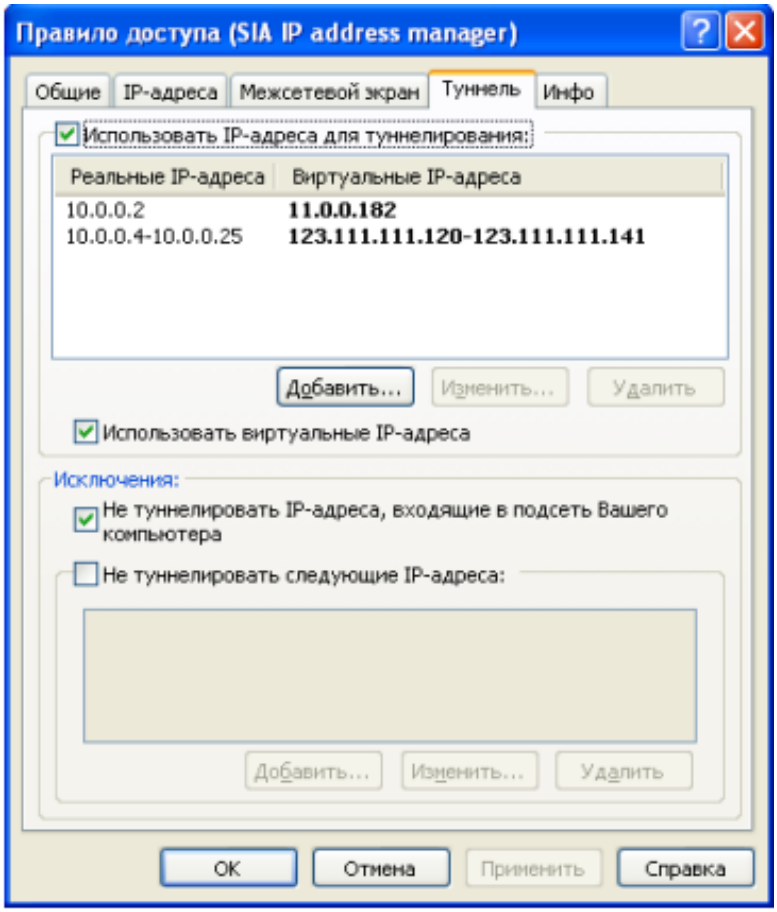
б) Егер пайдаланушы орнатылған жергілікті желіде ViPNet-координатор болмаса және жергілікті желі шекарасында орнатылған желіаралық экран туралы ақпарат болмаса, онда «желіаралық экран түрі» тізімінде «адрестерді динамикалық трансляциялаумен» тармағын таңдау қажет;

в) Егер пайдаланушы ViPNet-координаторы жоқ жергілікті желіде, бірақ жергілікті желі шекарасында орнатылған желілік экранда пайдаланушы үшін IP-адресті трансляциялау ережелері бапталса, онда «желіаралық экранның түрі» тізімінде «адрестердің статикалық трансляциясы» бар тармағын таңдау қажет.

3.1.4 Туннелирленетін компьютерлерге қатынауды теңшеу. Туннелирленетін құрылғыларға қатынауды қамтамасыз ету үшін туннелирленетін құрылғылардың IP-адрестері туралы барлық қажетті ақпарат берілмеген, онда тиісті координаторлармен туннеллирленетін IP-адрестерді көрсету қажет.

Баптау үшін «қорғалған желі» терезесінде біздің үйлестірушіміз атына тінтуірдің сол жақ батырмасын екі рет басу қажет. «Кіру ережесі» терезесі ашылады. Қорғалмаған компьютерлердің IP-пакеттерін туннелдеуге рұқсат етілген координатордың кіру ережесінде «Туннель» қойындысын таңдау

(3.10 сурет).



3.10 сурет – «Кіру ережесі» терезесі

«Туннель» бетінің сипаттамасына сәйкес келесі баптауларды жүргізу:

а) туннелдеу үшін жаңа диапазондарды немесе IP-адрестердің жеке мәндерін тапсыру үшін «туннелдеу үшін IP-адрестерді пайдалану» (тізімде берілген IP-адрестері бар пакеттерді шифрлау жүргізілмейді) жалаушасын орнату, одан әрі жаңа IP-адрестерді қосу немесе қолданыстағы баптауларды өзгерту;

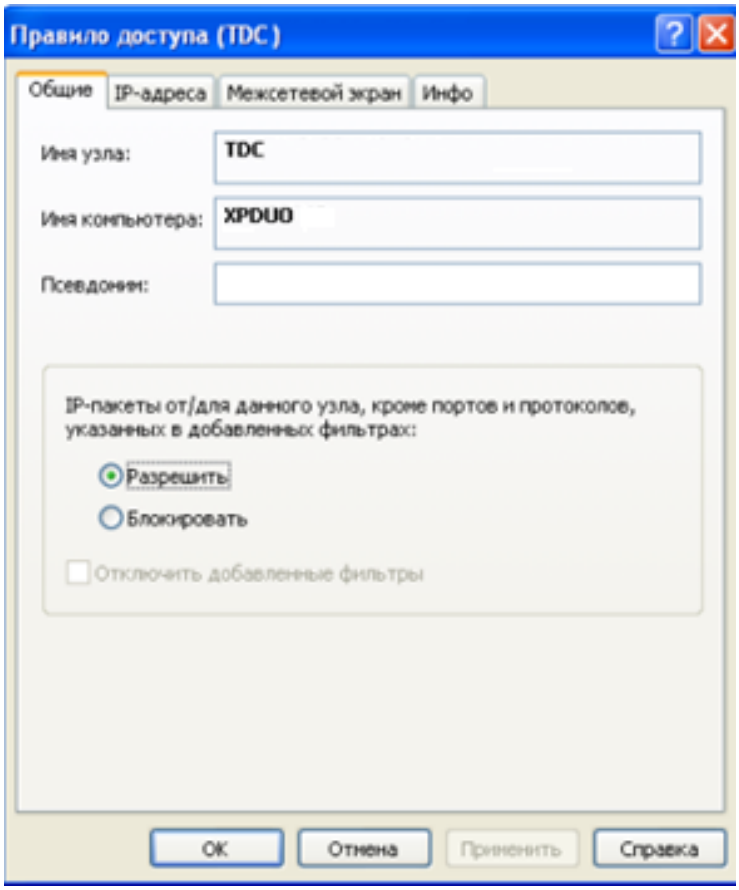
б) егер кейбір туннелирленетін IP-адрестердің координаторы пайдаланушының ішкі желісіне тиесілі болса, онда сіздің компьютеріңізге кіретін «IP-адрестерді туннелдеуге болмайды» жалаушасын қою ұсынылады;

в) егер координатормен туннелдейтін құрылғылардың кейбірі өзінің маршруттық кестесіне сәйкес өзінің координаторынан өтіп, яғни шифрленбеген түрде сіздің желілік торапқа IP-пакеттерді тікелей жіберсе, онда мұндай құрылғыларға қол жеткізу үшін келесі IP-адрестерді туннелдеуге жалауша қойылады: олардың мекен-жайларын төменде көрсетілген. Бұл жағдайда осы мекенжайлар бойынша пакеттер шифрланбайды. Ескерту: шифрлеу ажыратылған туннелдеуші құрылғылардың мекенжайына трафик туннелдеуші ViPNet-координатор арқылы өтпейтініне тағы бір рет көз жеткіземіз. Әйтпесе, трафик ViPNet-координатормен блокталады.

Барлық параметрлер аяқталғаннан кейін «кіру ережесі» терезесінде «OK» басыамыз.

Қажет болған жағдайда, туннельдеуші құрылғылар үшін DNS-аттар беріледі. DNS-аттар IP-мекенжай қойындысындағы туннелдеуші координатор үшін «кіру ережесі» терезесінде қойылады.

3.1.5 Қорғалған желі тораптарына қол жеткізу ережелері. Бұл терезеде «қорғалған желі» терезесінен желілік тораптармен жұмыс параметрлерін теңшейміз» (3.11 сурет).



3.11 сурет – «Кіру ережесі» терезесі

«Кіру ережесі» терезесі ашылады (3.11 сурет), тышқанның сол жақ батырмасымен қандай да бір пайдаланушының аты бар жолды екі рет басу кезінде немесе контекстік мәзірде «кіру/ашу ережесін» таңдау қажет.

(3.11 сурет) «кіру ережесі» терезесі теңшелетін торапқа байланысты беттер жиынтығын қамтиды: жалпы, IP-мекенжай, желіаралық экран, Инфо және Туннель. Беттер төменде сипатталатын болады. Параметрлерді сақтау үшін қолдану түймешігін (параметрлер терезесін жабусыз) немесе OK (параметрлер терезесін жабумен), болдырмау үшін – Жою түймешігін пайдаланыңыз.

3.2 VipNet SafeDisk бағдарламасын пайдалана отырып, клиенттің жеке компьютерінде құпия ақпаратты қауіпсіз сақтауды ұйымдастыру

ViPNet SafeDisk жұмыс істеу принциптері:

– дискідегі немесе сыртқы тасымалдағыштағы шифрланған файл түрінде контейнерді жасау және оны құпия сөз, файл-кілт немесе электрондық кілт түрінде қорғау әдісін орнату;

– жүйе контейнерін қалыпты ретінде қосқан кезде дискті көрсету үшін, ол құпия ақпаратты сақтауға болады;

– ақпаратты сақтау кезінде мөлдір шифрлеу, оқу кезінде - шифрлеу. Бұл процесс көп уақытты алмайды. Құжаттармен жұмыс әдеттегі режимде жүргізіледі, бірақ ақпарат сенімді қорғалған;

– ажыратылған кезде контейнер біздің жүйеде көрсетілмейді және құпия ақпараттың болуы және оған қол жеткізу мүмкін емес фактісінің өзі белгіленеді;

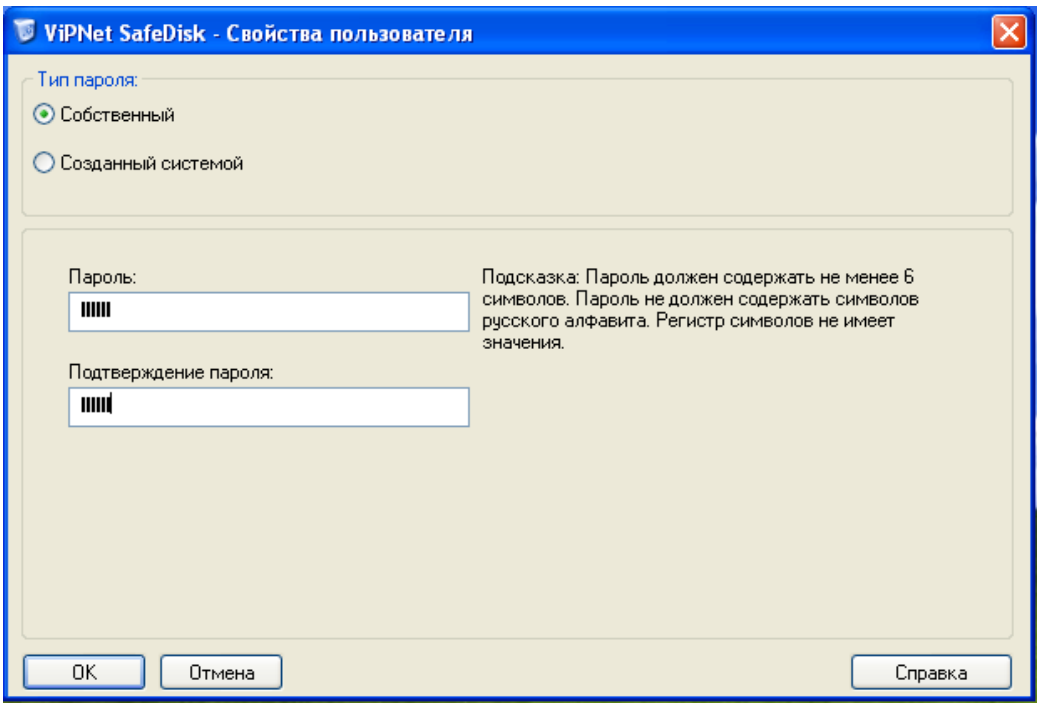
– контейнерде бұрын сақталған құпия ақпаратқа кіруді қалпына келтіру және онымен жұмысты жалғастыру үшін контейнерді қосу қажет. Бұл әрекет үшін бұрын таңдалған қорғау тәсіліне байланысты пароль, кілт-файл немесе электрондық кілт туралы ақпарат қажет.

3.2.1 Жаңа пайдаланушының құпия сөзін жасау үшін:

а) ViPNetSafeDisk іске қосу бағдарламасын жұмыс үстелінде немесе Бастау мәзірінде белгішені пайдалана отырып іске қосамыз;

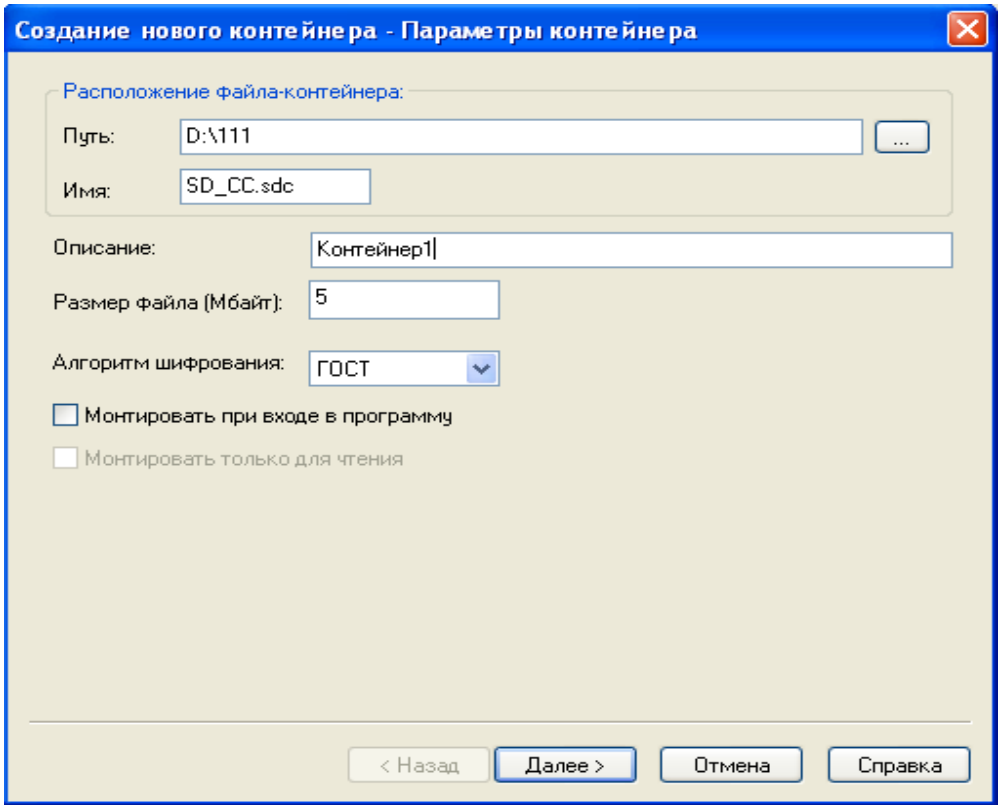
б) ViPNet SafeDisk бірінші іске қосылғанда пайдаланушының пароль терезесі ашылады. Жаңа пайдаланушының паролін келтіреміз (3.12 сурет);

в) әдепкі бойынша «жеке құпия сөз түрін» орнату ұсынылады. Құпия сөзді қойып, оны растау үшін тиісті жолақтарға енгіземіз. Келесі ViPNet SafeDisk іске қосылғанда бағдарламаға кіру үшін берілген пароль қолданылады.



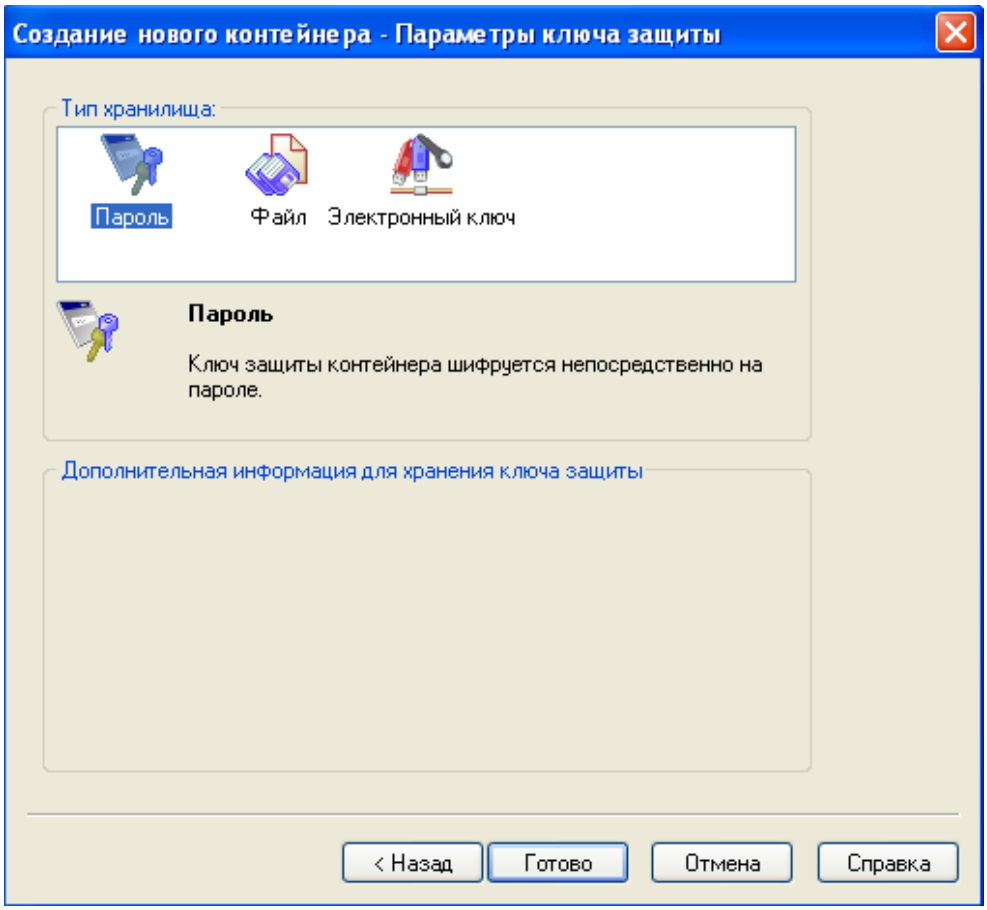
3.12 сурет – Жаңа пайдаланушының құпия сөзін жасау

3.2.2 Жаңа контейнерді құру және қосу. Жаңа пайдаланушының паролін жасағаннан кейін ViPNetSafeDisk бас терезесі ашылады; жасау батырмасын басамыз, контейнерді жасау шебері іске қосылады (3.13 сурет).



3.13 Сурет – Жаңа контейнер жасау

Контейнерді жасау шеберінің бірінші бетінде контейнер файлының аты мен орналасуын, оның сипаттамасын, өлшемі мен шифрлау алгоритмін белгілейміз. «Келесі» батырмасын басамыз. Терезеде қойманың түрі контейнерге кіру тәсілін таңдаймыз (3.14-сурет).



3.14 Сурет – Қауіпсіздік кілтінің параметрлері

Пароль. Контейнер бағдарламаға кіру үшін пайдаланылатын парольмен ғана қорғалады.

Файл-кілт. Контейнерге кіру үшін құпия сөз және кілт файл қажет. Осы қатынас әдісін таңдағанда, кілт файлының орны мен атауын орнатамыз.

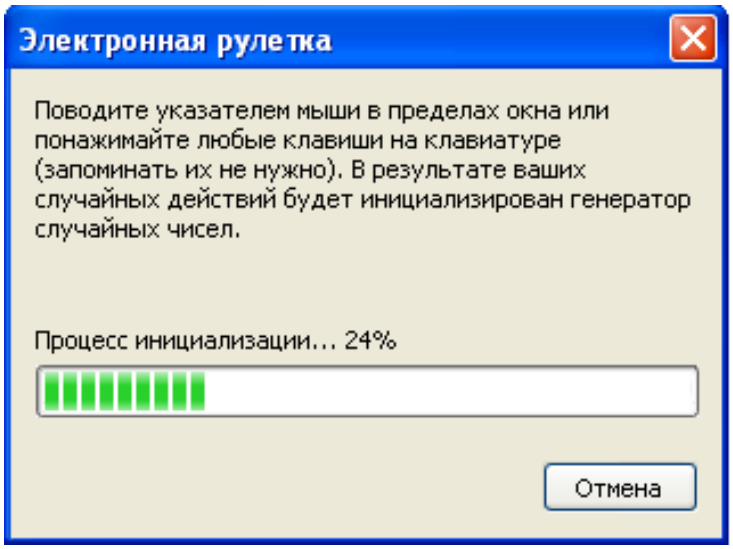
Үлкен қауіпсіздік үшін кілт-файлын сыртқы тасымалдағышта орналастыруға болады.

Электрондық кілт. Контейнерге кіру үшін пароль мен электрондық кілт қажет. Осы қатынас әдісін таңдағанда, электрондық кілтті оқу құралына саламыз.

«Құпия сөз» контейнеріне кіру тәсілін таңдаймыз – «дайын», содан кейін автоматты түрде электрондық рулетка терезесі пайда болады (3.15 сурет).

Контейнерді жасау үшін кездейсоқ сандар қажет. Кездейсоқ сандардың сенсоры кездейсоқ санды алу қажет болған кезде автоматты түрде шақырылатын электрондық рулеткамен іске қосылады.

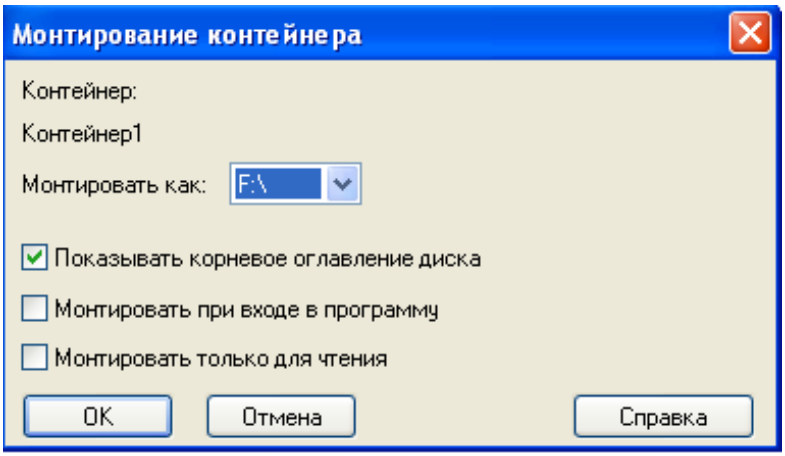
Бастау процесі аяқталғанға дейін электрондық рулетка пайда болған кезде әрекеттерді орындаймыз: тінтуір көрсеткішін терезе ішінде жылжытамыз немесе пернетақта пернелерін басамыз.



3.15 сурет – Электронды рулетка

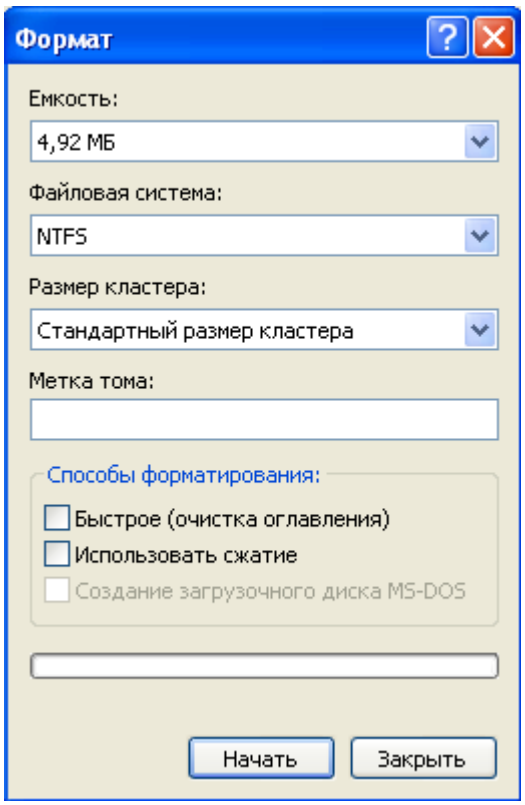
Контейнерді қосу. Контейнерге қорғау қажет деректерді сақтау үшін контейнерді қосамыз. Ол үшін тіркеу түймешігін басамыз. Контейнерді қосу терезесі ашылады.

Қосылу параметрлерді пайдаланып, ұсынылған әдепкі бойынша таңдаймыз (3.16-сурет).



3.16 сурет – Контейнерді қосу

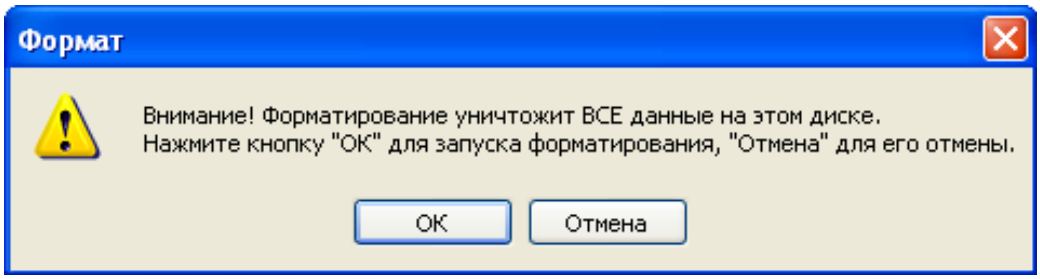
Бірінші рет қосылған контейнерді форматтау қажет. Әдепкі параметрлерді пайдаланамыз (3.17 сурет).



3.17 сурет – Контейнерді форматтау

Форматтауды бастау үшін «Бастауды» басамыз.

Диск форматталған және осы дискіде сақталған барлық ақпарат жоғалатыны туралы ескерту хабары пайда болады. Бұл жағдайда ешқандай ақпарат жоқ қосылған контейнерді форматтайды, сондықтан форматтау процесін бастау үшін OK түймесін басамыз.



3.18 сурет – Контейнерді форматтауды бастау

Форматтау процесі басталады. Форматтаудың аяқталғаны туралы хабары бар терезеде OK басыңыз.

3.2.2 Қорғалған ақпаратпен жұмыс. Қосылған контейнер әдеттегі Windows дискі ретінде көрсетіледі. Енді, мысалы, файлдарды осы дискіге жылжыта аламыз немесе мәтіндік редакторда жұмыс істей отырып, онда құжаттарды сақтай аламыз.

Қорғалған ақпаратпен жұмыс аяқталған кезде, оған кіруді жабу қажет. Ол үшін контейнерде сақталатын барлық файлдармен жұмысты аяқтаймыз

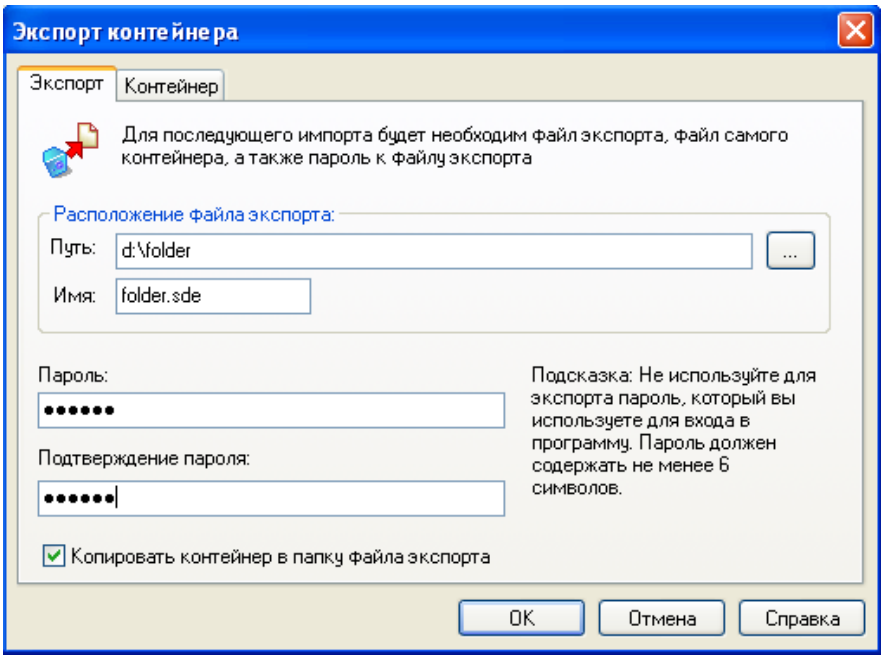
және контейнер файлдарын көрсететін өткізгіш терезесін жабамыз. Басты терезеде жою түймешігін басамыз. Контейнерді өшіргенде, қорғалған ақпаратқа кіру жабық болады және компьютеріңізде осындай ақпараттың болу фактісін жасырады.

Жұмыс сеансын аяқтау үшін SafeDisk мәзіріндегі шығыс тармағын қолданамыз.

3.2.3 Қорғалған ақпаратты резервтік көшіру. ViPNetSafeDisk қажет болған жағдайда ақпаратты қалпына келтіру мүмкіндігін қамтамасыз ету үшін қорғалған ақпараттың резервтік көшірмелерін жасауға мүмкіндік береді. Қорғалған деректердің сақтық көшірмесін жасау үшін контейнерді экспорттау процедурасы қолданылады. Экспорт процедурасының нәтижесінде контейнер экспортының файлы жасалады. Контейнер экспортының файлы қорғалған ақпараттың резервтік көшірмесі болып табылады және контейнер файлын және контейнер кілттерінің резервтік көшірмесін қамтиды**.**

Контейнерді экспорттау процедурасын жүргізу және қорғалған ақпараттың сақтық көшірмесін жасау үшін мыналарды орындаймыз:

а) ViPNetSafeDisk басты терезесінде сақтық көшірмесін жасау қажет деректер контейнерін таңдаймыз. Егер контейнер қосылған болса, оны өшіру керек;

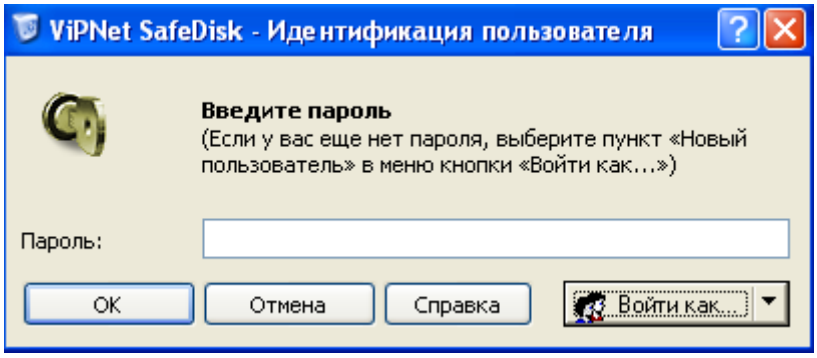


3.19 сурет – Компьютерді экспорттау

б) Контейнер мәзіріндегі Экспорт тармағын таңдаңыз. Контейнер экспорт шебері терезесі ашылады;

в) қалтаны таңдап, контейнерді экспорттау файлының атауын енгіземіз. Қауіпсіздік мақсатында экспорт файлын қорғалған ақпараттан бөлек сақтау ұсынылады, мысалы, сыртқы тасымалдағышта (3.19-сурет).

3.2.4 Жаңа пайдаланушыны тіркеу. ViPNet SafeDisk бір-біріне қарамастан, әрбір пайдаланушыға қорғалған деректермен жұмыс істеуге мүмкіндік беретін бірнеше бағдарлама. Егер бағдарлама іске қосылған болса, ағымдағы пайдаланушының жұмыс сеансын аяқтаймыз. Ол үшін SafeDisk мәзірінен шығу тармағын таңдаймыз. Бағдарламаны іске қосамыз. < Кіру > жаңа пайдаланушы таңдаймыз.



3.20 сурет – Жаңа пайдаланушыны құру

SafeDisk пайдаланушының паролі терезесі ашылады. SafeDisk пайдаланушысының құпия сөзі терезесінде әдепкі бойынша жеке құпия сөз түрі таңдалған. Жаңа пайдаланушының паролін орнатамыз, паролін растауды енгіземіз және OK басамыз.

ViPNetSafeDisk келесі іске қосылғанда тіркелген пайдаланушының жұмысын бастау үшін құпия сөзді енгізу терезесінде құрылған құпия сөзді енгізу қажет.

Қауіпсіздікті арттыру мақсатында өз құпия сөзіңізді өзгерту ұсынылады.

Қауіпсіздік мәзіріндегі құпия сөзді өзгерту тармағын таңдаймыз. Пайдаланушының құпия сөзін жасау терезесі пайда болады.

SafeDisk пайдаланушысының құпия сөзі терезесінде әдепкі бойынша жеке құпия сөз түрі таңдалған. Жаңа пайдаланушының құпия сөзін орнатамыз, құпия сөзді растауды енгізіп, OK түймесін басамыз.

ViPNetSafeDisk келесі іске қосылғанда, жұмыс сеансын бастау үшін жаңадан құрылған құпия сөзді пайдаланамыз.

Егер ViPNetSafeDisk пайдаланғанда құпия сөзді ауыстырғанға дейін одан әрі қажет болатын конфигурацияның сақтық көшірмелері жасалса, алдыңғы құпия сөзді есте сақтаймыз.

3.3 Вирусқа қарсы қорғау

Жұмыс станцияларына 5.0 нұсқасының Windows Workstation үшін Касперский антивирусы орнатылады.

Windows Workstations үшін Касперский антивирусы - бұл жұмыс станцияларын орталықтандырылған басқару мүмкіндігі бар зиянды бағдарламалар мен желілік шабуылдардан қорғау үшін қабылданған шешім.

Бұл антивирустың артықшылықтары**:**

– қорғау тұтастығы. Бағдарлама файлдық операцияларды, электрондық пошта мен интернет-трафикті бақылау арқылы жұмыс станциясын зиянды бағдарламалардан қорғайды, сондай-ақ желілік шабуылдардан базалық қорғауды жүзеге асырады;

– орталықтандырылған басқару. Қосымшаны өрістету, оның жұмыс параметрлерін теңшеу, вирусқа қарсы базаларды жаңарту және сыни жағдайларда жедел әрекет ету – барлық осы міндеттерді Kaspersky adminion kit пайдалана отырып, орталықтандырып шешуге болады;

– әлеуетті қауіпті БҚ қорғау. Шешім зиянды ғана емес, әлеуетті қауіпті бағдарламалық қамтамасыз ету (spyware, adware және басқа).

Серверге Windows File Servers 5.0 нұсқасы үшін Касперский антивирусы қойылады.

Windows File Servers үшін Касперский антивирусы Windows NT операциялық жүйелерінің басқаруында жұмыс істейтін деректер серверлерінің антивирустық қауіпсіздігін қамтамасыз етуге арналған 4.0/2000/2003 ескерту. Серверлерді сенімді қорғау - корпоративтік желіні вирустардан толық ауқымды қорғаудың маңызды элементі.

Windows File Servers үшін Касперский Антивирусында нақты уақыт режимінде іске қосылатын, ашылатын, түрлендірілген файлдарды зиянды бағдарламалардың болуын тексеруге, сондай-ақ әкімшінің талабы бойынша да, сондай-ақ берілген кестеге сәйкес автоматты түрде де деректерді сақтау орындарын тексеруді жүзеге асыруға мүмкіндік беретін екі деңгейлі деректерді қорғау жүйесі қолданылды.

Осы әдістерді бірлесіп қолдану вирустардың барлық әлеуетті ену көздерін сенімді бақылауды қамтамасыз етуге және сіздің желіңізді барынша қорғауға мүмкіндік береді.

Архивтерді сканерлеу бірегей технологиясының арқасында Касперский антивирусы 1200 форматтан астам архивтелген және оралған файлдарда вирустарды анықтайды және ZIP, ARJ, CAB, RAR форматтары мұрағаттарында файлдарды емдейді. Скрипт - вирустардың енуінен қорғау қамтамасыз етіледі: Script Checker™ скрипт - вирустардың әмбебап ұстаушысы скрипт-бағдарлама мен оны өңдеуші арасында сүзгі ретінде жүйеге интеграцияланады.

Касперский антивирусы карантиндік директорияның жүйелік әкімшісімен құрылған күдікті объектілерді оқшаулауға мүмкіндік береді. Ықтимал қауіпті объектілер одан әрі зерттеу үшін осы директорияға

орналастырылатын болады - мысалы, «Касперский Зертханасының» сарапшыларына талдауға жіберу үшін.

IChecker және iStreams технологияларын бірлесіп пайдалану Касперский Антивирус өнімділігін 3 есе арттыруға мүмкіндік берді, сонымен қатар жедел жад көлемінің алдыңғы нұсқамен салыстырғанда 2 есе төмендеуімен.

Серверде зарарланған файлдар пайда болған кезде желі әкімшісі уақтылы хабарландыру алады. Хабарламада мынадай ақпарат бар: жұқтырылған объектіге жол, вирустың атауы және оны бейтараптандыру бойынша қабылданған әрекеттер.

Windows File Servers үшін Касперский антивирусы Kaspersky Administration Kit басқару жүйесімен біріктірілген. Бұл модульді кез келген компьютерден корпоративтік желі немесе қашықтағы әкімшінің жұмыс орнынан орнатуға мүмкіндік береді. Жүйе әкімшісі оның баптаулары мен конфигурациясын орталықтандырып өзгертуге, баптауларға қолжетімділікті шектеуге немесе табыстауға, бағдарламалық компоненттерді жаңартуға, антивирустық бағдарламамен тіркелген желідегі барлық оқиғалар туралы толық есептер алуға мүмкіндігі бар.

3.4 PacketTracer ортасында виртуалды желіні моделдеу

Packettracer ортасын пайдалану арқылы Виртуалды жеке желіні модельдеу жүргіземіз. Желі сұлбасы 3.21 суретте көрсетілген.

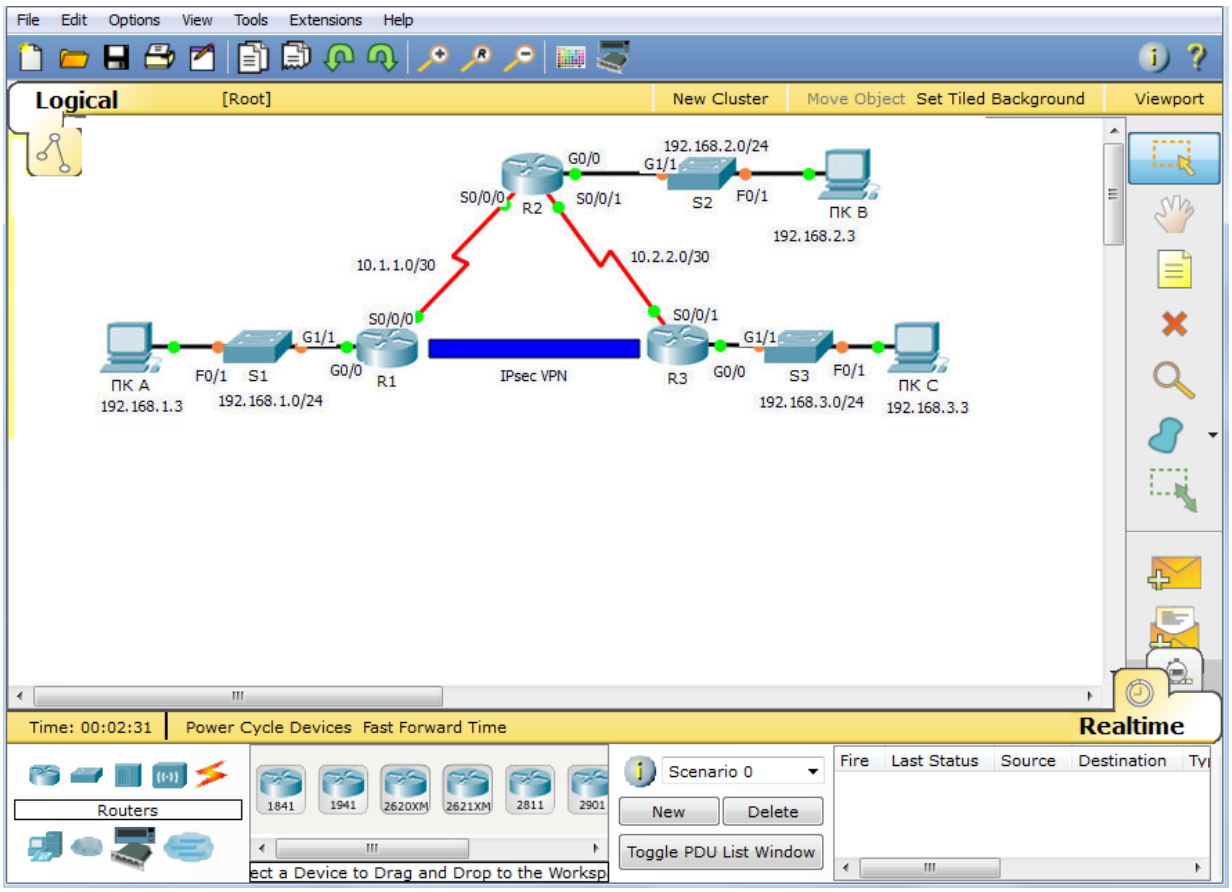
3.1 кесте – Желідегі Адресация

Құрылғы	Интерфейс	IP-адрес	Ішкі желі маскасы	Әдепкі Шлюз
R1	G0/0	192.168.1.1	255.255.255.0	Қол жетімсіз
	S0/0/0	10.1.1.2	255.255.255.252	Қол жетімсіз
R2	G0/0	192.168.2.1	255.255.255.0	Қол жетімсіз
	S0/0/0	10.1.1.1	255.255.255.252	Қол жетімсіз
	S0/0/1	10.2.2.1	255.255.255.252	Қол жетімсіз
R3	G0/0	192.168.3.1	255.255.255.0	Қол жетімсіз
	S0/0/1	10.2.2.2	255.255.255.252	Қол жетімсіз
ДК А	NIC	192.168.1.3	255.255.255.0	192.168.1.1
ДК В	NIC	192.168.2.3	255.255.255.0	192.168.2.1
ДК С	NIC	192.168.3.3	255.255.255.0	192.168.3.1

Қауіпсіздік мүмкіндіктерін қосу үшін securityk9 модулін іске қосу қажет.

Ол үшін R1 және R3 маршрутизаторларында (Security) қауіпсіздікті қамтамасыз ету технологиялары пакетінің лицензиясын қосамыз.

Құпия сөз ретінде Cisco құпия сөзі қолданылады.



3.21 сурет – Зерттелетін желі схемасы

Келесі маршрутизаторды жүктеу үшін security9 модулін іске қосамыз, лицензияны қабылдаймыз, орнатамыз және маршрутизаторды қайта жүктейміз.

R1(config)# license boot module c2900 technology-package security9
R1(config)# end
R1# copy running-config startup-config
R1# reload

Қайта жүктеуден кейін қауіпсіздік технологиясы пакетінің лицензиясы іске қосылғандығын тексеру үшін қайтадан көрсету командасын шығарамыз.

```
Technology Package License Information for Module:'c2900'
-----------------------------------------------------------------
Technology Technology-package Technology-package
Current Type Next reboot
-----------------------------------------------------------------
-
ipbase ipbasek9 Permanent ipbasek9
security security9 Evaluation security9
uc None NoneNone
data None NoneNone
```

R3 маршрутизаторы үшін активациялауды қайталаймыз.
R1 маршрутизаторында IPsec параметрлерін теңшеңіз:
ДК А-дан ДК С-ге эхо сұрау жіберу арқылы байланысты тексереміз.

R1 маршрутизаторындағы қызықты трафикті анықтаймыз.

Ол үшін R1 маршрутизаторындағы жергілікті желі трафигін R3 маршрутизаторындағы жергілікті желіге қызығушылық танытатыны ретінде анықтау үшін ACL-тізімді баптаймыз. Осы қызықты трафик R1 және R3 маршрутизаторларының жергілікті желілері арасында трафик болған кезде VPN IPsec іске қосылады. Осы жергілікті желілерден берілетін барлық қалған трафик шифрланбайды. «Deny any» тыйым салу әрекеті туралы және осы ережені тізімге қосу қажет емес екенін есте сақтаңыз.

```
R1(config)# access-list 110 permit ip 192.168.1.0 0.0.0.255 192.168.3.0 0.0.0.255
```

R1 маршрутизаторында isakmp 10 криптографиялық саясатының сипаттарын, сондай-ақ cisco шифрлаудың жалпы кілтін баптаймыз. Теңшеуге жататын нақты параметрлер ISAKMP 1 фазасының параметрлер кестесінде келтірілген. Әдепкі мәндерді теңшеу қажет емес, сондықтан тек шифрлауды, кілттерді алмасу әдісін және DH әдісін теңшеу қажет.

```
R1(config)# crypto isakmp policy 10
R1(config-isakmp)# encryption aes
R1(config-isakmp)# authentication pre-share
R1(config-isakmp)# group 2
R1(config-isakmp)# exit
R1(config)# crypto isakmp key cisco address 10.2.2.2
```

2 фазаның барлық параметрлерін бірге байланыстыратын VPN-MAP криптографиялық салыстыруды (crypto map) жасаймыз. 10 реттік нөмірін қолданыңыз және оны ipsec-isakmp салыстыру ретінде анықтаңыз.

```
R1(config)# crypto ipsec transform-set VPN-SET esp-3des esp-sha-hmac
R1(config)# crypto map VPN-MAP 10 ipsec-isakmp
R1(config-crypto-map)# description VPN connection to R3
R1(config-crypto-map)# set peer 10.2.2.2
R1(config-crypto-map)# set transform-set VPN-SET
R1(config-crypto-map)# match address 110
R1(config-crypto-map)# exit
```

Шығыс интерфейсі үшін криптографиялық салыстыруды баптаймыз.

```
R1(config)# interface S0/0/0
R1(config-if)# crypto map VPN-MAP
```

R3 маршрутизаторында IPsec параметрлерін орнату

1-қадам: R1 маршрутизаторы бар алаң арасында VPN желісін қолдау үшін R3 маршрутизаторын реттейміз.

Енді R3 маршрутизаторының екі бағытына да тасымалдау параметрлерін реттейміз. ACL-тізім 110 жергілікті R3 маршрутизаторы желісінен жергілікті R1 маршрутизаторы желісіне дейін трафикті қызықтыратыны ретінде анықтау үшін теңшейміз.

R3(config)# access-list 110 permit ip 192.168.3.0 0.0.0.255 192.168.1.0 0.0.0.255

R3 маршрутизаторында ISAKMP 1 фазасы параметрін орнату.

R3 маршрутизаторында ISAKMP 10 криптографиялық саясатының сипаттарын, сондай-ақ cisco шифрлау кілтін баптаймыз.

```
R3(config)# crypto isakmp policy 10
R3(config-isakmp)# encryption aes
R3(config-isakmp)# authentication pre-share
R3(config-isakmp)# group 2
R3(config-isakmp)# exit
R3(config)# crypto isakmp key cisco address 10.1.1.2
```

R1 маршрутизаторында ISAKMP 2 фазасын теңшейміз.

R1 маршрутизаторына ұқсас, esp-3des және esp-sha-hmac үшін VPN-SET түрлендіру жиынтығын құрайық. Содан кейін криптографиялық салыстыруды (crypto map) VPN-MAP жасайды, ол 2 фазаның барлық параметрлерін байланыстырады. 10 реттік нөмірін қолданамыз және оны ipsec-isakmp салыстыру ретінде анықтаймыз.

```
R3(config)# crypto ipsec transform-set VPN-SET esp-3des esp-sha-hmac
R3(config)# crypto map VPN-MAP 10 ipsec-isakmp
R3(config-crypto-map)# description VPN connection to R1
R3(config-crypto-map)# set peer 10.1.1.2
R3(config-crypto-map)# set transform-set VPN-SET
R3(config-crypto-map)# match address 110
R3(config-crypto-map)# exit
```

Шығыс интерфейсі үшін криптографиялық салыстыруды теңшеу.

Ол үшін VPN-MAP криптографиялық салыстыруды Serial0/0/1 Шығыс интерфейсіне байланыстырамыз.

```
R3(config)# interface S0/0/1
R3(config-if)# crypto map VPN-MAP
```

Ол үшін қажетті трафик өтпей тұрып, туннельді тексереміз.

R1 маршрутизаторында show crypto ipsec sa командасын енгіземіз. Барлық пакеттердің (инкапсуляцияланған, шифрланған, декапсуляцияланған және дешифрланған) саны 0 тең екеніне назар аударамыз.

R1# show crypto ipsecsa

```
interface: Serial0/0/0
Crypto map tag: VPN-MAP, local addr 10.1.1.2
protected vrf: (none)
local ident (addr/mask/prot/port):
(192.168.1.0/255.255.255.0/0/0)
remote ident (addr/mask/prot/port):
(192.168.3.0/255.255.255.0/0/0)
current_peer 10.2.2.2 port 500
PERMIT, flags={origin_is_acl,}
#pktsencaps: 0, #pkts encrypt: 0, #pkts digest: 0
#pktsdecaps: 0, #pkts decrypt: 0, #pkts verify: 0
#pkts compressed: 0, #pkts decompressed: 0
#pkts not compressed: 0, #pktscompr. failed: 0
#pkts not decompressed: 0, #pkts decompress failed: 0
#send errors 0, #recv errors 0
local crypto endpt.: 10.1.1.2, remote crypto endpt.:10.2.2.2
path mtu 1500, ipmtu 1500, ipmtuidb Serial0/0/0
current outbound spi: 0x0(0)
     < Деректер алынды >
```

Қажетті трафик өткеннен кейін туннельді тексереміз.

R1 маршрутизаторында show crypto ipsec sa командасын қайта енгіземіз. Енді пакеттердің саны 0-ден артық болғанын ескереміз. Бұл IPsec бойынша VPN желісінің туннелі жұмыс істейді дегенді білдіреді.

R1# show crypto ipsecsa

```
interface: Serial0/0/0
Crypto map tag: VPN-MAP, local addr 10.1.1.2
protected vrf: (none)
local ident (addr/mask/prot/port):
(192.168.1.0/255.255.255.0/0/0)
remote ident (addr/mask/prot/port):
(192.168.3.0/255.255.255.0/0/0)
current_peer 10.2.2.2 port 500
PERMIT, flags={origin_is_acl,}
#pktsencaps: 3, #pkts encrypt: 3, #pkts digest: 0
#pktsdecaps: 3, #pkts decrypt: 3, #pkts verify: 0
#pkts compressed: 0, #pkts decompressed: 0
#pkts not compressed: 0, #pktscompr. failed: 0
#pkts not decompressed: 0, #pkts decompress failed: 0
#send errors 1, #recv errors 0
local crypto endpt.: 10.1.1.2, remote crypto endpt.:10.2.2.2
```

```
path mtu 1500, ipmtu 1500, ipmtuidb Serial0/0/0
current outbound spi: 0x0A496941(172583233)
     <Деректер алынды>
```

R1 маршрутизаторында showcryptoipsecsa командасын қайта енгіземіз. Соңында, пакеттердің саны өзгермегенін ескерсек бұл қызықты трафик шифрленбейді дегенді білдіреді.

4 Өмір тіршілігінің қауіпсіздігі

4.1 Еңбек жағдайларын талдау

Өндірістік тәуекелдерді талдау - бұл қалыпты еңбек жағдайларын анықтауға бағытталған шаралар кешені, сондай-ақ еңбек жағдайында адамның денсаулығы мен өміріне зиян келтіретін факторларды анықтауға бағытталған.

Бұл дипломдық жоба компанияның ақпараттық қауіпсіздігіне қатер төндіру мүмкіндігін азайтуды әзірлеуге арналады. Ақпараттың қауіпсіздігін қамтамасыз ету компьютерлік технологиялар мен электронды жабдықтардың көмегімен жүзеге асырылады. Қарастырылып отырған офис бір жұмысшы бар, оның жеке жұмыс орны бар.

Әзірлеушіге 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.

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.

4.1.1 Жұмыс орнының сипаттамасы

Кеңсені жобалау және құру кезінде ҚР ҚНжЕ 3.02-04-2009 [1] ережелеріне сүйене отырып жасалған.

Кеңсе бір жұмыс орнына жабдықталған. Кеңсе Макатаева көшесіндегі Жар-су бизнес-орталығының, 4 қабатында орналасқан. Кеңсенің тезерелері ғимараттың кері жағында орналасқандықтан әр түрлі шу көздері жұмыс барысына әсер ете алмайды.

Бағдарламалық қамтамасыз етуді әзірлеу жүргізілетін бөлмені қарастырайық (5.1-сурет). Бөлме өлшемдері: ұзындығы (L) = 6 метр, ені (B) = 3,5 метр, биіктігі (H) = 2,8 метр. Жұмыс орнының жалпы ауданы 14 ш. м. болғандықтан санитарлық талаптарды қанағаттандырады.

4.1 сурет - Жұмыс бөлмесінің жоспары

4.1.2 Электромагниттік сәулелену

ГОСТ 12.1.006-84 [2] «ЕҚСЖ радио жиіліктердің электромагниттік өрісі» сәйкес өндірістік қауіптіліктің негізгі факторларының бірі ЭСТ мониторының экранынан шыққан электромагниттік сәуле болып табылады.

Компьютерлік монитордан иондаушы емес электромагниттік сәулелену параметрлерінің рұқсат етілген мәндері 4.1 кестеде келтірілген.

4.1-кесте - Ионданбайтын электромагниттік сәуле параметрлерінің рұқсат етілген мәні (СанПиН 2.2.2.542-96 [3] сәйкес)

Параметр атауы	Рұқсат етілген мәндер
Бейнемонитор бетінен 50см қашықтықта электромагниттік өрістің электр құраушысының кернеулігі	10В/м
Бейнемонитор бетінен 50 см қашықтықта электромагниттік өрістің магниттік құраушысының кернеулігі	0,3А/м
Электростатикалық өрістің кернеулігі	20кВ/м

4.1.3 Өрт қауіпсіздігі

Өртке қарсы су қондырғыларына қойылатын талаптар ҚР ҚНжЕ 2.02-05-2009 [4] құрылыс проект нормасымен анықталады. Электр тораптарына, соның ішінде электронды компьютерлерге қосылатын әртүрлі мақсаттағы құрылғылармен жұмыс істеу кезінде қадағаланды. Дұрыс жасалған құжат электрлік құрылғылармен жұмыс бөлмесінде сипаты дұрыс емес жағдайлардан туындайтын қауіпті жағдайларды болдырмауға көмектеседі.

Монитордан және жүйелік блоктан шығатын кабельдер, сондай-ақ CRT мониторларындағы жарық түтігі жұмыс істеп тұрған электр кернеумен жұмыс
істейді. Осы құрылғыларды абайлап, дәлме-дәл пайдалану шкафта өрттің пайда болуына немесе адамның электр тогына түсуіне себеп болады.

Осыдан жұмыс компьютерлік кабинетінде мінез-құлық ережелерін сақтаңыз:

- тек таза, құрғақ қолдармен электр құрылғылармен қолдану;
- жұмыс аймағына кірмеңіз;
- ақаулы түрі бар электр сым ашасын розеткаға салуға тыйым салынады;
- жұмыс үдерісі кезінде сымның қыздыру дәрежесін бақылау қажет;
- қосқыштарды, қуат сымдарын, жерге тұйықтау құрылғыларын, монитордың артқы жағына түртуге тыйым салынады;
- жабдықты өзіңіз жөндеуге болмайды;
- электр лампаларының бетіне қағаз, шүберек және басқа да жанғыш материалдарды қоюға тыйым салынады;
- жоғарғы қуатты электр құрылғыларын бір розеткада қосуға болмайды;
- егер құрылыс кодекстерімен көзделмесе, сыныпқа жиһаз және жабдықты қайта өңдеуді жүзеге асыруға тыйым салынады;

Егер ғимарат өртеле бастаған болса, қажет шаралар:

- барлық электронды жабдықты ажыратыңыз;
- өртті жою үшін сақтық шараларын қолданыңыз;
- мүмкіндігінше материалдық активтерді босату;
- тиісті қызметтерге өрт туралы есеп беру − кезекші, басқарушы бақылау пункті.

Мұндай жағдайда, егер электрлік кернеу ДК-ның металл бөліктерінде немесе жердегі сымдарда анықталса, жабдықты кешіктірусіз ажыратыңыз. Компьютерлік сыныпта жұмыс істейтін адамдар электр тогынан зардап шегетін адамдар мен күйіктерден зардап шеккен адамдардың басымдықты шараларын біледі.

Жұмыс ортасында тұтану көзідері:

- электр жабдықтарының ақаулары, сымдардағы, электр розеткалары мен ажыратқыштардағы ақаулар. Сондықтан, ақауларды уақтылы анықтау және жою, жоспарлы тексеріс жүргізу және барлық ақауларды уақтылы жою үшін өрттің алдын-алу өте маңызды;

- электр құрылғыларының ақаулығы. Өртті болдырмауға қажетті шараларға электр құрылғыларын уақтылы жөндеу, бұзылған электр құрылғыларын сапалы емес жөндеу кіреді;

- бөлмені ашық жылыту элементтері бар электр жылытқыштарымен жылыту. Қыздырылған беттердің шығуы өртке әкеледі, өйткені бөлмеде кітаптар, нұсқаулықтар және қағаз түріндегі қағаз құжаттары мен анықтамалықтар бар.

- жанғыш зат. Өрттің алдын алу үшін зертханада ашық жылыту құрылғыларын пайдаланбауды ұсынамын;

- сымдағы қысқа тұйықталу. Қысқа тұйықталу салдарынан өрт шығу ықтималдығын азайту үшін сымды жасырын істедім.

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

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

4.1.4 Электр қауіпсіздігі

Қоғамдық ғимараттардың электротехникалық құрылғылары Қазақстан Республикасының электр қондырғыларын орнату ережесіне, ҚР ҚНжЕ 2.04-01-2001 [5] талаптарына сәйкес жобаланады.

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

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

Токтың келесі шектік мәндерін бөліп атауға болады:

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

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

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

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

Тиімді жерлендірген желілерде электр қауіпсіздігі қамтамасыз етілген деп жерлендіргіштегі φж потенциалы 10 кВ-тан аспайтын, ал

жерлендіргіштің нәтижелі кедергісі жылдың кез-келген мерзімінде 0,5 Ом-нан аспайтын болып саналады.

4.2 Есептеу бөлімі

4.2.1 Қорғаныстық жерге тұйықтау есебі

1 кВ-қа дейінгі кернеуі бар электр қондырғыларының, сонымен қатар 1-ден 35 кВ-қа дейінгі электр қондырғыларының жерге қосылуын есептеу, әдетте, электродтың токтың таралуына рұқсат етілген кедергісін пайдалану әдісімен жүргізіледі. Бұл жағдайда жердегі электрод біртекті жерге орналастырылуына рұқсат етіледі.

Есептеу тогын А мына формула бойынша анықтадым:

$$I_З = \frac{U_Л(35L_К + L_В)}{350} \qquad (4.1)$$

$$I_З = \frac{6(35 \cdot 2 + 3{,}4)}{350} = 1{,}26 \text{ А},$$

Мұнда $U_Л$ = 6 кВ - желінің сызықтық кернеуі.

Жерге қосу желісінің қысқа тұйықталу тогының кедергісі:

$$R_\mu \leq \frac{U_{пр\ доп}}{К_{пр} I_З} \qquad (4.2)$$

$$R_\mu \leq \frac{40}{1{,}0 \cdot 1{,}26} = 31{,}75 \text{ Ом};$$

Жерге қосу құрылғысының кедергісінің жарамды мәні ретінде $R_а$ < 4 Ом қабылдадым.

Магистральды жер сымының ГПП-нің орталық жерге қосқышынан ең алыс электр қондырғысына кедергісі:

$$R_м = r_{ом} \cdot l_{мз} = 0{,}92 \cdot 1{,}0 = 0{,}92 \text{ Ом}, \qquad (4.3)$$

мұнда, $r_{ом}$ = 0,92 Ом/км - негізгі жер сымының АС-35 ұзындығының бірлігінің кедергісі, $l_{мз}$ = 1 км - сым ұзындығы.

Электрқондырғы сымының жерге тұйықтау желілерінің кедергісі:

$$R_{зж} \leq \frac{l_{зж}}{\gamma S_{зж}} = \frac{1000}{54{,}3 \cdot 25} = 0{,}73 \text{ Ом}, \quad (4.4)$$

$R_д$ < 4 Ом шартына негізделген орталық жердегі электродтың кедергісі:

$$R_{цз} = R_д - R_{зп} = R_д - (R_{мз} + R_{зж}) = 4 - (0{,}92 + 0{,}73) = 2{,}35 \text{ Ом}, \quad (4.5)$$

Мұнда, $R_{зп}$ – жерге тұйықтағыш өткізгіштердің орталық жердегі электродтан ең алыс жерге тұйықталған қондырғыға кедергісі.

Қосалқы станцияның орталық жерге қосу құрылғысы үшін d = 4 см, l = 300 см құбырларды қолданандым. Балшыққа төзімділік р = 0,4-10^4 Ом · см.

Электрод жүйесінің жер бетінен ортасына дейінгі қашықтық t = 70 + l / 2 = 220 см.

Жоғарғы ұшы жер деңгейінен төмен орналасқан тік құбырлы жерге тұйықтағыштың ағуына кедергі:

$$R_{зв} = \frac{0,366pK}{l}\left(lg\frac{2l}{d} + \frac{1}{2}lg\frac{4t+l}{4t-l}\right) =$$

$$\frac{0,366 \cdot 0,4 \cdot 10^4 \cdot 1,65}{300}\left(lg\frac{2 \cdot 300}{4} + \frac{1}{2}lg\frac{4 \cdot 220+300}{4 \cdot 220-300}\right) = 18,76 \text{ Ом},$$

(4.6)

мұнда, К =1,65 – 1 климаттық белдеу үшін маусымдық коэффициент.

Тік электродтардың орналасуы контур бойымен алынады. Тік құбырлы электродтар арасындағы қашықтық 6 м = 600 см қабылданады, пайдаланудың коэффициентін ескерместен орталық жердегі электродтың қажетті электродтарының саны:

$$n_э = \frac{R_{зв}}{R_{цз}} = \frac{18,76}{2,35} = 8 \text{ электродтар.}$$

Электродтар контур бойымен орналасқан кезде электродтар арасындағы қашықтықтың ұзындығына $\frac{a_э}{l} = \frac{600}{300} = 2$ қатынасы үшін тік электродтардың пайдалану коэффициенті $\eta_в$ = 0,7 болады.

$$n'_э = \frac{n_э}{\eta_в} = \frac{8}{0,7} = 12 \text{ электродтар.}$$

Қосылу жолағының ұзындығы:

$$l_n = 1,05a_э n'_э = 1,05 \cdot 600 \cdot 12 = 7560\text{см} = 75,6 \text{ м.}$$

Жолақтың ені b = 2,5 см, жолдың төсеу тереңдігі t = 70 см. Климаттық аймақтың К = 5,5 үшін маусымдық коэффициенті. Байланыстырушы жолақтың ағымдық кедергісі:

$$R'_{цз} = \frac{0,366рК}{l_п} lg\frac{2l_п^2}{bt} = \frac{0,366 \cdot 0,4 \cdot 10^4 \cdot 5,5}{7560} lg\frac{2 \cdot 7560^2}{2,5 \cdot 70} = 6,19 \text{ Ом.}$$

Электр тізбегіндегі электродтар саны бар тік электродтардың пайдалану коэффициенті $n'_з = 12\ \eta_в = 0,67$, қосу жолағының пайдалану коэффициенті $\eta_г =\ 0,41$. Тік электродтарды және байланыстырушы жолақты кәдеге жаратуды ескере отырып, жердегі орталық электродтың толық кедергісі:

$$R'_{пз} = \frac{1}{\frac{\eta_г}{R_{ог}} + \frac{n'_э \eta_в}{R_{эв}}} = \frac{1}{\frac{0,41}{6,19} + \frac{12 \cdot 0,67}{18,76}} = 2,02 \text{ Ом.}$$

Жердегі желінің ең алыс жерлендірілген қондырғыға жалпы кедергісі

$$R_{з.общ} = R'_{цз} + R_{мз} + R_{зж} = 2,02 + 0,92 + 0,73 = 3,67 \text{ Ом} \leq R_д = 4 \text{ Ом.}$$

Жанасудың нақты кернеуі:

$$U_{пр.ф} = I_з K_{пр} R_{з.общ} = 1,26 \cdot 1,0 \cdot 3,67 = 4,62B \leq U_{пр.доп} = 40\ B.$$

4.2.2 Алғашқы өрт сөндіру құралдарына қажеттілікті есептеу

Су көздері алыс немесе пайдалану мүмкін емес жағдайда алғашқы өрт сөндіру құралдары көмекке келеді. Оларға ішкі өрт гидранттары (ҚК), құм, су, отқа төзімді төсек жапқыш және басқа да құралдар кіреді.

Олар өртті алғашқы минуттарда сөндіруге, оның ғимарат ішінде таралуына жол бермейді. Бастапқы өрт сөндіру техникасын қолдану өте оңай. Мұны ұзақ уақыт зерттеудің қажеті жоқ, кез-келген адамға нұсқау беру жеткілікті.

Жабдықтау нормалары бірнеше параметрлерге байланысты:

- құралдар орналастырылуға тиіс алаңдар;
- жарылыс қауіптілігі және өрт қауіптілігі бойынша кеңсе санаттары;
- ішінде не болуы мүмкін (өрт класы).

Есептеулерді бастамас бұрын және нормаларды қадағаламас бұрын, кеңсе санатын анықтау, онда не сақталатынын талдау қажет. Кеңсе өрт немесе жарылыс қаупі бар ма осыған байланысты болады.

Нормада көрсетілгендей, алғашқы өрт сөндіру құралдары тақталарға бекітіліп, шкафтарға орнатылады. Егер ғимаратта ішкі сумен жабдықтау болмаса, ал гидрант 100 м-ден астам қашықтықта болса немесе мүлдем болмаса, қалқандар ілулі болады. Қандай қалқанды орнату керек және ол үшін қандай құралдарды таңдау ең ықтимал өрт сыныбына байланысты.

Бастапқы өрт сөндіру құралдарының қажетті санын анықтау өте қарапайым. Олардың көмегімен есептеулер жүргіземіз.

Жабық кішігірім бөлмелердің нормаларына сәйкес, көлемі 50 ш.м. аспайтын коммуналдық бөлмелер. м портативті өрт сөндіргіштерді ауыстыруға немесе өздігінен жүретін ұнтақпен толықтыруға болады. Көбінесе олар адамдар сирек баратын жерлерде орнатылады. Олар шамамен 100 ° қызған кезде жұмысқа қосылады.

Есептеу үшін ғимараттың қай категорияға жататынын және өрт класын біліп алдық. Біздің жағдайда, ауданы 14 ш.м. және от А (қатты заттардың жануы), соған 2 көбікті 5 литр өрт сөндіргіші орнаттық.

Немесе бірдей мөлшерде 5 литр (салмағы 4 кг) ұнтақты өрт сөндіргіш орнатуғада болады. Көріп отырғаныңыздай, есептеу қарапайым. Нормаларға қайшы келмеу үшін өнімді артығымен алуға болады.

Өртті сөндірудің маңызды құралы ретінде өрт сөндіргіштерге ерекше назар аудару керек. Олар үшін стандарттар бар және есептеулер жүргізіледі. Олар қол өрт сөндіргіш (10 л дейін) және жылжымалы. Біздің жағдайда қол өрт сөндіргішті қолдандық.

390 Қағиданың XIX бөлімінде ұйымдардың алғашқы өрт сөндіру құралдарын алуы және тығыздық есептеулер жүргізу ережелері сипатталған. Біздің ғимаратта өрт сөндіргіштің жоспарланған тұтанатын орнына дейінгі арақашықтық 20 м.

Алғашқы өрт сөндіру құралдарын олар алыстан байқалатын, бірақ эвакуациялау үшін жолды бөгемейтіндей етіп орналастырылды. Тіпті қысқа

адам бұл өрт сөндіргішке жете алады. Мұнда ерекше есептеулер қажет етпейді.

4.2 Кесте - Алғашқы өрт сөндіру құралдарының нормалары

Ғимараттың атауы	Қорғалатын аймақ немесе қондырғы	Өрт сөндіргіштер					Қосымша өрт сөндіру құралдары	
		көбік пенсу	ұнтақ	хладон	көмірқышқылдары	аралас көбік ұнтағы	құмсалғыш	асбестматасы немесе кошма
Әкімшілік-қызметтік ғимарат	14 ш.м.	2++	2+	-	2+	-	-	-

«++» белгісі қондырғылармен жабдықтауға ұсынылған сөндіргіштерді білдіреді.

"+" Белгісімен қолдануға ұсынылатын және тиісті негіздеме болмаған кезде жол берілетін өрт сөндіргіштер белгіленген.

Қорытынды

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

5 Ақпараттық қауіпсіздіктің тәуекелдерін есептеу

5.1. Тәуекелдерді талдау және бағалау

Дипломдық жұмыстың осы бөлігінде біз компанияның ақпараттық қауіпсіздік шаралары үшін тәуекелдерді 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 кемшілік. 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) - компанияның процестерінің бөлігі ретінде оның өмірлік циклінің барлық кезеңінде ақпаратты өңдеу үшін қолданылатын ақпарат және оны өңдеу құралдары (аппараттық және бағдарламалық жүйелер). Тәуекелдерді бағалау үшін біз компаниядағы ақпараттық ресурстарды анықтап, оларды түгендеу мен жіктеуді жүргіземіз. Айта кету керек, компанияның негізгі қызметін жүзеге асырумен айналысатын барлық ақпараттық ресурстар түгендеуге жатады.

Түгендеу кезінде ақпараттық ресурстарға олардың иелері, мақсаты, бірегей қасиеттері, орналасқан жері және т.б. туралы ақпарат кіретін атрибуттар жиынтығы тағайындалады. Компания үшін ресурстың құнын және қорғаудың талап етілетін деңгейін анықтау үшін оны құпиялылық, тұтастық және қол жетімділік санаттарына жіктеу қажет. Компанияның барлық ақпараттық ресурстарына тұтастық пен қол жетімділіктің жіктеу мәндерінің бірыңғай шкаласы енгізілген. Ақпараттық ресурстар санаттарын тағайындау қажетті жеткіліктілік қағидаттарына негізделуі керек, өйткені құпиялылық талаптарын асыра бағалау үрдісі бар және т.б. Ақпараттық ресурстарды түгендеу және санаттарға бөлу процесі циклдік сипатта болады және ақпаратты өңдеуге, беруге, сақтауға арналған ортадағы / мазмұндағы кез-келген маңызды өзгерістермен байланысты.

Ақпараттық ресурстарды түгендеу және жіктеу нәтижесінде біз ресурстар туралы ақпаратты және оларға қойылатын талаптарды қамтитын тізілім аламыз.

Маңызды объектілердің тәуекелдерін есептеу үшін бағалау әдістемесі қолданылды екі фактор үшін қауіп.

Бірінші кезеңде теріс әсер (ресурс көрсеткіші) қауіпке ұшыраған әрбір ресурс үшін алдын-ала анықталған шкала бойынша бағаланады.

Екіншіде - бірдей шкала бойынша әрбір қауіпті іске асыру мүмкіндігі бағаланады.

Үшінші кезеңде тәуекел көрсеткіші есептеледі. Техниканың қарапайым нұсқасында бұл көбейту арқылы жасалады. Дегенмен, көбейту операциясы сандық шкалалар үшін анықталғанын есте ұстаған жөн. Теріс әсердің және қауіптің ықтималдығының көрсеткіші болып табылатын дәреже (сапа) параметрлері үшін. Тиісінше, белгілі бір ұйымға қатысты қауіп-қатер көрсеткіштерін бағалау әдістемесі әзірленуі керек.

Қатердің ықтималдығы сарапшылардың пікірлерімен, болжауымен, сондай-ақ статистикалық мәліметтерге негізделген. Бұл белгілі бір уақыт ішінде қауіпті іске асырудың күтілетін санын анықтайтын оң сан.

Әрбір жобалық тәуекелділікті сипаттайтын келесі маңызды компонент - шығын мөлшері.

Ақпараттың ашылуына, рұқсатсыз өзгертілуіне, уақытша қол жетімсіздігіне немесе жойылуына байланысты қауіпсіздік инциденттері нәтижесінде ұйымға келтірілген залалдың мөлшері ақпараттық активтердің құнымен анықталады. Мұндай оқиғалардың салдары жоғалған пайда, бәсекелестік артықшылықты жоғалту, ұйымның беделінің нашарлауы, үшінші тұлғаның мүдделеріне нұқсан келтіру, айыппұлдар, тікелей қаржылық шығындар немесе қызметті қайта ұйымдастыруда көрініс табуы мүмкін. Оның үстіне, әрбір актив үшін ең нашар жағдайды қарастырған жөн.

5.1 кесте - Қауіптің туындау ықтималдығы шкаласы

Қауіптің туындау ықтималдығы шкаласы	
Ықтималдық деңгейі	Қатердің ықтималдығы
1 - өте төмен	10 жылда шамамен 2-3 рет
2 - төмен	Әр 5 жылда бірнеше рет және одан аз
3 – орташа	Жылына бірнеше рет
4 - жоғары	Шамамен айына бір рет
5 - өте жоғары	Айына бірнеше рет

Келесі кестеде деңгейлер бойынша тәуекел салдарының шамасы көрсетілген.

5.2 кесте-залал шамасының шкаласы

Залал шамасының шкаласы	
Мәні	Сипаттамасы
1-өте төмен	құны 50 000 теңгеге дейін
2-төмен	құны 200 000 теңгеге дейін
3-орташа	құны 500 000 теңгеге дейін
4-жоғары	құны 1 000 000 теңгеге дейін
5-өте жоғары	құны 1 000 000 теңгеден жоғары

Осы активтерді таңдау компанияның АҚ қатерін азайту мүмкіндігін әзірлеу және VPN желісін әзірлеу кезінде негізгі ресурстар маршрутизатор, сервер, брандмауэр және жұмыс станциялары болып табылады.

5.3 кесте – Тәуекелдерді бағалаудың қорытынды кестесі

№	Қауіптер	Осалдық	Тәуекелдің ең жоғары деңгейі	Сипаттамасы	Тәуекелдің қалдық деңгейі
1 Жұмыс Станциялары					
1.1	Тасымалдаушыларды немесе құжаттарды ұрлау	Бақылаусыз көшіру	5	Құпия ақпараттың ақпараттық жүйеден ағып кетуінің алдын алу	2
1.2	Бағдарламалық жаңылыс	DDOS шабуылдар немесе техниканы істен шығаруға бағытталған басқа да шабуылдар	9	Интрузияны анықтау жүйесі, жүйенің резервтік көшірмесі	4
1.3	Деректерді бұрмалау	АЖ-мен жұмыс істеу кезінде белгіленген ережелерді білмеу және / немесе сақтамау және деректерді өзгерту	5	NSD енгізу мүмкіндігін болдырмайды	2
1.4	Дұшпандық апплеттер мен вирустар	Зиянды БҚ орнату, қорғалмаған сайттарға бару	8	Дұрыс антивирустық бағдарламаны таңдау. Вирусты анықтау процедуралары	3
2 Маршрутизатор					
2.1	Бас тарту қызмет көрсетуде	Желілік жабдықтың дұрыс ұйымдастырылмауы, қашықтан өшіру	8	Басып кіруді анықтау жүйесі, жүйені резервтік қалпына келтіру	5

2.2	Деректерді бұрмалау		4	Конфигурация элементтеріне рұқсатсыз кіруден қорғау; жүйені резервтік қалпына келтіру	1
2.3	Белсенді желілік компоненттердің дұрыс емес конфигурациялары.	Алаяқтық туралы мәліметтерді тексерудің болмауы, қол жеткізуді дұрыс емес басқару	4	OS басқаруымен TCP / IP желілік сервистерін теңшеу	2
2.4	Бақыланбайтын көшіру	Бастапқы және ресурстық IP адрестерін алмастыру мүмкіндігі	7	Зиянды бағдарламалар мен сайттарды өткізу үшін сүзу параметрлері	4
3 Сервер					
3.1	Серверді басқаруға рұқсат етілмеген алу	Қатынау құқықтарының дұрыс бөлінбеуі	8	МТЖ жүзеге асыру мүмкіндігін болдырмайды	4
3.2	Жабдықтың істен шығуы	Кемшіліктері бар үздіксіздік жоспарлары	9	Басып кіруді анықтау жүйесі, жүйені резервтік қалпына келтіру	5
3.3	SQL-кодты енгізу	SQL сұраулары үшін сүзгілеу ережелерінің жеткіліксіздігі	9	ЭМ үшін АҚ саясаты, сүзгілерді пайдалану	5
3.4	Серверлік кеңейтулерді енгізу	Пайдаланушы берген деректерді сервермен түсіндірілген файлға сақтамас бұрын тексерудің болмауы.	8	Рұқсат етілмеген кіру мүмкіндігін болдырмайды	4
4 Брандмауэр					

4.1	Брандмауэрге рұқсатсыз кіру	Қауіпсіздік саясатын дұрыс орнатпау, жүйе администраторының қателері	9	Деректер конфигурациясы және OS қауіпсіздік саясаты	6
4.2	Зиянды БҚ (вирустар)	Құрылғыға арнайы құрылған XML-пакеттерді жіберу және еркін кодты қашықтан орындау мүмкіндігі.	9	Vpn функционалын желіаралық экрандарда теңшеу, ОЖ жаңартуын орнату.	5
4.3	Бұзушыға ерікті командаларды орындауға мүмкіндік беретін Endian Firewall қаупі	Басқарушы деңгейде деректерді тазалау бойынша шаралар қолданбау (командаға енгізу)	8	ЭМ үшін АҚ саясаты, сүзгілерді пайдалану, осалдықтардың сканерлері (желілік сканерлер).	4

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).

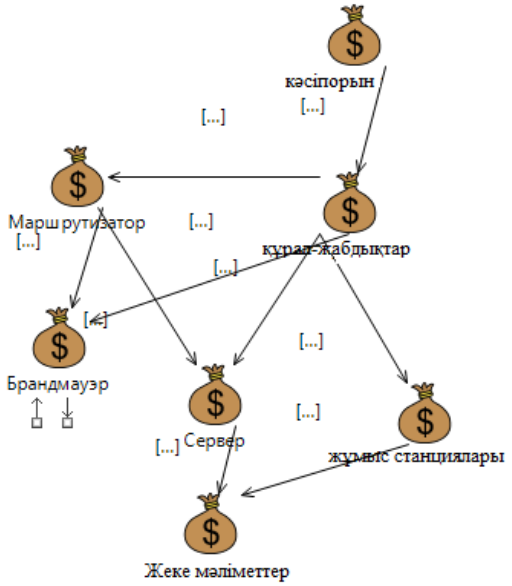
5.2 CORAS құралы арқылы тәуекелдерді талдау

CORAS әдісі-бұл тәуекелді модельдеу арқылы талдау нәтижелері туралы есептерді құжаттауға, жасауға мүмкіндік беретін компьютерленген құрал.

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

Тәуекелдерді талдаудың көрнекілігі үшін Coras бағдарламалық құралдарын пайдаланған. Жоғарыда сипатталған активтер диаграммасын және олардың арасындағы байланысты құрдық (5.1 сурет).

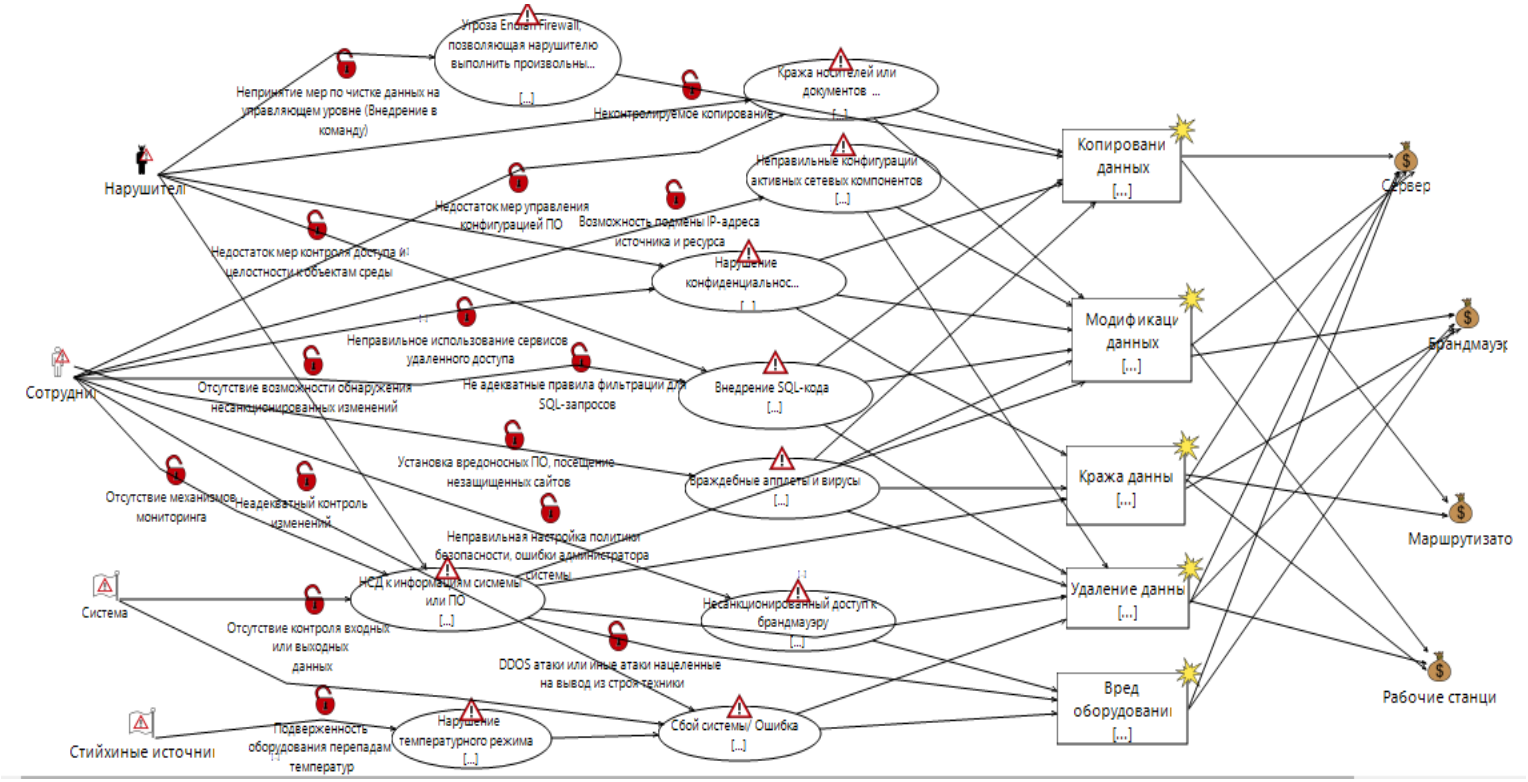
Бағдарламалық жасақтамада қорғауға жататын құндылықты (ақпаратты) білдіретін Asset элементі пайдаланылады.



5.1 сурет – Активтер диаграммасы

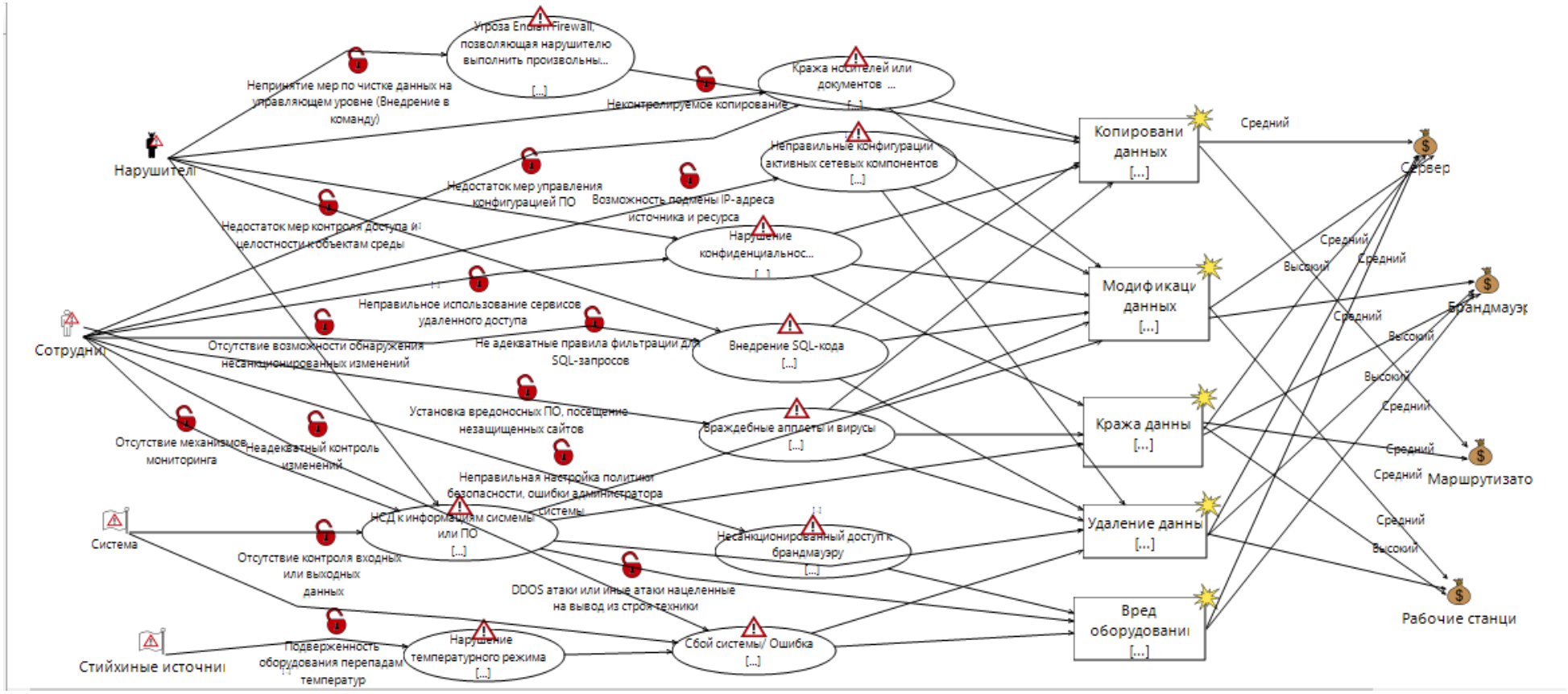
5.4-кестені пайдалана отырып, тәуекелдерді үлгілейміз. Тәуекелдер диаграммасын генерациялаймыз, бұдан әрі әрбір актив үшін әрбір тәуекел бойынша осы тәуекел жүзеге асырылған жағдайда салдарларды анықтаймыз. Алынған диаграмма 5.4 суретте көрсетілген

- Элементтер пайдаланылады:
- 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 Vulnerability;
- Жағымсыз оқиғаларды белгілеу үшін Unwanted Incident.



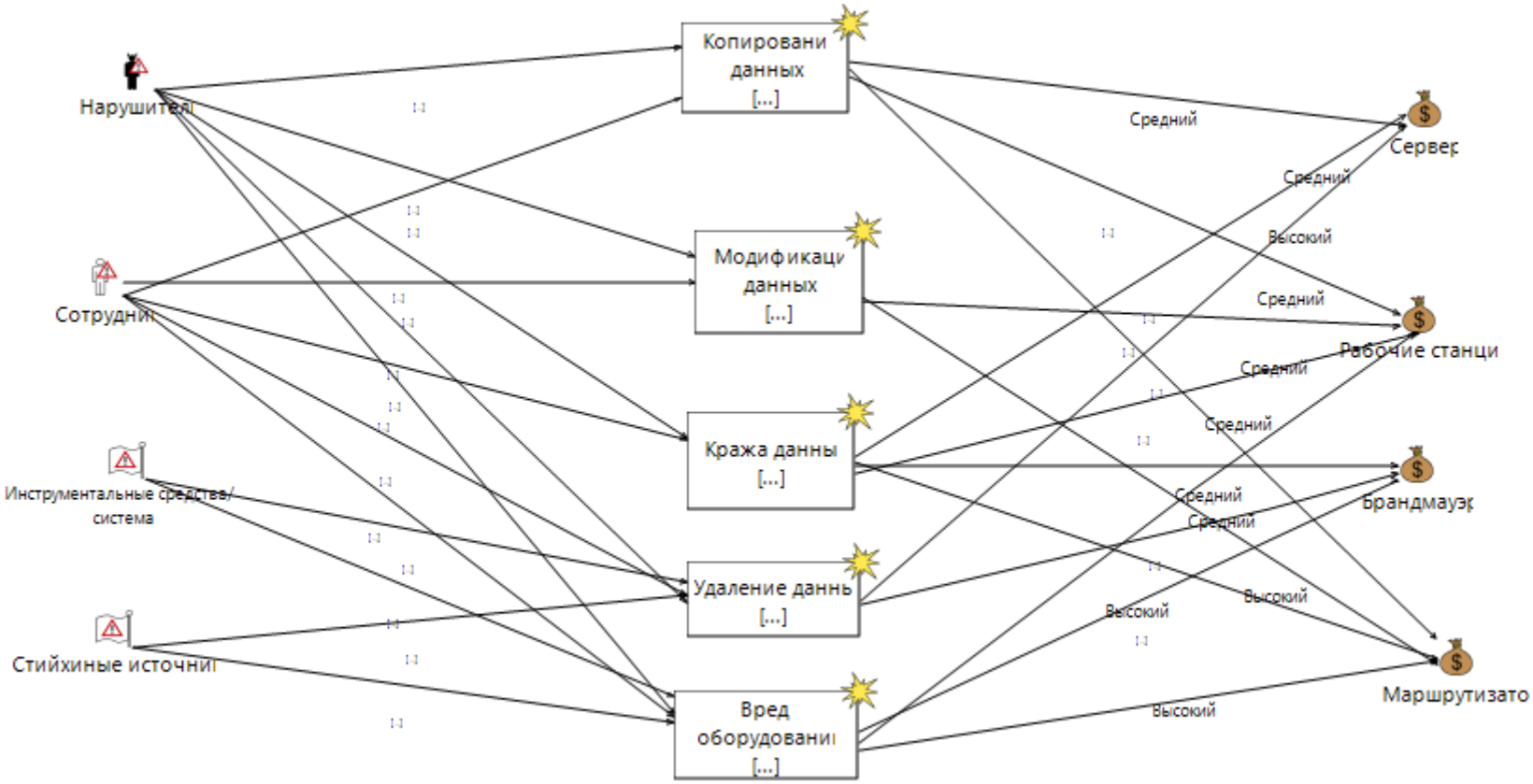
5.2 сурет - Қауіптер моделі

Бұдан әрі анықталған тәуекелдерді іске асыру жиілігін анықтаймыз (белгілі бір уақыт кезеңі ішінде қауіп-қатерді іске асырудың күтілетін саны).



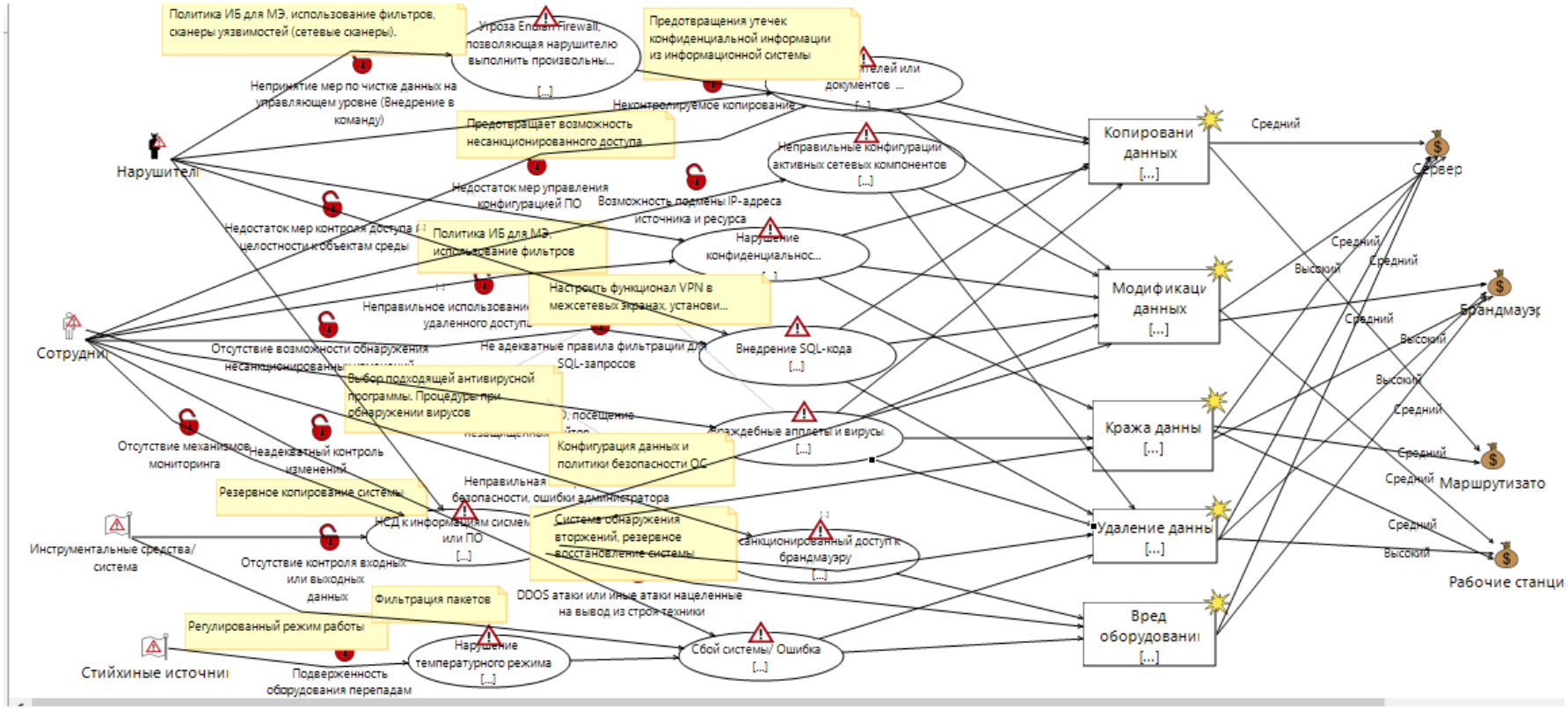
5.3 сурет - Ықтималды сипаттамалары бар қауіптер моделі

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



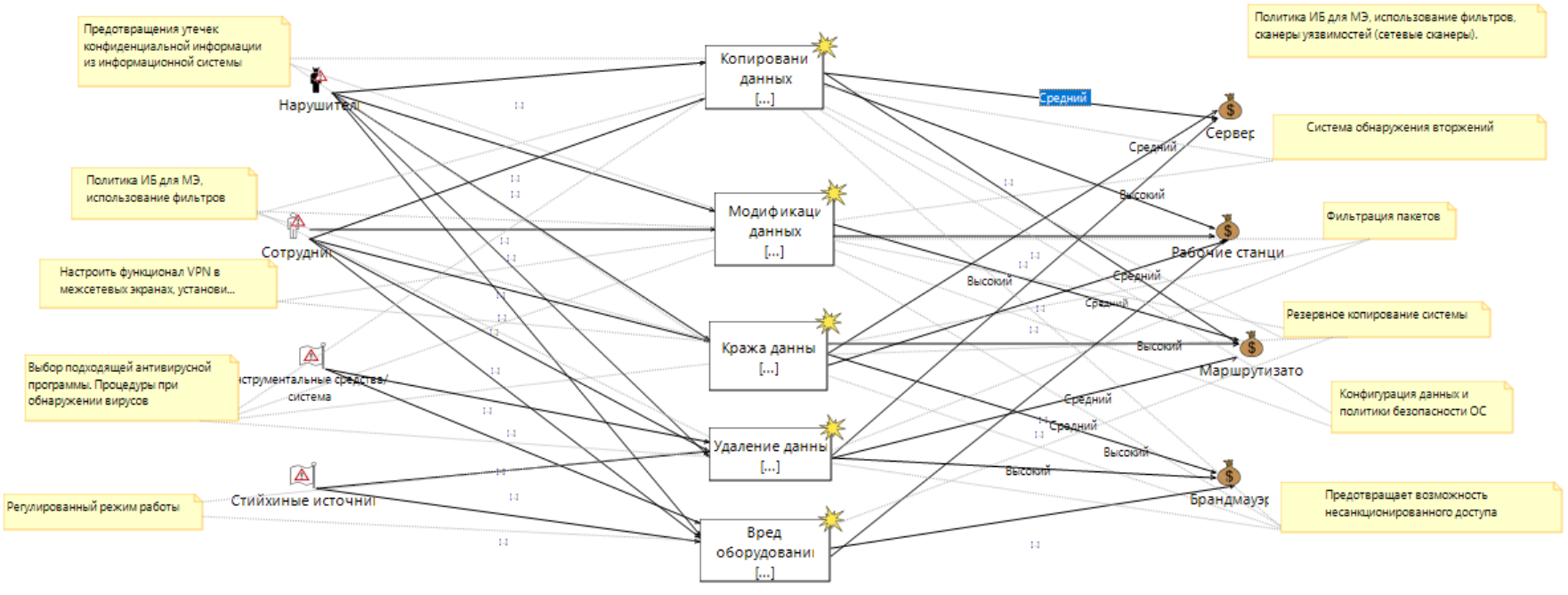
5.4 сурет - Қауіптің салдарын сипаттайтын тәуекелдер кестесі.

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



5.5 сурет - Қорғаныс шараларын қосқаннан кейінгі қауіптердің диаграммасы.

Қорғаныс шараларын қосқаннан кейін, қолайсыз қауіптер қалуы мүмкін. Мұндай жағдайларда шешім қабылдаушылар қалыпты қабылдау өлшемдеріне сәйкес келмейтін тәуекелдерді сақтауға мәжбүр болуы мүмкін. Қажет болған жағдайда шешім қабылдаушы тәуекелдер туралы нақты түсінік беріп, тәуекелді қабылдаудың қалыпты өлшемдерін алып тастау туралы шешім қабылдауға себеп болуы керек (5.6 сурет).



5.6 сурет - Рұқсат етілмейтін тәуекелдер диаграммасы

Қорытынды

Дипломдық жоба бөлігінің мақсаты (қауіп-қатерді бағалау) дамыған объектіні қорғау жүйесі үшін тәуекелдердің сипаттамаларын анықтау болып табылады.

Барлық анықталған ресурстар үшін тәуекелге талдау жасалды және ақпараттық жүйені қорғау шаралары анықталды. Тәуекелдерді бағалау процесінің негізгі жұмыстары қарастырылды. Таңдалған активтердің негізгі қауіптері мен осал тұстары қарастырылды. Біз екі факторды есептеу әдісін қолдана отырып, тәуекелдерді бағаладық. Қорғаныс шараларын қолдануды ұсынды. Содан кейін тәуекел ұсынылған қорғаныс шараларын ескере отырып қайта есептелді. Қорғау шараларын жүзеге асырғаннан кейін актив тәуекелі 2 есе азайды.

Екінші бөлімде CORAS және UML диаграммаларын қолдана отырып, ақпараттық қауіп-қатерлер талданды, олар активтерді анықтаудан бастап, қауіптер мен осалдықтар моделінен бастап, қарсы шаралар қолданумен аяқталды

Қорытынды

Дипломдық жобаны орындау барысында ақпараттық қауіпсіздік қатерлерінің негізгі түрлері және олардан қорғау әдістері зерделенді. Клиент VipNet күйге келтіру, сондай-ақ PacketTracer симуляторы бағдарламасын пайдалана отырып, осы желіні модельдеу жүргізілді.

Виртуалды желіні модельдеу нәтижелері анықталған арна бойынша желіні қорғауды пайдаланған кезде пакеттер саны қандай трафик өтетініне байланысты өзгеретінін көрсетті. Бізді қызықтыратын трафик шифрланбайды.

VPN-желі ашық стандарттар негізінде желілерді пайдаланатын коммуникациялардың барлық түрлері үшін, сондай-ақ корпоративтік желі ішіндегі ең жауапты жалғанушылар үшін деректерді қорғауға мүмкіндік береді.

Әдебиеттер тізімі

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

2. ГОСТ 12.1.006-84 Система стандартов безопасности труда (ССБТ). Электромагнитные поля радиочастот. Допустимые уровни на рабочих местах и требования к проведению контроля. - М.: ИПК Издательство стандартов, 2002.

3. Гигиенические требования к микроклимату производственных помещений: Санитарные правила и нормы СанПиН 2.2.2.542-96. -М.; Информационно-издательский центр Минздрава России, 2001. -20 с.

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

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

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

7. 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.

Әдебиеттер тізімі

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

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

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

4. 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).

Пайдаланған әдебиеттер тізімі

1 Столлингс В. Криптография и защита сетей: принципы и практика, 2-е изд. – М.: Издательский дом «Вильямс», 2001. – 455 б.

2 Конеев И.Р., Беляев А.В.. Информационная безопасность предприятия.- СПб.: Издательство БХВ-Петербург2003. – 215 б.

3 Олифер В.Г., Олифер Н.А. Виртуальные частные сети на основе MPLS. Журнал сетевых решений LAN, 2002. – № 3. – 54-58 б.

4 Норткат С. Обнаружение нарушений безопасности в сетях. – М.: Издательство Диалектика-Вильямс, 2003. – 512 б.

5 Петров А.А. Компьютерная безопасность. Криптографические методы защиты. – М.: Издательство ДМК, 2000. – 412 б.

6 Хетч Б., Колесников О. LINUX: создание виртуальных частных сетей (VPN). – М.: Издательство КУДИЦ-ОБРАЗ, 2004. – 312 б.

7 Щеглов А.Ю. Защита компьютерной информации от несанкционированного доступа. – СПб.: Издательство Наука и Техника, 2004. – 315 б.

8 Зима В.. Безопасность глобальных сетевых технологий.BHV-СПб., 2001. – 247 б.

9 Bradley, Mitchell. "VPN - Virtual Private Network." VPN - Virtual Private Network. 2008.

10 Развертывание сети ViPNet. Руководство администратора. – М.: ОАО «Инфотекс, 2011. URL: http://www.infotecs.ru.

11 Салливан К. Прогресс технологии VPN. PCWEEK//RE, 1999. - №2.

12 Штайнке С. VPN между локальными сетями. LAN//Журнал сетевых решений. – 1998. - №10. – т. 4.

13 Фратто М. Секреты виртуальных частных сетей// Сети и системы связи. – 1998. - №3 (25).