ҚАЗАҚСТАН РЕСПУБЛИКАСЫ БІЛІМ ЖӘНЕ ҒЫЛЫМ МИНИСТРЛІГІ

Қ.И. Сәтбаев атындағы Қазақ ұлттық техникалық зерттеу университеті

Ақпараттық және телекоммуникациялық технологиялар институты

«Киберқауіпсіздік, Ақпаратты Өңдеу және Сақтау» кафедрасы

Сейлбек Абзал Ерғалиұлы

«Ұйымның ақпараттық жүйесінің қауіпсіздік саясатын талдау және дамыту»

Дипломдық жоба

ТҮСІНІКТЕМЕЛІК ЖАЗБА

5В100200 – «Ақпараттық қаупсіздік жүйелері» мамандығы

Алматы 2019

ҚАЗАҚСТАН РЕСПУБЛИКАСЫ БІЛІМ ЖӘНЕ ҒЫЛЫМ МИНИСТРЛІГІ

Қ.И. Сәтбаев атындағы Қазақ ұлттық техникалық зерттеу университеті

Ақпараттық және телекоммуникациялық технологиялар институты

«Киберқауіпсіздік, Ақпаратты Өңдеу және Сақтау» кафедрасы

ҚОРҒАУҒА ЖІБЕРІЛДІ
Кафедра меңгерушісі,
т.ғ.к., ассистент-профессор
_____ Н.А.Сейлова
«14» 05 2019 ж.

Дипломдық жобаға
ТҮСІНІКТЕМЕЛІК ЖАЗБА

Тақырыбы: «Ұйымның ақпараттық жүйесінің қауіпсіздік саясатын талдау және дамыту»

Мамандығы 5В100200-Ақпараттық қаупсіздік жүйелері

Орындаған Сейлбек А.Е.

Пікір беруші
К.т.н Ассистент-профессор,
Зав.секцией СИБ
_____ Аманжолова С.Т.
«___» _____ 2019 ж.

Ғылыми жетекші
Сениор-лектор
_____ Зиро А.А.
«___» _____ 2019 ж.

Алматы 2019

ҚАЗАҚСТАН РЕСПУБЛИКАСЫ БІЛІМ ЖӘНЕ ҒЫЛЫМ МИНИСТРЛІГІ

Қ.И. Сәтбаев атындағы Қазақ ұлттық техникалық зерттеу университеті

Ақпараттық және телекоммуникациялық технологиялар институты

«Киберқауіпсіздік, Ақпаратты Өңдеу және Сақтау» кафедрасы

5В100200- Ақпараттық қаупсіздік жүйелері

БЕКІТЕМІН
Кафедра меңгерушісі,
т.ғ.к., ассистент-профессор
_____ Н.А.Сейлова
«14» 05 2019 ж.

Дипломдық жобаны орындауға
ТАПСЫРМА

Білім алушы *Сейлбек Абзал Ерғалиұлы*
Тақырыбы: *«Ұйымның ақпараттық жүйесінің қауіпсіздік саясатын талдау және дамыту».*
Университет Ректорының *2018 жылғы «16»* 10 №_____ бұйрығымен бекітілген
Аяқталған жұмысты тапсыру мерзімі *2019 жылғы «28»* 04
Дипломдық жобаның бастапқы берілістері: *Осы жобаны әзірлеу қажеттігін анықтайтын пәндік аумақты зерттеу және ақпаратты қорғау және ақпараттық қауіпсіздіктің қолданыстағы жүйесінде кемшіліктерді анықтау.*
Дипломдық жобада қарастырылатын мәселелер тізімі
1. Теориялық бөлім
2. Практикалық бөлім
3. *Қосымша*
Сызба материалдар тізімі (міндетті сызбалар дәл көрсетілуі тиіс)
Сызба материалдары 13 слайдта көрсетілген
Ұсынылған негізгі әдебиет *7 атаудан тұрады*

Дипломдық жобаны дайындау

КЕСТЕСІ

Бөлім атауы, қарастырылатын мәселелер тізімі	Ғылыми жетекші мен кеңесшілерге көрсету мерзімі	Ескерту
Теориялық бөлім	16.03.2019-26.03.2019	
Практикалық бөлім	07.04.2019-28.04.2019	

Дипломдық жобабөлімдерінің кеңесшілері мен норма бақылаушының аяқталған жобаға қойған қолтаңбалары

Бөлімдератауы	**Кеңесшілер аты, әкесінің аты, тегі (ғылымидәрежесі, атағы)**	**Қол қойылған күні**	**Қолы**
Норма бақылау	Зиро А.А.	14.05.2019	

Ғылыми жетекшісі Зиро А.А.

Тапсырманы орындауға алған білім алушы Сейлбек А.Е.

Күні «13» маусым 2019 ж.

ҚАЗАҚСТАН РЕСПУБЛИКАСЫНЫҢ БІЛІМ ЖӘНЕ ҒЫЛЫМ МИНИСТРЛІГІ
СӘТБАЕВ УНИВЕРСИТЕТІ

РЕЦЕНЗИЯ

Дипломдық жұмыс
(жұмыс түрінің атауы)

Сейлбек Абзал
(білім алушының Т.А.Ә.)

5В100200 – «Ақпараттық қауіпсіздік жүйелері» мамандығы

(мамандық атауы мен шифрі)

Тақырыбы: Ұйымның ақпараттық жүйесінің қауіпсіздік саясатын талдау және дамыту

Орындалды:
а) графикалық бөлім _____ парақ
б) түсініктеме _____ бет

ЖҰМЫСҚА ЕСКЕРТУ

Әрбір мекеменің басты қауіпсіздік мақсаттарының бірі ақпараттың ағып кетпеуінде. Компьютерлік желілер мен байланыс жолдарында болатын ақпараттан басқа, маңызды келіссөздер кезінде, телефон әңгімелерінде болатын ауызша хабарлар да қорғануы қажет. Ақпараттық тәуекелдің негізгі белгілейтін көзі - бұл ұйым үшін құндылық туралы ақпаратты қамтитын ақпараттық актив.

Студент Сейлбек А. дипломдық жұмысты орындау кезінде өзінің жұмысқа деген ынтасын, оқу кезінде алған теориялық білімін практикада дұрыс қолдана білетіндігін айқын түрде көрсеткен.

Жұмыста кәсіпорындағы ақпараттық қауіпсіздік тәуекелдерін сараптамалық бағалау мәнін, жіктелуін, әдістерін терең талдаған.

Орындалған дипломдық жұмыс мазмұны жоғары деңгейде ашылған және рәсімдеуі талаптарға сай келеді.

Дипломдық жұмыс алдына қойылған мақсат, міндеттерін толығымен ашқан, өз бетінше логикалық аяқталған жұмыс деп айтуға тұрады.

ЖҰМЫСТЫҢ БАҒАСЫ

Дипломдық жұмысты «___90___» бағалаймын және Сейлбек А. 5В100200 мамандығы бойынша әскери іс және қауіпсіздік бакалавры деген біліктілікке лайық деп санаймын.

ҚАЗАҚСТАН РЕСПУБЛИКАСЫНЫҢ БІЛІМ ЖӘНЕ ҒЫЛЫМ МИНИСТРЛІГІ
СӘТБАЕВ УНИВЕРСИТЕТІ

Пікір беруші
К.т.н. Ассистент–профессор,
кафедрасы меңгерушісі
_____С.Т Аманжолова
«13» января 2019 ж.

ҚАЗАҚСТАН РЕСПУБЛИКАСЫ БІЛІМ және ҒЫЛЫМ МИНИСТРЛІГІ
СӘТБАЕВ университеті

ҒЫЛЫМИ ЖЕТЕКШІНІҢ ПІКІРІ

Дипломдық жобаға
(жұмыс түрлерінің атауы)
Сейлбек Абзал Ерғалиұлына
(студенттің аты жөні)
5В100200-Ақпараттық қауіпсіздік жүйелері
(мамандық атауы мен шифрі)

Тақырыбы: «Ұйымның ақпараттық жүйесінің қауіпсіздік саясатын талдау және дамыту»

Сейлбек Абзал Ерғалиұлы дипломдық жұмысында ұйымның ақпараттық жүйесінің қауіпсіздігін арттыру бойынша зерттеу жұмысын жүргізген.

Қазіргі уақытта техника және телекоммуникациялық құралдар кеңінен таралған. Осындай құралдар арқылы әр түрлі ақпарат өте көп мөлшерде өңделеді және тасымалданады.

Алайда, ақпартты өңдеу, сақтау және тасымалдау құралдары жұмыс істеген кезде осы ақпаратдың ағып кетуі мүмкін.

Сондықтан Сейлбек А.Е. дипломдық жобасына таңдаған тақырыбы Кәсіпорынның ақпараттық қауіпсіздігін сырыптау және тәуекелдерін бағалау әдістемесін талдап, оның ерекшелеіктеріне сипаттама берумен байланысты.,

Сонымен қатар қолданыстағы тыңшылық - бағдарламаларға талдау жүргізген, олар құрылғының пайдаланушысы үшін жиі байқаусыз және вирусқа қарсы ақпаратты ұрлайды және қаскүнемге жібереді. Зерттеу барысында аса күрделі бағдарламаны орнату және тексеру жүргізген.

Дипломдық жобаны орындау барысында студент университеттен алған білімін толықтай пайдаланып, өзінің ғылыми және тәжірибелік білімінің жақсы деңгейде екенін көрсетті. Дипломдық жобаны өз бетінше орындады.

Сейлбек Абзал Ерғалиұлына дипломдық жобасы қойылған талаптарға сай келеді, қорғауға ұсыныс жасаймын.

Ғылыми жетекші

Магистр т.н. лектор
(қызметі, ғыл. дәрежесі, атағы)
_____ Зиро А. А.

«13» Маусым 2019 ж

Протокол анализа Отчета подобия Научным руководителем

Заявляю, что я ознакомился(-ась) с Полным отчетом подобия, который был сгенерирован Системой выявления и предотвращения плагиата в отношении работы:

Автор: Сейлбек Абзал

Название: Ұйымның ақпараттық жүйесінің қауіпсіздік саясатын талдау және дамыту

Координатор:Аасо Зиро

Коэффициент подобия 1:0,7

Коэффициент подобия 2:0

Тревога:1

После анализа Отчета подобия констатирую следующее:

☑ обнаруженные в работе заимствования являются добросовестными и не обладают признаками плагиата. В связи с чем, признаю работу самостоятельной и допускаю ее к защите;

☐ обнаруженные в работе заимствования не обладают признаками плагиата, но их чрезмерное количество вызывает сомнения в отношении ценности работы по существу и отсутствием самостоятельности ее автора. В связи с чем, работа должна быть вновь отредактирована с целью ограничения заимствований;

☐ обнаруженные в работе заимствования являются недобросовестными и обладают признаками плагиата, или в ней содержатся преднамеренные искажения текста, указывающие на попытки сокрытия недобросовестных заимствований. В связи с чем, не допускаю работу к защите.

Обоснование:

.....
.....
.....
.....
.....
.....

13.05.19 .....

Дата

.....

Подпись Научного руководителя

Протокол анализа Отчета подобия

заведующего кафедрой / начальника структурного подразделения

Заведующий кафедрой / начальник структурного подразделения заявляет, что ознакомился(-ась) с Полным отчетом подобия, который был сгенерирован Системой выявления и предотвращения плагиата в отношении работы:

Автор: Сейлбек Абзал

Название: Ұйымның ақпараттық жүйесінің қауіпсіздік саясатын талдау және дамыту

Координатор: Аасо Зиро

Коэффициент подобия 1:0,7

Коэффициент подобия 2:0

Тревога:1

После анализа отчета подобия заведующий кафедрой / начальник структурного подразделения констатирует следующее:

✓ обнаруженные в работе заимствования являются добросовестными и не обладают признаками плагиата. В связи с чем, работа признается самостоятельной и допускается к защите;
 обнаруженные в работе заимствования не обладают признаками плагиата, но их чрезмерное количество вызывает сомнения в отношении ценности работы по существу и отсутствием самостоятельности ее автора. В связи с чем, работа должна быть вновь отредактирована с целью ограничения заимствований;
 обнаруженные в работе заимствования являются недобросовестными и обладают признаками плагиата, или в ней содержатся преднамеренные искажения текста, указывающие на попытки сокрытия недобросовестных заимствований. В связи с чем, работа не допускается к защите.

Обоснование:

.....
.....
.....
.....
.....

....

Дата 14.05.19 *Подпись заведующего кафедрой /*

начальника структурного подразделения

Окончательное решение в отношении допуска к защите, включая обоснование:

.....

.....

.....

.....

.....

....

Дата 14.05.19

Подпись заведующего кафедрой /

начальника структурного подразделения

АҢДАТПА

Бұл жұмыстың мақсаты кәсіпорынның ақпараттық қауіпсіздігін қамтамасыз ету жүйесін құру жөніндегі іс-шараларды әзірлеу болып табылады.

Жұмыста шешілген міндеттер:

-осы жобаны әзірлеу қажеттігін анықтайтын пәндік аумақты зерттеу және ақпаратты қорғау және ақпараттық қауіпсіздіктің қолданыстағы жүйесінде кемшіліктерді анықтау;

- міндеттің қойылуы;
- бағдарламалық қамтамасыз етуді және инженерлік қорғауды таңдау;
- ұйымдастырушылық құжаттарды әзірлеу;
- жобаның экономикалық тиімділігін негіздеу.

АННОТАЦИЯ

Целью данной работы является разработка мероприятий по созданию системы обеспечения информационной безопасности предприятия.

К задачам, решаемым в работе, относятся:

-изучение предметной области и выявление недостатков в существующей системе обеспечения информационной безопасности и защите информации, определяющих необходимость разработки данного проекта;

- постановка задачи;
- выбор программных и инженерно-технических средств защиты;
- разработка организационных документов;
- обоснование экономической эффективности проекта.

ABSTRACT

The purpose of this work is to develop measures to create information security systems of the enterprise.

The tasks to be solved in the work include:

-study of the subject area and identification of shortcomings in the existing system of information security and the protection of information that determines the need to develop this project;

- problem statement;
- the range of program and technical means of protection;
- development of organizational documents;
- justification of economic efficiency of the project.

МАЗМҰНЫ

КІРІСПЕ

2017 жылдың аяғында - 2018 жылдың басында орын алған экономикалық құбылыстарға байланысты компаниялардың бәсекелестік жағдайын сақтап қалуына, ал кейбір жағдайларда тіпті аман қалуына деген күрес күшейе түсті. Дағдарысқа қарсы стратегиялардың асығыс жасалуы көбінесе артықшылығы жоқ міндеттер мен бағыттарға шығындарды төмендетумен тоғысты.

Осылайша, кейбір ұйымдар, өкінішке орай, ақпараттық қауіпсіздікті осы салаға жатқызады.

«Ақпараттық қауіпсіздік» термині ішкі немесе сыртқы қауіп-қатерлерден компьютерлік жабдық немесе автоматтандырылған жүйе өңдейтін ақпараттың қауіпсіздігі жағдайын білдіреді: қажетсіз жариялау (құпиялылықты бұзу), бұрмалау (тұтастығын бұзу), ақпаратқа қол жетімділікті жоғалту немесе азайту және оның иесіне немесе пайдаланушысына материалдық немесе моральдық зиян келтіретін заңсыз тираждау.Тиісінше, ақпаратты қорғау, қатер қауіпсіздікті бұзудың әлеуетті мүмкіндігі болып табылғанда қауіпсіздік қатерінің іс-қимылдарын болдырмау үшін қабылданған шаралар кешені болып табылады.

Ақпараттық қауіпсіздік туралы айтқан кезде, олар проблемалардың кең ауқымын білдіреді: табиғи апаттардан және электрмен жабдықтау проблемасынан, компьютерлік жүйелерді өздерінің пайдасына қолданатын зиянкестерге дейін.

Жоғарыда айтылғандарға сүйене отырып, таңдалған тақырыптың өзектілігі шығады.

Зерттеу нысаны - ақпараттық жүйе ЖШҚ «АвтоТрейд».

Зерттеу тақырыбы - ұйымның ақпараттық қауіпсіздік жүйесі болып табылады.

Бұл жұмыстың мақсаты кәсіпорынның ақпараттық қауіпсіздігін қамтамасыз ету жүйесін құру жөніндегі іс-шараларды әзірлеу болып табылады.

Жұмыста шешілген міндеттер:

Осы жобаны әзірлеу қажеттігін анықтайтын пәндік аумақты зерттеу және ақпаратты қорғау және ақпараттық қауіпсіздіктің қолданыстағы жүйесінде кемшіліктерді анықтау;

міндеттің қойылуы;

бағдарламалық қамтамасыз етуді және инженерлік қорғауды таңдау;

ұйымдастырушылық құжаттарды әзірлеу;

жобаның экономикалық тиімділігін негіздеу.

Жасалған зерттеудің теориялық және әдіснамалық негізі ретінде ақпараттық жүйелердің қауіпсіздігі саласындағы отандық және шетелдік ғалымдардың жұмыстары алынды. Жұмыста Қазақстан Республикасының заңдары мен нормативтік актілері қолданылады.

Жұмысты жазу кезінде зерттеу тақырыбы бойынша ғылыми әдебиеттерді, нормативтік-құқықтық базаларды оқу, аналитикалық және салыстырмалы әдістер сияқты ғылыми зерттеулер қолданылды.

Жұмысы төрт бөлімнен тұрады. Бірінші тарау кәсіпорынның сипаттамасына, оның ұйымдық құрылымына арналған аналитикалық болып табылады. Кәсіпорында бар, қауіпсіздік мәселелері шешілуі қажет, қолданыстағы технологиялар қарастырылды.

Екінші тарау – жобалық, ақпараттық қауіпсіздік жүйесін құру және дайындау үшін бағдарламалық қамтамасыз етуді таңдауға арналған.

Үшінші тарауда еңбек қорғау мәселелері қарастырылады.

Төртінші тарауда экономикалық тиімділікті есептеу әдістемесі таңдалып, экономикалық көрсеткіштер анықталады.

Нәтижелердің практикалық маңызы олар «АвтоТрейд» компаниясында қолданылуы мүмкін.

1 Сауда мекемесінің қолданыстағы АЖ қауіпсіздігі жүйесін талдау

1.1 Мекеменің сипаттамасы

«АвтоТрейд» ЖШҚ шетел машиналары үшін қосалқы бөлшектер сатады. Дүкен жапон, неміс, корей, қытай, америка, француз, италия, ағылшын автомобильдері үшін жаңа және түйіспе автобөлшектерді сатумен айналысады. Қосалқы бөлшектер қоймада болады немесе тапсырыс бойынша жеткізіледі.

Компания ең заманауи ақпараттық технологияларды, өзінің бағдарламалық жасақтамасын, жұмыс істеген жылдарында жинақталған, нарықтағы аналитикалық және статистикалық ақпаратты, жоғары білікті ұжымды пайдаланады.

Тұтынушыларға:

-автокөлік бөлшектерін on-line іздеу және тапсырыс беру жүйесі;

-еуропалық, жапондық және кореялық өндірушілердің автокөліктерінің қосалқы бөлшектеріне кеңейтілген онлайн каталог;

-қажет бөлшектерді әртүрлі жолдармен іздеу мүмкіндігі:көлік VIN-і бойынша, қосалқы бөлшек нөмірі бойынша, иллюстрацияланған каталог бойынша сұрау;

-бөлшек туралы ең толық ақпарат алу - әртүрлі өндірушілердің аналогтарының болуы, қолданылуы, бағасы және жеткізу уақыты.

-қосалқы бөлшектердің үлкен ассортименті. Баға тізімінде 1200 жетекші әлемдік өндірушілердің 26 миллионнан астам түпнұсқалық және түпнұсқалық емес қосалқы бөлшектері мен керек-жарақтары бар.

-арнайы көліктерге және тюнингке қосалқы бөлшектер.

-жеке қызмет көрсету. Әрбір клиенттің жеке менеджері болады, олар тапсырысты орналастырудан оны алуға дейінгі барлық тізбекті бақылайды.

-жеке қызмет көрсету;

-әрбір клиент бұйрықты тапсырудан толық тізбекті бақылайтын жеке менеджер алады.

-кез келген ыңғайлы төлем түрі.

-еліміздің 200-ден астам қалаларында, клиентке кез келген ыңғайлы әдіспен (автокөлік, әуе, пойыз, курьерді жеткізу) тапсырыстың минималды жеткізу уақыты.

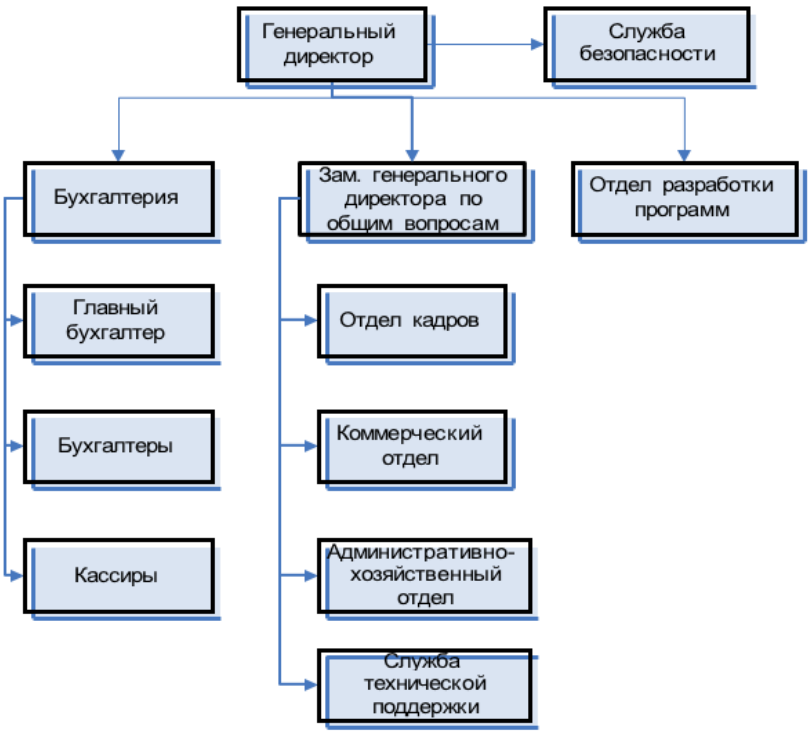
Басқарудың ұйымдастырушылық құрылымы 1.1 суретте көрсетілген. «АвтоТрейд» ЖШҚ қызметкерлері әкімшілік персоналдан, техникалық қолдау қызметінің және сату бөлімінің қызметкерлерінен тұрады.

Әкімшілік қызметкерлер құрамына бас директор, оның орынбасары, қаржы директоры, техникалық директор және бас бухгалтер кіреді. Олардың негізгі міндеті компанияны басқару және оның даму стратегиясын анықтау болып табылады.

Техникалық қолдау қызметтері - желіні басқару және CALL орталығының жұмысына тартылған мамандар. Бұл қызмет компанияның орталық кеңсесінде орналасқан. Желі әкімшісінің міндеттері:

- жаңа пайдаланушыларды қосу (жаңа есепке алу жазуын жасау), пайдаланушы статистикасын бақылау, жұмыс желісіндегі ақаулықтарды жою, бағдарламалық қамтамасыз етуді әзірлеу және жүргізу. Одан әрі қарай олардың міндеттері төменде талқыланады. Сонымен қатар оған CALL-орталығының операторлары кіреді. Күні бойы қоңырау шалынып, бағдарламаны орнатуды икемдеу туралы, сұрақтарға жауаптар және басқа да сұрақтар түседі.

Сату бөлімі сауда менеджерлерінен, сату бойынша кеңесшілерден тұрады. Бұл персоналдың штаты 12 адамнан тұрады.



1.1 Сурет– Фирманы басқаруды ұйымдастыру құрылымы

Кәсіпорынды басқаратын, басқарудың келесі негізгі функцияларын жүзеге асыратын: оралымды басқару, болашақ дамуды, қаржы-экономикалық стратегияны басқаруды жүзеге асыратын бас директор. Директордың функционалдық міндеттерінің шеңбері кадр саясатын, кәсіпорынның әлеуметтік инфрақұрылымын дамытуды, қызметкерлермен жұмыс жасауды қамтиды

Жеке басқару функциялары директорлардың орынбасарларына, ал қаржылық мәселелер бойынша бас бухгалтерге жүктеледі. Бас бухгалтер материалдық және қаржылық есеп функциясын атқарады.

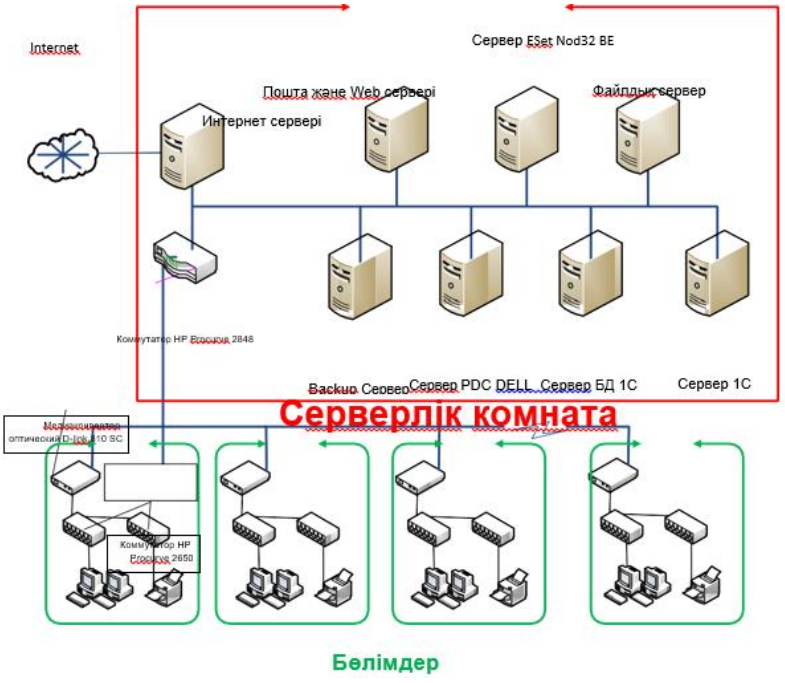
Осылайша, қаралып отырған компания бөлімшесінің ұйымдық құрылымы сызықты болып келеді. Бұл құрылымда әрбір басшы барлық қызмет түрлері бойынша төменгі бөлімшелерге басшылықты қамтамасыз етеді.

1.2Ақпараттық жүйені сипаттау

Компанияның жергілікті компьютерлік желісі компания ақпараттық жүйесінің бөлігі ретінде кеңейтіледі. Бұл есептеуіш, техникалық, бағдарламалық және коммуникациялық байланыстар кешені, кәсіпорын ішінде әртүрлі есептеу техникасымен жабдықталған қашықтағы жұмыс станциялары арасында ашық ақпараттарды тез алмасуға мүмкіндік береді.

Кәсіпорынның жергілікті желісінің құрылымдық схемасы 1.2 суретте келтірілген. Жергілікті желідегі ақпаратты өңдеудің негізгі мазмұны компания ішінде де, сыртқы ақпарат субъектілерімен де ашық ақпарат алмасу болып табылады.

Компанияның жергілікті-есептеу желісі пайдаланушылар мен серверлік сегменттерден тұрады.



1.2 – Жергілікті желінің құрылымдық сызбасы

Компанияның техникалық архитектурасының құрастырушылары серверлік бөлмеде орналасқан.

Келесі сервер жабдықтары пайдаланылады.

- BackupHPProliantDL180g5 сервері- бұл барлық серверлерден резервтік көшірмелерді сақтаушы болып табылады;
- PDCDELL Power Edge R910 сервері - кәсіпорынның басты домен контроллері (AD, DNS және т.б.);
- HP ProliantDL 585 Галактика дереккөз сервері- ERP Галактика негізгі дерекқоры сақталатын және жұмыс істейтін - сервер;
- HPProliantDL 160g6 Галактика сервері- жүйеде жұмыс істеу үшін пайдаланушыларға аппараттық кілтті тарататын ERP Галактика басқарушы сервері;
- Пошталық және Web -сервер HPProliantDL 370g6 - компанияның сайтында пошта және хост сервері ретінде қызмет ететін сервер;
- Esetnod32 BEIntelSR1500ALR Сервері - антивирус әкімшілік сервері ретінде қызмет етеді;
- HP ProliantML350g4 файл сервері - файлдық мұрағат (бағдарламалық жасақтама, пайдаланушы деректері және т.б.) ретінде қызмет етеді;

Интернет сервері - прокси сервердің функцияларын, шотты және трафикті басқаруды жүзеге асырады.

Жоғары жылдамдықтағы байланыс арнасын қамтамасыз ету үшін кәсіпорынның барлық қабаттары талшықты оптика арқылы серверге қосылған.

Пайдаланылған жұмыс станцияларының техникалық сипаттамалары 1.1-кестеде келтірілген.

1.2.1 кесте – Жұмыс станциясының техникалық сипаттамалары

Сипатамалар атауы	**Сипаттама мәні**
Процессор	Core2 Duo, Pentium Dual-Core, Celeron® 400, жүйе шинасының жиілігі 800/1066/1333МГц. (LGA775)
Жүйелік тақта	Intel® DG41TY
Микросхемалар жиынтығы	Intel® G41
Жад	От 512Мб до 8Гб DDR2-667/800 МГц
Бейне ішкі жүйесі	Кіріктірілген Intel® Graphics Media Accelerator X4500
Қтақыл диск	80Гбайттпн, 7200 айналым/мин, Serial-ATA II (4 порта SATA 300)
Қосымша жинақтаушылар	DVD / DVD-RW
Желілік контроллер	Кіріктірілген 1Gbit (Realtek RTL8111D)
Аудио	5.1 (кодек Realtek ALC888VC)
Кеңейту слоты	PCI - 2, PCI-e x1 - 1, PCI-e x16 - 1

Енгізу/шығ арудың стандартты порты	USB 2.0 (8), бірізді (опция), клавиатура PS/2, тышқан PS/2, LAN RJ-45, стереоға желілік кіру, микрофон, динамиктер/ желілік кіру
Корпус	InWin EMR018: MiniTower, БП 350Вт (2 сыртқы бөлігінен 5.25", 2 Сыртқы және 5 ішкі бөліктерден 3.5")MiniTower

АРМ -дегі операциялық жүйе ретінде Windows 7 3 Professional Edition 32-бит пайдаланылады, ал сервер ретінде Windows Server 2008 пайдаланылады. Барлығы желіде 65 пайдаланушы бар.

Office қосымшаларының пакеті ретінде MSWord 2007, MS Excel 2007, MS Outlook 2007 кіретін MS Office 2007 Prof орнатылған.

Бар серверлерді, сондай-ақ дискілік жүйені басқару IBMDirector бағдарламалық жасақтамасы арқылы жүзеге асады.

Компания бөлімшелерінің қызметі «1С: Бухгалтерия 8.0», «1С: Жалақы және қызметкерлерді басқару 8.2» сияқты компоненттерді қамтитын «1С: Кәсіпорын 8.0» бағдарламалық кешенін пайдалану арқылы автоматтандырылған.

Желінің пайдаланушыларының құқықтарын бөлу үшін домен құрылымы ActiveDirectory қызметін пайдалану арқылы ұйымдастырылады.

HandyBackup деректері резервтік көшіру және үндестіру үшін пайдаланылады. Қатты дискіден, жеке файлдардан және папкалардан деректерді, суреттерді, видеоларды, поштадан және т.б. деректердің сақтық көшірмесін кез келген тасымалдаушыға сақтап, жасауға және қалпына келтіруге мүмкіндік береді.

UserGateProxy & Firewall жергілікті желіден интернетке қоғамдық қол жеткізуді ұйымдастыруға арналған, трафикті есепке алудан және корпоративтік желіні сыртқы қауіптен қорғауға арналған бағдарламалық жасақтама шешімі болып табылады.

Сонымен қатар, кейбір жұмыс станцияларында сақталған жеке деректердің қауіпсіздігін ұйымдастыру үшін, КриптоПро CSP 3.0 бағдарламалық жасақтамасы қолданылады, ол деректерді шифрлаудың криптографиялық құралы болып табылады.

Компания сондай-ақ «Fast» бейнебақылау жүйесін, өрт дабылы мен күзет дабылы жүйесін, сондай-ақ «Elsys» қатынауды бақылау жүйесін пайдаланады.

«АвтоТрейд» ЖШҚ ақпараттық ресурстарын қорғаудың негізгі мақсаты - «АвтоТрейд» ЖШҚ ақпараттық жүйелерінің жұмысы барысында, немесе олардағы айналымдағы ақпараттарға рұқсатсыз қол жеткізу және оны рұқсатсыз пайдалануда, ақпараттық қатынас субъектілерін олардың кездейсоқ немесе қасақана рұқсат етілмеген кедергісі арқылы елеулі материалдық, физикалық, моральдық немесе өзге де зиян келтіруі мүмкіндігінен қорғау болып табылады.

Ақпараттық қауіпсіздік жүйесінің негізгі міндеттері:

«АвтоТрейд» ЖШҚ-нің бизнес-сабақтастықты қамтамасыз ету үшін ақпараттық ресурстарының қажетті қол жетімділігін қамтамасыз ету;

- «АвтоТрейд» ЖШҚ-ның ақпараттық саласында, соның ішінде шешімдерді қабылдау бойынша қызметтерді қажетті қолдауды жасау мақсатында ақпараттық ресурстардың тұтастығын қамтамасыз ету;
- «АвтоТрейд» ЖШҚ жабық ақпарат ретінде саналатын ақпараттың құпиялылығын қамтамасыз ету;
- өңделген ақпараттың сенімділігі мен өзектілігін қамтамасыз ету;
- «АвтоТрейд» ЖШҚ ақпараттық активтерін пайдалану және оларды басқару жауапкершілігін белгілеу;
- тұтастай алғанда ақпараттық технологиялар үшін де, «АвтоТрейд» ЖШҚ үшін де, негізделген, үнемді және үйлесімді ақпараттық қауіпсіздіктің ұйымдастырушылық - техникалық шараларын қолдану;
- ақпараттық қауіпсіздікті қамтамасыз ету мәселелері бойынша, қызметкерлердің хабардар болуын қамтамасыз ететін, бірыңғай корпоративтік этиканы бекіту;
- ақпараттық активтерді заңсыз пайдалану немесе теріс пайдалану жағдайында «АвтоТрейд» ЖШҚ және қызметкерлерінің заңды құқықтарын қорғау;
- ақпараттық жүйелердің жұмыс істеуінде рұқсат етілмеген әрекеттерден қорғау;
- ақпаратқа, серверлерге және жұмыс станцияларына, қорғау құралдарына кіру құқығын шектеу.

«АвтоТрейд» ЖШҚ-нің қауіпсіз жұмыс істеуі «АвтоТрейд» ЖШҚ-нің бизнес мақсаттарына ықтимал әсер ететін ақпараттық қауіпсіздік саласындағы проблемаларын өз кезегінде анықтаудың, мүмкін болатын проблемалардың себеп-салдарлық байланыстарын анықтаудың және осы негізде олардың дамуының дәл болжамын жасауға негізделген болуы керек.

Көптеген ақпарат компанияның ақпараттық жүйесімен өңделетіндіктен, ақпараттық қауіпсіздік әртүрлі техникалық шараларды қолдану жолымен қамтамасыз етіледі.

2 Ақпаратты қорғаудағы шараларды әзірлеу

2.1 Қорғаныс құралын таңдау

Жоғарыда аталған рұқсат етілмеген кіруден қорғау құралдарынан Secret Net таңдалды. Таңдау жүйенің келесі артықшылықтарына байланысты:
- кеңейтудің және басқарудың қарапайымдылығы;
- әртүрлі қолдану түрлері үшін икемді баптау параметрлері;
- Windows XP -ден Windows 8.1 және Windows Server 2012 R2 дейінгі операциялық жүйелердің кең ауқымын қолдау;
- автоматтандырылған жүйелерді қорғауға арналған заңды талаптардың сақталуы сізді өзіңізді әділетсіз бәсекелестіктен және тексеруші ұйымдардың назарынан қорғауға мүмкіндік береді;
- ішкі қауіптерден қорғау жүйесі есебінен тәуекелдерді азайту;

- жеке деректерді өңдеуде мониторинг және бақылау автоматтандыру деңгейін арттыруға және қауіпсіздік бойынша әкімшілік шараларына байланысты шығындарды азайтуға мүмкіндік береді.

2.2 Таңдалған қорғану шараларының сипаттамасы

Secret Net жүйесіне кіретін орталықтандырылған басқару құралдарын пайдалану үшін, келесі құрауыштар әкімші компьютеріне орнатылуы керек:
- желілік режимде «Secret Net 7» құрауышты (орнатқан кезде «орталықтандырылған кескіндеме құралдарын орнату» опциясын қосу керек);
- «Secret Net 7–«Басқару бағдарламасы» құрауышы.Windows орталықтандырылған басқару құралдарын пайдалану үшін стандартты ОЖ құрауыштары қауіпсіздік әкімшісінің компьютерінде орнатылуы керек. Операциялық жүйенің нұсқасына байланысты құрауыштарды орнату келесі мүмкіндіктермен орындалады:

Windows 8 операциялық жүйесімен жұмыс істейтін компьютерде «Windows 8 пакетіне қашықтағы серверді басқару құралдарын» орнату қажет. Орнатқаннан кейін Windows компоненттерінің тізімінде «Қашықтағы серверді басқару құралдары» бөлімін ашып, «Мүмкіндіктерді басқару құралдары» | «Топтық саясатты басқару құралдары» және «Рөлдерді басқару құралдары | AD DS және AD LDS құралдары қызметтері және Active Directory жеңіл қызметтер каталогы | Active Directory домен қызметтерінің құралдары Active Directory басқару орталығы» қызметтерін қосу керек.| AD DS құралдары | Active Directory басқару орталығы» қызметтерін енгізу қажет.

Windows 7 операциялық жүйесімен жұмыс істейтін компьютерде «Windows 7 үшін қашықтағы сервер басқару құралдарын» орнату қажет. Орнатқаннан кейін, Windows құрауыштарының тізімінде «Мүмкіндіктерді басқару құралдары» | «Топтық саясатты басқару құралдары» және «Рөлдерді басқару құралдары, Active Directory домен

Windows Vista жүйесінде жұмыс істейтін компьютерде «Windows Vista бумасына арналған қашықтағы серверді басқару құралдарын» орнату керек. Орнатқаннан кейін, Windows компоненттерінің тізімінде «Қашықтықтағы басқару сервері құралдары» бөлімін ашу және «Басқару мүмкіндіктері құралдары | Топтық саясатты басқару құралдары» және «Рөлдерді басқару құралдары» құралдары Active Directory домен қызметтері | Active Directory домен бақылаушы құралдары қызметтерін енгізу керек.

Windows Server 2012 операциялық жүйесімен жұмыс істейтін компьютерлер рөлдерді және мүмкіндіктерді қосу шеберін пайдалану арқылы «Топтық саясатты басқару» және «Қашықтағы серверді басқару құралдары» | Рөлдерді басқару құралдары | AD DS құралдары және AD LDS құралдары | AD DS құралдары | AD DS пәрмен жолының құралдары және қызметтік бағдарламалары құрауыштарын қосу керек.

Windows Server 2008 жүйесімен жұмыс істейтін компьютерде қосу құрауыштары шеберін қосу керек, «Топтық саясатты басқару және қашықтағы

серверді басқару құралдары» | Рөлдерді басқару құралдары | AD DS және AD LDS құралдары | AD DS құралдары | AD DS құралдары және пәрмен жолы құралдары «(Ағылшын тіліндегі нұсқасы:» Remote Server Administration Tools | Role Administration Tools | Active Directory Domain Services Tools | Active Directory Domain Controller Tools").

Windows XP немесе Windows Server 2003 жүйесінде жұмыс істейтін компьютерде Windows Server 2003 тарату бумасының Microsoft басқару құралдары жинағының құрамдас бөлігін орнату керек. Пайдаланушы параметрлері кіру қауіпсіздігі және авторластырылған қатынасты басқару арқылы пайдаланылады. Параметрлер түпнұсқаландыру және аутентификация рәсімдерінен кейін пайдаланушы кірген кезде қолданылады.

2.3 Құрылғыға кіру құқығын орнату

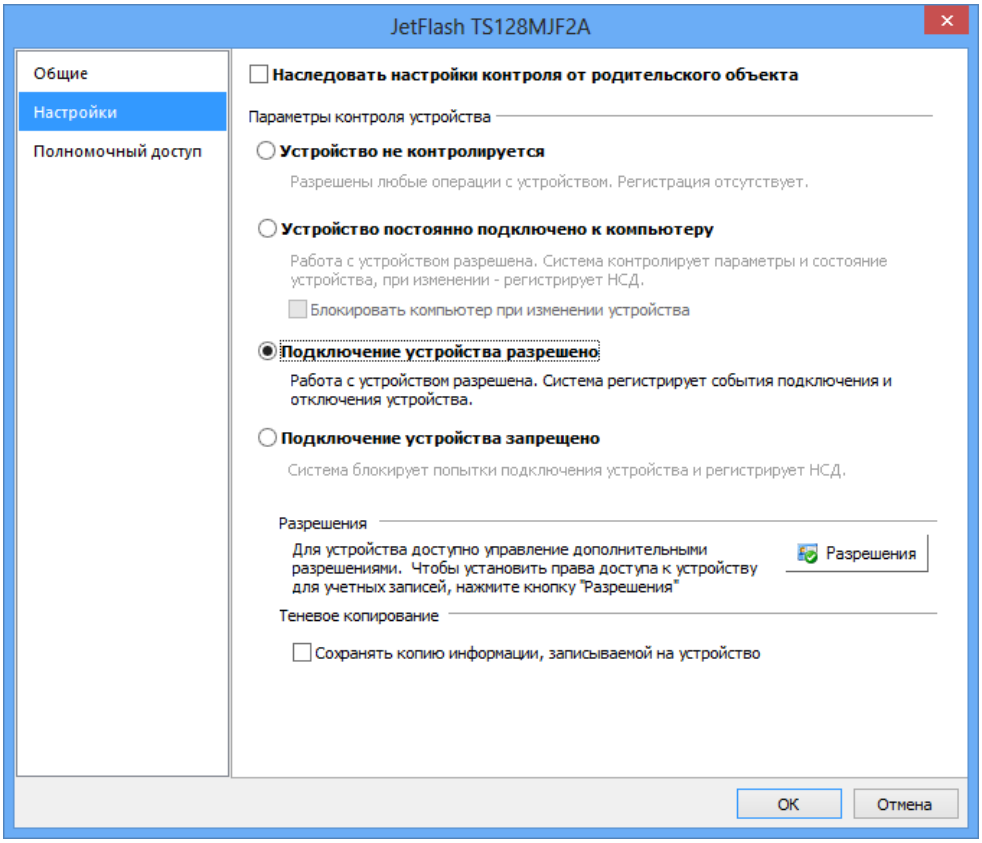
Пайдаланушыға кіру құқығын жеке құрылғылар немесе сыеыптар үшін орнатуға болады.

Құрылғыға кіру құқығын теңшеу үшін:

1) Топтық саясат нысандары параметрлерін басқару үшін қосалқы модульге қоңырау шалыңыз және «Қауіпсіздік параметрлері | Secret Net" параметрлері» бөліміне өтіңіз.
2) «Құрылғы» қалтасын таңдаңыз. Құрылғылар тізімі қосалқы терезенің оң жағында пайда болады.
3) Тізімнен нысан (класс немесе құрылғы) таңдаңыз, контекстік мәзірге қоңырау шалыңыз және «Ерекшелік» пәрменін таңдаңыз. Экранда объектінің параметрлерін орнату үшін диалог пайда болады. Параметрлер тобына өтіңіз.
4) «Ата-аналық нысаннан» бақылауды басқаруды иеленуді алып тастаңыз. Осыдан кейін құрылғының басқару параметрлері қол жетімді болады.
5) «Құрылғы компьютерге тұрақты қосылған» немесе «Құрылғыға қосылу рұқсат етіледі» бақылау режимін тексеріп, «Рұқсаттар» түймесін басыңыз. Экранда Windows тілқатысу терезесі «Рұқсаттар» пайда болады.

«Рұқсаттар ...» тіл қатысуды шақыру мүмкіндігі конфигурацияға рұқсат етілген құрылғылар үшін ғана ұсынылатынын ескеру керек. Рұқсаттар мен тыйым салулар: порттар, дискілер, сақтау құралдары (жүйелік дискінің рұқсатын басқаруға тыйым салынады).

6) Кіру параметрлерін өзгерту үшін тізімдегі есептік жазбаны таңдаңыз, содан кейін рұқсаттарды және әрекеттерге тыйым салуды орнатыңыз. Сонымен қатар, балалардың ата-аналық объектілер параметрлерінен мұрагерлік принципін қарастырыңыз: анық көрсетілген параметрлер ата-аналық объектілерден мұраланған параметрлерді қайта анықтайды.



2.1 сурет – Кіру құқықтарын орнату

Арнайы рұқсаттарды баптау үшін «Қосымша» түймешігін басып, ашылатын тілқатысу терезесіндегі параметрлерді теңшеңіз. Secret Net жүйесінің желілік режимінде домендік және жергілікті пайдаланушылар параметрлері, қорғалған компьютерлердің орталықтандырылған басқаруында және жергілікті дерекқорларында сақталады. Офлайн жұмыс домен және жергілікті пайдаланушы параметрлері жергілікті компьютер дерекқорында сақталады.

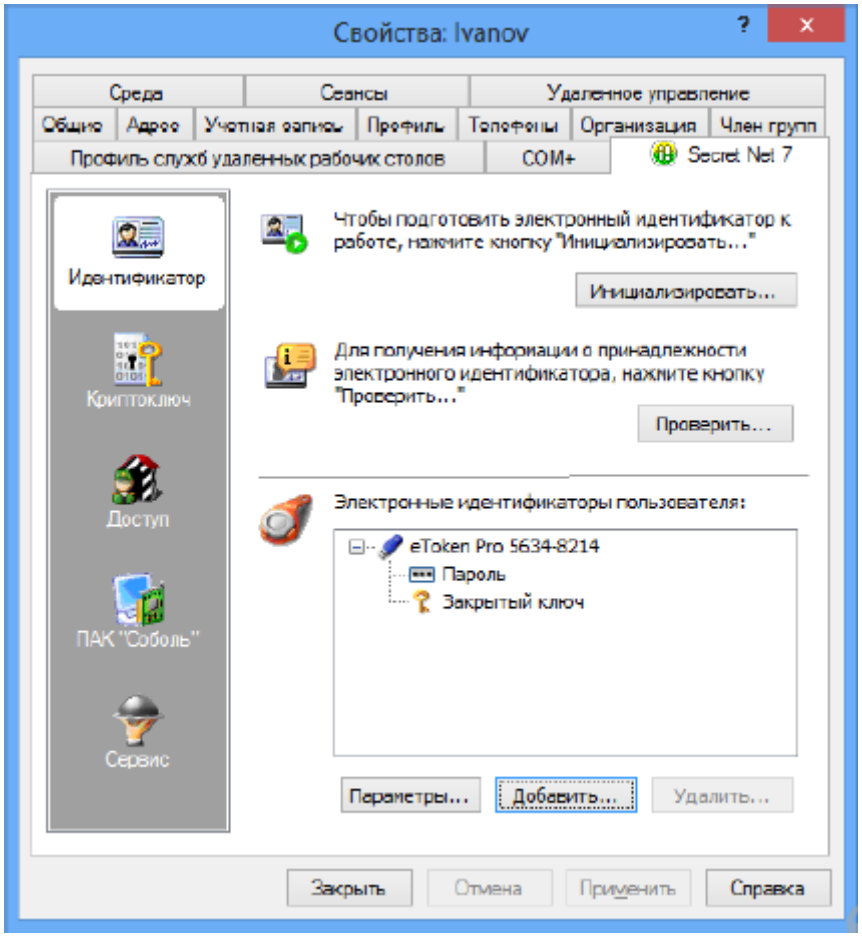
Жергілікті пайдаланушы параметрлері стандартты Windows операциялық жүйесі «Компьютерлерді басқару» қосымшасында жүзеге асады. Сондай-ақ, бұл жабдық құпия ақпарат желісінің жұмыс режимінде домен пайдаланушылары параметрлерін теңшеу үшін пайдаланылады.

«Active Directory пайдаланушылары мен компьютерлер» қосымшасымен жұмыс істеу үшін стандартты Windows орталықтандырылған басқару құралдары, қауіпсіздік әкімшісінің жұмыс орнында орнатылуы керек. Доменді пайдаланушыларға арналған Secret Net жүйесінің параметрлері төмендегі жағдайларда қол жетімді:

- Secret Net жүйесін орнату Active Directory сызбасын модификациялау арқылы орындалады немесе Secret Net конфигурациясының деректері AD тізімдемесінің кескіндеме бөлімінде тіркеледі (қауіпсіздік серверін орнатқанда немесе арнайы пакеттік файлды пайдаланғанда);
-Қауіпсіздік әкімшісінің жұмыс орнында, Secret Net жүйесінің орталықтандырылған параметрлері орнатылады (клиент желінің жұмыс режимінде орнатылғанда).

Пайдаланушы басқару бағдарламасын пайдалану үшін, қауіпсіздік әкімшісінің жұмыс орнында Secret Net жүйесінің орталықтандырылған кескіндемесінің құралдарын орнату жеткілікті.

Пайдаланушы сипаттарын орнату үшін терезеге қоңырау шалыңыз және «Secret Net 7» тілқатысу терезесіне барыңыз.



2.2 сурет – Баптаулар терезесі

Диалогтың сол жақ бөлігінде параметрлердің топтарын таңдау үшін панель бар.

Баптауға арналған құралдар тілқатысу терезесінің оң жағында көрсетіледі.Қажетті параметрлер тобына өту үшін панельдегі тиісті белгішені таңдаңыз:

- «сәйкестендіргіш» - жеке пайдаланушының сәйкестендіргіштерін басқару құралдары;
- пайдаланушы сәйкестендіргіштері;
- «Криптокілт» - пайдаланушының сәйкестендіруін жақсарту үшін негізгі басқару құралдарын қамтиды;
- «Рұқсат» - рұқсат етілген кірудің параметрлерін бақылау және жүйеге кіру мүмкіндігі бар;
- «ПАК «Соболь»» - орнатылған кешендері бар компьютерлерге қатынауды басқару құралдарын қамтиды.

«Соболь». Топ домендік режимде жұмыс істейтін домендік пайдаланушылар үшін ғана бар;

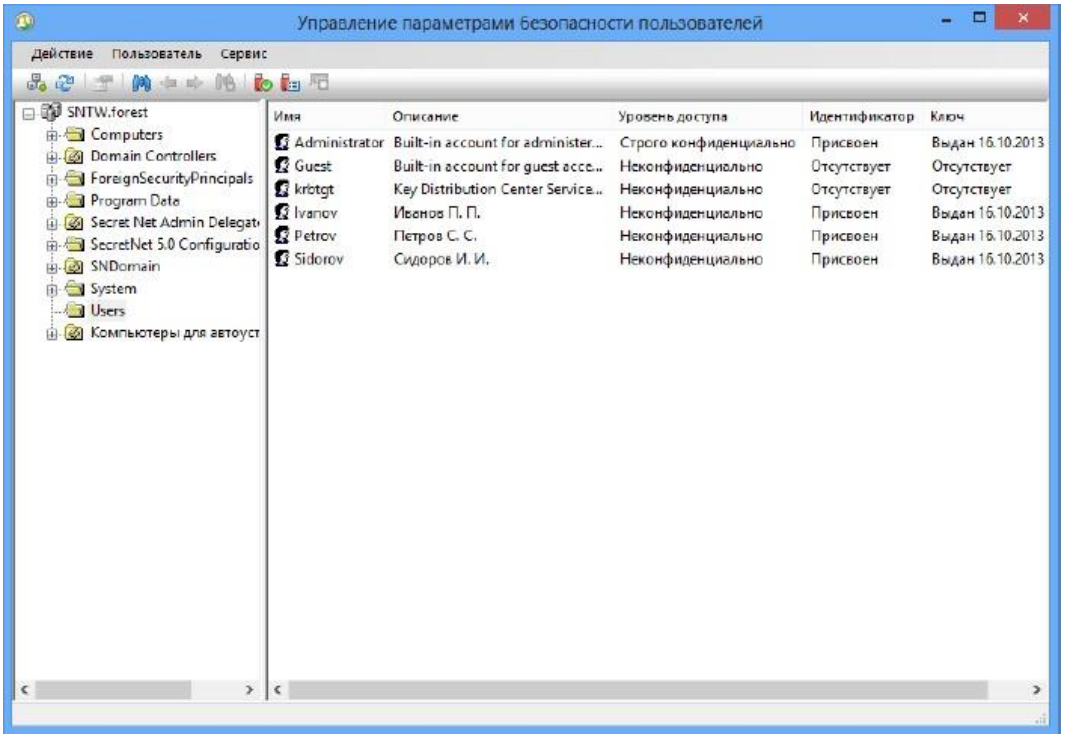
- «Сервис» - «Соболь» ПАК орталықтандырылған басқару және Secret Net жүйесімен TrustAccess бағдарламалық жасақтамасының біріктіруі үшін негізгі басқару құралдарын қамтиды.

Пайдаланушы басқару бағдарламасындағы параметрлерді көру және өзгерту үшін:

1. Орнатылған операциялық жүйенің нұсқасына байланысты тиісті әрекетті орындаңыз:

- Windows 8 немесе Windows Server 2012 жүйесімен жұмыс істейтін компьютерде «Қосу» экранын жүктеп, «Пайдаланушы басқару» тармағын таңдаңыз (Қауіпсіздік коды тобына жатады);
- Басқа операциялық жүйені іске қосатын компьютерде - «Бастау» түймесін басып, бағдарлама шақыру мәзірінде «Қауіпсіздік коды | Secret Net | - «Ақпараттарды басқару» пәрменін таңдаңыз.

Экранда пайдаланушы басқару бағдарламасы терезесі пайда болады:



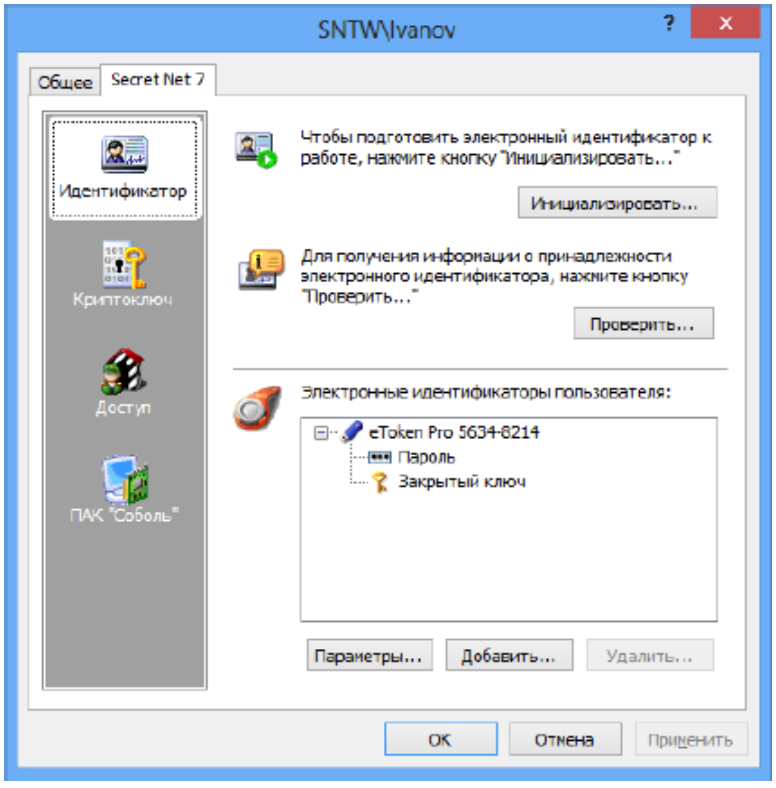
2.3 сурет – Пайдаланушылар қауіпсіздігі параметрлерін басқару

Бағдарламалық интерфейс стандартты Windows Active Directory - пайдаланушылар және компьютерлер ОС сияқты бірдей іске асырылады. Терезенің сол жағында доменнің құрылымдық бөлімшелері және доменнің ұйымдастыру бөлімшелері көрсетіледі, ал оң жағында - таңдалған контейнердегі пайдаланушылардың тізімі көрсетіледі. Пайдаланушылар тізімі кесте түрінде пайдаланушылар кіру деңгейлері, сәйкестендіргіштер мен күшті түпнұсқалық растау кілттері туралы ақпарат бар.

2.Әдепкіде ағымдағы иелік құрылымы бағдарламаға жүктеледі. Қажет болса, осы домендерге қосылуға болатын болса, басқа Active Directory иеліктерінің құрылымдарын жүктеуге болады. Ол үшін «Әрекет» мәзіріндегі «Active Directory домендеріне қосылу» пәрменін пайдаланыңыз.
3.Қалаған бөлімді немесе ұйымдық бөлімшені таңдаңыз. Пайдаланушылардың тізімі терезенің оң жағында пайда болады. Пайдаланушы параметрлерін көру және теңшеу үшін оны тізімнен таңдап, «Пайдаланушы» мәзіріндегі «Сипаттар» пәрменін таңдаңыз.

Экранда пайдаланушы сипаттарын орнату үшін тілқатысу терезесі пайда болады.
«Жалпы» диалогында жалпы пайдаланушы параметрлерін оқыңыз және «Secret Net 7» тілқатысу терезесіне барыңыз.

Тілқатысу интерфейсі, әдеттегі Windows амалдық жүйесінде бірдей атаудағы пайдаланушы қасиеттері параметрлерінің терезесінің тілқатысу терезесіндегідей орындалады. Айырмашылық, пайдаланушы басқару бағдарламасы диалогында параметрлердің «Қызмет» тобы жоқ - осы топтың функциялары негізгі бағдарлама терезесінің «Құралдар» мәзірінің тиісті пәрмендерінде көрсетіледі.



2.4 сурет – Пайдаланушылардың жалпы параметрлері

Қорғаныс жүйесін пайдаланған кезде келесі шараларды қабылдау қажет:
- АЖ үлгілік және жеке деректердің қауіпсіздігін қамтамасыз ету үшін жауапты АЖ қауіпсіздігінің әкімшісін тағайындау қажет;
- әр мердігер АЖ-де қауіпсіздік әкімшісімен тіркелуі тиіс;
- АҚБҚ және АҚЖ бағдарламалық қамтамасыз етуін орнатқан кезде осы қорларға арналған пайдалану құжаттамасын пайдалану қажет;
- ақпараттық қорларды қалпына келтіруді және ЖДҚЖ қамтамасыз ету бойынша шаралар қабылдау қажет. Негізгі тасымалдаушы талаптары мен ұсыныстарына сәйкес болуы керек.

2.4 Қауіпсіздік саясатының дамуы

Ұйымдастырушылық қорғау шарасы ретінде қауіпсіздік саясатын әзірлеуді ұсынуға болады.

АЖ саясаты - [16] үшін әдістемелік негіз болып табылады:

- шектеулі қолжетімділігі бар ақпаратқа қол жеткізу орындарында жүзеге асырылатын ақпаратқа қол жеткізу үшін ақпараттық рұқсатсыз кіруден – біріктірілген ақпараттық қорғау жүйесі нысанында ақпараттық қауіпсіздік кіші жүйесін (бұдан әрі - ЖИТ) дамыту;
- ақпаратты қорғаудың криптографиялық құралдарын пайдалану, сертификаттау орталықтарының жүйесін енгізу, электрондық цифрлық қолтаңбаларды пайдалану және қорғалатын ақпарат алмасудың жеке виртуалды желілерін пайдалану арқылы қауіпсіз электрондық құжаттардыәзірлеу;
- нақты нормативтік құжаттар мен шараларды әзірлеу
- ақпараттық қауіпсіздікті қамтамасыз ету жөніндегі қызметті реттеу; азаматтардың, ұйымдардың және мемлекеттің ақпаратты алуға, таратуға және пайдалануға құқықтарын жүзеге асыру.

ҚОРЫТЫНДЫ

Жұмыста компания қызметінің талдауы жүргізілді, қорғалатын ақпараттық активтер анықталды, осы активтерге қауіптер және ақпараттық қауіпсіздік тәуекелдері бағаланды. Талдау нәтижесінде: ақпараттық қауіпсіздік жүйесінің жаңғыртылуы қажет екендігі, әсіресе, телекоммуникация желілерін қорғау шаралары мен желілерге қосылуға мониторинг жүргізу нашар енгізілгені анықталды.

Компьютерлік жүйеде ақпараттық қорғаудың тиімділігін бағалау үшін ақпаратты қорғаудың мақсаттары мен міндеттерін біріктіруге негізделген осы шартты ішінара қарсы алу үшін бірнеше тәсілдерді таңдауға болады. Сонымен қатар, осы конвенцияны толығымен бұзу мүмкін болмайтындығын атап өту керек, бұл тиімділіктің тұжырымдамасына тән салыстырмалыққа байланысты.

Бірінші тәсіл - қорғау талаптарын қалыптастыру, оның орындалуы қабылданған шаралардың жеткіліктілігін көрсетеді. Содан кейін қорғаудың мақсаты осы талаптарға сай келетін шарттарға жету. Бұл жағдайда қорғаудың тиімділігі көрсетілген шарттарға жуықтаудың шарасы болып табылады.

Екіншіден, бірқатар сараптамалық қорытындылар белгілі бір сапа ауқымында қорғаныс мақсатына жету фактісіне сәйкес келеді, содан кейін нүктелер межелігіне аударылады. Сонымен қатар, ұпайлар, әдетте, жиынтық (немесе көбейтілген) және бұл сома (өнім) белгілі бір шекті мәннен асып кетсе, қабылданған қорғау шараларының барабарлығы туралы шешім қабылданады. Бұл жағдайда ұпайлардың сомасы (немесе өнімі) тиімділік шарасы ретінде әрекет етуі мүмкін.

Жиі, соманың (өнімнің) әрбір құнына қорғаудың тиімділігі туралы белгілі бір шешім беріледі.

Үшінші тәсілі - мысалы, компьютерлік жүйедегі ақпараттың қауіпсіздігіне қатысты барлық анықталған нақты қатерлерге қарсы тұру және мақсатқа жетуге бағытталған қорғау міндеттерін қалыптастырудан тұратын, ортақ («әмбебап») қорғаудың мақсаты. Бұл жағдайда қорғаудың тиімділігі көрсетілген мақсатқа жетудің шарасы болып табылады, яғни ақпараттың қауіпсіздігіне қатысты барлық анықталған қауіп-қатерлерге қарсы тұру.

Айта кету керек, бүгінгі күні іс жүзінде көрсетілген екі әдіс негізінен пайдаланылады. Олардың біріншісі бірнеше нұсқада жүзеге асырылады, бірақ, әдетте, «функционалдық әдіс» деп аталады.

«Функционалды әдістің» мәні мынада:

Компьютер жүйесіндегі ақпаратты қорғауға қойылатын талаптар компьютерлік жүйеде ақпараттық қауіпсіздіктің белгілі бір деңгейіне жету үшін орындалатын қызметтердің тізімі ретінде анықталады. Қауіпсіздік деңгейі (мұндай деңгейлер компьютерлік жүйенің қауіпсіздік сыныптары болуы мүмкін) сарапшылардың тәжірибесіне негізделе отырып, көбінесе декларативті түрде белгіленеді. Бұл жағдайда ақпараттық қауіпсіздік деңгейіне сәйкес келетін барлық қызметтер орындалса, қорғау тиімді деп саналады. Бұл қызметтер жиі қауіпсіздік қызметтері деп аталады .

«Функционалдық әдіс» кезінде қызметтің өз жұмысының тиімділігі бағаланбайды, оларды «өте тиімді» сертификатталған әдістермен жүзеге

асырылды деп бағалайды. Осы жетіспеушіліктің алдын алу үшін, «сенім талаптары» деп аталатын әдіснама енгізілген, ол орындалатын қауіпсіздік қызметтеріне пайдаланушылардың сенімділігін анықтайды.

Сенімділік деңгейін қалыптастырудың бір жолы - бағалаудың (мүмкін сандық негізде) қабылданатын шаралар мен емдеудің тиімділігі. Дегенмен, бүгінгі күні мұндай бағалау әдістемесі жетіспегендіктен, шын мәнінде сенім деңгейі кейбір сарапшылармен алдын-ала енгізілген ережелерге сәйкес анықталады.

Функционалдық тұрғыдан шын мәнінде «екілік» бағалауды жүзеге асыратындығын атап өту керек. Сонымен бірге, тиімділік тұжырымдамасы қорғаныс үшін қабылданатын шаралардың жеткілікті тұжырымдамасымен ауыстырылады және мұндай «тиімділік» қорғау мақсаттарына жақындату шарасы болып табылмайды. Сонымен бірге, «Функционалдық әдіс» қорғау мақсаттарына қол жеткізу үшін шараның мағынасында тиімділікті бағалауға мүмкіндік беретін көрсеткіштерді құру мүмкіндігін жоққа шығармайды.

Ақпаратты қорғаудың тиімділігін бағалаудың ұпайлық әдісі тиімділікті шартты бағалауға қарсы тұрудың екінші нұсқасын жүзеге асырады және мамандардың сараптамалық шолуларына негізделеді, олардың нәтижелерін өңдейді және оларды нүкте ретінде шығарады, содан кейін алынған ұпайды қабылданған қорғау шаралары тиімділігі туралы пікір түрінде түсіндіреді. Бұл әдіс ISO 17799 стандарты және оның құралдары сияқты, мысалы, COBRA бағдарламалық жасақтама өнімі немесе CRAMM әдісін қолданатын бағдарламалық өнім, RiskWatch бағдарламалық жасақтама өнімі және т.б. сияқты бірқатар халықаралық стандарттарда және бағдарламалық өнімдерде жүзеге асырылады. CRAMM әдісі ең кең таралған, сондықтан төмендегі мысал ұпай әдісімен сипатталады.

ПАЙДАЛАНЫЛҒАН ӘДЕБИЕТТЕР ТІЗІМІ

1.Абрамов А.М., Никулин О.Ю., Петрушин А.Н. Системы управления доступом. - М.: Оберег-РБ, 2011. - 192с.
2.Астахов А. Что такое аудит безопасности? Инфорбизнес/Бумажный бизнес № 38.-2012.
3.Бабаш А.В., Мельников Ю.Н., Баранова Е.К. Информационная безопасность. Лабораторный практикум: Учебное пособие. - М.: КноРус, 2013. – 136с.
4.Бартон Т., Шенкир У., Уокер П. Комплексный подход к безопасности сетей. — М.: Издательский дом «Вильямс», 2013. –208 с.
5.Бил Джей. Обнаружение вторжений. Snort 2.1. — М.: Бином, 2012, - 656 с.
6.Бирюков А.А. Информационная безопасность: защита и нападение. – М.: ДМК Пресс, 2012. – 474с.
7.Галатенко В.А. Стандарты информационной безопасности: курс лекций. – М.: Интернет-Университет Информационных технологий, 2012.
8.Герасименко В. А., Медатунян М. В. Организация комплексной защиты информации на современных объектах // Вопросы защиты информации, №1, 2014.