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

Бәкіров Темірлан Алмасұлы

«Кәсіпорынның ақпараттық қауіпсіздігін сырыптау және тәуекелдерін бағалау әдістемесі»

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
«13» 05 2019 ж.

Дипломдық жобаға
ТҮСІНІКТЕМЕЛІК ЖАЗБА

Тақырыбы: «Кәсіпорынның ақпараттық қауіпсіздігін сырыптау және тәуекелдерін бағалау әдістемесі»

Мамандығы 5В100200-Ақпараттық қаупсіздік жүйелері

Орындаған Бәкіров Т.А.

Пікір беруші
К.т.н Ассистент-профессор, секция жет.
_____Аманжолова С.Т.
«13» 05 2019 ж.

Ғылыми жетекші
Сениор-лектор
_____Зиро А.А.
«13» 05 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
«_13_» _05_____2019 ж.

Дипломдық жобаны орындауға
ТАПСЫРМА

Білім алушы *Бәкіров Темірлан Алмасұлы*
Тақырыбы: *«Кәсіпорынның ақпараттық қауіпсіздігін сырыптау және тәуекелдерін бағалау әдістемесі».*
Университет Ректорының *2018 жылғы «16» қазандағы №1162-б* бұйрығымен бекітілген.
Аяқталған жұмысты тапсыру мерзімі *20__жылғы «__»___*
Дипломдық жобаның бастапқы берілістері: *Әр түрлі объектілерде қауіпсіздік деңгейіне аудит жүргізу сапасын арттыру*
Дипломдық жобада қарастырылатын мәселелер тізімі
1. Теориялық бөлім
2. Практикалық бөлім
3. *Қосымша*
Сызба материалдар тізімі (міндетті сызбалар дәл көрсетілуі тиіс)
Сызба материалдары ___слайдта көрсетілген
Ұсынылған негізгі әдебиет *2 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.	13052019	

Ғылыми жетекшісі Зиро А.А.

Тапсырманы орындауға алған білім алушы Бәкіров Т.А

Күні «13» 05 2019ж.

ҚАЗАҚСТАН РЕСПУБЛИКАСЫНЫҢ БІЛІМ ЖӘНЕ ҒЫЛЫМ МИНИСТРЛІГІ
СӘТБАЕВ УНИВЕРСИТЕТІ

ҒЫЛЫМИ ЖЕТЕКШІНІҢ ПІКІРІ

Бәкіров Темірлан Алмасұлы
(студенттің Т.А.Ә.)
5В100200 Ақпараттық қауіпсіздік жүйелері
(мамандықтың шифрі және атауы)
дипломдық жобасына
(жұмыс түрінің атауы)

Тақырыбы: Кәсіпорынның ақпараттық қауіпсіздігін сыриптау және тәуекелдерін бағалау әдістемесі.

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 Бәкіров Т.А. дипломдық жобасына таңдаған тақырыбы Кәсіпорынның ақпараттық қауіпсіздігін сыриптау және тәуекелдерін бағалау әдістемесін талдап, оның ерекшелеіктеріне сипаттама берумен байланысты.,

Бәкіров Т.А дипломдық жұмысын негізгі екі бөліммен рәсімдеп, бірінші бөлімінде Ақпараттық тәуекелдер: мәні, жіктелуі, тәуекелдерді талдау және басқару әдістері, екінші тәжірибелік бөлімінде Көрсеткіштер жүйесін және бағалау өлшемдерін ескере отырып, аудит объектілерін салыстырмалы бағалау әдістемесі көрсетілген.

Дипломдық жобаны толық көлемде іске асыру стіуденттің университетте оқу кезіндегі игерілген теориялық білімдерінің деңгейін ғана көрсете қоймай, сонымен қатар берілген тапсырма бойынша тәжірибелік іс-шараларды жүзеге асыра алатындығын айқын көрсетті.

Жұмыстның мақсаты, оған жетудің міндеттері мен мазмұны, сондай-ақ жасалған қорытындылары арасындағы логикалық байланыс бар. Жобаның тұтастығы жұмыстың негізгі бөлімдері арасындағы тығыз қарым-қатынастпен және берілген тақырыбы мен зерттеу объектілерінен алшақтаудың жоқтығымен сипатталады.

Дипломдық жобаны жазу кезінде Бәкіров Т.А теориялық материалдарды жинақтау, оларды талдау бойынша жұмысты жүргізіп, білімі мен дағдыларын пайдалана отырып жана әдістемесін ойлаптапты. Сонымен бірге ол мақсаткерлікті, дұрыс шешімдер жасауды көрсете алды. Қателерді түзету бойынша жұмыс атқарды.

Жалпы алғанда, баяндалғандардың негізінде Бәкіров Темірлан Алмасұлының дипломдық жобасы аяқталған жұмыс болып табылады және қорғауға ұсынылуы мүмкін.

ҚАЗАҚСТАН РЕСПУБЛИКАСЫНЫҢ БІЛІМ ЖӘНЕ ҒЫЛЫМ МИНИСТРЛІГІ
СӘТБАЕВ УНИВЕРСИТЕТІ

Ғылыми жетекші
Магистр т.н. лектор
(лауазымы, ғылыми дәрежесі, атағы)
_____ ЗироА.А
(қолы)

2019 жылғы «13» мамыр

ҚАЗАҚСТАН РЕСПУБЛИКАСЫ БІЛІМ ЖӘНЕ ҒЫЛЫМ МИНИСТРЛІГІ
Қ.И.Сәтбаев атындағы қазақ ұлттық техникалық зерттеу университеті

5В100200- Ақпараттық қауіпсіздік жүйелері мамандығының студенті
Бәкіров Темірланның
«Кәсіпорындағы ақпараттық қауіпсіздік тәуекелдерін сараптамалық бағалау»
тақырыбына жазылған дипломдық жұмысына

СЫН-ПІКІР

Әзірленген:
а) графикалық бөлім 8 парақ
б) түсіндірме жазбасы 38 бетте

ЖҰМЫСҚА ЕСКЕРТУ ЖАСАУ

Ақпараттық тәуекелдің негізгі белгілейтін көзі - бұл ұйым үшін құндылық туралы ақпаратты қамтитын ақпараттық актив. Бұған қағазға жазылған, пошта арқылы жіберілген немесе бейнеде көрсетілген, дерекқор серверлерінде, веб-сайттарда, мобильді құрылғыларда, электронды тасымалдағышта, корпоративтік ақпараттық жүйелерде өңделетін ақпаратта және деректер беру арналары арқылы, сондай-ақ бағдарламалық қамтамасыз ету. Бұған Кәсіпорындағы ақпараттық қауіпсіздік тәуекелдерін сараптамалық бағалау барысында халықаралық және ұлттық стандарттардың көп саны әзірленген және олардың арасында ең танымал ISO/IES 27000 және ISO 17799 (BS7799) сериялы стандарттары алынған.

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

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

Сонымен қатар, аудит объектілерін салыстырмалы бағалау (АОСБ) ақпараттық қауіпсіздікті қамтамасыз ету әдістемесі толық қарастырылған.

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

Жұмыс бағасы

«Кәсіпорындағы ақпараттық қауіпсіздік тәуекелдерін сараптамалық бағалау» тақырыбына жазылған дипломдық жұмысты Мемлекеттік аттестациялау комиссиясының алдында сәйкесінше қорғалған жағдайда, өте жақсы деген бағаға (А 90) бағалауға болады.

Пікір беруші
К.т.н. Ассистент-профессор зав.секцией СИБ

_____Аманжолова С.Т
«13» 05 2019 ж

Подпись указанного лица удостоверяю
Аманжоловой С.Т
инспектор по кадрам

Отчет подобия

Университет:	Satbayev University
Название:	Кәсіпорындағы ақпараттық қауіпсіздік тәуекелдерін сараптамалық бағалау
Автор:	Temirlan Bakirov
Координатор:	Аасо Зиро
Дата отчета:	2019-05-08 07:55:01
Коэффициент подобия № 1: ?	**0,6%**
Коэффициент подобия № 2: ?	**0,0%**
Длина фразы для коэффициента подобия № 2: ?	25
Количество слов:	4 652
Число знаков:	39 361
Адреса пропущенные при проверке:	
Количество завершенных проверок: ?	50

К вашему сведению, некоторые слова в этом документе содержат буквы из других алфавитов. Возможно - это попытка скрыть позаимствованный текст. Документ был проверен путем замещения этих букв латинским эквивалентом. Пожалуйста, уделите особое внимание этим частям отчета. Они выделены соответственно.
Количество выделенных слов 3

>> **Самые длинные фрагменты, определеные, как подобные**

>> **Документы, в которых найдено подобные фрагменты: из RefBooks**

>> **Документы,содержащие подобные фрагменты: Из домашней базы данных**

>> **Документы,содержащие подобные фрагменты: Из внешних баз данных**

>> **Документы,содержащие подобные фрагменты: Из интернета**

Детали отчета подобия

Фрагменты, найденные в документах базы данных отмечены красным цветом.
Фрагменты, найденные в интернете отмечены в зеленый .
Фрагменты, найденные в базе данных Юридических актов отмечены синим фоном .

КІРІСПЕ

Ақпараттық тәуекелдерді басқару жөніндегі талаптар көптеген халықаралық және отандық регламенттеуші құжаттарда қамтылған және ақпараттық технологияларды дамытудың қолданыстағы практикасына негізделген. Сондықтан тәуекелдерді басқару проблемаларын және оларды шешу әдістерін зерттеу қазіргі заманғы ақпараттық қоғамда өзекті және сұранысқа ие болып табылады. Қазіргі уақытта тәуекелдерді талдау бойынша жеткілікті тәжірибе мен білім жинақталған. Әрине, ақпараттық қауіпсіздіктің негіздерін оқып-үйрену кезінде осы мәселеге қатысты кейбір жалпы көзқарастар ұсынылуы керек, бірақ қолданыстағы ақпараттық жүйелердің алуандығын ескере отырып, барлық материалдарды меңгеру мүмкін емес. Бұл қосымша зерттеу үшін қажет.

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: Temirlan Bakirov

Название: Кәсіпорындағы ақпараттық қауіпсіздік тәуекелдерін сараптамалық бағалау

Координатор: Аасо Зиро

Коэффициент подобия 1:0,6

Коэффициент подобия 2:0

Тревога:3

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 13.05.22 *Подпись заведующего кафедрой /*

начальника структурного подразделения

Окончательное решение в отношении допуска к защите, включая обоснование:

.....
.....
..... Допущена к защите
.....
.....

....

Дата 13.05.19г. *Подпись заведующего кафедрой /*

начальника структурного подразделения

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: Temirlan Bakirov

Название: Кәсіпорындағы ақпараттық қауіпсіздік тәуекелдерін сараптамалық бағалау

Координатор: Аасо Зиро

Коэффициент подобия 1:0,6

Коэффициент подобия 2:0

Тревога:3

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:

Данная работа является добросовестной, взаимствование объясняется использованием общепринятых стандартных словосочетаний.

13.05.2018

Дата

Подпись Научного руководителя

АҢДАТПА

Жұмыс мақсаты әр түрлі объектілерде қауіпсіздік деңгейіне аудит жүргізу сапасын арттыру болып табылады.

Қойылған мақсатқа жету үшін зерттеудің келесі міндеттерін шешу қажет:

1.Қауіп-қатерлерге талдау жасау және ақпараттық тәуекелдерді бағалау.

2.Ақпараттық қауіпсіздік тұрғысынан әлеуетті проблемалық салаларды анықтау.

3.Кәсіпорында ақпараттық қауіпсіздік тәуекелдерін бағалау әдістемесін әзірлеу.

4.Аудит объектілерін салыстырмалы бағалау әдістемесін әзірлеу.

АННОТАЦИЯ

Цель работы заключается в повышении качества проведения аудита уровня безопасности на различных объектах.

Для достижения поставленной цели необходимо решить следующие задачи исследования:

1.Произвести анализ угроз и оценку информационных рисков.

2.Выявить потенциальные проблемные области с точки зрения информационной безопасности.

3.Разработать методику оцениваниярисков информационной безопасности на предприятии.

4.Разработать методику сравнительного оценивания объектов аудита.

ANNOTATION

The purpose of the work is to improve the quality of the audit of the level of security at various sites.

To achieve this goal, it is necessary to solve the following tasks of the study:

1.To make the analysis of threats and assessment of information risks.

2.Identify potential problem areas in terms of information security.

3.To develop a methodology for assessing the risks of information security in the enterprise.

4.To develop a methodology for comparative evaluation of audit objects.

МАЗМҰНЫ

КІРІСПЕ

Ақпараттық тәуекелдерді басқару жөніндегі талаптар көптеген халықаралық және отандық регламенттеуші құжаттарда қамтылған және ақпараттық технологияларды дамытудың қолданыстағы практикасына негізделген. Сондықтан тәуекелдерді басқару проблемаларын және оларды шешу әдістерін зерттеу қазіргі заманғы ақпараттық қоғамда өзекті және сұранысқа ие болып табылады. Қазіргі уақытта тәуекелдерді талдау бойынша жеткілікті тәжірибе мен білім жинақталған. Әрине, ақпараттық қауіпсіздіктің негіздерін оқып-үйрену кезінде осы мәселеге қатысты кейбір жалпы көзқарастар ұсынылуы керек, бірақ қолданыстағы ақпараттық жүйелердің алуандығын ескере отырып, барлық материалдарды меңгеру мүмкін емес. Бұл қосымша зерттеу үшін қажет.

Ақпараттық тәуекелдерді зерделеудің қарастырылып отырған проблемасы қаржылық, банктік және басқа да тәуекелдермен салыстырғанда айтарлықтай жаңа. Бірақ оның маңыздылығы қоғамның ақпараттық технологияларға тәуелділігінің өсуіне қарай артады.

Ақпараттық технологиялармен қолданатын адамдардың барлығында "ақпараттық тәуекел", "АТ-тәуекелі", "операциялық тәуекел", "ақпараттық қауіпсіздік тәуекелі" және т.б. ұғымдар бар.

1 Ақпараттық тәуекелдер: мәні, жіктелуі, тәуекелдерді талдау және басқару әдістері

Қазіргі уақыттың даму барысында үрдістерді автоматтандыру ақпараттық технологияларды қолдану негізінде үрдістерді басқару тәсілдерінің бірі болып табылады. Бағдарламалық және аппараттық ресурстарды пайдалану арқылы біз адамдардың жұмысын жеңілдетеміз және операцияларды, деректерді, ақпарат пен ресурстарды басқаруға мүмкіндік береміз. Автоматтандырудың негізгі мақсаты кәсіпорында бизнес-үрдістерді орындау сапасы мен жылдамдығын арттыру болып табылады. Автоматтандырылған үрдіс қолмен орындалатын үрдіске қарағанда тұрақты сипаттамаларға ие. Көптеген жағдайларда үрдістерді автоматтандыру өнімділікті арттыруға, үрдістің орындалу уақытын қысқартуға, құнын төмендетуге, орындалатын операциялардың нақтылығын және тұрақтылығын арттыруға мүмкіндік береді.

Бірақ автоматтандыру туралы шешім қабылдау кезінде кәсіпорын басшысының алдында өте маңызды мәселе тұрады – кәсіпорынның бизнес-үдерістерінде ақпараттық технологияларды енгізу және пайдалану процесінде туындайтын тәуекелдерді бағалау.

Тәуекелдердің туындауынан болған теріс салдарларды қысқарту үшін тәуекелдерді дұрыс және тиімді басқара білу қажет.

Тәуекелдерді басқару - басқару шешімдерін қабылдау және іске асыру процесі болып табылады, ол қолайсыз нәтиже ықтималдығын азайтуға және оның жүзеге асырылуынан туындаған ықтимал шығындарды барынша азайтуға бағытталған.

Бизнес үдерістерді автоматтандыру және ақпараттық технологияларды пайдалану кезіндегі тәуекелдердің ерекше түрі ақпараттық тәуекелдер болып табылады.

Ақпарат технологиясы— объектінің, процестің немесе құбылыстың күйі туралы жаңа ақпарат алу үшін мәліметтерді жинау, өңдеу, жеткізу тәсілдері мен құралдарының жиынтығын пайдаланатын процесс.

Ақпараттық тәуекел (IT-риск) автоматтандырылған ақпараттық жүйелерді пайдалана отырып, ақпаратты өңдеу, сақтау және беру, сондай-ақ осы жүйелердің жұмысында сәтсіздікке әкеліп соқтыратын жоғалту немесе зақымдау қаупі.

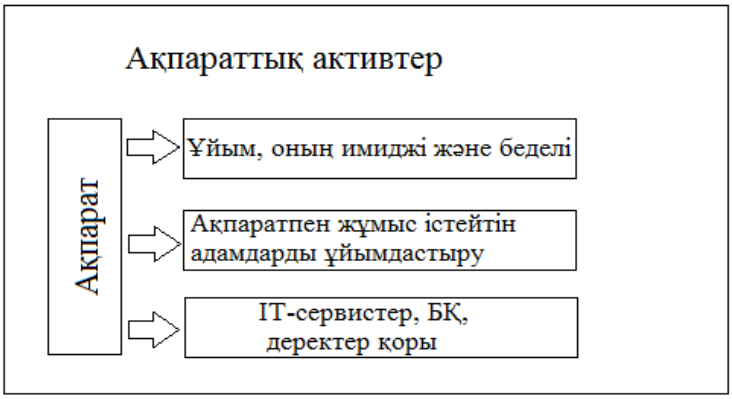
Ақпараттық технологиялық тәуекелдер ақпаратты құру, беру, сақтау және пайдалану арқылы электрондық тасымалдағыштар және басқа байланыс құралдары арқылы жүзеге асырылады.

Автоматтандырылған ақпараттық жүйе деп ақпаратты сақтауға, өңдеуге және беруге байланысты қызметті автоматтандыруға арналған бағдарламалық-аппараттық құралдардың жиынтығы жатады.

1.1 Ақпараттық тәуекелдердің мәні

Ақпараттық тәуекелдің негізгі белгілейтін көзі - бұл ұйым үшін құндылық туралы ақпаратты қамтитын ақпараттық актив. Бұған қағазға

жазылған, пошта арқылы жіберілген немесе бейнеде көрсетілген, ауызша берілген, дерекқор серверлерінде, веб-сайттарда, мобильді құрылғыларда, электронды тасымалдағышта, корпоративтік ақпараттық жүйелерде өңделетін ақпаратта және деректер беру арналары арқылы, сондай-ақ бағдарламалық қамтамасыз ету.



Сурет 1 - Ақпараттық активтердің әсері

Ұйымда ақпараттан басқа да активтін түрлері бар олар материялдық және материалдық емес болады. Ұйым оларды өзінің жұмыс істеуі үшін қолданады. Бұл ұйымның мүлкі, мүліктік және мүліктік емес құқықтар, зияткерлік меншік, кадрлық ресурстар, сондай-ақ ұйымның имиджі мен беделі. Қазіргі халықаралық стандарттар активтердің тағы бір санатын анықтайды – бұлар үдерістер, сондай-ақ ақпараттық және ақпараттық емес сервистер. *Бұл активтердің топтастырылған түрі. Олар қалған активтері мақсатқа жету үшін басқарады*.

Ұйымдағы активтерінің түрлері:

- материалдық;
- қаржылық;
- мүліктік және мүліктік емес құқықтар;
- зияткерлік меншік;
- кадрлық;
- ақпараттық;
- үрдістер мен сервистер;
- имидж және бедел.

Ұйымның көптеген активтерін шартты түрде негізгі және қосалқы активтерге бөлуге болады. Негізгі активтердің айналасында ұйымның негізгі бизнес-үрдістері құрылады, қосалқы активтер екінші роль атқарады. Ақпараттық технологияларды кәсіпорындарға қолданғанда немесе енгізгенде, ақпараттық активтер негізгі болып табылады кәсіпорындағы барлық техникалық, экономикалық, қаржылық құралдар кәсіпорынның ақпараттық қызметтерінің тиімділігіне негізделген. Активтердің барлық

түрлері арасында өзара байланыс бар. Активтердің бір түріне қарсы қатерлік табысты болса онда басқа активтердің қауіпсіздігінің бұзылуына алып келуі мүмкін. Мысалға алатын болсақ қаскүнем біздің серверлік бөлмемізге кіріп өзіне керекті ақпаратты алып өзінің мақсатында қолдануына болады. Болашақта бұл әрекеттер компанияның имиджі мен нарықтағы беделінің төмендеуіне әкелуі мүмкін. Немесе серверіміздің істен шығуы оған сақталған қолданбалардың, қызметтердің және ақпараттың қолжетімділігіне әсер етеді және оны қалпына келтіру үшін материалдық және қаржылық ресурстарды бөлу керек. IT-тәуекелдерді азайту үшін активтерге рұқсат етілмеген қолжетімділіктің, аварилар мен жабдықтардың іркілістерінің алдын алу, жұмыс үшін қажетті сервистер мен қосымшалардың қолжетімділігін қамтамасыз ету болып табылады. IT-тәуекелдерді азайту үшін бұл үрдісті кешенді қарастыру керек: алдымен мүмкін болатын мәселені анықтап, содан кейін оларды қандай тәсілдермен шешуге немесе ескертуге болатынын анықтау қажет.

Ақпараттық тәуекелдерді басқарудың мақсаты ақпараттық тәуекелдерге қарсы әрекетінен кәсіпорын шығысындағы сомасын және осы тәуекелдерден болатын жиынтық залалды азайту болып табылады.

Автоматтандырудағы тәуекелді басқарудағы негізгі қиындық - оны бағалау.

Тәуекелдерді бағалау - тәуекелдердің мөлшерін (дәрежесін) сандық немесе сапалы әдіспен анықтау.

Американдық танымал тәуекелдерді басқару жөніндегі сарапшы Б.Берлимер тәуекелдерді бағалауды талдау кезінде келесі болжамдарды қолдануды ұсынды.

- тәуекелдер бойынша шығындар бір-бірінен тәуелсіз;
- қызметтің бір бағыты бойынша жоғалту ықтималдығы басқа жолмен жоғалту ықтималдығын міндетті түрде арттырмайды (форс-мажорлық жағдайларды қоспағанда);
- тәуекел туындаған кезде теріс әсерінен мүмкін болатын залал ұйымның қаржылық мүмкіндіктерінен аспауы тиіс.

1.2 Ақпараттық тәуекелдерді жіктеу

Қауіп-қатерлердің әртүрлі сыныптамаларының едәуір санына қарамастан ақпараттық қауіпсіздік саласында, зерттелген әдебиетте ақпараттық тәуекелдердің белгіленген жіктемесі жоқ. Олар кәсіпорынның операциялық тәуекелдерінің бірі ретінде қарастырылады.

Әдетте, ақпараттық тәуекелдердің барлық түрлері өзара байланысты және олар кәсіпорын қызметіне әсер етеді. Бұл ретте бір тәуекелдің өзгеруі қалған тәукелдердің өзгеруіне әсер етеді.

Тәуекелдерді жіктеу дегеніміз ол тәуекелдердің белгілері мен критерийлердің біріктіруін білдіреді. Ақпараттық тәуекелдерді жіктеуге негізінде осындай критерийлер болуы мүмкін:

- ақпараттық қауіпсіздіктің негізгі аспектілері;

- пайда болу уақыты;
- пайда болу көзі;
- ақпараттық активтің сипаты;
- ақпараттық қауіпсіздік қатерінің сипаты;
- салдарының сипаты;
- әсер ету механизмі.

Ақпараттық қауіпсіздіктің негізгі аспектілері: ақпараттың қолжетімділігі, тұтастығы және құпиялылығы болып табылады.

Қолжетімділік деп субъектінің жұмыс уақытының кез келген уақыттында сұрау салу бойынша деректерге қол жеткізу мүмкіндігі түсініледі. Деректерді алу мүмкіндігі ақпараттық жүйенің элементтері мен оның деректерін жіберу арналарына байланысты.

Ақпараттың қол жетімділігін бұзу тәуекелі жабдықтың ақаулығына және компаниядағы бағдарламалық қамтамасыз етудегі іркілістерге, сондай-ақ одан тыс ақпараттық жүйеге іске асырылған желілік шабуылдарға байланысты болуы мүмкін.

Бұл тәуекел түрі ақпараттық жүйенің аппараттық және бағдарламалық компоненттерінің жұмыс істеуіне, сондай-ақ олардың жұмысын басқаратын персоналдың құзыреттілік деңгейіне тікелей байланысты. Қол жетімділікті бұзу, жобалау кезеңінде және, жүйені өндіру немесе пайдалану кезеңінде түрлі стандарттардың талаптарын сақтамаудан туындайды. Тұтастық деп ақпараттың өзектілігі мен қарама-қайшы еместігі, оны бұзудан және рұқсатсыз өзгертуден және жоюдан қорғау деңгейі түсініледі. Тұтастықтың бұзылу тәуекелі жабдықтар мен бағдарламалық қамтамасыз етудің бас тарту ықтималдығымен, алгоритмдердің ойлану дәрежесімен және ақпаратты редакциялауға құқығы бар жүйені пайдаланушылардың қол жеткізу құралдарының сенімділігімен, жүйеде құжатталмаған мүмкіндіктердің болуы ықтималдығымен, АЖ ұйымдық құрылымының жетілдірілмеуімен, сондай-ақ жүйені жобалау, өндіру және пайдалану кезеңінде стандарттар талаптарын сақтамаумен қамтамасыз етіледі.

Құпиялық - ақпараттың рұқсатсыз кіруден қорғау деңгейін білдіреді. Құпиялықты бұзу тәуекелі пайдаланушылардың аутентификация алгоритмдерінің деңгейіне және АЖ-мен жұмыс істеу кезінде құжатталмаған жағдайлардың болу ықтималдығына, ұйымдық құрылымның жетілдірілмеуіне, стандарттарды сақтамауына және адам факторына байланысты.

Пайда болу уақыты бойынша ақпараттық тәуекелдер ретроспективті, ағымдағы және перспективалық тәуекелдерге бөлінеді. Ретроспективті тәуекелдерді анализдеу арқылы біз олардың сипаты мен оларды барынша азайту әдістерін талдап ағымдағы және перспективалық тәуекелдерді нақты болжауға мүмкіндік береді.

Пайда болу ортасына байланысты тәуекелдер сыртқы және ішкі болып бөлінеді. Сыртқы тәуекелдерге кәсіпорынның ішкі құрамдас бөлігі әсер

етпейді,олар кәсіпорынның тікелей қызметімен байланысты емес және олардың деңгейіне ешқандай әсер ете алмайды. Олардың деңгейі елдегі және мемлекеттер арасындағы саяси жағдайға, нарықтағы экономикалық жағдайға, азаматтардың әлеуметтік деңгейіне және т. б. байланысты.

Ішкі ақпараттық тәуекелдерге кәсіпорынның және оның персоналының тікелей қызметіне байланысты тәуекелдер жатады Олардың деңгейіне келесі факторлар әсер етуі мүмкін: ұйымның өндірістік әлеуеті, техникалық жабдықталу деңгейі, персоналдың біліктілік деңгейі, ақпаратты қорғау құралдарының болуы, АЖ-мен жұмыс істеу кезінде лауазымдық нұсқаулықтардың болуы.

Ақпараттық активтің табиғаты бойынша ақпараттық тәуекелдерді аппараттық және бағдарламалық тәуекелдерге бөлуге болады. Аппараттық тәуекелдер серверлер, дербес компьютерлер, желілік коммутаторлар және маршрутизаторлар, Өндірістік жабдықтар, станоктар және т. б. сияқты кешендердің істен шығуы кезінде туындайды. Бағдарламалық тәуекелдер кәсіпорынның бағдарламалық қамтамасыз ету жұмысындағы жаңылысымен, зиянды бағдарламалық қамтамасыз етудің, АЖ пайдаланушыларының операциялық жүйелерінің әрекеттерімен, сондай-ақ ақпараттың ағып кетуімен және желілік шабуылдардың әрекеттерімен тікелей байланысты. Ақпараттық қауіпсіздіктің сипатына байланысты жіктеуді қалыптастыра отырып, келесі тәуекелдерді бөліп көрсетуге болады.

Ұйымдастырушылық тәуекелдер-бұл АЖ пайдаланатын және қызмет көрсететін персоналдың қызметіне, ішкі бақылау жүйесінің проблемаларына, жұмыстың нашар әзірленген ережелеріне байланысты тәуекелдер,яғни компания жұмысының ішкі ұйымдастыруға байланысты тәуекелдер.

Техникалық тәуекелдер жабдықпен, бағдарламалық қамтамасыз етумен, олардың міндеттерімен, АЖ жобалау, әзірлеу және пайдалану тәсілдерімен байланысты. Бұл тәуекелдер АЖ өмірлік циклімен тікелей байланысты.

Табиғи ақпараттық тәуекелдерге адамның қызметіне байланысты емес тәуекелдер жатады. Олар кәсіпорын қызметінің толық тоқтауына зиян келтіруі мүмкін. Олар жер сілкінісі, су тасқыны, дауыл, дауыл, және т. б. сияқты табиғи құбылыстардың қызметімен байланысты.

Жоғарыда келтірілген жіктемелерден басқа, тәуекелдерді салдардың сипаты бойынша жіктеуге болады.

Ықтимал тәуекел - бұл ұйымдардың кәсіпорынның қызметінен күтілетін пайда көлемінен аспайтын шығынға ұшырауы және оның қызметі орынды болып қалу қаупі.

Сыни тәуекел-бұл нәтижесінде кәсіпорын қызметінен түсетін болжамды пайдадан асатын шығындар қауіп төндіреді және жобаны іске асыруға салынған барлық қаражаттың жоғалуына алып келуі мүмкін. Кәсіпорынның тәуекелінен туындаған залал тікелей қызметтен түскен пайдадан асып кетсе немесе кәсіпорынның мүліктік жағдайынан асып кетсе, онда мұндай тәуекелдер апатты деп аталады. Оларға сондай-ақ адамдардың өмірі мен денсаулығы үшін қауіпті\немесе экологиялық апаттардың

туындауына байланысты тәуекелдер, сондай-ақ өндірістік кәсіпорынға залал келтіретін тәуекелдер жатады. Ақпараттық тәуекелдердің ең үлкен жіктеліу тобының бірі әсер ету механизмі болып табылады. Осы белгі бойынша ақпараттық тәуекелдерді:

- Мамандардың қателіктері
- Техникалық құралдардың істен шығуы
- Желілік жабдықтың істен шығуы
- Бағдарламалық құралдардың істен шығуы
- Зиянды БҚ
- Тыңшылық бағдарламалар
- Рұқсатсыз қол жеткізу
- Авторлық құқықты бұзушылық
- Жалған ақпарат тарату
- Апаттар

1.3 Тәуекелдерді талдау әдістері

Ф. Найт өзінің "тәуекел, белгісіздік және пайда"еңбегінде белгісіздіктің сандық шамасы ретінде тәуекел туралы алғаш рет айтқан. Ол тәуекелді "өлшенетін белгісіздік", "ықтималдық (стохастикалық) айқындық"деп анықтады. Сонымен қатар ол "белгісіздік" және "тәуекел" ұғымдарының өзара байланысын белгілеп, тәуекелдің ықтимал-математикалық түсіндірмесі белгіленген.

Тәуекелдерді талдаудың бір-бірін толықтыратын өзара екі түрге бөлуге болады: сапалық және сандық.

Тәуекелдерді зерттеуде сапалы тәсілдің ерекшелігі, жоба тәуекелдерін бірінші дәрежелі сәйкестендіру болып табылады,оның негізінде ұйым тап болуы мүмкін барлық ықтимал тәуекелдер анықталады. Сапалы талдаудың келесі кезеңі осындай тәуекелдердің туындауынан болған зардаптарды қаражаттық бағалау және олармен күресу әдістері болып табылады. Сапалы талдау жүргізу кәсіпорын қызметін жоспарлау сатысында жүргізілуі тиіс. Ықтималдық теориясының және математикалық статистиканың механизмдері мен әдістеріне негізделген сандық талдау сандық өлшемде жобаның тиімділігін өзгертуге жобаның тәуекел факторларының әсер ету деңгейін анықтайды. Ол жүргізілген сапалы талдау нәтижелеріне және жобаның бизнес-жоспарына негізделеді .

Сапалы талдаудың негізгі міндеті барлық ықтимал тәуекелдерді сәйкестендіру болып табылады. Оны орындау кезінде осы тәуекелдің пайда болу факторлары және пайда болу салалары анықталады. Осы тәуекелдерден келген шығынның шамасы, олардың пайда болу көздері және осы тәуекелдерден кәсіпорын шығынының ықтимал шамасы сандық талдаудың көмегімен анықталады.

Қазірге уақытта кен тараған тәуекелді талдаудың келесі түрлері бар :

- статистикалық;
- сараптамалық бағалау;
- талдау;

- қаржылық тұрақтылық пен төлем қабілеттілігін бағалау;
- шығындардың орынды болуын бағалау;
- тәуекелді жинақтау салдарын талдау;
- аналогтарды пайдалану әдісі;
- аралас әдіс.

Статистикалық әдіс оқиғаның ықтималдығын анықтайды және тәуекел шамасын белгілеу мақсатында кәсіпорында орын алған шығындар мен пайда статистикасын зерделеуден тұрады. Ықтималдылық белгілі бір нәтижені алу мүмкіндігін білдіреді.

Бұл әдістің басты ерекшелігі бір тәсіл шеңберінде әртүрлі тәуекел факторларын бағалау және жобаны іске асырудың әртүрлі сценарийлерін талдау мүмкіндігі болып табылады.

Бұл әдістің басты кемшілігі ықтималдық сипаттамаларды пайдалану болып табылады, бұл оны практикалық қолдануда пайдалануды қиындатады.

Сараптамалық бағалау әдісі. Сараптамалық бағалау-бұл арнайы әдістеме бойынша анықталған белгілі бір мәселе бойынша сарапшылардың пікірі. Бұл әдістің басты ерекшелігі тәуекел қисығын құру үшін ақпаратты жинау әдісі. Тәуекелдердің туындауынан болатын шығындардың туындау мүмкіндігін бағалайтын әр түрлі мамандар мен сарапшыларды бағалау – бұл талдауға арналған ақпараттың негізгі көзі. Бұл әдісті қолдану күрделілігі бағалау көрсеткіштерінің саны ұлғайған кезде өседі.

Сараптамалық бағалау әдісі отандық және шетелдік тәжірибеде үнемі қолданылады. Жобаны дамытудың әртүрлі кезеңдерінде әртүрлі көрсеткіштерді анықтау үшін сараптамалық қорытындылардың рөлі өте үлкен,себебі есептеу үшін пайдаланылатын көрсеткіштер өзгеріссіз болып табылмайды.

Сараптамалық бағалау нәтижесі белгілі бір тақырып бойынша арнайы зерттеулер жүргізілгеннен кейін де, осы саладағы жетекші мамандардың жинақталған тәжірибесін пайдаланған кезде де алынуы мүмкін.

Жобаны жүзеге асыру кезінде тәуекелдің өсуі оны іске асырудың қиын сәттерін мұқият бағалауды талап етеді. Өзара жиі бәсекелес көптеген бастапқы көрсеткіштері жоба сапасының критерийін құрастыру үшін сараптамалық бағалауды пайдалануды көздейді. Сондықтан қазіргі жағдайда инвестицияларды бағалау жүйесі қажеттігіне байланысты "адам-алгоритмдік" болып табылады, әрі сарапшы-адамның рөлі айқындаушы болып табылады.

Қадамдық тәуекелді бағалау әрбір жоба кезеңінде жеке тәуекелдер анықталатынына негізделеді, содан кейін бүкіл жобаның жалпы нәтижесі анықталады. Әдетте әрбір жоба кезеңінде ерекшеленеді:

- дайындық (жобаны іске асыруды бастау үшін қажетті барлық жұмыстар кешенін орындау);
- құрылыс (қажетті ғимараттар мен құрылыстарды салу, жабдықтарды сатып алу және монтаждау);
- жұмыс істеуі (жобаны толық қуатқа шығару және пайда табу).

Барлық есептер екі рет орындалады – жоба жасалған сәтте және оның аса қауіпті элементтері анықталғаннан кейін.

Инвестициялық жобаның сипаты жеке тәртіппен жасалатын нәрсе ретінде тәуекелдердің мәнін бағалау үшін жалғыз мүмкіндік – сарапшылардың пікірлерін пайдалану.

Жұмыс істейтін әрбір сарапшыға жобаның барлық кезеңдері бойынша бастапқы тәуекелдер тізбесі ұсынылады және келесі бағалау жүйесіне сәйкес тәуекелдердің басталу ықтималдығын бағалау ұсынылады:

0-25-тәуекел маңызды емес ретінде қарастырылады;

25-50-тәуекелді іске асырудың аз ықтималдығы;

50-75-осы оқиғаның басталуы туралы ештеңе айтуға болмайды;

75-99-тәуекелді іске асырудың жоғары ықтималдығы;

100-тәуекел іске асырылады

Сарапшылардың бағалауы алынған деректердің қарама-қайшы еместігіне талдау жасалады, ол белгілі бір ережелер бойынша орындалады. Кез келген фактор бойынша екі сарапшының бағалаулары арасындағы ең жоғары жол берілетін айырмашылық 50-ден аспауы тиіс. Қорытындылардың нәтижелерін салыстыру модуль бойынша жүргізіледі (қосу немесе алу белгісі есепке алынбайды), бұл сарапшылардың жеке тәуекелдің басталу ықтималдығы бағаларындағы жол берілмейтін айырмашылықтарды жоюға мүмкіндік береді. Егер сарапшылар саны үштен көп болса, онда салыстыруға тең пікірлер ұшырайды.

Сараптамалық талдаудың жалпы әдісі Дельфи әдісі болып табылады. Оның ерекшелігі-басқарылатын кері байланыс. Комиссия мүшелері қойылған мәселелерді топтық талқылаудың мүмкін еместігін қамтамасыз етеді. Нәтижесі өңделгеннен кейін қорытылған нәтиже комиссияның әрбір мүшесіне хабарланады. Мұндай әрекеттің негізгі мақсаты-басқа комиссия мүшелерінің бағаларымен танысуға мүмкіндік беру. Осыдан кейін бағалау қайталануы мүмкін.

Бұл әдісті қолданудағы басты міндет құзыретті сарапшыларды іріктеу болып табылады, өйткені олардың пікірлеріне байланысты жобаны басқару шешімін таңдайды

Қауіпті зерттеудің тағы бір маңызды әдісі - "шешім ағашы" бұл шешім көмегімен таңдау міндетін модельдеу. Бұл әдіс қабылдануы мүмкін шешімдердің нұсқаларын графикалық құруды көздейді. "Ағаштың" тармақтары бойынша ықтимал оқиғалардың субъективті және объективті бағаларына сәйкес келтіреді Салынған тармақтардың жолымен жүре отырып және ықтималдылықты есептеудің арнайы әдістерін пайдалана отырып, әрбір жолды бағалайды және одан кейін тәуекелділігі төменін таңдайды. Алайда, бұл әдіс өте қиын. Сонымен қатар," ағашта " кәсіпкер жасауға ниет білдірген іс-әрекеттер ғана және оның көзқарасы бойынша орын алуы мүмкін нәтижелер ғана ескеріледі. Бұл ретте сыртқы ортаның кәсіпкерлік фирманың қызметіне әсері мүлдем ескерілмейді, ал кәсіпкер әрқашан серіктестердің, бәсекелестердің іс-әрекеттерін болжай алмайды.

Аналитикалық әдіс. Қисық тәуекел құру аналитикалық тәсілі ең күрделі, өйткені оның негізінде жатқан ойын теориясының элементтері тек кейбір мамандарға қол жетімді. Аналитикалық әдістің кіші түрі жиі қолданылады-модельдің сезімталдығын талдау. Ол мынадай қадамдардан тұрады: сезімталдықты бағалау жүргізілетін негізгі көрсеткішті таңдау (кірістіліктің ішкі нормасы, таза келтірілген кіріс және т.б.); факторларды таңдау (инфляция деңгейі, экономиканың жай-күйі және т. б.); жобаны жүзеге асырудың әртүрлі кезеңдерінде (шикізатты сатып алу, өндіру, өткізу, тасымалдау, күрделі құрылыс және т. б.) негізгі көрсеткіштің мәндерін есептеу. Осылайша қалыптастырылған қаржы ресурстарының шығындары мен түсімдерінің реттілігі әрбір сәтке (немесе уақыт бөлігі) үшін ақша қаражаты қорларының ағындарын анықтауға, яғни тиімділік көрсеткіштерін анықтауға мүмкіндік береді. Таңдалған нәтижелік көрсеткіштердің бастапқы параметрлердің шамасына тәуелділігін көрсететін диаграммалар жасалады. Алынған диаграммаларды өзара салыстыра отырып, жобаның кірістілігін бағалауға барынша әсер ететін негізгі көрсеткіштерді анықтауға болады.

Морфологиялық талдау әдісімен зерттелетін мәселе бойынша ақпараттың көлемі аз болған кезде пайдаланылады.

Бұл әдіс жоғары дәрежелі тәуекелдерді зерттеуде қолданылады. Мұндай тәуекелдер тұтынушылардың жаңа қажеттіліктерін және жаңа өткізу нарықтарын қалыптастыру кезінде туындайды.

Бұл тәсіл зерттеленетін мәселенің ықтимал шешімдері бойынша жүйелендірілген деректерді алуға мүмкіндік береді. Ол келесі зерттеулер үшін деректерді жинақтауға, нысандарды, құбылыстар мен тұжырымдамаларды өзара байланыстыруға мүмкіндік береді. Морфологиялық тәсілдің принципті айырмашылығы объект туралы толық білім жиынтығын пайдалану болып табылады. Талдау барысында барлық процестер мен объектілер мұқият талдауға жататын топтарға бөлінеді.

Төменде морфологиялық талдау кезеңдері:

- Тәуекел-проблеманы нақты тұжырымдау;

- Осы тәуекел проблемасын шешу тұрғысынан маңызды барлық параметрлерді мұқият талдау.

- Барлық шешімдерді әлеуетті қамтитын" морфологиялық жәшікті " құру. Мұндай "жәшік" көп өлшемді кеңістік болып табылады. Егер мәселе шешілсе, онда мұндай "жәшіктің" әрбір бөлімшесі тек бір ғана мүмкін шешімді қамтитын болады немесе ол мүлде болмайды (бір бөлімшеде екі және одан да көп шешім пайда болуы барлық параметрлер есепке алынбағанын немесе жүйеге енгізілмегенін көрсетеді, сондықтан жіберілген параметрлерді іздеу жүргізіледі);

- "Морфологиялық жәшік "" ағаш " немесе матрица түрінде құрылады, оның торларында тиісті параметрлер орналастырылған.

2 Көрсеткіштер жүйесін және бағалау өлшемдерін ескере отырып, аудит объектілерін салыстырмалы бағалау әдістемесі

2.1 Әдістің мақсаты мен мақсаты

Аудит объектілерін салыстырмалы бағалау әдістемесі (АОСБ) ақпараттық қауіпсіздікті қамтамасыз ету саласында әртүрлі кәсіпорындардың ақпараттық жүйелерінің рейтингтік бағалауын қалыптастыруға арналған.

Осы Әдістеменің мақсаты АҚ-ның неғұрлым проблемалық салаларын талдау және анықтау үшін АҚ-ның сәйкестік дәрежесі тұрғысынан тексерілген объектілерді саралау, сондай-ақ ақпараттық қауіпсіздікті қамтамасыз ету жүйелерін құру және дамыту жөніндегі ұсыныстарды негіздеу болып табылады.

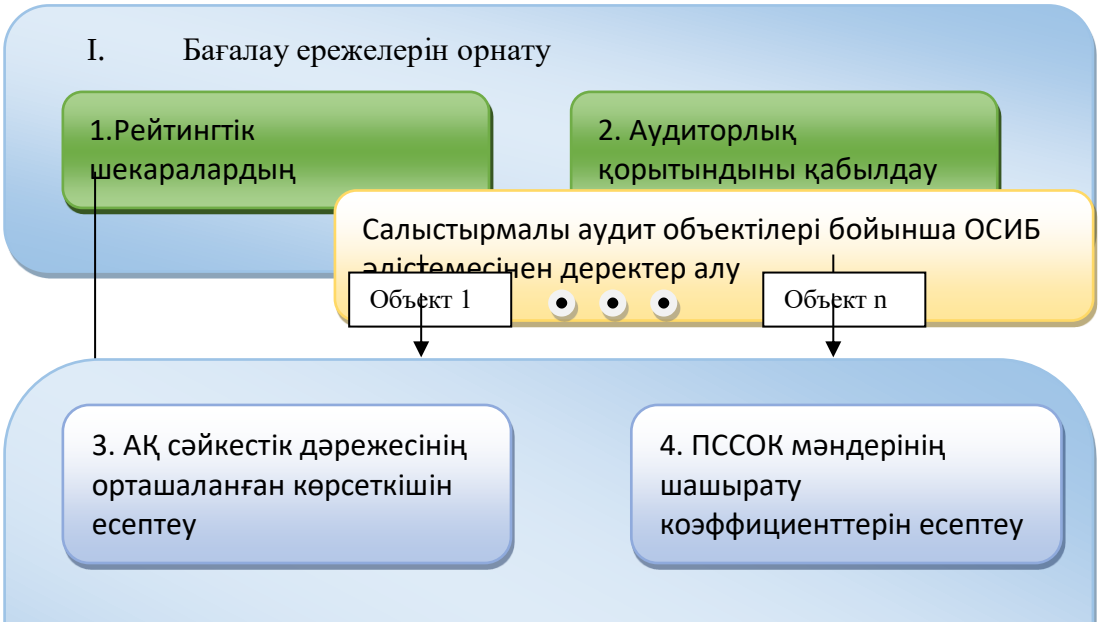
Рейтингтік баға кәсіпорынның жетілу деңгейінің моделіне сәйкес бес балдық шкала бойынша қойылады.

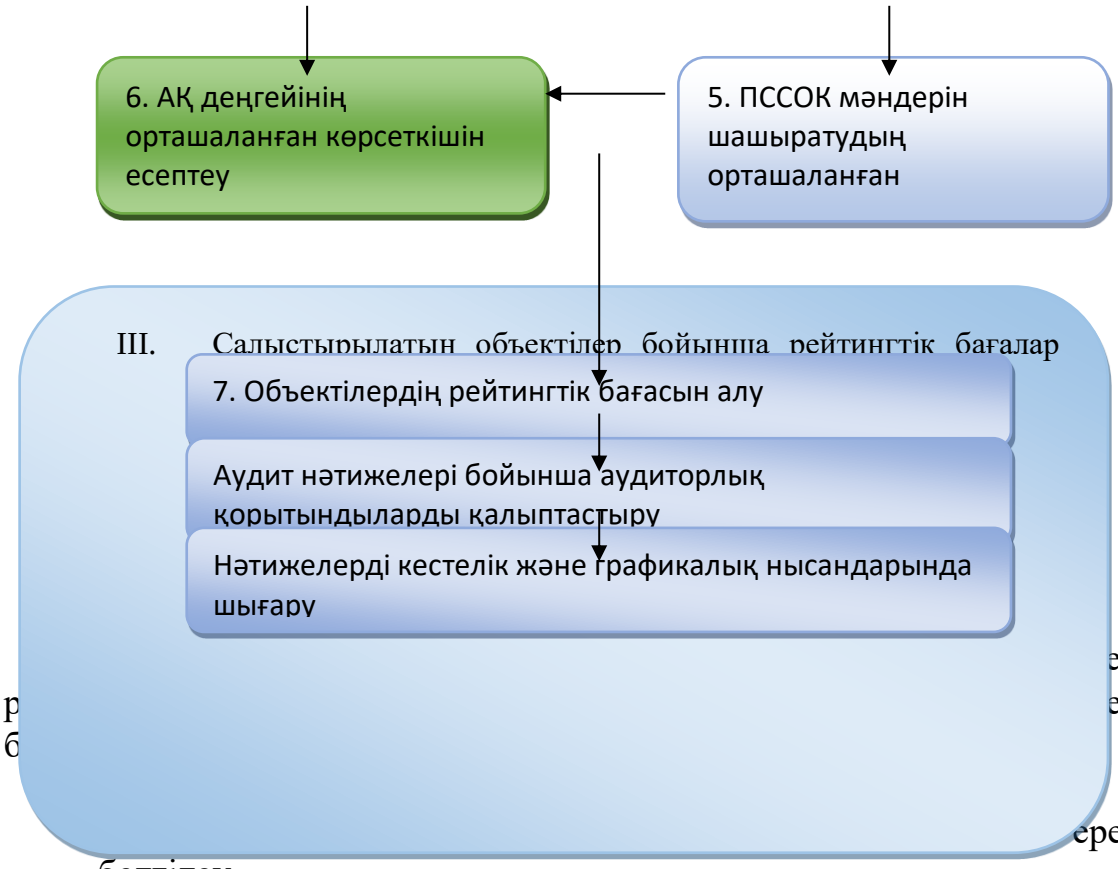
АОСБ әдістемесі ОИСБ әдістемесімен жиынтықта кәсіпорындардың КАЖ ақпараттық қауіпсіздігінің жай-күйін бағалау кезінде бірыңғай тәсілді қолдануға мүмкіндік береді.

2.2 Әдістемесі кезеңдерінің қысқаша сипаттамасы

Аудит объектілерін салыстырмалы бағалау әдістемесі үш негізгі кезеңнен тұрады, әр кезең блоктардан тұрады (2-суретті қараңыз). I және II кезеңдер– маңызды, олардың орындалуын ақпараттық қауіпсіздік саласындағы сарапшылар жүзеге асырады.

АОСБ әдістемесі келесі негізгі кезеңдерден тұрады (2 суретті қараңыз).





ектілерді
р ең келесі
б

ережелерін белгілеу.

II кезең-есептеулерді жүргізу:

3 Блок- КАЖ АҚ сәйкестік дәрежесінің орташаланған көрсеткішін есептеу;

4 Блок- бақылау салалары бойынша АҚ сәйкестік дәрежесінің жалпыланған көрсеткіштерінің мәндерінің таралу коэффициенттерін есептеу;

5 Блок- орташаланған шашырату коэффициентін есептеу;

6 Блок- кәсіпорынның КАЖ АҚ деңгейінің жалпыланған көрсеткішін есептеу.

III кезең-салыстырмалы объектілер бойынша рейтингтік бағалар мен аудиторлық қорытындыларды қалыптастыру

7 Блок- кәсіпорындардың КАЖ АҚ деңгейі рейтингтік бағалауын қалыптастыру;

8 Блок- аудит нәтижелері бойынша аудиторлық қорытындыларды қалыптастыру;

9 Блок- нәтижелерді кестелік және графикалық формада шығару.

2.3 Бағалау ережелерін баптау кезеңі

Жоғарыда атап өтілгендей, АСОБ әдістемесінің мақсаты КАЖ АҚ қамтамасыз ету саласындағы кәсіпорынның рейтингтік бағасын анықтау болып табылады. Ол үшін бастапқыда бағалау ережелерін анықтау керек, яғни рейтингтік бағалау объектілерінің АҚ деңгейінің алынатын жалпылама

көрсеткіштерінің сәйкестік шкаласын анықтау керек. Бұдан басқа, кәсіпорындардың қалыптасқан рейтингтік бағалары негізінде аудиторлық шешім қабылдау принциптерін айқындау қажет.

Рейтингтік бағалар шекарасын анықтау кезінде АСОБ әдістемесімен келісу мүмкіндігі ескерілген. 1 кестеде рейтингтік бағалар шекарасын белгілеудің ұсынылған нұсқасы келтірілген.

Аудит объектілеріне объективті салыстырмалы бағалау алу үшін рейтингтік шкала тұрақты болуы тиіс. Ол өзгерген кезде (қандай да бір себептермен) аудит объектілерінің алынған рейтингтік бағалары өзгеруі мүмкін.

Ақпараттық қауіпсіздіктің қорытынды көрсеткіші (IPU)	Рейтингтік бағалау
< 0,4	1
0,4 – 0,6	2
0,6 – 0,8	3
0,8 – 0,95	4
0,95 – 1	5

1-кесте Рейтингтік бағалау шекаралары

Рейтингтік бағаларға сәйкес аудиторлық қорытындыны қабылдаудың мынадай ережелері белгіленеді

Рейтинговая оценка	Аудиторское заключение
1	Не соответствует требованиям
2	Условно соответствует
3	В основном соответствует
4	Соответствует требованиям
5	Полностью соответствует

2-кесте Аудиторлық қорытындыны қабылдау ережесі

2.4 Есептеу кезеңі

АСОБ әдістемесі үшін кіріс параметрлері (деректер) ретінде ОИСБ әдістемесін қолданғаннан кейін алынған нәтижелер болып табылады. Ақпараттық қауіпсіздіктің нормативтік құжаттардың талаптарына сәйкестігін бағалау әдістемесі негізінде бақылау саласы бойынша АҚ-ның (ОРОК) сәйкестік дәрежесінің 10 жалпыланған көрсеткішінен жиын аламыз.

Бақылау салалары бойынша жинақталған көрсеткіштер	ОРОК1	ОРОК2	ОРОК3	ОРОК4	ОРОК5	ОРОК6	ОРОК7	ОРОК8	ОРОК9	ОРОК10
Мәні	0,564	0,647	0,462	0,517	0,789	0,556	0,640	0,616	0,610	0,915

3- кесте ОИСБ әдістемесінен алынатын деректер

Жеке кәсіпорынның (ОРОКср) ИБ сәйкестігінің орташаланған көрсеткішін алу үшін №1 формуланы қолданамыз

$$OPOK_{ср} = \sum_{i=1}^{n} OPOK_i \Big/ n$$

мұндағы ОРОКі-бақылаудың і саласы бойынша жалпыланған көрсеткіштің мәні;

n – бақылау салалары бойынша жинақталған көрсеткіштердің саны.

Біздің жағдайда бақылаудың 10 саласы үшін және 4-кестедегі деректерге сәйкес иеміз:

$$OPOK_{ср} = \sum_{i=1}^{10} OPOK_i \Big/ 10 = 0.632$$

Ақпараттық қауіпсіздікті қамтамасыз ету жүйесінің теңгерімділігі маңызды рөлге ие, оны бақылау салалары бойынша жалпыланған көрсеткіштер мәндерінің біркелкілігі бойынша бағалауға болады. Осы аспектіні ескеретін көрсеткіш ретінде АСОБ әдістемесінде KR мәндерінің шашыраңқы коэффициенті қолданылады. Бақылау салалары бойынша АҚ-ның сәйкестік дәрежесінің жалпыланған көрсеткіштерінің мәндерінің шашыраңқы коэффициенттерін жалпыланған көрсеткіштерді тепе-тең салыстыру нәтижесінде аламыз (ОРОК) 3 формула бойынша (блок 4).

$$KR = \sum_{\substack{j=1 \\ j \neq i}}^{n} \left| \frac{(OPOK_i - OPOK_j)}{(OPOK_i + OPOK_j)} \right| \Big/ (n-1).$$

Осылайша, бақылау саласының n үшін $\frac{n(n-1)}{2}$ шашыраңқы мәндер коэффициенттері бар (N =10 үшін 45 KR бар). 4-кестедегі деректермен KR есебінің мысалы 5-кестеде көрсетілген.

		$OPOK_1$	$OPOK_2$	$OPOK_3$	$OPOK_4$	$OPOK_5$	$OPOK_6$	$OPOK_7$	$OPOK_8$	$OPOK_9$	$OPOK_{10}$
		0,564	**0,647**	**0,462**	**0,517**	**0,789**	**0,556**	**0,640**	**0,616**	**0,610**	**0,915**
$OPOK_1$	**0,564**		*0,068*	*0,099*	*0,044*	*0,166*	*0,007*	*0,062*	*0,044*	*0,039*	*0,237*
$OPOK_2$	**0,647**	*0,068*		*0,166*	*0,112*	*0,099*	*0,075*	*0,006*	*0,025*	*0,029*	*0,172*
$OPOK_3$	**0,462**	*0,099*	*0,166*		*0,055*	*0,261*	*0,092*	*0,161*	*0,142*	*0,137*	*0,328*
$OPOK_4$	**0,517**	*0,044*	*0,112*	*0,055*		*0,209*	*0,037*	*0,106*	*0,088*	*0,083*	*0,278*
$OPOK_5$	**0,789**	*0,166*	*0,099*	*0,261*	*0,209*		*0,173*	*0,105*	*0,123*	*0,128*	*0,074*
$OPOK_6$	**0,556**	*0,007*	*0,075*	*0,092*	*0,037*	*0,173*		*0,070*	*0,051*	*0,046*	*0,244*
$OPOK_7$	**0,640**	*0,062*	*0,006*	*0,161*	*0,106*	*0,105*	*0,070*		*0,019*	*0,024*	*0,177*
$OPOK_8$	**0,616**	*0,044*	*0,025*	*0,142*	*0,088*	*0,123*	*0,051*	*0,019*		*0,005*	*0,195*
$OPOK_9$	**0,610**	*0,039*	*0,029*	*0,137*	*0,083*	*0,128*	*0,046*	*0,024*	*0,005*		*0,200*
$OPOK_{10}$	**0,915**	*0,237*	*0,172*	*0,328*	*0,278*	*0,074*	*0,244*	*0,177*	*0,195*	*0,200*	

4-кесте ОРОК мәндерінің таралу коэффициенттерін есептеу үлгісі

Шашыраудың орташаланған коэффициенті шашырату коэффициенттерінің математикалық күтуін табу нәтижесінде аламыз (5 – блок) - 4 формуласы.

$$KR_{cp} = \sum_{i-1}^{n} K\,R_i/n$$

4 кесте үшін шашыраудың орташаланған коэффициенті K R ср=0,112 тең .

Шашыраудың орташаланған коэффициенті бақылау салалары бойынша АҚ-ның сәйкестік дәрежесінің жинақталған көрсеткіштерінің теңгерілмеу дәрежесін көрсетеді. Жалпы OPOKі көрсеткіштерінің мәндерінің таралуын азайту кезінде шашырату коэффициенті 0 – ге ұмтылады, көбейген кезде-1-ге ұмтылады.

Кәсіпорынның АҚ КАЖ (IPU) деңгейінің қорытынды көрсеткішін шашыраудың орташаланған коэффициентін (KRср) және АҚ КАЖ (OPOKср) сәйкестік дәрежесінің орташаланған көрсеткішін 5 (блок 6) формула бойынша есепке алу нәтижесінде алады.

$$IPU = OPOK_{cp}(1 - KR_{cp})$$

Осылайша, келтірілген мысал үшін АҚ деңгейінің қорытынды көрсеткіші төмендегіндей болады

$$IPU = OPOK_{cp}\left(1 - KR_{cp}\right) = 0.632 \times (1 - 0.112) = 0.560$$

2.5 Салыстырмалы объектілер бойынша рейтингтік бағалар мен аудиторлық қорытындыларды қалыптастыру кезеңі

Соңғы кезең аудит объектісіне рейтингтік баға беруге және аудиторлық қорытындыны қалыптастыруға арналған. 1-кестеге сәйкес аудит объектілеріне алынған АҚ (IPU) қорытынды көрсеткішіне байланысты рейтингтік бағалар беріледі және олардың салыстырмалы талдауы жүргізіледі (7-блок).

Рейтинг бағасын беру кестесі 4 кестеде көрсетілген. Объектілерді саралау рейтингтік бағалау бойынша да, АҚ (IPU) деңгейінің қорытынды көрсеткіші бойынша да жүзеге асырылуы мүмкін.

тексерілетін объектінің № (атауы)	Ақпараттық қауіпсіздіктің қорытынды көрсеткіші (IPU)	Рейтингтік бағасы
Кәсіпорын 1	0,621	3
Кәсіпорын 2	0,560	2
Кәсіпорын 3	0,439	1
Кәсіпорын 4	0,342	1
…		

5-кесте АҚ аудит объектілеріне рейтингтік бағалар беру

Бұдан әрі 2-кестеге сәйкес аудит нәтижелері бойынша аудиторлық қорытынды (8 блок) қабылданады.

Тексері летін объектң № (атауы)	Ақпараттық қауіпсіздіктің қорытынды көрсеткіші (IPU)	Рейтингтік бағасы	Аудиторлық қорытынды
Кәсіпорын 1	0,621	3	Негізінен
Кәсіпорын 2	0,560	2	Шартты түрде
Кәсіпорын 3	0,439	1	Келмейді
Кәсіпорын 4	0,342	1	Келмейді
…			

6-кесте Тексерілетін объектілердегі АҚ-ның жай-күйі туралы аудиторлық қорытындыны қалыптастыру

Әр түрлі нысандарды шығаруды қарастыру қажет (блок 8):

- рейтинг бойынша жалпы тізім (IPU) - объектілерді жалпы саралау;
- рейтингтік бағалау бойынша (аудиторлық қорытынды); екі және одан да көп объектілерді және т. б. салыстыру.

ҚОРЫТЫНДЫ

Ақпараттық тәуекелдерді тиімді басқару үшін халықаралық және ұлттық стандарттардың көп саны әзірленді, олардың арасында ең танымал ISO/IEC 27000 және ISO 17799 (BS7799) сериялы стандарттар алынды.

Тәуекелдерді бағалау саласында ақпараттық қауіпсіздікті қамтамасыз ету кезінде екі әдістеме бар: сапалық және сандық. Біріншісі қандай да бір стандартқа немесе саясатқа сәйкес тәуекелдерді анықтау үшін қызмет етеді. Екіншісі-кәсіпорындардың АЖ мұқият қарауы, жеке элемент үшін де, тұтастай жүйе үшін де тәуекелді төмендету үшін пайдаланады. Бұл жұмыста аудит объектілерінің ақпараттық қауіпсіздігінің нормативтік құжаттардың талаптарына сәйкестігі үлгісінде кәсіпорында ақпараттық қауіпсіздік тәуекелдерін бағалаудың сапалы әдістемесі әзірленді, сондай-ақ аудит объектілерін салыстырмалы бағалау әдістемесі әзірленді. АСОБ әдістемесі ОСИБ әдістемесімен жиынтықта кәсіпорындардың корпоративтік ақпараттық жүйесінің ақпараттық қауіпсіздігінің жай-күйін бағалау кезінде бірыңғай тәсілді қолдануға мүмкіндік береді.

Бұл жұмыста сондай-ақ бағдарламалық кешен әзірленді, онда анықтамалық жүйе түрінде АТ басқарудың сапалы әдістемесі іске асырылды, өйткені бұл кәсіпорынның ақпараттық қауіпсіздігін өзекті жағдайда ұстап тұру үшін ажырамас құрамдас бөлік болып табылады. ISO 17799 стандарты негізге алынды.

Тәуекелдерді сараптамалық бағалаудың бағдарламалық кешені тәуекелдерді бағалау кезінде сапалы тәсілді көрсетеді және кез келген кәсіпорынның ақпараттық қауіпсіздігінің ажырамас бөлігі болып табылады. Осы бағдарламалық кешеннің Шығыс ақпараты АҚ-ның жоғары деңгейін құру және одан әрі өзекті күйде ұстап тұру туралы барлық қажетті ақпарат көрсетілетін есеп болып табылады.

Тәуекелдерді жүйелі түрде қайта бағалау кәсіпорынның АЖ қауіпсіздігі туралы деректерді өзекті жағдайда ұстап тұруға, жаңа қауіпті тәуекелдерді тез арада анықтауға және оларды экономикалық қолайлы тәсілмен бейтараптандыруға мүмкіндік береді.

Практикалық маңыздылығы- ұсынылған әдіс нақты кәсіпорынның немесе ұйымның осалдықтарын пайдалану нәтижесінде сыни қасиеттердің бұзылу ықтималдығын анықтауға мүмкіндік береді.

ҚОЛДАНҒАН ӘДИБЕТТЕР

1 Cnews аналитика http://www.cnews.ru/ [Электронды мәлімет көзі]
2 Искусство управления http://анализ-риска.рф [Электронды мәлімет көзі]
3 Искусство управления информационной безопасностью http://iso27000.ru/ [Электронды мәлімет көзі]
4 Мескон М., Альберт М., Хедоури Ф. Основы менеджмента

5 Найт Ф. Понятие риска и неопределенности // Thesis: теория и история экономических и социальных институтов и систем. 1994. № 5.
6 Луман Н. Понятие риска // Thesis: теория и история экономических и социальных институтов и систем. 1994. № 5.
7 Долматов А.С. Математические методы риск-менеджмента: учеб. пособие. – М.: Экзамен, 2007. – 319 с.
8 Менеджмент качества http://www.kpms.ru/Automatization [Электронды мәлімет көзі]
9 Управление рисками на предприятии. http://www.risk24.ru/ [Электронды мәлімет көзі]
10 Исаев Г.Н. Информационные технологии: учебное пособие М: Омега-Л, 2012, 464 с.
11 Активы организации как ключевые факторы риска http://анализриска.рф [Электронды мәлімет көзі]
12 Берлимер Б. Риски в современном бизнесе. – М.: Аланс, 1994. – 200 с.
13 Мазов Н.А., Ревнивых А.В., Федотов А.М. Классификация рисков информационной безопасности: Вестник НГУ. Серия: Информационные технологии, 2011. Том 9, выпуск 2, С.80-89.
14 Виды и классификация рисков. http://www.risk24.ru/ [Электронды мәлімет көзі] 97
15 Классификация и проблемы оценки рисков промышленного предприятия Интернет-журнал «Науковедение» ISSN 2223-5167. http://naukovedenie.ru/ [Электронды мәлімет көзі]

Қосымша А

Ақпараттық жүйелердің ақпараттық қауіпсіздік деңгейін бағалау және салыстырмалы талдау бағдарламалық кешенін әзірлеу

Бағдарламалық кешеннің құрамын, құрылымын және функцияларын негіздеу

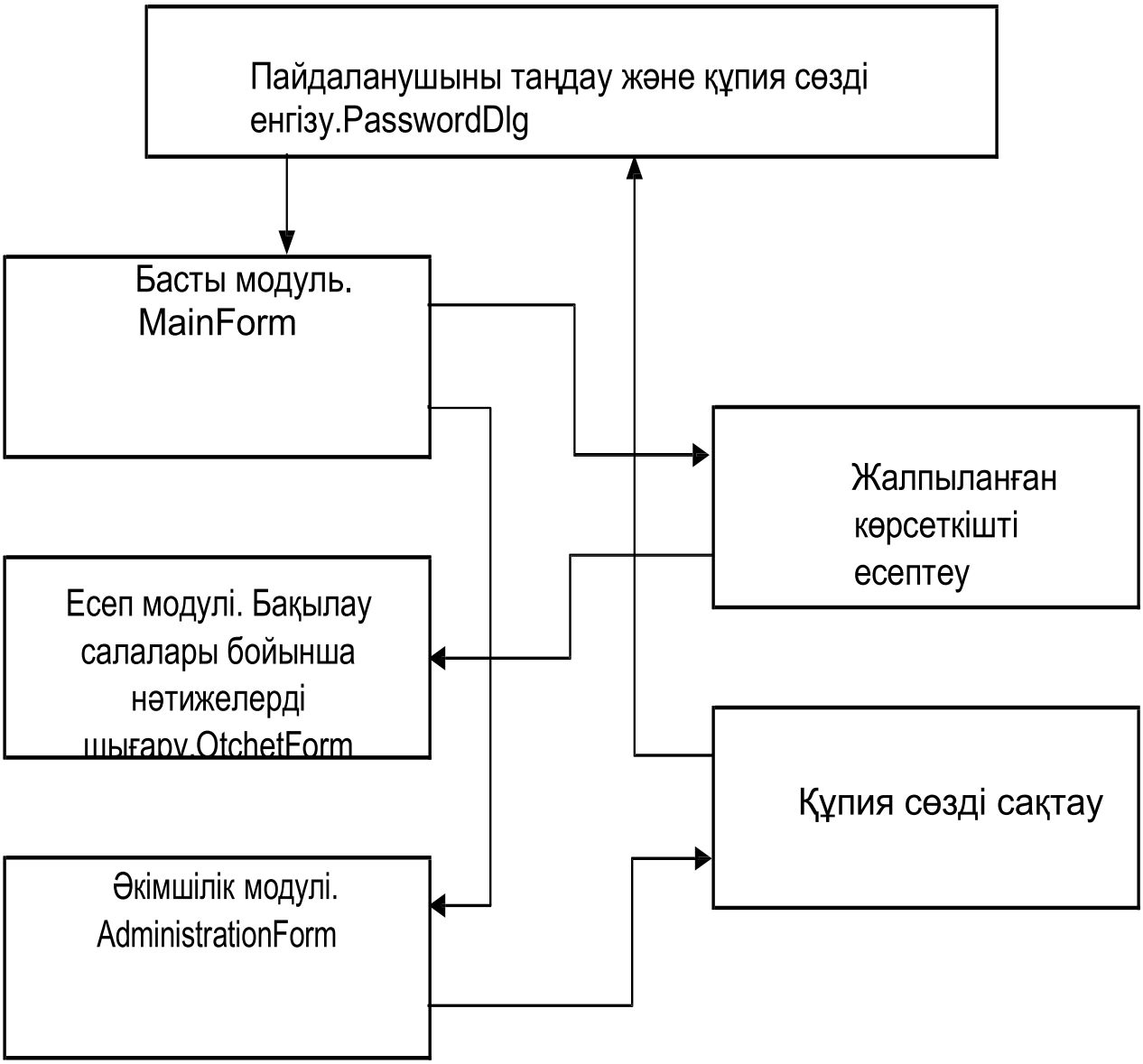
Бағдарламалық кешен – бұл соңғы (талап етілетін) нәтижеге қол жеткізу бойынша бір процесс шеңберінде деректерді өңдеудің әртүрлі кезеңдері мен блоктарын іске асыратын бағдарламалар мен алгоритмдер жиынтығы. Жеке жағдайда бағдарламалық кешен бір орындалатын файлдан тұрады, оған деректерді өңдеудің әртүрлі кезеңдері құрылымы енгізілген, сондай-ақ өңдеу параметрлерін және аралық нәтижелерді сақтауға арналған қосалқы файлдардан тұрады.

Жалпы жағдайда бағдарламалық кешен бірнеше орындалатын файлдарды білдіреді, әдетте, олардың біреуі басқа орындалатын файлды немесе бір орындалатын файлды және динамикалық қосылатын кітапханалар түрінде іске асырылған бірнеше файлдарды орындайды (іске қосады), олар

өзінің құрылымы бойынша орындалатын файлға ұқсас, бірақ шақыру кезінде өз процесін жасамайды, ал орындалатын файлмен жасалған процестің адрестік кеңістігіне жүктеледі.

Белгілі бір іске асырудың болуы бағдарламашының тапсырмасы негізінде анықталады. Сонымен бірге бір немесе бірнеше блоктың болуы әр кезеңде шешілген алгоритм мен міндеттер топтарын іске асыру арқылы анықталады. Қарастырылып отырған міндет шеңберінде бағдарлама кешені келесі блоктан (модульден) тұрады:

- пайдаланушы таңдау және пароль енгізу модулі-бағдарламалық кешенмен жұмыс істейтін пайдаланушы таңдайды;
- негізгі модуль - Бұл модульде пайдаланушыға бақылау саласын таңдау мүмкіндігін ұсыну қарастырылған, бөлім және сәйкестік дәрежесін көрсету; Бағдарламалық кешеннің басқа модульдеріне өту мүмкіндігі ұсынылған;
- қорытынды нәтижелері бар есеп модулі;
- пайдаланушы аты мен құпия сөзді орнатуға болатын басқару модулі.



1 сурет-бағдарламалық кешеннің құрамы

Бағдарламалық кешен жұмысының алгоритмін әзірлеу

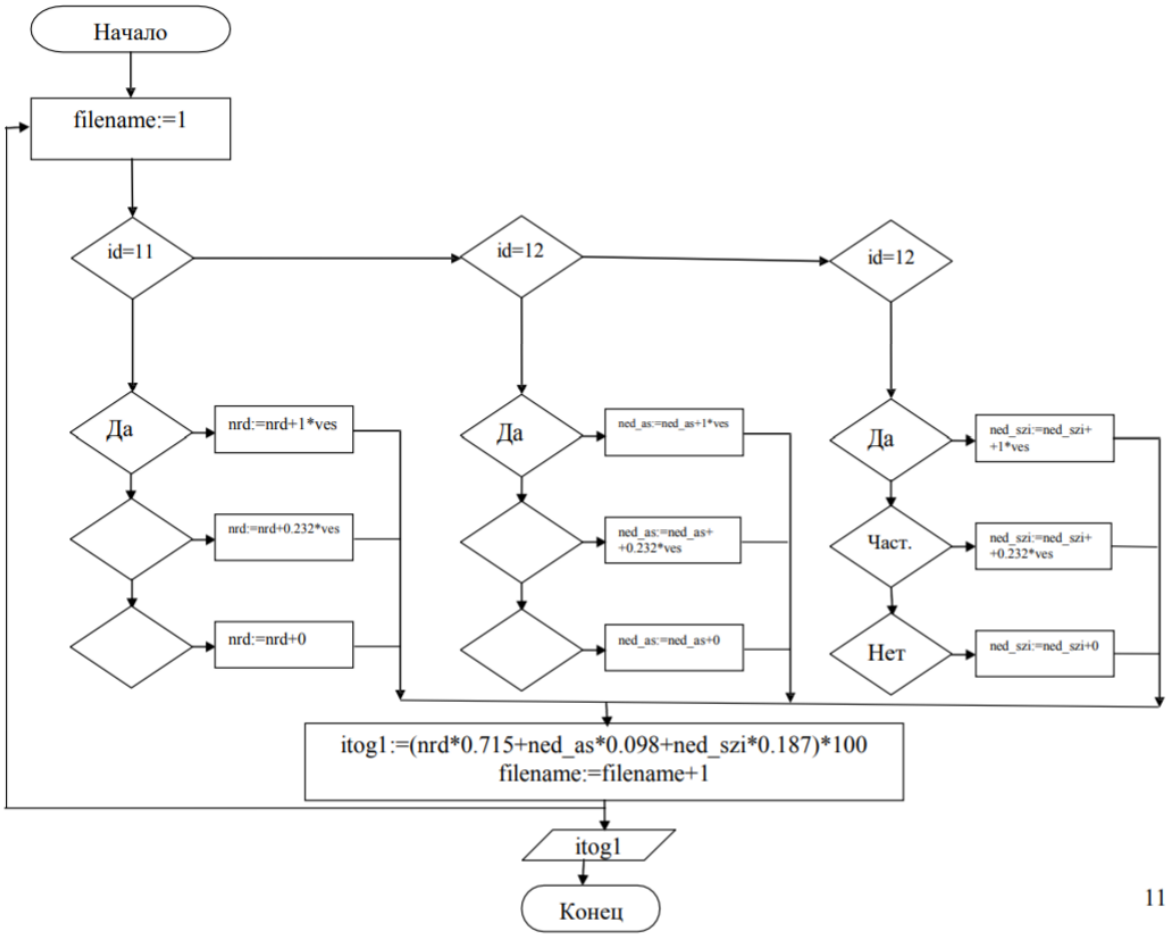
ОСИБ әдістемесіне сәйкес әрбір бақылау саласына сәйкес сипаттамалардың иерархиясы әзірленді. "Ақ нормативтік-Құжаттамалық қамтамасыз ету" бақылау саласы бойынша 3 топтық көрсеткіш бар:

- нормативтік-Құжаттамалық қамтамасыз ету-GP1;
- автоматтандырылған жүйелерге нормативтік-пайдалану құжаттамасы (оның ішінде қолданбалы жүйелер) – GP2;
-ақпаратты қорғау құралдарына арналған нормативтік – пайдалану құжаттамасы-GP3.

Осылайша, "АҚ нормативтік-құжаттамалық қамтамасыз ету" бақылау саласы үшін суретте көрсетілген көрсеткіштердің иерархиясы бар

"Көрсеткіштер иерархиясын қалыптастыру "және" сараптамалық бағалауға алдын ала дайындық" кезеңдері құрал-саймандық құралда қазірдің өзінде орындалды, яғни көрсеткіштердің иерархиясы барлық деңгейдегі көрсеткіштерге салмақ коэффициенттері қалыптастырылды және тағайындалды және барлық көрсеткіштер үшін басымдық векторы құрылды.

Пайдаланушы сәйкестік дәрежесін көрсеткеннен кейін 2.29, 2.30, 2.31 формулаларына сәйкес жалпыланған көрсеткіштердің есебі жүргізіледі.



111

Бағдарлама жұмысының сипаттамасы

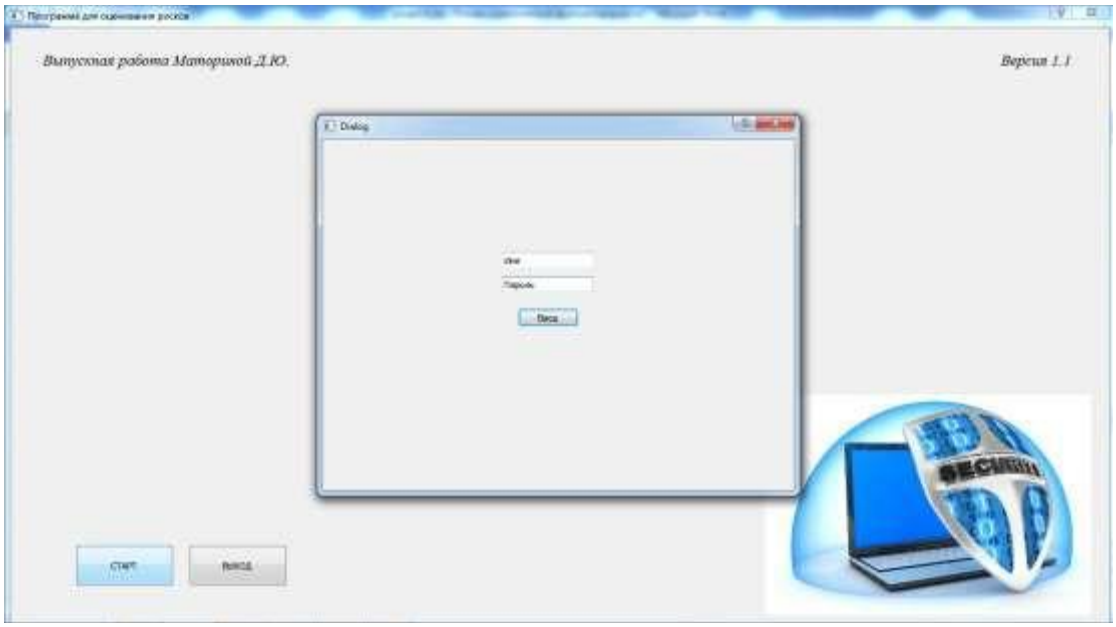
Бағдарламаны іске қосқан кезде монитор экранында Б. 3-суретте келтірілген бастапқы заставка көрсетіледі.

2 сурет-бастапқы заставка

"Бастау" батырмасын басқан кезде бағдарламалық кодты орындау іске қосылады және пайдаланушыны авторландыру рәсімінің басталуы басталады.

"Шығу" батырмасын басқан кезде экрандық заставка жабылады және бағдарламалық кодты орындау аяқталады.

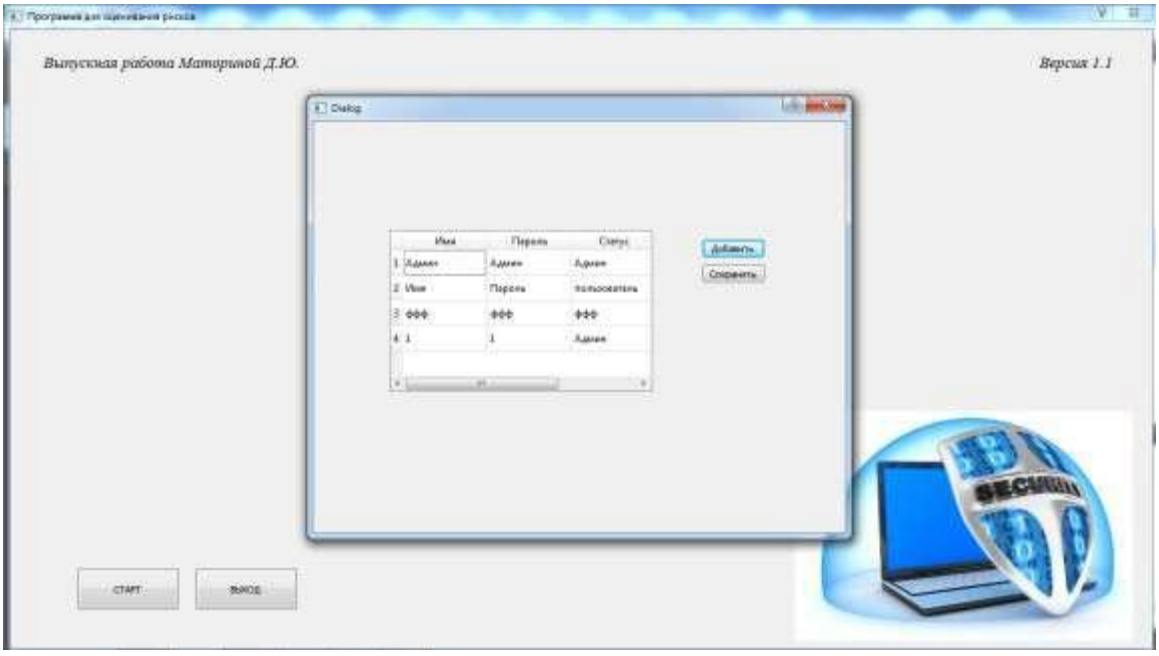
Авторизация процедурасын орындау авторизация параметрлерін енгізуге арналған жаңа экрандық нысанды монитордың экранында бейнелеуден басталады. Экрандық форманың түрі Б. 4 суретте көрсетілген.



3 сурет -авторизация параметрлерін енгізу

Пайдаланушы аты мен паролін тиісті терезелерге енгізгеннен кейін "енгізу" батырмасын басу арқылы негізгі бағдарламалық код іске қосылады.

Егер авторизацияланған пайдаланушы "әкімші" мәртебесіне ие болса, әкімшілендіру режимі басталады, оның экрандық нысаны Б. 5-суретте келтірілген.



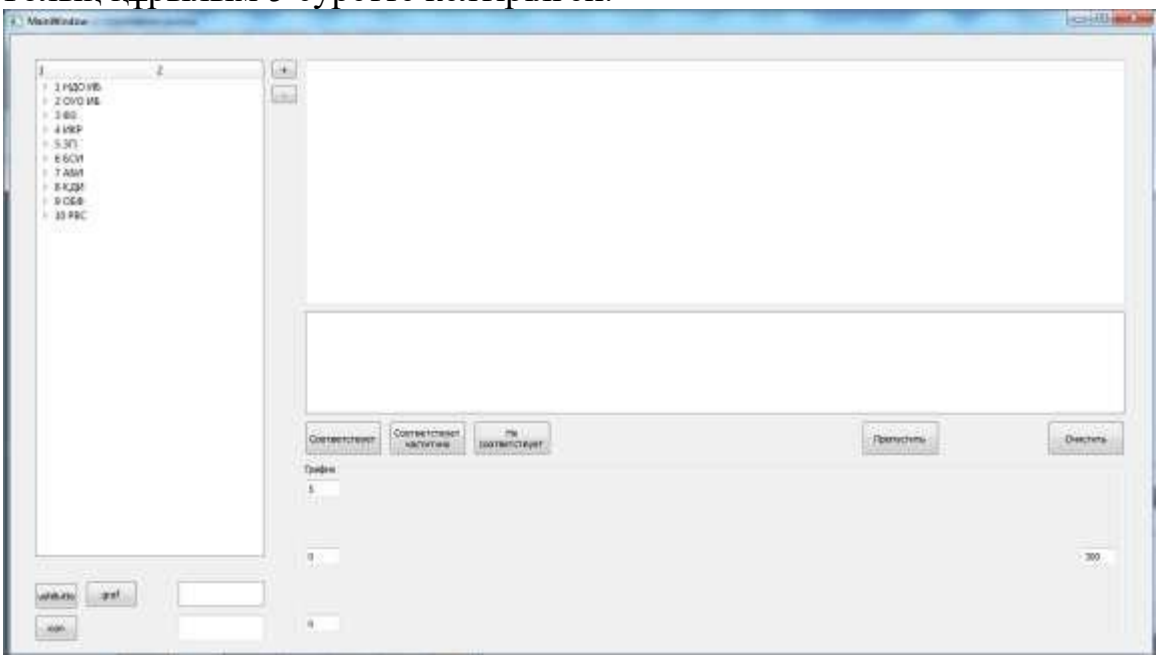
4-сурет-әкімшілендіру режимінің экрандық нысаны

Егер авторизацияланған пайдаланушы "пайдаланушы" мәртебесіне ие болса, негізгі жұмыс режимі басталады, оның экрандық нысаны Б-6 суретте келтірілген.

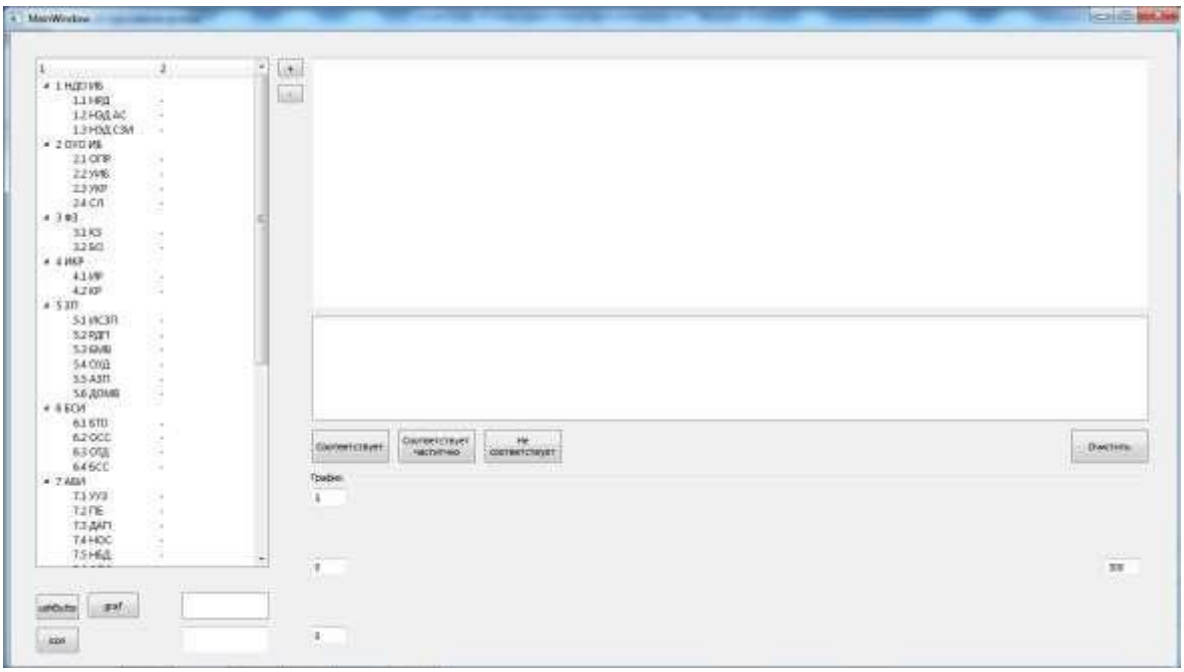
Негізгі жұмыс режимі сарапшыға кәсіпорынды бағалауды орындауға мүмкіндік береді.

Он топқа топтастырылған сұрақтар ағаш тәрізді құрылым түрінде ұсынылған. "+" Және "-" түймелері құрылымды өрістетуге және бұрауға мүмкіндік береді.

Толық құрылым 5 суретте келтірілген.



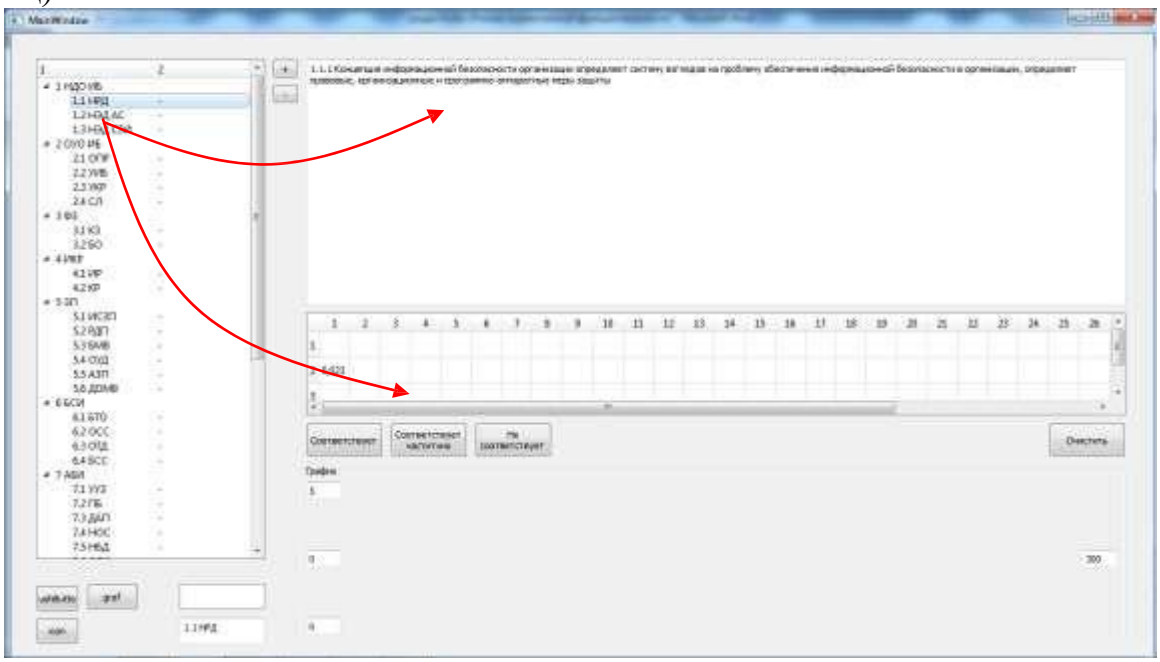
6 сурет - негізгі жұмыс режимі



7 сурет -кеңейтілген құрылым

Экрандық меңзерді сұрақтар кіші тобына бағыттау браузерлік терезеде топтың бірінші сұрағы мен кіші топтың сұрақтарының санына тең бағандар

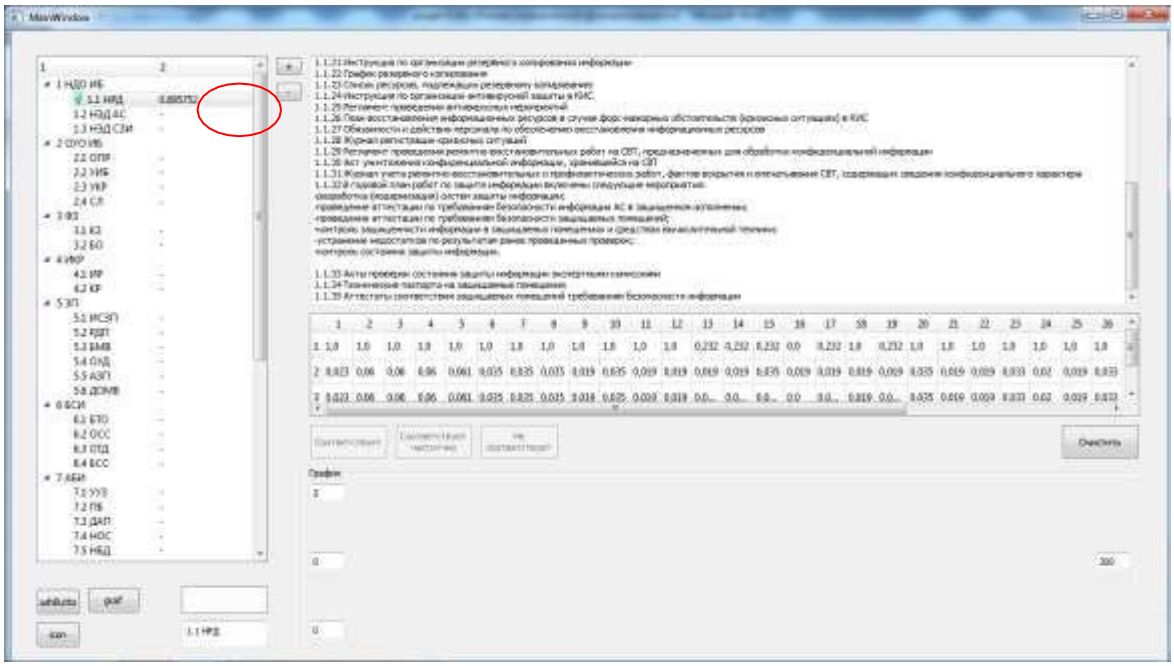
саны бар кестенің пайда болуына әкеп соғады (Б. 8-суретті қараңыз). Кестенің екінші жолында бағаланатын сұрақ салмағының мәні пайда болады (6-сұрақ)



8 сурет -сұрақтардың экрандық формасы

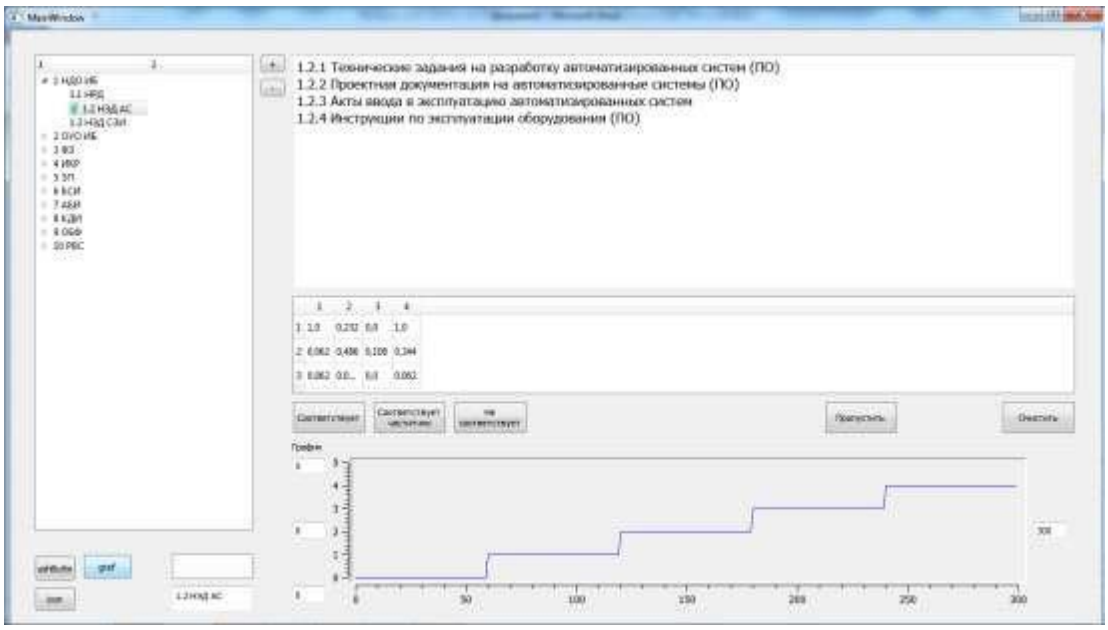
"Сәйкес келеді", "ішінара сәйкес келеді" және "сәйкес келмейді" кнопкаларын пайдалана отырып, сарапшы кәсіпорынды бағалайды. Бағалау нәтижесі кестенің ағымдағы бағанында көрсетіледі.

Кіші топтың барлық тармақтарын бағалағаннан кейін сәйкестік индексін есептеу орындалады және есептелген мән ағаш тәрізді құрылымның тиісті ұяшығында көрсетіледі (9-сурет).



9-сурет-сәйкестік индексін есептеу

Бағалау рәсімі аяқталғаннан кейін нәтижелерді графикалық түрде көрсетуге болады (10 сурет).



Әзірленген бағдарламалық кешен сараптамалық бағалауды жинау, әзірленген әдістемелерге сәйкес бағалау нәтижелерін өңдеу және қорытынды есепті құжатты қалыптастыру кезеңдерін автоматтандыруға мүмкіндік береді.