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

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

ДИПЛОМДЫҚ ЖОБА

Тақырыбы: Ақпараттық қауіпсіздік тәуекелдерін талдаудың құралын әзірлеу

Мамандығы: 5В100200 – «Ақпараттық қауіпсіздік жүйелері»
Орындаған: Тлеуберген Ақзер Қуатқызы Тобы: СИБк-16-1
(аты-жөні)
Ғылыми жетекші: аға оқытушы Дмитриева Маргарита Валерьевна
(ғылыми дәрежесі, атағы, аты-жөні)
Кеңесшілер:
Мамандығы бойынша:
аға оқытушы Дмитриева Маргарита Валерьевна
(ғылыми дәрежесі, атағы, аты-жөні)
_____«_____»_____ 2020 ж.
(қолы)
Тіршілік қауіпсіздігі бөлімі бойынша:
доцент Жандаулетова Фарида Рустембековна
(ғылыми дәрежесі, атағы, аты-жөні)
_____«_____»_____ 2020 ж.
(қолы)
Мөлшер бақылаушы:
аға оқытушы Альмуратова Камшат Бимуратовна
(ғылыми дәрежесі, атағы, аты-жөні)
_____«_____»_____ 2020 ж.
(қолы)
Пікір беруші:
Шаяхметова Асем Серикбаевна
(ғылыми дәрежесі, атағы, аты-жөні)
_____«_____»_____ 2020 ж.
(қолы)

Алматы 2020

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

Басқару және ақпараттық технологиялар институты
Ақпараттық қауіпсіздік жүйелері кафедрасы
5В100200 – «Ақпараттық қауіпсіздік жүйелері» мамандығы

Дипломдық жобаны орындауға берілген
ТАПСЫРМА

Студент: Тлеуберген Ақзер Қуатқызы
(аты-жөні)

Жобаның тақырыбы: Ақпараттық қауіпсіздік тәуекелдерін талдаудың құралын әзірлеу

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

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

Жобаға алғашқы деректер (талап етілетін зерттеу (жоба) нәтижелерінің параметрлері және зерттеу нысанының алғашқы деректері):
1. Қауіп-қатерлер мен осалдықтарды талдау моделі
2. Бағдарламаны әзірлеу құралы ретінде PHP бағдарламалау тілі
3. DevelNext ортасының 16.7.0 нұсқасы
4. SQLite деректер базасы

Диплом жобасындағы әзірленуі тиіс мәселелер тізімі немесе диплом жобасының қысқаша мазмұны:
1. Кіріспе
2. Ақпараттық қауіпсіздік тәуекелдерін талдау және бағалау
3. АҚ қауіптері мен тәуекелдерін бағалаудың қолданыстағы әдістемелерін сипаттау және талдау
4. АҚ тәуекелдерін бағалауды алгоритмдік және бағдарламалық қамтамасыз ету
5. Өміртіршілік қауіпсіздігі бөлім
6. 6.Ақпараттық қауіпсіздіктің тәуекелдерін есептеу
7. Қорытынды
8. Әдебиеттер тізімі

Графикалық материалдардың (міндетті түрде дайындалатын сызбаларды көрсету) тізімі:

Компанияның қызметі мен ұйымдық құрылымын зерттеу

2.2-сурет – АҚ тәуекелдерін бағалау әдістемелерін салыстырмалы талдау

2.1-кесте – Ақпараттық қауіпсіздік тәуекелдерін бағалау әдістерін салыстырмалы талдау

2.2-кесте – АҚ тәуекелдерін бағалау әдістемелерін салыстырмалы талдау нәтижелері

2.3-кесте – АҚ тәуекелдерін басқару үшін бағдарламалық құралдарды салыстыру

3.1-кесте – Активтердің қауіптері мен осалдықтар тізімі

3.3-кесте – Қауіптердің іске асыру ықтималдығы мен маңыздылығын есептеу

3.7-кесте – «Қауіп-қатерлер мен осалдықтарды талдау моделі» бойынша тәуекелдерді бағалаудың қорытынды кестесі

3.1-сурет – Құрылымдық сұлба

5.4 кесте – Тәуекелдерді бағалаудың қорытынды кестесі

Негізгі ұсынылатын әдебиеттер:

1. Ажмухамедов, И.М. Управление рисками информационной безопасности в условиях неопределенности / И.М. Ажмухамедов, О.Н. Выборнова, Ю.М. Брумштейн // Проблемы информационной безопасности. Компьютерные системы. – 2016. – Т. 1. – С. 7-14.

2. Разумников С.В. Анализ возможности применения методов OCTAVE, RISKWATCH, CRAMM для оценки рисков ИТ для облачных сервисов / С.В. Разумников // Современные проблемы науки и образования. – 2014. – № 1. – С. 247.

3. Плетнёв П.В. Сравнительный анализ существующих методов определения рисков информационной безопасности/ П.В. Плетнёв, В.М. Белов // Ползуновский вестник. - 2011. - №3/1. - С. 221-223.

Жоба бойынша жобаның бөлімдеріне қатысты белгіленген кеңесшілер

Бөлімдері	Кеңесшілері	Мерзімі	Қолы
Негізгі бөлім	Дмитриева М.В.		
Өміртішілік			
қауіпсіздігі	Жандаулетова Ф.Р.		
Тәуекелдерді есептеу			
бөлімі	Дмитриева М.В.		
Нормабақылаушы	Альмуратова К.Б.		

Диплом жобасын дайындау
КЕСТЕСІ

Бөлімдердің атауы, әзірленетін мәселелердің тізімі	Ғылыми жетекшіге ұсыну мерзімдері	Ескерту
Кіріспе	12.02.20 – 14.02.20	орындалды
1 Ақпараттық қауіпсіздік тәуекелдерін талдау және бағалау	18.02.20 – 24.03.20	орындалды
1.1 Ақпараттық қауіпсіздік тәуекелін талдаудың өзектілігі	18.02.20 – 24.02.20	орындалды
1.2 Ақпараттық қауіпсіздік тәуекелін басқарудың мақсаттары мен тәсілдері	28.02.20 – 10.03.20	орындалды
1.3 АҚ қауіптері мен тәуекелдерін бағалаудың қолданыстағы әдістемелерін сипаттау және талдау	10.03.20 – 24.03.20	орындалды
2 АҚ қауіп-қатерлері мен тәуекелдерін бағалау әдістемесі	26.03.20 – 15.04.20	орындалды
3 АҚ тәуекелдерін бағалауды бағдарламалық қамтамасыз ету	26.03.20 – 15.04.20	орындалды
3.1 Бағдарламалау тілі және ортасы	28.03.20 – 01.04.20	орындалды
3.2 Бағдарламалық қамтаманың алгоритм	02.03.20 – 27.04.20	орындалды
3.3 Пайдаланушы нұсқаулығы	28.04.20 – 25.05.20	орындалды
4 Өміртіршілік қауіпсіздігі бөлімі	19.04.20 – 15.05.20	орындалды
4.1 Жұмыс жағдайын талдау	19.04.20 – 02.05.20	орындалды
4.2 Есептеу бөлімі	02.05.20 – 15.05.20	орындалды
5 Жобалық тәуекелдерді бағалау	08.05.20 – 26.05.20	орындалды
5.1 Жобалық тәуекелдерді талдау және бағалау	08.05.20 – 15.05.20	орындалды
5.2 CORAS құралы арқылы жобалық тәуекелдерді талдау	15.05.20 – 26.05.20	орындалды
Қорытынды	27.05.20 – 28.05.20	орындалды

Тапсырманың берілген уақыты «12» ақпан 2020 ж.

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

Жобаның
ғылыми жетекшісі: _____ (Дмитриева М.В.)
(қолы) (аты-жөні)

Орындалатын тапсырманы
қабылдаған студент: _____ (Тлеуберген А.Қ.)
(қолы) (аты-жөні)

Аңдатпа

Бұл дипломдық жобада ұйымдағы ақпараттың қауіпсіздігін қамтамасыз етуге байланысты талаптарды толық талдауға және құжаттауға мүмкіндік беретін қауіптермен мен осалдықтарды талдау моделі негізінде тәуекелдердің мәнін бағалау құралын әзірлеу мәселесі қаралды. Бұл әдісті қолдану тәуекелдерді субъективті бағалау кезінде туындайтын қауіпсіздік шараларының артық шығындарын болдырмауға, ақпараттық жүйелердің өмірлік циклінің барлық кезеңдерінде қорғауды жоспарлауға және жүзеге асыруға, сонымен қатар жұмыстың қысқа мерзімде орындалуын қамтамасыз етуге мүмкіндік береді.

Бастапқы бөлімдерде кең таралған тәуекелдерді талдаудың әдістемелері және тәуекелдерді бағалаудың бағдарламалық өнімдері талданды және салыстырмалы талдау нәтижелеріне сүйене отырып қорытынды жасалды, ұсынылған үлгіге сәйкес есептер жүргізілді. Таңдалған модельдің негізінде ақпараттық қауіпсіздік тәуекелдерін бағалау үшін бағдарламалық қамтамасыз етуді құру ұсынылды.

Сонымен қатар жобалық тәуекелдерді бағалау мәндері келтірілді және өміртіршілік қауіпсіздігі мәселелері қарастырылды.

Аннотация

В данном дипломном проекте рассмотрен вопрос разработки инструментального средства на основе модели анализа угроз и уязвимостей при защите информации в организациях, позволяющий полностью проанализировать и документально оформить требования, связанные с обеспечением безопасности информации в организации. Использование данной методики даст возможность избежать расходов на избыточные меры безопасности, возникающие при субъективной оценке рисков, оказать помощь в планировании и осуществлении защиты на всех стадиях жизненного цикла информационных систем, а также обеспечить проведение работ в сжатые сроки.

В первичных разделах были анализированы распространенные методики анализа рисков и программных продуктов оценки рисков и сделан вывод исходя из результатов сравнительного анализа, проведены расчеты согласно предложенной модели. Предложен создание программного обеспечения для оценки рисков информационной безопасности на основе выбранной модели.

Также приведены значения оценки проектных рисков, и рассматривались вопросы по безопасности жизнедеятельности.

Annotation

In this diploma project, the issue of developing a tool based on the threat and vulnerability analysis model for protecting information in organizations is discussed, which allows you to fully analyze and document the requirements related to ensuring the security of information in an organization. Using this method will make it possible to avoid the costs of excessive security measures arising from a subjective risk assessment, to assist in the planning and implementation of protection at all stages of the life cycle of information systems, as well as to ensure that work is carried out in a short time.

In the primary sections, common methods of risk analysis and risk assessment software were analyzed and a conclusion was made based on the results of comparative analysis, calculations were made according to the proposed model. It is proposed to create software for assessing information security risks based on the selected model.

The values of project risk assessment are also given, and questions on life safety were considered.

Мазмұны

Кіріспе

Ақпараттық қауіпсіздік – ұлттық, салалық, корпоративтік, дербес деңгейлердегі жалпы қауіпсіздіктің маңызды аспектілерінің бірі. Бұл қазіргі әлемде ақпараттың көбеюі оны екінші реттік ресурстан қоғамдық өмірдің барлық салаларына әсер ететін негізгі факторға айналдырып, қоғамның ақпараттық тәуелділігінің өсіп келе жатқандығын көрсетеді.

Ақпараттық технологиялардың бизнес саласында кеңінен қолданылуын ескере отырып, сонымен қатар ақпаратты экономикалық категория ретінде қарастыра отырып, қазіргі нарықтық жағдайда ақпарат экономикалық субъектінің құнды активіне айналатынын атап өткен жөн.

Ақпараттық активтер – бұл ақпараттық технологияларды, ақпараттық жүйелерді, желілік инфрақұрылымды қолдана отырып, ақпараттық ресурстардың жиынтығы. Ақпараттық жүйелер мен технологияларға тәуелділік ұйымдардың түрлі қауіп-қатерлерге осал болып келетіндігін білдіреді, сондықтан кез-келген басқа активтер сияқты құпия ақпаратты қорғауды қажет етеді. Ақпараттық активтердің қауіпсіздігін бағалау саласындағы жағдайдың талдауы көрсеткендей, оларға қарсы зиянды әрекеттер азайып қана қоймайды, сонымен бірге өсудің тұрақты тұрақты тенденциясына ие. Алаяқтық, зиянкестік, өнеркәсіптік шпионаж, компьютерлік бұзу, компьютерлік ақпараттық жүйелердің зиянды бағдарламалармен зақымдануы және т. б. сияқты қауіпсіздік қатерлері көбейіп келеді.

Қазіргі таңда басшылардың ықтимал тәуекелдердің пайда болу дәрежесін алдын ала болжау, бағалау және азайту қабілеті кез келген қызмет саласындағы табыстың аса маңызды шарты болып табылады. Ақпараттық қорғауды басқару жүйесін бағалау жөніндегі іс-әрекетте объективтік сәйкестендіру және кәсіпорын үшін неғұрлым маңызды ақпараттық тәуекелдердің дәрежесін бағалау негізгі элементтер болып табылады, олардың нәтижесінде басымдықтар қойылады, ұйымның ақпараттық қауіпсіздігіне қойылатын талаптар айқындалады.

Экономикалық дамудың қазіргі кезеңінде ақпараттық тәуекелдерді бағалау қауіп-қатерден қорғанудың негізгі бағыттарының бірі болып табылатындығын ескере отырып, ақпараттық тәуекелдерді бағалауға қолданылатын әдіснамалық тәсілдерді одан әрі жетілдіру қажет. Сондықтан ақпараттық қауіптерді бағалаудың теориялық және практикалық мәселелерін шешу бүгінгі күннің өзекті ғылыми мәселесі болып табылады.Бұл ретте ақпараттық активтердің экономикалық мәні, оларға тұрақсыздандыратын әсер ету нәтижесінде олардың құнының өзгеруі, ақпараттық активтерді қорғаудың түрлі құралдары мен әдістерін қолданудың экономикалық тиімділігі және басқалар сияқты маңызды мәселелер аз зерттелінген болып қала береді.

Сондықтан, бүгінгі таңда ақпаратты қорғау саласындағы басқарудың жаңа нысандары мен әдістерін құру ғана емес, сонымен қатар ақпараттық

активтердің қауіпсіздігін бағалау саласында жаңа әдіснамалық тәсілдерді қалыптастыру қажет.

Тақырыптың өзектілігі

Қазіргі уақытта ақпараттық қауіпсіздік режимін ұйымдастыру кез келген компанияның дамуындағы маңызды стратегиялық факторға айналуда. Ақпараттық-телекоммуникациялық жүйелер мен технологиялардың ұйымдардың қызметіндегі рөлінің артуына байланысты ақпараттық жүйелердің қауіптері мен тәуекелдерін бағалау мен басқару процедураларын қолданудың өзектілігі мен қажеттілігі тұрақты түрде артып келеді.

Мақсаты: ақпараттық қауіпсіздік тәуекелдерінің мәнін бағалау үшін қауіп-қатерді бағалаудың бағдарламалық қамтамасыз етуін әзірлеу.

Осы мақсатқа жету үшін келесі тапсырмалар қойылды:

- қауіптер мен тәуекелдерді бағалаудың қолданыстағы алгоритмдері мен әдістемелерін зерттеу және талдау, өндірістік қызметте олардың жеткіліктілігі мен қолданылуы туралы қорытынды жасау;
- ұсынылған әдістемені толық зерттей келе, ақпараттық жүйелердің қауіптері мен тәуекелдерін бағалау;
- ұсынылған әдістеме негізінде бағдарламалық қамтамасыз етуді әзірлеу және оның жұмысқа қабілеттілігін көрсету.

Бұл жұмыстың зерттеу объектісі көп деңгейлі құрылымы бар кәсіпорындардың ақпараттық жүйесі болып табылады.

Зерттеу нысаны – зерттеу объектісіндегі ақпараттық қауіпсіздік жағдайларының тәуекелдерін бағалауға мүмкіндік беретін қауіптер мен осалдықтарды талдау моделі.

Жұмыстың жаңалығы зерттелетін әдіс ақпараттық қауіпсіздік маманына осы процесті автоматтандыру арқылы АЖ қауіптерін бағалау процедуралары кезінде кететін уақытты азайтуға және ақпараттық қауіпсіздікке қауіп төндіретін қателіктер мен ақпараттық қауіпсіздік сарапшыларының кәсіби дағдыларын азайтуға мүмкіндік беретін бағдарламалық жасақтама түрінде жүзеге асырылатындығында.

1 Ақпараттық қауіпсіздік тәуекелдерін талдау және бағалау

1.1 Ақпараттық қауіпсіздік тәуекелін талдаудың өзектілігі

Соңғы бірнеше жылда ақпарат адам өмірінің барлық салаларында шешуші рөл атқара бастады, бұл ақпараттық қоғамның біртіндеп қалыптасуымен байланысты. Адамзаттың дамуы үшін материалдық, аспаптық және басқа ресурстар ғана емес, сонымен қатар ақпараттық ресурстар қажет болды. Қазіргі уақытта бүкіл жер шарын қамтитын ақпараттық ағындардың тез өсуі байқалады, өйткені техникалық және технологиялық инновациялардың өсіп келе жатқан қарқынымен сипатталатын дамудың қазіргі кезеңіне көшумен оларды негіздеу, әзірлеу, іске асыру және тарату үшін қажетті білімнің көлемі айтарлықтай өсуі тиіс. Ақпарат көлемінің едәуір өсімі өнеркәсіп, сауда, білім беру және қаржы саласы сияқты салаларда байқалады. Ақпарат өнімнің құнды түріне айналады, оның жиынтық құны жақын болашақта материалдық өндіріс өнімдерінің жиынтық құнынан асып түсуі тиіс, өйткені материалдық игіліктер мен қызметтерді табысты ресурс үнемдейтін құруды қамтамасыз ету үшін білімнің өсуін, оларды тиімді іздестіруді, сақтауды, таратуды және енгізуді қамтамасыз ететін принципті жаңа технологияны пайдалану қажет.

Экономикада болған осы өзгерістерге байланысты ақпарат, ақпараттық технологиялар және пайда болған ақпараттық қызмет көрсету нарығы өзіне жіті назар аударуды және зерделеуді талап етеді, өйткені құнды және маңызды ақпаратты иелену, пайдалану және беру салдарынан компанияның, мемлекет пен тұтастай экономикаға елеулі зиян келтіруі мүмкін бірқатар тәуекелдер туындауы мүмкін. Әрбір корпорацияда өндіріс құпиялары, бірегей инновациялар, зияткерлік меншік туралы деректер, клиенттердің, серіктестердің, жеткізушілердің, қызметкерлердің деректер базасы бар, оларда барлық өндірістік процесс негізделген және бұл деректердің бәсекелестердің немесе өзге де қолайсыз адамдардың қолына түсуі-компанияның жай-күйі мен жұмыс істеуіне айтарлықтай қауіп төндіреді. Желілік технологиялар мен мобильді құрылғылардың кең таралуына байланысты құнды ақпаратты қорғау мәселесі бұрынғысынан да өткір болып тұр. Компаниялардың негізгі міндеттерінің қатарына, әдеттегіден басқа, құпиялылықты қорғау және қамтамасыз ету, ақпараттық қауіптерді азайту және хакерлік шабуылдардың алдын алу сияқты мәселелер пайда болды. Ешкім ұрлық, ақпаратты ұстап алу, компьютерді вирусты жұқтыру, ақпаратты жою және т.б. сияқты жағымсыз салдардан сақтандырылмаған. Компанияның ақпараттық қауіпсіздігін қамтамасыз ету жоғары басшылықтың маңызды міндеттерінің бірі ғана емес, сонымен қатар жалпы ұйым менеджментінің маңызды құрамдас бөлігі болып табылады [1].

Осылайша, қазіргі заманғы бизнес алдында өзінің ақпараттық ресурстарын сенімді қорғауды қамтамасыз ету қажет. Алайда, кез келген басқа қорғаныс сияқты, ақпаратты қорғау өте қымбат іс болып табылады және кәсіпорын басшылары мұндай салымдардың ақпараттық тәуекелдермен

байланысты шығындарды айтарлықтай төмендетуге мүмкіндік бере отырып, өте тиімді болып табылатынына әрдайым келісе бермейді.

Ақпараттық қауіпсіздік мәселелеріне арналған жарияланымдардың көпшілігі техникалық егжей-тегжейлермен мол, алайда қандай да бір шешімдердің экономикалық орындылығы мәселесін елемейді. Сонымен, қолданыстағы стандарттардың көп бөлігі ақпаратты қорғау жүйесі бағытталған шабуылдаушының мүмкіндіктерін анықтауға мүмкіндік беретін «зиянкестер моделі» түсінігін қолданады. Алайда, бұл тәсіл тек жүйенің сенімділігін бағалауға мүмкіндік береді және оның шығын сипаттамаларын ескермейді. Сонымен бірге, экономикалық тиімділік мәселесі жеке бағдарламаларды және ақпараттық қауіпсіздікті қамтамасыз ету шараларын іске асыру үшін әртүрлі көлемдегі ақша бөлу туралы шешім қабылдаудағы шешуші фактор болып табылады. Бүгінгі күні осы мәселені шешудің ең көп таралған тәсілі ақпараттық жүйеде тәуекелдерді бағалауға және тиімді қарсы шаралар таңдауға мүмкіндік беретін тәуекелдерді талдау жүйесін қолдану болып табылады.

1.2 Ақпараттық қауіпсіздік тәуекелін басқарудың мақсаттары мен тәсілдері

Кез келген ұйымның мақсаты оның қызметінің нәтижелерін сипаттайтын белгілі бір көрсеткіштерге қол жеткізу болып табылады. Мысалы, коммерциялық компаниялар үшін бұл пайда табу, капиталдандырудың өсуі, нарық немесе айналым үлесі, ал үкіметтік ұйымдар үшін – халыққа мемлекеттік қызмет көрсету және басқару міндеттерін шешу. Қалай болғанда да, ұйымның мақсатына қарамастан, осы мақсатқа қол жеткізуге ақпараттық қауіпсіздік тәуекелдерін енгізу арқылы кедергі келтірілуі мүмкін. Сонымен бірге, әр ұйым тәуекелдерді және оларды азайтуға инвестициялау мүмкіндігін бағалайды.

Осылайша, ақпараттық қауіпсіздік тәуекелдерін басқарудың мақсаты тәуекелдерді ұйым үшін қолайлы деңгейде ұстап тұру болып табылады. Осы мәселені шешу үшін ұйым ақпараттық қауіпсіздіктің кешенді жүйелерін (АҚЖ) құрады.

Мұндай жүйелерді құру кезінде талдау процесінде анықталған ақпараттық қауіпсіздік тәуекелдерін осы құралдарды енгізу мен қолдауға артық шығынсыз төмендетуді қамтамасыз ететін қорғаныс құралдарын таңдау мәселесі туындайды. Ақпараттық қауіпсіздік тәуекелдерін талдау бізге ақпаратты қорғау құралдарының қажетті және жеткілікті жиынтығын, сондай-ақ ақпараттық қауіпсіздік тәуекелдерін төмендетуге бағытталған ұйымдастырушылық шараларды анықтауға және ұйымның нақты қызметі үшін ең тиімді және ақпараттық қауіпсіздік тәуекелдерін төмендетуге бағытталған АҚЖархитектурасын жасауға мүмкіндік береді.

Ақпараттық қауіпсіздікке қатысты барлық тәуекелдер екі параметрмен сипатталады: ұйымға ықтимал залал және оның іске асу ықтималдығы. Тәуекелдерді талдау үшін осы екі сипаттаманың тіркесімін

қолдану тәуекелдерді әртүрлі деңгейлермен және ықтималдылықтармен салыстыруға мүмкіндік береді, бұл оларды ұйымдағы тәуекелдерді азайту туралы шешім қабылдаған адамдарға түсінікті жалпы көрініске әкеледі. Сонымен қатар, тәуекелдерді басқару процесі құрамы мен мазмұны қолданылатын тәуекелдерді бағалау мен қолданылатын басқару әдіснамасына байланысты келесі кезеңдерден тұрады:

- ұйым үшін қауіптің қолайлы деңгейін анықтау - тәуекелді қабылдау немесе оны өңдеу туралы шешім қабылдауда қолданылатын өлшем. Осы критерий негізінде болашақта анықталған қандай тәуекелдер сөзсіз қабылданып, әрі қарай қарастырудан шығарылатындығы анықталды, әрі қарай талдауға ұшырап, тәуекелдерге әрекет ету жоспарына енгізілді;
- тәуекелдерді анықтау, талдау және бағалау. Тәуекелдерге қатысты шешім қабылдау үшін олар бірегей анықталуы және тәуекелді іске асырудан келтірілген залал және оны іске асыру мүмкіндігі тұрғысынан бағалануы керек. Залалды бағалау кезінде ұйымның ақпараттық активтеріне және олар қолдау көрсететін бизнес-процестерге әсер ететін тәуекел дәрежесі анықталады. Ықтималдылықты бағалау кезінде тәуекелдің туындау ықтималдығына талдау жасалады. Бұл параметрлерді бағалау тәуекелге ұшырауы мүмкін ақпараттық технологиялар (АТ) активтеріне тән осалдықтарды және осы осалдықтарды пайдалану арқылы жүзеге асырылатын қауіптерді анықтауға және талдауға негізделуі мүмкін.

Сондай-ақ тәуекелдерді бағалаудың қолданылатын әдістемесіне байланысты оларды бағалау үшін бастапқы деректер ретінде қаскүнем моделі, ұйымның бизнес-процестері және ұйымның қызметі ортасындағы саяси, экономикалық, нарықтық немесе әлеуметтік жағдай сияқты тәуекелді іске асыруға факторлар туралы ақпарат пайдаланылуы мүмкін. Тәуекелдерді бағалау кезінде оларды бағалауға сапалық, сандық немесе аралас тәсіл пайдаланылуы мүмкін. Сапалы тәсілдің артықшылығына оның қарапайымдылығы, тәуекелдерді бағалауды жүргізуге мерзімдерді және еңбек шығындарын азайтуы жатады, ал шектеулеріне – экономикалық негіздеу және тәуекелдерге ден қою шараларына инвестициялардың орындылығын бағалау үшін тәуекелдерді талдау нәтижелерін пайдаланудың жеткіліксіз көрнекілігі мен күрделілігі болып табылады. Сандық тәсілдің артықшылығы тәуекелдерді бағалаудың дәлдігі, нәтижелердің көрнекілігі және осы тәуекелге ден қою үшін қажетті инвестициялар көлемімен ақшаға көрсетілген тәуекелдің мәнін салыстыру мүмкіндігі, кемшіліктері – күрделілігі, жоғары еңбек сыйымдылығы және орындалу ұзақтығы болып табылады;

- тәуекелдерді дәрежелеу. Тәуекелдерге әрекет ету әзірлеу кезінде басымдықты айқындау және әрекет ету жоспарын одан әрі әзірлеу үшін барлық тәуекелдерді дәрежелеу қажет. Тәуекелдерді саралау кезінде пайдаланылатын әдістемеге байланысты тәуекелдерді іске асырудан болатын залал, іске асыру ықтималдығы, тәуекел әсер ететін АТ-активтер және бизнес-процестер, қоғамдық резонанс және тәуекелді іске асырудан болатын беделдік залал және т. б. сияқты критерийлер қолданылуы мүмкін;

- тәуекелдер бойынша шешім қабылдау және тәуекелдерге әрекет ету жоспарын әзірлеу. Тәуекелдерге әрекет ету шараларының жиынтығын анықтау үшін олардың әрқайсысына қатысты мынадай шешімдердің бірін қабылдау мақсатында сәйкестендірілген және бағаланған тәуекелдерге талдау жүргізу қажет;
- тәуекелден қашу;
- тәуекелді қабылдау;
- тәуекелді беру;
- тәуекелді азайту.

Әрбір тәуекел бойынша қабылданған шешім тәуекелдерге әрекет ету жоспарында тіркелуі тиіс. Сондай-ақ осы жоспар пайдаланылатын әдістемеге байланысты тәуекелдерге әрекет ету үшін қажетті мынадай ақпаратты қамтуы мүмкін:

- әрекет ету шараларының сипаттамасы;
- әрекет етуге жауапты;
- әрекет ету шараларына қажетті инвестицияларды бағалау;
- осы шараларды іске асыру мерзімі.
- тәуекелдерге әрекет ету бойынша іс-шараларды іске асыру. әрекет ету шараларын іске асыру үшін жауапты тұлғалар тәуекелге әрекет ету жоспарында сипатталған іс-әрекеттің қажетті мерзімде орындалуын ұйымдастырады;
- іске асырылған шаралардың тиімділігін бағалау. Әрекет ету жоспарына сәйкес қолданылатын шаралар тиімді және тәуекелдер деңгейі ұйым үшін қолайлы екендігіне сенімділікке қол жеткізу үшін тәуекелге ден қоюдың әрбір іске асырылған шараларының тиімділігін бағалау, сондай-ақ ұйымның тәуекелдерін тұрақты сәйкестендіру, талдау және бағалау жүргізіледі;
- тәуекелдерді бағалау нәтижелері тәуекелдерді өңдеу жөніндегі іс-шараларды жүргізудің экономикалық орындылығы мен басымдығын айқындау үшін пайдаланылады, тәуекел деңгейін төмендететін қорғау шараларын таңдау жөнінде негізді шешім қабылдауға мүмкіндік береді.

Бүгінгі таңда ақпараттық қауіпсіздіктің кешенді мәселелерін шешуге маманданған көптеген шетелдік компаниялар ақпараттық тәуекелдерді басқарудың жеке әдістемелерін әзірлеп, ұсынды. Бұл әдістемелер, ең алдымен, тәуекелдерді бағалау рәсімдерінің негізіне алынған қолданылатын математикалық әдістердің деңгейі мен жетілдірілуі бойынша ерекшеленеді. Осыған байланысты олар нақты факторларды барабар есепке алудың әртүрлі мүмкіндіктеріне ие, бұл өз кезегінде алынған тәуекелді бағалаудың дәлдігі мен сенімділігін алдын ала анықтайды [2].

Тәуекелдерді басқаруға қызығушылықтың артуына қарамастан, қазіргі уақытта пайдаланылатын әдістемелердің көпшілігі салыстырмалы түрде тиімсіз, өйткені бұл процесті көптеген компаниялардағы әрбір бөлімдеріне байланысты тәуелсіз жүзеге асырады. Олардың іс-қимылдарын

орталықтандырылған бақылау көбінесе жоқ, бұл бүкіл ұйымда тәуекелдерді басқарудың бірыңғай және тұтас тәсілін іске асыру мүмкіндігін болдырмайды.

Ақпараттық қауіпсіздік тәуекелдерін бағалау мәселесін шешу үшін классикалық мынадай бағдарламалық кешендер болып қолданылуда: CRAMM, FRAP, RiskWatch, Microsoft Security Assessment Tool (MSAT), ГРИФ, CORAS және басқалар. Барлық белгілі әдістерді келесідей жіктеуге болады:

- тәуекелді бағалауды сапалы деңгейде қолданатын әдістемелер (мысалы, «жоғары», «орташа», «төмен» шкаласы бойынша), мұндай әдістемеге FRAP жатады;
- сандық әдістемелер (тәуекел сандық мән арқылы бағаланады, мысалы, күтілетін жылдық шығындардың мөлшері), RiskWatch әдістемесі осы санатқа жатады;
- аралас бағалауды қолданатын әдістемелер (мұндай әдістемеге CRAMM, MSAT жатады).

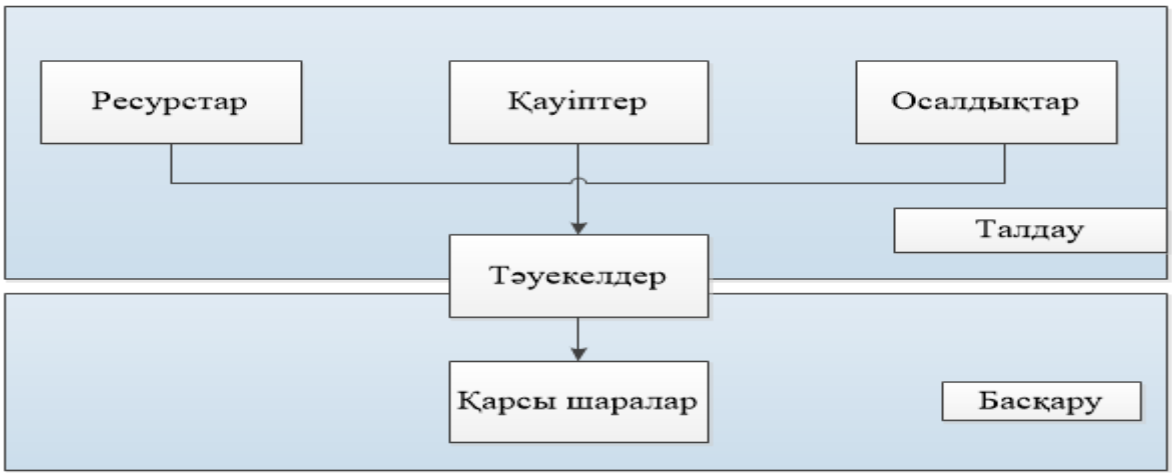
Ақпараттық қауіпсіздік тәуекелдерін талдау және бағалау әдістемелерінің қатарын оларды ықтимал пайдалану тұрғысынан қарастырайық.

АҚ тәуекелдерді басқарудың қандай да бір әдістемесін енгізу туралы шешім қабылдағанға дейін оның компанияның бизнес-қажеттіліктерін, оның ауқымын жеткілікті түрде толық ескеретініне, сондай-ақ үздік әлемдік практикаларға сәйкес келетініне және процестер мен талап етілетін іс-әрекеттердің егжей-тегжейлі сипаттамасы бар екеніне көз жеткізу керек [3].

1.3 АҚ қауіптері мен тәуекелдерін бағалаудың қолданыстағы әдістемелерін сипаттау және талдау

1.3.1 CRAMM

1985 жылы Ұлыбританияның қауіпсіздік қызметі әзірлеген CRAMM (CCTA Risk Analysis and Management Method) әдістемесі BS7799 сериялы ақпараттық қауіпсіздікті басқару стандарттарына негізделеді (қазіргі уақытта ISO 27000 стандартына айналған) және тәуекелдерді сапалы бағалау тәсілін сипаттайды. Бұл ретте сапалық көрсеткіштер мәндерінің шкаласына көшу сапалық және сандық көрсеткіштер арасындағы сәйкестікті анықтайтын арнайы кестелер көмегімен жүргізіледі. Тәуекелді бағалау бизнес үшін АТ-активтің құндылығын, осалдықтарды, қауіптерді және оларды іске асыру мүмкіндігін талдау негізінде жүргізіледі.



1.1 сурет – CRAM әдісінің кезеңдері

CRAMM әдістемесі бойынша тәуекелдерді басқару процесі келесі кезеңдерден тұрады:

- Бастама (Initiation). Бұл кезеңде ақпараттық қауіпсіздік тәуекелдерін талдау процесіне мүдделі тұлғалармен, оның ішінде тәуекелдерге талдау жүргізілетін АТ-активтерін пайдалану, әкімшілік ету, қауіпсіздікті қамтамасыз ету және пайдалану үшін жауапты тұлғалармен сұхбат жүргізіледі. Нәтижесінде одан әрі зерттеу үшін облыстың, оның шекараларының формалды сипаттамасы беріледі және талдауға тартылған тұлғалардың тәуекелдерінің құрамы анықталады.

- АТ–активтерін сәйкестендіру және бағалау (Identification and Valuation of Assets). Бұрын анықталған зерттеу аймағында ұйым қолданатын АТ-активтерінің тізімі анықталды. CRAMM әдіснамасына сәйкес

АТ-активтер келесі түрлердің бірі бола алады:

- деректер;
- бағдарламалық қамтамасыз ету;
- физикалық активтер.

Әрбір актив үшін ұйымның қызметі үшін оның маңыздылығы анықталады және қолданбалы міндеттерді шешу үшін АТ-активін пайдаланатын бөлімдердің өкілдерімен бірлесіп, ұйымның қызметі үшін оның құпиялылығын, тұтастығы мен қол жетімділігін бұзудан болатын салдарлар бағаланады.

- Қауіптер мен осалдықтарды бағалау (Threat and Vulnerability Assessment). АТ-активтерінің маңыздылығын бағалауға қосымша CRAMM әдістемесінің маңызды бөлігі АТ-активтерінің қатерлері мен осалдықтарының ықтималдығын бағалау болып табылады. CRAMM әдістемесі АТ-активтерінің осалдықтары мен осы осалдықтар арқылы активтерге әсер етуі мүмкін қауіптер арасындағы сәйкестікті сипаттайтын кестелерді пайдаланады. Сондай-ақ осы қауіп-қатерлерді іске асырған жағдайда АТ-активтері үшін залалды сипаттайтын кестелер бар. Бұл кезең ақпараттық қауіпсіздікті қамтамасыз ету шараларының базалық жиынтығын жеткіліксіз енгізу үшін ең

қиын АТ-активтер үшін ғана орындалады. Өзекті осалдықтар мен қауіп-қатерлерді анықтау АТ-активтерін басқару мен пайдалануға жауапты тұлғаларды сұхбат жүргізу жолымен жүргізіледі. Қалған активтер үшін CRAMM әдістемесі ақпараттық қауіпсіздікті қамтамасыз етудің қажетті базалық шараларының жиынтығын қамтиды.

- Тәуекелді есептеу (Risk Calculation). Тәуекелді есептеу мынадай формула бойынша жүргізіледі:

$$\text{Тәуекел} = \text{Р (іске асыру)} * \text{Залал} \quad (1.1)$$

Бұл ретте тәуекелді іске асыру ықтималдығы мынадай формула бойынша есептеледі:

$$\text{Р (іске асыру)} = \text{Р (қауіптер)} * \text{Р (осалдықтар)} \quad (1.2)$$

Әрбір АТ-актив үшін тәуекелдерді есептеу кезеңінде "1" – ден "7" - ге дейінгі шкала бойынша оның ақпараттық қауіпсіздігін қамтамасыз ету жөніндегі шаралар жиынтығына қойылатын талаптар анықталады, мұнда "1" мәніне ақпараттық қауіпсіздікті қамтамасыз ету жөніндегі шаралардың ең төменгі қажетті жиынтығы, ал "7" - ең жоғарғы мәніне сәйкес келеді.

- Тәуекелді басқару (Risk Management). Тәуекелді есептеу нәтижелері негізінде CRAMM әдістемесі ақпараттық қауіпсіздікті қамтамасыз ету бойынша қажетті шаралар жиынтығын анықтайды. Ол үшін 4 мыңға жуық шараны қамтитын арнайы каталог пайдаланылады. CRAMM әдістемесімен ұсынылған шаралар жиынтығы ұйым қабылдаған шаралармен салыстырылады. Нәтижесінде қорғау шараларын қолдану бөлігінде қосымша назар аударуды талап ететін аймақтар және артық қорғау шаралары бар аймақтар сәйкестендіріледі. Осы ақпарат тәуекел деңгейін қажетті деңгейге келтіру үшін - ұйымда қолданылатын қорғау шараларының құрамын өзгерту жөніндегі іс-шаралар жоспарын қалыптастыру үшін пайдаланылады.

Практикалық қолдану тұрғысынан CRAMM әдістемесінің келесі артықшылықтарын атап өтуге болады:

- CRAMM қолдану нәтижелерін халықаралық институттар мойындайды;
- әдістеменің түсінікті формальды сипаттамасының болуы тәуекелдерді талдау және басқару процестерін іске асыру кезінде қателердің туындау мүмкіндігін барынша азайтады;
- тәуекелдерді талдауды автоматтандыру құралдарының болуы еңбек шығындарын және тәуекелдерді талдау және басқару бойынша іс-шараларды орындау уақытын азайтуға мүмкіндік береді;
- қауіптер, осалдықтар, салдарлар, ақпараттық қауіпсіздікті қамтамасыз ету шаралары каталогтары тәуекелдерді талдау және басқару жөніндегі іс-шараларды тікелей орындаушылардың арнайы білімі мен құзыреттілігіне қойылатын талаптарды жеңілдетеді.

CRAMM әдістемесіне келесі кемшіліктер тән:

- ұйым ішінде немесе сырттан елеулі ресурстарды тартуды талап ететін бастапқы деректерді жинаудың жоғары күрделілігі мен еңбек сыйымдылығы;

- ақпараттық қауіпсіздік тәуекелдерін талдау және басқару процестерін іске асыруға ресурстар мен уақыттың үлкен шығындары;
- мүдделі тұлғалардың көп санының тартылуы жобалау командасы ішінде бірлескен жұмысты, коммуникацияларды ұйымдастыруға және нәтижелерді келісуге айтарлықтай шығындарды талап етеді;
- ақша арқылы тәуекелдерді бағалау мүмкін еместігі ақпаратты қорғау құралдары мен әдістерін енгізу үшін қажетті инвестицияларды техникалық-экономикалық негіздеу кезінде АҚ тәуекелдерін бағалау нәтижелерін пайдалануды қиындатады.

CRAMM Ұлыбританияда ақпараттық қауіпсіздік тәуекелдерін басқарудың нақты стандарты бола отырып, бүкіл әлем бойынша үкіметтік және коммерциялық ұйымдарда кеңінен қолданылады. Әдістеме халықаралық өзара іс-қимылға және ақпараттық қауіпсіздік тәуекелдерін басқару процестерін бастапқы енгізуді жүзеге асыратын және сол арқылы ұйымдағы барлық тәуекелдерді төмендету үшін халықаралық басқару стандарттарына сәйкестігіне бағдарланған ірі ұйымдарда табысты қолданылуы мүмкін. Бұл ретте, ұйымдар CRAMM қолдану үшін елеулі ресурстар мен уақытты бөлу мүмкіндігі болуы тиіс [4].

1.3.2 RiskWatch

RiskWatch бағдарламасы – тәуекелдерді талдау мен басқарудың қуатты құралы. RiskWatch құрамына қауіпсіздік аудитінің әр түрлі түрлерін жүргізетін бағдарламалық өнімдер кіреді. Ол аудит және тәуекелдерді талдау құралдарын қамтиды:

- RISKWATCH for Physical Security – АЖ физикалық қорғау әдістері үшін;
- RiskWatch for Information Systems – ақпараттық тәуекелдер үшін;
- HIPAA - WATCH for Healthcare Industry – HIPAA стандартының талаптарына сәйкестігін бағалау үшін (US Healthcare Insurance Portability and Accountability Act);
- RiskWatch RW17799 for ISO 17799 – ISO 17799стандартының талаптарына сәйкестігін бағалау үшін.

RiskWatch әдістемесінде тәуекелдерді бағалау және басқару үшін өлшемдер ретінде жылдық шығындарды болжау (Annual Loss Expectancy, ALE) және инвестициялардан қайтаруды бағалау (Return on Investment, ROI) пайдаланылады [5].

RiskWatch бағдарламалық өнімдері көптеген артықшылықтарға ие. RiskWatch тәуекелдерге талдау жүргізуге және қорғау шаралары мен құралдарының негізделген таңдауын жасауға көмектеседі. RiskWatch бағдарламасы CRAMM-ге қарағанда қауіпсіздік қатерлері мен қорғаныс жүйесін құруға кеткен шығындардың ара қатынасын нақты сандық бағалауға бағытталған. Сондай-ақ, бұл өнімде компьютерлік желінің ақпараттық және физикалық қауіпсіздігі саласындағы тәуекелдер бірлесіп қаралатынын атап өткен жөн.

RiskWatch өнімінің негізінде тәуекелдерді талдау әдістемесі жатыр, онда төрт кезеңді атауға болады.

Бірінші кезең – зерттеу нысанын анықтау. Мұнда ұйымның типі, зерттелетін жүйенің құрамы (жалпы сипаттарда), қауіпсіздік саласындағы базалық талаптар сияқты параметрлер сипатталады. Ұйымның үлгісіне сәйкес келетін үлгілерде ("коммерциялық ақпараттық жүйе", "мемлекеттік/әскери ақпараттық жүйе" және т.б.) аналитиктің жұмысын жеңілдету үшін қорғалатын ресурстар, шығындар, қауіптер, осалдықтар және қорғау шаралары санаттарының тізімі бар. Олардың ішінен ұйымда нақты қолданылатындарын таңдау керек.

Мысалы, шығындар үшін осындай санаттар қарастырылған:

- кідіріс және қызмет көрсетуден бас тарту;
- ақпаратты ашып көрсету;
- тікелей шығындар (мысалы, жабдықтардың өрттен жойылуы);
- өмір және денсаулық (қызметкерлер, тапсырыс берушілер және т. б.);
- деректерді өзгерту;
- жанама шығындар (мысалы, қалпына келтіруге арналған шығындар);
- ұйымның беделі.

Екінші кезең – жүйенің нақты сипаттамаларын сипаттайтын деректерді енгізу кезеңі. Деректер қолмен енгізілуі немесе компьютерлік желілердің осалдығын зерттеудің асаптың құралдарымен жасалған есептерден импортталуы мүмкін. Бұл кезеңде ресурстар, шығындар мен инциденттердің санаттары егжей-тегжейлі сипатталады.

Инциденттер кластары шығындар санаты мен ресурстар санатын салыстыру жолымен алынады. Ықтимал осалдықтарды анықтау үшін осы ресурстарға байланысты 600-ден астам сұрақтан тұратын сауалнама пайдаланылады. Сұрақтарды түзетуге, жаңаларын алып тастауға немесе қосуға болады. Әрбір бөлінген қауіптің туындау жиілігі, ресурстардың осалдық дәрежесі мен құндылығы қойылады. Мұның бәрі қорғаныс құралдарын енгізудің тиімділігін есептеу үшін қолданылады.

Үшінші кезең – тәуекелдерді бағалау. Алдымен алдыңғы кезеңдерде анықталған ресурстар, шығындар, қауіптер мен осалдықтар арасында байланыс орнатылады. Тәуекелдер үшін бір жылдағы шығындардың математикалық күтулері мынадай формула бойынша есептеледі:

$$m = p \cdot v, \tag{1.3}$$

мұндағы p – жыл бойы қауіп-қатердің туындау жиілігі, v – қауіп-қатерге ұшырайтын ресурстың құны.

Мысалы, егер сервердің құны \$150 000 болса, ал ол жыл ішінде өрттен жойылу ықтималдығы 0.01 тең болса, онда күтілетін шығындар \$1500 құрайды. Қорғау шараларын енгізгендегі және оларсыз күтілетін шығындарды салыстыра отырып, осындай іс-шаралардың тиімдігін бағалауға болады.

Төртінші кезең – есептер генерациясы. Есептердің түрлері: 1) қысқаша қорытындылар; 2) 1 және 2 сатыларда сипатталған элементтер туралы толық және қысқаша есептер; 3) қауіп-қатерлерді іске асырудан күтілетін шығындар мен қорғалатын ресурстардың құны туралы есеп; 4) қауіп-қатерлер мен қарсы іс-қимыл шаралары туралы есеп; 5) қауіпсіздік аудитінің нәтижелері туралы есеп [6].

Riskwatch кемшіліктеріне мыналарды жатқызуға болады:

- мұндай әдістеме қолайды, егер ұйымдық және әкімшілік факторларды ескермей, қорғаудың бағдарламалық-техникалық деңгейінде тәуекелдерге талдау жүргізу талап етілсе, тәуекелдердің алынған бағалары жүйелі ұстанымдардан тәуекелді түсінуді жоққа шығармайтын жағдайда. Әдістеме ақпараттық қауіпсіздіктің кешенді тәсілін ескермейді;
- RiskWatch тек ағылшын тіліндегі бағдарлама;
- лицензия бағасының жоғары болуы (шағын компания үшін бір жұмыс орны үшін $15 000 және корпоративтік лицензия үшін $125 000).

1.3.3 ГРИФ

Ақпараттық тәуекелдерді толық талдауды жүргізу үшін, ең алдымен, ақпараттық қауіпсіздік тұрғысынан ақпараттық жүйенің толық моделін құру қажет. Бұл міндетті шешу үшін ГРИФ нарықта ұсынылған батыс тәуекелдерін талдау жүйелеріне қарағанда, компанияның ақпараттық жүйелерінің қауіпсіздігін қамтамасыз етуге жауапты IT-менеджерлердің және жүйелік администраторлардың дербес қолдануын қажет етпейтін пайдаланушы үшін өте қарапайым және түсінікті интерфейске ие. Алайда, сыртқы қарапайымдылық талдау негізінде ақпараттық жүйеде бар тәуекелдерді дәл бағалауға мүмкіндік беретін, жүзден астам параметрлерді ескеретін күрделі тәуекелдерді талдау алгоритмін жасырады.

ГРИФ жүйесінің негізгі міндеті – IT-менеджерлердің өз бетінше (сыртқы сарапшыларды тартусыз) ақпараттық жүйедегі тәуекелдер деңгейін және компанияның қауіпсіздігін қамтамасыз ету жөніндегі қолданыстағы тәжірибенің тиімділігін бағалауға мүмкіндік беру, сондай-ақ компания басшылығы үшін оның ақпараттық қауіпсіздігі саласына инвестициялардың қажеттілігі туралы дәлелдерді сандардамен ұсыну.

ГРИФ әдісінің бірінші кезеңінде компания үшін маңызды ақпараттық ресурстардың толық тізімін анықтау мақсатында IT-менеджерге сауалнама жүргізіледі [7].

Екінші кезеңде компания үшін маңызы бар ақпараттың барлық түрлерін ГРИФ жүйесіне енгізу мақсатында IT-менеджерге сауалнама жүргізіледі. Енгізілген маңызды ақпарат топтарын пайдаланушы алдыңғы кезеңде көрсетілген ақпаратты сақтау объектілерінде (серверлерде, жұмыс станцияларында және т.б.) орналастыруы тиіс. Қорытынды кезеңде қауіптердің барлық түрлері бойынша тиісті ресурстарда орналасқан маңызды ақпараттың әрбір тобы бойынша залалдар көрсетіледі.

Үшінші кезеңде әр топтағы пайдаланушылар санын көрсете отырып, пайдаланушы топтарының барлық түрлерін анықтау өтеді.

Содан кейін ресурстардағы ақпараттың қандай топтарына пайдаланушылар топтарының әрқайсысына қол жетімдігі тіркеледі. Маңызды ақпаратты қамтитын барлық ресурстарға пайдаланушылардың қол жетімділігінің түрлері (жергілікті немесе қашықтағы) және құқықтары (оқу, жазу, жою) анықталады.

Төртінші кезеңде ресурстардағы маңызды ақпаратты қорғау құралдарын анықтау үшін IT-менеджерге сауалнама жүргізіледі. Бұдан басқа, жүйеге ақпаратты қорғаудың қолданылатын құралдарын сатып алуға арналған бір жолғы шығындар және оларды техникалық қолдауға арналған жыл сайынғы шығындар, сондай-ақ компанияның ақпараттық қауіпсіздік жүйесін сүйемелдеуге арналған жыл сайынғы шығындар туралы ақпарат енгізіледі.

Соңғы кезеңде жүйеде іске асырылған қауіпсіздік саясаты жөніндегі сұрақтарға жауап беру қажет, бұл жүйенің қорғалуының нақты деңгейін бағалауға және тәуекелдерді бағалауды нақтылауға мүмкіндік береді.

Жүйені дұрыс пайдаланбаған кезде және қауіпсіздікті қамтамасыз етудің барлық аспектілерін, оның ішінде қорғауды, физикалық қауіпсіздікті, қызметкерлердің қауіпсіздігін, бизнестің үздіксіздігін қамтамасыз етпеген жағдайда бірінші кезеңде атап өтілген ақпараттық қауіпсіздік құралдарынөздігіне қолдану өздігінен көмектесе алмайды. Осы кезеңдер бойынша барлық іс-қимылдарды орындау нәтижесінде нәтижесінде қауіпсіздік саясатының талаптарын нақты орындалуын ескере отырып, ақпараттық қауіпсіздік тұрғысынан ақпараттық жүйенің толық моделі қалыптастырылады, бұл тәуекелдерді бағалаудың және қорытынды есепті қалыптастыру үшін енгізілген деректерді бағдарламалық талдауға көшуге мүмкіндік береді. Мүмкін болатын залал көрінісін беретін жүйе бойынша толық есеп компания басшылығына ұсыну үшін дайын [8].

Грифтің кемшіліктеріне мыналарды жатқызуға болады:

- бизнес-үдерістерге байланыстың болмауы;
- есептерді әр түрлі кезеңдерде салыстыру мүмкіндігінің болмауы;
- қорғауды қамтамасыз ету бойынша шаралар кешенін енгізу;
- осы компания үшін қауіпсіздік саясатының жаңа талаптарын қосу мүмкіндігінің болмауы.

1.3.4 OCTAVE

Ақпараттық тәуекелдерді талдауға 2000 жылы ақпараттық қауіпсіздік Доктринасын қабылдағанға дейін дәстүрлі түрде тиісті назар аудармаған (қазіргі уақытта 2016 жылғы 5 желтоқсанда бекітілген жаңа нұсқа болып табылады). Бұл ретте тәуекелдерді талдаудың қазіргі әдіснамаларын практикалық қолдануға және оларды жетілдіруге ерекше көңіл бөлінеді.

Сонымен қатар, соңғы жылдары ақпараттық қауіпсіздікті басқару жүйесіне қойылатын талаптарды анықтайтын 27000 сериялы халықаралық стандарттар ұйымдарының АЖ жүйесінде әзірлеу және енгізу бойынша

жұмыс жалғасуда. Соңғы уақытта Карнеги Меллон университетінің (Carnegie Mellon University) құрамындағы Software Engineering Institute (SEI) институты әзірлеген OCTAVE ақпараттық қауіпсіздік тәуекелдерін талдау әдісі кеңінен танымал.

OCTAVE – елеулу қауіптер, активтер мен осалдықтарды жедел бағалау әдісі. Әдістеме АЖ тәуекелдерін талдау тобын құруды қарастырады. Талдау тобына жүйені басқаратын құрылымдық бөлімшелердің қызметкерлері және ақпарат бөлімінің қызметкерлері кіреді.

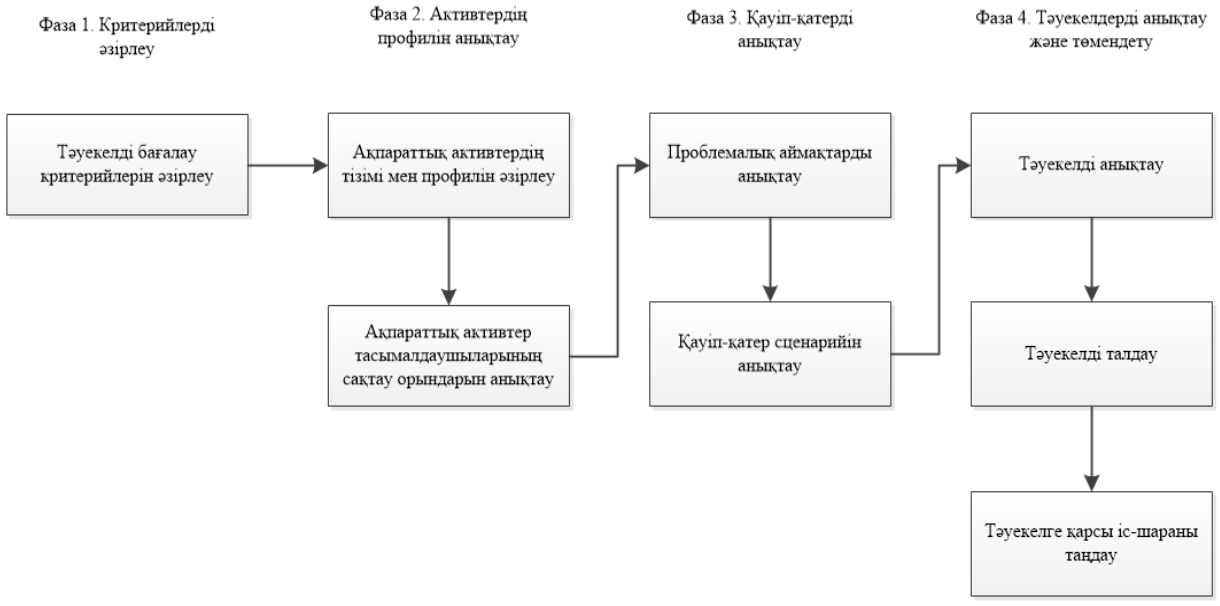
Бұл әдістемеде кейбір кемшіліктер бар. Мәселен, әдістеме ұйымда тәуекел талдауын интеграциялауды көздемейді, тәуекелдер мониторингін ұйымдастырумен және тәуекелдерді қайта бағалауды жүргізумен мәселелер бар, қалдық тәуекелдерді басқаруды болжамайды, тәуекелдерді болдырмауға мүмкіндік бермейді.

OCTAVE әдістемесінде тәуекелдерді талдау үшін төрт фазаға біріктірілген сегіз қадамнан тұратын тәсіл ұсынылады (1.2-сурет).

Тәуекелдерді талдау барысында қолданылатын жұмыс парақтары мен сауалнамалары әдістемесінің ағылшын тіліндегі нұсқасынд қамтылған "Introducing OCTAVE Allegro: Improving the Information Risk Assessment Process" сайтында ұсынылған www.cert.org [9].

OCTAVE әдістемесінде негізделген тәуекелдерді талдау тобының іс - қимылдарының жалпы алгоритмін, сондай-ақ тұрақты негізде тәуекелдерді бағалауды ұйымдастыруға және АҚ тәуекелдерінің мониторингіне енгізу бойынша ұсыныстарды қарастырайық.

Бірінші өадамда АҚ тәуекелдерін бағалау өлшемдерін, яғни тәуекелді бағалау мәнін және тәуекелдің іске асырылу салдарын белгілеуге мүмкіндік беретін сапалық көрсеткіштердің жиынтығын анықтау қажет. Мұндай критерийлерді енгізбестен ұйымның қандай да бір тәуекелдерге тәуелділігін бағалау мүмкін емес.



1.2 сурет – OCTAVE әдісі бойынша тәуекелдерді талдау кезеңдері

Мұндай өлшемдер ретінде кәсіпорында қолданылатын қауіпсіздік талаптары, АҚ инвестициялар мен шығындар деңгейі, қозғалған ақпараттық активтер мен т. б. стратегиялық құндылығы мен маңыздылығы пайдаланылуы мүмкін.

Бірінші қадамда ұйым үшін аса басым және елеулу АҚ-ға әсер етуді белгілеу қажет (мысалы, құпия ақпараттың шығуы, нарықтағы беделге нұқсан келуі, әріптестер мен клиенттер арасындағы беделге нұқсан келуі, қызметкерлердің денсаулығы мен физикалық қауіпсіздігі). Тәуекелдерді бағалау критерийлері ұйымның қызметі саласында бар ақпараттық тәуекелдерді қамтуды көрсетуі тиіс. Критерийлер тәуекелді іске асыру салдарының диапазонын белгілейді: "төмен", "орташа" және "жоғары".

Екінші қадам ақпараттық активтердің тізімін құрудан және олардың бейінін анықтаудан басталады. Профиль - бұл активтің оның бірегей ерекшеліктерін, қасиеттерін, құнын сипаттайтын ақпарат. Профильдеу активтің "шекарасын" және оған қойылатын қауіпсіздік талаптарын нақты анықтауға мүмкіндік береді. Профиль әрбір актив үшін жасалады және жеке парақта сипатталады.

Бұдан әрі 3-ші қадам орындалады. Ақпараттық активтер тек ұйымның өзінде ғана емес, одан тыс жерлерде де сақталуы мүмкін. Мысалы, ұйым өз инфрақұрылымына қызмет көрсетуге басқа да жеткізуші ұйымдарға рұқсат бере алады. Егер мұндай қызмет көрсетуші оларға қызмет көрсетуге рұқсат етілген активтердің қауіпсіздік талаптарын орындамаса, онда бұның өзі тәуекелге айналады. Қауіп активті бөгде жерде сақтау, беру немесе өңдеу фактісінде болуы мүмкін және бұл ақпараттық активті қорғауды бұзады.

Осылайша, активтің профилін алу үшін активті сақтаудың, берудің және өңдеудің барлық орындарын, сондай-ақ ол ұйымды тікелей басқару аймағында орналасқан ба жоқ па анықтау маңызды.

Үшінші қадамда талдау тобы активтің картасын жасайды, онда осалдықтың нүктелері немесе активтің қорғалуына кепілдік бере отырып толығымен бақылауға болатын барлық сақтау, беру және өңдеу орындары көрсетіледі.

Активтің сақталатын орны ретінде техникалық құралдар, бағдарламалық қамтамасыз ету, қағаз жүзіндегі немесе ұйымының қызметкері болуы мүмкін. Бұл жерде адамдар өте маңызды, өйткені қорғалған ақпаратты алған кезде олар активтің "контейнеріне" айналады. Мұндай тәуекелдерді уақтылы анықтау қажет.

4-ші қадамда ұйымның АҚ-дағы мәселелік салалар анықталады. Бұл қадамның мақсаты барлық ықтимал қауіптердің толық тізімін құру емес, аналитик үшін бірден айқын қауіптерді жедел анықтау болып табылады.

5-ші қадамда анықталған проблемалық облыстар негізінде қауіп-қатерлердің сценарийлері жасалады, оларды көзбен шолып ағаш түрінде тиімді ұсыну қажет, онда қауіптерді неғұрлым сенімді қарау мақсатында әрбір тармақ әрбір ақпараттық актив үшін қаралады.

Әрбір тармақ бойынша қауіп сценарийін анықтауды жеңілдету үшін сауалнама сауалнамаларын пайдалану қажет. Бұл қадам сондай-ақ қауіп-қатерді іске асыру ықтималдығын ескеруге мүмкіндік береді, бұл қауіп-қатерді азайту жөніндегі іс-шараларды неғұрлым кейінгі қадамдарда әзірлеуге көмектеседі.

Әдетте, бұл жағдайда сапалық шкала және қауіп - қатерді іске асыру ықтималдығының үш деңгейі (жоғары, орташа және төмен) қолданылады.

6-шы қадамда қауіп-қатерлерді және оларды іске асырудың салдарларын анықтағаннан кейін АҚ тәуекелдерін анықтайды. Тәуекел ұйымға немесе активке қалай әсер ететінін анықтау қажет, бұл ретте тәуекел ұйым немесе активтің өзі үшін оның маңыздылығын бағалау үшін әрбір актив үшін анықтайды.

7-қадамда қауіп-қатерді іске асыру кезінде ұйымға келтірілетін залалдың сандық мөлшері анықталады. Бұл олардың басымдылығы бойынша тәуекелдерді анықтауға мүмкіндік беретін салыстырмалы баға. Мысалы, егер компанияның нарықтағы беделі аса маңызды болса, онда бірінші кезекте осы мәселенің тәуекелдерін төмендету керек.

Соңғы қадамда ұйым үшін олардың басымдығын ескере отырып, белгілі бір тәуекелдерге қарсы іс-шаралар таңдалады.

Практикалық қолдану тұрғысынан OCTAVE Allegro әдісінің келесі артықшылықтарын атап өтуге болады:

- тәуекелдерді талдау және бағалау процесінің қарапайымдылығы мен ашықтығы процесті ең аз мерзімде жүзеге асыруға кірісуге мүмкіндік береді.;
- итеративтік тәсіл ұйымның өзекті қажеттіліктеріне және осы үшін қажетті ресурстардың қол жетімділігіне байланысты ақпараттық қауіпсіздік тәуекелдерін талдаудың тереңдігін біртіндеп арттыруға мүмкіндік береді;
- тәуекелдерді талдау мен бағалауды орындауға кететін еңбек шығындарының төмендігі осы процестерді ең аз ресурстарды тартумен және қысқа мерзімде іске асыруға мүмкіндік береді;
- қосымша материалдардың тәуекелдерін талдау процесін қолдайтын болуы нәтижелердің қайталану мүмкіндігін қамтамасыз етеді, процестерді тікелей орындаушыларға жүзеге асыруды жеңілдетеді.

Бұл ретте OCTAVE Allegro әдістемесіне келесі кемшіліктер тән:

- қауіптер, осалдықтар, салдарлар, ақпараттық қауіпсіздікті қамтамасыз ету шаралары каталогы сияқты егжей-тегжейлі көмекші материалдардың болмауы тәуекелдерді талдау және басқару жөніндегі іс-шараларды тікелей орындаушыларда арнайы білім мен біліктілікті талап етеді.;
- ақшалай тәуекелдерді бағалау мүмкіндігінің болмауы ақпаратты қорғау құралдары мен әдістерін енгізуге қажетті инвестициялардың техникалық-экономикалық негіздемесін есептеу кезінде ақпараттық қауіпсіздік тәуекелдерін бағалау нәтижелерін пайдалануды қиындатады.

OCTAVE әдісі ақпараттық қауіпсіздік тәуекелдерін сапалы бағалау үшін кеңінен қолданылады. Ең жоғары дәрежеде ол тәуекелдерді басқару

процестерін бастапқы енгізуді жүзеге асыратын, барлық ұйымға ақпараттық қауіпсіздік тәуекелдерін талдау және басқару процестерін енгізу үшін ресурстары жоқ және жоғарғы деңгейдегі аса қиын тәуекелдерден төменгі деңгейдегі тәуекелдерге ақпараттық қауіпсіздік тәуекелдерін біртіндеп декомпозициялауға қажеттілігі бар ұйымдарға қолайлы. Әдіс барлық ұйымға тәуекелдерді басқару процестерін итерациялық таратуға мүмкіндік береді [6].

1.3.6 CORAS

Қауіпсіздік тәуекелдерін талдаудың Coras әдістемесі тәуекелдер мен қатерлерді модельдеуге арналған құрал болып табылады. CORAS әдістемесі UML моделін қолданады (модельдеудің біріздендірілген тілі – бағдарламалық қамтамасыз етуді әзірлеу саласында объектілі модельдеуге арналған графикалық сипаттама тілі). Аралық нәтижелерді құжаттау үшін және ақпараттық қауіпсіздік тәуекелдерін талдау туралы толық қорытындыларды ұсыну үшін UML ішіне енгізілген CORAS арнайы диаграммалары пайдаланылады. Бағалау нәтижелерінің визуализациясы граф түрінде беріледі. Бағдарламалық құралдар еркін таратылады.

CORAS әдістемесі – бұл құжаттауды, тәуекелді модельдеу арқылы талдау нәтижелері туралы есептерді жасайтын бағдарламалық құрал.

Тәуекелдерге қатысты барлық жұмыстар келесі рәсімдер арқылы жүргізіледі:

- дайындық іс-шаралары-талдау объектісі туралы жалпы мәліметтерді жинау;
- талдау қажет объектілерді клиенттің ұсынуы;
- аналитиктің тапсырмаларды егжей-тегжейлі сипаттауы;
- талдау үшін ұсынылған құжаттардың дұрыстығы мен толықтығын тексеру;
- аналитик басқаратын тәуекелдерді анықтау бойынша іс-шаралар (мысалы, семинар түрінде жүзеге асырылады);
- ақпараттық қауіпсіздік инциденттерінің ықтималдығы мен салдарын бағалау;
- қолайлы және алдағы уақытта қайта талданы, жойылуы мүмкін тәуекелдерді анықтау;
- ақпараттық қауіпсіздік саласындағы инциденттердің ықтималдығын және салдарын қысқарту мақсатында қауіптерді жою.

CORAS "ақпараттық қауіпсіздік саласында қызметкерлердің хабардарлығын арттыру бағдарламасы"сияқты тәуекелдерді басқару бойынша тиімді шараларды көздемейді. Мұндай бағдарлама компания қызметкерлерінің осы саладағы корпоративтік талаптарға және ақпараттық жүйелерді қауіпсіз пайдалану ережелеріне қатысты хабардар болмауы себебінен ақпараттық қауіпсіздік режимін бұзумен байланысты АҚ тәуекелдерін төмендетуге мүмкіндік береді. Сондай-ақ CORAS-да тәуекелдерді бағалауды жүргізу мерзімділігі және олардың шамаларын

жаңарту қарастырылмаған, бұл әдістеме бір жолғы бағалауды орындау үшін жарамды және тұрақты пайдалануға жарамсыз болып табылады [10].

CORAS-тың жақсы жағы осы әдістемені іске асыратын бағдарламалық өнім тегін таратылады және орнату және қолдану үшін маңызды ресурстарды талап етпейді.

1.3.7 Microsoft Security Assessment Tool

Microsoft Security Assessment Tool (MSAT) ақпараттық технологиялық ортаның осалдығын бағалауда ұйымдарға көмек көрсетуге арналған қауіпсіздікті бағалау құралы. Ол басымдықтар бойынша қойылған мәселелердің тізімін және осы қатерлерді азайту жөніндегі ұсыныстардың тізімін қарастырады, содан кейін инфрақұрылымның осы қатерлерге жауап беру қабілетін ұдайы тексеруге мүмкіндік береді.

MSAT қауіпсіздік деңгейін өлшеудің біртұтас тәсілін қолданады және қызметкерлер, процестер мен технологиялар сияқты тақырыптарды қамтиды. MSAT негізгі мүмкіндіктері:

- қауіпсіздік деңгейі туралы түсінікті, толық және тұрақты хабардарлықты ұсынады;
- салалық стандарттарға сәйкес келетін қорғаныс инфрақұрылымын сипаттайды;
- негізгі көрсеткіштерді қол жеткізілген жетістіктермен салыстыратын толық, тұрақты есептерді ұсынады;
- тексерілген ұсыныстар мен қауіпсіздікті жақсарту бойынша басымдықтар бойынша қойылған іс-әрекеттерді сипаттайды;
- салалық тиістілігіне байланысты Microsoft компаниясынан құрылымдалған ұсыныстар береді.

MSAT сауалнамасы инфрақұрылымды, қосымшаларды, операцияларды және қызметкерлерді қамтитын 200-ден астам сұрақтан тұрады. Оларға қатысты сұрақтар жауаптар мен ұсыныстар ISO 27000 және NIST-800 сияқты жалпы қабылданған практикалық ұсыныстардан, стандарттардан шығарылады, сондай-ақ Microsoft сенімді есептеу тобының және басқа сыртқы қауіпсіздік көздерінің ұсыныстары мен нұсқауларын қамтиды.

Компанияның бизнес-моделі туралы сұрақтар сериясынан бастап MSAT белгілеген BRP-дің салалық және бизнес-үлгілерге сәйкес компанияның іс-қимылдарына байланысты тәуекелді өлшей отырып, бизнес-тәуекел профилін (BRP) құрады. Сұрақтардың екінші сериясы уақыт өте келе компания ашқан қауіпсіздік шараларының тізімін жасауға арналған.

Қауіпсіздік шаралары бірлесіп, қауіпсіздік деңгейлерін құрайды, бұл қауіпсіздік пен нақты осалдықтардан үлкен қорғауды қамтамасыз етеді. Әр деңгей терең қорғаныс стратегиясына ықпал етеді. Олардың қосындысы терең қорғаныс индексі (DiDI) деп аталады. Содан кейін BRP және DiDI инфрақұрылым, қосымшалар, операциялар және адамдарға әсер етуі бойынша қауіп-қатерлердің таралуын өлшеу үшін салыстырылады

Жоғарыда аталған MSAT көрсеткіштерінен басқа, ұйымның қауіпсіздік деңгейін өлшейді. Қауіпсіздік деңгейі қауіпсіздікті қамтамасыз етудің жоғары тиімді және тұрақты әдістерін дамытуды білдіреді. Төмен деңгейде қорғау әдістерінің шектеулі саны қолданылады. Жоғары деңгейде компанияға алдын алу шараларын қолдануға және қажет болған жағдайда одан да тиімді әрі келісілген әрекет етуге мүмкіндік беретін қалыптасқан және тексерілген процестер қолданылады.

MSAT нақты технологиялардың немесе процестердің терең талдауын ұсыну үшін емес, ортада әлеуетті тәуекел облыстарын кеңінен қамтуға арналған. Сондықтан, құрал қолданылған қауіпсіздік шараларының тиімділігін бағалай алмайды. Оны аса назар аударуды талап ететін нақты салаларда шоғырландыру үшін базалық көрсеткіштерді әзірлеуге көмектесетін алдын ала басшылық ретінде пайдалану керек. MSAT-ты тұрақты түрде қолдануға болады.

Кіріс деректері. Жұмыс барысында АҚ мәселелеріне жауапты аналитик рөлін атқаратын пайдаланушы екі сұраныс тобымен жұмыс істейді. Олардың біріншісі компания осы салада және таңдалған бизнес-модель жағдайында тап болатын бизнес үшін тәуекелді бағалауға арналған. Бизнес үшін тәуекел профилі құрылады.

Тәуекелді талдау кезеңінде активтерді сәйкестендіру жүргізіледі, олардың сапалы жіктелуі ұсынылады (бизнеске жоғары, орташа және төмен әсер етуі бойынша), сондай-ақ қауіптер мен осалдықтар тізімі айқындалады.

Тәуекелді бағалау үшін сапалық және сандық үш деңгейлі шкалалар (жоғары, орташа және төмен әсер ету) қолданылады [11].

Бұл бағалау сұрақтар, қарсы іс-шаралар мен ұсыныстарды қамтитын 50-ден 500-ге дейінгі үстел компьютерлері бар орта кәсіпорындарға (ұйымдарға) арналған. Ол нақты технологияға немесе процеске терең талдау жүргізудің орнына ортада ықтимал қауіп-қатер салаларын кеңірек қорғауды болжайды. Таким образом, полученные сведения следует использовать как предварительное руководство, позволяющее сосредоточить внимание на определенных областях, требующих более пристального изучения. Осылайша, алынған ақпаратты алдын-ала нұсқаулық ретінде пайдаланылуы керек, бұл сізге мұқият зерттеуді қажет ететін белгілі бір салаларға назар аударуға мүмкіндік береді.

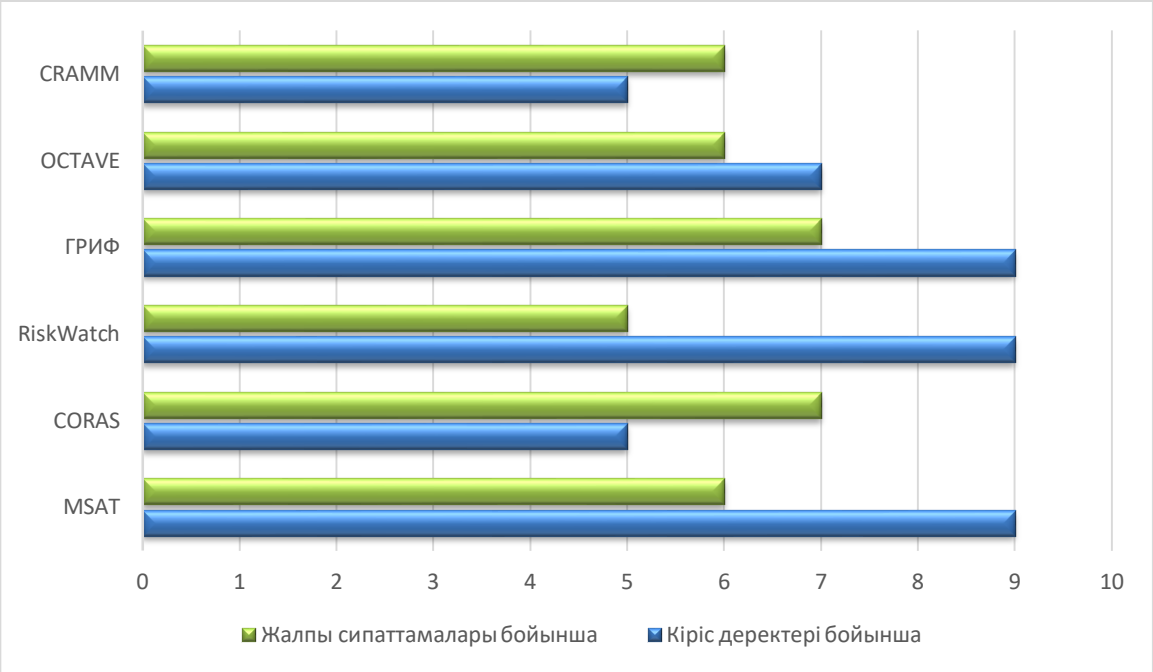
1.4 Қауіптер мен тәуекелдерді бағалау алгоритмдерін, әдістемелерін салыстырмалы талдау

IT саласы өте тез дамып келеді, күн сайын тәуекелдерді талдаудың жаңа әдістері пайда болуда. Нарықта көптеген анализаторлар мен шектеулі функциялы қарапайым антивирустар бар. Ақпараттық қауіпсіздікті бағалау және тәуекелдерді анықтау үшін көптеген әдістерді зерттей отырып, деректерді салыстырмалы талдау жасауға болады.

Шағын және орта бизнес ұйымдары үшін АҚ тәуекелдерін бағалаудың неғұрлым лайықты әдістемесін айқындау үшін ұйымдардың қажеттіліктерін,

сондай-ақ олардың мүмкіндіктеріне сәйкес келетін критерийлер бойынша жоғарыда қарастырылған әдістемелерге талдау жүргізілді.

АҚ тәуекелдерін бағалау әдістемелерінің салыстырмалы талдауы (1.1-кесте) берілген және қорытынды диаграммада (1.3-сурет) көрсетілген.



1.3 сурет – АҚ тәуекелдерін бағалау әдістемелерін салыстырмалы талдау

Талдау екі бағалаудың жиынтығы бойынша орындалды-жалпы сипаттамалар бойынша бағалаудың ең жоғарғы мәні және кіріс деректері бойынша бағалаудың ең төменгі мәні.

Бұл таңдау ұйым үшін әдістемені пайдаланудың қарапайымдылығы оның бағасы және бағалау нәтижелерінің толықтығы неғұрлым басым критерий болып табылатындығынан, ал әдістемені пайдалану үшін кіріс деректерінің көп болуы оны қолдануды қиындатуынан туындайды.

Ұйымдар үшін АҚ тәуекелдерін бағалау әдістемелерін салыстырмалы талдау нәтижелері 1.1-кестеде келтірілген.

1.1-кесте – Ақпараттық қауіпсіздік тәуекелдерін бағалау әдістерін салыстырмалы талдау

Салыстыру критерийлері	Әдістеме атауы					
	ГРИФ	MSAT	OCTAVE	RiskWatch	CORAS	CRAMM
Жалпы сипаттамалары						
Өндіруші шағын және орта кәсіпорындар үшін әдісті ұсынады	0	1	0	0	1	1
Әдістеме қызметтің түрлі салаларын ұйымдастыруға арналған	1	0	1	1	1	1
Пайдаланудың қарапайымдылығы	1	1	1	0	1	0
Тегін таратылады	0	1	1	0	1	0
Сандық бағалау	1	0	0	1	0	1
Сапаны бағалау	1	1	1	1	1	1
Қызметкерлердің хабардарлығын арттыру	1	1	1	1	1	1
Тұрақты пайдалануға жарамдылығы	1	1	1	1	0	1
Тәуелсіз бағалауды пайдалану	1	0	0	0	1	0
Барлығы:	7	6	6	5	7	6
Кіріс деректері						
Ресурстар	1	1	1	1	1	1
Ресурстардың құндылығы	1	1	1	1	1	1
Қауіптер	1	1	1	1	1	1
Осалдықтар	1	1	1	1	1	1
Қарсы іс-шараларды таңдау	1	1	0	1	1	1
Қауіпсіздік саласындағы базалық талаптар	0	0	1	1	0	0
Шығындар	0	0	0	1	0	0
Ақпараттық қауіпсіздік шаралары	0	1	1	1	0	0
Қауіптердің туындау жиілігі	0	0	0	1	0	0
Желілік жабдықтар	1	1	1	0	0	0
Ақпарат түрлері	1	1	0	0	0	0
Пайдаланушылар топтары	1	1	0	0	0	0
Ақпаратты қорғау жүйелері	1	0	0	0	0	0
Барлығы:	9	9	7	9	5	5

1.2-кесте – АҚ тәуекелдерін бағалау әдістемелерін салыстырмалы талдау нәтижелері

Әдістеме атауы	Талдау нәтижесі	Қолданылатын әдістер мен стандарттар
ГРИФ	Әдістеме тәуекелдердің сапалық да, сандық да бағалауын пайдаланады, тәуекелдерді компания қабылдай алатын шарттарды анықтайды. Бұл әдістеме мемлекеттік секторға бағдарланған және ШОБ ұйымдарының пайдалануы үшін бейімделмеген.	Ақпараттық ағындардың моделін талдау
MSAT	Тәуекелдерді сапалық бағалайды. Негізгі көрсеткіштері тәуекел профилі. Ақпаратты қорғау жүйесіне инвестициялардың тиімділігін бағалауға мүмкіндік береді.	ISO/IEC 27002, FRAP
OCTAVE	Әдістеме АҚ тәуекелдеріне сандық баға бермейді, пайдалануға қатысты қарапайым, қызметтің әртүрлі ерекшелігі бар ұйымдар үшін қолайлы. Талдау жүргізу үшін кіріс деректерінің орташа санын пайдаланады.	OCTAVE
RiskWatch	Әдістеме АҚ тәуекелдерін сандық және сапалық бағалауды пайдаланады, пайдалану оңай, өте икемді. АҚ тәуекелдерін талдау кезінде әкімшілік және ұйымдастыру факторларының есебін пайдаланбайды, ал бұл факторлар ұйымдарға елеулі әсер етеді.	ISO 27002
CORAS	Бағдарламалық құрал тегін таратылады, орнату және қолдану үшін маңызды ресурстарды талап етпейді. Әдістеме пайдалану оңай және арнайы білімді қажет етпейді. Әдістеменің кемшілігі АҚ тәуекелдеріне бағалау жүргізу мерзімділігі қарастырылмаған.	CORAS
CRAMM	CRAMM әдістемесі сандық және сапалық талдау әдістерін үйлестіретін тәуекелдерді бағалаудың кешенді тәсілін қолданады. Әдіс әмбебап болып табылады және ірі және шағын ұйымдар үшін де, үкіметтік және коммерциялық сектор үшін де қолайлы. Аудитордың арнайы дайындығы мен жоғары біліктілігін талап етеді	CRAMM, ISO 27002

1.3-кесте – АҚ тәуекелдерін басқару үшін бағдарламалық құралдарды салыстыру

Салыстыру критерийлері	CRAMM	ГРИФ	RiskWatch	CORAS	MSAT
Тәуекелдер					
Тәуекел санаттарын қолдану	+	+	+	+	+
Максималды рұқсат етілген тәуекел түсінігін пайдалану	+	+	+	+	+
Тәуекелдерді азайту бойынша іс-шаралар жоспарын дайындау	+	+	+	–	+
Басқару					
Басшыны хабардар ету	+	+	+	+	+
Тәуекелдерді азайту бойынша жұмыс жоспары	–	+	+	–	+
Оқу, семинарлар, кездесулерді қамтиды	–	+	+	–	+
Бизнес тәуекелдерін / операциялық тәуекелдерін бағалау	–	+	+	+	–
Ұйымдастыру деңгейінде тәуекелдерді бағалау	+	+	–	+	+
Техникалық деңгейде тәуекелдерді бағалау	+	+	+	+	+
Тәуекелдерді төмендетудің ұсынылатын тәсілдері					
Тәуекелді айналып өту (болдырмау)	–	+	+	–	–
Тәуекелді төмендету	+	+	+	+	+
Тәуекелді қабылдау	–	+	–	+	+
Процестер					
Материалдық активтер	+	+	+	+	+
Материалдық емес активтер	+	+	+	+	+
Қауіптер	+	+	+	+	+
Активтердің құндылығы	+	+	+	+	+
Осалдықтар	+	+	+	+	+
Қауіпсіздік шаралары	+	+	+	–	+
Ықтимал залал	+	+	+	+	+
Қауіптерді іске асыру ықтималдығы	+	+	+	+	+
Қарастырылатын тәуекел түрлері					
Бизнес-тәуекелдер	–	+	+	+	–
Заңнамалық актілерді бұзумен байланысты тәуекелдер	–	+	–	–	+
Технологияларды пайдаланумен байланысты тәуекелдер	–	+	–	+	+
Коммерциялық тәуекелдер	+	+	+	+	+
Үшінші тараптармен байланысты тәуекелдер	+	+	+	+	+
Қызметкерлердің тәуекелі	+	+	–	+	+
Тәуекелді өлшеу тәсілдері					
Сапалы бағалау	+	+	+	+	+
Сандық бағалау	–	+	+	–	–
Басқару тәсілдері					
Тәуекелдерді сапалы саралау	+	+	+	+	+
Тәуекелдерді сандық саралау	+	+	+	+	+
Тәуелсіз бағалауды қолдану	–	+	–	+	+
Инвестицияларды қайтару есебі	–	+	–	–	–

1.3-кестенің жалғасы

Қауіпсіздік шараларының әртүрлі түрлері арасындағы оңтайлы балансты есептеу					
Алдын алу шаралары	−	+	+	−	+
Анықтау шаралары	−	+	+	−	+
Түзету бойынша шаралар	−	+	+	−	+
Қалпына келтіру бойынш	−	+	+	−	+
Басқару тәсілдерін интеграциялау	−	+	−	−	−
Басқару тәсілдерінің мақсатын сипаттау	−	+	+	+	+
Қалдық тәуекелдерді қабылдау тәртібі	+	+	−	−	+
Қалдық тәуекелдерді басқару	−	+	−	−	+
Тәуекелдер мониторингі					
АҚ шараларының тиімділігі мониторингін қолдану	−	+	+	−	−
Тәуекелдерді төмендету бойынша іс-шаралар өткізу	−	+	+	−	+
АҚ саласындағы инциденттерге әрекет ету процесін пайдалану	−	+	−	−	+
Тәуекелдерді бағалау нәтижелерін құрылымдық құжаттау	−	+	+	−	+

Талдауларды қорытындай келе, қаралған әдістемелер "Тәуекелдер" және "Процестер (тәуекел элементтерін пайдалану)" топтарының критерийлеріне жақсы сәйкес келеді, бірақ олардың кейбіреулері (CRAMM, CORAS) "Мониторинг" және "Басқару" бөлімдеріне, сондай-ақ "Процестер" бөлімдеріне сәйкес кемшіліктерге ие.

Әдістемелердің барлығы (ГРИФ, RiskWatch, MSAT) тәуекелдерді қайта бағалау кестесін жасау жөнінде толық ұсыныстар бере бермейді. Орташа мөлшердегі компаниядағы тәуекелдер деңгейін тек бір жолғы бағалауды орындау қажет болған жағдайларда CORAS әдістемесін пайдалануды ұсыну орынды. Техникалық деңгейде мерзімді бағалау негізінде тәуекелдерді басқару үшін ең жақсы CRAMM.

CRAMM, FRAP, RiskWatch, Microsoft Security Assessment Tool (MSAT), ГРИФ әдістемелерін пайдалану үшін жоғары біліктілік мамандардың қажеттілігін (CRAMM, FRAP, ГРИФ) және тәуекелдерді бағалау процесінің еңбек сыйымдылығы мен ұзақтығына (MSAT) байланысты қолдану қиындықтарын көрсетті. Сонымен қатар, бағдарламалық өнімнің жоғары құнын атап өту керек (RiskWatch). Microsoft Security Assessment Tool және RiskWatch әдістемелерін тұрақты бағалау негізінде АҚ тәуекелдерін басқаратын және тәуекелдерді азайту жөніндегі іс-шаралардың дұрыс жоспарын қажет ететін ірі компанияларда пайдалану үшін қолайлы.

АҚ тәуекелдерін талдау және бағалау үшін мамандандырылған бағдарламалық құралдар саласындағы соңғы әзірлемелерді бірнеше сөзбен сипаттау керек, оның ішінде олардың кейбіреулері шағын және орта бизнеске арналған [12].

- RA2 art of risk (AEXIS Security Consultants). RA2 art of risk-да түсіну үшін қарапайым процесс әдісі іске асырылған. Тәуекелдерді тиімді бағалау және басқару үшін бастапқы ақпаратты жинау ұйымда әр түрлі ақпарат

көздерінен алынуы қажет, осы мақсатта RA2 art of risk-ке RA2 Information Collection Device арнайы модулі қосылған.

Ақпараттық қауіпсіздікті басқару жүйесін жобалау және енгізу процесі аяқталғаннан кейін RA2 art of risk нәтижелерді сақтау үшін мұрағат жасауға мүмкіндік береді, бұл АҚ тәуекелдерін кейінгі бағалау үшін өте маңызды болып табылады. RA2 заманауи бизнес үшін ақпараттық тәуекелдерді басқару бойынша шешімдер қабылдауды қолдаудың тиімді жүйесі болып табылады.

- vsRisk – ISO 27001: 2005 Compliant Information Security Risk Assessment Tool (IT Governance). ISO/IEC 27001 және BS 7799-3 стандарттарының талаптарына сәйкес ақпараттық қауіпсіздік тәуекелдерін бағалауға арналған бағдарламалық қамтамасыз ету.

vsRisk – қазіргі заманғы халықаралық стандарттарға сәйкес әзірленген тәуекелдерді бағалауға арналған жаңа және бірегей құрал. Бизнес үшін құпиялылықтың, тұтастықтың және ақпараттың қол жетімділігінің бұзылу тәуекелдерін, сондай-ақ заңнаманы және келісімшарттық міндеттемелерді сақтау тұрғысынан бағалауға мүмкіндік береді, ISO/IEC 27001, ISO/IEC 17799, ISO/IEC TR 13335-3:1998, NIST SP 800-30 сияқты халықаралық стандарттарды қолданады. vsRisk BS7799-3 талаптарына сәйкес келетін қауіптер мен осалдықтардың интеграцияланған, тұрақты жаңартылып отыратын деректер базасын қамтиды.

- Proteus (InfoGov). Proteus – тәуекелдердің бизнеске әсерін талдайтын және бағалайтын, бизнестің үздіксіздігін, инциденттер мен активтерді басқару құралдарын қамтитын қуатты жүйе. Жүйе ұйымдарда пайдаланылуы мүмкін бір пайдаланушы нұсқасынан, ірі корпорацияларда ақпараттық қауіпсіздікті басқаруға мүмкіндік беретін көп пайдаланушы нұсқасына дейін масштабталады.

Жүйеде жүргізілетін барлық әрекеттер аудит журналында тіркеледі. Жүйе ISO/IEC 27001, ISO/IEC 17799, PCI, NIST және басқа да стандарттарды қолдауды қамтамасыз етеді. Proteus-да бизнес әсерін талдау және АҚ тәуекелдерін бағалау үдерістері арасында деректерді бірлесіп пайдалану жүзеге асырылды. Сонымен қатар, графикалық пішінде нақты уақытта нәтижелерді визуализациялаудың қуатты құралдары бар.

- РискМенеджер тәуекелдерді басқаруды, аудит жүргізуді, бақылауды, банктік және басқа да инфрақұрылымдар мен бизнес-процестердің қауіпсіздігін автоматтандыру жүйесі.

РискМенеджер талдау жүйесі келесі процесстерді автоматтандырады:

- қауіптер, потенциалды қауіптерді бағалау, объектілер, ұйымдық құрылымдар, бизнес-процестердің модельдерін құруды;
- қорғау модельдерін, қорғаныс құралдарының жүйенің қауіпсіздігін өзгертуге әсер ету модельдерін құруды;
- қорғау шараларының неғұрлым тиімді кешендерін таңдауды;
- қауіпсіздікті бұзу тәуекелдерін есептеуді;
- қорғау іс-шаралары кешендерін қолданғаннан кейін қалдық тәуекелдерді есептеуді;

- жүйенің қауіпсіздігіне қойылатын талаптардың өзектілік, толықтылық сапасын бақылауды;

- қайталаудың болмауы, ұйымның бәсекеге қабілеттілігіне әсер ету және қауіпсіздікке қойылатын талаптар жүйесіне өзгерістер енгізуді.

ISO/IEC 17799 "Ақпараттық технологиялар – ақпараттық қауіпсіздікті басқарудың практикалық ережелері», ISO/IEC 27005 "Ақпараттық қауіпсіздік менеджмент жүйесі. Талаптар", ГОСТ Р ИСО/МЭК 15408-2012" Ақпараттық технологиялар қауіпсіздігін бағалаудың жалпы критерийлері» стандарттарына сәйке аудит, мониторинг, бақылау және ұйымның және бизнес-үдерістердің қауіпсіздігінің ішкі аудитін жүргізуге болатын құрал [13].

Қорытындылай келе, ақпараттық қауіпсіздік тәуекелдерін басқару рәсімін жүргізу қажеттілігі күмән тудырмайды және ұйымдар АҚ тәуекелдерін бастапқы бағалау нәтижелерін ғана емес, оларды төмендету бойынша ұсыныстарды да, сондай - ақ мұндай бағалаудың қымбат емес құралдарын да қолдануы қажет. Мәселе, АҚ тәуекелдерін талдау және бағалау процесстерін жүргізу үшін, осы мақсаттар жеті үшін бағдарламалық құралдарды сатып алуға инвестициялардың қажеттігіне және процесстерді жүргізу үшін білікті мамандардың болуына келіп тіреледі. АҚ жүйесіне бөлінетін инвестициялар тұтастай алғанда ұйымның қорғалатын активтерінің құнын (активтер құнының 10-20%) негізге ала отырып айқындалады.

Бөлім бойынша қортыныды: бірінші тараудың негізгі мақсаты - зерттеу аймағын және зерттеу объектісін зерттеу болды.

Бұл тарауда ақпараттың өзекті қауіп-қатерлерін анықтау, тәуекелдерді бағалау нәтижесінде алынған деректерге сүйене отырып, тәуекелдердің деңгейін төмендету үшін қарсы іс-шаралар жасалыну қажеттілігі анықталды.

АҚ тәуекелдерін бағалаудың қазіргі қолданыстағы әдістері сипатталды және талданды. Оларға салыстырмалы талдау жүргізілді және АҚ тәуекелдерді басқарудың қандай да бір әдістемесін енгізу туралы шешім қабылдағанға дейін ол ұйымның бизнес-қажеттіліктерін, оның ауқымын жеткілікті түрде толық ескеруі керек, сондай-ақ үздік әлемдік практикаларға сәйкес келетін және процестер мен талап етілетін іс-әрекеттердің егжей-тегжейлі сипаттамасы болуы керек деген тұжырым жасалынды.

2 АҚ қауіп-қатерлері мен тәуекелдерін бағалау әдістемесі

"Қауіп-қатерлер мен осалдықтарды талдау моделі"-не сәйкес ақпарат тәуекелін бағалау үшін ақпараттық жүйеге әсер ететін барлық қауіптерді және олар іске асыру мүмкін болатын осалдықтарды талдау қажет.

Ақпараттық жүйенің иесі енгізген деректерді негізге ала отырып, компанияның ақпараттық жүйесі үшін өзекті қауіптер мен осалдықтар моделін құруға болады. Алынған модельдің негізінде әрбір ресурсқа ақпараттық қауіпсіздік қауіптерінің іске асыру ықтималдығына талдау жүргізіледі және осыған орай тәуекелдер есептелген болады.

Алгоритм жұмысының екі режимі бар:

- бір негізгі қауіп;
- үш негізгі қауіп.

АҚ тәуекелдерін талдау ұйымның ақпараттық жүйесінің (АЖ) моделін құру көмегімен жүзеге асырылады.

АЖ иесіне алдымен өз желісінің архитектурасын сипаттау қажет:

- бағалы ақпарат сақталатын барлық ресурстар (сервер, жұмыс станциясы, мобильді компьютер және т. б.);
- ресурстың маңыздылығы – ақпараттық жүйе үшін ресурстың маңыздылық дәрежесі, яғни ресурстың ақпараттық қауіпсіздік қауіптері іске асқанда оның қаншалықты ақпараттық жүйенің жұмысына әсер ететінін білдіреді.
- ресурстарға әсер ететін қауіптер;
- қауіптер жүзеге асырылатын осалдықтар;
- осы осалдық арқылы қауіптің іске асу ықтималдығы;
- осы осалдық арқылы қауіптің іске асу маңыздылығы.

Тәуекелді бағалау үшін ақпараттық жүйеге әсер ететін барлық қауіп-қатерлер және осы қауіптер жүзеге асырылатын осалдықтар талданады және соның нәтижесінде тәуекелдер есептелінеді [14].

Әдістемені меңгеру кезінде мысал ретінде ақпараттық жүйенің қорғалу нысандарының (активтерінің) тәуекелдерін есептейміз.

- қызметкер;
- серверлер;
- коммерциялық құпияны құрайтын мәліметтерді өңдейтін қызметкерлердің автоматтандырылған жұмыс орны (АЖО);
- ақпарат тасымалдаушылар.

Қорғалатын активтердің негізінде АҚ-ның аса маңызды қауіптері мен осылдықтарын анықтаймыз. Олардың тізімі 2.1-кестеде берілген.

2.1-кесте – Активтердің қауіптері мен осалдықтар тізімі

Ресурс	Қауіп-қатер	Осалдық
Қызметкер	Коммерциялық құпияны құрайтын ақпаратты жария ету, өзгерті, жою, ұрлау	Қорғауға жататын ақпаратты жарияламау туралы келісімді сақтамау
		Коммерциялық құпияны қорғау жөніндегі құжаттардың, регламенттердің болмауы немесе өзекті болмауы
	Қызметкерлердің АЖО-да сақталатын ақпаратты түрлендіруі, жоюы	Коммерциялық құпия өңделетін ғимаратқа (бөлмеге) кіру регламентінің болмауы
		Уәкілетті емес қызметкерлердің АЖО-нан қорғауға жататын ақпаратты модификациялауға немесе жоюға тыйым салудың болмауы
Сервер	Сервер орналасқан бөлмеге рұқсатсыз кіру	Өткізу режимін бұзу
		Ғимараттың күзет сигнализациясының болмауы
		Ғимаратқа кіру регламентінің болмауы
	Серверде сақталған деректерге рұқсатсыз қол жеткізу	Рұқсат етілмеген қол жеткізуді жасай алатын бағдарламаның болуы
		Жүйедегі зиянды бағдарламаның болуы
Коммерциялық құпияны құрайтын мәліметтерді өңдейтін қызметкерлердің АЖО	Қызметкерлердің АЖО-ға рұқсатсыз кіруі	Рұқсат етілмеген қол жеткізуді жасай алатын бағдарламаның болуы
		АЖО-ға қол жеткізу регламентінің болмауы
		Жүйедегі зиянды бағдарламаның болуы
		Аппараттық деңгейде авторизациялаудың болмауы
		АЖО корпусын пломбалаудың болмауы
		Өткізу режимін бұзу
Ақпарат тасымалдаушылар	Ақпарат тасымалдаушыларды түрлендіру, жою, ұрлау	Өткізу режимін бұзу
		Коммерциялық құпиясы бар тасымалдаушыларды есепке алудың болмауы

Тәуекелдерді есептеу алгоритмінің жұмыс принципі:

1. Бірінші кезеңде (1) формула бойынша осы осалдық арқылы қауіпті іске асырудың маңыздылығы мен ықтималдығы негізінде қауіптің деңгейі Th есептеледі. Қауіптің деңгейі осы қауіптің іске асырылу ықтималдығын ескере отырып, ресурсқа қаншалықты әсер ететінін көрсетеді.

$$Th = \frac{ER}{100} \cdot \frac{P(V)}{100}, \tag{2.1}$$

мұндағы, $ER-$ пайызбен берілетін қауіптің іске асырылуының маңыздылығы, яғни қауіптің іске асырылуы ресурстың жұмысына қаншалықты әсер ететінін көрсетеді. Құпиялылық, тұтастық және қол жетімділік бойынша қауіп-қатерді іске асырудың маңыздылығынан тұруы мүмкін (ER_c, ER_i, ER_a);

PV – пайызбен көрсетілген қауіптің жыл ішінде осы осалдық арқылы іске асырылу ықтималдығы.

2. Ресурста осы қауіпті жүзеге асыруға болатын барлық осалдықтар үшін қауіп деңгейін CTh есептеу үшін (2) формула қолданылады.

$$CTh = 1 - \prod_{i=1}^{n} (1 - Th_i) \tag{2.2}$$

мұнда Th – осалдық бойынша қауіп деңгейі.

Барлық осалдықтар бойынша қауіп деңгейінің мәні 0-ден 1-ге дейінгі аралықта алынады.

3. Ресурс бойынша қауіптердің жалпы деңгейі $CThR$ (ресурсқа әсер ететін барлық қатерлерді ескере отырып) (3) формула бойынша есептелінеді.

$$CThR = 1 - \prod_{i=1}^{n} (1 - CTh_i) \tag{2.3}$$

мұнда CTh – барлық осалдықтар бойынша қауіп деңгейі.

Қауіптің жалпы деңгейінің мәні 0-ден 1-ге дейінгі аралықта алынады.

4. Ресурс бойынша тәуекел R (4) формулаға сәйкес есептеледі:

$$R = CThR \cdot D \tag{2.4}$$

мұндағы, D – ресурстың ақшалай немесе пайызбен көрсетілген маңыздылығы;

$CThR$ – ресурс бойынша қатерлердің жалпы деңгейі.

Өлшем бірлігі (% немесе ақша және валюта түрі) жобаның баптауларында беріледі. Деңгейлерде қауіп-қатерді берген кезде деңгейлер саны және деңгейлерді бағалау жоба баптауларының деңгейі парағында беріледі (2.2-кесте).

2.2-кесте – Деңгейлердің өлшем бірлігі

Деңгейдің атауы	Деңгейді бағалау, %
1	33,33
2	66,66

3	100

Қолжетімділік (қызмет көрсетуден бас тарту) қауіп төнген жағдайда ресурстың маңыздылығы:

$$D_{жыл} = D_{саг} \cdot T_{\max} \quad (2.5)$$

мұндағы, $D_{жыл}$ – жылына қолжетімділік қаупі бойынша ресурстың маңыздылығы;

$D_{саг}$ – сағатына қолжетімділік қаупі бойынша ресурстың маңыздылығы;

$T_{\max}$ – жылына ресурстардың максималды тоқтау уақыты (ұйым үшін өте маңызды жұмыс уақыты).

Үш негізгі қауіпі бар режимдегі ресурстың әр қауіп үшін тәуекелдің мәні және тәуекелдің үш қауіп бойынша жиынтық мәні ақшалай немесе деңгеймен келесі өрнектермен анықталады:

$$R_c = CThR_c \cdot D_c;\ R_i = CThR_i \cdot D_i;\ \ R_a = CThR_a \cdot D_a;$$

$$R_{\sum} = \left(1 - \left(\left(1 - \frac{R_c}{100}\right) \cdot \left(1 - \frac{R_i}{100}\right) \cdot \left(1 - \frac{R_a}{100}\right)\right)\right) \cdot 100.$$

5. Ақпараттық жүйе бойынша тәуекелді CR ақшалай немесе деңгейлердегі жұмыс режимі үшін және үш қауіпі бар жұмыс режимі үшін қарастырамыз.

Ақшалай немесе деңгейлердегі бір негізгі кауіппен жұмыс істеу режимі үшін:

$$CR = \sum_{i=1}^{n} R_i,\ CR = \left(1 - \prod_{i=1}^{n}\left(1 - \frac{R_i}{100}\right)\right) \cdot 100$$

Ақшалай немесе деңгейлердегі үш қауіп бойынша жұмыс режимі үшін:

$$CR_{a,c,i} = \sum_{i=1}^{n} R_i,\ CR_{a,i,c} = \left(1 - \prod_{j=1}^{n}\left(1 - \frac{R_i}{100}\right)\right) \cdot 100,\ CR_{\sum} = CR_c + CR_i + CR_a;$$

$$CR_{\sum} = \left(1 - \left(\left(1 - \frac{CR_c}{100}\right) \cdot \left(1 - \frac{CR_i}{100}\right) \cdot \left(1 - \frac{CR_a}{100}\right)\right)\right) \cdot 100.$$

Пайдаланушы қарсы іс-шаралар қолдана алады. Енгізілген қарсы іс-шаралардың тиімділігін есептеу үшін алгоритм бойынша берілген қарсы әрекеттерді ескере отырып жүйелі түрде өту керек. Яғни, нәтижесінде пайдаланушы екі тәуекелдің мәнін алады - қарсы іс-шаралар қолданылғаға дейінгі тәуекел мәні (R_{old}) және қарсы іс-шаралар қолданылғаннан кейінгі тәуекел мәні (R_{new}). Қарсы іс-шараларды енгізудің тиімділігі мынадай формула бойынша есептеледі:

$$E = \frac{R_{old} - R_{new}}{R_{old}}$$

Осы алгоритмді қолдану негізінде қауіп-қатердің іске асу ықтималдылығы және осалдылық арқылы қауіптің іске асуының маңызыдылығы алынды. Нәтижелер 2.3-кестеде көрсетілген.

2.3-кесте – Қауіптердің іске асыру ықтималдығы мен маңыздылығын есептеу

Қауіп/Осалдық	Осалдық арқылы қауіптің іске асу ықтималдығы (%), P(V)	Осалдық арқылы қауіптің іске асу маңыздылығы (%), ER
Қызметкер		
Қауіп 1/ Осалдық 1	50	80
Қауіп 1/ Осалдық 2	20	50
Қауіп 2/ Осалдық 1	40	50
Қауіп 2/ Осалдық 2	50	80
Сервер		
Қауіп 1/ Осалдық 1	20	80
Қауіп 1/ Осалдық 2	30	70
Қауіп 1/ Осалдық 3	20	50
Қауіп 2/ Осалдық 1	50	80
Қауіп 2/ Осалдық 2	20	70
Коммерциялық құпияны құрайтын мәліметтерді өңдейтін қызметкерлердің АЖО		
Қауіп 1/ Осалдық 1	30	70
Қауіп 1/ Осалдық 2	30	70
Қауіп 1/ Осалдық 3	20	50
Қауіп 1/ Осалдық 4	30	60
Қауіп 1/ Осалдық 5	20	60
Қауіп 1/ Осалдық 6	30	70
Ақпарат тасымалдаушылар		
Қауіп 1/ Осалдық 1	40	70
Қауіп 1/ Осалдық 2	30	60

Алынған мәліметтер негізінде және (2) формуланы пайдалана отырып, осалдықтар бойынша қауіп деңгейін есептейміз. Алынған мәндер 3.4-кестеде келтірілген.

2.4 – Қауіп деңгейі

Қауіп/Осалдық	Қауіп деңгейі, Th	Барлық осалдықтар бойынша қауіп деңгейі CTh
Қызметкер		
Қауіп 1/ Осалдық 1	0,4	0,46

2.4-кестенің жалғасы

Қауіп 1/ Осалдық 2	0,1	
Қауіп 2/ Осалдық 1	0,2	0,52
Қауіп 2/ Осалдық 2	0,4	
Сервер		
Қауіп 1/ Осалдық 1	0,16	0,4
Қауіп 1/ Осалдық 2	0,21	
Қауіп 1/ Осалдық 3	0,1	
Қауіп 2/ Осалдық 1	0,4	0,48
Қауіп 2/ Осалдық 2	0,14	
Коммерциялық құпияны құрайтын мәліметтерді өңдейтін қызметкерлердің АЖО		
Қауіп 1/ Осалдық 1	0,21	0,68
Қауіп 1/ Осалдық 2	0,21	
Қауіп 1/ Осалдық 3	0,1	
Қауіп 1/ Осалдық 4	0,18	
Қауіп 1/ Осалдық 5	0,12	
Қауіп 1/ Осалдық 6	0,21	
Ақпарат тасымалдаушылар		
Қауіп 1/ Осалдық 1	0,28	0,41
Қауіп 1/ Осалдық 2	0,18	

Қауіптер деңгейінің алынған мәні және (3) формуласы негізінде қауіптердің жалпы деңгейі есептелінеді.

2.5-кесте – Қауіптердің жалпы деңгейі

Қауіп/Осалдық	Барлық осалдықтар бойынша қауіп деңгейі CTh	Ресурс бойынша қауіптердің жалпы деңгейі, CThR
Қызметкер		
Қауіп 1/ Осалдық 1	0,46	0,74
Қауіп 1/ Осалдық 2		
Қауіп 2/ Осалдық 1	0,52	
Қауіп 2/ Осалдық 2		
Сервер		
Қауіп 1/ Осалдық 1	0,4	0,69
Қауіп 1/ Осалдық 2		
Қауіп 1/ Осалдық 3		
Қауіп 2/ Осалдық 1	0,48	
Қауіп 2/ Осалдық 2		

2.5-кестенің жалғасы

Коммерциялық құпияны құрайтын мәліметтерді өңдейтін қызметкерлердің АЖО		
1	2	3
Қауіп 1/ Осалдық 1	0,68	0,32
Қауіп 1/ Осалдық 2		
Қауіп 1/ Осалдық 3		
Қауіп 1/ Осалдық 4		
Қауіп 1/ Осалдық 5		
Қауіп 1/ Осалдық 6		
Ақпарат тасымалдаушылар		
Қауіп 1/ Осалдық 1	0,41	0,59
Қауіп 1/ Осалдық 2		

Алынған деректер негізінде және (4) формуланы пайдаланып ресурс тәуекелін есептейміз. Алынған мәндер 2.6-кестеде көрсетілген.

2.6-кесте – Ресурс тәуекелі

Қауіп/Осалдық	Ресурс бойынша қауіптердің жалпы деңгейі, CThR	Ресурс тәуекелі, R
Қызметкер		
Қауіп 1/ Осалдық 1	0,74	74
Қауіп 1/ Осалдық 2		
Қауіп 2/ Осалдық 1		
Қауіп 2/ Осалдық 2		
Сервер		
Қауіп 1/ Осалдық 1	0,69	69
Қауіп 1/ Осалдық 2		
Қауіп 1/ Осалдық 3		
Қауіп 2/ Осалдық 1		
Қауіп 2/ Осалдық 2		
Коммерциялық құпияны құрайтын мәліметтерді өңдейтін қызметкерлердің АЖО		
1	2	3
Қауіп 1/ Осалдық 1	0,32	32
Қауіп 1/ Осалдық 2		
Қауіп 1/ Осалдық 3		
Қауіп 1/ Осалдық 4		
Қауіп 1/ Осалдық 5		
Қауіп 1/ Осалдық 6		
Ақпарат тасымалдаушылар		
Қауіп 1/ Осалдық 1	0,59	59
Қауіп 1/ Осалдық 2		

2.7-кестеде – Қорытынды кесте

Ресурстар	Қауіптер	Осалдықтар	Осалдық арқылы қауіптің іске асу ықтималдығы	Осалдық арқылы қауіптің іске асу маңыздылығы	Қауіп деңгейі, Th	Барлық осалдықтар бойынша қауіп деңгейі	Ресурс бойынша қауіптердің жалпы деңгейі, CThR	Ресурс тәуекелі, R
Қызметкер	1. Коммерциялық құпияны құрайтын ақпаратты жариялау, өзгерті, жою, ұрлау	1. Қорғауға жататын ақпаратты жарияламау туралы келісімді сақтамау	50	80	0,4	0,46	0,74	74
		2. Коммерциялық құпияны қорғау жөніндегі құжаттардың, регламенттердің болмауы немесе өзекті болмауы	20	50	0,1			
	2. Қызметкерлердің АЖО-да сақталатын ақпаратты түрлендіруі, жоюы	1. Коммерциялық құпия өңделетін ғимаратқа кіру регламентінің болмауы	40	50	0,2	0,52		
		2. Уәкілетті емес қызметкерлердің АЖО-нан қорғауға жататын ақпаратты модификациялауға немесе жоюға тыйым салудың болмауы	50	80	0,4			

2.7-кестенің жалғасы

Сервер	1. Сервер орналасқан бөлмеге рұқсатсыз кіру	1. Өткізу режимін бұзу	20	80	0,16	0,4	0,69	69
		2. Ғимараттың күзет сигнализациясының болмауы	30	70	0,21			
		3. Ғимаратқа кіру регламентінің болмауы	20	50	0,1			
	2. Серверде сақталған деректерге рұқсатсыз қол жеткізу	1. Рұқсат етілмеген қол жеткізуді жасай алатын бағдарламаның болуы	50	80	0,4	0,48		
		2. Жүйедегі зиянды бағдарламаның болуы	20	70	0,14			
Коммерциялық құпияны құрайтын мәліметтерді өңдейтін қызметкерлердің АЖО	1. Қызметкерлердің АЖО-ға рұқсатсыз кіруі	1. Рұқсат етілмеген қол жеткізуді жасай алатын бағдарламаның болуы	30	70	0,21	0,68	0,32	32
		2. АЖО-ға қол жеткізу регламентінің болмауы	30	70	0,21			
		3. Жүйедегі зиянды бағдарламаның болуы	20	50	0,1			
		4. Аппараттық деңгейде авторизациялаудың болмауы	30	60	0,18			
		5. АЖО корпусын пломбалаудың болмауы	20	60	0,12			
		6. Өткізу режимін бұзу	30	70	0,21			
Ақпарат тасымалдау шылар	1. Ақпарат тасымалдаушыларды түрлендіру, жою, ұрлау	1. Өткізу режимін бұзу	40	70	0,28	0,41	0,59	59
		2. Коммерциялық құпиясы бар тасымалдаушыларды есепке алудың болмауы	30	60	0,18			

3 АҚ тәуекелдерін бағалауды алгоритмдік және бағдарламалық қамтамасыз ету

3.1 Бағдарламалау тілі және ортасы

Бағдарламаны әзірлеу құралы ретінде PHP бағдарламалау тілі таңдалды.

PHP-бұл бағдарламалаудың скрипті тілі, ол кез келген тапсырмаларды орындауға қолайлы, бірақ негізінен серверлік қосымшаларды құру үшін қолданылады. Оның танымалдығы есебінен оны Интернет хостингтердің көпшілігін қолдайды және JS сияқты web-құжатта динамикалық элементтерді құру үшін өте жиі қолданылады.

PHP негізгі артықшылығы ретінде көп ағынмен жақсы жұмысы және деректерді шифрлау модульдерінің үлкен жиынтығы болып табылады. Бұл таңдау PHP бағдарламалау тілінің келесі артықшылықтары: қауіпсіздік; архитектуралық бейтараптылық; төзімділік; жоғары өнімділік; көп шоғырлану; динамикалық; пайдалану қарапайымдылығы; нысандарға бағдарлау.

Бағдарламалық іске асыру үшін DevelNext ортасының 16.7.0 нұсқасы пайдаланылды.

DevelNext-өз қосымшаларын, веб-сервистерді, дайын компоненттен клиенттерді құруға және Windows/Linux/Mac негізіндегі функционалды прототиптерді жасауға арналған әзірлеу ортасы.

DevelNext пайдаланушыға дайын компоненттер жиынтығын ұсынатын конструктор болып табылады интерфейс элементтері, олардың артынан жасырынған оқиғалар мен сценарийлер – толыққанды қосымшаны жасау үшін қажет.

Конструктор көмегімен бай интерфейсі бар толыққанды кросс-платформалық қосымшаларды жасауға болады. Ол үшін JavaFX деп аталатын технология қолданылады, бұл әртүрлі платформалар астында GUI үшін фреймворк. Жоба Java тілін платформа ретінде ғана пайдаланады, ал DevelNext бағдарламалау тілі PHP болып табылады, алайда Java, Groovy, Scala және басқа да JVM тілдерінде жазылған қосымша кітапханаларды жазу және қосу мүмкіндігі бар.

DevelNext тегін таратылады, орыс тілінде интерфейсті қолдайды және өте күрделі бағдарламалық өнімдерді жасауға мүмкіндік береді.

Php ортасы жобаның нәтижелерін синтаксистік қателерге тексере алады, жобаларды айнымалыларды баптау режимінде іске қосуға мүмкіндігі бар. DevelNext барлық көздер үшін ашық MPL 2.0 лицензиясымен таратылады.

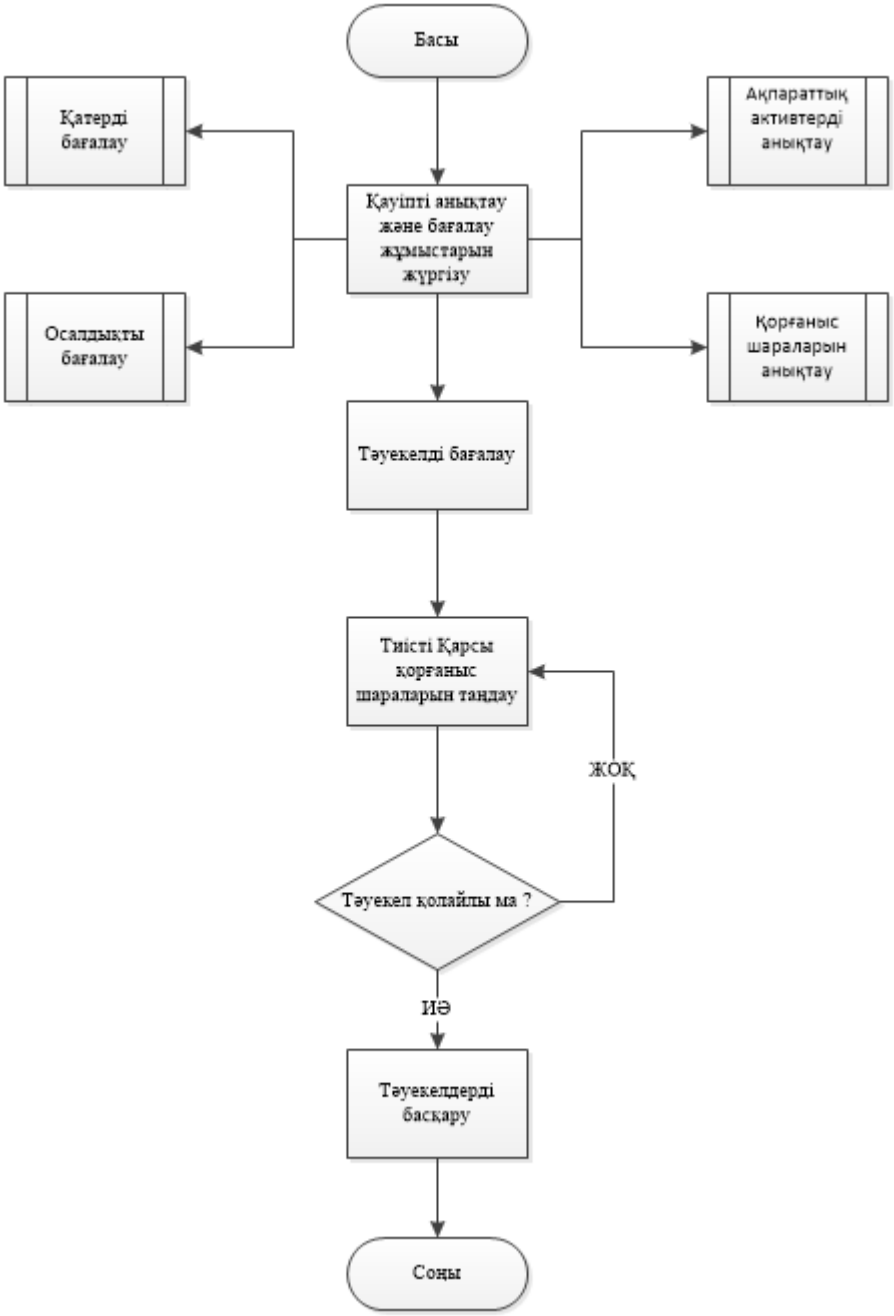
Сонымен қатар, SQLite деректер базасы пайдаланылды. SQLite – бұл SQL командаларының толық жиынтығын қолдайтын және бастапқы кодтарда (C тілінде) қол жетімді кроссплатформлы деректер базасы.

SQLite – бұл жылдам өсіп келе жатқан мәліметтер базасының қозғалтқыштарының бірі, бірақ ол танымал емес, мөлшері бойынша өсуде. SQLite-тің бастапқы коды көпшілікке қол жетімді.

QLite сервердің немесе жүйенің жеке процесін талап етпейді. Толық деректер қоры бір кросс-платформалық дискіде сақталады. Ол автономды болып табылады, бұл сыртқы тәуелділіктердің жоқтығын білдіреді. Транзакциялар бірнеше процестерге немесе ағындарға қауіпсіз қатынауды қамтамасыз ете отырып, ACID-мен толығымен үйлесімді. SQLite sql92 (SQL2) стандартында табылған сұраныс тілінің көптеген функцияларын қолдайды.

SQLite ANSI-C жазылған және API пайдалану оңай және UNIX (Linux, Mac OS-X, Android, iOS) және Windows (Win32, WinCE, WinRT) операциялық жүйелерінде пайдалануға қолжетімді.

3.2 Бағдарламалық қамтаманың алгоритмі



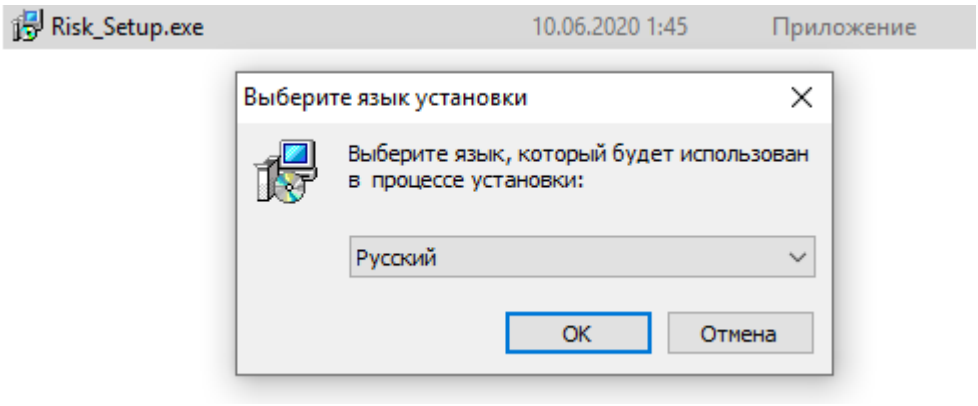
3.1-сурет – Құрылымдық сұлба

3.3 Орнату процессі

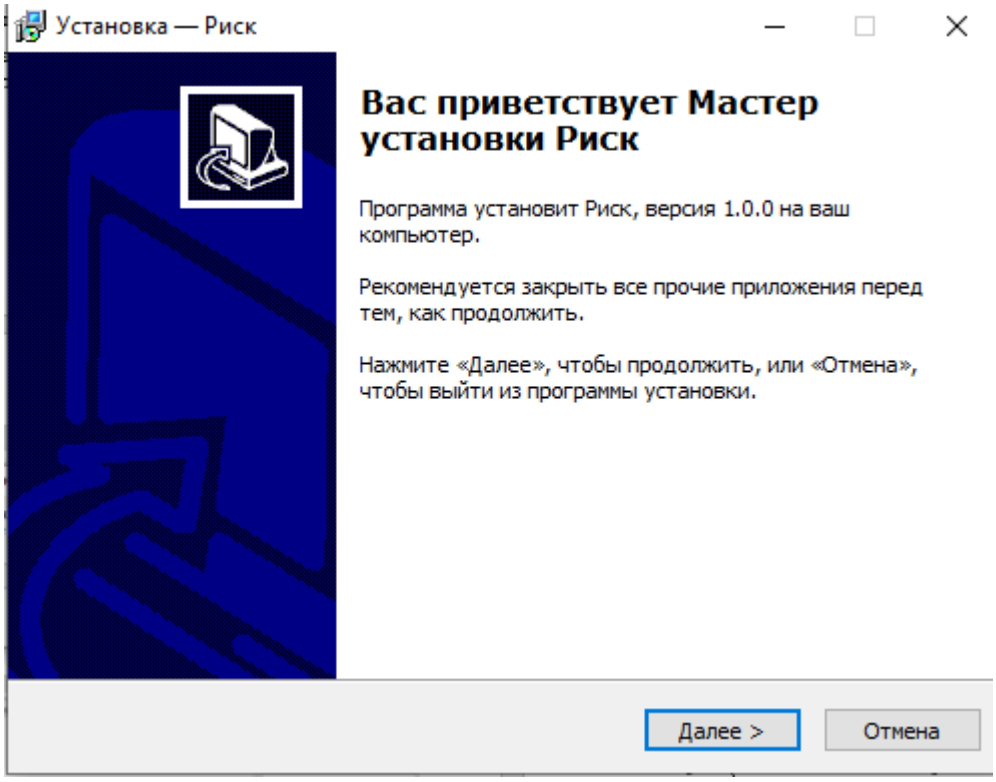
Бағдарламалық жасақтаманы компьютерде дұрыс орнату үшін, бағдарламаны орнату процесін дамытуды қамтамасыз ету қажет.

Соңғы пайдаланушы компьютеріндегі бағдарламалық жасақтаманы орнату операциялық жүйеде қамтылған немесе орнату құралы арқылы бағдарламалық жасақтамаға кіретін арнайы бағдарлама (пакет менеджері) арқылы жүзеге асырылады. Соңғы пайдаланушы компьютеріндегі бағдарламалық жасақтаманы орнату операциялық жүйеде қамтылған немесе орнату құралы арқылы бағдарламалық жасақтамаға кіретін арнайы бағдарлама (пакет менеджері) арқылы жүзеге асырылады. Бағдарлама дұрыс жұмыс істеуі үшін оның негізгі каталогында барлық файлдар, проекттер, сондай-ақ деректер базасы болуы тиіс.

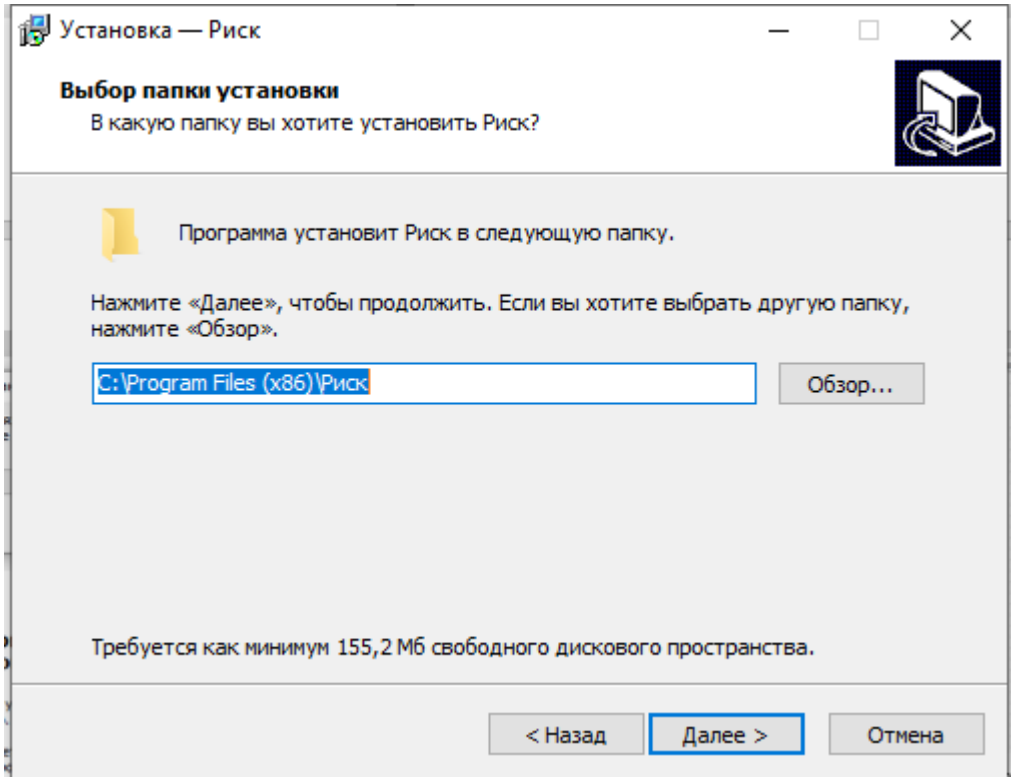
Осылайша, орнату бағдарламасын іске қосып, жаңа орнатушы жасауды таңдаймыз. Осыдан кейін орнатуды жасау диалогтық терезесі ашылады (3.19-сурет).



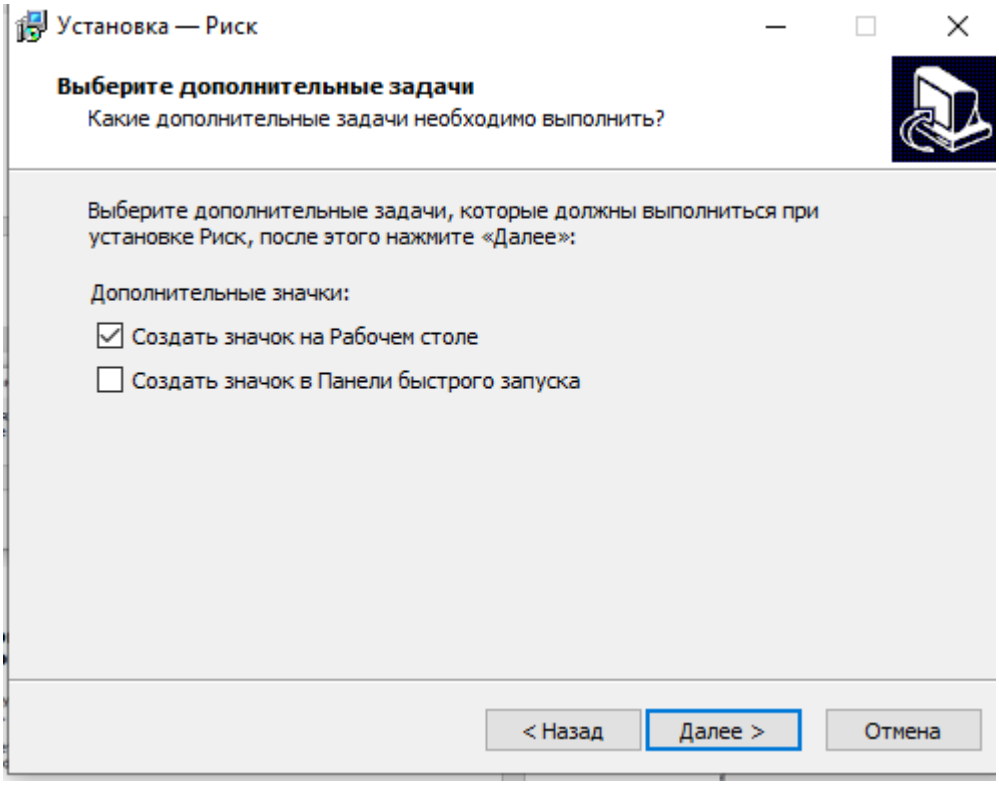
3.2 сурет – Бағдарламалық жасақтама орнату тілін таңдау



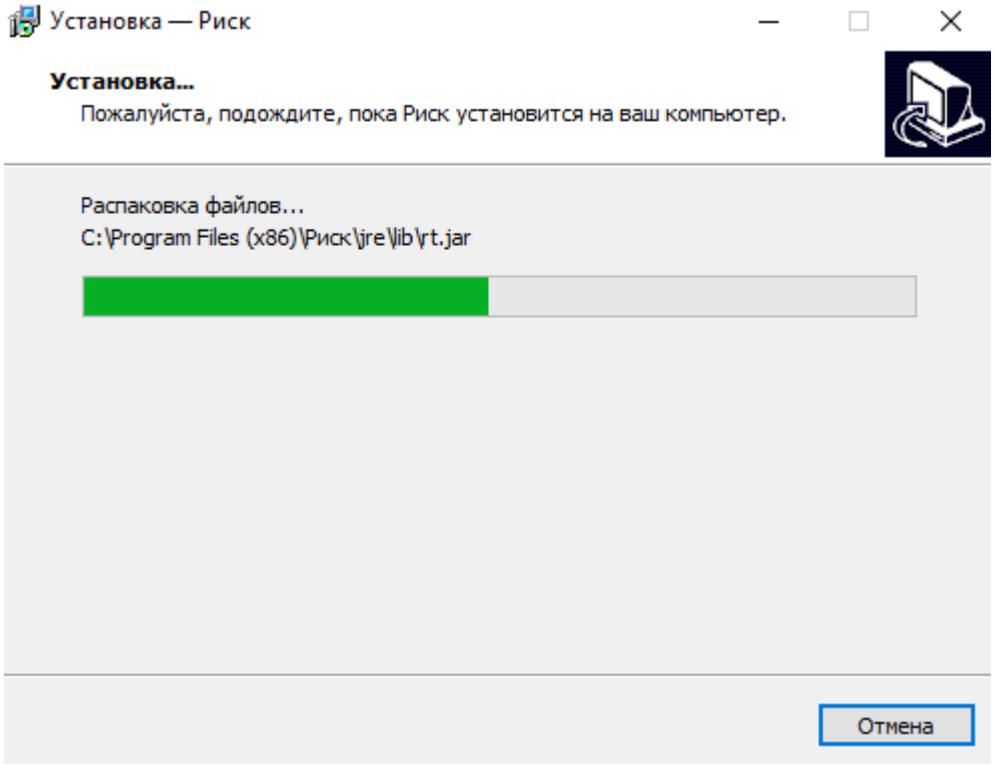
3.3 сурет – Орнату терезесі



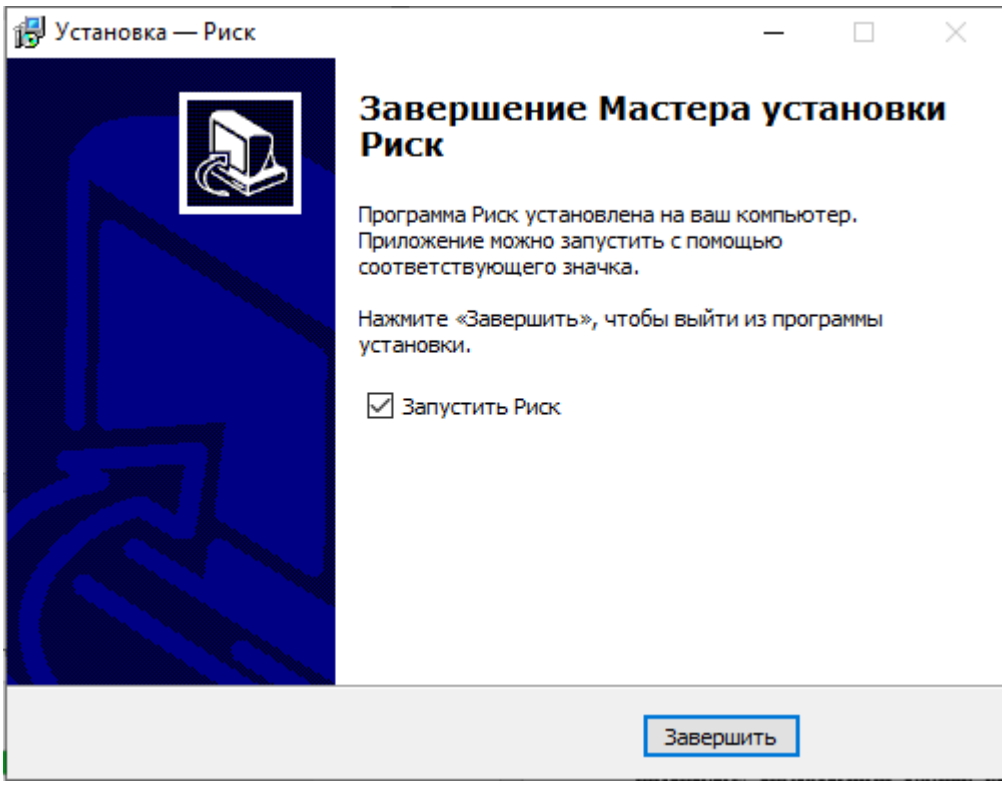
3.4 сурет – Орнату қалтасын таңдау



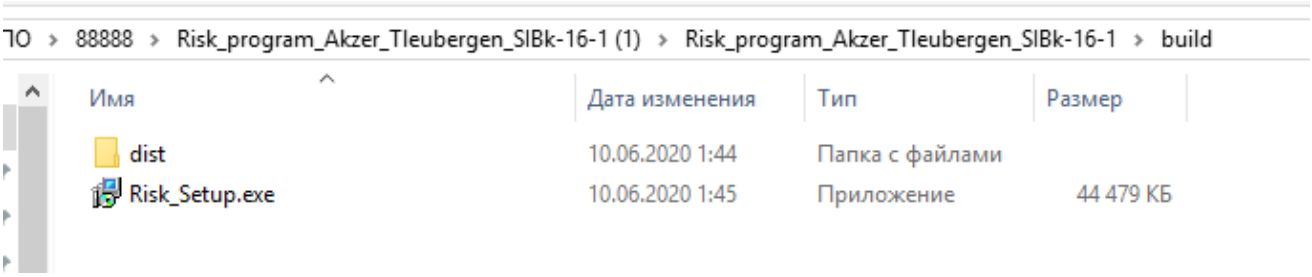
3.5 сурет – Орнату процессі



3.6 сурет – Орнату процессі



3.7 сурет – Орнату процесін аяқтау



3.8 сурет – Бағдарламалық жасақтаманың орнату орнын тексеру

3.3 Тестілеу

Барлық пайдаланушы параметрлерін бекітіп болғаннан кейін бағдарламалық жасақтаманы талдап, жобалаудан кейін бағдарламалық жасақтаманы тексеру кезеңі жүргізіледі. Тестілеу − бағдарламалық қамтамасыз етуді іске асыру функциялары, логикасы және нысаны бойынша қателерді анықтау бойынша бағдарламаны жүзеге асыру. Бағдарламалық өнімді әзірлеу процесінде тестілеу программалық қамтамасыз етуді бағдарламалық өнімнің жұмыс нұсқасын алу үшін жүзеге асырады. Тестілеу барысында бағдарламадағы барлық форманың және операторлардың жұмысын тексеру және бағдарламада қарастырылған барлық нәтижелерді жасай отырып, кіріс деректерін (бақылау мысалы) жасау жүзеге асырылады.

Бағдарламалық жасақтама өнімінің функционалды тестілеуі бағдарламаның жұмыс істеу қабілеттілігін және онда көрсетілген барлық функцияларды тексеруден тұрады. Тесттер орындалады, алынған барлық нәтижелер бағаланады. Нақты тест нәтижелері күтілетін нәтижелермен салыстырылады. Сәйкес келмеу анықталса, қате тіркеледі − баптау басталады.

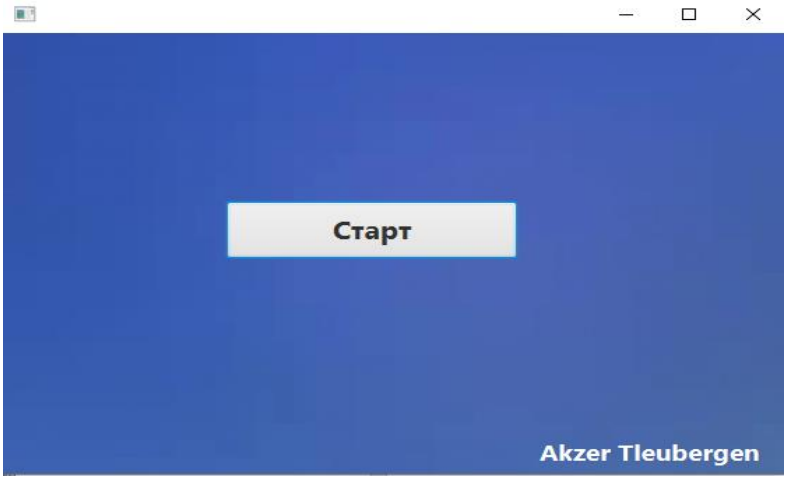
Бағдарламалық жасақтаманы тестілеу бағдарламаның көрінуін қамтамасыз ету үшін экранды шпионы және жасырын тексеру үлгісі арқылы жүргізіледі.

Тестілеу Acer ноутбугінде жүргізіледі, Intel(R) Core(TM) i3-3120M CPU процессорімен, 2.50 ГГц жиілікті, орнатылған жады (ОЗУ) 4 ГБ, 64-разрядтық Windows 10 операциялық жүйесі, ноутбук жергілікті желіге қосылмаған және жұмыс станциясы.

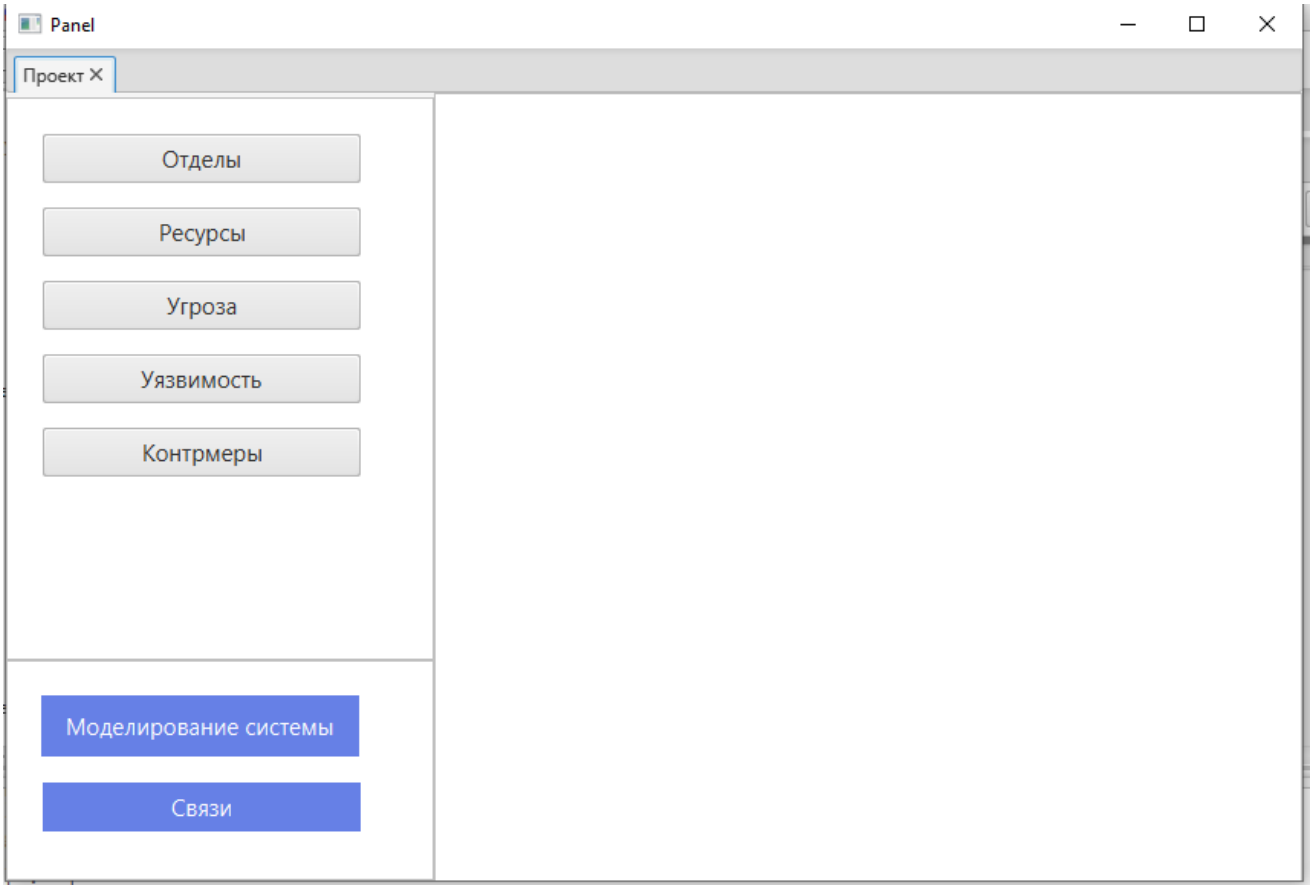
Ресурс бойынша тәуекелді анықтау үшін пайдаланушы өзінің ақпараттық жүйесінің объектілерін енгізуі тиіс: бөлімдер, ресурстар (осы модель үшін ерекше объектілер: ақпараттық жүйенің каупі, қауіп-қатер іске асырылатын осалдықтар), қорғану шаралары (контрмеры). Бұдан әрі пайдаланушы осы объектілерді өзара байланыстыру қажет, яғни ресурстардың қандай бөлімдерге жататынын, ресурсқа қандай қауіп төнетінін және олар қандай осалдықтар арқылы іске асырылатынын анықтау қажет.

Жүйені модельдеу – бұл ақпарат жүйенің барлық объектілері туралы деректер енгізілетін бөлім.

Пайдаланушы үшін ақпараттық жүйенің моделін құру кезінде бірінші кезеңдегі басты міндет барлық объектілерді, ресурстарды, сондай-ақ қауіптер мен осалдықтарды енгізу болып табылады. Ақпараттық жүйенің бөлімдері келесідей көрінеді (3.10-сурет).



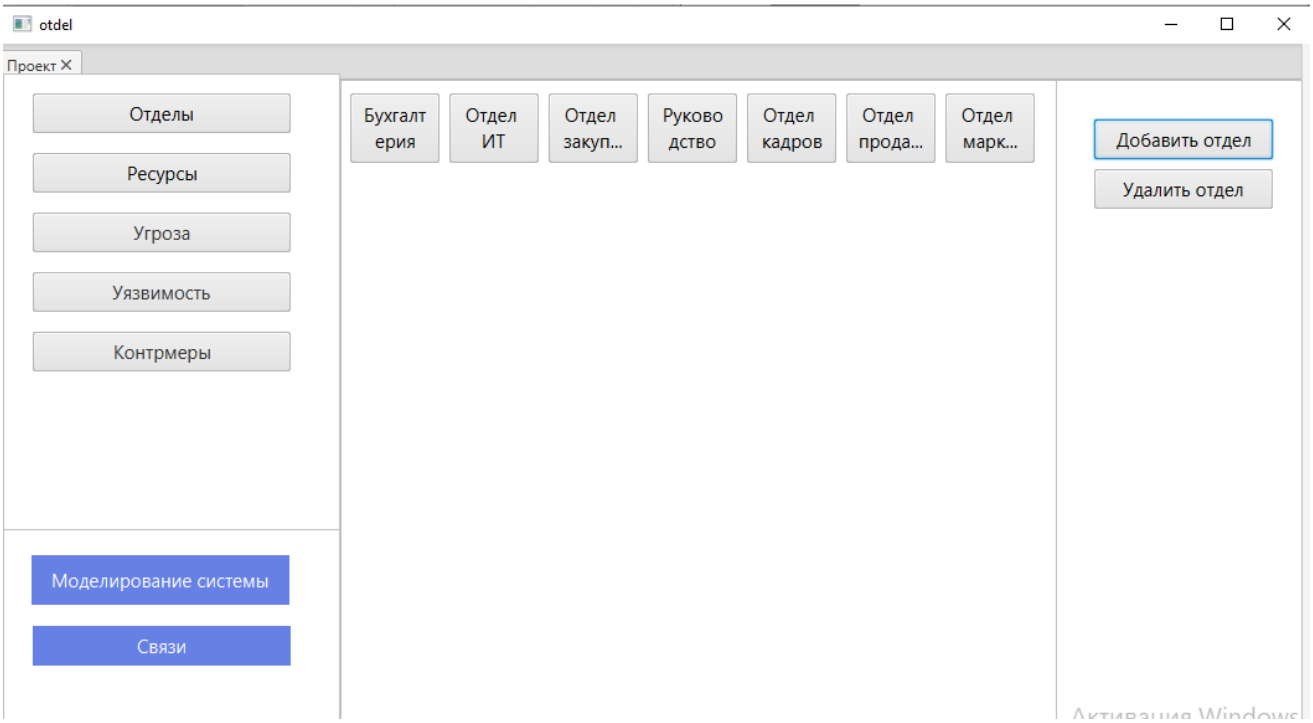
3.9 сурет – Бағдарламаның қосылуы



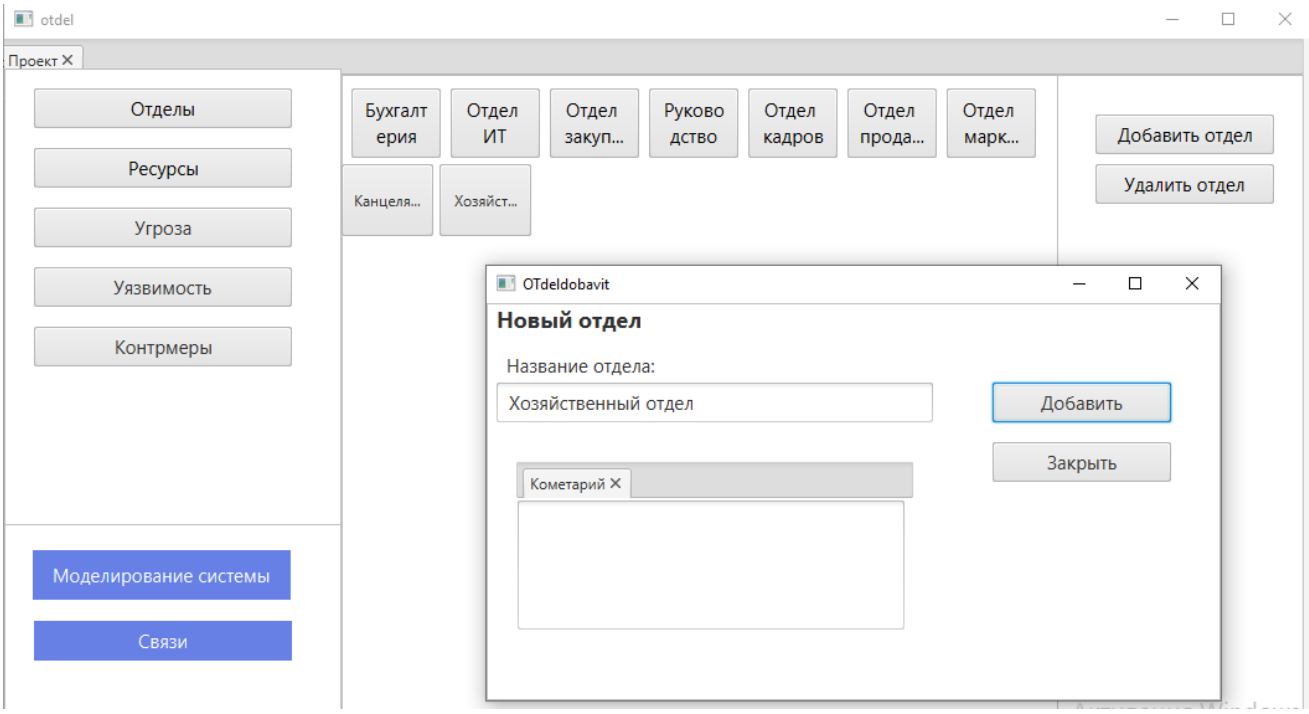
3.10 сурет – Бағдарламаның интерфейсі

«Бөлімдер»

Бөлімді қосу үшін "Добавить" батырмасын басу қажет, пайда болған терезеде бөлім атауын енгізіп, " Добавить " батырмасын басу қажет. Осы бөлімнің интерфейсі 3.12-суретте көрсетілген.



3.11 сурет – Енгізілген бөлімдер



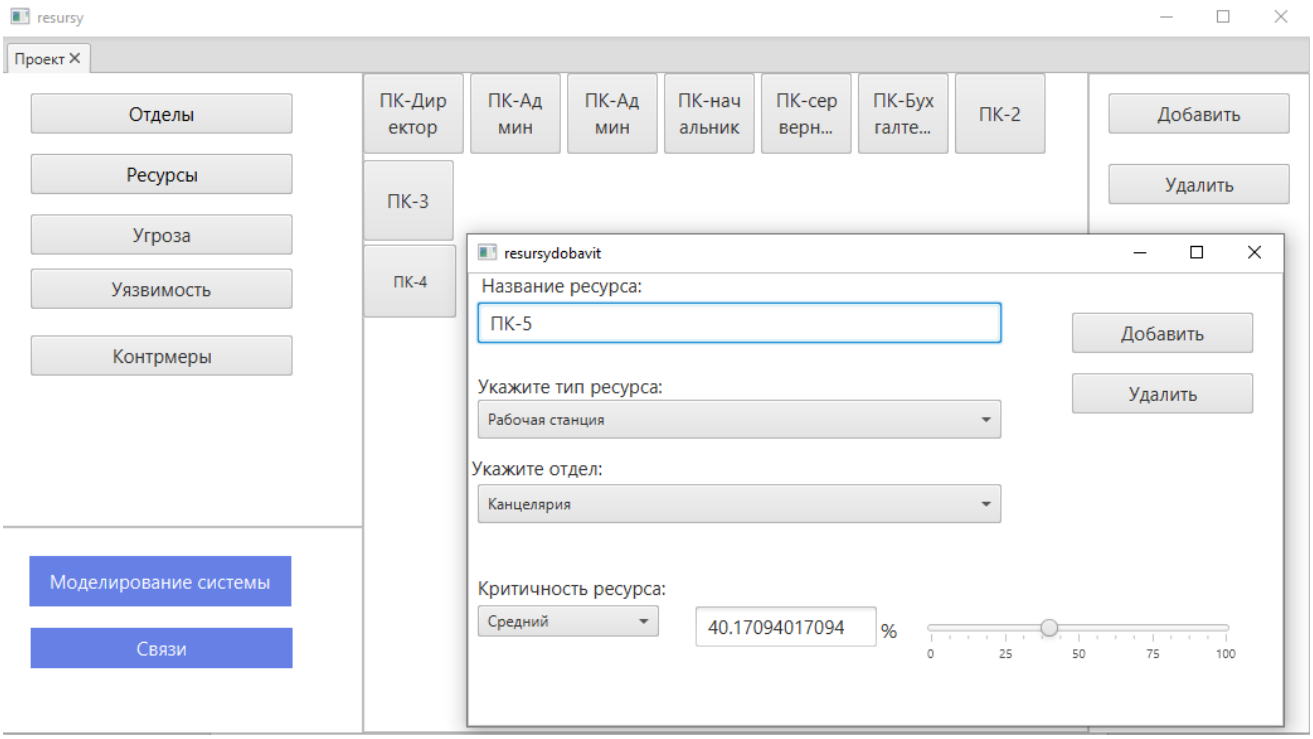
3.12 сурет – Жаңа бөлімді қосу

«Ресурс» бөлімі

Ресурсты қосу үшін ресурстың санатын көрсету қажет (сервер, жұмыс станциясы, мобильді компьютер, қатты көшірме, веб-сервер), осы ресурс қолданылатын бөлімді, сондай-ақ ресурстың маңыздылығын көрсету қажет

(ресурс үшін қауіптің іске асуы ақпараттық жүйенің жұмысына қаншалықты әсер етеді). Әр ресурстың маңыздылығын сіз өз қалауыңыз бойынша таңдай аласыз. Осы бөлімнің интерфейсі 3.14-суретте көрсетілген.

3.13 сурет – Енгізілген ресурстар



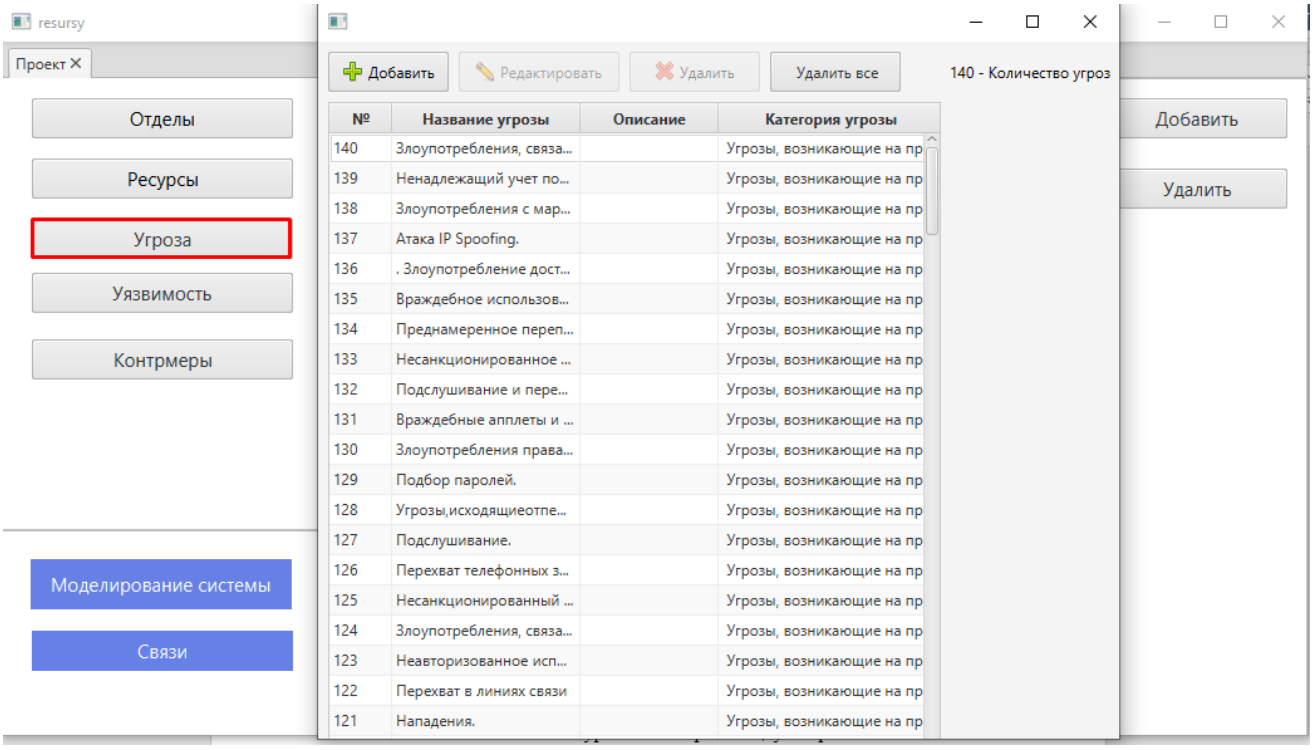
3.14 сурет – Жаңа ресурсты қосу

«Қауіптер» бөлімі

Бағдарламада алты қауіп санаты бар:

1. адамның физикалық қаупі (потенциалды бұзушының);
2. физикалық қауіптер (форс-мажорлық жағдайлардан туындаған);
3. ресурсқа бағытталған жергілікті бағдарламалық қауіптер (байланыс арналарын пайдаланбаған жағдайда);
4. ресурсқа бағытталған қашықтағы бағдарламалық қауіптер (байланыс арналарын пайдаланған жағдайда);
5. байланыс арнасына бағытталған бағдарламалық қауіп-қатерлер (кабельдік жүйе, коммуникациялық);
6. қызметкердің жасауы мүмкін қауіптер (компания қызметкерлерінің әрекеттерінен туындаған).

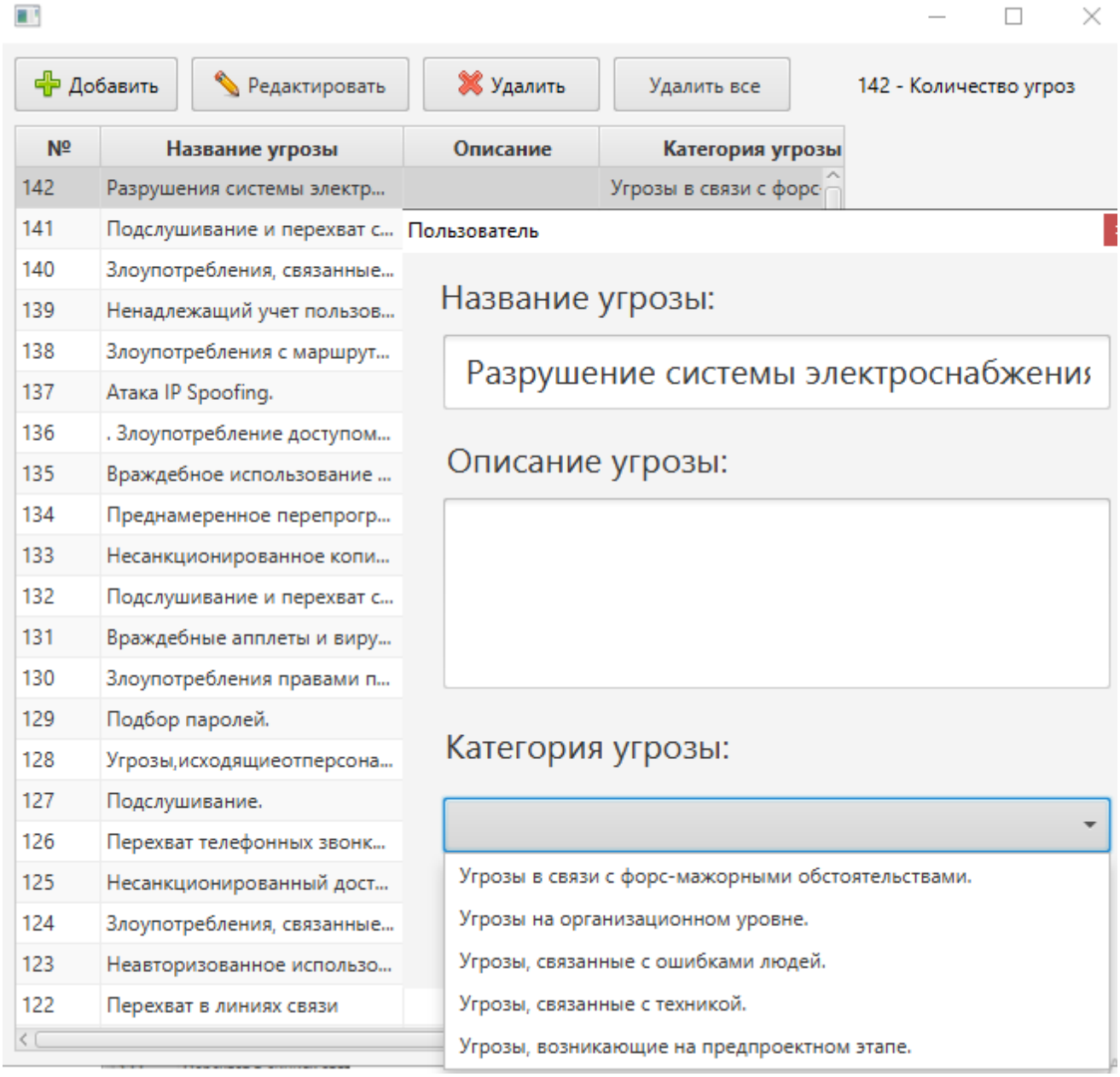
Бағдарламаға қауіпті екі жолмен қосуға болады, біріншісі тізімнен қауіпті таңдау, яғни тізімнен қауіпті екі рет басу арқылы таңдауға болады.



3.15 сурет –Деректер базасынадағы қауіптер

Екінші әдіс-пайдаланушыға тізімде жоқ қауіп-қатерлерді жаңадан қосу.

Жаңа қауіптерді қосу үшін " Добавить " бастырмасын басу қажет, пайда болған терезеде қауіптің атауын енгізу және осы қауіптің қандай санатына жататынын көрсету қажет және " Добавить " бастырмасын басу қажет. Осы бөлімнің интерфейсі 3.16-суретте көрсетілген.



3.16 сурет – Жаңа қауіпті қосу

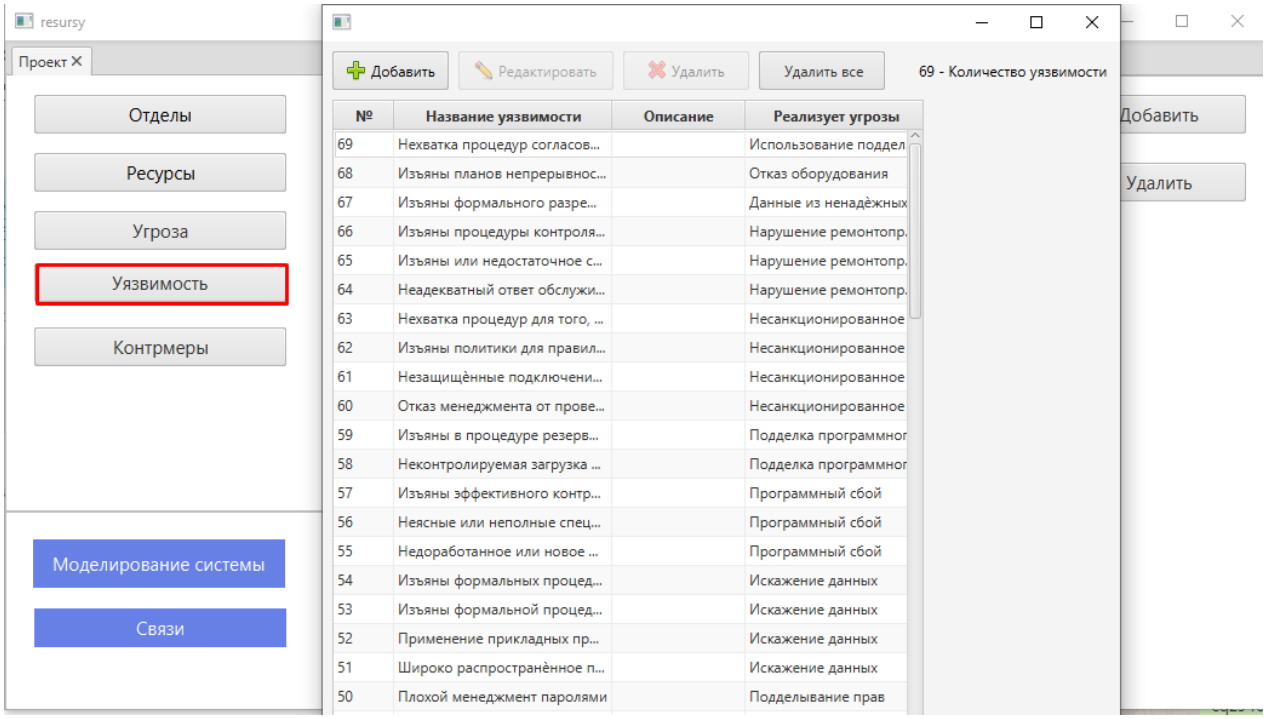
«Осалдықтар» бөлімі

Бағдарламаға қауіпті екі жолмен қосуға болады, біріншісі тізімнен қауіпті таңдау, яғни тізімнен қауіпті екі рет басу арқылы таңдауға болады.

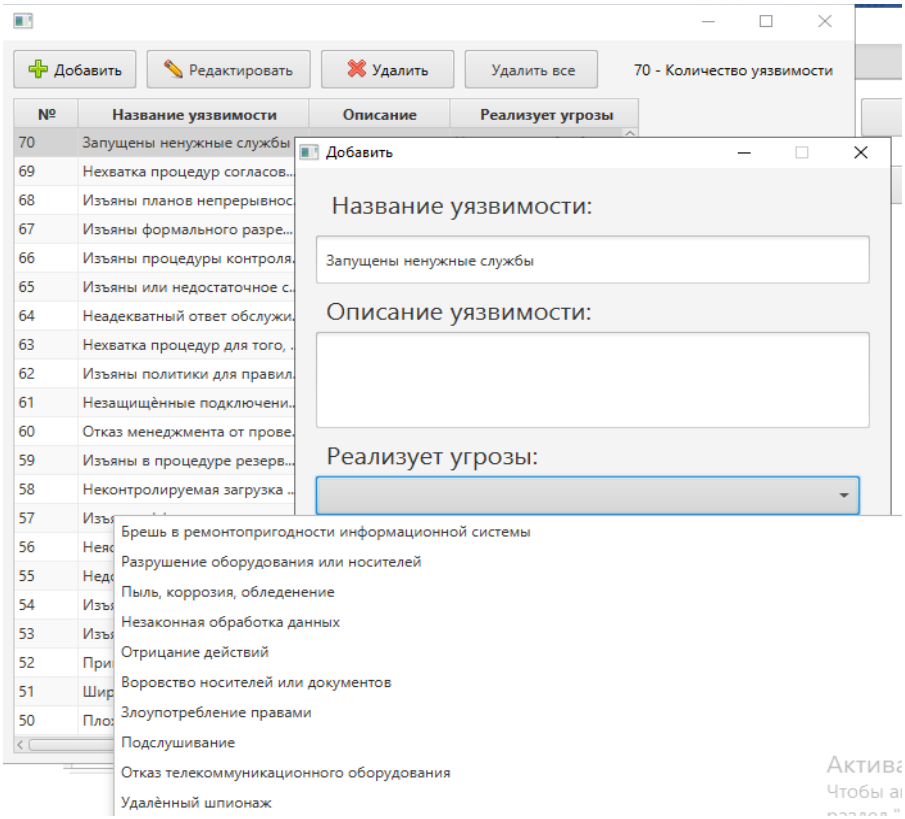
Жүйеде бар осалдықтарды қосу үшін "Уязвимости " бөлімін таңдап, тізімнен керекті осалдыққа екі рет басу арқылы таңдауға болады. Алдыңғы қадамда анықталған қауіптерге сәйкес осы қауіптерді іске асыруға себеп болуы мүмкін осалдықтарды көрсетіңіз.

Тізімде жоқ жаңа осалдықты қосу үшін " Добавить " батырмасын басу, пайда болған терезеде осалдықтың атауын енгізу және осы осалдықтың қандай

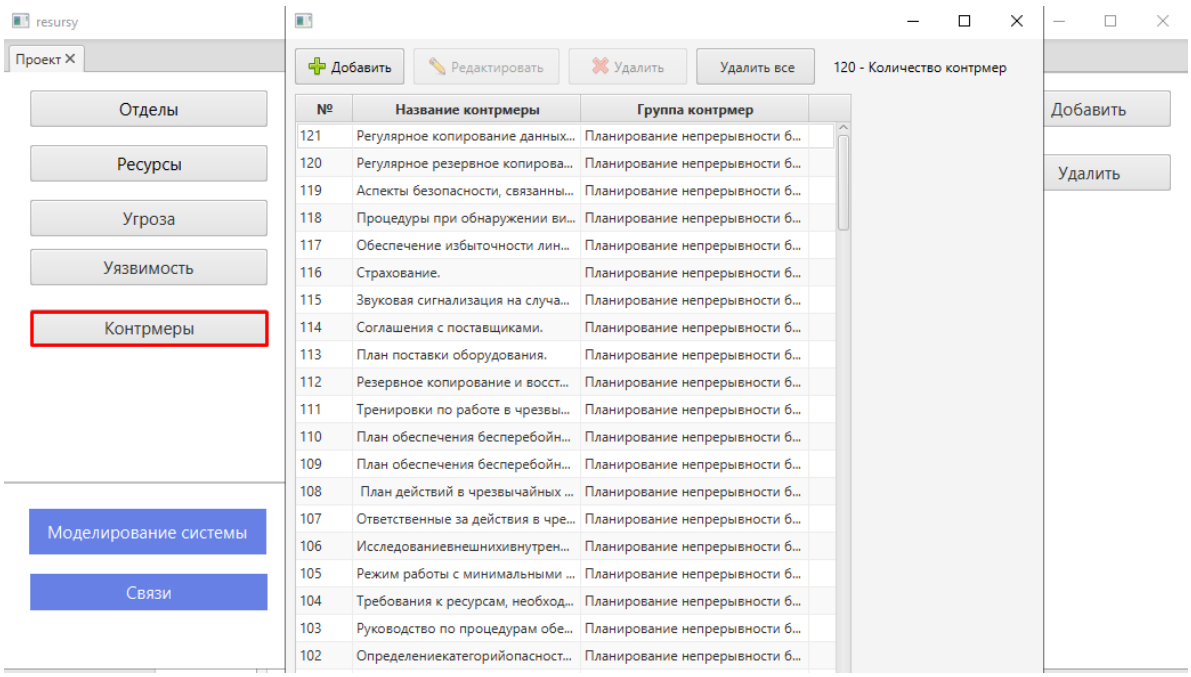
қауіп-қатерді іске асыратынын көрсету және "Қосу" батырмасын басу қажет (3.18-сурет).



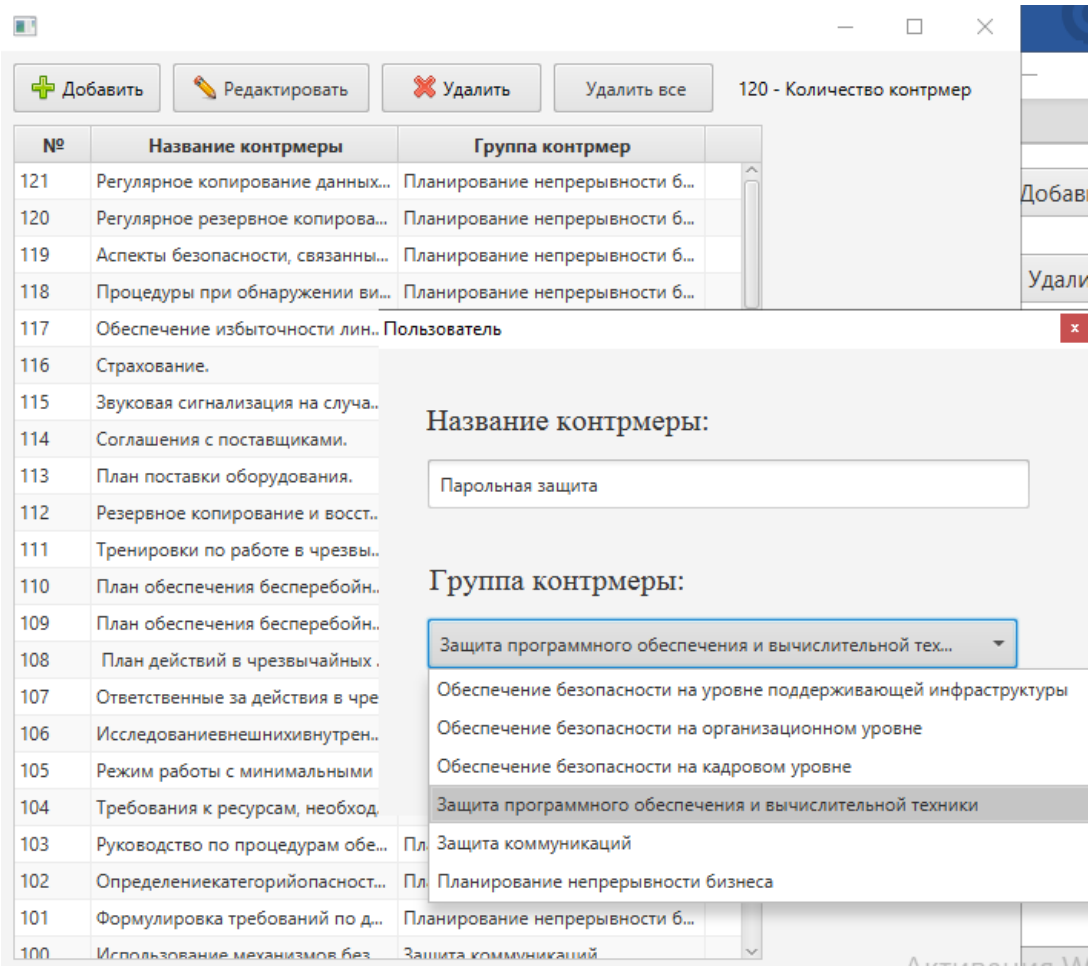
3.17 сурет –Деректер базасынадағы осалдықтар



3.18 сурет – Жаңа осалдықты қосу



3.19 сурет –Деректер базасынадағы контрмерлер



3.20 сурет – Жаңа контрмер қосу

«Байланыстар» бөлімі

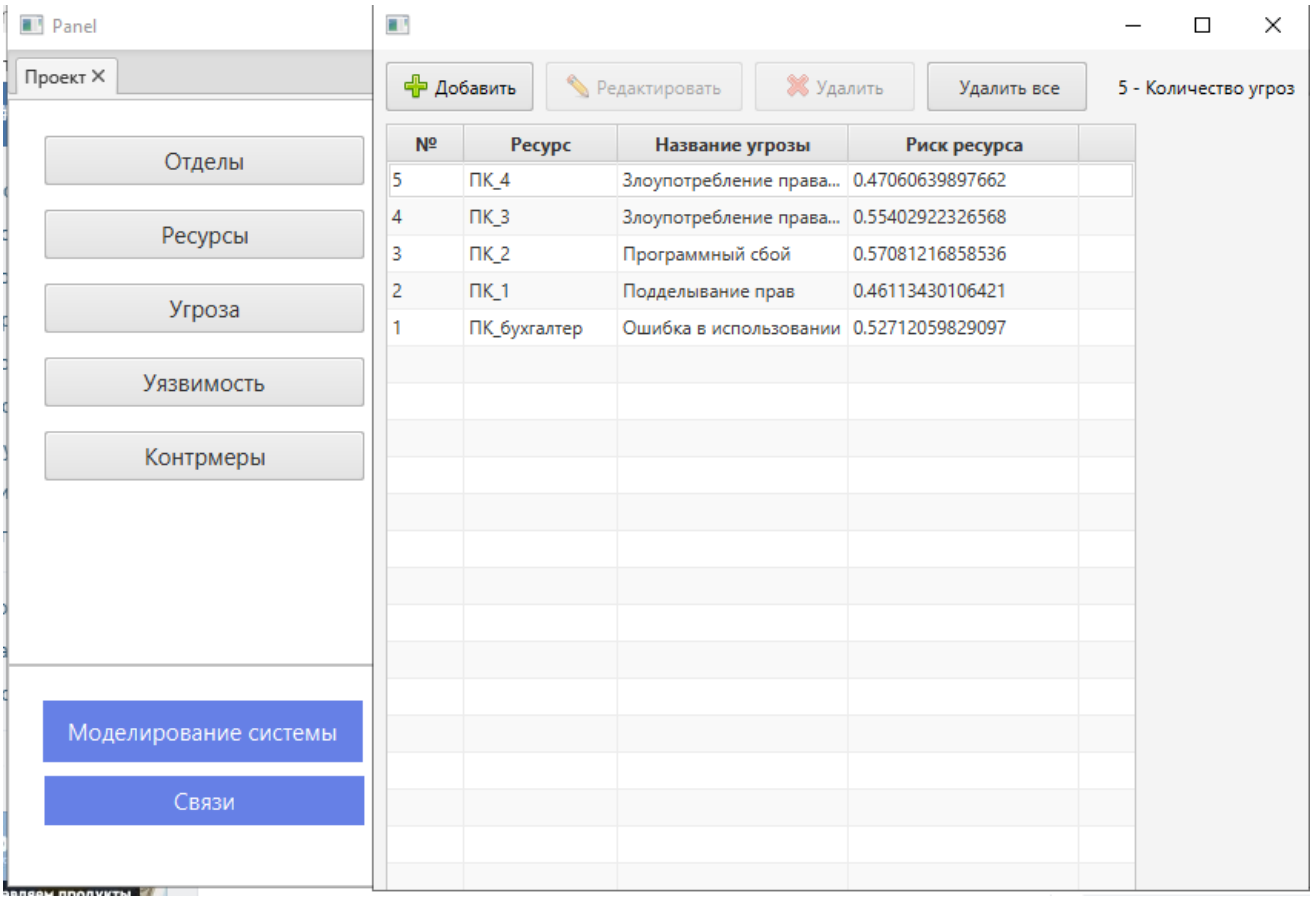
Байланыс – "Жүйені моделдеу" бөлімінің объектілері арасындағы байланысты анықтауға арналған бөлім.

Бұл бөлімде пайдаланушы ашылмалы мәзірден ресурсты таңдайды. Бұдан әрі пайдаланушы байланыс қою керек, яғни ресурсқа қандай қауіп-қатерлер әсер етеді және олар қандай осалдықтар арқылы іске асырылады.

"Добавить" батырмасын басқан кезде, бағдарламада ресурс бойынша тәуекел есептелетін келесі терезе ашылады (3.21-сурет). 3.1-бөлімде сипатталған формулалар бойынша бағалау жүргізіледі.

Мұнда ең алдымен ресурс содан соң қауіптер және әрбір қауіп іске асырылуы мүмкін осалдақтар таңдалынады және міндетті түрде осы осалдық арқылы жыл бойы қауіп-қатердің ықтималдығы мен қауіптің іске асу маңыздылығы сандық мән түрінде беріледі.

«Уровень угрозы» батырмасын басқан кезде екі параметрді негізге ала отырып осы осалдық арқылы қауіп мәні есептелінеді. Ең соңында «Риск ресурса» батырмасын басқанда ресурстың тәуекел мәні көре аласыз.

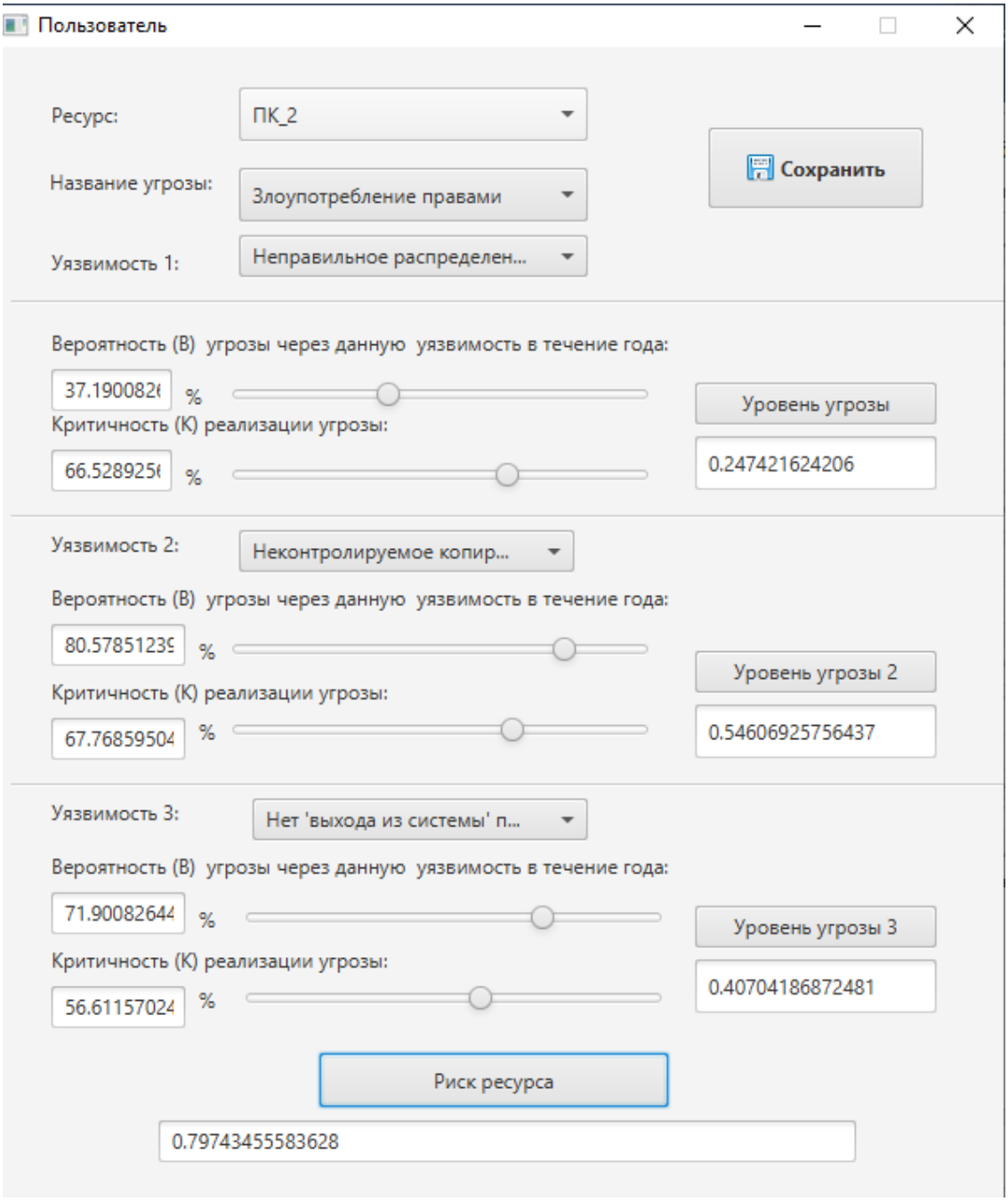


3.21 сурет – Ресурс бойынша тәуекел мәні

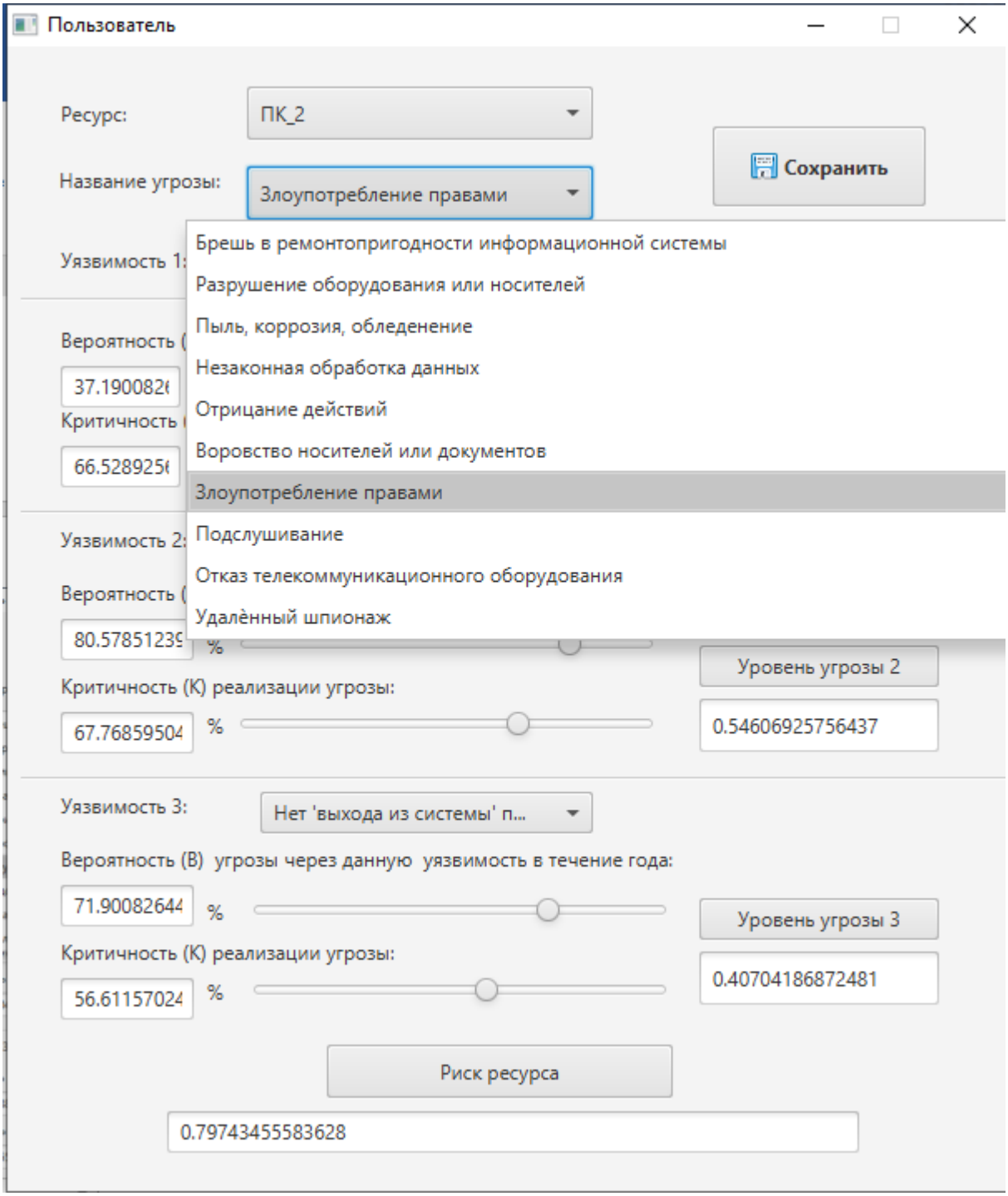
Қауіптердің бірін таңдағаннан кейін "Добавить" батырмасын басыңыз, содан кейін осы қауіптен туындайтын осалдықтарды көрсету және екі параметрді қою қажет:

- осы осалдық арқылы жыл бойы қауіп-қатердің ықтималдығы;
- қауіптің іске асу маңыздылығы.

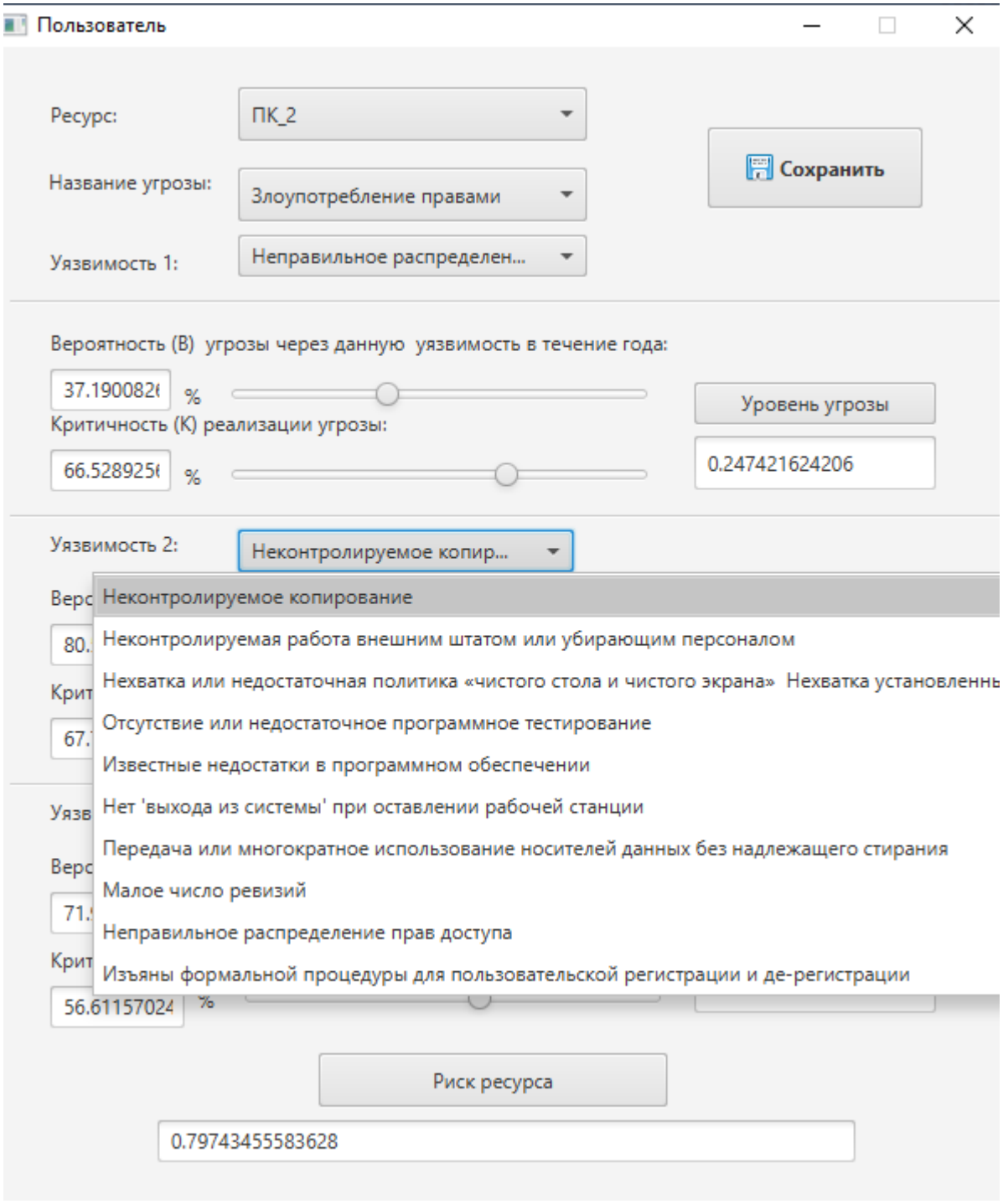
Осылайша, қауіп-қатерлер мен осалдықтарды ақпараттық жүйенің ресурстарымен байланыстырыңыз. Әрбір ресурс үшін қауіптер мен осалдықтар тізімі шығады. Осы бөлімнің интерфейсі 3.22-суретте көрсетілген.



3.22 сурет – Барлық осалдықтар бойынша қауіп

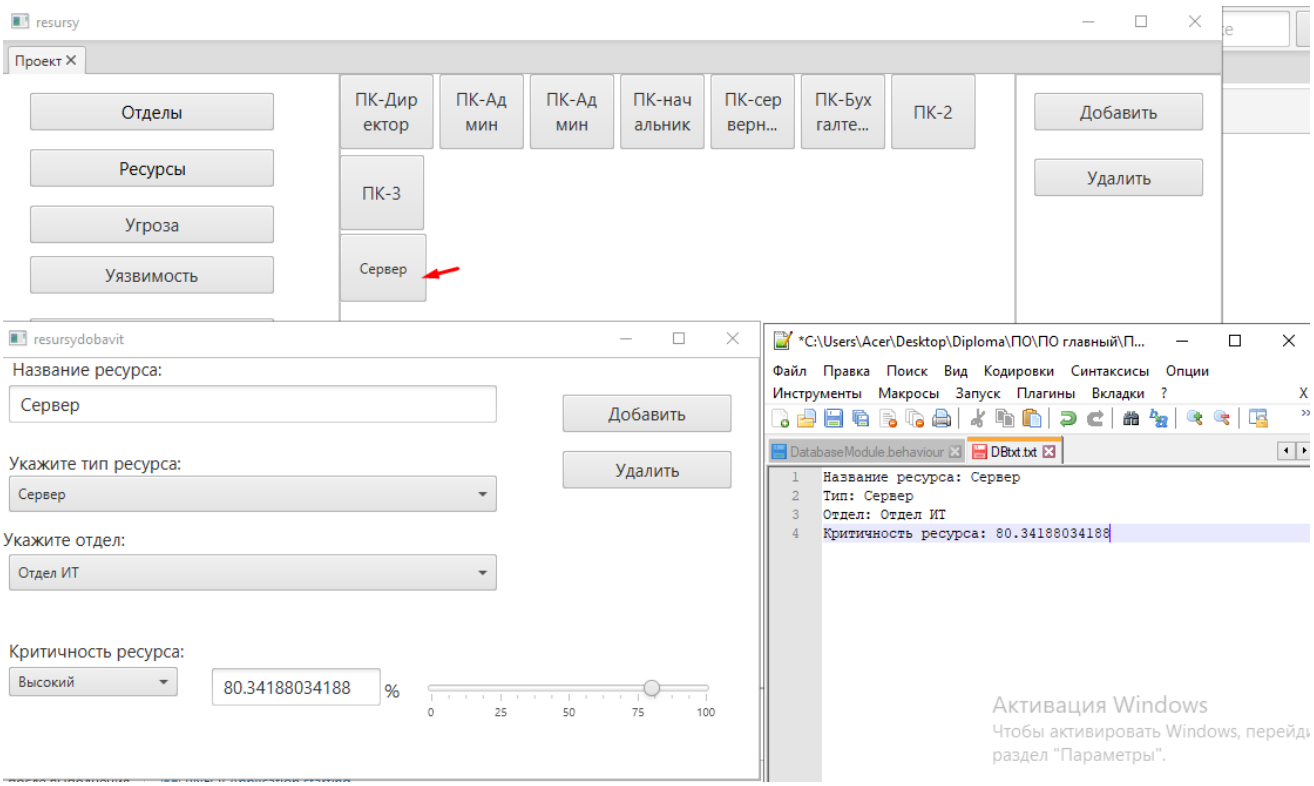


3.23 сурет – Барлық осалдықтар бойынша қауіп (қауіптердің ашылмалы тізімі)

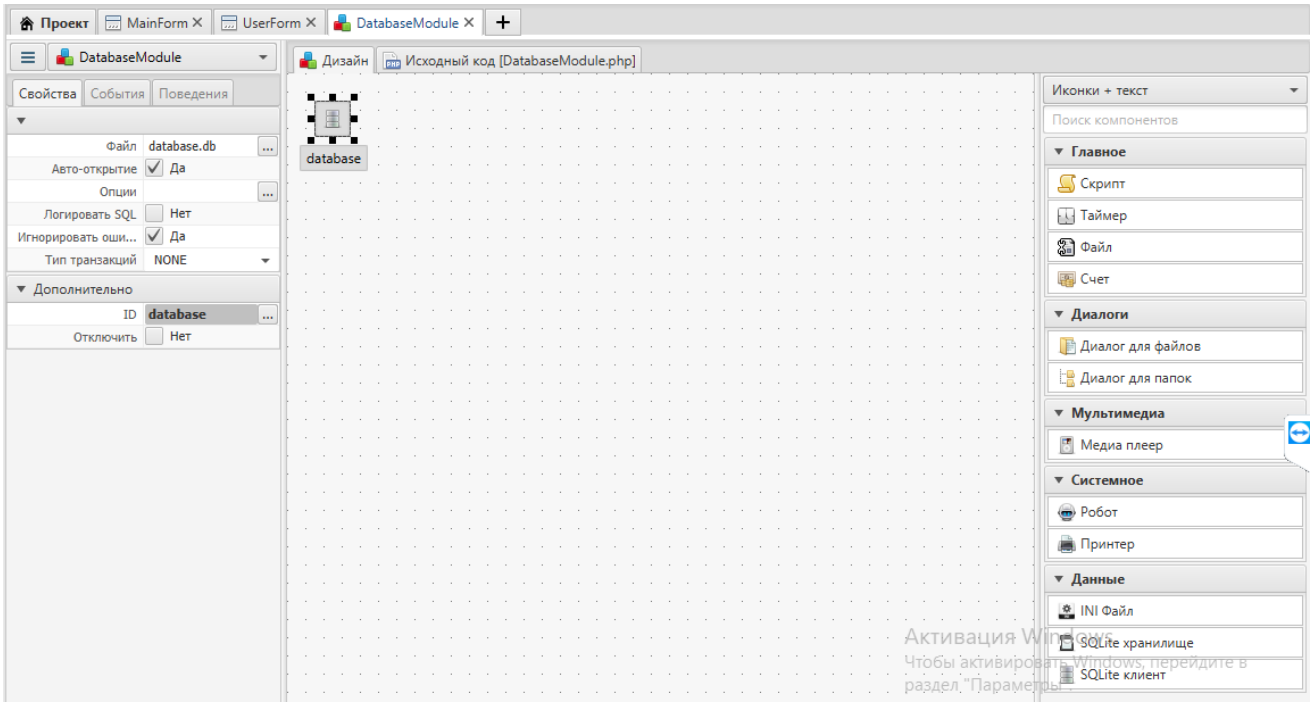


3.24 сурет – Барлық осалдықтар бойынша қауіп (осалдықтардың ашылмалы тізімі)

Енгізілген ресустар деректер базасынан тыс лог файл ретінде белгіленген «тхт» форматындағы құжатқа жазылып отырады, яғни есеп ретінде.



3.25 сурет – Есептеме ретінде сақтау



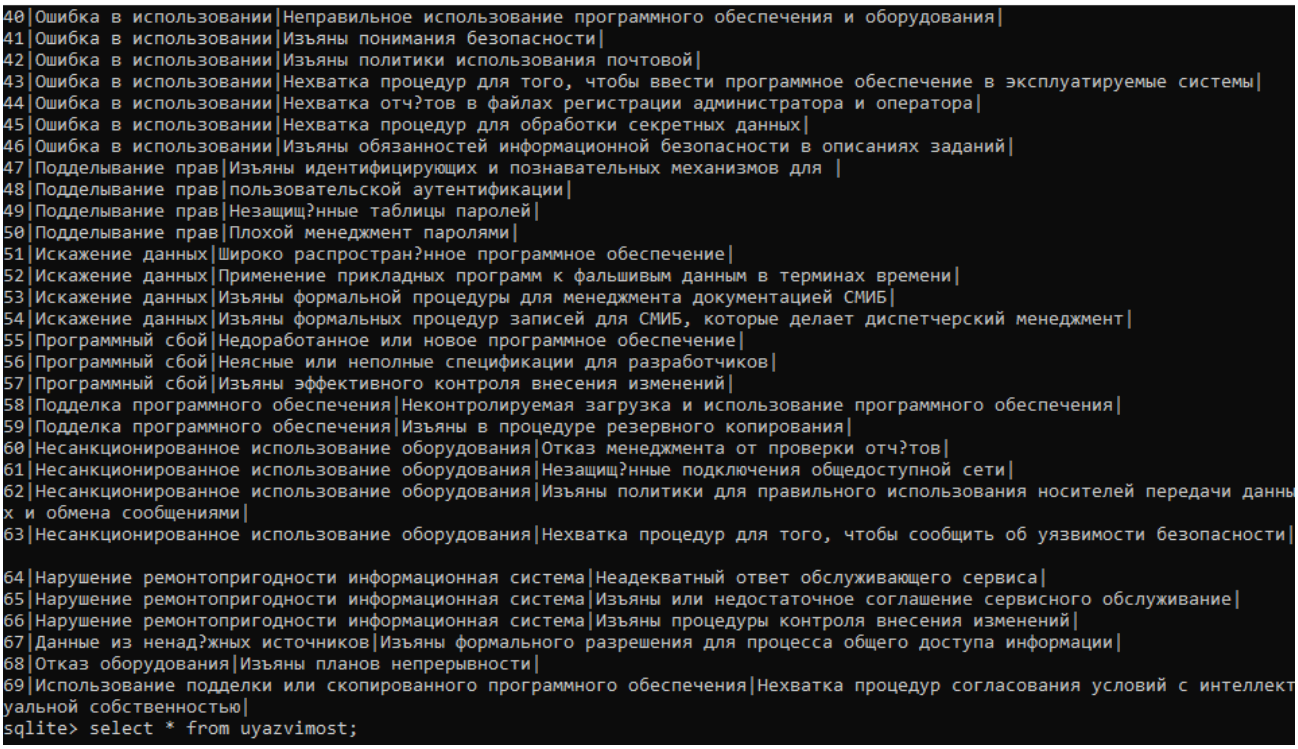
3.26 сурет – Деректер базасының қосылуы

```
91|Защита коммуникаций||Блокировка консоли сервера.
92|Защита коммуникаций||Конфигурации для второго (дублирующего) администратора.
93|Защита коммуникаций||Оборудование для соединения сетей.
94|Защита коммуникаций||Экранирование удаленного доступа.
95|Защита коммуникаций||Экранирование доступа извне.
96|Защита коммуникаций||Обзор сетевых сервисов.
97|Защита коммуникаций||Использование механизмов безопасности для NFS.
98|Защита коммуникаций||Использование механизмов безопасности для NIS.
99|Защита коммуникаций||Использование механизмов безопасности для sendmail.
100|Защита коммуникаций||Использование механизмов безопасности для rlogin, rsh. rcp.
101|Планирование непрерывности бизнеса||Формулировка требований по доступности.
102|Планирование непрерывности бизнеса||Определениекатегорийопасности,персональнаяответственностьза обеспечение безо
ости.
103|Планирование непрерывности бизнеса||Руководство по процедурам обеспечения безопасности
104|Планирование непрерывности бизнеса||Требования к ресурсам, необходимым для работы приложений
105|Планирование непрерывности бизнеса||Режим работы с минимальными ресурсами. Приоритеты информационных процессов.
106|Планирование непрерывности бизнеса||Исследованиевнешнихивнутреннихвозможностейобеспечения бесперебойной работы.
107|Планирование непрерывности бизнеса||Ответственные за действия в чрезвычайных ситуациях
108|Планирование непрерывности бизнеса|| План действий в чрезвычайных ситуациях
109|Планирование непрерывности бизнеса||План обеспечения бесперебойной работы в отдельных ситуациях.
110|Планирование непрерывности бизнеса||План обеспечения бесперебойной работы при выходе из строя связи.
111|Планирование непрерывности бизнеса||Тренировки по работе в чрезвычайных ситуациях.
112|Планирование непрерывности бизнеса||Резервное копирование и восстановление данных.
113|Планирование непрерывности бизнеса||План поставки оборудования.
114|Планирование непрерывности бизнеса||Соглашения с поставщиками.
115|Планирование непрерывности бизнеса||Звуковая сигнализация на случай чрезвычайных обстоятельств.
116|Планирование непрерывности бизнеса||Страхование.
117|Планирование непрерывности бизнеса||Обеспечение избыточности линий.
118|Планирование непрерывности бизнеса||Процедуры при обнаружении вирусов.
119|Планирование непрерывности бизнеса||Аспекты безопасности, связанные с FDD (дискеты).
120|Планирование непрерывности бизнеса||Регулярное резервное копирование жесткого диска сервера.
121|Планирование непрерывности бизнеса||Регулярное копирование данных конфигурации.
sqlite> select * from kontrmery;
```

3.27 сурет – Деректер базасындағы «Контрмерлер» тізімі

```
119| Угрозы, возникающие на предпроектном этапе.|Нарушения системы контроля доступа в помещениях. |
120| Угрозы, возникающие на предпроектном этапе.|Воровство.|
121| Угрозы, возникающие на предпроектном этапе.|Нападения.|
122| Угрозы, возникающие на предпроектном этапе.|Перехват в линиях связи|
123| Угрозы, возникающие на предпроектном этапе.|Неавторизованное использование информационной системы. |
124| Угрозы, возникающие на предпроектном этапе.|Злоупотребления, связанные с удаленным доступом.|
125| Угрозы, возникающие на предпроектном этапе.|Несанкционированный доступ к конфиденциальным данным, сохраненным в про
цессе инсталляции офисной АТС.Несанкционированный доступ к конфиденциальным данным, сохраненным в процессе инсталляции о
фисной АТС.|
126| Угрозы, возникающие на предпроектном этапе.|Перехват телефонных звонков и передаваемых данных. |
127| Угрозы, возникающие на предпроектном этапе.|Подслушивание.|
128| Угрозы, возникающие на предпроектном этапе.|Угрозы,исходящиеотперсонала(штатныхсотрудников)впроцессе обслуживания/а
дминистрирования информационной системы.|
129| Угрозы, возникающие на предпроектном этапе.|Подбор паролей.|
130| Угрозы, возникающие на предпроектном этапе.|Злоупотребления правами пользователей|
131| Угрозы, возникающие на предпроектном этапе.|Враждебные апплеты и вирусы.|
132| Угрозы, возникающие на предпроектном этапе.|Подслушивание и перехват сообщений|
133| Угрозы, возникающие на предпроектном этапе.|Несанкционированное копирование носителей данных.|
134| Угрозы, возникающие на предпроектном этапе.|Преднамеренное перепрограммирование факсимильных машин.|
135| Угрозы, возникающие на предпроектном этапе.|Враждебное использование методов социальной инженерии. |
136| Угрозы, возникающие на предпроектном этапе.|. Злоупотребление доступом к отдаленным портам для получения чужих данн
ых. |
137| Угрозы, возникающие на предпроектном этапе.|Атака IP Spoofing.|
138| Угрозы, возникающие на предпроектном этапе.|Злоупотребления с маршрутизацией данных. |
139| Угрозы, возникающие на предпроектном этапе.|Ненадлежащий учет пользователей, имеющих свободный доступ к сетевым рес
урсам.|
140| Угрозы, возникающие на предпроектном этапе.|Злоупотребления, связанные с удаленным управлением ресурсами информацио
нной системы.|
sqlite> select * from ugrozy;
```

3.28 сурет – Деректер базасындағы «Қауіптер» тізімі



3.29 сурет – Деректер базасындағы «Қауіптер» тізімі

Бөлім бойынша қорытынды: осы тарауда коммерциялық ақпарат қауіпсіздігі саласындағы ресурс үшін мүмкін тәуекелдер мәнін бағалауға және қорғаныс шараларын анықтауға бағытталған «Қауіптер мен осалдықтар моделі» негізінде тәуекелдерді бағалау бағдарламасы әзірленді. Бағдарламаның жұмыс алгоритмі мен интерфейсі сипатталды және жұмыстың толық функционалдығы көрсетілді, сонымен қатар компьютерге «Риск» бағдарламалық қамтамасыздандыруын орнатуға мүмкіндік беретін орнатушы әзірленді.

Сондай-ақ бағдарламалық тестілеу өткізілді. Нәтижесінде «Риск» 100% ауытқусыз тұрақты және болжамды түрде жұмыс істеді және барлық талаптарға және техникалық сипаттамаларға сәйкес келді.

4 Өміртіршілік қауіпсіздігі

4.1 Жұмыс жағдайын талдау

Дипломдық жұмыстың мақсаты ақпараттық қауіпсіздік қауіптерінің ықтималдығының мәнін болжау үшін қауіп-қатерді бағалаудың бағдарламалық қамтамасыз етуін әзірлеу.

Жұмыстың бұл бөлімінде «Ақпараттық және есептеуіш технологиялар институты» ғимаратының бірінші қабатында өрт хабарлағыш қондырғыларын жобалау және эвакуация жолдарын есептеу туралы шешім қабылданды.

«Ақпараттық және есептеуіш технологиялар институты» шаруашылық жүргізу құқығындағы республикалық мемлекеттік кәсіпорны. Институт құрамын 217 қызметкер, оның ішінде 4 ҰҒА академигі, 1 ҰҒА корр. мүшесі, 42 ғылым докторы, 42 ғылым кандидаты еңбек етеді. Институтта 90 жас мамандар (жасы 39-ға дейінгі) жемісті жұмыс істейді.

Ғимаратта ұзындығы 7 м, ені 5 м болатын 2 бөлме, ұзындығы 8 м, ені 7 м болатын 1 бөлме, ұзындығы 7 м, ені 4 м болатын 10 бөлме бар. Барлық бөлмелердің биіктігі 3 м. Әр бөлмеде 1-5 адамнан күніне 8 сағат жұмыс істейді [15].

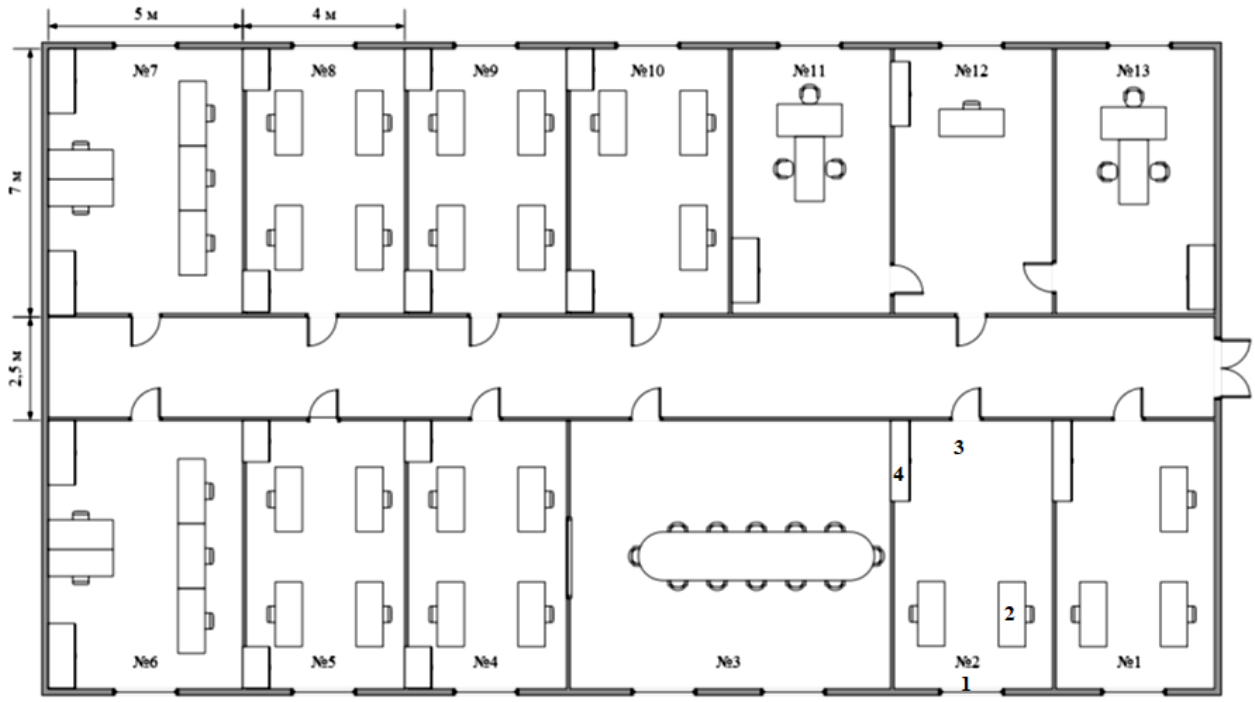
Бағдарламаны әзірлеу компьютерлік техниканы және электрондық жабдықты қолдану арқылы жүзеге асырылады. Бөлмеде 2 қызметкер жұмыс істейді, жұмыс режимі 9:00-ден 18:00-ге дейін. Еңбек қызметі В санатына жатады (бағдарламаларды жөндеу, аудару және редакциялау және т.б.) [16].

Қарастырылып отырған ғимараттағы жұмыс бөлмесі теміржолдардан, автомагистральдардан, әуежайдан алыс орналасқан, сондықтан жұмыс процесіне әсер ететін сыртқы шу көзі жоқ. Шу деңгейі ГОСТ 12.1.003-2014 [17] талаптарына сәйкес келеді.

Жұмыс бөлмесінің параметрлері:

- терезенің өлшемі 1,5 м*1,2 м;
- бөлме өлшемдері: ұзындығы 7 м, ені 4 м, биіктігі 3 м;
- жарық көздері: жарықшамдар – 4 дана, әрқайсысында 2 люминесцентті лампалар;
- бөлме мен жиһаздардың безендірілуі адамдарға жағымды жағдай жасау үшін көрнекі әрі қабырғалары жарық жасалған;
- бөлмені артық жарықтан қорғау үшін терезелерге пердешелер орнатылған;
- жасанды желдеткіш – салқындатқыш орнатылған;
- жұмыс орны жеңіл жұмыс санатына жатады (жеңіл физикалық, Іа санаты, жұмыс отырып жасалынады және физикалық белсенділікті талап етпейді).

4.1-суретте ғимараттың жоспары көрсетілген, онда жұмыс бөлмесі №2 бөлме 1 − терезе, 2 − жұмыс орны, 3 − есік, 4 − салқындатқыш.



4.1 сурет – Ғимараттың бірінші қабатының жоспары

Мекеме қызметкерлері көп уақытын компьютер алдында өткізеді, ал компьютерде жұмыс жасау тікелей жарық дәрежесіне, көру қабілетіне бағытталғандықтан, жарықтандыру жүйесі ескерілген жөн. Көздің көру қабілеті аймақтың жарықтандырылуымен тығыз байланысты. Бірінші қабатта орналасқан жұмыс аймағына қажетті табиғи жарық көзі жеткіліксіз. Сонымен қатар компьютерлердің саны көп болғандықтан олар бөлмеге шамадан тыс жылу және де химиялық заттар бөледі, осыған байланысты ауаның ауысу жүйесі тежеледі.

Зерттеулерге сәйкес, ДК пайдаланушылардың өздерін нашар сезіну себептерінің бірі монитор экранындағы кескіннің жарықтылығынан пульсациялану болып табылады. Жарықтандырудың пульсациясы жалпақ монитор жарықтану жұмысының ерекшелігіне байланысты. Қазіргі уақытта бұл параметр қалыпқа келтірілмеген, бірақ оған жалпы және жергілікті жарықтандырудың пульсациясы әсер етеді.

Компьютерде сағат бойы жұмыс істегенде, көздің демалуға қажетті фазалары болмайды, көз одан әрі күшейе түседі, олардың өнімділігі төмендейді. Көру органы ақпарат түсіргенде үлкен жүктеме алады, себебі пайдаланушы жиі экраннан бөлек әр түрлі қашықтықта орналасқан және әртүрлі жарықтандырылған мәтінге, пернетақтаға қарайды. Бүгінгі таңда миллиондаған пайдаланушылар көздің бұлыңғырлануына, жақын және алыс қашықтықтан жақын объектілерді ауыстыру қиындықтарына, көз аймағындағы жағымсыз әсерлерді сезіну - қызу әсері, қабақтың қызаруы, көздің қозғалысы кезіндегі ауыртпалыққа шағымданады.

ГОСТ 50923-96 [16] талаптарына сәйкес келесі кеңестер үздіксіз жұмыс істеу үшін оңтайлы болып табылады:

- арқа артқы жақа бірнеше градусқа созылады (бұл жағдай омыртқаны жеңілдетеді);
- қолдар үстелдің қолшаларына еркін түсіріледі;
- білезіктер мен білектер босаңсып, қылқаламдар білекпен ортақ осьте болады және олар иілмейді;
- аяқ еденге немесе арнайы тіреуішке мықтап қойылады.

4.1.1 Өртке қарсы шаралар

ҚР ҚНжЕ 2.02-05-2009 [18] талаптарына сәйкес барлық өндіріс мекемелері, қоймалар, әкімшілік және қосымша ғимараттар өрт сөндіргішпен және басқа өрт сөндіру құралдарымен қамтамасыз етіледі. Алғашқы өрт сөндіру құраладарының саны мен түрін анықтау үшін олардың физика-химиялық қасиеттерін, жанатын заттардың өрт сөндіру құралдарына қатынасын, ғимарат немесе бөлменің ауданы ескеріледі. Қысқа тұйықталу, желінің шектен тыс жүктелуі, үлкен ауысу кедергісі салдарынан болатын өрттердің алдын-алу үшін электр құрылғыларын монтаждау, эксплутациялау ережелері сақталынады.

Алғашқы өрт сөндіру құраладарының саны мен түрін анықтау үшін олардың физика-химиялық қасиеттері, жанатын заттардың өрт сөндіру құралдарына қатынасы, ғимарат немесе бөлменің ауданы ескеріледі.

Алғашқы құралдардың санын әр қабаттың деректерін ескеріп 4.1-кесте бойынша анықтаймыз.

Өртті автоматты түрде анықтау құралдары өрт жөнінде тез арада білуге мүмкіндік беретіндіктен, өрт қауіпсіздігінің шарттарының негізгілерінің бірі болып табылады.

Өрт хабарлағыштары жылулық, түтіндік және жарықтық болады. Өрт хабарлау құралдарының таңдауда электрлік сигнализация сенімді саналатындықтан таңдалынды.

Қысқа тұйықталу, желінің шектен тыс жүктелуі, үлкен ауысу кедергісі салдарынан болатын өрттердің алдын-алу үшін электр құрылғыларын дұрыс монтаждау, эксплутациялау ережелері сақталынады.

4.1.2 Өрт автоматикасы жүйелері мен қондырғыларын жобалауға қойылатын талаптар

Объектілерді автоматты өрт сөндіру және автоматты өрт сигнал беру жабдықтары, өрт кезінде хабарлау мен адамдарды эвакуациялауды басқару жүйелерімен жабдықтау бойынша жобалау-сметалық құжаттаманы әзірлеу кезінде Қазақстан Республикасының аумағында қолдануға рұқсат етілген мемлекеттік, мемлекетаралық және халықаралық стандарттардың талаптары, сондай-ақ ҚР ҚНжЕ 2.02-05-2009 [18] және ҚР ҚН 2.02-11 [19] Қазақстан

Республикасының құрылыс нормалары мен ережелері және белгіленген тәртіпте бекітілген басқа да нормативтік құжаттарды басшылыққа алынды.

Объектілерді импорт өндірісінің өрт автоматикасы жүйелері мен қондырғыларымен жабдықтау бойынша жобалау-сметалық құжаттамаларды әзірлеуге өрт қауіпсіздігі саласындағы уәкілетті органның жобалық шешімімен келіскен кезде өндіруші елдің қолдануға белгіленген тәртіпте рұқсат етілген нормативтік және техникалық құжаттамаларының талаптарына сәйкес рұқсат етіледі.

Объектілерді өрт автоматикасының жүйелері мен қондырғыларымен жабдықтауға арналған жобалау-сметалық құжаттаманы әзірлеуді осы қызмет түріне лицензиясы бар заңды және (немесе) жеке тұлғалар жүзеге асырады.

"Жобалауға арналған тапсырма" объектілерді өрт автоматикасының жүйелері мен қондырғыларымен жабдықтауға арналған жобалау-сметалық құжаттаманы әзірлеу үшін міндетті құжат болып табылады.

Жобалауға арналған тапсырманы әзірлеу тәртібі ҚР ЕЖ 2.02-05-2009 [18] басшылық құжаттың талаптарына сәйкес жүзеге асырылады.

Объектіні ішкі істер органдарының ведомстволық бағынысты мамандандырылған бөлімшелерінің қорғауына берген кезде өрт-күзет сигнал беру жабдығы жүйелерімен жобалауға арналған тапсырма аталған мамандандырылған бөлімшелермен келісілуге жатады.

Өрт автоматикасының жүйелері мен қондырғыларымен жабдықталуға жататын объектілерге арналған жобалау-сметалық құжаттама жобаның бас сәулетшісінің (бас инженердің) жауапты орындаушысының тиісті жазбасымен куәландырылады.

Объектілерді өрт автоматикасының жүйелері мен қондырғыларымен жобалаған кезде нормативтік құжаттардың міндетті талаптарынан бас тартуға жол берілмейді.

Кей жағдайларда осы нормативтік құжаттарды бекіткен мемлекеттік органдардың келісімі (рұқсаты) бар болғанда ғана нормативтік құжаттардың міндетті талаптарынан негізделген бас тартуға рұқсат етіледі.

Жобалаушылардың немесе тапсырыс берушілердің нормативтік құжаттардың міндетті талаптарынан бас тартуы жөніндегі өтінімдерін (сауалдарын) қажетті жағдайларда басқа да мүдделі уәкілетті органдар мен ұйымдарды тарта отыра, сәулет, қала құрылысы және құрылыс қызметі істері жөніндегі уәкілетті органның тиісті бөлімшелері қарайды. Мемлекеттік нормативтік құжаттардың талаптарынан негізді бас тартуды қарау үшін жобалаушылар және (немесе) тапсырыс берушілер дайындаған ұсынылған бас тартуды өтейтін қосымша шаралар тізбесі бар негіздеме мен мүдделі уәкілетті органдардың тиісті бөлімшелерінің қорытындысы (келісімі) беріледі.

Автоматты өрт сөндіру қондырғыларымен жабдықталуға жататын объектілерді және оларда нормативтік құжаттамалар бойынша тек қана өрт

сигнал беру жабдығы талап етілетін жеке үйлердің болуын жобалаған кезде олардың орнына техникалық-экономикалық негіздемелерді есепке ала отыра осы үйлерді автоматты өрт сөндіру қондырғыларымен қорғау қарастырылуға рұқсат етіледі.

4.1.3 Эвакуациялық жолдар мен шығуларды күтіп ұстауға қойылатын өрт қауіпсіздігі талаптары

Қоғамдық ғимараттардың эвакуациялық жолдары мен шығуларды пайдалану кезіндегі өрт қауіпсіздігі шешімдері ҚР ҚН 2.02-11-2002 [19] талаптарына сәйкес жобаланады.

Осыған орай эвакуациялық жолдар мен шығуларға жарық түсіру, саны, өлшемдері және көлемдік-жоспарлау шешімдері, сондай-ақ эвакуациялау жолдарында өрт қауіпсіздігі белгілері анықталады.

Эвакуациялық жолдары мен шығуларды пайдалану кезіндегі өрт қауіпсіздігін жобалауда келесі ережелерді сақтаңыз:

- эвакуация жолдарындағы есіктер еркін және ғимараттан шығатын бағыт бойынша ашылады.
- эвакуациялық шығулар есіктеріндегі тиектер ғимарат (құрылым) ішінде болатын адамдардың тиектерді ішінен кілтсіз ашу мүмкіндігін қамтамасыз етіледі.
- көлемді өздігінен жарқырайтын, автономды және электр желісінен қоректенетін, эвакуациялау жолында пайдаланылатын өрт қауіпсіздігі белгілері (оның ішінде "Эвакуациялық (қосалқы) шығу", "Эвакуациялық шығу есігі" деген жарық нұсқағыштар) үнемі дұрыс және қосылған күйінде болады.
- көрермен, көрсету, көрмелік және басқа залдарда жарық нұсқағыштарды адамдардың қатысуымен іс-шаралар өткізген уақытта қосуға рұқсат етіледі.
- эвакуациялық жарық түсіру жұмыстық жарық түсіру электр қорегі тоқтатылған кезде қосылады.

Эвакуациялық жолдар мен шығуларды пайдаланған кезде:

- эвакуациялық жолдар мен шығуларды (оның ішінде өтетін жерлер, дәліздер, тамбурлар, галереялар, лифті холлдары, басқыш алаңдары, басқыш шабақтары, есіктер, эвакуациялық люктер) түрлі материалдармен, бұйымдармен, жабдықтармен, өндірістік қалдықтармен, қоқыспен және басқа заттармен үйіп тастауға, сондай-ақ эвакуациялық шығу есіктерін шегелеп тастауға;
- шығу тамбурларында (пәтерлер мен жеке тұрғын үйлерді қоспағанда) киімге арналған кептіргіштер мен ілгіштер, гардеробты орналастыруға, сондай-ақ керек-жарақтар мен материалдарды сақтауға (оның ішінде уақытша);
- эвакуациялау жолдарында табалдырықтар (есіктердің ойықтарындағы табалдырықтарды есептемегенде), қозғалмалы және көтеріліп-түсірілетін есіктер мен қақпалар, айналатын есіктер мен турникеттер, сондай-ақ адамдарды еркін эвакуациялауға кедергі келтіретін басқа құрылғыларды орнатуға;

- қабырғалары мен төбелерін өңдеуге, қаптауға және бояуға арналған жанғыш материалдарды, сондай-ақ отқа төзімділік деңгейі V ғимараттарды есептемегенде, эвакуациялау жолындағы сатылар мен басқыш алаңдарын қолдануға;

- басқыш шабақтарының, дәліздердің, холлдар мен тамбурлардың өздігінен жабылатын есіктерін ашық күйінде бекітуге, сондай-ақ оларды алып тастауға;

- түтіндемейтін басқыш шабақтарының ауа аймақтарының терезе жапқыштарын шынылауға немесе жабуға;

- арқауланған шыныны есіктер мен фрамугтарды шынылауда жай шынымен ауыстыруға тыйым салынады.

Үй-жайдың технологиялық, көрмелік және басқа жабдықтарын орналастырған кезде, жобалау нормаларына сәйкес, эвакуациялаудың басқыш шабақтарына және басқа жолдарына эвакуациялық өтетін жерлер қамтамасыз етіледі.

Көпшілік адамдар болатын объектілерде электр энергиясы сөніп қалған жағдайда, қызмет көрсететін қызметкерлер құрамы электрлік қолшамдар қолданылады.

Қолшамдар санын басшы объектінің ерекшеліктеріне, кезекші қызметкерлер құрамының болуына, ғимараттағы адамдар санына байланысты анықталады, бірақ кезекші қызметкерлер құрамының әрбір кезекшісіне біреуден кем болмайды.

Көпшілік адамдар болатын ғимараттағы кілемдер, кілем алашалар және басқа еден төсеніштері еденге сенімді бекітіледі.

Эвакуациялау жолында жанған кезде жанғыш және уытты өңдеу материалдарды, кілемдерді және үстіңгі бетке жануды тез таратуға қабілетті басқа еден төсеніштерін қолдануға тыйым салынады.

4.2 Есептеу бөлімі

4.2.1 Өрт хабарлағыш қондырғыларының қажетті санын анықтау

Есеп әдістемелік нұсқауды негізге ала отырып орындалды [20]. Ғимаратта орналасқан, бөлмелер үшін жылулық және қол өрт хабарлағыш қондырғыларының қажетті санын анықтаймыз. Ғимаратта ұзындығы 7 м, ені 5 м болатын 2 бөлме, ұзындығы 8 м, ені 7 м болатын 1 бөлме, ұзындығы 7 м, ені 4 м болатын 10 бөлме және ұзындығы 29 м, ені 2,5 м болатын дәліз бар. Барлық бөлмелердің биіктігі 3 м.

ҚР ҚНжЕ 2.02-05-2009 [21] сәйкес, өрт сөндіру хабарлама қондырғыларының сан есебін бөлменің барлық ауданы бойынша жүргіземіз. Ол үшін келесі формуланы қолданамыз:

$$n = \frac{F_ф}{F_з} \quad (4.1)$$

мұндағы, Fф – бөлменің ауданы, м2;

Fз – бір хабарлама қондырғысымен бақыланатын аудан 20 м^2 деп қабылдаймыз (техникалық мәліметтер).

Өрт хабарлағыш қондырғысының орнату биіктігі 3,5 м-ге дейін болса, бақыланатын аудан 25 м2, мұнда барынша көп аралық алынады, яғни хабарлама қондырғыларының арасында 5 м аспайтын, хабарлама қондырғысынан қабырғаға дейін аралық 2,5 м болады.

Осыған сәйкес ғимараттың бірінші қабатында орналасқан барлық бөлмелер үшін автоматты өрт сөндіру хабарлама қондырғылар санын анықтаймыз.

№6 және №7 бөлмелерінің ауданы – 35 м^2.

$$n = \frac{F_ф}{F_з} = \frac{35}{20} = 1{,}75$$

Бұл екі бөлмеге 2 жылулық хабарлағыштан қолданамыз.

№3 бөлме ауданы – 56 м^2.

$$n = \frac{F_ф}{F_з} = \frac{56}{20} = 2{,}18$$

Бұл бөлмеде 3 жылулық хабарлама қондырғысын қолданамыз.

Қалған он бөлме ауданы – 28 м^2.

$$n = \frac{F_ф}{F_з} = \frac{28}{20} = 1{,}14$$

Бұл бөлмелер үшін 2 жылулық хабарлағыштан қолданамыз.

Дәліздің ені 3 м-ден аз болса, түтіндік хабарлама қондырғылары арасындағы аралықты 15 м-ге дейін ұзартылады, сонымен бірге қабырғадан хабарлама қондырғысына дейінгі аралық 4,5 м-ден аспайды.

Дәліздің ауданы – 72,5 м^2.

$$n = \frac{F_ф}{F_з} = \frac{72{,}5}{20} = 3{,}625$$

Дәлізде 4 жылулық хабарлама қондырғысын қолданамыз.

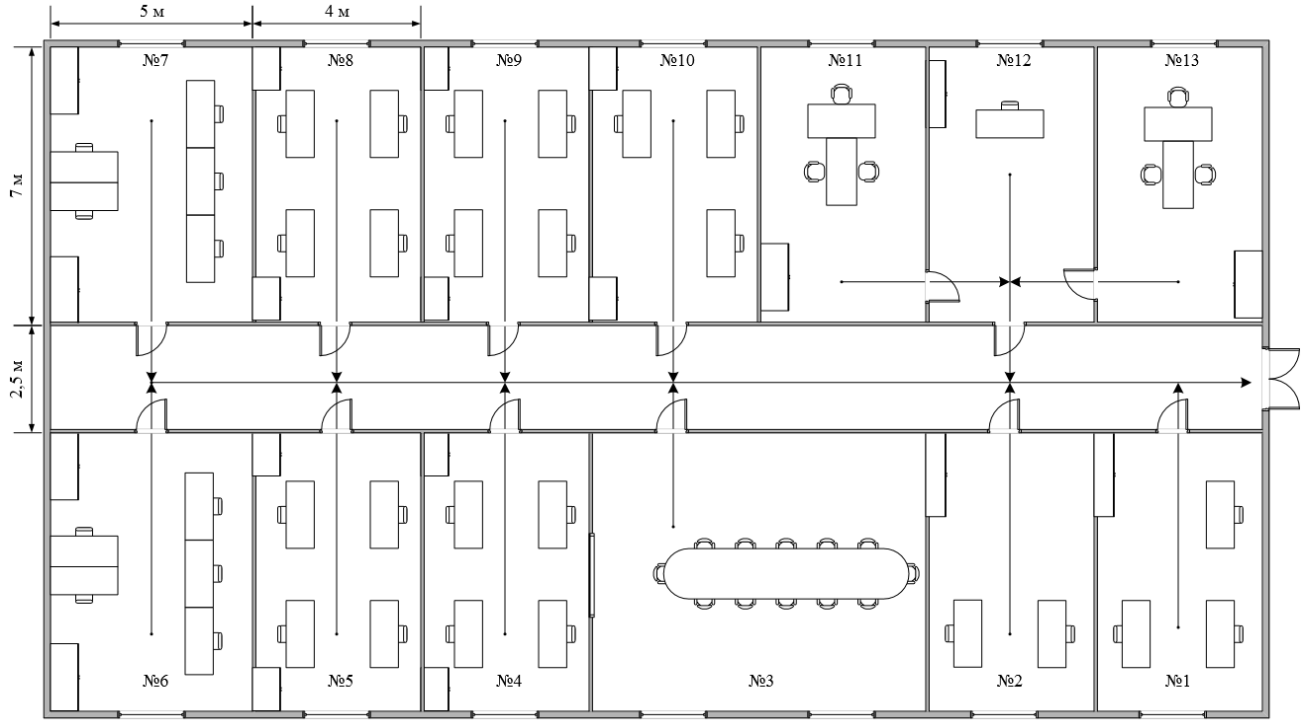
Қол өрт сөндіру хабарлама қондырғыларының санын қолданамыз. Әкімшілік бөлмелерде ғимараттың шығу есіктерінде және баспалдақ алаңына шығу жерлерінде 2-ден аспайтын қол өрт сөндіру хабарлама қондырғыларын орнату рұқсат етіледі. Сондықтан 2 қол өрт сөндіру хабарлама қондырғысын қолданамыз.

Есептеудің нәтижесінде ғимаратқа барлығы 31 жылулық өрт хабарлағыш қондырғысы және 2 қол өрт хабарлағыш қондырғысы орнатылды.

4.2.2 Эвакуация жолдарын есептеу

Есеп әдістемелік нұсқауды негізге ала отырып орындалды [22]. Адамдарды эвакуациялаудың есептік уақыты ғимараттан соңғы адамның шыққан уақытымен белгіленеді.

Эвакуация процесін модельдеудің алдында ғимараттағы эвакуация жолдарының схемасы беріледі. Эвакуация жолдарының барлығы ұзындығы l және ені d эвакуациялық учаскелерге бөлінеді. Жобаланатын ғимараттар үшін эвакуация жолдарының әрбір бөліктің ұзындығы мен ені жоба бойынша, ал салынған ғимараттар үшін факт бойынша қабылданады. Эвакуациялық учаскелер жазық және еңіс (төмен түсетін баспалдақ, жоғары көтерілетін баспалдақ және пандус) болуы мүмкін. Есік ойығындағы жол ұзындығы нөлге тең деп қабылданады.



4.2 сурет – Ғимараттың бірінші қабатының эвакуациялық жолдарының жоспары

Жалпы ғимараттан эвакуациялау уақытын табу үшін эвакуациялау жолын екі учаскеге бөлеміз. Бірінші учаскеде бөлмеден шығу уақытын, екінші учаскеде дәліз бойымен қозғалыс уақытын тауып, бір-біріне қосамыз.

Жалпы ғимараттан эвакуациялау уақыты мынадай формула бойынша анықталады:

$$t = t_1 + t_2 + ... + t_i \quad (4.2)$$

Әр бөлікті жүріп өту уақыты келесі формула бойынша анықталады:

$$t_i = \frac{l_i}{\vartheta_i} \quad (4.3)$$

мұндағы, D – адам ағынының тығыздығы, төмендегі формула бойынша есептеледі:

$$D = N\frac{f}{ld} \quad (4.4)$$

мұндағы, N – адам саны;

l – жолдың ұзындығы;

d – жолдың ені;

f – адамның көлбеу проекциясының орташа ауданы, ол 0,1-қа тең.

Бөлме ішіндегі адам ағынының тығыздығы:

$$D_1 = N_1\frac{f}{l_1 d_1} = 5\cdot\frac{0{,}1}{5\cdot 1{,}5} = 0{,}066\ \text{м}^2/\text{м}^2$$

4.1-кесте – Адам ағынының тығыздығы бойынша оның жылдамдығы және қарқындылығы

Адам ағынының тығыздығы D, $м^2/м^2$	Көлденең жол		Есіктің ойығы
	Жылдамдық ϑ, м/мин	Қарқындылық q, м/мин	Қарқындылық q, м/мин
0,01	100	1	1
0,05	100	5	5
0,1	80	8	8,7
0,2	60	12	13,4
0,3	47	14,1	16,5
0,4	40	16	18,4
0,5	33	16,5	19,6
0,6	27	16,2	19
0,7	23	16,1	18,5
0,8	19	15,2	17,3
0,9	15	13,5	8,5

4.1-кесте бойынша 0,066 м^2/м^2 адам ағынының тығыздығына горизонтальды жолда адам ағынының 100 м/мин-ге тең жылдамдық және 5 м/мин-ге қарқындылық сәйкес келеді [23].

Бөлмеден шығу уақыты:

$$t_i = \frac{l_i}{\vartheta_i} = \frac{5}{100} = 0{,}05 \text{ мин}$$

Есіктер алдында адамдар жиналып, қозғалыс ақырындайды. Кідіру уақыты мынадай формула бойынша анықталады:

$$\Delta t_i = N_{эв} f \left(\frac{1}{q_{ec} d_{ec}} - \frac{1}{q_i d_i} \right) \tag{4.5}$$

$$\Delta t_i = N_{эв} f \left(\frac{1}{q_{ec} d_{ec}} - \frac{1}{q_i d_i} \right) = 5 \cdot 0{,}1 \left(\frac{1}{5 \cdot 1} - \frac{1}{5 \cdot 1{,}5} \right) = 0{,}93 \text{ мин}$$

Дәліз бойымен қозғалатын адам ағынының тығыздығы:

$$D_2 = N_2 \frac{f}{l_2 d_2} = 37 \cdot \frac{0{,}1}{29 \cdot 2{,}5} = 0{,}051 \text{ м}^2/\text{м}^2$$

4.1- кесте бойынша ϑ_2=5 м/мин, q_2=5 м/мин.

$$t_2 = \frac{l_2}{\vartheta_2} = \frac{29}{100} = 0{,}29 \text{ мин}$$

Басты есік алдында кідіру уақыты:

$$\Delta t_i = N_{эв} f \left(\frac{1}{q_{ec} d_{ec}} - \frac{1}{q_i d_i} \right) = 37 \cdot 0{,}1 \left(\frac{1}{5 \cdot 2} - \frac{1}{5 \cdot 2{,}5} \right) = 0{,}074 \text{ мин}$$

Жалпы ғимараттан эвакуациялау уақыты:

$$t = 0{,}05 + 0{,}93 + 0{,}29 + 0{,}074 = 1{,}344 \text{ мин}$$

Есептеу нәтижесінде жалпы ғимараттан эвакуациялау уақыты 1,344 мин болатыны анықталды. Бұл эвакуациялауға қажетті 2 мин уақыттан аспайды, демек талап орындалады.

Бөлім бойынша қорытынды: бұл бөлімінде жұмыс аймағындағы жұмыс жағдайына талдау жасалды. Еңбек жағдайларының деңгейі жұмысшылар үшін қолайлы деп танылды. Ғимаратының бірінші қабатында өрт хабарлағыш қондырғыларын жобалау және эвакуация жолдарын есептеу орындалды. Ғимаратқа барлығы 31 жылулық өрт хабарлағыш қондырғысы және 2 қол өрт хабарлағыш қондырғысы қажет. Жалпы ғимараттан эвакуациялау уақыты 1,344 мин болды. Бұл эвакуациялауға қажетті 2 мин уақыттан аспайды, яғни талапқа

сай келеді. Бұл есептеулердің нәтижесінде ғимараттағы адамдар өрттің басталғанын дер кезінде біліп, ғимараттан уақытысында шығып үлгереді.

5 Жобалық тәуекелдерді бағалау

5.1 Тәуекелді талдау және бағалау

Дипломдық жұмыстың осы бөлімінде біз бағдарламалық қамтамасыз етуді әзірлеу кезінде туындайтын жобалық тәуекелдерді бағалаймыз.

Жобалық тәуекелі (project risk) – жоба нәтижелеріне оң немесе теріс әсер ететін кез келген оқиға немесе шарт. Жобалық тәуекелдердің ағымдағы проблемалардан айырмашылығы-тәуекелдер болашақ, ықтимал теріс нәтижелерге әсер етеді. Егер тәуекелдерді басқару процесі тиімсіз болса немесе мүлде болмаса, онда теріс тәуекелдер жобаның орын алған мәселелеріне айналуы мүмкін. Бәсекеге қабілетті болу үшін компаниялар жобалар портфелі бойынша тәуекелдерді басқару процесін қолдауы тиіс.

Маңызды объектілердің тәуекелдерін есептеу үшін екі фактор бойынша тәуекелді бағалау әдістемесі қолданылды.

Бірінші кезеңде теріс әсер қауіптілікке ұшыраған әрбір ресурс үшін алдын-ала анықталған шкала бойынша бағаланады. Екінші кезеңде, берілген шкала бойынша, әрбір қауіпті іске асыру мүмкіндігі бағаланады. Үшінші кезеңде тәуекел көрсеткіші есептеледі. Төртінші кезеңде қауіп-қатер факторының мәні бойынша дәрежеленеді.

Әрбір теріс тәуекел қандай да бір түрде зиян келтіреді (жобаның құнын немесе мерзімін ұлғайту, жоба сапасының төмендеуі және т. б.). Залалдың сандық мәнін анықтау үшін тәуекел қаупі ұғымы енгізілді.

Тәуекел қаупі (V) – тәуекелге әкеп соғатын теріс салдардың қауіптілік дәрежесі. Бұл шара абсолютті (мысалы, ақшалай) шаманы, бастапқы мәннен шаманың пайыздық ұлғаюын, сондай-ақ тәуекел қатерін бағалаудың кейбір салыстырмалы шкаласынан жай мәнді де білдіруі мүмкін. Ақша эквивалентіндегі тәуекел қатерлерін айқындау жоба инвесторлары үшін неғұрлым түсінікті.

Әдетте, жобалық тәуекел қаупінің төрт негізгі түрін анықтайды: жобаның құны, жобамен жұмыс істеу мерзімі, жобаның мазмұны мен сапасы. Осы тұста жоба тәуекелдерінің қайсысын қалай анықтауға болады деген сұрақ туындайды.

5.1-кесте – Әр түрлі шамаларды бағалау шкаласы

Тәуекел қаупі	Жобаның құнын ұлғайту	Мерзімі	Техникалық мәліметтер
1 – Төмен	1%-дан аз	1 аптаға өсу	Пайдалану сапасына болмашы әсер ету
2 – Орташа	5%-дан аз	2 аптаға өсу	Пайдалану сапасына орташа әсер ету

5.1-кестетің жалғасы

3 – Жоғары	10%-дан аз	1 айға өсу	Пайдалану сапасына жоғары әсер ету
4 – Өте жоғары	10% және одан жоғары	1 айдан көп уақытқа өсу	Мақсат орындалмауы мүмкін

Әрбір жобалық тәуекелді сипаттайтын келесі маңызды компонент тәуекел ықтималдығы болып табылады.

Тәуекел ықтималдығы (Р) - бұл тәуекел тұжырымдамасында сипатталған салдардың туындау мүмкіндігін айқындайтын пайыздық шама. Тәуекел салдарларының пайда болу ықтималдығының мәні әрдайым 0% - дан артық болады, әйтпесе, тәуекел ешқашан орын алмайтын оқиға болып табылады. Осыған ұқсас, тәуекел ықтималдығы 100% - ға тең болуы мүмкін емес, әйтпесе тәуекелде белгісіздік жоқ және ол қазірдің өзінде аяқталған оқиға (бар мәселе немесе алынған пайда) болып табылады. Жобалаушы топ үшін тәуекелдің ықтималдығын бағалау қарапайым оңай жұмыс емес болып табылмайды, алайда жобалық топта бар тәуекелдер туралы статистикалық деректер ұқсас жобалардағы тәуекелдердің ықтималдығын бағалауға көмектеседі.

Көптеген жағдайларда жинақталған деректер мен тәжірибені пайдалана отырып, одан әрі сандық мәндер түрінде өзгертілуі мүмкін қарапайым сөздік тұжырымдар түріндегі тәуекел салдарларының ықтималдығын бағалауға болады.

Келесі кестеде жеті деңгей бойынша тәуекел салдарларының туындау ықтималдығын көрсетілген (5.2-кесте).

5.2-кесте – Тәуекел ықтималдығының жеті деңгейі

Сөздік сипаттамасы	Ықтималдықтың мүмкін аралығы	Есептеулердің орташа мәні
1 - Өте төмен ықтималдылық	1% - 14%	7%
2 - Төмен ықтималдық	15% - 28%	21%
3 – Болмау мүмкіндігі жоғары	29% - 42%	35%
4 - Орташа ықтималдық	43% - 57%	50%
5 – Болу мүмкіндігі жоғары	58% - 72%	65%
6 - Жоғары ықтималдық	73% - 86%	79%
7 – Өте жоғары	87% - 99%	93%

Тәуекелдің сөздік сипаттамасын немесе сандық интервалды пайдалана отырып, ұқсас кестелердің көмегімен тәуекелдің ықтималдығына баға беруге болады. Бағалау жүргізу кезінде тәуекелдердің әрқайсысы үшін мәндердің бір аралығын пайдалану қажет, әрі қарай олардың әрқайсысынан жұмыс басымдығын анықтау үшін.

Тәуекелдермен жұмыс істеу басымдылығы үшін жоғарыда қарастырылған тәуекел компоненттерінің (ықтималдықтар мен қауіптер) жиынтығын пайдаланылады. Бұл жиынтық тәуекелдің мәні деп аталады [24].

Тәуекелдің күтілетін мәні (R) – тәуекелдің ықтималдығы мен оның қауіптілігін ескере отырып, қауіп-қатер салдарларының маңыздылығының әмбебап өлшемі. Тәуекелдің мәні келесі формула бойынша, сонымен қатар кесте арқылы да есептелінеді:

$$R = P \cdot V, \tag{5.1}$$

мұндағы P – тәуекел ықтималдығы, V – тәуекел қаупі.

5.3-кесте – Оқиғалар қаупі мен ықтималдығы бойынша тәуекелді анықтау шкаласы

Тәуекелді анықтау шкаласы								
	Ықтималдық аралығы	Өте төмен ықтималдылық	Төмен ықтималдылық	Болмау мүмкіндігі жоғары	Орташа ықтималдық	Болу мүмкіндігі жоғары	Жоғары ықтималдық	Өте жоғары
Тәуекел қаупі	Төмен	1	2	3	4	5	6	7
	Орташа	2	4	6	8	10	12	14
	Жоғары	3	6	9	12	15	18	21
	Өте жоғары	4	8	12	16	20	24	28

Ақпаратты өңдеу құралдарын, әдістерін және қорғалатын ақпарат тізбесін талдау нәтижесінде активтердің келесі тізбесін бөліп көрсетуге болады:

- бағдарламалық қамтамасыз ету құжаттары;

1. архитектуралық/жобалық – бағдарламалық қамтамасыз етуді шолу, оның ішінде бағдарламалық қамтамасыз етуді жасау кезінде пайдаланылуы тиіс жұмыс ортасы мен қағидаттарының сипаттамасы;
2. код, алгоритмдер, интерфейстер, API техникалық құжаттамасы;
3. пайдаланушы құжаттамасы – соңғы пайдаланушылар, жүйе әкімшілері және басқа қызметкерлер үшін нұсқаулар;
4. маркетингтік құжаттама;
5. коммерциялық ақпарат

- деректер қоймасы
- бағдарламаның бастапқы коды
- қызметкер;

- Аспаптық құралдар-жобалауды және әзірлеуді немесе конфигурацияны басқару құралдары, кодтар талдағыштары, баптау бағдарламалары, тестілік талдағыштар, датчиктер, генерациялайтын және құрастыратын бағдарламалық құралдар, бағдарламалар кодын оңтайландыру құралдары, кітапханалар жиынтығы, байланыс редакторы, сервистік құралдар (утилиттер), бағдарламаларды әзірлеудің біріктірілген ортасы, бағдарламалық кешен өнімдерін қолдау және басқару жүйесі.

Алынған мәліметтер негізінде және (5.1) формуланы пайдалана отырып, ресурс тәуекелін есептейміз. 5.4-кестеде активтер мен әрбір қауіптің осалдығы үшін ақпараттың қол жетімділігінің, тұтастығының және құпиялылығының әлеуетті қатерлері берілген.

Бірінші кезеңде ағымдағы тәуекел деңгейі есептелді, содан кейін ГОСТ Р ИСО/МЭК 15408-1-2012 [24] белгілеген қауіпсіз БҚ әзірлеу бойынша шаралар қолданылды. Кейін тәуекелді қайта есептеу жүргізілді. Алынған мәндер 5.4-кестеде көрсетілген.

5.4 кесте – Тәуекелдерді бағалаудың қорытынды кестесі

№	Қауіптер	Осалдықтар	Жоғарғы мәні	Қорғаныс шаралары	Қалдық мәні
1 Бағдарламалық қамтамасыз ету құжаттамасы					
1.1	Құжаттардың немесе тасымалдаушылардың ұрлануы	Рұқсатсыз көшіру	12	Қолжетімділікті шектеу, парольдік қорғауды ұйымдастыру	9
1.2	Заңнаманы немесе нормативтік базаны бұзу	Криптографиялық тәсілдердің дұрыс қолданылмауы	4	Ақпараттық қауіпсіздік саясатын анықтау, құжаттау және сақтау	2
1.3	Деректерді өзгерту	Ақпараттық жүйемен жұмыс істеу кезінде белгіленген ережелерді білмеу немесе сақтамау және деректерді өзгерту	8	Конфигурация элементтеріне рұқсатсыз қолжеткізуден қорғау; конфигурация элементтерін резервтік көшіру; оқиғаларды тіркеу	6
2 Деректер қоймасы					
2.1	Деректерді ұрлау	Пайдаланылмайтын қызметтер және ашық порттар	12	Порттардың анализаторлары, желілік мониторинг	8

5.4 кестетің жалғасы

2.2	Ақпаратқа рұқсатсыз қол жеткізу	Қол жетімділікті басқару саясатының болмауы немесе дұрыс қолданылмауы, сақтау құралын дұрыс тазартусыз беру немесе қайта пайдалану	12	Қол жеткізуді басқару, серверлерде сақталатын мәліметтерді қорғауға арналған криптографиялық шешімдер жиынтығы, үнемі жаңартулар	9
2.3	Ақпаратты сақтау құралдарының ескіруі	Жабдықты мерзімді ауыстыру схемасының болмауы	2	Құралдардың эксплуатациясы	1
3 Аспаптық құралдар					
3.1	Температуралық режимнің бұзылуы	Жабдықтың температуралар ауытқуына ұшырауы	2	Реттелетін жұмыс режимі	1
3.2	Ақпаратты жоғалту	Физикалық қорғаудың, резервтік көшіру рәсімдерінің болмауы	9	Қолжетімділікті басқару жүйелері, қоршау және физикалық оқшаулау, конфигурация элементтерінің резервтік көшіру	6
3.3	Қызмет көрсетуден бас тарту	Өзгерістерді басқарудың жеткіліксіздігі, алмасу буферінің толып кетуі	12	Басып кіруді анықтау жүйесі, жүйені резервтік қалпына келтіру	10

5.4 кестетің жалғасы

4 Бағдарламаның бастапқы коды					
4.1	Бастапқы кодқа осалдықтарды енгізу қаупі	Аспаптық құралдарды пайдалану саясатының болмауы және БҚ конфигурациясын басқару шараларының жеткіліксіздігі	6	Бағдарлама архитектурасының нақтыланған жобасы негізінде бағдарламаны жасау;бағдарламаның бастапқы кодын статистикалық талдау, бағдарламаның бастапқы кодын сараптау, бағдарламаның осалдығын жүйелі түрде іздеу жүргізу	3
4.2	Бағдарламаның жаңартуларына осалдықтарды енгізу қаупі	Рұқсатсыз өзгерістерді анықтау мүмкіндігінің болмауы	2	Пайдаланушыға жіберу процесінде тұтастықтың бұзылуына байланысты ақпараттың қауіпсіздігіне қауіп-қатерден БҚ қорғауды қамтамасыз ету; бағдарламаның осалдықтарын жүйелі түрде іздестіруді жүргізу; конфигурация элементтерін резервтік көшіру	1
4.3	Деректер модификациясы	АҚ шабуылдары мен қатерлерінің типтік сценарийлерін ескерілмеуі	6	Қолжетімділікті шектеу, парольдік қорғау; конфигурация элементтерін резервтік көшіру	4

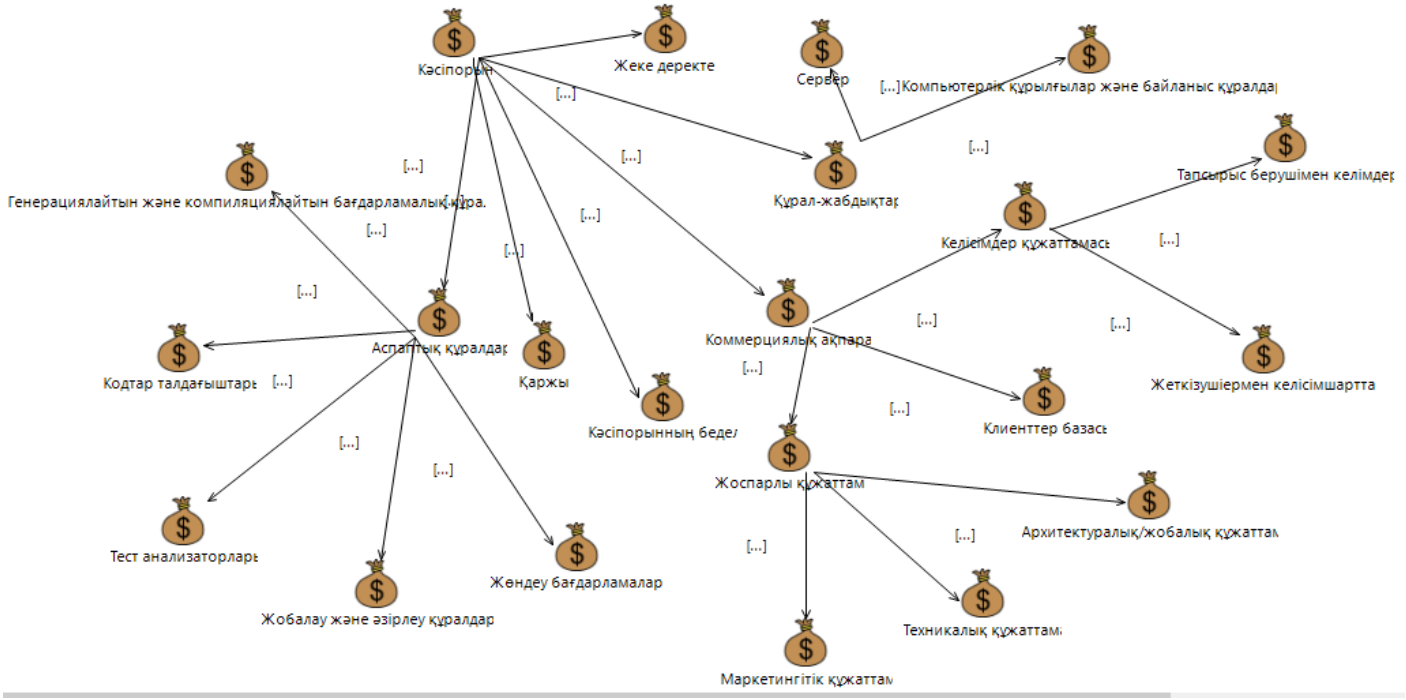
5.4 кестетің жалғасы

5 Қызметкер						
5.1	Жүйенің ақпараттарына немесе бағдарламаға рұқсатсыз қол жеткізу	БҚ әзірлеу ортасының объектілеріне қолданылатын және сыни ақпаратқа рұқсаты бар тұлғалар шеңберін және әзірлеу ортасының объектілерімен орындалуы мүмкін операцияларды шектеуге бағытталған қол жеткізуді бақылау шараларындағы кемшіліктер	8	Қолжетімділікті шектеу, парольдік қорғау; басып кіруді анықтау жүйесі, жүйені резервтік қалпына келтіру	6	
5.2	Деректерді өзгерту	Өңделетін деректерді тексерудің болмауы, қолжетімділікті шектеудің дұрыс болмауы	8	Конфигурация элементтеріне рұқсатсыз қолжеткізуден қорғау; конфигурация элементтерін резервтік көшіру; оқиғаларды тіркеу	6	
5.3	Бағдарламалық қате	Қызметкердің біліксіздігі, құралдардың дұрыс жұмыс істемеуі	9	Қызметкерлерді мерзімді оқыту	6	

5.2 CORAS құралы арқылы тәуекелдерді талдау

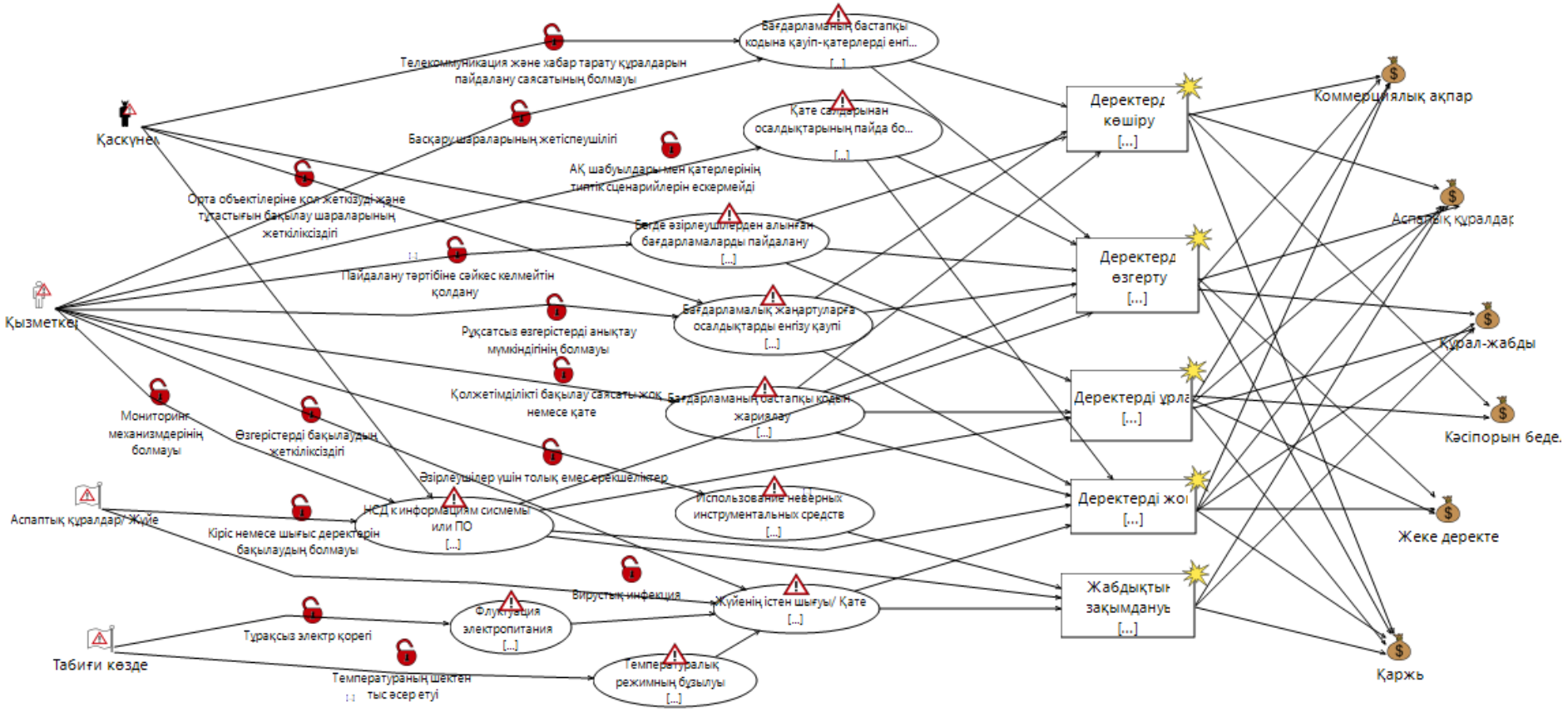
Coras бағдарламалық қамтамасыз ету саласында объектілі модельдеу үшін UML-графикалық сипаттау тілін қолданады.

Тәуекелдерді талдаудың көрнекілігі үшін Coras бағдарламалық құралы пайдаланылды. Жоғарыда сипатталған активтердің диаграммасын және олардың өзара байланысын құрамыз (5.1-сурет).



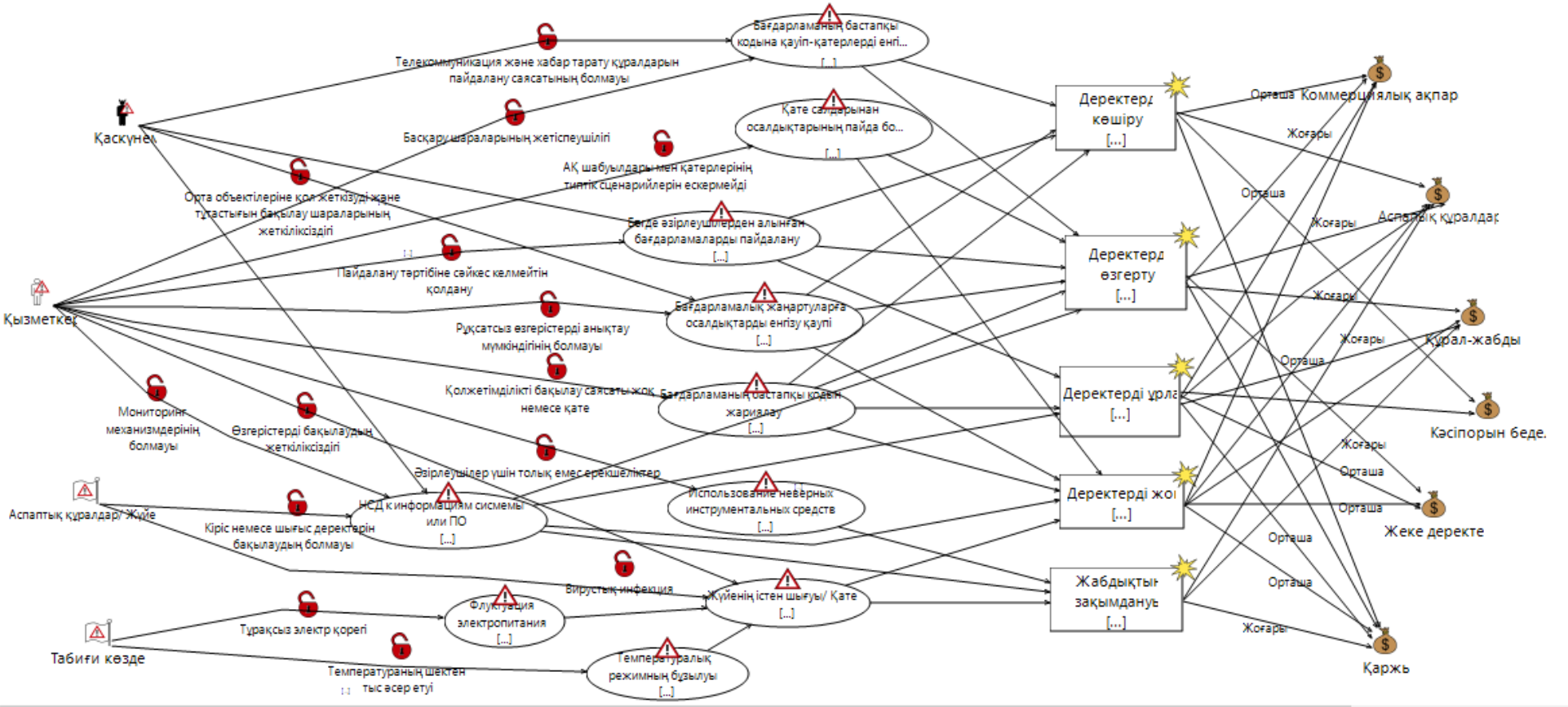
5.1 сурет – Активтер диаграммасы

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



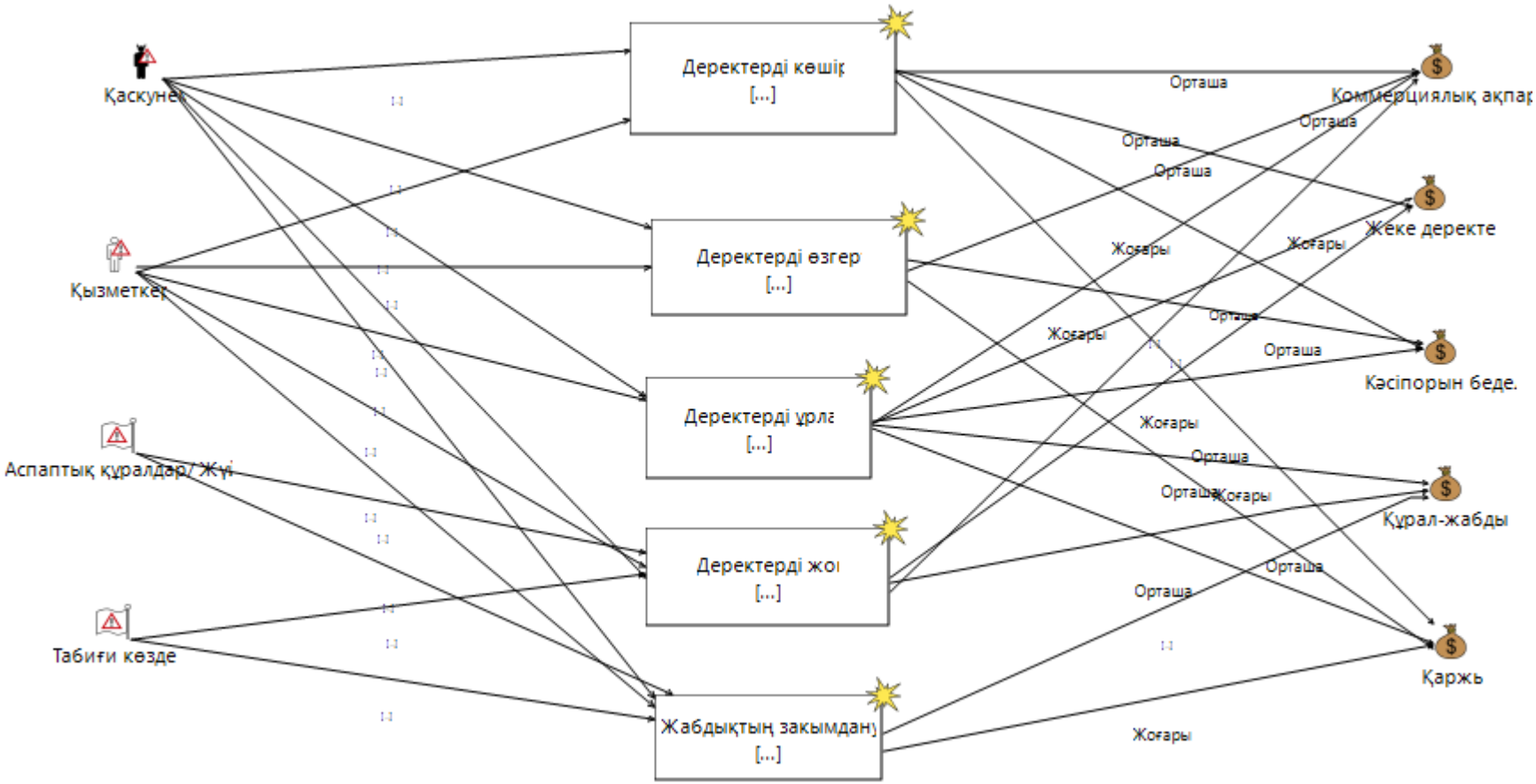
5.2 сурет – Қауіптер моделі

Әрбір актив үшін өмірлік цикл кезеңінде әрбір қауіптің туындау ықтималдығын белгілейміз.



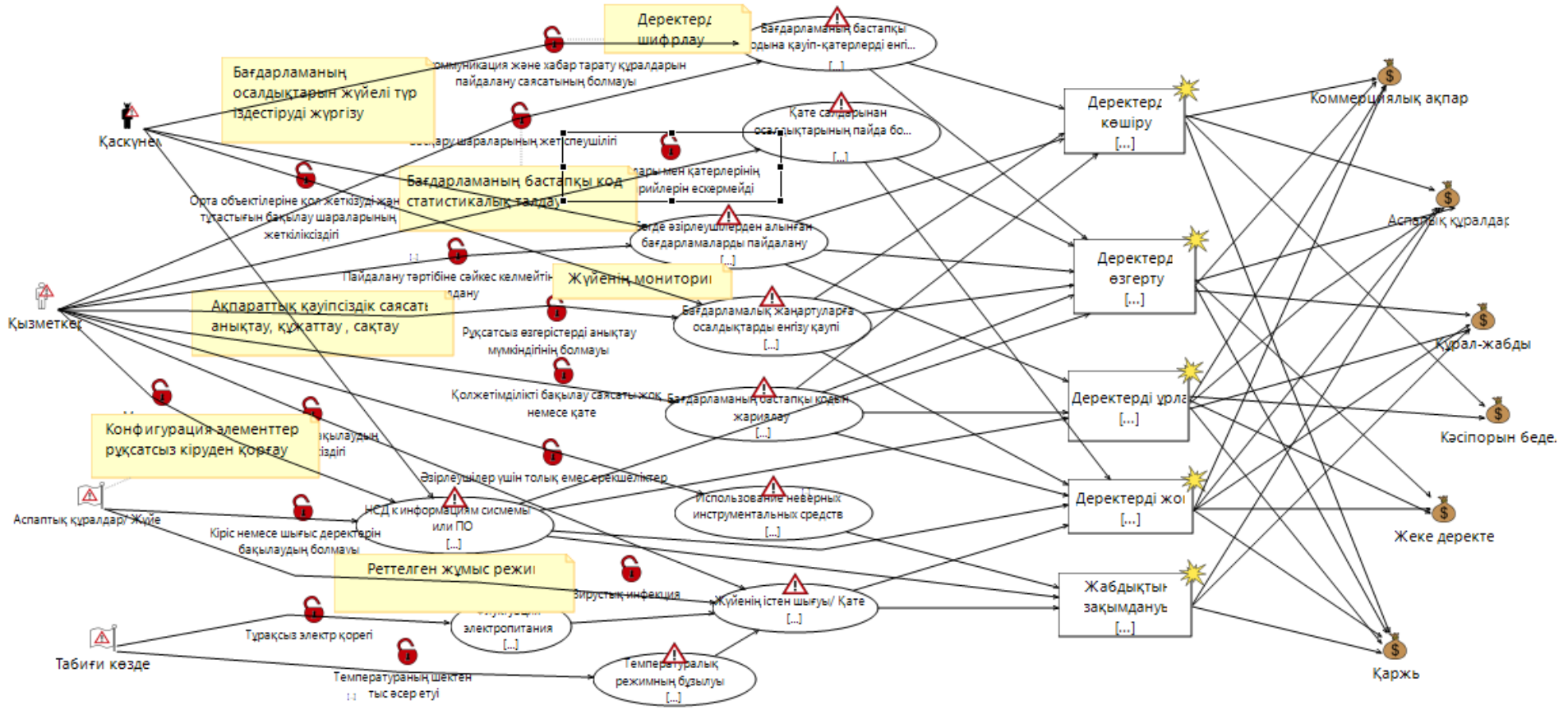
5.3 сурет – Ықтимал сипаттамалары бар қауіптер моделі

Әсер ету дәрежесін, әрбір актив үшін қауіп-қатерді іске асырудың салдарын анықтаймыз.



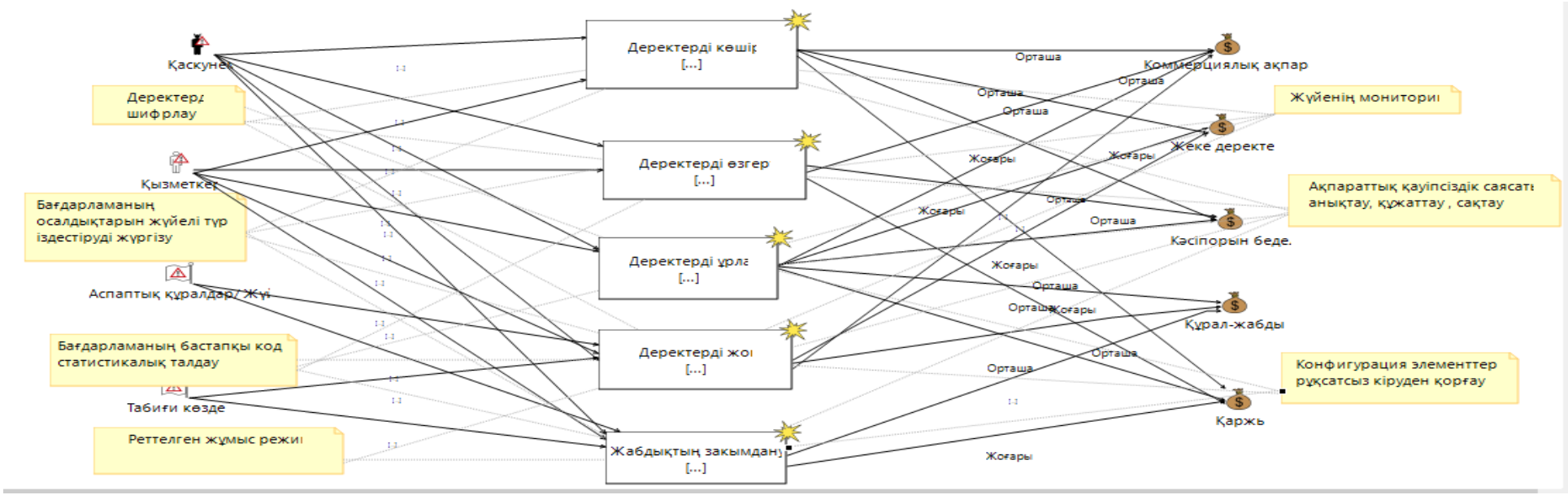
5.4 сурет – Қауіпті жүзеге асыру салдарларының сипаттамасы бар тәуекелдер диаграммасы

Тәуекел деңгейін азайту үшін әрбір осалдыққа арналған қорғаныс іс-шаралар қабылданды.



5.5 сурет – Қорғаныс шараларын қосқаннан кейінгі қауіптер диаграммасы

Бұл диаграммада қорғаныс шараларын қосқан кезде де қалуы мүмкін тәуекелдерді көрсетеді. Жүйелердің толық мониторингі кезінде қауіптердің пайда болуы азайтылуы тиіс.



5.6 сурет – Қолайсыз тәуекелдер диаграммасы

Бөлім бойынша қорытынды: дипломдық жұмыстың осы бөлімінде бағдарламалық қамтамасыз етуді әзірлеу кезінде туындайтын тәуекелдер анықталды. Тәуекелдерді басқару үдерісіне арналған негізгі жұмыстар қаралды. ГОСТ Р ИСО/МЭК 15408-1-2012 [24] стандартына сәйкес негізгі қауіп-қатерлер мен осалдықтар қаралды. Тәуекелдер деңгейін бағалаудың бастапқы және қайталама есебі жасалды, сондай-ақ тәуекелді өңдеу бойынша қорғаныс шаралары қабылданды. Жобалық тәуекелдің алынған моделі әрбір жобалық тәуекелді бір мәнді сипаттауға мүмкіндік береді, сондай-ақ тәуекелдерді сапалық және сандық талдау үшін де қолайлы. Ұсынылған қорғау шараларын ескере отырып, тәуекелдерге қайта есептеу жүргізілді. Қорғау шараларын қолдану нәтижесінде тәуекелдің орташа көрсеткіші 2 есе төмендеп, активтер үшін қолайлы болды.

Екінші бөлімде CORAS бағдарламсының көмегімен ақпараттық тәуекелдерге талдау жүргізілді және активтерді сәйкестендіруден бастап, қауіп-қатер мен осалдықтар моделі, қарсы өлшемдерді енгізуі секілді UML диаграммалары салынды.

Қорытынды

Дипломдық жобада ақпараттың қауіпсіздігін қамтамасыз етуге байланысты «Қауіптермен мен осалдықтарды талдау моделі» негізінде тәуекелдердің мәнін бағалау үшін бағдарламалық қамтама әзірленді.

Бұл әдісті қолдану тәуекелдерді субъективті бағалау кезінде туындайтын қауіпсіздік шараларының артық шығындарын болдырмауға, ақпараттық жүйелердің өмірлік циклінің барлық кезеңдерінде қорғауды жоспарлауға және жүзеге асыруға, сонымен қатар жұмыстың қысқа мерзімде орындалуын қамтамасыз етуге мүмкіндік береді.

Ақпараттық қауіпсіздік тәуекелдерін талдаудың өзектілігі, оларды басқарудың мақсаттары мен тәсілдері анықталды. Қазіргі уақытта қауіптер мен тәуекелдерді бағалаудың қолданыстағы әдістемелері мен бағдарламалық құралдары толығымн сипатталып, артықшылықтары мен кемшіліктерін талдау нәтижесінде оңтайлы шешімдер көрсетіліп қорытынды жасалынды.

«Қауіптермен мен осалдықтарды талдау моделі» алгоритмінің жұмыс принципі зерттелініп, мысал түрінде таңдалынған ресурстардың тәуекелдері бағаланды.

Тәжірибелік бөлімде бағдарлама әзірлеу барысында PHP бағдарламалау тілінің және Develnext бағдарламалау ортасы және SQLite деректер базасының таңдалу себебі негізделді. Бағдарламаның жұмыс алгоритмінің блок-схемасы мен интерфейсі сипатталды. Сонымен қатар, жұмысқа қабілеттілігі тестіленіп пайдаланушы нұсқаулығы ұсынылды.

Өміртіршілік қауіпсіздігі бөлімінде қызметкердің жұмыс аймағындағы жұмыс жағдайына талдау жасалынды. Өрт жағдайында хабарлағыш қондырғыларын жобалау және эвакуация жолдарын есептеу орындалды.

Жобалық тәуекелдерді бағалау бөлімінде бағдарлама әзірлеу процессінде активтер үшін туындайтын тәуекелдер бағаланып, қорғау шешімдері көрсетілді.

Қорытындылай келгенде, бастапқыда қойылған мақсаттарға қол жеткізіліп, барлық тапсырмалар орындалды.

Пайдаланылған әдебиеттер

1. Грушо А. А., Применко Э. А., Тимонина Е. Е. Теоретические основы компьютерной безопасности; Академия - Москва, 2009. - 272 с.
2. Семкин С. Н., Беляков Э. В., Гребенев С. В., Козачок В. И. Основы организационного обеспечения информационной безопасности объектов информатизации. М.: Гелиос АРВ, 2010. – 192 с.
3. Губарева, О.Ю. Оценка рисков информационной безопасности в телекоммуникационных сетях // Вестник Волжского университета имени В.Н. Татищева. Серия Информатика. – 2013. – №2. – С. 76-81.
4. Губарева, О.Ю. Методика CRAMM применяемая для анализа рисков в сфере информационной безопасности / О.Ю. Губарева, В.В. Пугин // тезисы докладов XIX Российской научной конференции профессорско-преподавательского состава, научных сотрудников и аспирантов – Самара, 2012. – С. 51.
5. Губарева, О.Ю., Пугин В.В. Методика RISK WATCH применяемая для анализа рисков в сфере информационной безопасности // тезисы докладов XIX Российской научной конференции профессорско-преподавательского состава, научных сотрудников и аспирантов – Самара, 2012. – С. 53.
6. Разумников С.В. Анализ возможности применения методов OCTAVE, RISKWATCH, CRAMM для оценки рисков ИТ для облачных сервисов. – М.: ГЛТ, 2014. – 247 с.
7. Вихляев, С.А. Применение программной системы DIGITAL SECURITY OFFICE для проведения аудита безопасности информационной системы обработки персональных данных / С.А. Вихляев, И.В. Белов, М.А. Кононова // Молодой ученый. – 2014. – № 8. – С. 75-78.
8. Куканова, Н. Современные методы и средства анализа и управления рисками информационных систем компаний // Digital Securitu [Электронный ресурс] / URL: http://www.dsec.ru/about/articles/ar_compare/ (дата обращения: 12.06.2016).
9. Баранова, Е.К. Процедура применения методологии анализа рисков OCTAVE в соответствии со стандартами серии ИСО/МЭК / Е.К. Баранова, А.С. Забродоцкий // Образовательные ресурсы и технологии. – 2015. – №2(10). – С. 73-80.
10. Глатенко. В.А. Основы информационной безопасности: учебное пособие для вузов / В.А. Глатенко. – М.: ИНТУИТ, 2012 – 205 с.
11. Ажмухамедов, И.М. Управление рисками информационной безопасности в условиях неопределенности / И.М. Ажмухамедов, О.Н. Выборнова, Ю.М. Брумштейн // Проблемы информационной безопасности. Компьютерные системы. – 2016. – Т. 1. – С. 7-14.
12. Плетнёв П.В., Белов В.М. Сравнительный анализ существующих методов определения рисков информационной безопасности // Ползуновский вестник. – 2011. – №3/1. – С. 221-223.

13. Баранова, Е.К. Методики и программное обеспечение для оценки рисков в сфере информационной безопасности // Управление риском. – 2009. – № 1 (49). – С. 15-26.

14. Плетнёв П.В., Белов В.М. Методика оценки рисков информационной безопасности на предприятиях малого и среднего бизнеса // Доклады ТУСУР. – 2012. – №1(25). –Часть 2. – С. 83-87.

15. Жандаулетова, Ф. Р. Охрана труда: учебник для вузов / Ф.Р. Жандаулетова, Т.Е. Хакимжанов, Т.С. Санатова; МОН РК, НАО АУЭС. – Алматы, АУЭС, 2019. - 399 с.

16. ГОСТ 50923-96 «Дисплеи. Рабочее место оператора. Общие эргономические требования и требования к производственной среде. Методы измерения», Стандартинформ, 2008 - 11 б.

17. ГОСТ 12.1.003-2014 «Система стандартов безопасности труда. Шум. Общие требования безопасности», Стандартинформ, 2014. - 45б.

18. Құрылыс комитеті, Индустрия және сауда министрлігі: ҚР ЕЖ 2.02-102-2012/ Ғимараттар мен имараттардың өрт автоматикасы: - Астана, 2015. - 195 б.

19. Құрылыс комитеті, Индустрия және сауда министрлігі: ҚР ҚН 2.02-11-2002/ Ғимараттарды, бөлмелерді және имараттарды автоматты өрттік сигналдаудың жүйелерімен, автоматты өрт сөндіру және өрт туралы адамдарға хабарлау қондырғыларымен жабдықтау нормалары. – Астана, 2002. – 118 б.

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

21. ҚР Құрылыс және тұрғын үй-коммуналдық шаруашылық істері агенттігі: ҚР ҚНжЕ 2.02-05-2009/ Ғимараттар мен имараттардың өрт қауіпсіздігі. Сәулет, қала құрылысы және құрылыс саласындағы мемлекеттік нормативтер: - Астана, 2010. – 107 б.

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

23. Орлов Г.Г., Булыгин В.И., Виноградов Д.В. Инженерные решения по охране труда в строительстве. – М.: Стройиздат, 1985. – 278 с.

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

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

26. ISO/IEC 17799. Информационная технология. Практические правила управления информационной безопасностью. 2012-12-01. М., 2012. 69 с.

Қысқартулар тізімі

1. АЖ– ақпараттық жүйе
2. АТ–ақпараттық технологиялар
3. АҚ–ақпараттық қауіпсіздік
4. MSAT–Microsoft Security Assessment Tool
5. АЖО–автоматтандырылған жұмыс орны
6. БҚ–бағдарламалық қамтама
7. ДК–дербес компьютер
8. ДҚ–деректер қоры
9. JS – JavaScript

А қосымшасы

```
<?php
namespace app\forms;
use std, gui, framework, app;
class Panel extends AbstractForm
    /**
     * @event Ugrozaknopka.click-Left
     */
    function doUgrozaknopkaClickLeft(UXMouseEvent $e = null)
    {
        execute('SQLiteDatabase-ugroza/build/dist/SQLiteDatabase.exe');
    }
    /**
     * @event Uyazvimostknopka.click-Left
     */
    function doUyazvimostknopkaClickLeft(UXMouseEvent $e = null)
    {
       execute('SQLiteDatabase-uyazvimost/build/dist/SQLiteDatabase.exe');
    }
    /**
     * @event buttonAlt.click-Left
     */
    function doButtonAltClickLeft(UXMouseEvent $e = null)
    {               }

    /**
     * @event button.click-Left
     */
    function doButtonClickLeft(UXMouseEvent $e = null)
    {
       execute('SQLiteDatabase-kontrmery/build/dist/SQLiteDatabase.exe');
    }

    /**
     * @event panelAlt.click-Left
     */
    function doPanelAltClickLeft(UXMouseEvent $e = null)
    {
       execute('SQLiteDatabase-ugroza/build/dist/SQLiteDatabase.exe');
    }
    /**
     * @event button13.click-Left
     */
```

```
    function doButton13ClickLeft(UXMouseEvent $e = null)
    {
        execute('SQLiteDatabase-svyazi/build/dist/SQLiteDatabase.exe');
    }
    /**
     * @event Rasxodknopka.click-Left
     */
  <?php
namespace app\forms;
use std, gui, framework, app;
class resursy extends AbstractForm
         * @event button7.click-Left
     */
    function doButton7ClickLeft(UXMouseEvent $e = null)
    {             }
    /**
     * @event button8.click-Left
     */
    function doButton8ClickLeft(UXMouseEvent $e = null)
    {       }    /**
     * @event button9.mouseDown-Left
     */
    function doButton9MouseDownLeft(UXMouseEvent $e = null)
    {
          }
    /**
     * @event button3.click-Left
     */
        function doButton13ClickLeft(UXMouseEvent $e = null)
    {
        execute('SQLiteDatabase-svyazi/build/dist/SQLiteDatabase.exe');
    }
    /**
     * @event Ugrozaknopka.click-Left
     */
    function doUgrozaknopkaClickLeft(UXMouseEvent $e = null)
    {
        execute('SQLiteDatabase-ugroza/build/dist/SQLiteDatabase.exe');
    }
   /**
     * @event Uyazvimostknopka.click-Left
     */
    function doUyazvimostknopkaClickLeft(UXMouseEvent $e = null)
    {
```

```
        execute('SQLiteDatabase-uyazvimost/build/dist/SQLiteDatabase.exe');
    }
    /**
     * @event button.click-Left
     */
    function doButtonClickLeft(UXMouseEvent $e = null)
    {
        execute('SQLiteDatabase-kontrmery/build/dist/SQLiteDatabase.exe');
    }
<?php
namespace app\forms;
use php\gui\UXDialog;
use php\sql\SqlStatement;
use php\sql\SqlResult;
use php\gui\framework\AbstractForm;
use php\gui\event\UXEvent;
use php\gui\event\UXMouseEvent;
use php\lib\arr;
use php\lib\bin;
use php\lib\char;
use php\lib\fs;
use php\lib\str;
use php\lib\num;
use php\lib\reflect;
use php\io\Stream;
use php\io\File;
use php\io\IOException;
use php\io\FileStream;
use php\io\MemoryStream;
use php\io\ResourceStream;
use php\net\NetStream;
use php\util\Flow;
use php\util\Locale;
use php\util\Regex;
use php\util\Configuration;
use php\net\URL;
use php\net\Socket;
use php\net\SocketException;
use php\net\ServerSocket;
use php\net\Proxy;
use php\lang\Thread;
use php\lang\Environment;
use php\gui\UXMenuItem;
use php\gui\UXButton;
```

```
use php\gui\UXTooltip;
use php\gui\UXToggleButton;
use php\gui\UXToggleGroup;
use php\gui\UXImageView;
use php\gui\UXImageArea;
use php\gui\UXSlider;
use php\gui\UXSpinner;
use php\gui\layout\UXVBox;
use php\gui\UXTitledPane;
use php\gui\layout\UXPanel;
use php\gui\layout\UXFlowPane;
use php\gui\UXForm;
use php\gui\UXWindow;
use ide\bundle\std\UXAlert;
use php\gui\UXContextMenu;
use php\gui\UXControl;
use php\gui\UXDirectoryChooser;
use php\gui\UXFileChooser;
use php\gui\UXFlatButton;
use php\gui\UXHyperlink;
use php\gui\UXList;
use php\gui\UXMediaPlayer;
use php\gui\UXParent;
use php\gui\UXPopupWindow;
use php\gui\UXPasswordField;
use php\gui\UXProgressIndicator;
use php\gui\UXProgressBar;
use php\gui\UXTab;
use php\gui\UXTabPane;
use php\gui\UXTreeView;
use php\gui\UXTrayNotification;
use php\gui\UXWebEngine;
use php\gui\UXWebView;
use php\gui\UXCell;
use php\gui\UXColorPicker;
use php\gui\UXCanvas;
use php\gui\layout\UXStackPane;
use php\gui\layout\UXPane;
use php\gui\layout\UXScrollPane;
use php\game\event\UXCollisionEvent;
use php\gui\event\UXKeyEvent;
use php\gui\event\UXDragEvent;
use php\gui\event\UXWebEvent;
use php\gui\event\UXWindowEvent;
```

```
use php\gui\framework\AbstractModule;
use action\Animation;
use action\Collision;
use game\Jumping;
use action\Element;
use action\Geometry;
use action\Media;
use action\Score;
use php\framework\Logger;
class MainForm extends AbstractForm
{
    /**
     * @event showing
     */
    function doShowing(UXEvent $event = null)
    {
        $this->reloadUsers();
    }
    /**
     * @event addButton.action
     */
    function doButtonAction(UXEvent $event = null)
    {
        $userForm = app()->getNewForm('UserForm');
        $userForm->showAndWait();
        $this->reloadUsers();
        $this->table->selectedIndex = 0;
    }
    /**
     * @event editButton.action
     */
    function doEditButtonAction(UXEvent $event = null)
    {
        $userForm = app()->getNewForm('UserForm');
        $userForm->id = $this->table->selectedItem['id'];
         $userForm->showAndWait();
        $index = $this->table->selectedIndex;
        $this->reloadUsers();
        $this->table->selectedIndex = $index;
    }
        /**
     * @event deleteButton.action
     */
    function doDeleteButtonAction(UXEvent $event = null)
```

```
    {
        if (UXDialog::confirm('Вы уверены, что хотите удалить контрмеру?')) {
            $this->deleteUser($this->table->selectedItem['id']);

            $index = $this->table->selectedIndex;
                    $this->reloadUsers();
                    $this->table->selectedIndex = $index;
                    if ($this->table->selectedIndex == -1) {
                $this->table->selectedIndex = $index - 1;           }       }    }
    /**
     * @event table.click
     */
    function doTableClick(UXMouseEvent $event = null)
    {
        $this->deleteButton->enabled = $this->table->selectedIndex != -1;
        $this->editButton->enabled = $this->deleteButton->enabled;
    }
    /**
     * @event deleteAllButton.action
     */
    function doDeleteAllButtonAction(UXEvent $event = null)
    {
        if (UXDialog::confirm('Вы уверены, что хотите удалить все контрмеры?'))
{
            $this->deleteAllUsers();
            $this->reloadUsers();
        }    }    /**
     * @event table.mouseDown-2x
     */
    function doTableMouseDown2x(UXMouseEvent $event = null)
    {
        $this->doEditButtonAction();
    }
    public function addUserToTable(SqlResult $record)
    {
        $this->table->items->add($record->toArray());
    }
    public function addUsersToTable(SqlStatement $records)
    {
        foreach ($records as $record) {
            $this->addUserToTable($record);        }    }
        public function reloadUsers()    {
        $this->table->items->clear();
                $users = $this->getUsers();
```

```
        $this->addUsersToTable($users);
            $count = $this->getUserCount();
        $this->countLabel->text = $count . " - Количество контрмер";
            $this->deleteAllButton->enabled = $count > 0;
            if ($count == 0) {
           $this->deleteButton->enabled = false;
           $this->editButton->enabled = false;
      }   } }
class UserForm extends AbstractForm
{
    /**
     * @var int
     */
    public $id;
        /**
     * @var string
     */
    public $name;
        /**
     * @var string
     */
    public $nick;
        /**
     * @var int
     */
    public $age;
    /**
     * @event ageSelect.construct
     */
    function doAgeSelectConstruct(UXEvent $event = null)
    {
 /*       for ($i = 1; $i < 120; $i++) {
            $this->ageSelect->items->add($i);
        }
        $this->ageSelect->value = 18;*/    }    /**
     * @event button.action
     */
    function doButtonAction(UXEvent $event = null)
    {
        $data = [
            'name' => $this->ageSelect->value,
            'age'  => $this->nameEdit->text
        ];
        if (!$this->id) {
```

```
            $id = $this->addUser($data);
            app()->getMainForm()->toast("Создан новый пользователь с id = $id");
        } else {
            $this->saveUser($this->id, $data);
             app()->getMainForm()->toast("Данные успешно сохранены.");
        }
        $this->hide();    }
    /**
     * @event showing
     */
    function doShowing(UXWindowEvent $event = null)
    {
        if ($this->id) {
            $user = $this->getUser($this->id);

            if ($user) {
                $this->name = $user->get('name');
                $this->age  = (int) $user->get('age');
            }       }
            $this->nameEdit->text = $this->name;
        $this->ageSelect->value = $this->age;
    } class DatabaseModule extends AbstractModule
{
    /**
     * @event action
     */
    function doAction(ScriptEvent $event = null)
    {     //
        $this->database->query(
            'create table if not exists users (id integer primary key, name text, nick text,
age integer)'
        )->update();    }
        /**
     * @return SqlStatement
     */
    function getUsers()
    {
        return $this->database->query('select * from users order by id desc');
    }
    /**
     * @return int
     */
    function getUserCount()
    {
```

```
        return (int) $this->database->query('select count(*) from users')->fetch()->get('count(*)');
    }
    /**
     * @return SqlResult|null
     */
    function getUser($id)
    {        return arr::first($this->database->query('select * from users where id = ?', [$id]));
    }
      /**   *
     * @return int
     */
    function addUser(array $data)
    {        $statement = $this->database->query('insert into users values(null, ?, ?, ?)', [$data['name'], $data['nick'], $data['age']]);
        $statement->update();
              return $statement->getLastInsertId();
    }        function saveUser($id, array $data)
    {        $this->database->query('update users set name = ?, nick = ?, age = ? where id = ?', [
            $data['name'], $data['nick'], $data['age'],
            $id
        ])->update();
    }        /**
     * h
     * @return int
     */
    function deleteUser($id)
    {        return $this->database->query('delete from users where id = ?', [$id])->update();
    }
       /**
     *
     * @return int
     */
    function deleteAllUsers()
    {
       return $this->database->query('delete from users where 1 = 1')->update();
    }}}
```