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

«ҚОРҒАУҒА ЖІБЕРІЛДІ»
Кафедра меңгерушісі с.ғ.к., доцент Бердібаев Р. Ш.
_____ « 31 » 05 2019 ж.
(қолы)

ДИПЛОМДЫҚ ЖОБА

Тақырыбы: «Кәсіпорындағы ақпарттық қауіпсіздік қатерлерін талдау және азайту әдістерін жобалау»
Мамандығы: 5В100200 – «Ақпараттық қауіпсіздік жүйелері»
Орындаған: Мұхаммеджанова Динаргүл Тобы: СИБк-15-1
Ғылыми жетекші: с.ғ.к., доцент Бердібаев Р. Ш.

Кеңесшілер:
Экономикалық бөлім бойынша:
э.ғ.к., профессор Әрепбаева Ж.Г.
(ғылыми дәрежесі, атағы, аты-жөні)
_____ « 29 » 04 2019 ж.
(қолы)

Тіршілік қауіпсіздігі бөлімі бойынша:
аға оқытушы Торғаев Д.Д.
(ғылыми дәрежесі, атағы, аты-жөні)
_____ « 30 » 04 2019 ж.
(қолы)

Есептеу техникасын қолдану бойынша:
с.ғ.к., доцент Бердібаев Р.Ш.
(ғылыми дәрежесі, атағы, аты-жөні)
_____ « 31 » 05 2019 ж.
(қолы)

Мөлшер бақылаушы:
аға оқытушы Ақарова Н.Б.
(ғылыми дәрежесі, атағы, аты-жөні)
_____ « 30 » 05 2019 ж.
(қолы)

Пікір беруші:
_____
(ғылыми дәрежесі, атағы, аты-жөні)
_____ « _____ » _____ 201__ ж.
(қолы)

Алматы 2019

ҚАЗАҚСТАН РЕСПУБЛИКАСЫ БІЛІМ ЖӘНЕ ҒЫЛЫМ МИНИСТРЛІГІ
«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: Мухамедманова Динаргүл
(аты-жөні)

Жобаның тақырыбы: Кәсіпорындағы ақпараттық қауіпсіздік қатерлерін талдау және ауайту әдістерін әзірлеу

2018 ж. «26» 10 № 124 университет бұйрығымен бекітілді.

Аяқталған жұмысты тапсыру мерзімі: «____»_____20___ ж.

Жобаға алғашқы деректер (талап етілетін зерттеу (жоба) нәтижелерінің параметрлері және зерттеу нысанының алғашқы деректері): Кәсіпорынның берілген ақпараттық инфрақұрылымына байланысты ақпараттық қауіпсіздік шараларын ұйымдастыру, оның ішінде ақпараттық қауіпсіздік тәуекелдерін талдау, тиімді ұсыныстарды әзірлеу.

Диплом жобасындағы әзірленуі тиіс мәселелер тізімі немесе диплом жобасының қысқаша мазмұны: Кәсіпорынның ақпараттық қауіпсіздігінің ағымдағы тай - күйі деректерін бағалауға, әлеуетті шығын-дарды ауайтуға, анықталған қауіптерден қорғау шараларын ұйымдастыруға мүмкіндік беретін әдістерді, сол әдістер негізінде тиімді шараларды бағдарламалық

ақпараттық жүйелерді басқыстыра отырып, кәсіпорын ақпараттық қауіпсіздігін қамтуға тілді бағдарламамен жұмыс жасау

Графикалық материалдардың (міндетті түрде дайындалатын сызбаларды көрсету) тізімі: 1. Ақпараттық түйіндерді таңдаудың негізгі кезеңдері
2. Кәсіпорынның локалдық желі жүйесінің сұлбасы
3. СКАДА жүйесінде түйіндерді басқару
4. Зерттеу нүктесінің топологиялық сұлбасы
5. Бағдарламалардың салыстырмалығының сұлбасы

Негізгі ұсынылатын әдебиеттер: 1. Шаньгин В.Ф. Информационная безопасность и защита информации / В.Ф. Шаньгин. - М.: ДМК, 2014-Ж.
2. Симонов С.В. Методические анализа рисков в информационных системах // Конфидент. Защита информации. - № 1 - 2002 - С. 402
3. Бекишева А.И. Методическое указание к выполнению экономической части дипломной работы для бакалавров специальности 5В070300 - Информационные системы - Алматы : АУЭС: 2013. - 24 с.

Жоба бойынша жобаның бөлімдеріне қатысты белгіленген кеңесшілер

Бөлімдері	Кеңесшілері	Мерзімі	Қолы
Негізгі бөлім	Бердібаев Р.Қ.	21.01 - 15.05. 19	
Экономика бөлімі	Әлібаева Ж.Г.	04.03 - 29.04.19	
Өміртіршілік қауіпсіздігі бөлімі	Торжаев Ә.Ә.	08.04-30.04	

Диплом жобасын дайындау
КЕСТЕСІ

Бөлімдердің атауы, әзірленетін мәселелердің тізімі	Ғылыми жетекшіге ұсыну мерзімдері	Ескерту
Кіріспе	21.01.2019	
Кәсіпорынның ақпараттық	4.02.2019	
тәуекелдерін бағалау және талдау		
Кәсіпорынның ақпараттық	18.02.2019	
қауіпсіздікті қамтамасыз		
ету шаралары		
Кәсіпорынның ақпараттық	4.03.2019	
қауіпсіздік тәуекелдерін талдау		
Тәуекелдерді бағалаудың	25.03.2019	
бағдарламалық		
құралын таңдау		
Ақпараттық қауіпсіздік	2.04.2019	
құралдарын тағайындаудың		
салыстырмалы талдауы		
Кәсіпорынның ақпараттық	15.04.2019	
қауіпсіздік тәуекелдерін		
төмендету және		
алдын ала жобалау		
Техникалық - экономикалық	17.04.2019	
негіздеме		
Ақпараттың сенімділік	18.04.2019	
қауіпсіздігі		
Қорытынды	15.05.2019	

Тапсырманың берілген уақыты «28» қазан 2018 ж.

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

Жобаның
ғылыми жетекшісі _____ (с.ғ.к. Бердібаев Р.Ш.)
(қолы) (аты-жөні)

Орындалатын тапсырманы
қабылдаған студент _____ (Мухамедханова Д.М.)
(қолы) (аты-жөні)

АҢДАТПА

Дипломдық жобада кәсіпорында орын алуы ықтимал ақпараттық қауіпсіздік тәуекелдеріне, олардың алдын-алып, болдырмау мақсатында ақпараттық тәуекелдерді бағалау мен талдаудың әртүрлі программалық-аппараттық әдістеріне талдау жасалып, берірген кәсіпорын үшін тиімді шешім ұсынылған.

Қарастырылған әдістер мен таңдалған бағдарлама кәсіпорынның ақпараттық қауіпсіздігінің ағымдағы жай – күйінің деңгейін бағалауға, әлеуетті шығындарды азайтуға, анықталған қауіптерден қорғау жоспарларын ұйымдастыруға мүмкіндік береді.

АННОТАЦИЯ

В дипломном проекте представлен анализ различных программно-аппаратных методов анализа и оценки информационных рисков с целью выявления и предотвращения возможных рисков информационной безопасности на предприятии.

Рассмотренные методы и выбранная программа позволяют оценить уровень текущего состояния информационной безопасности предприятия, уменьшить потенциальные затраты, организовать планы защиты от выявленных угроз.

ANNOTATION

The diploma project presents an analysis of various software and hardware methods of analysis and evaluation of information risks in order to identify and prevent possible risks of information security in the enterprise.

The considered methods and the selected program allow to assess the level of the current state of information security of the enterprise, to reduce potential costs, to organize protection plans against identified threats.

Мазмұны

Кіріспе

Қазіргі уақытта жаппай компьютерлендіру жағдайында кәсіпорынның нарықтағы әл-ауқаты мен табысты дамуы ақпараттық инфрақұрылымының қауіпсіздігін қамтамасыз етуге, сондай-ақ әр түрлі объектілерді бақылау мен басқаруға байланысты. Мұндай объектілерге телекоммуникация жүйелерін, банк жүйелерін, атом станцияларын, әуе және жер үсті көлігін басқару жүйелерін, сондай-ақ құпия және құпия ақпаратты өңдеу және сақтау жүйелерін жатқызуға болады. Ақпараттық қауіпсіздік деп бүкіл компанияның, оның иелеріне немесе пайдаланушыларына ақпарат саласында зиян келтіретін қасақана немесе кездейсоқ әрекеттерден қорғалуы түсініледі.

Ақпараттық қауіпсіздікті қамтамасыз ету ең алдымен олардың салдарын жоюға емес, тәуекелдерді болдырмауға бағытталуы тиіс. Ақпараттың құпиялылығын, тұтастығын, қол жетімділігін қамтамасыз ету бойынша алдын алу шараларын қабылдау және ақпараттық қауіпсіздік жүйесін құрудағы неғұрлым дұрыс тәсіл болып табылады.

IT – нарықта қазір нормативтік құжаттардан (стандарттардан) бастап бағдарламалық қамтамасыз етумен аяқталатын тәуекелді талдау және азайту құралдарының көптеген түрі бар. Практикалық қызметте пайдалану үшін оларды таңдағанда, сарапшы «Қандай параметрлерді пайдалану керек?», «Қандай математикалық әдістер қолдану керек?», «Статистикалық деректерсіз қалай бағалау керек?», «Анық емес жағдайда тәуекелдерді талдау мен бағалауды қалай жүргізуге болады?» және т. б. факторлар бағалаудың тиісті құралдарын таңдауда бірқатар қиындықтар туғызады.

Сондай-ақ, негізінен тәуекелдерді талдау және төмендету үшін ақпараттық қауіпсіздіктің инциденттері мен қатерлері туралы статистикалық деректер пайдаланылатынын атап өткен жөн.

Көптеген елдерде, соның ішінде Қазақстанда да осындай статистиканы тіркеуге және қолдануға қатысты тиісті мемлекеттік тәжірибе толық қалыптаспаған. Бұл өз кезегінде талдау және тәуекелдерді төмендету құралдарының мүмкіндіктерін шектейді. Бұдан басқа, мұндай құралдарда пайдаланылатын параметрлер жиынтығына белгілі шектеулер бар, бұл олардың икемділігін төмендетуге алып келеді, яғни оларды шамалардың кең спектрін бағалау үшін қолдануға мүмкіндік бермейді. Сондай-ақ, уақыт кезеңін, саланы, экономикалық ерекшелікті ескере отырып, анық айқындалған, әлсіз қалыптасқан ортада жасалған сараптамалық бағалауды қалыптастыру мәселелері де аз зерттелген.

Осыған байланысты, бұл тақырыптың өзектілігі ақпараттық қауіпсіздік тәуекелдерін талдау және төмендету құралдарын, статистикалық деректер базасында және әлсіз формальды ортада жасалған сараптамалық бағалау базасында да пайдалануға болатын, көптеген әдістер мен құралдарды әзірлеу және зерттеу қажеттігіне негізделеді.

Жобаның мақсаты – кәсіпорын қызметінде тәуекелдерді талдап және оларды азайту бойынша әдістерді әзірлей отырып, кәсіпорынның ақпараттық қауіпсіздігін қамтамасыз ету жолдарын ұсыну.

Қойылған мақсат бірқатар өзара байланысты міндеттерді шешуді қажет етеді:

- кәсіпорындардағы ақпараттық қауіпсіздік мәселелерін қарастыру;
- тәуекелдер туралы түсінікті, оның пайда болу себептерін, оларды талдау және төмендету әдістерін қарастыру;
- қарастырылған әдістерге сүйене отырып, кәсіпорын тәуекелдерін азайту бойынша шаралар ұсыну.

1 Кәсіпорынның ақпараттық тәуекелдерін бағалау және талдау

1.1 Кәсіпорында ақпараттық қауіпсіздікті қамтамасыз ету мәселелері

Біздің қоғам дамуының қазіргі кезеңінде адами прогрестің көптеген дәстүрлі ресурстары өзінің бастапқы мәнін бірте-бірте жоғалтуда. Олардың орнына жаңа ресурс, жойылмайтын, қайта, уақыт өте келе маңыздылығы арта түсетін, ақпарат деп аталатын жалғыз өнім келуде.

Ақпараттық қоғамның біртіндеп қалыптасуына байланысты, соңғы бірнеше жыл ішінде ақпарат адам өмірінің барлық салаларында маңызды рөл атқара бастады. Адамзат дамуы үшін тек материалдық, аспаптық және басқа да ресурстар ғана емес, сонымен қатар ақпараттық ресурстар да 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 саласы және банк-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, бағалы ақпаратты қорғау мәселесі бұрынғыдан да маңызды болып тұр. Компанияның негізгі міндеттерінің қатарында үйренгендерден басқа, деректердің құпиялылығын қорғау және қамтамасыз ету, ақпараттық тәуекелдерді азайту және хакерлік шабуылдардың алдын алу сияқты мәселелер пайда болды. Ешкім ұрлық, ақпаратты ұрлау, компьютерді вирусты енгізу, ақпаратты жою және т.б. сияқты жағымсыз салдардан сақтандырылмаған. Сондықтан кәсіпорын мен ұйымда ақпараттық технологияларды дамытудың маңызды проблемаларының бірі –

ақпараттық қауіпсіздікті сенімді қамтамасыз ету. Оның шешімі – ақпараттық саладағы қауіптілікті анықтау және алдын алу нысандары мен әдістерін зерттеу, сондай-ақ кәсіпорында ақпараттық қауіпсіздікті басқару, қорғаныс құралдарын таңдау [1].

Қорғалатын ақпаратты иеленушінің қорғау қызметі, ең алдымен, құпия ақпараттың таралуының алдын алуға байланысты.

Құпия ақпарат – бұл осы ақпаратқа рұқсаты бар субъектілер тобына шектеу енгізу қажеттілігін көрсететін және оған қол жеткізу өкілеттігі жоқ субъектілерден көрсетілген ақпаратты құпия сақтау қабілеті қамтамасыз етілетін ақпараттың субъективті – анықталатын сипаттамасы немесе қасиеті. Бәсекелестер үшін қызығушылық тудыруы мүмкін құпия ақпарат қорғалуы тиіс. Ақпаратты жасыру тек құпия деректердің таралып кетуінен сақтандыру үшін ғана емес, сонымен қатар деректер базасына немесе жұмыс құжаттамасына өзгерістер енгізуге әрекет етуден қорғау. Себебі, бұл тек шығынға ғана әкеліп қоймай, сонымен қатар кәсіпорынның жұмысын тоқтату да мүмкін.

Ақпараттың кез келген жылыстауы компания үшін маңызды проблемалар әкелуі мүмкін, елеулі қаржылық шығындардан толық жойылғанға дейін. Әрине, ағып кету проблемасы бүгінгі күні пайда болған жоқ, өндірістік тыңшылық және біліктілік мамандарының құлауы компьютерлендіру дәуіріне дейін де болған. Бірақ ДК мен интернеттің пайда болуымен ақпаратты заңсыз алудың жаңа тәсілдері пайда болды. Егер бұрын ол үшін қағаз құжаттардың тұтас бумаларын ұрлап, фирмадан шығару қажет болса, қазір маңызды мәліметтердің үлкен көлемін портмонада орналасқан флешкаға жай ғана салуға болады, руткиттер, трояндар, бэкдорлар, кейлоггер және ботнеттер отбасын пайдалануға барғанда желі арқылы жіберуге болады немесе диверсия жасап, вирустар арқылы жай ғана жоюға болады.

Компаниялардан көбінесе қаржылық сипаттағы құжаттар, технологиялық және конструкторлық әзірлемелер, басқа ұйымдардың желісіне кіру үшін логиндер мен құпия сөздер ағады. Бірақ ұйымдардың және қызметкерлердің жеке мәліметтерінің жылыстауы да компанияға елеулі зиян әкелуі мүмкін. Бұл көбінесе батыс елдері үшін өзекті болып табылады, ол жақта мұндай ысыраптарға байланысты сот талап-арыздары көбінесе үлкен айыппұлдарға әкеп соқтырады, оларды төлегеннен кейін компаниялар елеулі шығынға ұшырайды.

Кейде, құпия ақпараттар бәсекелестердің немесе журналистердің қолына түскеннен кейін бірнеше ай немесе жыл өткен соң компанияға зиян келтіруі де мүмкін. Сондықтан қорғау кешенді болуы керек. Ақпаратты өте маңызды және аз маңызды бөлуге болмайды. Компания қызметіне қатысты және жариялауға арналмаған барлық нәрсе компанияның ішінде қалуы және қауіп-қатерден қорғалуы тиіс. Қазіргі уақытта ақпараттық қауіпсіздікті қамтамасыз ететін үш базалық міндет қалыптастырылды:

- деректердің бүтіндігі – ақпаратты жоғалтуға алып келетін іркілістерден қорғау, сондай-ақ, деректерді заңсыз құрудан немесе жоюдан қорғау, деректердің бүтіндігін бұзудың мысалы ретінде бухгалтерлік базалардың зақымдануы бола алады, ол компанияны теріс болатын салдарға әкеп соғады;

- ақпараттың құпиялылығы – ақпаратты заңсыз жария ету, ағып кету, бүлдіру;

- барлық пайдаланушылар үшін ақпараттың қолжетімділігі – зиянкестердің вирустық белсенділігінен немесе әрекеттерінен туындауы мүмкін қызмет көрсетуден немесе қызметтерден бас тарту.

Осы аспектілердің бірінің бұзылуы кәсіпорынның қалыпты жұмыс істеуіне кедергі келтіруі мүмкін. Кез келген бұзушылықтардың болуына ішкі және сыртқы қауіп-қатерлер әсер етуі мүмкін. Ақпараттық қоғамның бүгінгі дамуын ескере отырып, қауіпсіздік қатерлері санының өсу үрдісі туралы қорытынды жасауға болады.

Құпия ақпарат бәсекелес фирмалар үшін үлкен қызығушылық тудырады. Ол зиянкестер тарапынан қол сұғушылықтың себебі болып табылады.

Көптеген мәселелер қауіптің маңыздылығын жете бағаламаумен байланысты, нәтижесінде кәсіпорын үшін бұл банкротқа ұшырауы мүмкін. Тіпті жұмысшы персоналдың салғырттығының бір ғана жағдайы компанияға миллиондаған шығын мен клиенттердің сенімін жоғалтуға алып келуі де ғажап емес. Компанияның құрамы, мәртебесі және қызметі туралы деректер қауіп-қатерге көп ұшырайды. Мұндай қауіптердің көздері оның бәсекелестері, сыбайлас жемқорлар және қылмыскерлер болып табылады. Олар үшін қорғалатын ақпаратпен танысу, сондай-ақ қаржылық залал келтіру мақсатында оның модификациясы ерекше құнды болып табылады. Мұндай нәтижеге ақпараттың тіпті 20% - ға ағып кетуі де алып келе алады. Кейде компанияның құпияларын жоғалту қызметкерлердің тәжірибесінің жеткіліксіздігінен немесе қорғау жүйелерінің жоқтығынан кездейсоқ орын алуы мүмкін [2].

Әрбір кәсіпорын компьютерлік техникамен және дүниежүзілік интернет желісіне қатынаумен жабдықталған. Зиянкестер іс жүзінде осы жүйенің әрбір құрамдас бөлігіне және көптеген арсеналдың (вирустар, зиянды бағдарламалар, құпия сөздерді таңдау және басқалар) көмегімен құнды ақпаратты ұрлайды. Ақпараттық қауіпсіздік жүйесі әрбір ұйымға енгізілуі тиіс. Басшыларға қорғауды қажет ететін ақпараттың барлық түрлерін жинау, талдау, жіктеу және қауіпсіздікті қамтамасыз етудің тиісті жүйесін пайдалану қажет. Бірақ бұл аз болады, өйткені техникадан басқа, бәсекелестерге ақпарат бере алатын адам факторы бар. Кәсіпорынның қауіпсіздігін барлық деңгейде дұрыс ұйымдастыру маңызды. Осы мақсаттар үшін ақпараттық қауіпсіздік менеджменті жүйесі пайдаланылады, оның көмегімен басшы бизнес мониторингінің үздіксіз процесін жолға

қояды және өз деректерінің қауіпсіздігінің жоғары деңгейін қамтамасыз етеді.

Кәсіпорында ақпараттық қауіпсіздіктің мәні барлық деректер белгілі бір алгоритмдер бойынша қолмен немесе компьютерлік құрылғының көмегімен шифрлану болып табылады. Шифрлеу алгоритмі немесе үнемі өзгеретін ақпарат кілті тек санаулы адамдарға ғана белгілі. Мұндай криптографиялық шифрді пайдалану алгоритмді білмей ақпаратты шифрлей алмайтын зиянкестердің көп санынан ұйымның қауіпсіздігін қамтамасыз етуге мүмкіндік береді.

Іскерлік құжаттаманы жүргізу, хат алмасу және байланыс көптеген жағдайларда электрондық пошта, нақты уақыт режимінде қарым-қатынас жасауға арналған бағдарламалар, түрлі Web-технологиялар арқылы жүргізіледі. Ал бұл кәсіпорынның ақпараттық қауіпсіздігін өмірге енгізудің өзектілігін тағы да атап көрсетеді. Тек сыртқы қауіп-қатерлерге жіті назар аударып қана коймау керек, өйткені кәсіпорынның өзінің сенімді қызметкерлерінің ұйымның ақпараттары мен ақша қаражатын ұрлаған көп жағдайлары белгілі. Көбінесе бұл қауіпсіздік қызметінің жұмысын ұйымдастырған адамдар болады. Олар маңызды деректерді жоюы немесе өзгертуі, жеке мақсатта пайдалануы немесе жасырын ақпаратты қарсылас адамдарға беруі мүмкін.

Зиянкестер ірі кәсіпорындардан ғана емес, қарапайым азаматтардан да ұрлайды. Ал барлық үйреншікті қорғау шаралары компьютерлік технологиялар саласында әрекетке қабілетсіз болады, сондықтан деректерді қорғау бойынша әртүрлі іс-шаралар жүйесін құру басшы мен оның клиенттерін қорғай алады. Жаңа технологияларды дамыту орнында тұрмайды және үнемі жақсарып келеді, басшылар уақыт өте келе кәсіпорында ақпараттық қауіпсіздік жүйесін жетілдіруді жүргізуі қажет [3].

Кәсіпорында ақпараттық қауіпсіздік ұғымы – бұл тек компьютерлік ақпаратты қорғау ғана емес, сонымен қатар, барлық ақпарат түрлерінің, клиенттердің, қызметкерлердің және кәсіпорынның тұтас бөлімшелерінің мәліметтерінің қауіпсіздігін қамтамасыз ету бойынша тұтас жүйе.

Шифрлау әдістерінің арасында деректерді жасырудың тағы бір тәсілі бар – стеганография, ол ақпаратты ғана емес, оның берілу фактісінің өзін де жасырады. Дәл осы әдіс азаматтардың тұтас, құпия және шынайы ақпаратты қамтамасыз ету құқығын бұзады. Мұндай тәсілге зиянкестер бағдарламалық қамтамасыз ету түрінде мүлдем басқа функцияны орындайтын зиянды бағдарламаларды орналастырады.

Ұйым үшін қауіп-қатерлер тізімі:

- аппараттардың жұмысындағы іркілістер;
- алаяқтық;
- ақпаратты бұрмалау немесе қызметкердің ұқыпсыздығы;
- желілік анализаторларды пайдалану;
- алаяқтық немесе ұрлау;
- электрондық және бағдарламалық «бетбелгілер»;

- электромагниттік сәулелену, радиосәулелену немесе акустикалық сигналдарды пайдалану;

- діріл сигналдары.

Кәсіпорынның ақпараттық жүйесіне қатысты ақпараттық қауіпсіздік қатері ішкі немесе сыртқы болуы мүмкін. Ішкі кәсіпорынның ақпараттық ресурстарын пайдалануға қатысты кәсіпорын регламентін бұзу, компанияның деректерін жеке мақсатта пайдалану, қызметкерлердің вирусты ақпараттық желіге енгізу, құпия деректерді және т. б. ұрлау болып табылады. Сыртқы қауіп-қатерлер компанияға қатысы жоқ субъектілердің іс-қимылының салдары болып табылады, ақпараттық жүйеге хакерлік шабуыл және қолдаушы инфрақұрылымның саботажы неғұрлым типтік мысал болып табылады. Қауіп-қатерлерді белгілері бойынша түрлі топтарға бөлуге болады. Ол 1-кестесінде анық көрсетілген.

Кесте 1 – Ақпараттық қауіпсіздік қатерлері

Белгілері			Қауіптің үлгісі
Пайда болу табиғаты	Табиғи	Әдеттегі физикалық процестерден немесе табиғи апаттардан туындаған қауіптер	-цунами; -торнадо; -өрт.
	Жасанды	Адам әрекетінен соң туындаған қауіптер	-вирустары бар спам-хабарламаларды тарату; -сайттарға DdoS-шабуылдар жасау; -жабдықтың бұзылуы.
Мотивация дәрежесі	Әдейі емес	Жобалаудағы, бағдарламалық қамтамасыз етудегі кездейсоқ қателер, персонал жұмысындағы қателіктер	-ақпарат тасығыштардың ойдан тыс бүлінуі; -жабдықты кездейсоқ өшіру немесе бұзу; -маңызды ақпараты бар файлдарды жою.

1-кестенің жалғасы

	Әдейі	Материалдық пайда алу үшін басқа адамдардың идеялық, айқын мақсаттары. Кейде кек алу немесе моральдық наным-сенім себеп болады	-тыңдайтын құрылғыларды пайдалану; -парольдер мен логиндерді заңсыз алу; -есептен шығарылған ақпарат тасығыштарды ұрлау.
Бақыланатын аймаққа қатысты ереже	Ішкі	Ақпараты бар тасымалдаушыларды ұрлау, жабдықтарды бүлдіру	-USB-құрылғыны ұрлау; қызметкерді сатып алу, бопсалау.
	Сыртқы	Деректерді ұстап қалу	-Skype арқылы сөйлескенде деректерді қолға түсіру; -құпия ақпаратты қамтитын электрондық хабарламаларды қолға түсіруі.
Іске асыру тәсілі	Заңсыз қол жеткізу	Аккаунттарға, есептік жазбаларға, жеке кабинетке рұқсатсыз кіру	-фишинг сайттарын поштаға жіберуден деректерді беру.
	Ақпаратқа қасақана ықпал ету	Ақпаратты әдейі өзгерту немесе жою	-DdoS-шабуылдан кейін сайтта ақпаратты өзгерту немесе бұрмалау.

1-кестенің жалғасы

Ақпараттық қауіпсіздіктің бұзылған аспектісі	Құпиялылық	Ақпаратқа заңсыз қол жеткізуге байланысты қатерлер	-байланысты техникалық арналары бойынша берілетін ақпаратты ұстап қалу;
	Қол жетімдік	Белгілі бір ақпаратты алу немесе оны пайдалану мүмкін еместігіне байланысты қатерлер	-пайдалану DdoS-шабуылға ұшыраған сайтқа кіре алмауы; -найзағай салдарынан жабдықтың зақымдануы.
	Тұтастық	Ақпаратты заңсыз өзгерту немесе көшірмелеу жасау	-компания ресми сайтында ақпаратты қолдан жасау; -ақпаратты рұқсатсыз өзгерту және бұрмалау.

Ірі кәсіпорындар алдында белгілі ақпараттық қауіптер санының тұрақты өсуі және жаңа түрлерінің пайда болуы жағдайында корпоративтік желілерді зиянды бағдарламалар мен желілік шабуылдардан сенімді қорғауды қамтамасыз ету міндеті жиі туындайды. Өйткені зиянкестер жиі зиянды бағдарламалардың әртүрлі түрлерін пайдаланады:

- вирустар;
- троян құрттары;
- вирусты бағдарламалар ашылатын ойын бетбелгілері;
- жалған мұрағатшылар, деректер алмасу үдеткіштері және басқа да бағдарламалар.

Вирустық бағдарламаламалар қазіргі таңда тез дамиды. Кәсіпорында ақпараттық қауіпсіздік жүйесін жетілдіру ғана сыртқы және ішкі қатерлерден, Интернет-сервистер тарапынан шабуылдардан, желі арқылы кілттерді және парольдерді басқарудан және ақпаратты ұрлау немесе бұрмалау бойынша көптеген басқа да қатерлерден қорғай алады [4].

Қазіргі жағдайда ақпараттармен жұмыс істеу ресурстардың массивімен және алуан түрлілігімен ғана емес, оны өңдеу технологияларын үнемі жаңартумен, қызметкерлерді жоғары ілтипатпен және бақылаумен, сонымен қатар фирманы басқарудың сауатты деңгейімен де ерекшеленеді.

Компьютерлік техника мен ақпараттық технологияларды жаппай енгізу процесі прогрессивті бастаумен қатар қосымша проблемаларды туғызатыны белгілі. Олар кәсіпорындардың қауіпсіздігіне нақты қауіп-қатерлермен, стратегиялық маңызды ақпаратты жоғалтумен, сонымен бірге компанияның басқаруын жоғалтумен байланысты.

Жаңа ақпараттық технологияларды жаппай пайдаланудың жанама құбылыстарын қысқарту мақсатында ұйым басшылығы ақпараттық саладағы өз қызметінің стратегиясын анықтайды. Мұндай стратегияның өзекті бастамасы ақпараттық саладағы кәсіпорындар мен ұйымдар мүдделерінің қорғалу жағдайы ретінде айқындалатын ақпараттық қауіпсіздік болуы тиіс. Ақпараттық технологиялар тікелей немесе жанама пайдаланылатын кәсіпорын қызметінің барлық бағыттары ақпараттық қауіпсіздікті қамтамасыз ету шеңберінде фокусталады.

Халықаралық тәжірибе көрсетіп отырғандай, ақпараттық қауіпсіздікті қамтамасыз ету саласындағы негізгі проблема ақпараттық технологиялар саласындағы қазіргі әлеуметтік-саяси және экономикалық жағдайларға және жетістіктеріне жауап беретін нормативтік-құқықтық, заңнамалық актілерді тәжірибеде уақытылы қолдануға мүмкіндік беретін бірыңғай тиімді тетікті құру болып табылады. Технологиялар саласын, ақпараттандыру саласын дамыту ақпараттық қауіпсіздікті қамтамасыз ету мәселесін өзекті етеді.

Ақпараттық қауіпсіздікті қамтамасыз ету проблемасы екі құрамдас – технологиялық және идеологиялық болып табылады. Біріншісі – ақпараттық ресурстарды, ақпараттық базаларды қорғау жүйесін әзірлеумен және енгізумен байланысты, екіншісі – ақпаратты таратумен, оның жеке адамның, қоғамның, мемлекеттің өміріне ықпалымен байланысты.

Іс жүзінде кез келген жаңа технология қоғамдағы әлеуметтік-экономикалық өзгерістерге алып келеді, халықаралық қатынастарға әсер етеді. Бүгінгі күні жалпы әлемдік ақпараттық кеңістік құру туралы айтуға болады. Ақпарат, ақпараттық технологиялар трансшекаралық, өткізгіштігі сияқты қасиеттермен сипатталады, жаппай пайдалану мүмкіндігіне ие, ұлттық шекараларға қарамастан қол жетімді болады.

Ақпараттың қатері деп қорғалатын мәліметтерді заңсыз игеруге әкелетін ақпараттық ресурстарға қатысты әлеуетті немесе нақты мүмкін болатын іс-әрекеттерді түсіну қабылданған.

Осындай іс-әрекеттер болып табылады:

- ақпараттармен оның тұтастығын бұзбай түрлі жолдармен және тәсілдермен танысу;

- мәліметтердің құрамы мен мазмұнын ішінара немесе айтарлықтай өзгерту ретінде қылмыстық мақсаттарда ақпаратты түрлендіру;

- материалдық зиян келтіру мақсатында вандализм актісі ретінде ақпаратты бұзу (жою).

Ақыр соңында ақпаратпен бірге құқыққа қарсы әрекеттер оның құпиялылығын, толықтығын, шынайылығын және қол жетімділігін бұзуға әкеледі, бұл өз кезегінде жалған немесе толық емес ақпарат жағдайында басқару режимін де, оның сапасын да бұзуға әкеледі. Әрбір қауіп-қатер белгілі бір залал – моральдық немесе материалдық, ал қауіп-қатерді қорғау және қарсы әрекет оның көлемін төмендетуге бағытталған, ең дұрысы – толық, нақты айтарлықтай немесе кем дегенде ішінара. Бірақ бұл әрдайым бола бермейді. Қауіп-қатерлер саны үнемі өссе де, жаңа вирустар саны пайда болуда, түрлі шабуылдардың қарқындылығы мен жиілігі артқанмен, ақпаратты қорғау құралдарын әзірлеушілер де орнында тұрмайды.

Компанияның толыққанды ақпараттық қауіпсіздігі ақпаратты қорғаудың сенімділігіне әсер ететін барлық елеулі оқиғалар мен жай-күйлерді тұрақты бақылауды көздейді. Сонымен қатар, ақпаратты қорғау тұрақты түрде жүзеге асырылуы және деректердің барлық өмірлік циклін, яғни оның түсуінен, құрылуынан немесе маңыздылығы мен өзектілігі жойылғанға немесе жоғалғанға дейін қауіпсіздікті қамтамасыз етуі тиіс. Кәсіпорында ақпарат пен деректерді қорғауға әсер ететін негізгі факторлар:

- компанияның серіктестермен ынтымақтастығын арттыру;
- бизнес-процестерді автоматтандыру;
- қол жетімді байланыс арналары бойынша берілетін кәсіпорынның ақпарат көлемінің өсу үрдісі;
- компьютерлік қылмыстардың өсу үрдісі.

Кәсіпорынды ақпараттық қорғау маңызды ақпараттың қауіпсіздігіне бағытталған қабылданатын шаралардың тұтас үйлесімімен анықталады. Бұл шараларды екі топқа бөлуге болады:

- ұйымдастыру шаралары;
- техникалық шаралар.

Ұйымдастыру шаралары ресми рәсімдер мен маңызды ақпаратпен, ақпараттық сервистермен және қорғау құралдарымен жұмыс істеу ережелерінен тұрады. Техникалық шаралар қолжетімділікті бақылаудың бағдарламалық құралдарын пайдалануды, ақпараттың жылыстауы мен ұрлануының мониторингін, антивирустық қорғауды, электромагниттік сәулеленуден қорғауды және т. б. қамтиды.

Компания кәсіпорында ақпаратты қорғаудың техникалық әдістеріне ғана емес, сонымен қатар арнайы әзірленген нормативтік-құқықтық құжаттарды пайдалануға да назар аударуы тиіс. Құқықтық қамтамасыз ету жүйесіне міндетті түрде мемлекеттік заңдар, нормалар мен нұсқаулықтар, кәсіпорынның құжаттары (қызметкерлердің құқықтары мен міндеттері, өзіне алған міндеттерін бұзғаны үшін жаза мөлшерін міндетті түрде көрсете отырып) кіреді. Ақпарат қауіпсіздігінің құқықтық негізін құрғаннан кейін ықтимал қауіп көздерін анықтауға кіріседі. Әрбір деректер түрінің залалын талдап және бағалай отырып, ықтимал зардаптардың тізімін және

келтірілген зиянның мөлшерін жасау қажет. Бірінші кезектегі қорғау деңгейін міндетті түрде бөле отырып, қорғауға жататын құжаттардың, деректердің және кез келген ақпараттың тізбесі жеке жасалады. Қажетті ақпаратты жинай отырып, басшылық ақпарат қауіпсіздігі бойынша жеке бөлімше құрады, онда міндетті түрде компьютершілер мен қауіпсіздік қызметінің қызметкерлері болады.

Компанияның ақпараттық қауіпсіздік жүйесінің міндеттері көп қырлы. Мысалы, бұл әртүрлі тасымалдағыштардағы деректердің сенімді сақталуын қамтамасыз ету; байланыс арналары арқылы берілетін ақпаратты қорғау; кейбір деректерге қолжетімділікті шектеу; резервтік көшірмелер құру; жүйелік ақпаратқа рұқсатсыз енуге жол бермеу; күтпеген жағдайлар кезінде кәсіпорында ақпараттың тұтастығын қамтамасыз ету және басқалар. Қорғау әдістерінің арасында таңдауға болады:

- шифрлаудың криптографиялық тәсілі;
- электрондық қолтаңба;
- жүйенің және құжаттардың резервтік көшірмелерін жасау;
- құпия сәйкестендіру;
- аудит және хаттамалау жүйесі;
- электрондық кілттерді, смарт-карталарды пайдалану;
- желіаралық экрандау.

Құпия деректермен жұмыс істейтін үй-жайларда тек оларға тікелей жауап беретін адамдарға ғана міндетті түрде рұқсат берілуі тиіс. Мұндай қызметкерлерді басшылық таңдайды, ал жұмыс басталар алдында олар міндетті тестілеуден өтеді. Құпия үй-жайдағы ақпараттың қауіпсіздігі мақсатында техникалық персонал қызметкердің бақылауынсыз болмауға тиіс.

Компанияның ақпараттық қауіпсіздігін толық қамтамасыз ету деректерді қорғауға дұрыс қадамдар нәтижесінде ғана нақты болады. Ақпараттық қауіпсіздік жүйесін құру барысында бүгінгі таңда өзекті қатерлер мен осалдықтарды ескеру қажет.

Қазіргі заманғы ақпараттық жүйелердің көп қырлылығын ескере отырып, «қолданушылардың барлық қателіктері туралы айтпағанда, зиянкестердің іс-әрекеттерін көздеу мүмкін емес болғандықтан, ақпараттық қауіпсіздіктің барлық ойлы және ойсыз қауіптерінен қорғауға болмайды» деген тұжырыммен келісуге болады. Сондықтан, «ақпараттық қауіпсіздікті» қамтамасыз ету – бір реттік акт емес. Бұл қорғау жүйесін жетілдіру мен дамытудың неғұрлым ұтымды әдістерін, тәсілдері мен жолдарын негіздеу және іске асыру, оның жай-күйін үздіксіз бақылау, оның тар және әлсіз жерлерін және құқыққа қарсы әрекеттерін анықтау болып табылатын үздіксіз процесс [5].

1.2 Кәсіпорынның ақпараттық қауіпсіздік тәуекелдерін талдау

Ақпараттық жүйелер мен технологияларды пайдалану тәуекелдердің белгілі бір жиынтығымен байланысты.

Тәуекелдерді талдау – ақпараттық қауіпсіздіктің кез келген жүйесін құру неден бастау керек және ақпараттық қауіпсіздік аудитін жүргізу үшін қажет. Ол қандай ресурстарды және қандай қауіп-қатерден қорғау қажеттігін, сондай-ақ қандай да бір ресурстарды қорғауға мұқтаждығын анықтау мақсатында кәсіпорынның қауіпсіздігін тексеру жөніндегі іс-шараларды қамтиды. Дұрыс контрмер жиынтығын анықтау тәуекелдерді басқару барысында жүзеге асырылады. Тәуекел қауіпсіздікке қатер төнген жағдайда ақпараттық жүйелердің ресурстарына келтірілген залал келтіру ықтималдығымен және залал шамасымен анықталады.

Кәсіпорынның ақпараттық қауіпсіздік тәуекелдерін талдау барлық ықтимал қауіп-қатерлерді қарастырудан басталады. Бұл күтпеген жағдайлар туындаған жағдайда тексеру тәсілдерін анықтау, сондай-ақ тиісті қорғау жүйесін қалыптастыру үшін қажет. Барлық ақпараттық тәуекелдерді бірнеше критерийлердің негізінде әр түрлі топтарға жіктеуге болады:

- ақпараттық тәуекелдер көзі бойынша: ішкі және сыртқы;
- сипаты бойынша: әдейі және әдейі емес;
- түрі бойынша: тікелей немесе жанама;
- нәтижесі бойынша: ақпараттың дұрыстығын бұзу, ақпараттың өзектілігін бұзу, ақпараттың толықтығын бұзу, құпиялылықты бұзу және т. б.;
- әсер ету механизмі бойынша: табиғи апаттар, авариялар, мамандардың қателіктері және т. б. болып бөлінеді.

Ақпараттық қауіпсіздік тәуекелдерінің түрлері олардың пайда болу көздеріне, заңсыз басып кіруді іске асыру тәсіліне және мақсатына байланысты айқындалады. Техникалық тұрғыдан ең қарапайым, бірақ кәсіби орындауды талап ететін қауіп физикалық қауіптер болып табылады. Олар жабық көздерге рұқсатсыз кіру қатерін туғызады. Яғни, бұл процесс кәдімгі ұрлық болып табылады. Ақпаратты мекеме аумағына, кабинеттерге, мұрағаттарға техникалық жабдықтарға, құжаттарға және басқа да ақпарат тасымалдаушыларға қол жеткізу үшін басып кіріп, өз қолымен алуға болады.

Ұрлық тіпті деректердің өзінде емес, оларды сақтау орнында, яғни тікелей компьютерлік жабдықтың өзінде де болуы мүмкін. Ұйымның қалыпты қызметін бұзу үшін зиянкестер ақпарат тасымалдағыштардың немесе техникалық жабдықтардың жұмысындағы іркілісті қамтамасыз ете алады. Физикалық қауіп-қатерді жариялылығы жоқ жабық ақпаратқа рұқсаты бар әр түрлі топтардың мүшелері де қамтамасыз ете алады. Олардың мақсаты – құнды құжаттар.

Ақпараттық қауіпсіздік тәуекелдері интернет желісі мен ішкі компьютерлік жүйені қызметкерлердің орынсыз пайдалануына байланысты жиі туындайды. Зиянкестер ақпараттық қауіпсіздікке қатысты кейбір адамдардың тәжірибесіздігі, немқұрайлылығы мен беймәлімділігін өз пайдаларына асырады. Құпия деректерді ұрлаудың осы нұсқасын болдырмау үшін көптеген ұйымдардың басшылығы өз ұжымының арасында

арнайы саясат жүргізеді. Оның мақсаты адамдарды өзін-өзі ұстау және желілерді пайдалану ережелеріне үйрету болып табылады. Бұл өте кең таралған тәжірибе болып табылады, себебі осындай жолмен пайда болатын қауіптер де кең таралған. Кәсіпорын қызметкерлерінің ақпараттық қауіпсіздік дағдыларын алу бағдарламасына мынадай сәттер кіреді: аудит құралдарын тиімсіз пайдалануды еңсеру; деректерді өңдеу үшін адамдарды арнайы құралдарды пайдалану дәрежесін азайту; ресурстар мен активтерді қолдануды төмендету; желілік құралдарға тек белгіленген әдістермен қол жеткізуге үйрету; әсер ету аймағын бөлу және жауапкершілік аумағын белгілеу [6].

Ақпараттық қауіпсіздіктің тәуекелдері мен қатерлері көбінесе бөгде адамдарға қол жеткізуге болмайтын ақпаратты заңсыз алумен байланысты. Бірінші және ең көп таралған ағу арнасы байланыс пен қарым-қатынастың әр түрлі тәсілдері болып табылады. Қазіргі уақытта көптеген ақпарат тасымал тасығыштарда сақталғандықтан, зиянкестер осы техника түрі арқылы ақпаратты белсенді игеріп, қолға түсіреді. Байланыс арналарын тыңдау өте танымал болып табылады, енді техникалық генийлердің барлық күш-жігері смартфондардың қорғаныс кедергілерін бұзуға бағытталған. Құпия ақпаратты ұйым қызметкерлері аңдаусызда ашуы мүмкін. Олар барлық «логин және құпия сөздерді» тікелей бермесе де, қаскүнемдерге абайсызда дұрыс жолды көрсетуі мүмкін. Ақпараттық қауіпсіздікті қамтамасыз ету көбінесе сенімді техникалық қорғау құралдарын қолдануға негізделген. Егер қамтамасыз ету жүйесі жабдықтың өзінде жұмыс істеуге қабілетті және тиімді болса, онда бұл табыстың жартысы. Ақпарат қауіпсуздігін толыққанды қамтамасыз ету үшін, ақпараттық тәуекелдерді талдау керек.

Ақпараттық тәуекелдерді талдау – тәуекелдердің сандық немесе сапалық көрсеткіштеріне көшумен ақпараттық жүйенің қорғалуын кешенді бағалау үдерісі. Бұл ретте тәуекел – жүйенің қорғалуына байланысты болатын ықтимал залал. Тәуекелдерді басқару деп ақпараттық жүйеге әсер етуі мүмкін тәуекелдерді сәйкестендіру және азайту процесі түсініледі. Талдау нәтижелері қорғау құралдарын таңдау, ақпаратты қорғау жүйесінің қолданыстағы және жобаланатын кіші жүйелерінің тиімділігін бағалау кезінде пайдаланылады.

Ақпараттық технологияның өмірлік циклінің барлық сатыларында тәуекелдерді талдау, тәуекелдерді басқару тұжырымдамаларын ақпараттық қауіпсіздік мәселелерімен айналысатын көптеген ірі ұйымдар ұсынды. Қолданыстағы әдістемелерді нақтылау ұйымның даму деңгейінің көптеген жүйе құраушы факторларына, персоналдың біліктілігіне, оның қызметінің ауқымы мен ерекшелігіне және кейбір басқа факторларға байланысты. Осылайша, тәуекелдерді басқарудың кейбір тұжырымдамасына сәйкес келетін біртұтас, баршаға қолайлы әмбебап әдістеме ұсыну мүмкін емес. Тәуекелдерді басқару тұжырымдамасын іске асыру кезінде жиі туындайтын мәселелерді және оларды шешудің ықтимал тәсілдерін қарастырайық.

Қандай да бір сипатты өлшеу үшін шкаланы таңдау қажет. Шкалалар әртүрлі «күш» болуы мүмкін, қандай да бір шкаланы таңдау өлшенетін шаманың қасиеттеріне де, қолда бар өлшеу құралдарына да байланысты. «Ақпараттық ресурстың құндылығы» сипаттамалық қасиеттерін өлшеу үшін шкаланы таңдау нұсқаларын қарастырайық. Ол ресурсты қалпына келтіру құны, ресурсты қалпына келтіру уақыты және т.б. сияқты қатынастар шкалаларында тікелей өлшенуі мүмкін. Басқа нұсқа лингвистикалық айнымалының үш ықтимал мәні бар сараптамалық баға алу үшін рангтік шкаланы анықтау:

- арзан бағалы ақпараттық ресурс: оған өте маңызды міндеттер тәуелді емес, ол аз уақыт пен шамалы ақша шығынымен қалпына келтірілуі мүмкін;

- орташа құндылық ресурсы: оған бірқатар маңызды міндеттер тәуелді, бірақ ол жоғалған жағдайда, ол рұқсат етілген уақыттан кем емес уақыт ішінде қалпына келтірілуі мүмкін, қалпына келтіру құны жоғары;

- құнды ресурс: оған өте маңызды міндеттер тәуелді, қалпына келтіру уақыты және құны өте жоғары.

Тәуекелдерді өлшеу үшін абсолютті шкала жоқ. Тәуекелдерді объективті немесе субъективті өлшемдер бойынша бағалауға болады. Объективті критерийдің мысалы қандай да бір жабдықтың, мысалы, белгілі бір уақыт аралығында дербес электрондық есептеу машинасының істен шығу ықтималдығы болып табылады. Субъективті өлшемнің мысалы дербес электрондық есептеу машинасының істен шығу қатерінің ақпараттық ресурс әкімшілігінің бағалауы болып табылады. Ол үшін әдетте бірнеше градациялы рангтік шкала әзірленеді: төмен, орташа, жоғары деңгейлер. Тәуекелдерді өлшеуге бірқатар тәсілдер бар. Қарапайым жағдайда екі факторды бағалау қолданылады: оқиғаның ықтималдығы және ықтимал салдардың ауырлығы. Әдетте, оқиға ықтималдығы мен зардаптардың ауырлығы көп болған сайын тәуекел соғұрлым көп деп есептеледі. Жалпы идеяны келесі формуламен келтіруге болады:

ТӘУЕКЕЛ = Т оқиға * ШЫҒЫН БАҒАСЫ

Егер айнымалылар сандық шамалар болса, тәуекел – шығынды математикалық тұрғыдан бағалау. Егер айнымалылар сапалы шамалар болса, көбейту операциясы анықталмаған. Сапалы шамаларды пайдалану нұсқасын қарастырайық.

Тәуекелді бағалаудың сапалық әдістемелері оларды іске асыру кезінде туындайтын қауіп-қатерлер мен салдарлардың туындау ықтималдығын бағалау кезінде лингвистикалық мәндерді пайдалануды көздейді. Мұндай мәндер ретінде «өте төмен», «төмен», «орташа», «жоғары», «өте жоғары», «сыни» және т.б. шамалар қолданылуы мүмкін. Бұл тәсіл бірқатар артықшылықтарға ие: нәтижелерді көрнекі түрде ұсыну және персоналдың кез келген біліктілікті түсінуі үшін қарапайымдылық, осы әдісті іске

асыруға арналған ең аз қаржылық, уақытша және еңбек шығындары, кіріс деректерін жеткіліксіз жинау кезінде тәуекелдерді бағалауды жүргізу мүмкіндігі.

Алдымен мұндай шкаладағы оқиғалардың лингвистикалық айнымалы ықтималдығының мәндері анықталуы тиіс:

- A – оқиға ешқашан орын алмайды;
- B – оқиға сирек кездеседі;
- C – қарастырылып отырған уақыт аралығындағы оқиғаның ықтималдығы шамамен 0,5;
- D – оқиға орын алуы мүмкін;
- E – оқиға міндетті түрде орын алады.

Бұдан басқа, оқиғалар күрделілігінің субъективті шкаласы анықталады, мысалы:

- N (Negligible) – әсерді елемеуге болады;
- Mi (Minor) – болмашы оқиға: салдарлар жеңіл жойылады, салдарды жоюға кететін шығындар, ақпараттық технологияға әсер ету елеусіз;
- Mo (Moderate) – орташа нәтижемен болған оқиға: салдарларды жою ірі шығындармен байланысты емес, ақпараттық технологияға әсер ету үлкен емес және маңызды міндеттерді қозғамайды;
- S (Serious) – елеулі зардаптары бар оқиға: салдарларды жою елеулі шығындармен байланысты, ақпараттық технологияларға әсер ету айтарлықтай маңызды міндеттерді орындауға әсер етеді;
- C (Critical) – оқиға сыни маңызды міндеттерді шешудің мүмкін еместігіне әкеледі.

Тәуекелдерді бағалау үшін үш мәннен тұратын шкала қолданылады. Олар келесідей болады:

- төмен тәуекел;
- орташа тәуекел;
- жоғары тәуекел.

Белгілі бір оқиғамен байланысты тәуекел екі факторға байланысты және 2-кестедегідей анықталуы мүмкін.

Кесте 2 – Екі факторға байланысты тәуекелді анықтау

	Negligible	Minor	Moderate	Serious	Critical
A	Төмен тәуекел	Төмен тәуекел	Төмен тәуекел	Орташа тәуекел	Орташа тәуекел
B	Төмен тәуекел	Төмен тәуекел	Орташа тәуекел	Орташа тәуекел	Жоғары тәуекел
C	Төмен тәуекел	Орташа тәуекел	Орташа тәуекел	Орташа тәуекел	Жоғары тәуекел
D	Орташа тәуекел	Орташа тәуекел	Орташа тәуекел	Орташа тәуекел	Жоғары тәуекел
E	Орташа тәуекел	Жоғары тәуекел	Жоғары тәуекел	Жоғары тәуекел	Жоғары тәуекел

Тәуекел факторларының шкаласы және кестенің өзі басқаша анықталуы мүмкін, градациялардың басқа саны болуы мүмкін. Тәуекелдерді бағалаудағы мұндай үш шкала арқылы бағалау тәсілі өте кең таралған. Тәуекелдерді бағалау әдістемелерін әзірлеу (пайдалану) кезінде мынадай мүмкіндіктерді ескеру қажет:

- шкалалардың мәндері нақты анықталуы (сөздік сипаттамасы) және сараптамалық бағалау рәсімдерінің барлық қатысушылары бірдей түсінілуі тиіс;

- таңдалған кестенің негіздемесі қажет, тәуекел факторларының бірдей үйлесімімен сипатталатын әр түрлі инциденттердің сарапшылар тұрғысынан тәуекелдердің бірдей деңгейі бар екеніне көз жеткізу қажет.

Мұндай әдістеме базалық деңгейдегі тәуекелдерді бағалау және талдау жүргізу барысында кеңінен қолданылады. Ақпараттандыру объектісіндегі оқиғаның ықтималдығын бағалау 3-кестеде көрсетілгендей пайда болу жиілігіне байланысты бағаланады. Шығын бағасын бағалау 4-кестеде келтірілген. Ақпараттандыру объектісінің ақпараттық тәуекелдерін бағалау 5-кестеде көрсетілген.

Кесте 3 – Оқиғаның ақпараттандыру объектісіне ықтималдығын бағалау

Оқиға ықтималдығы	Оқиғаның пайда болуының орташа жиілігі	Оқиғаның ықтималдылық коэффициенті
A – оқиға ешқашан орын алмайды	Жылына бір реттен кем	1
B – оқиға сирек кездеседі	Жылына бір рет	2
C – қарастырылып отырған уақыт аралығындағы оқиғаның ықтималдығы шамамен 0,5	Айына бір рет	3
D – оқиға орын алуы мүмкін	Аптасына бір рет	4
E – оқиға міндетті түрде орын алады	Күніне бір рет	5

Кесте 4 – Ақпараттандыру объектісіне шығын бағасын бағалау

Шығын бағасы	Шығын бағасының коэффициенті
N (Negligible) – әсерді елемеуге болады	1
Mi (Minor) – болмашы оқиға: салдарлар жеңіл жойылады, салдарды жоюға кететін шығындар, ақпараттық технологияға әсер ету елеусіз	2

4-кестенің жалғасы

Mo (Moderate) – орташа нәтижемен болған оқиға: салдарларды жою ірі шығындармен байланысты емес, ақпараттық технологияға әсер ету үлкен емес және маңызды міндеттерді қозғамайды	3
S (Serious) – елеулі зардаптары бар оқиға: салдарларды жою елеулі шығындармен байланысты, ақпараттық технологияларға әсер ету айтарлықтай маңызды міндеттерді орындауға әсер етеді	4
C (Critical) – оқиға сыни маңызды міндеттерді шешудің мүмкін еместігіне әкеледі	5

Ақпараттандыру объектісінің тәуекелдерін талдау келесі міндеттерді шешуге мүмкіндік береді:

- іске асыру ықтималдығын азайту немесе алып тастау қажет қауіптерді анықтау;
- жүйенің жалпы қорғалуын бағалау;
- енгізілген қорғау жүйесінің тиімділігін бағалау.

Кесте 5 – Ақпараттандыру объектісінің ақпараттық тәуекелдерін бағалау

№	Оқиға	Ықтималдылық коэффициенті	Шығын бағасы коэффициенті	Ақпараттық тәуекел
1	Қорғалған ақпаратпен машиналық тасымалдағыштарды көшіру	2	3	6
2	ЖЭСЖН ұстап қалу үшін арнайы ТЖ пайдалану	1	2	2
3	Қорғалатын ақпаратты рұқсатсыз жариялау	2	3	6
4	Қорғалатын ақпараты бар есептеуіш техника құралдарын жою	3	2	6

5-кестенің жалғасы

5	Пайдаланушының бағдарлама-ақпараттық компоненттеріне және өңделетін деректерге рұқсатсыз өзгерістер енгізуі	2	5	10
6	БҚ рұқсатсыз көшіру	3	2	6
7	Визуалды бақылау	2	2	4
8	Қорғалатын ақпаратты ұсынуды ашу	2	4	8
9	АЖ аппараттық және бағдарламалық компоненттерін жобалау және әзірлеу қателерін айқындау	1	4	4
10	Штаттан тыс аппараттық немесе бағдарламалық қамтамасыз етуді орнату және пайдалану	3	2	6
11	Арнайы құралдарды пайдалана отырып, қорғау жүйелерін еңсеру жолымен немесе айналып өту арқылы АЖ ресурстарына пайдаланушының ЖТӘ	3	4	12

5-кестенің жалғасы

12	Байланыс желілері бойынша беру кезінде қорғалатын ақпаратты бұрмалау немесе қолға түсіру	3	3	9
13	Компьютерлерге бағдарламалық вирустарды енгізу	4	3	12
14	Дезинформацияны енгізу	2	3	6
15	Қорғалатын ақпаратты пайдалануға тыйым салу	3	2	6
16	Істен шығып қалуы	2	3	5
17	ТЖ мен жүйелердің істен шығуы, авариялар	1	5	5
Нәтижесі		114		

Осы жобаға қатысты ақпараттандыру объектісінің тәуекелдерін талдау келесі аса қауіпті қатерлерді анықтауға мүмкіндік берді:

- қорғалатын ақпараты бар есептеуіш техника құралдарын және машиналық тасығыштарды жою;
- қорғалатын ақпаратты ұсынуды ашу;
- бағдарламалық вирустарды енгізу;
- байланыс желілері арқылы беру кезінде қорғалатын ақпаратты бұрмалау немесе қолға түсіру;
- дезинформацияны енгізу.

Ақпараттық тәуекелдердің қорытынды коэффициенті АЖ қорғалу деңгейі жеткіліксіз жоғары екендігін көрсетеді. Модельде ақпаратты қорғаудың ішкі (ішкі көздерден шығатын қатерлерді болдырмау) және сыртқы (сырттан шығатын қатерлерді болдырмау) құралдары бөлінеді.

Сыртқы ортадағы ақпараттандыру объектісіне қауіп-қатер көздері келесідей болады:

- табиғи жүйелер – астрономиялық, планетарлық, физикалық, химиялық, биологиялық;

- жасанды жүйелер – ұйымдық-экономикалық және техникалық жүйелер, сондай-ақ, аралас сипаттағы (мысалы, биотехникалық жүйелер);

- абстракты жүйелер – символдық (модельдер, алгоритмдер, бағдарламалар, технологиялық карталар және т.б.) және сипаттамалы (мысалы, діни немесе этникалық сипаттағы оқу түрінде).

Ақпараттандыру объектісі жүйелерінің ішіндегі қауіп көздері оның кіші жүйелері мен элементтері болып табылады:

- адамдар;
- техникалық құрылғылар мен жүйелер;
- технологиялық өңдеу схемалары;
- деректерді өңдеу жүйесінде қолданылатын модельдер, алгоритмдер, бағдарламалар [7].

Ақпараттандыру объектісі үшін ақпаратты қорғау жүйесін жобалау ақпараттық технологияларды пайдаланумен байланысты ықтимал теріс салдарларды төмендетуге ықпал етуі және кәсіпорынның негізгі мақсаттары мен міндеттерін орындау мүмкіндігін қамтамасыз етуі тиіс. Тиімді тәсілдердің бірі ақпараттық жүйенің өмірлік циклін басқару жүйесіне тәуекелдерді басқару жүйесін ықпалдастыру болып табылады. Ол 6-кестеде көрсетілген.

Кесте 6 – АҚ жүйесінің өмірлік циклінің әртүрлі сатыларында тәуекелдерді басқару

Ақпараттық технологияның өмірлік циклінің фазасы	Тәуекелдерді басқару фазасына сәйкестігі
АҚ жүйесінің жобалау алдындағы сатысы (осы ақпараттық жүйенің тұжырымдамасы: мақсаттар мен міндеттерді анықтау және оларды құжаттау)	АҚ-ның осы жүйесі үшін мақсаттар мен міндеттерден туындайтын тәуекелдердің негізгі санаттарын анықтау, АҚ-ны қамтамасыз ету тұжырымдамасы
АҚ жүйесін жобалау	Ақпараттық қауіпсідік жүйесіне тән тәуекелдерді анықтау (ақпараттық қауіпсіздік жүйесі архитектурасының ерекшеліктерінен туындайтын)
АҚ жүйесін құру: элементтерді жеткізу, монтаждау, баптау және конфигурациялау	Ақпараттық қауіпсіздік жүйесінің жұмыс істеуі басталғанға дейін барлық санаттар сәйкестендірілуі тиіс, сонымен қатар міндетті түрде назарға алынуы тиіс
АҚ жүйесінің жұмыс істеуі	Сыртқы жағдайлардың өзгеруіне және ақпараттық қауіпсіздік жүйесінің конфигурациясына байланысты тәуекелдерді мерзімді қайта бағалау

6 – кестенің жалғасы

АҚ жүйесінің жұмыс істеуін тоқтату (ақпараттық және есептеу ресурстары бұдан әрі мақсаты бойынша пайдаланылмайды)	Ақпараттық ресурстарға қатысты АҚ талаптарын сақтау

Кәсіпорынның ақпараттық жүйесіне әсер ететін тәуекелдерді талдаудың сандық әдістері:

- статистикалық талдау әдісі;
- сараптамалық бағалау әдісі;
- аналитикалық әдіс;
- аналогтар әдісі.

Статистикалық әдістер инциденттердің ықтималдығын және ықтимал шығын мөлшерін анықтау мақсатында осы немесе ұқсас кәсіпорында орын алған қандай да бір ақпараттық қатерлерді іске асыру және кейінгі ақшалай шығындар туралы статистикалық деректерді жинақтаудан тұрады. Тәуекелдің шамасы немесе дәрежесі екі көрсеткішпен өлшенеді: орташа мәнмен және ықтимал нәтиженің өзгергіштігімен. Тәуекелдің орташа күтілетін мәні барлық ескерілген нәтижелердің орташа өлшемді шамасы түрінде көрсетіледі. Алайда орташа шама түпкілікті шешім қабылдауға мүмкіндік бермейді. Бұл шешім үшін үлестірудің берілген заңында кездейсоқ шаманың орташа квадраттық ауытқуын ескеру қажет.

Статистикалық әдістерді қолдану кезінде көптеген факторларға байланысты кездейсоқ шамаларды бөлудің ең ықтимал заңдары туралы гипотезалар қолданылады. Ең жиі дискретті шамалар үшін үздіксіз шамалар мен көрсеткіштік үлестіру үшін қалыпты үлестіру гипотезасы қабылданады. Бастапқы таралу заңдарының гипотезасы дұрыс кезінде статистикалық әдістер таңдалған критерий мағынасында оңтайлы тәуекелді бағалауға қол жеткізуге мүмкіндік береді.

Статистикалық әдістерге Монте-Карло әдісі деп аталатын статистикалық сынақ әдісі жатады. Оның артықшылығы ақпараттық ресурстарға шабуылдардың әртүрлі «сценарийлерін» талдау және бағалау немесе баламалы қатерлерді іске асыру мүмкіндігі болып табылады. Бұл әдіс өте күрделі модельдер үшін тәуекелді нақты бағалауға мүмкіндік береді. Алайда, бұл әдісті тек өзгермейтін статистикалық жағдайларда ғана пайдалануға болады. Нақты жағдай өзгерген кезде бағалау дұрыс болмауы мүмкін.

Статистикалық әдістер қандай да бір шамада тәуекелді талдау бойынша барлық бағдарламаларда пайдаланылады. Статистикалық ақпаратты өңдеудің теориялық әдістері жеткілікті жақсы әзірленген, алайда нақты жағдайлардың белгісіздік деңгейі соншалықты жоғары болып табылады, бұл статистикалық әдістердің барабарлығы қосымша дәлелдемелерді талап етеді.

Сараптамалық әдістер статистикалық әдістерден, тәуекел моделін құру үшін бастапқы ақпаратты жинау тәсілімен ерекшеленеді. Бұл ретте статистикалық деректерді жинау мен талдауды ол үшін барлық қажетті білімі бар сарапшылар орындайды деп болжанады. Сараптамалық жолмен алынған бағалар тәуекелдің барлық факторларын есепке алуға негізделеді және ең жоғары дәрежеде нақты ортаның ерекшелігін ескереді деп есептеледі. Мұндай болжамдар кезінде сараптамалық бағалау сапасы сарапшылардың біліктілігі мен құзыреттілігіне айтарлықтай тәуелді екені түсінікті.

Тәуекелді бағалаудың параметрлік рәсімдерінде сараптамалық бағалар пайдаланылатын параметрлердің бағаларын алу үшін пайдаланылады. Осылайша әр түрлі қауіп-қатерлер мен мүмкін зияндардың ықтималдықтарына сараптамалық бағалау беріледі. Көптеген жобалар процестерінің статистикалық сипаты осы әдістерді барынша әмбебап ете отырып, тәуекелді анықтау кезінде сараптамалық бағалаудың рөлін арттырады.

Ақпараттық жүйелерде тәуекелдің өсуі ілеспе факторларды неғұрлым мұқият бағалауды талап етеді. Альтернативті сипатқа ие көптеген бастапқы деректер неғұрлым шындыққа жақын баламаларды таңдау үшін сараптамалық бағалауды пайдалануды болжайды. Сондықтан ақпараттық тәуекелдерді бағалаудың қазіргі заманғы жүйелері сараптамалық жүйелерге көбірек жақындап келеді, және де сарапшының рөлі бұрынғыдан маңызды болады.

Сарапшылардың бағалауы, әдетте, белгілі бір ережелер бойынша орындалатын қарама-қайшылыққа талдауға түседі. Біріншіден, кез келген фактор бойынша екі сарапшының бағалаулары арасындағы барынша жол берілетін айырмашылық өте үлкен болмауы тиіс. Егер сарапшылар саны үштен көп болса, онда салыстырылатын бағалар талданады. Екіншіден, сарапшылардың барлық тәуекелдер жиынтығы бойынша пікірлерінің келісімділігін бағалау үшін пікірлері бір-біріне әлдеқайда сәйкестендірігмеген екі сарапшы таңдалады. Сарапшылардың пікірлері арасында бағалаудың жол берілмейтін алшақтықтары анықталған жағдайда басқа сарапшыларды тарта отырып, кеңестерде талқыланады. Үлкен алшақтықтар болмаған жағдайда сарапшылардың барлық бағалары қорытынды баға алу үшін пайдаланылады.

Сараптамалық бағалауды алудың қуатты тәсілі «шешім ағашын» пайдалану болып табылады. Бұл әдіс инциденттерді жүзеге асыру кезінде орын алуы мүмкін ықтимал тәуекел сценарийлерін графикалық құруды болжайды. «Ағаштың» тармақтары ықтимал оқиғалардың субъективті және объективті бағаларына сәйкес келеді. Салынған тармақтарды бойлай отырып және ықтималдылықты есептеудің арнайы әдістерін пайдалана отырып, әрбір жолды бағалайды және одан кейін тәуекелділігі төменірегін таңдайды. Алайда, бұл әдіс өте қиын.

Кез келген жағдайда сараптамалық бағалауды алу әдістері сарапшыларды іріктеуге аса назар аударуды талап етеді, өйткені бағалау сапасы олардың білімі мен құзыреттілігіне тікелей тәуелді.

Тәуекел қисығын құрастырудың *аналитикалық әдістері*, тек кәсіби мамандарға ғана қол жетімді, өте күрделі әдіс. Көбінесе, аналитикалық әдістер бизнес – процестер деңгейіндегі тәуекелдерді бағалау үшін қолданылады. Әдетте, аналитикалық әдістердің негізінде таңдалған модельдің сезімталдығын талдау жатыр. Ол бірнеше қадамдардан тұрады:

- сезімталдыққа бағалау жүргізілетін негізгі экономикалық көрсеткішті таңдау (кірістің ішкі нормасы, таза келтірілген кіріс және т. б.);
- әсер ететін факторларды таңдау (ресурстың құпиялылығын, тұтастығын немесе қол жетімділігін жоғалту және т.б.);
- әсер ететін факторлардың шамасына байланысты жобаны жүзеге асырудың әртүрлі кезеңдерінде негізгі көрсеткіштің вариацияларын есептеу.

Бұдан әрі тұрақсыздандыратын факторларға қатысты негізгі көрсетушінің сезімталдығы талданады. Жоғары сезімталдыққа тәуекелдің жоғары дәрежесі сәйкес келеді және керісінше, егер негізгі көрсеткіштің тұрақсыздандырғыш фактордың вариациясына сезімталдығы елеусіз болса, онда бұл, әдетте, тәуекелдің төмен дәрежесінің дәлелі. Алайда мұндай әдіс басқа балама сценарийлерді іске асыру мүмкіндігі мен ықтималдығын ескермейтіндіктен, елеулі әдіснамалық кемшіліктерге ие. Жобаның қаржылық жағдайын талдау үшін деректерді дайындау кезінде есептік ақша бірлігін таңдау өте маңызды болып табылады. Қатерді азайту есептеулерінің сенімділігін арттыру үшін аналитикалық әдістердің сенімділігін арттыруға мүмкіндік беретін әртүрлі әдістерге сүйенеді: Монте-Карло әдісі, экономикалық-математикалық моделдеу және т.б. Түрлі тұрақсыздандыратын факторларды ескере отырып, пайданы қалыптастыру тетігінің әрекетін неғұрлым нақты түсінген кезде тәуекел азайтылуы мүмкін деп болжанады. Өндірістік қызмет процесінде кәсіпорын тап болуы мүмкін ақпараттық тәуекелдер анықталғаннан кейін, тәуекел деңгейіне әсер ететін тұрақсыздандырғыш факторларды анықтау және тәуекелдерге бағалау жүргізу, сондай-ақ, олармен байланысты әлеуетті шығындарды анықтау кәсіпорын алдында тәуекел деңгейін рұқсат етілген шамаға дейін төмендетуді қамтамасыз ететін қорғау бағдарламасын әзірлеу міндеті тұр.

Аналогтар әдісі басқа әдістерді қолдану нәтиже бермеген жағдайда қолданылады. Жалпы байланыстарды анықтау үшін ұқсас объектілердің базасы құрылады және нәтижелер зерттелетін объектіге ауыстырылады. 7-кестеде ақпараттық тәуекелдерді бағалау әдістерінің негізгі артықшылықтары мен кемшіліктері көрсетілген [8].

Қорғауды бағалау үшін тәуекелдерді талдау әдіснамасы ақпараттық қауіпсіздіктің халықаралық стандарттарымен (COBIT, ISO 17799, ISO 27001 және т.б.) айқындалады. Тәуекелдерді талдау келесі алдын ала кезеңдерді болжайды:

- ақпараттық ресурстарды бағалау;

- ақпараттық жүйенің қауіпсіздігі қатерлерін талдау;
- ақпараттық жүйенің осалдығын талдау.

Алдын ала кезеңдер мен тәуекелдерді талдау рәсімдерінің өзара байланысы 1-суретте көрсетілген.

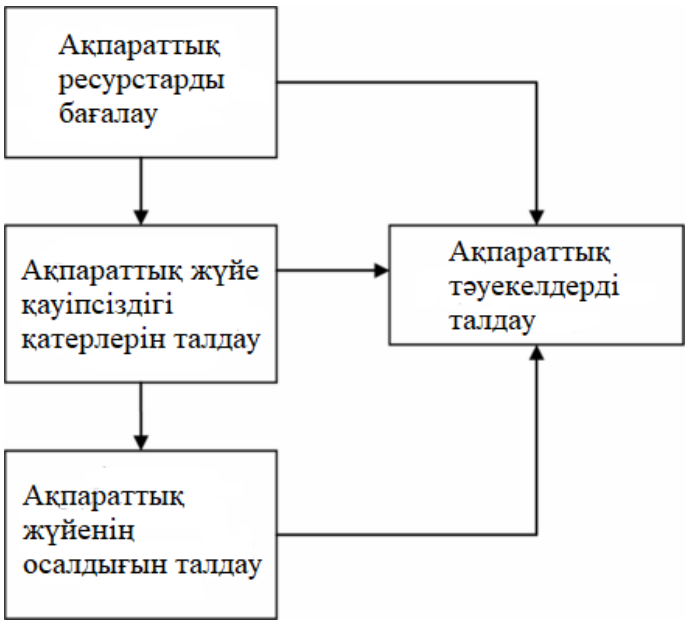
Ақпарат, аппараттық, бағдарламалық және техникалық құралдар енгізілетін ақпараттық ресурстарды бағалау қаралып отырған жағдайларда ақпараттық қауіпсіздікті бұзудан болатын ықтимал залалды бағалауды болжайды. Әдетте, бұл ықтимал шығындарды бағалау үшін ресурстар пайдаланылатын бизнес-процестердің моделін жасауды талап етеді.

Кесте 7 – Ақпараттық тәуекелдерді талдау әдістерін зерттеу нәтижелері

Атауы	Артықшылықтары	Кемшіліктері	Қолдану саласы
Статистикалық әдістер	Жоғары теориялық даму	Нақты жағдайдың белгісіздігінің жоғары деңгейінде практикалық іске асырудың күрделілігі болып табылады	Нақты құбылыстар мен процестердің статистикалық модельдерін зерттеу
Сараптамалық бағалау әдісі	Тәуекелдің барлық факторлары мен ортаның ерекшелігі ең жоғары деңгейде ескеріледі	Сарапшылар арасында көшбасшы пікірінің үстемдігі	Объект туралы деректер жеткіліксіз болғанда талдаудың басқа әдістерін қолданбаса пайдаланады
Аналитикалық әдістер	Негізгі көрсеткіштің тұрақсыздандырғыш әсерлерге сезімталдығына талдау жүргізіледі	Басқа балама сценарийлерді іске асыру мүмкіндігі мен ықтималдығын ескермейді	Математикалық модельдеу негізінде шығындар алу ықтималдығы анықталады, экономикалық тәуекелдерді талдау үшін қолданылады

7-кестенің жалғасы

Аналогтар әдісі	Ұқсас объектінің тәуелділіктері сәйкес келген кезде тәуекелді бағалаудың жоғары дәлдігі	Ұқсас объектілерді ң деректер базасын құрудың еңбек сыйымдылығы	Жалпы тәуелділіктерді анықтау және оларды зерттелетін жобаға көшіру үшін ұқсас жүзеге асырылған жобалардың деректер базасы пайдаланылады



Сурет 1 – Ақпараттық тәуекелдерді талдаудың негізгі кезеңдері

Қауіптерді талдау сыртқы ортадан төнетін қауіп-қатерлерді анықтауды қамтиды. Қауіптерді талдауды талданатын жағдайларда жеткілікті жұмыс тәжірибесі бар мамандар орындауы және нақты жағдайларда болуы мүмкін жағдайлардың барлық спектрін қамтуы тиіс. Осалдықтарды талдау конфигурациядағы ақпараттық жүйені бағалаумен және осы ақпараттық жүйе бизнес-процестерде пайдаланылатын жұмыс баптауларымен байланысты. Бастапқы кезеңдерде тәуекелдерді талдаудың негізгі рәсімі үшін қажетті ақпарат қалыптастырылады. Тәуекелдерді талдау рәсімі тәуекелдерді бағалаудың кейбір математикалық құралын пайдалануды меңзейді. Тәуекелді бағалау негізінде контрмерлерді таңдау және олардың тиімділігін бағалау жүзеге асырылады,сондай-ақ қалдық тәуекелдердің шамасы айқындалады. Тәуекелдерді талдаумен аудит

нәтижесі басқару тетіктерін енгізу бойынша іс-қимыл жоспары (қорғау жоспары) болуы тиіс.

Ақпараттық тәуекелді сапалы талдаудың нәтижесі ақпараттық жүйенің қатерлері мен осалдықтарын, сондай-ақ, қауіпті дамытудың ықтимал сценарийлерін айқындау болады:

- ықтимал қауіп сценарийлерін анықтау;
- кәсіпорын қызметі барысында туындайтын қауіптерді анықтау;
- ақпараттық қауіп-қатерлердің әсерінен болуы мүмкін артықшылықтары мен кемшіліктерін анықтау.

Бағалаудың сапалық әдісінің артықшылығы, ол кәсіпорынның ақпараттық жүйесіне әсер ететін қауіптердің негізгі түрлерін анықтауға мүмкіндік береді. Мұндай әдістің артықшылығы, жобаны іске асырудың бастапқы кезеңдерінде жобаға сәйкес келетін ықтимал тәуекелдерді анықтауға және жобаны іске асыру немесе одан бас тарту туралы шешім қабылдауға болады. Жүргізілген талдау нәтижесінде жоба басшысы сандық талдау жүргізудің мәні бар қауіптер туралы ақпарат алады, яғни нақты міндетті іске асыру кезінде болатын тәуекелдерді ғана бағалау жүргізіледі.

Ақпараттық қауіпсіздік саласындағы мамандар ақпараттық тәуекелдерді анықтау және ықтимал салдарларды болжау үшін, негізінен талдау мен тәуекелдерді төмендетудің түрлі әдістерін пайдаланып, ақпараттық қауіпсіздікті қамтамасыз ету үшін түрлі бағдарламалар қолданады. Бұл бағдарламалар туралы келесі тарауда егжей-тегжейлі жазылған [9].

Дипломдық жобаны жүзеге асыру үшін «LawDes» ЖШС заң компаниясының құрылымы қарастырылды.

«LawDes» ЖШС заң компаниясы мүмкін болатын келеңсіз салдардың алдын алуға, сондай-ақ, түрлі құқықтық мәселелер бойынша жедел заңгерлік көмек пен қолдау көрсетуге бағытталған. Компания бизнес үшін де, азаматтар үшін де түрлі заң қызметтерін ұсынады. Олар:

- Клиенттің мүдделерін барынша ескере отырып, ықтимал тәуекелдер мәніне шарттарды әзірлеу және заңдық сараптау;
- Мемлекеттік сатып алу жөніндегі тендерлерге қатысу үшін құжаттарды дайындау;
- Еңбек заңнамасы бойынша жұмыс берушілердің мүдделерін қорғау;
- Банктерде мемлекеттік субсидиялар, кредиттер алу үшін құжаттарды дайындау;
- Мұрагерлік құқық мәселелері;
- Жеке/мемлекеттік сот орындаушыларының заңсыз әрекеттеріне шағымдану;
- Соттық даулар, түрлі санаттағы істер: борышты өндіріп алу, неке-отбасы, жер, тұрғын үй, мұрагерлік, еңбек, денсаулығына келтірілген зиянды өтеу/мүлкіне, шығаруға, тұтынушылардың құқықтарын қорғау және т.б.

2. Кәсіпорынның ақпараттық қауіпсіздік тәуекелдерін бағалауды және төмендетуді жобалау

2.1. Тәуекелдерді бағалаудың бағдарламалық құралын таңдау

Тәуекелдерді бағалау әдістемелері көптеген технологиялық және экономикалық дамыған елдерде қолданылады. Бұл әзірлемелер қарапайым, танымал және негізінде халықаралық стандарттардың ережелері мен талаптары базасы жатыр, көбінесе жалпы қабылданған ISO 17799 стандарты. ISO/IEC 17799:2005 халықаралық стандарты ISO/IEC 27002:2005 болып өзгерді «Ақпараттық технологиялар. Қауіпсіздікті қамтамасыз ету әдістері. Ақпараттық қауіпсіздікті басқарудың тәжірибелік ережелері» (Information technology. Security techniques. Code of practice for information security management). Стандарт нөмірі ғана өзгерді. Оның атауы мен мазмұны өзгеріссіз қалды. Оны әлемнің түрлі елдеріндегі кәсіпорындар мен ұйымдар жиі пайдаланады, бұл стандарт ерікті негізде ақысыз қолданылады. Оны толығырақ қарастырайық.

ISO 17799 халықаралық стандарты екі ережеден тұрады.

Бірінші ережеде (ақпараттық қауіпсіздікті басқару және бақылау жөніндегі ұсыныстар) ұйымдағы ақпарат қауіпсіздігі режимін ұйымдастырудың маңызды аспектілері көрсетілген:

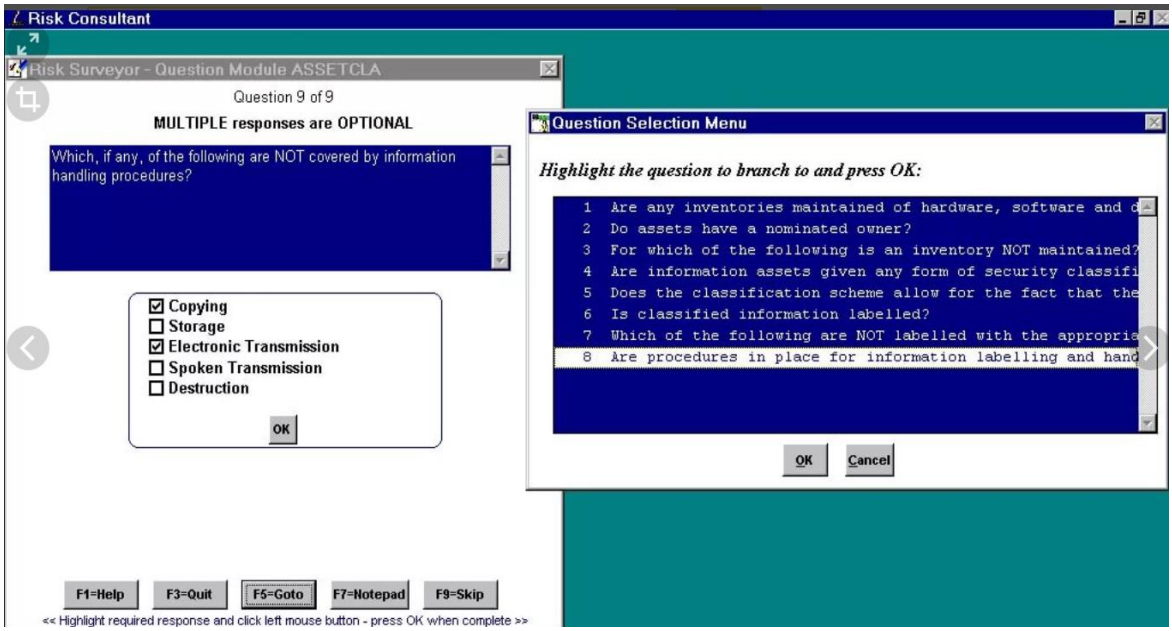
- ақпараттық жүйенің қауіпсіздігі;
- бақылау және басқару құралдарын әзірлеу;
- кәсіпорынның ресурстарын сипаттау және бақылау;
- кадрларды басқару;
- жеке қауіпсіздік;
- кәсіпорынның жергілікті есептеу желілерін баптау;
- ресурстарға қол жеткізуді бақылау;
- басқару жүйелерін баптау, әзірлеу және қызмет көрсету;
- кәсіпорынның үздіксіз жұмысын ұйымдастыру;
- жүйенің талаптарға сәйкестігін тексеру.

Екінші ереже бірінші сияқты, бірақ компанияның қауіпсіздік режимінің стандарт талаптарына сәйкестігі тұрғысынан қарайды. Практикалық жағынан бұл ереже тексерушіге арналған құрал болып табылады және кез келген ұйымның ақпараттық жүйесінің қауіпсіздігіне ішкі немесе сыртқы тексеруді жедел жүргізуге мүмкіндік береді. ISO / IEC 17999 талаптары негізіндегі тәуекелдерді бақылаудың негізгі әдістері COBRA және RA Software Tool стандарттары болып табылады. COBRA әдістемесін қарастырайық.

2.1.1 COBRA әдістемесі

C&A Systems Security Ltd компаниясы COBRA деп аталатын ақпараттық тәуекелдерді талдау және бақылау үшін әдістеме мен бағдарламалық кешенді енгізді. Бұл кешен ақпараттық жүйенің, кез келген компанияның қауіпсіздік тәуекелдерін бағалаудың базалық нұсқасын

автоматты режимде орындауға мүмкіндік береді. Ол үшін ISO 17799 халықаралық стандартының талаптарына бағытталған стандартты білім жинақтарын және шығару рәсімдерін пайдалану қажет. Бұл әдістің жүзеге асырылуын «Risk Consalting» деп аталатын бағдарлама арқылы көруге болады (Сурет 2). Сауалнамалар бізге ақпараттық активтер мен бизнес транзакциялардың тәуекелдерін бағалауға мүмкіндік береді. Бұл бағдарламада консалтинг үшін көптеген функциялар бар, оның көмегімен аналитикалық есеп жүргізуге болады. Бағдарламалық қамтамасыз ету жиынтығына COBRA ISO 17799 модульдері, сондай-ақ, COBRA модулінің менеджері кіреді. Сауалнаманың көмегімен тікелей бағалау жүзеге асырылады: жоғары деңгейлі; ақпараттық технологиялардың қауіпсіздігі; жедел ақпараттық технология және бизнес; электрондық коммерция инфрақұрылымы. APPCNTRL үшін деректерді инициализациялау мысалы: «соңғы 2 жылда ұрлықтың қанша инциденті болды?», мұндай қақтығыстар саны оннан көп болған кезде «10» санын енгізуге болады.



Сурет 2 – бағдарламаның chek list – і

Сауалнамада ұрланған зат бойынша, бұл зиян келтіру дәрежесін нақты анықтауға және қандай да бір оқыс оқиға ақпараттық жүйелер ресурстарының қауіпсіздігіне әсер еткенін нақтылау жоқ. Мұндай тәсіл тек қана тәуекелді дәл емес бағалауды іске асыруға мүмкіндік береді. COBRA әдісі үшін тәуекелдің базалық сипаттамаларына келетін болсақ, BC1, BC2 құрамдастарын бейнелеуге болады. Мысалы, BC1 компонентіне BC11= «ұрлық» мәні (көрсетілген мысалдан) сәйкес келеді. Бұл әрекет шабуылдар ресурстарының белгілі бір қауіпсіздік сипаттамаларын бұзуға әкеледі және BC27= «НКЦД» мәнімен байланысты болуы мүмкін. Енгізілген деректерді өңдегеннен кейін бағдарлама есепті тәуекелдің мынадай сипаттамалары бойынша егжей-тегжейлі бағалауды генерациялайды: санаты; деңгейі;

бағалау. Мысалы: тәуекел санаты – «бизнестегі күтпеген жағдай»; тәуекел деңгейі – 96,61%. Ақпараттық қауіпсіздік тәуекелін бағалау осылайша көрінуі мүмкін – «Қызметкерлер күтпеген жағдайларға дайын емес». Әдістемеде одан әрі кезеңмен оларды төмендету бойынша ұсынылатын шаралар келтіріледі. Осылайша, келтірілген мысалда көрсетілген тәуекел санаты үшін ұсыныс беріледі: «Пайдаланушылар өздерінің ең төменгі қызмет көрсету талаптарын формальды түрде анықтап, күтпеген жағдайларға дайын болуы тиіс» [10].

2.1.2 CRAMM әдістемесі

CRAMM бағдарламалық өнімі (the UK Goverment Risk Analysis and Managment Method) – бұл ақпараттық жүйелердің өмірлік циклінің барлық сатыларында тәуекелдерді талдау есептерін шешуге мүмкіндік беретін өте қуатты және әмбебап құрал.

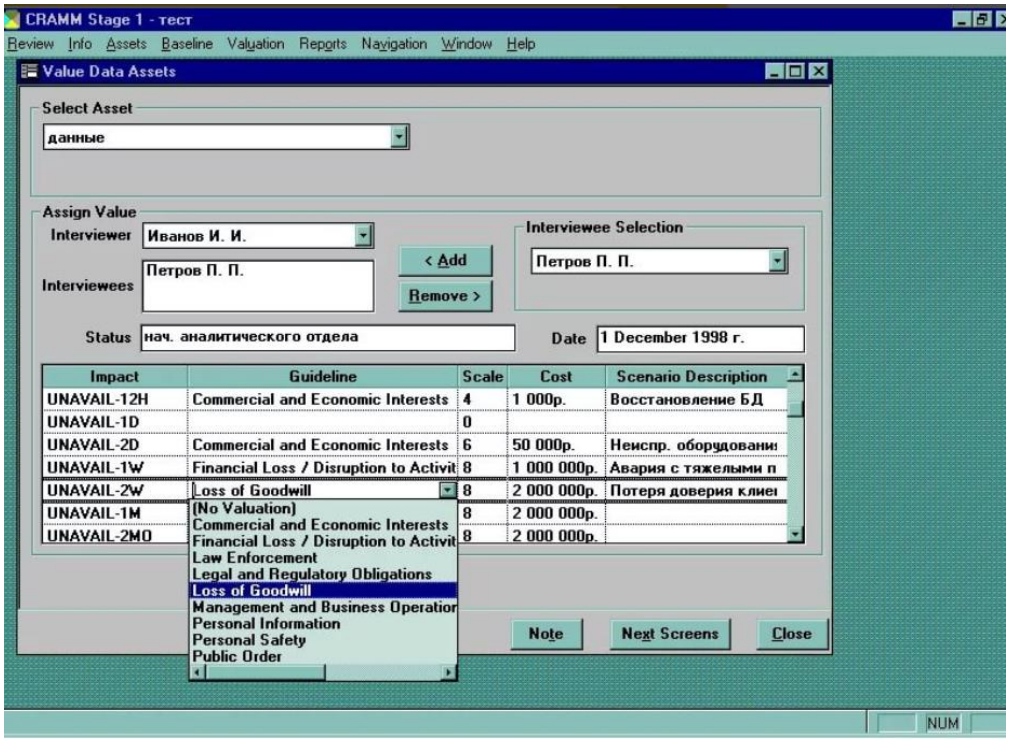
Ол құпия ақпаратты өңдеумен айналысатын мемлекеттік мекемелерде пайдалану үшін Ұлыбританияның қауіпсіздік қызметімен әзірленген. Әдіс Ұлыбританияның мемлекеттік стандарты ретінде бекітілген. CRAMM әдісін іске асыратын бағдарламалық өнімді әзірлеу және сүйемелдеумен Insight Consulting Limited фирмасы айналысады. Қазіргі уақытта фирма бағдарламалық өнімнің бірнеше нұсқасын әзірледі. Нұсқалар қорғаныс министрлігінің, азаматтық мемлекеттік мекемелердің, қаржы құрылымдары мен жеке ұйымдардың талаптарына сай бағытталған.

Барлық нұсқалардың негізін BS 7799 стандартының ұсынымдарына негізделген ақпараттық қауіпсіздік саласындағы контрмерлер бойынша жеткілікті көлемді білім базасы құрайды. CRAMM фирмасының бағдарламалық өнімі әртүрлі ұйымдармен пайдаланылады, әрбір ұйым тиісті білім базасы бар өз профилін жасайды. Коммерциялық ұйымдар үшін коммерциялық профиль, үкіметтік ұйымдар үшін үкіметтік профиль және т. б. ұсынылады. CRAMM әдістемесінде тәуекелдерді басқару бірнеше кезеңде жүзеге асырылады (Сурет 3).

Сурет 3 – CRAMM әдістемесінде тәуекелдерді басқару

Бұның мәні техникалық сипаттағы аспектілерді (АТ-жабдықтар, БҚ), сонымен қатар техникалық емес сипаттағы (мысалы, физикалық және адами)

қоса алғанда, тәуекелдерді талдауға талапшыл көзқарас болып табылады (Сурет 4).



Сурет 4 – Бастапқы деректерді енгізу процесі

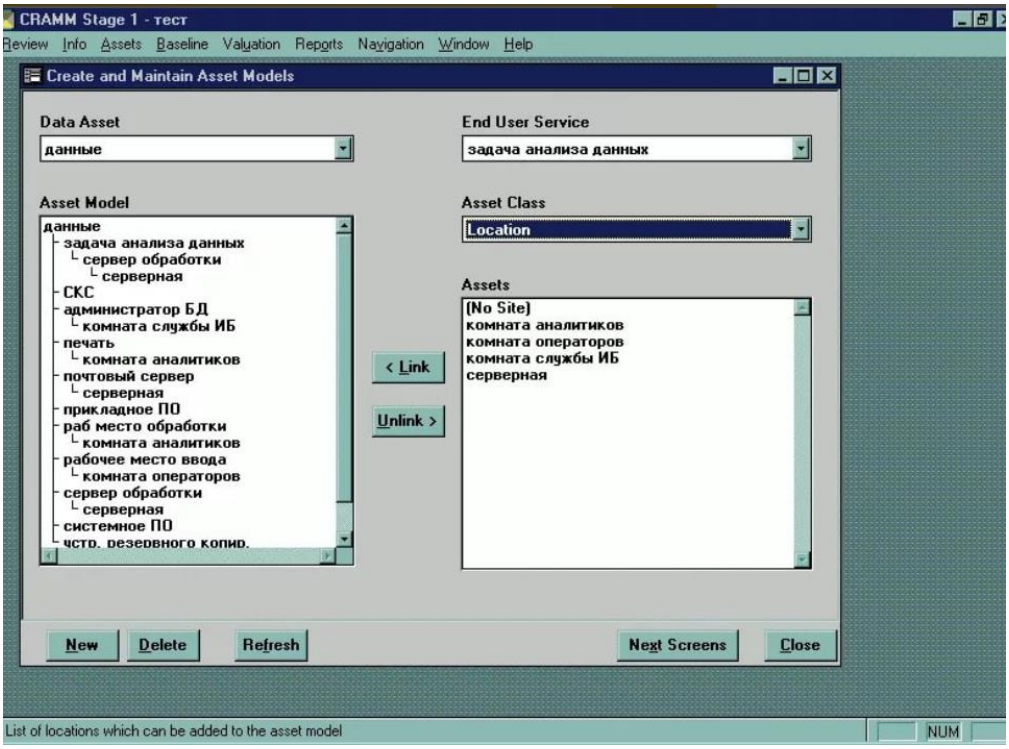
CRAMM тәуекелдерді 3 қадамда бағалауды білдіреді. Бастапқы қадамда жүйенің шекараларының ішінде қамтылған физикалық, бағдарламалық және ақпараттық ресурстарды сәйкестендіру өтеді. Бағдарламада физикалық ресурстардың құндылығы бұзылған жағдайда оларды қалпына келтіру құнымен анықталады.

Екінші қадам түрлі ресурстар мен олардың осалдықтарына арналған қауіптер деңгейін сәйкестендіру мен бағалауға қатысты барлық нәрселерді анықтайды. CRAMM әр ресурстар тобы және 39 қауіптер түрлері үшін деректерді енгізгеннен кейін деңгейлерді бағалау өте жоғары, жоғары, орташа, төмен, өте төмен (қауіп үшін), және жоғары, орташа және төмен сияқты басым сұрауларды қалыптастырады.

Өңдеу үшін белгілі бір балл санын нұсқаудың көмегімен сұрау салу деректерін инициализациялау нұсқалары ұсынылады: a) бір реттен (0 бал); ... d) орташа есеппен жылына бір реттен жиі (30 бал) және т.б. осы ақпараттың негізінде тәуекел деңгейлері есептеледі (тәуекел 1-ден 7-ге дейінгі градациялы дискретті шкалада залал келтіруге қабілетті қандай да бір іс-әрекет немесе оқиға нәтижесінде шығынның мүмкіндігі ретінде анықталады.

Тәуекелді талдау бірінші және екінші кезеңдерінде жүргізіледі, содан кейін оны бағалау жүзеге асырылады (Сурет 5). Талдау кезінде қауіптің пайда болу жиілігі мен қауіп-қатерді іске асыру ықтималдығы тұрғысынан әрбір ресурс үшін коэффициенттер қою ұсынылады, осыған байланысты

мұнда есепке ала отырып, ВС5 және ВС3 компоненттерін бөліп көрсетуге болады.



Сурет 5 – Талдау үшін деректерді енгізу процесі

Ресурстар құнының бағаларына сүйене отырып, «болжанатын жылдық ысыраптарды» біледі. Кестеде күтілетін шығындарды бағалау матрицасының мысалы келтірілген, мұнда сол жақтағы екінші баған ресурс құнының мәндерін қамтиды, кесте тақырыбының жоғарғы жолы – жыл бойы қауіптің туындау жиілігін бағалау мәнін (қауіптің деңгейі), тақырыптың төменгі жолы – қауіптің іске асырылуы жетістігінің ықтималдығын бағалау (осалдықтың деңгейі) мәнін білдіреді (Кесте 8, Сурет 6).

Кесте 8 – Күтілетін жылдық шығындар матрицасы

		0.1 0.1	0.1 0.5	0.1 1	034 0.11	0.34 0.5	0.34 1	1 0.1	1 0.5|	1 1|	3.3 3 0.1	3.3 3 0.5	3.3 3 1	10 0.1	10 0.5
1	1000	1.0E+01	5.0E+01	1.0E+02	3.4E+01	1.7E+02	3.4E+02	1.0E+02	5.0E+02	1.0E+03	3.3E+02	1.7E+03	3.3E+03	5.0E+03	5.0E+03
2	10000	1.0E+02	5.0E+02	1.0E+03	3.4E+02	1.7E+03	3.4E+03	1.0E+03	5.0E+03	1.0E+04	3.3E+O3	1.7E+04	3.3E+04	5.0E+04	5.0E+04
3	30000	3.0E+02	1.5E+03	3.0E+03	1.0E+03	5.1E+03	1.0E+04	3.0E+03	1.5E+04	3.0E+04	1.0E+04	5.0E+04	10E+5	1.5E+05	1.5E+05

8-кестенің жалғасы

4	100 00	1.0E +03	5 0E+ 03	1.0E +04	3.4 E+0 3	1.7E +04	34E+ 04	1.0E +04	50E+ 04	1.0 E+ 05	3.3 E+0 4	1.7 E+0 5	3.3 E+ 05	5.0E+ 05	5.0E +05
5	300 000	30E +03	1.5E +04	3.0E +04	1.0 E+0 4	5.1E +04	1 0E+0 5	30E +04	1.5E+ 05	3.0 E+ 05	1.0 E+0 5	5 0E+ 05	1.0 E* 06	1.5E+ 06	1.5E +06
6	100 000 0	1.0E +04	5.0E +04	1.0E +05	3.4 E+0 4	1.7E +05	3.4E+ 05	1.0E +05	5.0E+ 05	1.0 E+ 06	3.3 E+0 5	1.7 E+0 6	3.3 E+ Об	5.0E+ 06	5.0E +06
7	300 000 0	3.0E +04	1.5E +05	3.0E +05	1.0 E+0 5	5.1E +05	1.0E+ 06	3.0E +05	1.5E+ 06	3.0 E+ 06	1.0 E+0 6	5.0 E+0 6	1.0 E+ 07	1.5E+ 07	1.5E +07
8	1E+ 07	1.0E +05	5.0E +05	1.0E +06	3.4 E+0 5	1.7E +06	3.4E+ 06	1.0E +06	5.0E+ 06	1.0 E+ 07	3.3 E+0 6	1.7 E+0 7	3.3 E+ 07	5.0E+ 07	5.0E +07
9	ЗЕ+ 07	3.0E +05	1.5E +06	3.0E +06	1.0 E+0 6	5.1E +06	1.0E+ 07	3.0E +06	1.5E+ 07	3.0 E+ 07	1.0 E+0 7	5.0 E+0 7	1.0 E+ 08	1.5E+ 08	1.5E +08
10	1E+ 08	1.0E +06	5.0E +06	1.0E +07	3.4 E+0 6	1.7E +07	3.4E+ 07	1.0E +07	5.0E+ 07	1.0 E+ 08	3.3 E+0 7	1.7 E+0 8	3.3 E+ 08	5.0E+ 08	5.0E +08

CRAMM Measure of Risk	"Annual Loss of Expectancy"
1	<£1,000
2	<£10,000
3	<£100,000
4	<£1,000,000
5	<£10,000,000
6	<£100,000,000
7	<£1,000,000,000

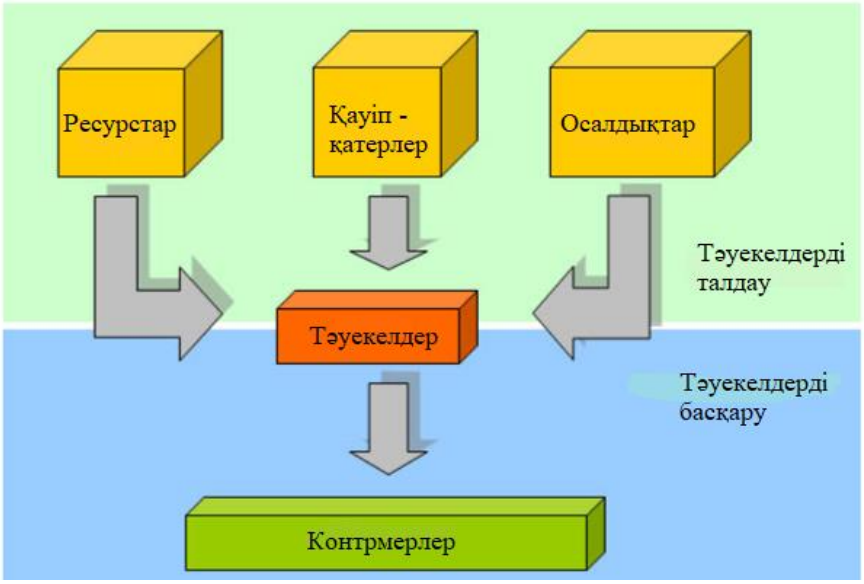
Сурет 6 – Бағалау шкаласы

Зерттеудің үшінші кезеңі – тиісті контрмерлерді іздеу. Мұнда CRAMM күрестің бірнеше нұсқаларын шығарады (Кесте 9).

Кесте 9 – Тәуекелді бағалау матрицасы

Threat	Very	Very	Very	Low	Low	Low	Medium	Medium	Medium	High	High	High	Very	Very	Very
	Low	Low	Low										High	High	High
Vuln. / Asset Value	Low	Medium	High	Low	Medium	High	Low	Medium	High	Low	Medium	High	Low	Medium	High
1	1	1	1	1	1	1	1	1	2	1	2	2	2	2	3
2	1	1	2	1	2	2	2	3	3	2	3	3	3	3	4
3	1	2	2	2	2	3	2	3	3	3	3	4	3	4	4
4	2	2	3	2	3	3	3	3	4	3	4	4	4	4	5
5	2	3	3	3	3	4	3	4	4	4	4	5	4	5	5
6	3	3	4	3	4	4	4	4	5	4	5	5	5	5	6
7	3	4	4	4	4	5	4	5	5	5	5	6	5	6	6
8	4	4	5	4	5	5	5	5	6	5	6	6	6	6	7
9	4	5	5	5	5	6	5	6	6	6	6	7	7	7	7
10	5	5	6	5	6	6	6	6	6	6	7	7	7	7	7

CRAMM әдісі бойынша зерттеу жүргізудің тұжырымдамалық схемасы 7-суретте көрсетілген:



Сурет 7 – Зерттеу жүргізудің тұжырымдамалық схемасы

Әдебиетте осы әдістің артықшылығы жиі атап өтіледі, оларға ең алдымен бизнестің үздіксіздік жоспарын және ұйымның ақпараттық

қауіпсіздік саясатын әзірлеу үшін пайдалануға болатын тәуекелдің нақты бағалауын алу мүмкіндігі жатады. CRAMM технологиясын кәсіби қолдану ұйымның қауіпсіздік саясатын өзекті жағдайда қамтамасыз етуге және қолдауға арналған шығындарын (экономикалық) негіздеуге мүмкіндік береді.

CRAMM әдісінің кемшіліктері келесідей:

- сауалнамаға жауап берушілерден алынған тақ және лингвистикалық деректерді пайдаланудың мүмкін еместігі;
- жеке есептерді жасау және қолда бар есеп үлгілерін түрлендіру мүмкіндігінің болмауы;
- ақпараттық жүйенің сипаттамалары туралы толық ақпараттың көп санының қажеттілігі;
- қағаз есептік құжаттардың көп саны [11].

2.1.3 Riskwatch

Riskwatch американдық компаниясы әзірлеген RiskWatch бағдарламалық жасақтамасы тәуекелдерді талдау және басқарудың қуатты құралы болып табылады. RiskWatch тобына қауіпсіздік аудитінің әр түрлі түрлерін жүргізу үшін 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;
- HIPAAA – WATCH for Healthcare Industry-HIPAA стандартының талаптарына сәйкестігін бағалау үшін;
- RISKWATCH RW17799 for ISO17799 – ISO17799 стандартының талаптарын бағалау үшін.

RiskWatch әдістемесінде тәуекелдерді бағалау және басқару үшін өлшемдер ретінде «жылдық шығындарды болжау» (Annual Loss Expectancy – ALE) және «инвестициялардан қайтаруды» (Return on Investment – ROI) бағалау пайдаланылады. RiskWatch бағдарламалық өнімдерінің көптеген артықшылықтары бар. RiskWatch тәуекелдерге талдау жүргізуге және қорғау шаралары мен құралдарының негізделген таңдауын жасауға көмектеседі. Бағдарламада қолданылатын әдістеме 4 фазаны қамтиды:

Бірінші кезең – зерттеу пәнін анықтау. Бұл кезеңде ұйымның жалпы параметрлері: ұйымның типі, зерттелетін жүйенің құрамы, қауіпсіздік саласындағы базалық талаптар сипатталады. Сипаттама егжей-тегжейлі сипаттау немесе жіберіп алу үшін таңдауға болатын бірқатар тармақшаларда қалыптастырылады. Одан әрі таңдалған тармақтардың әрқайсысы толыққанды сипатталады. Талдаушының жұмысын жеңілдету үшін шаблондарда қорғалатын ресурстар, шығындар, қауіп-қатер, осалдықтар және қорғау шаралары санаттарының тізімі беріледі. Олардың ішінен ұйымда нақты барын таңдау керек.

Екінші кезең – жүйенің нақты сипаттамаларын сипаттайтын деректерді енгізу. Деректер қолмен енгізілуі немесе компьютерлік желілердің осалдығын зерттеудің құралдық құралдарымен жасалған есептерден импортталуы мүмкін. Бұл кезеңде инциденттердің ресурстары, шығындары мен сыныптары егжей-тегжейлі сипатталады. Инциденттер кластары шығындар санаты мен ресурстар санатын салыстыру жолымен алынады. Ықтимал осалдықтарды анықтау үшін база ресурстар категорияларымен байланысты 600-ден астам сұрақтан тұратын сауалнама пайдаланылады. Мәселелерді түзетуге, жаңаларын алып тастауға немесе қосуға жол беріледі. Әрбір бөлінген қауіптің туындау жиілігі, ресурстардың осалдық дәрежесі мен құндылығы қойылады. Осының барлығы бұдан әрі қорғаныс құралдарын енгізудің тиімділігін есептеу үшін қолданылады.

Үшінші кезең – тәуекелдерді бағалау. Алдымен алдыңғы кезеңдерде бөлінген ресурстар, шығындар, қатерлер мен осалдықтар арасында байланыс орнатылады.

Мысалы, егер сервердің құны $150 000, ал ол жыл ішінде өртпен жойылатын ықтималдығы 0.01 тең болса, онда күтілетін шығындар $1 500 құрайды. Қосымша «егер... » қорғау құралдарын енгізу жағдайында ұқсас жағдайларды сипаттауға мүмкіндік беретін. Қорғаныс шараларын енгізген жағдайда және оларсыз күтілетін шығындарды салыстыра отырып, осындай іс-шаралардың әсерін бағалауға болады.

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

Riskwatch кемшіліктеріне жатқызуға болады:

- мұндай әдіс, егер ұйымдастыру және әкімшілік факторларды ескермей, қорғаудың бағдарламалық-техникалық деңгейінде тәуекелдерге талдау жүргізу қажет болса, қолайлы. тәуекелдердің алынған бағалары (шығындарды математикалық күту) жүйелі позициялардан тәуекелді түсінуді жоққа шығармайды, әдіс ақпараттық қауіпсіздікке кешенді көзқарасты ескермейді;
- RiskWatch тек ағылшын тілінде бар;
- лицензияның жоғары құны – шағын компания үшін бір жұмыс орны үшін $15 000 және корпоративтік лицензия үшін $125 000 [11].

2.1.4 Falcongaze SecureTower

Falcongaze SecureTower – ыңғайлы DLP-шешім, ол арқылы ақпараттың таралып кетуіне қарсы күрес үшін көптеген іс-әрекеттер жасауға болады.

SecureTower 5.5 компанияны ішкі қатерлерден қорғауға арналған кешенді бағдарламалық шешім болып табылады, онда көптеген деректер

беру арналарын бақылау, құпия ақпараттың ағып кетуін болдырмау және жұмыс станцияларын пайдаланушылардың белсенділігін мониторингілеу үшін функциялардың кең жиынтығы іске асырылған.

Бұл өнім өрістету және пайдалану оңай, соның арқасында тек орта және ірі компанияларда ғана емес, шағын компанияларда да табысты пайдаланылуы мүмкін. Сонымен қатар, SecureTower 5.5 басқа да көптеген DLP-жүйелерден ерекшеленетін көптеген қызықты шешімдерді атап өтуге болады. 5.5 SecureTower 5.5 құпия ақпараттың жылыстауынан қорғау үшін кең функционалдан басқа, персоналдың желілік белсенділігін талдау және жұмыс уақытын бақылау үшін тиімді құралдар іске асырылды. Олардың ішінде: берілген мерзімділікпен немесе белсенді терезені ауыстырған кезде жұмыс үстелінің скриншоттарын автоматты түрде алып тастау; белсенді жұмыс уақыты мен компьютердің тоқтап тұру уақыты бойынша статистиканы жазу, түрлі қосымшаларды пайдалану; алмасу буферін бақылау; пернелерді басуды ұстап қалу; браузерлерде пайдаланушылардың белсенділігін қадағалау; персоналдың өзара байланысын интерактивті талдағыш; жұмыс станцияларының микрофондарынан нақты уақытта тыңдау және жазуды жүзеге асыру мүмкіндігі [12].

2.2 Ақпараттық қауіпсіздік құралдарын таңдаудың салыстырмалы талдауы

IT саласы күннен-күнге өте жылдам дамуда, тәуекелдерді талдаудың жаңа әдістері көбірек пайда болады. Нарықта көптеген талдағыштар мен функционалы шектеулі қарапайым антивирустар бар. Ақпараттық қауіпсіздікті бағалау және тәуекелдерді анықтау үшін көптеген әдістерді зерттей отырып, деректерді салыстырмалы талдау жасауға болады. Әрине, салыстыру үшін бізге бірдей өлшемдерді салыстыру қажет. Баға және ыңғайлылық (баптауда, сондай-ақ одан әрі модельдеуде, қауіптер тізілімін жаңартуда) сияқты аспектілер негізінде салыстырмалы талдау жүргізілді. Барлық әдістердің функционалы әртүрлі екенін атап өту керек, сондықтан келесі кестелерде негізгі сәттерді көрсетеміз(Кесте 10, 11, 12, 13, 14, 15, 16, 17, 18).

Кесте 10 – Баға бойынша салыстырмалы талдау

№	Бағдарламаның атауы	Нарықтағы лицензиялардың бағасы ($)	Танысу үшін күн саны
1	COBRA әдістемесі	895$ бастап	15 күндік нұсқа
2	CRAMM әдістемесі	1500$ - 2600$ бастап	демо-нұсқалар жоқ, тек презентация
3	Risk Watch	15,000$ - бір жұмыс орнына 125,000$ корпоративтік лицензияға	Таныстыру презентациясы бар, 2 ай бұрын алдын ала сұрау жасай отырып алуға болады
4	SecureTower 5.5	30,000$ компанияға	30 күндік нұсқа

Бұдан әрі әрбір бағдарламаның функционалы қарастырылады.

Кесте 11 – Функционалдың салыстырмалы талдауы

Пакет	CRAMM	COBRA	RISK Watch	Secure Tower
Жоғары лицензия құны	✓	✓	✓	✓
Тек ағылшын тілінде	-	✓	✓	-
Есептіліктегі ұсынымдар	✓	✓	-	✓
Компьютерге оңай орнату	-	✓	✓	✓

11-кестенің жалғасы

Қорытынды нәтиже есеп түрінде шығарылады	-	✓	✓	✓
ISO 2700117779 стандарты негізінде	✓	✓	✓	-
Тәуекелдер базасын автоматты түрде жаңарту	-	-	✓	✓

Кесте 12 – Бағдарламаның артықшылық/кемшіліктерін салыстырмалы талдау

Атауы	Артықшылығы/ерекшелігі	Кемшіліктері
COBRA әдістемесі	Кең функционал, тәуекелдер тізілімі үнемі жаңартылып отырады;	Тек ағылшын тілінде бар;
CRAMM әдістемесі	Тәуекелді талдау мен бағалауға қатаң көзқарас, қауіпсіздіктің техникалық және техникалық емес сипаттағы емес аспектілерді қамтиды;	Аудит – процесс жеткілікті еңбекті қажет ететін және аудитордың үздіксіз жұмыс істеу айларын талап етуі мүмкін;
Risk Watch	Қандай қауіп-қатерлер және қандай мерзімділікпен болып жататыны сипатталады; Ресурстың құнын ескере отырып күтілетін шығындарды бағалау жүзеге асырылады;	Мұндай әдіс, егер ұйымдық, әкімшілік факторларды ескермей, қорғаудың бағдарламалық – техникалық деңгейінде тәуекелдерге талдау жүргізу талап етілсе қолайлы;
SecureTower	Трафикті ұстау және өңдеу бойынша кең функционалдық мүмкіндіктер, орыс тілінде және ағылшын тілінде де бар;	Контенттік талдаудың кейбір перспективалық технологияларының болмауы.

Кесте 13 – АҚ тәуекелдерін басқаруға арналған бағдарламалық құралдарды салыстыру (тәуекелдер)

Салыстыру критерийлері	CRAMM	Cobra	RiskWatch	Falgongaze SecureTower
Тәуекелдер санаттарын пайдалану	+	+	+	+
Ең жоғары рұқсат етілетін тәуекел ұғымын пайдалану	+	+	+	+
Тәуекелдерді төмендету бойынша іс-шаралар жоспарын дайындау	+	+	+	+

Кесте 14 – АҚ тәуекелдерін басқаруға арналған бағдарламалық құралдарды салыстыру (басқару)

Салыстыру критерийлері	CRAMM	Cobra	RiskWatch	Falgongaze SecureTower
Басшыны хабардар ету	+	+	+	+
Тәуекелдерді төмендету бойынша жұмыс жоспары	-	+	+	+
Тренингтерді, семинарларды, жиналыстарды өткізуді қамтиды	-	+	+	+
Бизнес/операциялық /АТ-тәуекелдерді бағалау	-	+	+	-
Тәуекелдерді ұйымдастыру деңгейінде бағалау	+	+	-	+
Тәуекелдерді техникалық деңгейде бағалау	+	+	+	+

Кесте 15 – АҚ тәуекелдерін басқаруға арналған бағдарламалық құралдарды салыстыру (тәуекел шамасын өлшеу тәсілдері)

Салыстыру критерийлері	CRAMM	Cobra	RiskWatch	Falgongaze SecureTower
Сапалық бағалау	+	+	+	+
Сандық бағалау	-	+	+	+

Кесте 16 – АҚ тәуекелдерін басқаруға арналған бағдарламалық құралдарды салыстыру (тәуекелдерді төмендетудің ұсынылатын тәсілдері)

Салыстыру критерийлері	CRAMM	Cobra	RiskWatch	Falgongaze SecureTower
Тәуекелді айналып өту тәсілі (алып тастау)	+	+	+	-
Тәуекелдерді төмендету	+	+	+	+
Тәуекелдерді қабылдау	-	+	-	+
Материалдық активтер	-	+	+	-
Материалдық емес активтер	+	+	-	+
Қауіп – қатерлер	+	+	+	+
Активтердің құндылығы	+	+	+	+
Осалдықтар	+	+	+	+
Қауіпсіздік шаралары	+	+	+	+
Әлеуетті залал	+	+	+	+
Қауіптерді іске асыру ықтималдығы	+	+	+	+

Кесте 17 – АҚ тәуекелдерін басқаруға арналған бағдарламалық құралдарды салыстыру (қарастырылатын тәуекелдер түрлері)

Салыстыру критерийлері	CRAMM	Cobra	RiskWatch	Falgongaze SecureTower
Бизнес тәуекелдер	-	+	+	-
Заңнамалық актілерді бұзуға байланысты тәуекелдер	-	+	-	+

17-кестенің жалғасы

Технологияларды пайдаланумен байланысты тәуекелдер	-	+	-	+
Коммерциялық тәуекелдер	+	+	+	+
Үшінші тұлғаларды тартуға байланысты тәуекелдердің түрлері	+	+	+	+
Қызметкерлерді тартуға байланысты тәуекелдер	+	+	-	+
Тәуекелдерді қайта бағалау	-	+	-	+
Тәуекелдерді қабылдау қағидаларын айқындау	-	+	-	+

Кесте 18 – АҚ тәуекелдерін басқаруға арналған бағдарламалық құралдарды салыстыру (басқару тәсілдері)

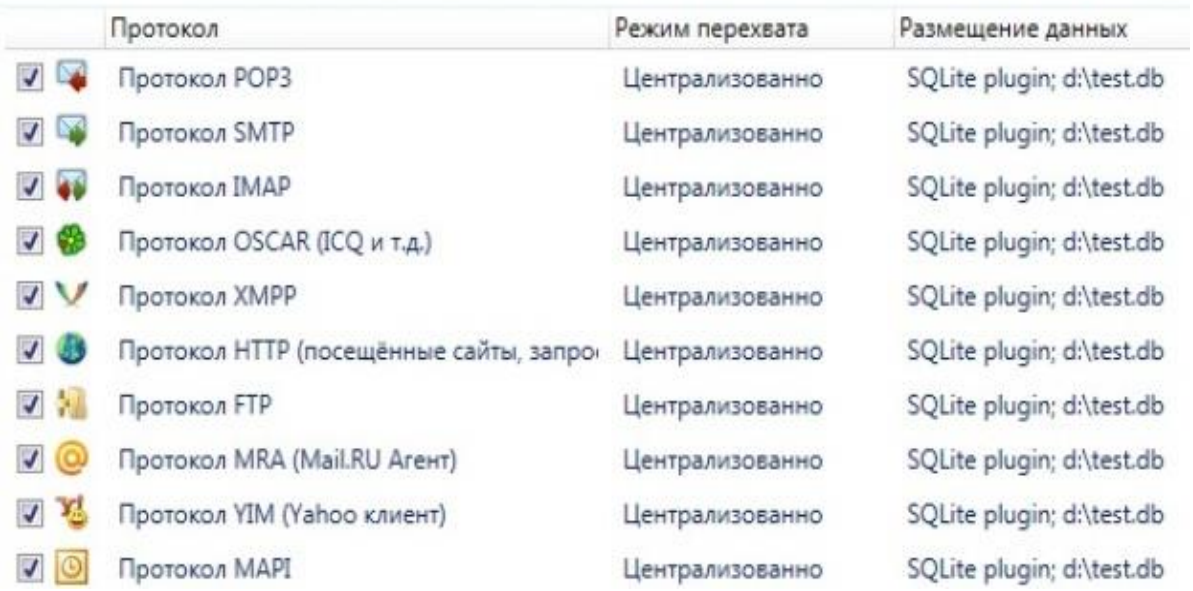
Салыстыру критерийлері	CRAMM	Cobra	RiskWatch	Falgongaze SecureTower
Тәуекелдерді сапалық түрде саралау	+	+	+	+
Тәуекелдерді сандық түрде саралау	-	+	+	+
Тәуелсіз бағалауды пайдалану	-	+	-	+
Инвестицияларды қайтару есебі	-	+	-	-

2.3 Кәсіпорынның ақпараттық қауіпсіздік тәуекелдерін төмендету және алдын алуды жобалау

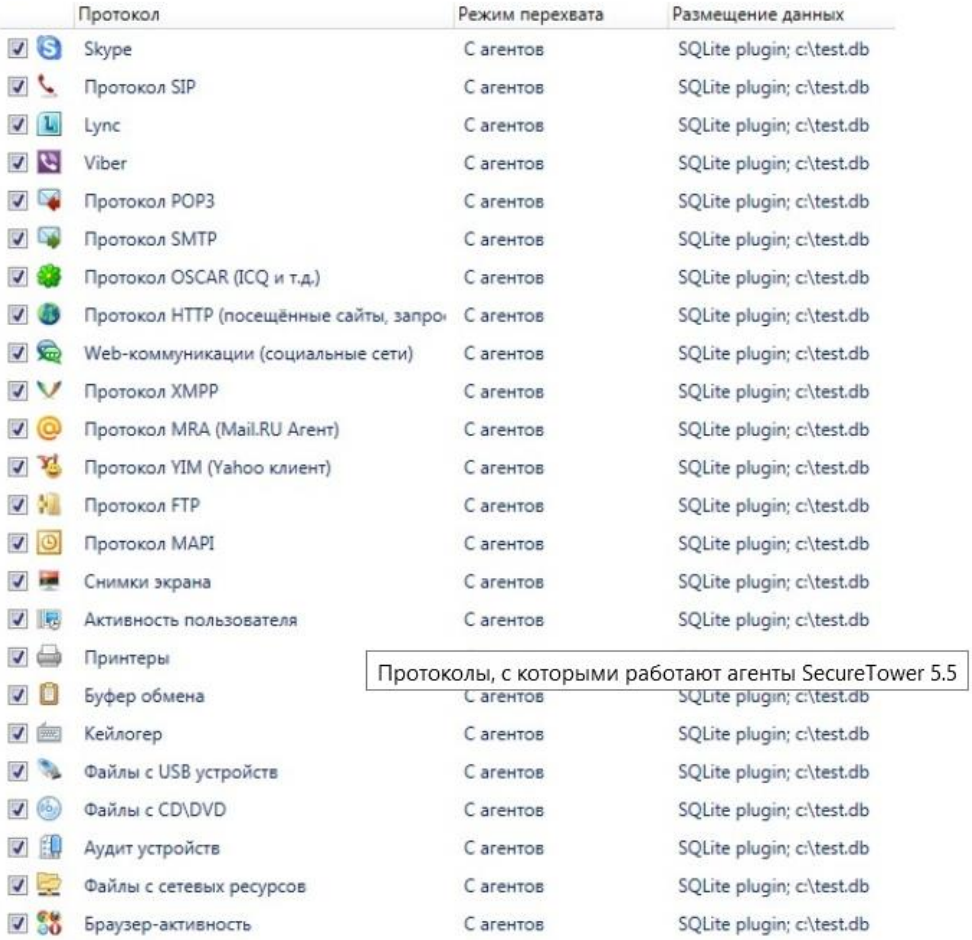
Салыстырмалы талдау негізінде, Falcongaze SecureTower 5.5 бағдарламалық өнімі тиімдірек деген негізде таңдалды.

DLP-жүйелерді қолдану құпия ақпараттың саны үлкен, ал ағу салдарынан мүмкін болатын қаржылық және беделдік шығындар ұйымның толық бұзылуына әкелуі немесе оның тапсырыс берушілеріне, серіктестеріне немесе клиенттеріне зиян келтіруі мүмкін ұйымдар үшін аса өзекті болып табылады. DLP-жүйелерді қолдану аймағы бұрыннан бері тек деректердің ағуын болдырмау үшін қолданылатын. Қазіргі заманғы жүйелер әртүрлі байланыс арналары бойынша ақпаратты беруді бұғаттауға, перифериялық құрылғыларға көшіруге, қызметкерлердің жұмысы туралы ақпаратты жинауды жүзеге асыруға және т.б. мүмкіндік береді. Қазіргі DLP-жүйелер банк саласында, энергетикада, мемлекеттік секторда, өнеркәсіптік компанияларда, ғылыми-зерттеу орталықтарында және т. б. қолданылады. Сондай-ақ, олар құпия ақпаратты бақылау міндеттерін ғана емес, экономикалық қауіпсіздік міндеттерін де шешеді, оқыс оқиғаларды тексеруге ықпал етеді, оның ішінде персонал жұмысының тиімділігін бағалау үшін пайдаланылады.

Үйреншікті арналардан басқа, DLP-жүйелерімен бұлтты қоймалар (Google Drive, Apple iCloud, Cloud Mail.Ru, Яндекс.Диск), танымал Skype, Telegram, Viber, WhatsApp мессенджерлері, сондай-ақ кейбір жүйелер қызметкерлердің ұялы компьютерлерін, смартфондары мен планшеттерін бақылауға мүмкіндік береді. Сонымен қатар, осы бағдарламаның көмегімен қызметкерлердің жұмыс үстелдерінің скриншоттарын қадағалауға және жасауға, олардың жұмыс орындарында жұмыс істеу барысындағы тарихын көруге, алмасу буферінен деректерді ұстап тұруға, қызметкердің пернетақтада тергенін жазуға, браузерлерде белсенділікті бақылауға болады. Ал Falcongaze SecureTower нақты қосымшаларда қанша қызметкер отырғандығын анықтай алады. Мүмкін бұл құпия ақпаратты қорғауға нақты қатысы жоқ шығар, бірақ соған қарамастан, компания басшылары үшін өте пайдалы. Secure Tower деректерді қауіп-қатерден қорғай алады және де компания қызметкерлерінің пайдалылық коэффициентін арттыруға мүмкіндік береді. DLP-жүйенің басты функцияларының бірі ішкі қатерлерге қарсы тұру болып табылады. Бағдарламаның жұмыс жасау принципін қарастырсақ (Сурет 8, 9).



Сурет 8 – Бақылауға болатын хаттамалар тізімі



Сурет 9 – SecureTower 5.5 жұмыс істейтін хаттамалар

SecureTower 5.5 серверлік бөлігіне бірнеше компоненттер кіреді, олар туралы бөлек айту керек (Кесте 19).

Кесте 19 – Серверлік бөліктің компоненттері

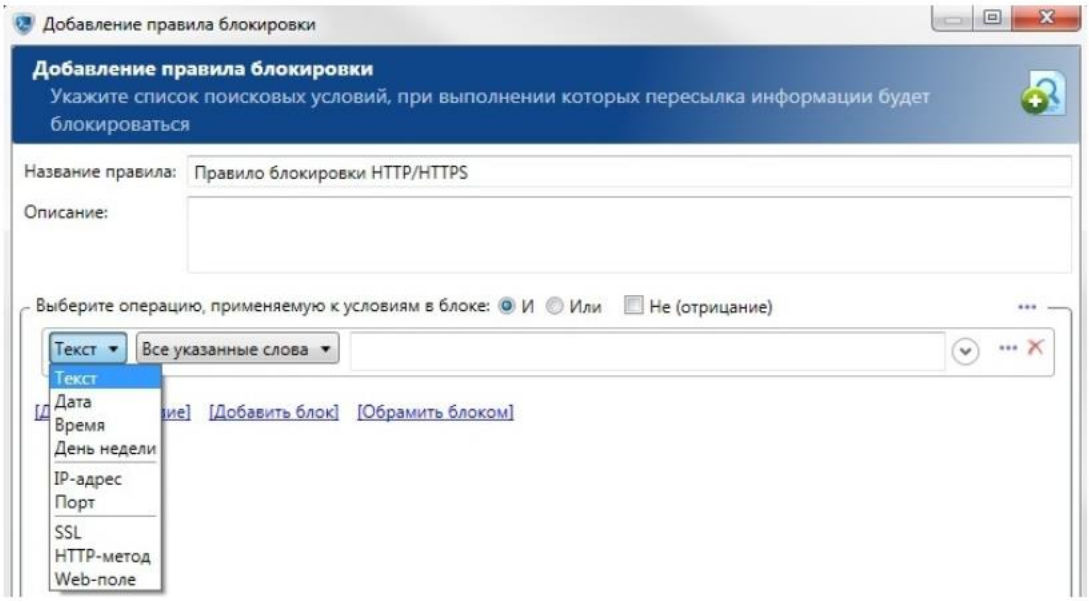
Орталықтандырылған ұстап қалу қызметі –	шлюздік шешімді білдіретін және Интернетке шығу алдында тұрған коммутатордың айналау портынан (span-портынан) алынатын трафикті алу және бастапқы өңдеу үшін жауап беретін компонент. Бұл желі периметрінен тыс барлық трафикті бақылауға мүмкіндік береді.
Оқиғалар мен хабарламалар сервисі –	орталықтандырылған ұстап қалу сервисінің жұмысындағы барлық оқиғаларды тіркейді және қажет болған жағдайда, маңызды оқиға немесе іркіліс болған жағдайда жүйе әкімшісіне хабарлама жібереді.
Агенттерді бақылау сервисі –	қызметкерлердің жұмыс станцияларына инсталляцияланатын агенттермен жұмыс істеу үшін қолданылады. Оларды орталықтандырып басқаруға мүмкіндік береді: агенттерді орнату/жою, параметрлер профильдерін жасау/өзгерту, байланыс ақпаратын пайдаланушы карточкаларына енгізу. Агенттерді пайдалану, ұстап алудың орталықтандырылған тәсіліне қарағанда, шифрланған арналар (Skype, SSL) бойынша берілетін ақпаратты ұстап тұруға мүмкіндік береді, сондай-ақ қызметкерлердің белсенділігін бақылау, алмасу буферіне көшірілетін ақпаратты ұстап қалу, басып шығаруға жіберілетін құжаттарды ұстап қалу, пернетақтадағы барлық басуларды тіркеу, қосылатын құрылғыларды бақылау және т.б. сияқты бірқатар қосымша мүмкіндіктер береді.
Поштаны өңдеу қызметі –	корпоративтік пошта сервері арқылы өтетін пошта хабарламаларын ұстап алуға арналған компонент. Microsoft ES, Lotus Domino сияқты корпоративтік стандарттардан бастап, Linux және Unix платформаларында шешімдерге дейін пошта серверлерінің кең ауқымымен жұмыс істеуге қолдау көрсетіледі.
Деректерді өңдеу қызметі –	бұл компонент бірқатар міндеттерді шешу үшін қажет: SecureTower басқа компоненттері үшін лицензиялау, ұсталған деректерді индекстеу, құжаттардың сандық таңбаларымен жұмыс істеу, іздеу операцияларын жүзеге асыру және т.б. жүзеге асыру үшін қажет.

19-кестенің жалғасы

ICAP сервері –	ICAP протоколын қолдайтын прокси – серверлерден HTTP/HTTPS трафигін алады. Бұл трафикті ұстап қана қоймай, құпия ақпаратқа желі периметрінен кетуге мүмкіндік бермейтін бұғаттау ережелерін жасауға мүмкіндік беріледі. SecureTower – де мазмұнды тек сыртқы атрибуттары бойынша ғана емес, пайдаланушы аты, IP мекенжайы, күні немесе уақыты сияқты блоктауға мүмкіндік беретін зияткерлік бұғаттау механизмі іске асырылған. Қазіргі уақытта келесі прокси-серверлермен жұмыс істеу ұсынылады: SQUID, TMG және Blue Coat

2.3.1 Falcongaze SecureTower 5.5 функционалдық мүмкіндіктері

Falcongaze SecureTower бағдарламасында трафикті ұстап қалу және оны құлыптау функциясы бар. Егер ол корпоративтік қауіпсіздік саясатын бұзса ғана трафик қолданбасын бұғаттау мүмкін. Блоктау функционалы ICAP серверінде іске асырылған. Блоктау параметрлері өте көп, 10-суретте толық тізім көрсетілген. Бірнеше топтарды таңдап, бір уақытта қолдануға болады.

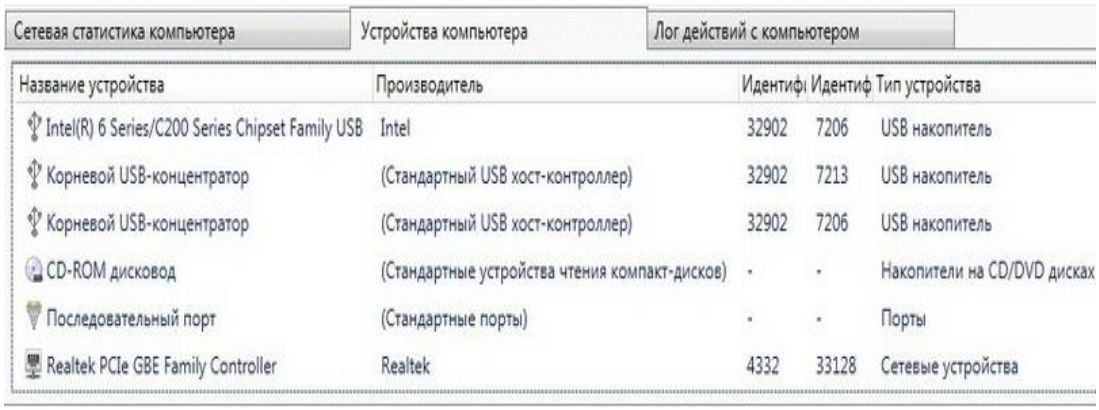


Сурет 10 – SecureTower-де трафикті бұғаттау шарттарының тізімі

ICAP сервері HTTP және HTTPS протоколдары бойынша бұғаттауды қоя алады. Сондай-ақ, бағдарлама көмегімен Компьютер құрылғыларына, USB қосылымына және желілік ресурстарға қосылу мүмкіндігін шектеуге болады. Мұндай трафикті бұғаттау арқылы құпия ақпаратты пошта арқылы жіберумен байланысты мәселені шешуге, қызметкерлердің қажетсіз сайттарға баруын және USB құрылғысын пайдалануды шектеуге болады.

Әзірлеушілер жалпы, шығыс және кіріс электрондық пошта бақылауын бағдарламалады. Бұл мәселені шешу үшін пошта протоколдары (POP3, SMTP, IMAP, MAPI) бойынша Берілетін трафик мониторингі ғана емес, сонымен қатар корпоративтік пошта серверлерімен интеграциялау де қолданылады. Сонымен қатар, бұл желі периметрінен тыс сыртқы трафикті бақылауды қамтамасыз етіп қана қоймай, қызметкерлердің ішкі хат-хабар алмасуын қадағалауға мүмкіндік береді. Сондай-ақ, S/MIME стандарты бойынша қорғалған электрондық поштамен жұмыс істеуге қолдау көрсетіледі.

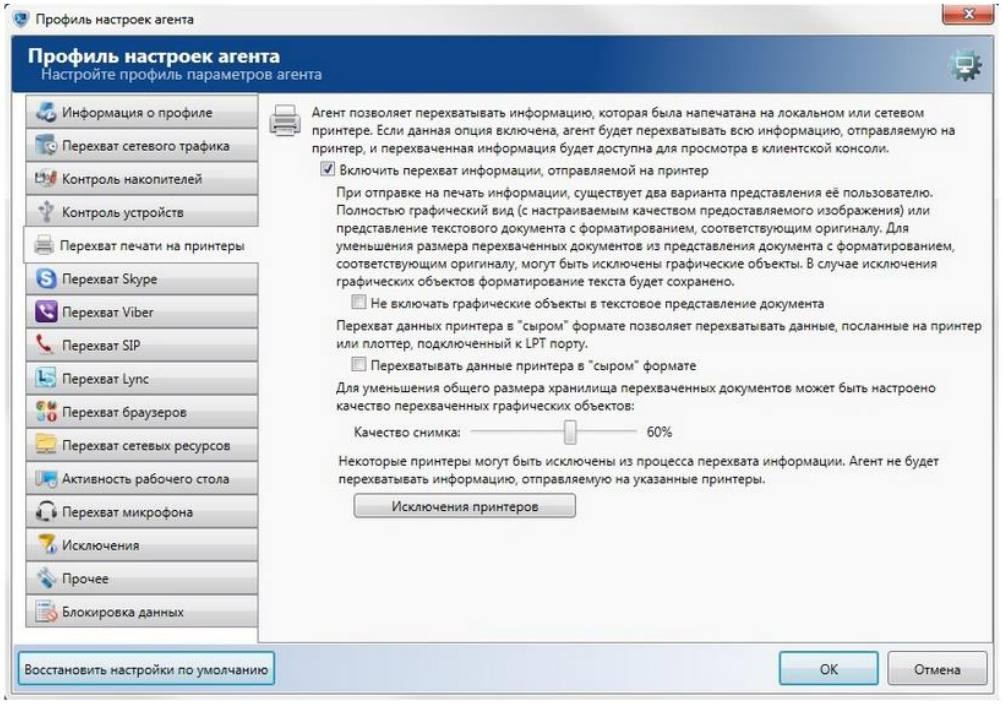
SecureTower-де ақпараттың таралып кетуінің жергілікті арналарын бақылау бұрын болған сияқты тек USB-жинақтағыштарды ғана емес, сондай-ақ ішкі интерфейстер бойынша компьютерге қосылған құрылғыларды да қамтитын құрылғыларды бақылауға арналған құрал іске асырылды (Сурет 11). Бұл ретте жүйе құрылғы түрін (USB жинақтағыш, порт, желілік құрылғы және т.б.) автоматты түрде анықтайды.



Сурет 11 – Желілік статистика

2.3.2 Құжаттарды басып шығаруды бақылау

Бағдарлама жергілікті және желілік принтерлерде кім және не басып шығарғанын бақылауға мүмкіндік береді. Бұл бағдарламаның үлкен артықшылығы оқиға туралы стандартты деректер ғана емес (уақыт, пайдаланушы, принтер және т.б.) жазылады, сонымен қатар осы басып шығарылған құжаттардың көшірмелері сақталады. Егер баптауға кірсеңіз, баспаға жіберілетін файл берілетін сапаны баптауға болады. Бақылау қажет емес принтерлер бар болса, мысалы бастықтың принтері, оны ерекше тізімге енгізуге болады (Сурет 12).



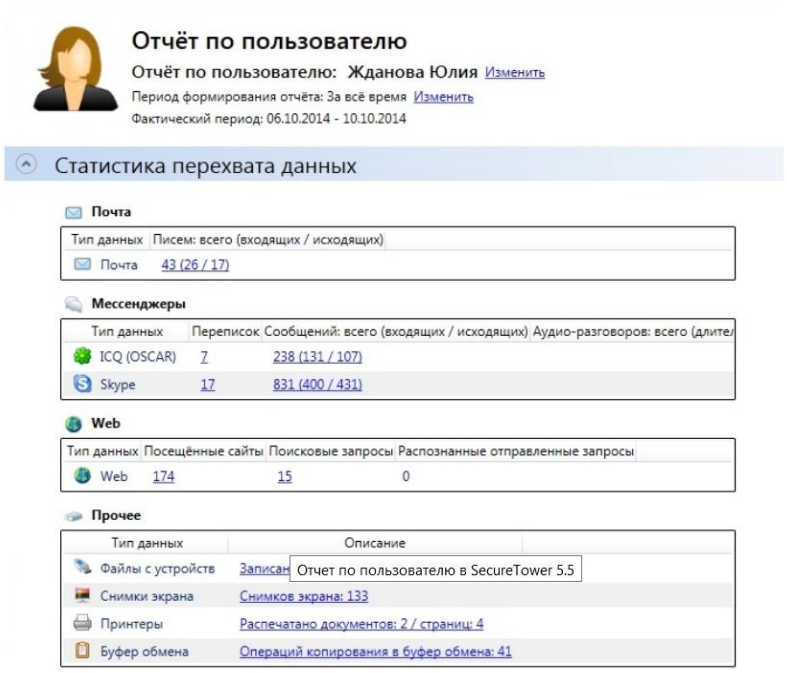
Сурет 12 – Басып шығарылған құжаттарды ұстап қалу параметрлері

Қарастырылып отырған бағдарламада қызметкерлердің жұмыс орнында белсенділігін бақылауға мүмкіндік беретін жаңа құралдарды іске асыру бар. Оларға жатады:

- жұмыс үстелінің скриншоттарын уақытында жасау;
- монитордың белсенді жұмыс уақыты бойынша жазу;
- нақты қосымшаларда пайдаланушылардың белсенді жұмыс уақытын бақылау;
- айырбастағышты бақылау;
- кейлоггер;
- браузерлерде пайдаланушының белсенділігін қадағалау.

SecureTower 5.5 басқалардан айырмашылығы – қызметкерлердің желілік белсенділігінің толық көрінісін бере алатын статистикалық есептердің көп саны. Есептер интерактивті түрде ұсынылған. Есептің 3 түрі бар: топ-есептер, пайдаланушы бойынша есептер және қауіпсіздік орталығы бойынша есеп. Топ-есептер – бұл барлық белсенді қызметкерлерді көрсететін есеп (Сурет 14, 15). Мысалы, жіберілген смс саны бойынша топ-есеп чаттарда белсенді түрде жазылатын қызметкерлердің аттарын бірден білуге мүмкіндік береді (Сурет 13).

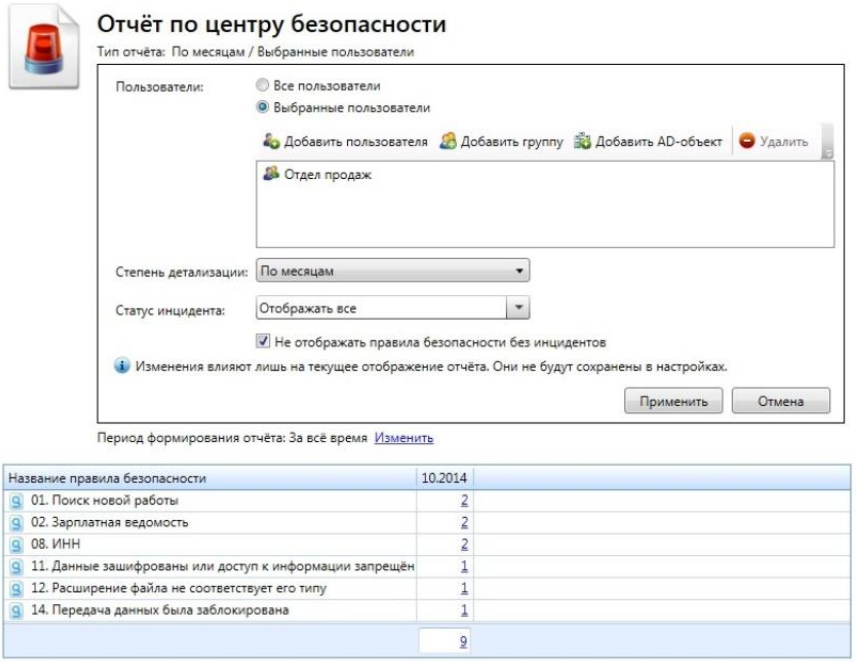
Сурет 13 – Пайдаланушы бойынша есеп көрсетілген уақыт кезеңінде нақты қызметкер бойынша толық есепті білдіреді.



Сурет 14 – Пайдаланушы жайлы есеп

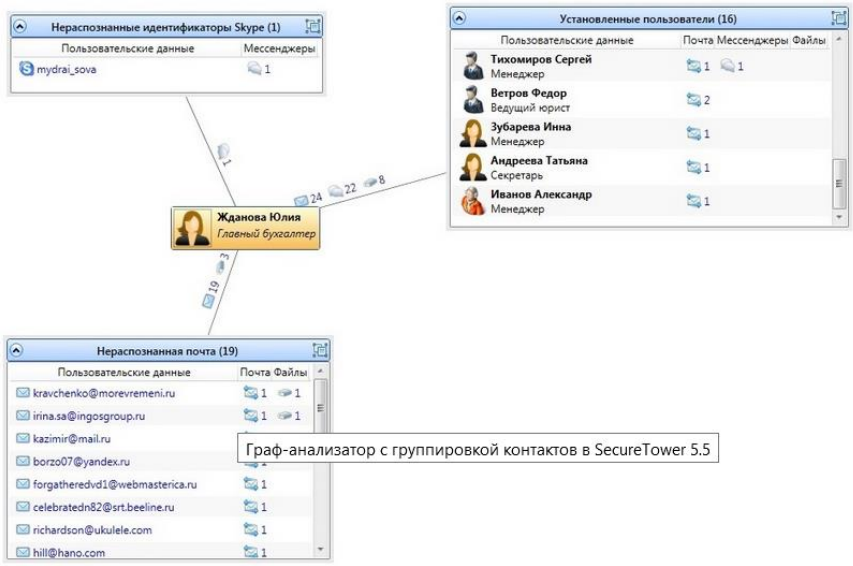
Сурет 15 – Пайдаланушының белсенділік есебі

Қауіпсіздікті қамтамасыз ету орталығы бойынша есеп барлық ережелерді атап өтуге және белгілі бір уақыт аралығында қауіпсіздікті қамтамасыз ету орталығында бір пайдаланушы бойынша іске қосылу санын білдіреді (Сурет 16). Қажет болған жағдайда қауіпсіздік ережесі жұмыс істеген нақты құжатқа көшуге болады, сонымен қатар бір пайдаланушыға емес, тұтас топ бойынша есеп құру мүмкіндігі бар.

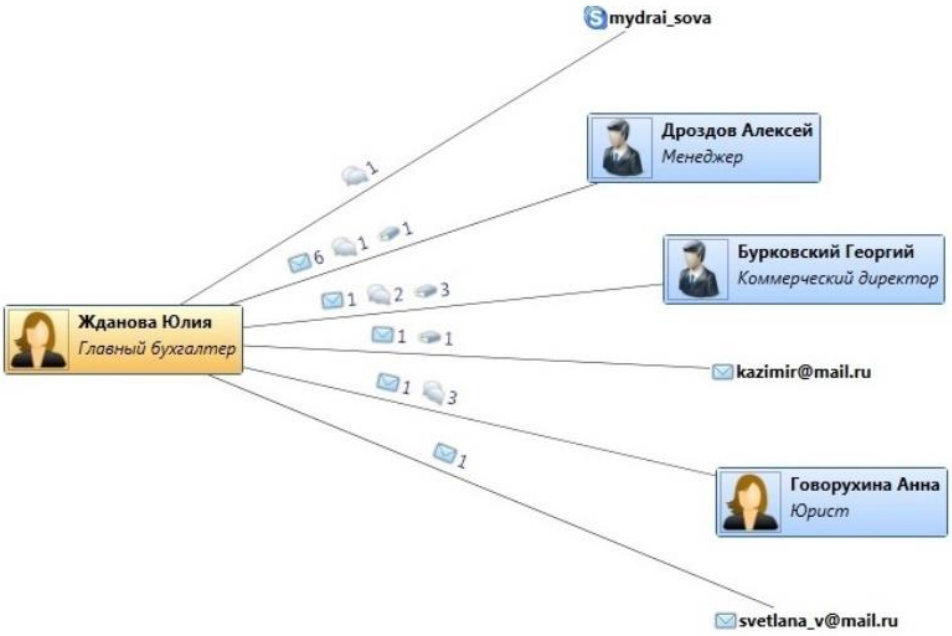


Сурет 16 – Пайдаланушылар тобына арналған қауіпсіздікті қамтамасыз ету орталығы бойынша есеп

Баған талдауыш басшылыққа көрнекі түрде қызметкерлердің бірінің ішкі және сыртқы контактілермен қарым-қатынасының барлық шеңберін көруге көмектеседі, бұл функцияны күдікті байланыстарды анықтау үшін пайдалануға болады (Сурет 17, 18).

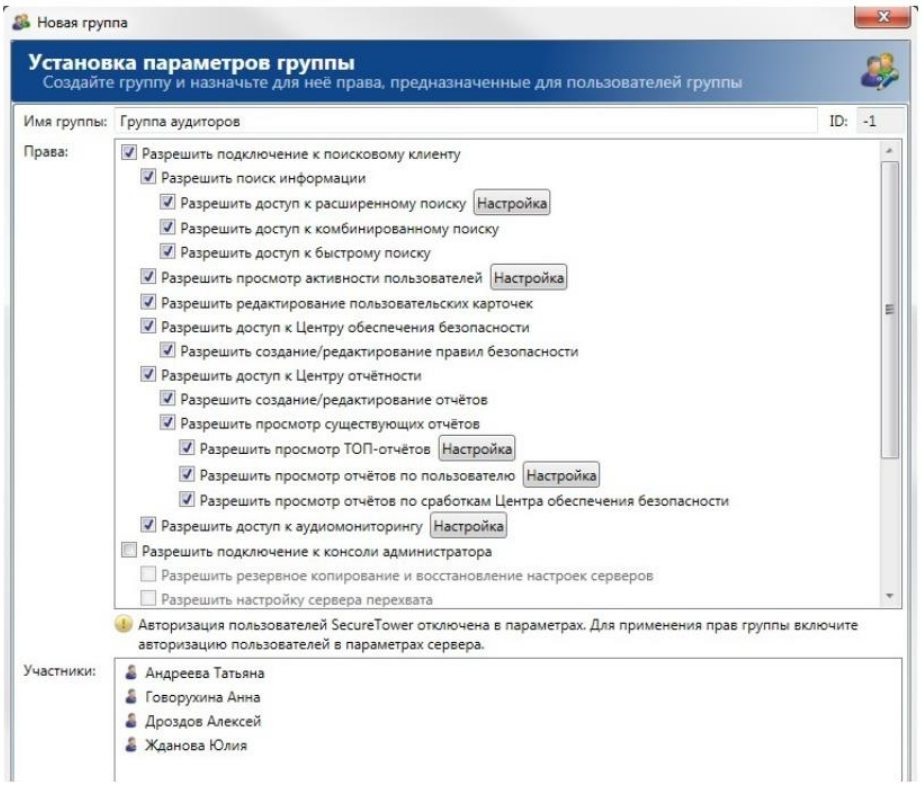


Сурет 17 – Контактілерді топтайтын баған талдағышы



Сурет 18 – Баған талдағышының кеңейтілген түрі

SecureTower 5.5-те SecureTower компоненттеріне қол жеткізу құқықтарын шектеудің икемді жүйесі іске асырылған (Сурет 19).

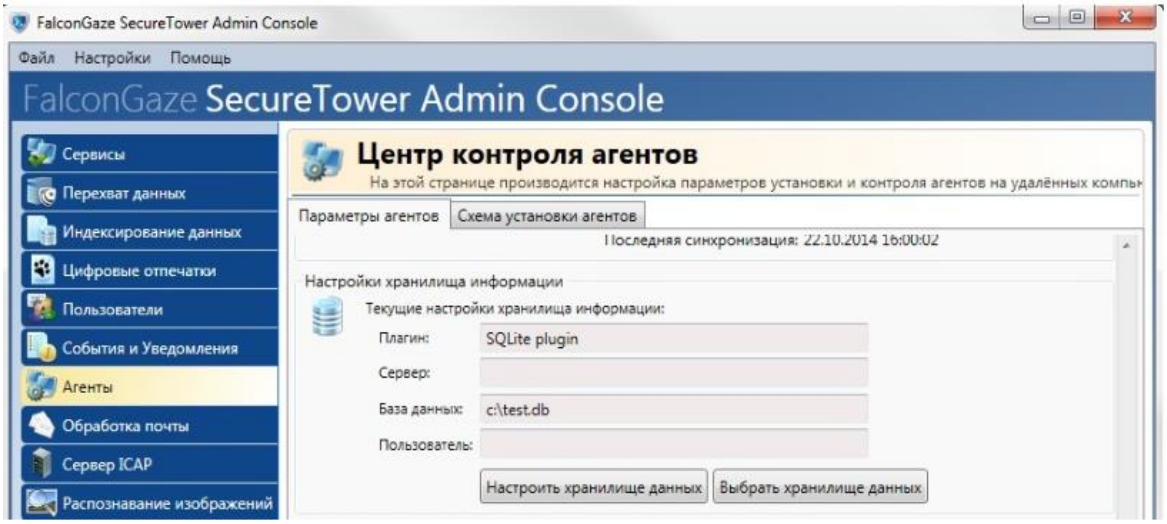


Сурет 19 – Жеке аудиторлар тобы үшін SecureTower 5.5 компоненттеріне қол жеткізу құқығын таңдау

SecureTower сервистеріне ғана емес, сонымен қатар олардың жеке құрамдас бөліктеріне де қол жеткізу құқығын беру мүмкіндігі қарастырылған. Мысалы, бөлім бастықтарына тек бөлім қызметкерлерін бақылау мүмкіндігін ұсынуға болады.

SecureTower 5.5 тарату процесі осы бапта бұрын көрсетілген жүйелік талаптарға сәйкес келетін компьютер немесе серверді таңдаудан басталады. Бірінші танысу кезінде DLP жүйесінің барлық компоненттері бір серверге орнатылады.5.5 SecureTower-мен танысу процесін агенттерді бақылау сервисінен бастау керек, өйткені осы сервистің көмегімен ақпаратты ұстап қалу әдісі тек күйге келтіруде қарапайым ғана емес, сонымен қатар трафикті бақылау бойынша, оның ішінде шифрланған, сондай-ақ компания қызметкерлерінің жұмыс уақытын пайдалануын мониторингілеу үшін (басып шығару, экранды түсіру, алмасу буферін бақылау және т.б.) ең кең мүмкіндіктер береді. Агенттерді бақылау сервисіне әкімшінің консоліне «агенттер» қойындысы жауап береді. «Ақпарат қоймасын баптау» бөлімінде агенттердің барлық ұстап қалған ақпаратты жинайтын деректер базасын көрсету керек. Қолдау көрсетілетін деректер қорының тізімі өте үлкен және қамтиды: SQLite, Microsoft SQL Server, MySQL, PostgreSQL және Oracle DB.Үшінші тарап деректер базасын өрістетуге қосымша уақыт жұмсамау үшін, тестілеу кезінде SecureTower ішіне енгізілген SQLite деректер базасын пайдалануға болады. Деректер қоры, оның аты мен

кеңейтімі сақталатын жолды көрсету жеткілікті .db (Сурет 20). SecureTower барлық қалған жұмысын өз бетінше жасайды.



Сурет 20 – SecureTower 5.5 SQLite деректер базасын баптау

Келесі қадам ағымдағы деректер қоры бойынша индексті жасау болады, өйткені, ұсталған деректерді клиенттік консольде көруге болады, оларды алдымен индекстеу қажет. Ол үшін Әкімші консоліне «деректерді индекстеу» қойындысына өтіп, онда индекс жасау керек. Деректер көзі ретінде «SecureTower серверінен» тармағын таңдау ұсынылады, себебі бұл жағдайда DLP-жүйе қазіргі уақытта SecureTower сервистері үшін бапталған барлық деректер базасын өзі табады. Балама шешім ретінде «SecureTower деректер базасынан» тармағын таңдауға болады. Бұл жағдайда деректер қорының орналасқан жерін көрсету керек.

Әдепкі бойынша индекс автоматты түрде әр 30 минут сайын жаңартылады, бірақ бұл кестені индекс сипаттарында оңай өзгертуге болады. Индексті қолмен жаңарту мүмкіндігі де қарастырылған.Жұмыс станцияларына агенттер орнату үшін осы компьютерлерде әкімші құқығы бар тіркелгі болуы керек. Осы есептік жазбаның атынан әкімші консолінде «сервистер» қойындысынан табуға болатын агенттерді бақылау қызметін іске қосу керек. Осыдан кейін агенттерді тікелей орнатуға кірісуге болады. Таңдауда агенттерді орнатудың екі стратегиясы бар: тек көрсетілген компьютерлерге орнату немесе барлық компьютерлерге орнату.

2.3.3 Falcongaze SecureTower 5.5 бағдарламасымен жұмыс жасау

Ақпараттық қауіпсіздік бөлімі қызметкерлерінің жұмысы клиенттік консольдің көмегімен жүзеге асырылады.Клиенттік консоль алты бөлімнен тұрады: «пайдаланушылардың белсенділігі», «ақпаратты іздеу», «аралас іздеу», «қауіпсіздікті қамтамасыз ету орталығы», «есептілік орталығы» және «Аудиомониторинг». Алғашқы үшеуі жиналған SecureTower 5.5 ақпаратты қарау үшін пайдаланылады, төртіншісі қауіпсіздік ережелерін күйге келтіруге арналған, бесінші – пайдаланушылар бойынша есептерді

құру және қарау үшін, ал соңғысы – бақыланатын жұмыс станцияларының микрофондарынан аудио ағындарын бақылау жолымен сөйлесу сөздерінде құпия ақпаратты тарату оқиғаларын мониторингілеу үшін.

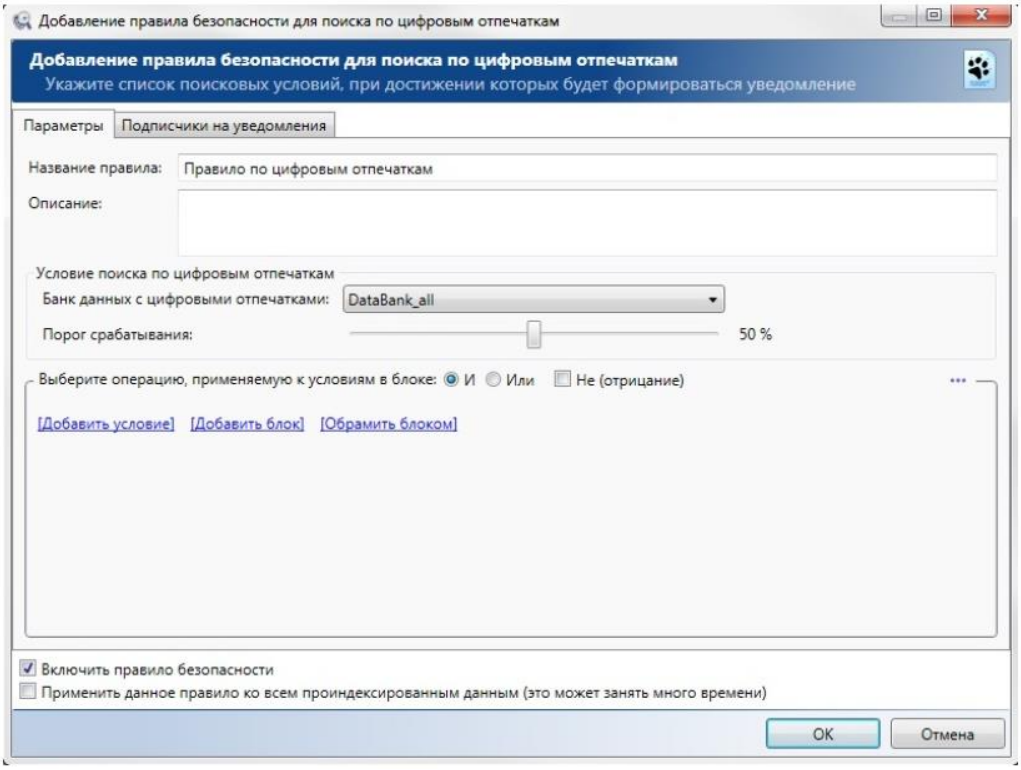
Бірінші кезекте «қауіпсіздікті қамтамасыз ету орталығын» қарастырайық. Бұл модульдің мәні қарапайым: қауіпсіздік әкімшісі ақпаратты талдау үшін ерікті ережелер санын қалыптастырады. SecureTower 5.5 барлық ұстап қалған деректерді өңдейді және осы ережелердің кез келгені іске қосылған кезде жауапты қызметкерге хабарлама жібереді. Бұл ақпараттық қауіпсіздіктің корпоративтік саясатын бұзуға жедел реакцияны қамтамасыз етеді. Әрбір ережеге (немесе олардың тұтас тобына) жазылушылар (хабарлама алатын жауапты қызметкерлер) бірнеше болуы мүмкін.Ыңғайлы болу үшін ережелер кез келген дәрежедегі иерархиялық құрылымдарды құруға болатын топтарға біріктірілуі мүмкін. Ереже ақпаратты талдаудың үш негізгі түрі болып табылады: контентті, оқиғалы және статистикалық, олар жүйеде ережелердің келесі түрлерімен ұсынылған.

2.3.4 SecureTower 5.5 қауіпсіздік орталығының іздеу ережесі

Біріншісі әдеттегі ереже болып табылады. Олар негізгі сөздер, тұрақты өрнектер (үлгілер) және атрибуттар бойынша трафикті контекстік талдау үшін пайдаланылады. Бұл ережелер құрамды болуы мүмкін, яғни логикалық операциялармен біріктірілген жағдайлардың көп санынан «және», «немесе», «емес» болуы мүмкін. Мұндай ережелер ақпараттың таралуын мониторингілеу үшін ғана емес, сонымен қатар адал емес қызметкерлерді анықтау үшін де қолданылуы мүмкін. Мысалы, Интернетте жаңа жұмыс іздейтіндер.

Сөздік бойынша іздеу ережелері бір немесе бірнеше берілген сөздер бойынша емес, тұтас сөздікте іздестіруді жүзеге асыруға мүмкіндік береді, бұл жіберілетін құжаттың тақырыбын анықтауға және оны, мысалы, бухгалтерлік немесе қаржылық санатқа жатқызудың дәлдік дәрежесімен мүмкіндік береді. Бұл ретте, ережені өзгертіп, «сезімталдықты» таңдауға болатын іске қосу шегі (мәтінде болуы тиіс сөздіктің пайызы) белгіленеді.

Ережелердің үшінші түрі алдын ала анықталған құпия құжаттардың немесе деректер қорының мазмұнын жіберу фактілерін анықтауға мүмкіндік беретін, сандық таңбалар бойынша іздеу ережелері. Ол үшін сандық таңбалар технологиясы қолданылады. Бұл ретте, жіберілетін құжаттың немесе деректер қоры мазмұнының жүйеге енгізілген құжаттардың сандық кескіндерімен ұқсастығы пайызын дербес белгілеуге болады (Сурет 21).

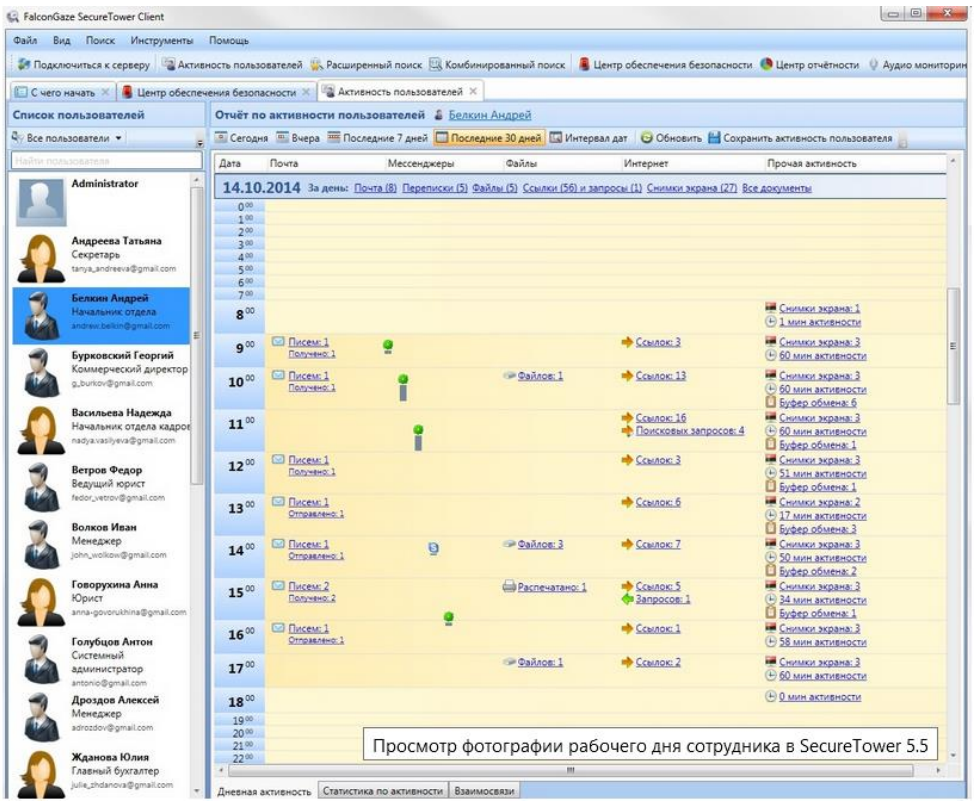


Сурет 21 – SecureTower 5.5 қауіпсіздік орталығының сандық іздері бойынша ереже

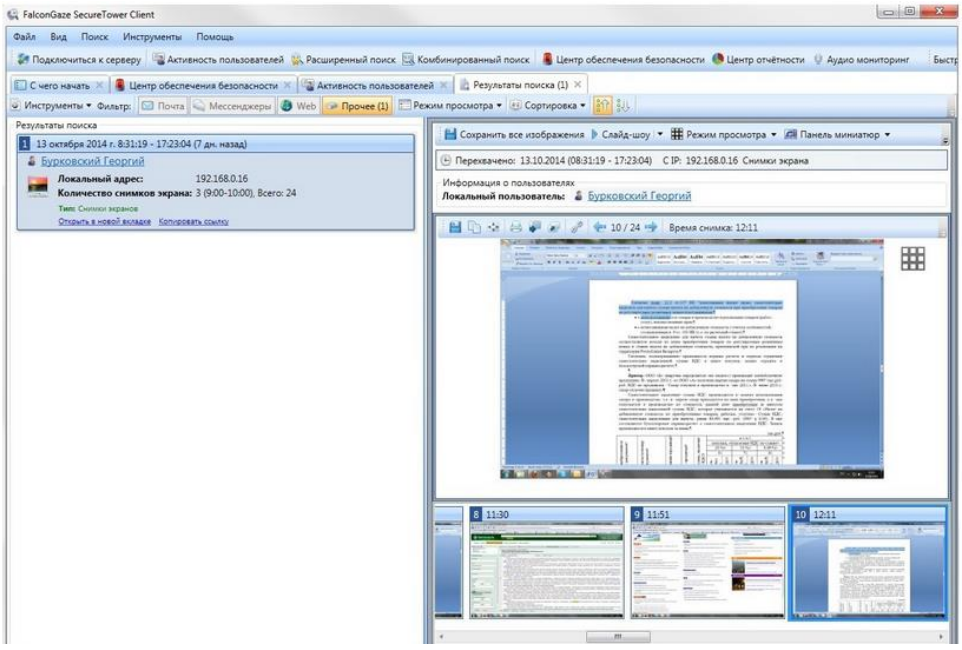
Қажет болса, жүйе жіберген ережелердің іске қосылуы туралы ескертулерді жылдам қарауға болады.

2.3.5 Жұмыс күнінің фотосуреті

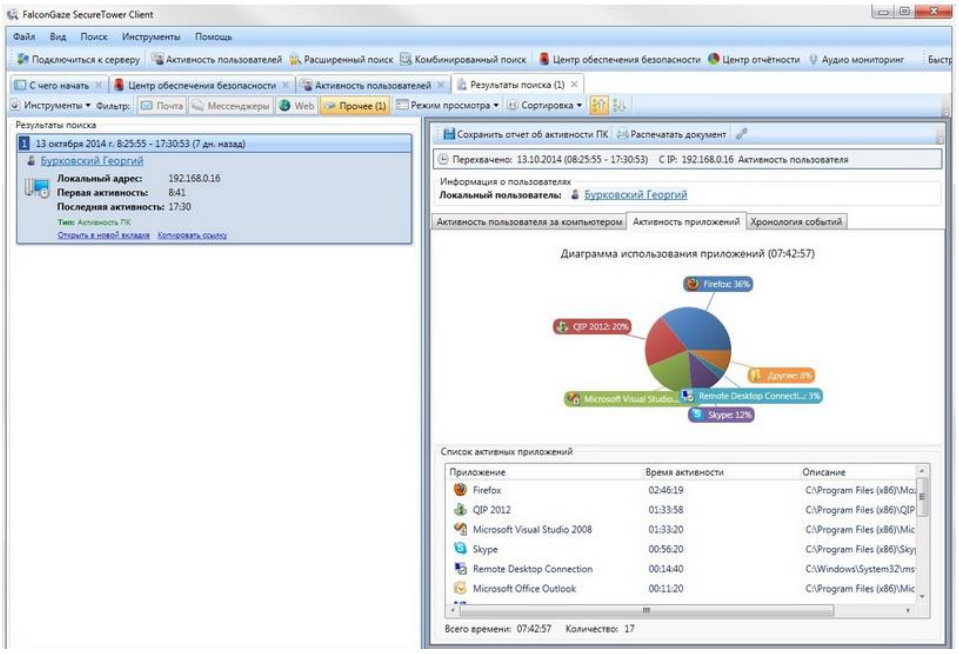
Олардың тағы бір маңызды функциялары – күннің жалпы көрінісі. Яғни, жүйе жетекшінің қалауы бойынша жалпы есепті шығара алады ,онда қызметкердің бір күн ішінде немен айналысқанын көруге болады: қанша хат жіберді және алды, қанша сайт келді, ал қанша уақыт мессенджерлерде сөйлесуге арнады (Сурет 22, 23, 24).



Сурет 22 – Қызметкердің жұмыс күнінің суретін көру

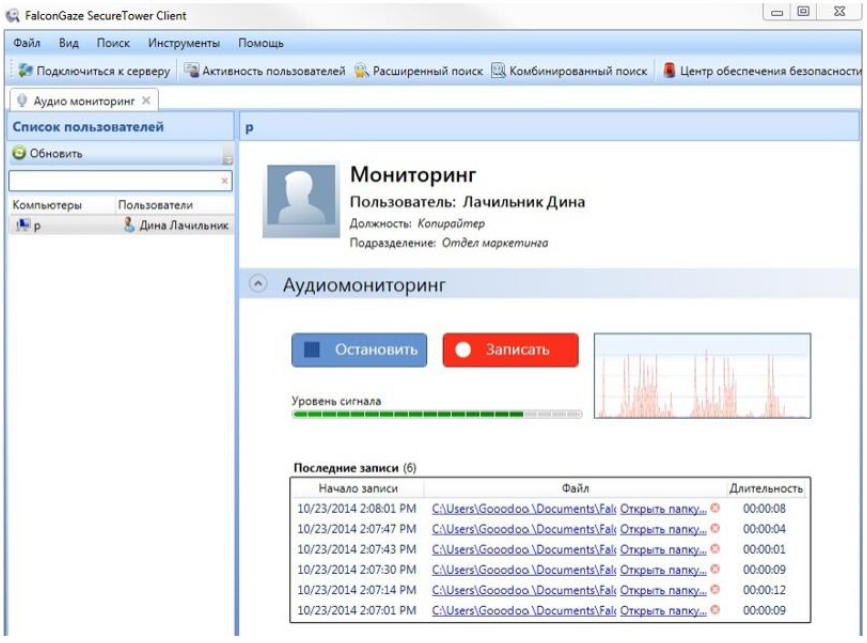


Сурет 23 – Қызметкердің жұмыс үстелінің скриншоттарын қарау



Сурет 24 – Қолданбалардың белсенділігін көру

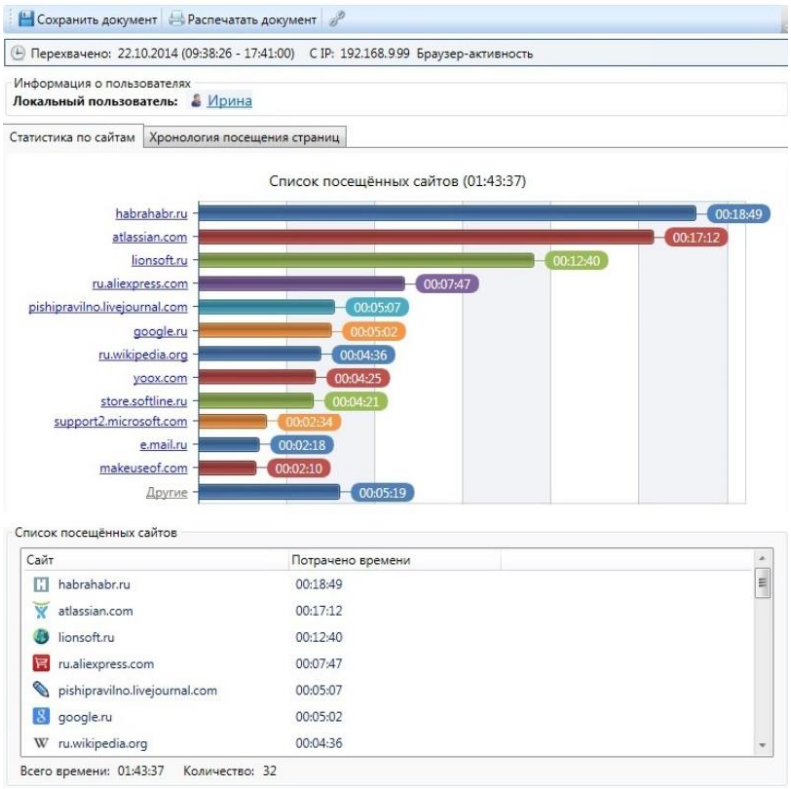
SecureTower 5.5-те жаңа бөлім – «Аудиомониторинг» пайда болды, ол жұмыс станцияларына кіріктірілген немесе қосылған микрофондардан дыбыс ағындарын бақылау арқылы қызметкерлердің сөйлесу сөздерінде құпия ақпаратты жария ету фактілерін анықтауға мүмкіндік береді (Сурет 25). Сондай-ақ, жеке сөйлесулерді жазу мүмкіндігі бар.



Сурет 25 – SecureTower 5.5 аудиомониторингінің мысалы

SecureTower 5.5 тағы бір назар аударарлық жаңалық браузерлерде пайдаланушылардың белсенділігін бақылау мүмкіндігінің пайда болуы болды. Бұл функционал белгілі бір қызметкер кірген сайттардың мекен-жайларын ғана емес, нақты сайтты қарауға жұмсалған нақты уақытты да белгілеуге

мүмкіндік береді (Сурет 26). Осының арқасында пайдаланушы кәсіби қызметке қатысы жоқ сайттарда қанша жұмыс уақытын өткізетінін анықтауға болады.



Сурет 26 – SecureTower 5.5 браузерлерде белсенділікті бекіту

SecureTower 5.5 – бұл функционалы үлкен қорғаушы бағдарлама. Деректер ағуына қарсы күреспен қатар, Бағдарлама ұйымда бұл ағулар қолайлы екенін анықтай алады. Пайдалану оңай және жаңадан келгендерге түсінікті, қызметкерлерді бақылауға қатысты көптеген шешімдер бар. Қосымша арқылы тәуекелдердің әр түрі бойынша көптеген есептерді басып шығаруға болатын сәт бонус болып табылады.

SecureTower 5.5 жұмыс орнынан скриналарды түсіруге, сөйлесулерді жазуға, қызметкерлердің кіммен байланысатынын көруге мүмкіндік береді. SecureTower 5.5 бағдарламасы өте көп.

SecureTower кемшіліктеріне 5.5. корпоративтік желіде жұмыс станцияларындағы құпия деректерді іздеу мүмкіндігі жоқ екенін ғана жатқызуға болады, бірақ әзірлеушілердің жақын болашақта осы функцияны іске асыруы тұр. Сондай-ақ, SecureTower өз арсеналында басып алынатын контентті талдаудың кейбір перспективалық әдістері жоқ, мысалы, жасанды интеллект технологиясы (машинада салынған), сканерленген құжаттардың қозғалысын бақылау, мөрлері бар құжаттар, бинарлық құжаттарға арналған сандық таңбалар. Өнімнің аздаған кемшіліктеріне енгізілген веб-сайт категоризаторының болмауы және бөгде өнімдермен интеграцияның әлсіз болуы жатады [13].

3 Техникалық-экономикалық негіздеме

3.1 Жобаның сипаттамасы

Бұл дипломдық жобаның мақсаты Falcongaze SecureTower тәуекелдерін бағалау және талдау үшін бағдарламалық қамтамасыз етуді зерттеу болып табылады.

Жоғарыда айтылғандай, бұл бағдарламалық өнім қанықпаған нарықта әрекет етеді, сондықтан оның әлеуетті бәсекеге қабілеттілігі өте жоғары. Егер осындай немесе ұқсас өнімнің бағасы белгілі фирманың ұқсас өнімінің бағасынан жоғары болған жағдайда, бәсекеге қабілеттілік төмендетіледі, баға арнайы төмендеген жағдайда өнім өндірісі экономикалық тиімсіз болып табылады, бұл да оны өндіруге кедергі бола алады. Бұл жобаны иерархиялық қағидат бойынша ұйымдастырылған мамандар тобын пайдалана отырып жүзеге асыру жоспарланып отыр. Топқа: жоба жетекшісі, әзірлеуші-бағдарламалаушы кіруі тиіс.

Жоба жетекшісі жұмысты орындаудың толық күнтізбелік кестесін әзірлеуге көмек көрсету және оның сақталуын бақылау, бітіру біліктілік жұмысының жоспарын жасауға көмек көрсету, әңгімелесу және консультациялар өткізу, орындалған бітіру біліктілік рботын бөліп-бөліп, сондай-ақ тұтастай тексеруге тиіс. Бағдарламалаушы-әзірлеуші теориялық негіздемені әзірлеуі, жобаны жасауы, алгоритм және интерфейстік идеологияны әзірлеуі тиіс. Осылайша, әзірлеуші-бағдарламалаушыға жоспарлау үшін жауапкершілік және жобаны іске асыру үшін жалпы жауапкершілік жүктеледі. Әзірлеуші-бағдарламалаушы жүйенің бағдарламалық модульдерін іске асыруға, жұмыс тестін жүргізуге міндетті.

Менің жұмысымда әзірлеу мен енгізудің техникалық-экономикалық негіздемесі мыналарды қамтиды:

- бағдарламаны әзірлеудің еңбек сыйымдылығын анықтау;
- бағдарламаны әзірлеуге арналған шығындарды есептеу;
- әзірленген бағдарламаның ықтимал бағасын анықтау;
- қызмет етудің әлеуметтік-экономикалық нәтижелерін бағалау.

3.2 Бағдарламалық өнімді әзірлеудің еңбек сыйымдылығы

Дипломдық жұмыстың осы бөлігінің мақсаты БӨ әзірлеудің еңбек сыйымдылығын анықтау, БӨ әзірлеудің желілік кестесін құру, БӨ әзірлеудің кезеңдері бойынша шығармашылық еңбектің үлес салмағын, жобалық жұмыстың өзіндік құнын бағалау, БӨ пайдасын және шарттық бағасын анықтау, жұмыстың ғылыми және ғылыми-техникалық нәтижелілігін бағалау болып табылады. Жұмыстың еңбек сыйымдылығы талдау мен зерттеулерді жүргізуге арналған уақыт нормаларына сәйкес анықталды. Әрбір жұмыс түрі бойынша кезеңдерге БӨ әзірлеу процесін бөлшектей отырып және әрбір жұмыс түрін орындаудың күтілетін еңбек сыйымдылығын анықтаймыз.

Дипломдық жұмысты жүргізудің әр кезеңінде әр жұмыс түрі бойынша орындаушылардың біліктілік деңгейі анықталады (Кесте 20).

Кесте 20 – Еңбек сыйымдылығының қорытынды көрсеткіштері

БӨ әзірлеу кезеңдері	Осы кезеңдегі жұмыс түрі	БӨ әзірлеудің еңбек сыйымдылығы, адам. х сағ.
1 кезең	Міндеттер қою	12
2 кезең	БӨ әзірлеуге техникалық тапсырманы әзірлеу және бекіту	12
3 кезең	Қорғауды әзірлеудің қазіргі әдістерімен танысу	14
4 кезең	«Деректерді қорғау үшін БӨ әзірлеу»тақырыбы бойынша әдебиеттерді таңдау және зерттеу	24
5 кезең	БӨ әзірлеу тақырыбын әзірлеу жағдайына аналитикалық шолу жасау	18
6 кезең	Кешенді қорғауды әзірлеудің әртүрлі әдістеріне талдау жүргізу	24
7 кезең	Бағдарламалық жобаның теориялық бөлігін рәсімдеу	16
8 кезең	Бағдарламалық жобаның тәжірибелік бөлігін әзірлеу	30
9 кезең	Әзірлеу ортасын таңдау	12
10 кезең	Математикалық есептеулерді әзірлеу және бағдарламаны жазу	16
11 кезең	Жобаны іске асыру	50
12 кезең	Қолданбаны баптау	18
13 кезең	Атқарылған жұмыс туралы есеп және қорытынды жасау	12
14 кезең	Сынақ тестілеу	14
15 кезең	БӨ әзірлеу қорытындысын шығару	8
16 кезең	Енгізу	10
17 кезең	Тестілеу	6
Нәтижесі	Жобалық жұмысты орындаудың еңбек сыйымдылығы	296

Жұмыс күнінің ұзақтығы 8 сағатқа тең. Нәтижесінде бағдарламалық қамтамасыз етуді іске асыру үшін 37 жұмыс күні қажет.

3.3 БӨ әзірлеуге жұмсалатын шығындарды есептеу

Өзіндік құнды есептеу БӨ әзірлеу кезінде жасалған шығыстар бойынша жүргізіледі. Жобалау жұмыстарын жүргізуге кететін шығындар өндіріс

алдындағы шығындарға жатады – бұл БӨ әзірлеушілері орындайтын барлық жұмыстарға арналған бір реттік шығындар.

Шығындар өзіндік құн калькуляциясының баптарын қосу жолымен анықталады:

- материалдар;
- ғылыми және тәжірибелік жұмыстарға арналған арнайы жабдықтар;
- жалақы төлемі;
- еңбекақы төлеу қорына есептеу;
- басқа ұйымдар орындайтын жұмыстарға арналған шығындар;
- басқа шығындар;
- үстеме шығынтар.

Бұл жоба бағдарламаны әзірлеу мен сынақтан өткізуді қарастырады. Демек, қойылған мақсаттарға қол жеткізу үшін бағдарламаны әзірлеу және тестілеу шығындарын, қорытынды бағдарламаның құнын, тиісті жабдықты сатып алуды, сонымен қатар, шығындардың өтелімділігін есептеу қажет. Материалдық шығындар негізгі және қосалқы шығындарға, материалдарға, энергияға және БӨ әзірлеу үшін қажетті басқа да шығындарға бөлінеді. Материалдық шығындарды есептеу 21-кестеде берілген нысан бойынша жүргізіледі.

Кесте 21 – Материалдық ресурстарға арналған шығындар

Материал атауы	Өлшем бірлігі	Саны	Бірлікүшін бағасы ,теңге	Сомасыт еңгемен
Кеңсеқағазы	Қаптама	4	1 400	5 600
Дәптер	Дана	2	120	240
Қалам	Дана	2	140	280
Компьютер тышқаны	Дана	1	5 000	5 000
Нәтижесі:				11 120

Материалдық құралдарға ($З_м$) қажетті жалпы соманы мынадай формула бойынша есептеуге болады:

$$З_м = \sum Р_i * Ц_i, \quad (3.1)$$

мұнда, $Р_i$ - материалдық ресурстың і түрінің шығысы, заттай бірліктер;
$Ц_i$ – материалдық ресурстың і түрінің бірлігінің бағасы, тг;
і – материалдық ресурстың түрі;
n – материалдық ресурстар түрлерінің саны.

Бағдарламалық қамтамасыз етуді әзірлеу үшін ASUS VivoBook S14 s410un-BV381T Gray ноутбук қолданылады, ноутбук қуаты қойылған міндеттерді орындау үшін жеткілікті. Бағдарламалық өнімді тестілеу үшін орнатылған операциялық жүйесі бар ДК қажет болады. Windows 7/8/10 нұсқалары. Ноутбукке сым арқылы қосылу үшін смартфон қажет. Қажетті жабдықтар мен бағдарламалық қамтамасыз етуге кететін шығындарды есептеу 22-кестеде келтірілген нысан бойынша жүргізіледі.

Кесте 22 – Жоба үшін қажетті жабдық пен БҚ шығындарын есептеу

Материалдық ресурстыңатауы	Өлшем бірлігі	Осы материалдан шығындар саны	Бірлік үшін бағасы ,тг	Нәтижесі, тг
MS Windows 8 операциялық жүйесі және MS Office кеңселік бумасы бар жеке компьютер	дана	1	120000	120000
ASUS VivoBook S14 s410un-BV381T Gray ноутбугы	дана	1	312 000	312 000
USB Manhattan 307178, A(M)/microB(M),	дана	2	200	400
Xperia Z3 смартфоны	дана	1	140000	140000
Нәтижесі				572 400

Осы кестеге сәйкес жобаға материалдық шығындар 583 520,00 теңгені құрайды.

$$З_{м} = 572\,400 + 11120 = 583\,520$$

Электр энергиясын тұтынатын болғандықтан, бағдарламалық қамтамасыз етуді әзірлеу кезінде электрэнергиясына жұмсалатын шығындарды есептеу қажет.

20 – кестеге сәйкес бағдарламалаушы үшін бағдарламалық қамтамасыз етуді әзірлеу үшін шамамен 296 сағат, ал жетекшіге 140 сағат қажет. Енді 296 сағат ішінде жұмсалатын электр энергиясының құнын есептеу қажет (Кесте 23). Принтер үшін есептеу 24 сағат кезеңі үшін жүргізіледі, себебі принтерді үнемі пайдалану қажет емес.

$$Э = З_{эл.эн.жабд} + З_{кос.кажет.}, \quad (3.2)$$

мұнда, $З_{эл.эн.жабд.}$ – жабдықтың электр энергиясына арналған шығындары;
$З_{кос.кажет.}$ – қосымша қажеттіліктерге электр энергиясының шығындары.

Жабдық үшін қажетті электр энергиясын есептеу мынадай формула бойынша анықталады:

$$З_{эл.эн.жабд} = \sum W * K_{пайда} * S * T, \quad (3.3)$$

мұнда, W – тұтынылатын қуат, Вт;
$K_{пайда}$ – пайдалану коэффициенті ($K_{пайда}$ = 0,7..0,9).

Кесте 23 – Электр энергиясына кететін шығындар

Аспаптардың атауы	Қуаты, кВт	Қуат коэффициенті	Жабдықтың жұмыс жасау уақыты, сағ	ЭЭ құны тг/кВт сағ	Сомасы, тг.
Ноутбук	0,5	0,7	296	23,85	2470,86
Жұмыс станциясы	0,4	0,9	296	23,85	2541,45
Принтер	0,5	0,9	20	23,85	214,65
Кондиционер	0,9	0,9	160	23,85	3090,96
Жарықтандыру	0,35	0,7	296	23,85	1729,6
Нәтижесі:					10 048

$$З_{эл.эн.жабд} = 10048,00(\text{тенге})$$

Қосымша қажеттіліктерге шығындар электр энергиясына арналған шығынның 5% көлемінде жоғары көрсеткіш негізінде есептеледі:

$$З_{кос.кажет.} = 5\% * З_{эл.эн.жабд}, \quad (3.4)$$

(3.4) формулаға сәйкес қосымша қажеттіліктерге жұмсалатын шығындарды анықтаймыз:

$$З_{кос.кажет} = 0,05 * 10048 = 502,40$$

Барлық есептеулерге сүйене отырып, электрэнергиясына кететін толық шығын құрайды:

$$Э = 502,40 + 10048 = 10550,40(\text{тенге})$$

Бағдарламалыққамтамасызетудіәзірлеуүшінбұрынкөрсетілгендей, екіқызметкеркажет:

- жоба жетекшісі – жұмыс уақытын басқару, жұмыс процестерін түзету, үйлестіру, пәндік облысты зерттеу;
- бағдарламалаушы-әзірлеуші – БҚ әзірлеу, тестілеу және сүйемелдеу.

Еңбекақы төлеу шығындарының сомасын келесі формула бойынша есептеуге болады:

$$З_{ен} = \sum ЧС_i + Т_i \quad (3.5)$$

мұнда, $ЧС_i$ – і қызметкердің сағаттық ақысы, тг;
$Т_i$ – модельді әзірлеудің еңбек сыйымдылығы, адам.×сағ;
і – қызметкердің санаты;
n – БӨ әзірлеумен айналысатын қызметкерлердің саны

Жобаны іске асыру кезінде қатысушылардың жұмыс уақыты біркелкі емес, сондықтан әрбір қызметкердің сағаттық ақысы және жалпы жалақы көлемін белгілеу қажет. Қызметкердің сағаттық ақасын келесі формуламен есептеуге болады:

$$ЧС_i = \frac{ЗП_i}{ФРВ_i} \quad (3.6)$$

мұнда, $ЗП_i$ – і қызметкердің айлық жалақысы, тг;
$ФВР_i$ – і қызметкердің айлық жұмыс уақытының қоры, сағ.

Жетекшінің айлық жалақысы 180 000 теңгеге тең және әзірлеушінің айлық жалақысы 120 000 теңгеге тең. Әр қызметкердің сағаттық ақысын (3.6) формулаға сәйкес есептейміз:

$$ЧС_{жетекші} = \frac{180000}{21*8} = 1071{,}42,$$

$$ЧС_{программалаушы} = \frac{120000}{21*8} = 714{,}28$$

Жетекшінің сағаттық ақысы 1071,42 (тг/сағ) құрайды, еңбек сыйымдылығы 140 сағатқа тең. Әзірлеушінің сағаттық ақысы 714,28 (тг/сағ), әзірлеудің еңбексыйымдылығы 296 сағатқа тең. (3.5) формулаға сәйкес қызметкерлердің еңбекақысына арналған шығындар сомасын есептеуге болады:

$$З_{ен} = 1071{,}42*140 + 714{,}28*296 = 150000 + 214427 = 364427$$

Еңбекақы төлеу бойынша шығындарды есептеу 24-кестеде көрсетілген.

Кесте 24 – Жалақыны есептеу

Қызметкер санаты	Біліктілігі	БӨ еңбек сыйым дылығы, сағ.	Сағаттық ақысы, тг/сағ	Сома, тг.
Әзірлеуші	Бағдарламалаушы	296	714, 28	214427
Жетекші	Инженер-жобалаушы	140	1071, 42	150000
Нәтижесі:				364427

Қазақстан Республикасының Салық кодексіне сәйкес әлеуметтік салық еңбекақы төлеу қорының 9,5% - ын құрайды. Әлеуметтік салықты келесі формула бойынша есептеуге болады:

$$С_с = (ФОТ - ПО) * 0,095 \quad (3.7)$$

мұнда, ПО –зейнетақы қорына аударымдар, олар ФОТ 10% құрайды.

$$ПО = 364427 * 0,1 = 36442,70(тенге)$$

$$С_с = (364427 - 36447,2) * 0,095 = 31158,50(тенге)$$

Есептеу нәтижелері 25-кестеде көрсетілген.

Кесте 25 – Әлеуметтік салықты есептеу

Қызметкер санаты	Адам саны	Жалақы, тг	Зейнетақы аударымы, тг	Әлеуметтік салық, тг
Жетекші	1	150 000	15 000	12 825
Әзірлеуші	1	214 427	21 442,7	18 333,50
Нәтижесі:				31 158,50

Негізгі қорлар амортизациясының нормаларын ҚР Салық кодексіне сәйкес анықтау қажет. НҚ амортизациясын келесі формула бойынша анықтауға болады:

$$А_ж = \frac{С_{жабд} * Н_а}{100} \quad (3.8)$$

мұнда, $С_{жабд}$ – жабдықтың құны;
$Н_а$ – амортизация нормасы (амортизация нормасы = 25);

(3.8) формуласы ноутбук үшін бір жыл ішінде амортизациялық аударымдар үшін қажетті соманы есептеуге мүмкіндік береді:

$$А_ж = \frac{312000 * 25}{100} = 78000,00$$

Енді әзірлеу кезеңі үшін амортизация нормасын есептеу қажет:

$$А_{ж} = \frac{78000 * 37}{25} = 7906,80$$

Осылайша, барлық жабдық үшін амортизация нормасын есептеу қажет. Есептеу нәтижелері 26-кестеде келтірілген.

Кесте 26 – Негізгі қорлардың амортизациясы

Жабдық және БҚ атауы	Жабдық және БҚ бағасы, тг	Амортизацияның жылдық нормасы,%	Жыл ішіндегі амортизация сомасы, тг	Әзірлеу кезіндегі амортизация сомасы, тг
Ноутбук	312 000	25	78 000	7 906,800
Смартфон	140 000	15	21 000	2 128,70
ДК	120 000	20	24 000	2 432,50
Нәтижесі:			136 000	12 468

Барлық берілген есеп-қисаптардың негізінде 27-кестеде келтірілген нысан бойынша әзірлеуге арналған шығынтар сметасын рәсімдеу қажет.

Кесте 27 – БҚ әзірлеуге арналған шығындар сметасы

Шығындарбаптары	Сомасы, тг
Жабдыққа кеткен шығын	572 400
Электр энергиясына кеткен шығын	10 550,60
Еңбекақы төлеу шығындары	364 427
Әлеуметтік салық	31 158,50
Негізгі қорлардың амортизациясы	12 468
Өзге де шығындар (мат., интернет)	15 655
Смета бойынша қорытынды:	1 006 659

3.4 Бағдарламалық өнімнің ықтимал (шарттық) бағасын анықтау

БӨ ықтимал (шарттық) бағасының шамасы тапсырыс берушінің (тұтынушының) және орындаушының экономикалық мүдделеріне жауап беретін деңгейде оның орындалу тиімділігі, сапасы мен мерзімдері ескеріле отырып белгіленуі тиіс. Қолданбалы БӨ үшін шарттық баға ($Ц_К$) мынадай формула бойынша есептеледі:

$$Ц_К = З_{нир}(1 + Р/100), \qquad (3.9)$$

мұнда, Знир – БӨ әзірлеуге жұмсалатын шығындар (27-кестеден), тг;
Р – бағдарламалық өнімнің рентабельділігінің орташа деңгейі, % (20-30% мөлшерінде қабылданады).Бұл параметр 25% тең.

$$Ц_д = 1\,006\,659 + 1\,006659 * 0,25 = 1\,258\,323,75$$

Бұдан әрі қосылған құн салығын (ҚҚС) есепке ала отырып, өткізу құнын анықтау қажет, ҚҚС ставкасы ҚР заңнамалық Салық кодексімен белгіленеді. 2019 жылға ҚҚС ставкасы 12% мөлшерінде белгіленген. Іске асыру құнын ҚҚС-ты ескере отырып мынадай формула бойынша есептеуге болады:

$$Ц_Р = Ц_К + Ц_К * ҚҚС \quad (3.10)$$

$$Ц_р = 1258323,75 + 1258323,75 * 0,12 = 1258323,75 + 150998,85 = 1409322,60$$

Бұл бағаны 1 409 400 теңгеге дейін дөңгелектеуге болады.

3.5 Бағдарламалық өнімніңжұмысістеуініңәлеуметтік-экономикалықнәтижелерінбағалау

Бұл жобаның экономикалық мақсаттылығы сандық және сапалы құрамдастардан құралатын болады. Әзірлеушілер үшін экономикалық тиімділік жеке әзірлеушілер мен жобаны іске асырумен айналысатын кәсіпорындардың қаржылық жағдайын жақсартудан тұрады. Осы жобаны сәтті іске асыру кезінде әзірлеушілер 214 427 теңгені құрайтын жалақы алады. Әзірлеушілер үшін сапалы тиімділік-бұл жобаны нарыққа шығарудың алғашқы тәжірибесі, онда әзірлеуші одан әрі жобалау мәселелерін шешеді, жобаның тиімділігі, одан әрі жұмыс негіздерін жобалау. Сондай-ақ , жобаны іске асыру барысында жарнама маркетингі, бағдарламалық қамтамасыз ету нарығын игеру мәселелері шешілетін болады. Бұл жобаның өзіндік құны 1 006 659 теңгені, пайда 258 323 теңгені құрады. Қорытындылай келе, бұл жобаның ықтимал бағасы 1 409 400 теңге [14].

4 Өміртіршілік қауіпсіздігі

4.1 Компьютерден бөлінетін сәулелер

Компьютер – адам интеллектінің ең тамаша жетістіктерінің бірі. ЭЕМ және ДК үлкен ресурстары арқылы қолданушылардың тікелей диалог жүргізе алу мүмкіндігі миллиондаған адамдардың экран алдында көп уақыт өткізуіне алып келді. Уақыт өте келе компьютер пайдаланушыларында өзіндерін сезінуге байланысты шағымдар жиынтығы пайда болады.

Бұл компьютерден адамның денсаулығына сәулеленудің әсері туралы ойлаға алып келді. Мұндай ойлар үшін көптеген себептер бар. Бірқатар ғалымдар тұрмыстық АЖЖ көздерінен адамдарға электромагниттік сәулеленудің әсерімен байланыстырады.

Электрондық құрылғылар әртүрлі түрдегі сәуле шығарады – электромагниттік толқындар, электростатикалық кернеу және радиация. Электростатикалық кернеу электрді пайдаланатын барлық құрылғыларда болады, оның негізгі көздері – электр беру желілерін құрады. Қалада тұрып, одан құтылу мүмкін емес, компьютерлерден сәулелену осы әсерден аз көлемді құрайды. Сондықтан электромагниттік толқындарға толығырақ тоқтай кетсек.

Олар сезілмейді, денсаулыққа айтарлықтай зиян әкелмейді, бірақ дүниежүзілік денсаулық сақтау ұйымы экология үшін қауіпті факторлардың тізіміне электромагниттік сәулені енгізді. Электр желісінен жұмыс істеу кезінде аспаптар Жерді қоршаған физикалық өрісте импульстердің тербелісін жасайды. Бұл тербелістер экожүйенің жай-күйіне теріс әсер ете отырып, ғаламшардың жалпы электромагниттік өрісінің қозуын тудырады. Ал үйде компьютерден зиянды сәулелену денсаулыққа теріс әсер етуі мүмкін.

Әрбір дербес компьютерден электромагниттік сәуле шығады: төмен жиілікті және радиожиілікті. Дүниежүзілік денсаулық сақтау ұйымының пікірінше, толқындардың екі түрі де канцерогенді болып табылады – ол обыр ауруын тудыруы мүмкін.

4.1.1 Компьютер мониторынан бөлінетін сәуле

Мониторлардың ішінде электронды-сәулелі түтікшелілері ең зиянды екені анықталды. Олады пайдаланған кезде, компьютер сәуле шағарады ма деген сұрақ туды. Иә, монитордан бөлінетін радиацияның зиянын рентген сәулелерінің зиянымен салыстыруға болады. Құрал 2 және одан да көп сағат компьютерді өшіргеннен кейін де сақталатын қуат өрістерін және жоғары электр кернеуін шығарады.

Сұйық-кристалды мониторлар айтарлықтай қауіпсіз, олар шамамен 50 Гц сәулелену қалыптастырады. Бұл доза ағзаға нақты зиян келтіру үшін аз, бірақ тұрақты әсер ету кезінде жағымсыз салдарлардан қашып құтылу мүмкін емес. Аналық плата мен корпустың қызуына байланысты ауаның деионизациясы және қоршаған ортаға зиянды заттардың бөлінуі орын алады. Міне, сондықтан тұрақты жұмыс істейтін есептеу техникасы бар бөлмелердегі ауа тыныс алу үшін өте ауыр. Тыныс алу жүйесі әлсіз адамдар үшін бұл

фактор демікпені тудырып, кері әсер етуі мүмкін. Ол компьютердің электростатикалық өрісінің және монитордың ауадағы өлшенген шаң бөлшектеріне әсерімен одан әрі күрделене түседі. Электрленіп алып, олар «тозаңды коктейль» құрайды, тыныс алуды ауырлатады.

Сенсорлы экранның болуы радиацияның жоқтығына кепілдік бермейді. Себебі, сіздің саусақтарыңыз экранда манипуляциялар жасай отырып, онымен, wi-fi-антеннадан бірнеше миллиметрде жанасады.

Әсіресе, жол жағдайында жұмыс істеуге арналған портативті құрылғы ретінде ойланған ноутбук сәуле шығару мәселесін де назарсыз қалдыруға болмайды. Бұл ыңғайлы және көпфункционалды құралдарды толық жұмыс күні ішінде пайдалану әртүрлі патологиялар мен аурулардың себебі болуы мүмкін. Өйткені, ол қарапайым компьютер сияқты электромагниттік сәулелену көзі болып табылады, бірақ ол адамға компьютерден айтарлықтай жақын орналасады. Сол себепті, олардың ада ағзасына зияны да көбірек.

4.1.2 Компьютерлік жүйе блогынан бөлінетін сәуле

Жүйелік блок өзі айналасында электромагниттік өрісті белсенді жасайды. 2 мгтс (миллигаусс) минималды фондау ағзаға теріс әсер етеді. Ол адамнан 50-ден 100 см-ге дейінгі қашықтықта орналасқан құрылғы тудыра алады. Процессор неғұрлым жақынырақ болса, соғұрлым күшті әсер етеді.

4.1.3 Құлаққаптар мен гарнитуралар

Олар ерекше қауіп тудырады, өйткені әрқашан басқа тікелей киіледі. Сымсыз гарнитуралар мен Bluetooth жүйелері – бұл ең нашар нұсқа: олар арқылы адам ағзасына радио толқындары да енеді. Кабель айтарлықтай қауіпсіз, бірақ ұмытпаған дұрыс: оның ішінде металл – компьютер процессорынан тікелей кез келген сәулелер үшін тамаша өткізгіш. Жалпы, құлаққаптарды алып тастау және колонкадан дыбыс шығару мүмкіндігі пайда болған соң, оны бірден пайдаланған жөн.

4.1.4 Колонкалар

Кейбір қуатты колонкалар, әсіресе вуферлер айналасында елеулі электромагниттік өріс жасайды. Олардан кемінде 50 см қашықтықта ұстаған жөн.

4.1.5 Принтерлер

Мөлшері әртүрлі және тиісінше қуаты бар. Ең қарапайым, үй принтері 50 см қашықтықта ұстаған дұрыс. Үлкен кеңсе үшін арналған принтерді адамдардан 65 см арақашықтықта қалдыру керек.

4.1.6 Роутерлер, модемдер, маршрутизаторлар

Олардың радиожиілік магнит өрістері айнала көп метрге созылады. Бұлар сонысымен ыңғайлы, бірақ денсаулық үшін зиян. Тіпті егер оларды компьютерге кабель арқылы қосқан күнде де төмен жиіліктер адамға әсер етеді. Сондықтан оларды 35 см кем емес қашықтықта қою керек.

4.1.7 Зарядтау құрылғылары мен трансформаторлар

Олар жоғарыда аталған барлық техника үшін өте қуатты төмен жиіліктерді шығарады. Оларды бір метр қашықтықта ұстау керек.

4.2 Компьютерден бөлінген сәулелердің адамға әсері

Компьютерден бөлінетін сәулелердің адам ағзасына неге зиянды екенін анықтайық. Адам ағзасы да электрлік импульстерді шығарады. Олардың көмегімен ми мен жұлынға жүйке үштары арқылы сигналдар келіп түседі, қаңқа бұлшықеті мен жүрек бұлшықеттері азаяды. Жүйке үштары арқылы секундына мыңдаған сигналдар беріледі, сондықтан компьютерден қандай зиян келетінін оңай түсінуге болады, сәулелер электрлік импульс жіберудің қиын жүйесіне әсер етіп, олардың өзара байланысына бөгет келтіруі мүмкін. Оның әсері бір сәтте сезілмейді,ол ағзада жинақталып, мүшелер мен жүйелердің жұмысын біртіндеп нашарлатады. Екі маңызды жүйе ең осал болып табылады:

- жүйке жүйесі
- жүрек-қан тамырлар жүйесі.

Бұның әсерінен ми сигналдары патологиялық түрде өзгеруі мүмкін. Бұл мидың және жүрек-тамыр жүйесі органдарының бұзылуына себеп болады. Жүрек-қантамыр жүйесінің қалыпты жұмыс істеуі импульстердің когеренттігіне және беріктігіне байланысты. Үйдегі бір немесе одан да көп құрылғылар жүрек жұмысын елеулі бұзылуға алып келмейді, бірақ үнемі сәулелену аритмия мен жүрек-тамыр қабілетінің бұзылуына әкелуі мүмкін. Ұзақ уақыт бойы әсер етуі бас ауруы, мигреньдер, иммунитеттің төмендеуі, депрессия, гормоналды теңгерімсіздік және ұйқының бұзылуына әкелуі мүмкін. Компьютерде көп жұмыс істеу Альцгеймер ауруы, Паркинсон ауруы, қатерлі ісік ауруы және ұрпақты болу жүйесінің бұзылу қаупін арттырады. Сонымен қатар миокард және перикард ауруларына, ағзаның жалпы гормональды фонының бұзылуына, су-тұз алмасуының нашарлауына, гомеостаздың бұзылуына алып келуі мүмкін.

Үй компьютері, ноутбук немесе смартфон зиянды сәуле көзі болып табылады. Компьютерден қанша сәуле алатынымыз түрлі факторларға байланысты: құралдың түрі, пайдалану уақыты, орналасуы.

4.3 Сәулеленуден қорғанудың іс-шаралары

Компьютерден қандай сәуле бөлінетінін және оның адам ағзасына калай әсер ететінін анықтаған соң, одан қорғану шараларын қарастыра кетсек.

Келесі кеңестерді орындай отырып, компьютерден бөлінетін сәулелердің әсерін бәсеңдетуге болады:

- егер бірнеше компьютер немесе ноутбуктер үнемі бір үй-жайда (мысалы, сыныпта, кеңседе) тұрса, оларды құрылғылар бөлменің периметрі бойынша тұратындай, ал орталық бос болатындай етіп орналастыру керек;
- мүмкіндігінше электрмагниттік сәулеленудің саны мен қарқындылығын азайтатын арнайы қорғаныс құралдары орнатылған

мониторларды пайдаланған жөн. әсіресе, бұл кеңес компьютер алдында көп уақыт жұмсайтын балаларға өзекті болып табылады;

- мониторды таңдау барысында, оның кеңеюіне, қорғау деңгейіне және радиациялық сәулелену мөлшеріне назар аудару керек. low radiain жазуы бар экрандарға көбірек назар адару қажет, себебі бұл ең аз радиация санын білдіреді;

- монитор көру үшін ыңғайлы қашықтықта, ал жүйелік блок пайдаланушыдан барынша алыста орналасуы тиіс;

- жұмыс аяқталғаннан кейін компьютерді өшіру керек, өйткені ол қаншалықты ұзақ жұмыс істесе, соғұрлым көп сәуле шығарады және ауаны арқылы қоршаған ортаға зиянды заттардың үлкен мөлшерін бөледі;

- арнайы қорғаныс пленкасын пайдалану электромагниттік сәуле шығару қарқындылығын және пайдаланушы ағзасына зиянды әсер ету мөлшерін азайтады;

- шаңды жүйелі түрде шығару, ылғалды жинау және мүмкіндігінше ионизаторларды қолдану компьютер жұмысының нәтижесінде алынған заттар әсер ететін дем шығаратын ауаның сапасын жақсартады, сондай-ақ адамның денесіне электромагниттік сәулеленудің зиянды факторларының әсерін азайтады;

- монитордың жандарынан және артқы бөлігінен шығатын сәулелер компьютермен бір бөлмеде, бірақ оны қолданбайтын адамға әсер етпеуі үшін, оны бөлменің бұрышына орналастырған жөн. Сондай-ақ, монитор көзге ыңғайлы жағдайда (бірақ кемінде 40 см) болуы тиіс, ал жүйелік блок пайдаланушыдан мүмкіндігінше алыс орналасуы тиіс [15].

4.4 Қолданушының компьютерден қауіпсіздік қашықтығын есептеу

Компьютер алдында жұмыс жасау барысында, барынша қауіпсіздікте болу үшін, монитордан көзге дейінгі ең аз арақашықтықты білу керек. Егер монитордың экраны қолданушыға қатысты дұрыс орналасса, қолданушының жақсы көру қабілетін ұзақ сақтап, остеохондроз және омыртқаның қисаюын болдырмайды.

Монитор мен көздің арасындағы қашықтық, ең алдымен, оның өлшемді параметрлеріне байланысты. Қазіргі уақытта ең танымал модельдер 14-тен (ноутбуктар) 27 дюймге дейінгі диагоналдармен, ал ең үлкені диагоналі 30-дан асатын экрандармен жабдықталған. Мониторлардың техникалық мүмкіндіктері мен қолдану салалары олардың дюйм өлшемдеріне байланысты.

Ең көп таралған модельдер келесі түрде болады:

- 14 – 16''. Бұл бұқаралық ноутбуктар, олардың өлшемдері оңтайлы өнімділікті процессорларды ендіруге мүмкіндік береді. Кішкентай диагоналды портативті құрылғылардың қолданыс аясы тар.

- 17''. Көлемді ноутбуктар кеңсе үшін ыңғайлы нұсқа. Алып жүру ыңғайлы болмағанымен, жұмыс аймағында кеңістікті үнемдйді.

- 18,5 – 20,1''. Шағын стационарлы модельдер, көбінде мәтін редакторында жұмыс жасау үшін пайдаданылады.

- 21,5 – 24''. Орташа диагоналды бейнемониторлар қолданушыға ыңғайлы түрде мәтін теруге, бейнебаяндарды редакциялауға, бейнефильмдерді көруге мүмкіндік беретін әмбебап нұсқа болып табылады. 3D бейнесі бар ойынды қолдау үшін диагоналі кемінде 23 дюйм болуы керек.

- 27'' және одан жоғары. Олар көбінесе фильмдер көруге, фото, бейне, аудио материалдырды редакциялау үшін қолданылады. Бұл мониторлар студияда, әсіресе, дыбыс жазу және фильм түсіру барысында таптырмас құрал болып табылады. 32 және одан да жоғары дюймді мониторлар бейнебақылау үшін пайдаланылады. Ал қабырға мониторын теледидар ретінде пайдалану керек болса, оның диагоналі 31-34 дюйм болғаны жөн.

Ғылыми зерттеулерге сүйенсек, адамның көзі 17 градус шеңберіндегі кескінді анық көре алады. Бұл жауап математикалық түрде алынады: пайдаланушының беті мен экран арасындағы ең аз рұқсат етілген қашықтық оның диагональды ұзындығы болып табылады.

Көз бен бейне монитор арасының қанша сантиметр болу керек екенін анықтағанда, оның өлшемдерін ғана емес, сонымен қатар жобалау ерекшеліктерін де ескеру қажет. TFT панелі бар СК-дисплейді қолдану қауіпсіздірек.

Электронды-сәулелік түтікке негізделген дәстүрлі құрылғылармен салыстырғанда, скд үлгілері мынадай артықшылыққа ие:

- элетромагниттік сәулеленудің өте аз мөлшерде болуы;
- көрінетін аймақтың үлкен өлшемі (15 дюймдік скд мониторы 17 дюймдік crt аналогы сияқты);
- сурет бұрмалауының жоқтығы;
- үлтелде үнемді орын алуы.

CRT бар болған жағдайда компьютер мониторынан 60-70 см қашықтықта болу керек, ал СКД барлық шарттарға қарамастан арақашықтықты 30-50 см қысқартуға мүмкіндік береді. Көзге түсетін жүктемені азайту үшін кескінді дұрыс бейідеу маңызды, сонымен қатар, бірінші мониторды арнайы бағдарлама арқылы тексеріп алған жөн.

Медициналық стандарттарға сәйкес, компьютерлік мониторға оңдайлы қашықтық – ең аз дегенде – бір жарымнан екі диагоналға дейін болуы керек. Есептеу үшін келесі формула қолданылады:

$$S - L * 2,54 * 1,75, \qquad (4.1)$$

мұнда, L – диагональдың дюймдік ұзындығы;
2,54 – дюймді сантиметрге айналдыру коэффициенті;
1,75 – 1,5 және 2 диагоналі арасындары арифетикалық орта.

Формулаға сәйкес диагоналі 17 дюйм болатын кеңсе ноутбугынан оңтайлы қашықтықты есептесек:

$$S = 17 * 2{,}54 * 1{,}75 = 75(\text{см}) \qquad (4.2)$$

Дәл осындай жолмен диагоналдың өлшеміне негізделе отырып, адам көзіне оңтайлы қашықтық есептеледі. Компьютерлердің әртүрлі модельдері бойынша есептеулердің нәтижелері 28-кестеде келтірілген.

Кесте 28 – Компьютерлердің әртүрлі модельдері бойынша есептеулердің нәтижелері

Диагоналдың өлшемі, дюйм	Экраннан көзге дейінгі оңтайлы қашықтық, см
14	62
15	67
16	71
17	75
18	80
19	85
20	89
21	94
22	98
23	102
24	107
25	111
26	116
27	120
28	125
29	129
30	134
31	138
32	142

Студенттер мен оқушылардың, операторлардың, қызметкерлердің еңбекгін қорғау мақсатында олардың монитор алдындағы жұмыс орнын SanPiN 2.2.2.542-96 және SanPiN 2.4.2.1178-02 санитарлық нормалары және ережелеріне сай жабдықталуы керек. Бұл мәселеге құзіретті көзқарас визуалды шаршау мен басқа да аурулардың алдын алуға көмектеседі.

Қазіргі кезде кәсіпорындардың, мекемелердің немесе дүкендердің қорғалуы мен басқаруы бейнебақылау арқылы жүзеге асырылуда.

Тағы бір маңызды ерекшелігі – бір дисплейдің бірнеше камераларда жұмысы болып табылады, яғни, камералардың әрқайсысы белгілі бір аймақта орналасқан және әрбіреуі өз бейнесін көрсетеді (бейне өрісі). Дисплейді тиімді бақылау үшін 20-24 өріс болғаны жөн деп саналады.

Қажетті санына қарай бейнеқұрылғының диагоналын есептейді, шыққан мәнге сүйене отырып экранның бақылаушы көзіне дейінгі арақашықтықты

есептейді. Барлық үш параметрдің дұрыс коэффициенттері 29-кестеде келтірлген.

Кесте 29 – Барлық үш параметрдің дұрыс коэффициенттері

Өріс саны	Диагональ ұзындығы, дюйм (см)	Бақылаушы мен дисплей арасындағы қашықтық, м
4	Минималды – 17 (43)	1,7
9	19-дан 22-ге дейін (50 – 56)	2,0
16	19-дан 40-қа дейін (50 – 102)	2,0 – 3,0
20	Ең аз 32 (81)	2,5

Аудиторияны жоспарлау кезінде копмьютерлік аудиторияның ішіндегі жұмыс орындарын шектеуді ұсынатын санитарлық норманың SanPiN 2.2.2.542-96 SanPiN 2.4.2.1178 -02 пунктілері ескерілуі тиіс. Бір қолданушыға арналған алаң 2,5-тен 3,5-м^2-ге дейін болуы керек. Бір компьютер үшін рұқсат етілген ең аз аймақ 6 м^2 жетеді.

Аудиторядағы жұмыс орындары үш жолмен ұйымдастырылады:

- қатар түрінде – қолданушылар бір-бірінің артында отырады, барлық дисплейлер бір бағытта бұрылады;
- кеңсенің ортасында компьютері бар үстелдердің екі қатары аудиторияның ортасыда бос орынсыз орналасады, ал компьютерлердің экрандары бір – біріне теріс бағытта айналдырылады;
- периметр бойынша – компьютері бар үстелдер қабырға бойымен орналастырылады.

Жұмыс орнын жабдықтау кезінде пайдаланушы көзінен монитор экраны кемінде 50-70 см қашықтықта болуы керек. Пайдаланушының үстелде дұрыс отырғаны жөн. Сонымен қатар, келесі ескертулердің де назарсыз қалмағаны дұрыс:

Дисплей жазықтығы тігінен орналасса, оның орталығы (немесе 2/3 биіктігіндегі нүктесі) көздің деңгейінде орналасу керек;

- көздің экранға 90 ˚ бұрышпен түскені жөн (перпендикулярдан 5-10˚ ауытқу рұқсат етіледі);
- бас аздап алға қарай қарағаны дұрыс – максималды 15˚.

Бұл шарттар үшін 30-кестені қолданған дұрыс.

Кесте 30 – Параметрлер кестесі

Қолданушының бойы, см	Үстел бетінің еденнен қашықтығы, см	Орындықтың еденнен қашықтығы, см	Орындық тереңдігі, см
100 – 115	46	26	26
115 – 130	52	30	29
130 – 145	58	34	33
145 – 160	64	38	36
160 – 175	70	42	38
175-тен көп	76	46	40

Жоғарыдағы ережелерге сүйене отырып, қолданушы өзіне сәйкестендіріп монитордың орналасу орнын жабдықтай алады. Келтірілген ережелерді сақтау омыртқаның тіктігіне және көз саулығына көп септігін тигізеді [15].

Қорытынды

Бұл дипломдық жұмыста бағалау және талдау құралдарын таңдау жүйесі қарастырылды. Бағалау әдістері өте көп болды, SecureTower 5.5 бағдарламалы қамтамасыз ету негізінде мысалдар келтірілді. Әрбір бағдарламаның тәсіл, бағалаудың әртүрлі әдістері бар екенін, кейбірі ISO стандарттарын ұстанатыны, кейбірі өз әдісі бар екендігі анықталды.

Бағдарламалық жасақтаманы қарай отырып, салыстыру кестесі түрінде қорытынды жасалып, осы бағдарламамен жұмыс барысында, лайықты және кемшіліктер анықталды.

Ақпаратты қорғау міндеттерін шешу тиімділігін арттыру үшін тиісті компаниялардың мамандарының алдында ақпараттық жүйелер ресурстарының қауіпсіздік тәуекелдерін бағалаудың қазіргі бар құралдарын таңдау немесе жаңа құралдарын әзірлеу туралы мәселе туындайды.

Тиісті таңдау немесе әзірлеу процесін тиімді ұйымдастыру үшін тәуекел сипаттамаларын толық көрсету қажет. Осыған байланысты жұмыста ақпараттық қауіпсіздік саласы үшін тәуекелдің көптеген базалық сипаттамалары анықталған.

Осының негізінде берілген сәйкестендіруші және бағалау сипаттамаларын тұрақты интеграцияланған кортеж моделі түрінде көрсету ұсынылады. Практикада мұндай модельді қолданыстағы құралдарды таңдауды іске асыру үшін және тәуекелдерді бағалаудың жаңа жүйелерін құру кезінде әзірлеушілерге көмек көрсету үшін тиісінше қолданылатын талдамалық және синтетикалық екі жеке кортежге бейнелеу түрінде пайдалану ұсынылады.

Қысқартулар тізімі

ISO (International Organization for Standardization) – стандарттарды шығарумен айналысатын халықаралық ұйым

CRAMM (the UK Goverment Risk Analysis and Managment Method) – бұл ақпараттық жүйелердің өмірлік циклінің барлық сатыларында тәуекелдерді талдау есептерін шешуге мүмкіндік беретін өте қуатты және әмбебап құрал

COBIT (Control Objectives for Information and Related Technologies) – ақпараттық технологияларды басқару әдіснамасы

COBRA (Consultative Objective and Bi-Functional Risk Analysis) – тәуекелдерді талдау және bs7799 стандартына сәйкестікті бағалау құралы

ЭЕМ – электрондық есептеуіш машина

АҚ – ақпараттық қауіпсіздік

АЖ – ақпараттық жүйе

ТЖ – технология жүйесі

АТ – ақпараттық технологиялар

ДК – дербес компьютер

БҚ – Бағдарламалық қамтамасыз ету

БҚ – бағдарламалық құралдар

БӨ – бағдарламалық өнім

ҚҚС – қосылған құн салығы

АҚЖ – ақпаратты қорғау жүйесі

НҚ – негізгі қорлар

ДБ – деректер базасы

ТД – тәуекел деңгейі

ЖЭСЖН – жанама электромагниттік сәулелену және нысаналар

ЕТ – есептеу техникасы

РК – рұқсатсыз кіру

Әдебиеттер тізімі

1 Шаньгин, В.Ф. Информационная безопасность и защита информации / В.Ф. Шаньгин. - М.: ДМК, 2014. - 702 с.

2 Малюк, А.А. Информационная безопасность: концептуальные и методологические основы защиты информации / А.А. Малюк. — М.: ГЛТ, 2016. — 280 с.

3 Барсуков В.С., Водолазний В.В. Современные технологии безопасности. - М.: «Нолидж», 2000. - 496 с.

4 Хорев, П.Б. Программно-аппаратная защита информации: Учебное пособие / П.Б. Хорев. - М.: Форум, 2013. - 352 с.

5 Информационная технология. Методы защиты.: BS ISO/IEC 27005:2002.

6 П. П. Бескид, П. И. Силин Управление информационными рисками : базовые понятия, классификация, стандартизация - М.: «Нолидж», 2001.- 356 с.

7 Симонов С.В. Методология анализа рисков в информационных системах // Конфидент. Защита информации. - №1. - 2008. - С. 72-76.

8 Симонов С.В. Анализ рисков в информационных системах. Практические аспекты // Конфидент. Защита информации. - №2. - 2001. - С. 48-53.

9 Байдешев А.И. Информационные риски: оценка рисков / / Information security (Информационная безопасность) -2004. – №6 – Б. 18

10 Ақпараттық тәуекелдерді талдауға шолу. URL: https://studwood.ru/1756276/informatika/analiz_informatsionnyh_riskov.html (кіру уақыты 15.04.2019)

11 CRAMM тәуекелдерін талдау жүйесіне шолу. URL: https://studref.com/325288/informatika/programmnoe_obespechenie_otsenki_riskov_informatsionnoy_bezopasnosti. html (кіру уақыты 19.04.2019)

12 Ломаков Ю. А. Методики оценивания рисков и их программные реализации в компьютерных сетях // Молодой ученый. — 2013. — №2. — С. 43-46. — URL https://moluch.ru/archive/49/6279/ (кіру уақыты: 01.05.2019).

13 Falcongaze Secure Tower бағдарламалық өніміне шолу. URL: https://falcongaze.ru/ (кіру уақыты 19.04.2019)

14 Бекишева А.И. Методические указания к выполнению экономической части дипломной работы для бакалавров специальности 5В0703 - Информационные системы – Алматы: АУЭС; 2013. –24 с.

15 Вербовецкий А.А. Основы компьютерных технологий и современные ПК. - М.: АЛЕКС, 2002. - 264 с.