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

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

ДИПЛОМДЫҚ ЖОБА

Тақырыбы: «INFINITE VIP GROUP» ЖШС-нің кеңсесіне бөгде енуден және бұзудан ақпараттық қорғауды әзірлеу

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

Алматы 2020

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

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

Дипломдық жобаны орындауға берілген

ТАПСЫРМА

Студент: Омарова Гұлбану Бағдатқызы
(аты-жөні)

Жобаның тақырыбы: “INFINITE VIP GROUP» ЖШС-нің кеңсесіне бөгде енуден және бұзудан ақпараттық қорғауды әзірлеу

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

Аяқталған жұмысты тапсыру мерзімі: «____»_____ 2020 ж.

Жобаға алғашқы деректер (талап етілетін зерттеу (жоба) нәтижелерінің параметрлері және зерттеу нысанының алғашқы деректері): _____
2.8 ГГц кем емес тактілік жиілігі бар Процессор
Жедел жады кемінде 4 Гигабайт
1024 Мбайттан кем емес бейне карта
Монитордың рұқсаты кемінде 1600х1200 пикс
Windows 7 операциялық жүйесі немесе одан кейінгі нұсқасы
Антивирустық бағдарлама Dr.Web
_____
_____
_____

Диплом жобасындағы әзірленуі тиіс мәселелер тізімі немесе диплом жобасының қысқаша мазмұны:
Кіріспе
1.Компанияның қызметі мен ұйымдық құрылымын зерттеу
2. Зерттеу тапсырмаларын қою
3. Ұйымдастыру шаралары
4. Техникалық және физикалық қорғау
5. Өміртіршілік қауіпсіздігі бөлім
6.Ақпараттық қауіпсіздіктің тәуекелдерін есептеу
Қорытынды
Әдебиеттер тізім

Графикалық материалдардың (міндетті түрде дайындалатын сызбаларды көрсету) тізімі:

Компанияның қызметі мен ұйымдық құрылымын зерттеу_____
“INFINITE VIP GROUP» компаниясының үй-жайлары мен техникалық архитектурасын талдау_____
“INFINITE VIP GROUP» компаниясымен өңделетін бағдарламалық архитектураны және деректерді талдау_____
Қауіпсіздікті ықтимал бұзушының моделін әзірлеу_____
«INFINITE VIP GROUP» компаниясының қауіпсіздік қатерлері мен осалдықтарын талдау_____
«INFINITE VIP GROUP» компаниясының ақпараттық қорғалуын қамтамасыз ету принциптері_____
Ұйымдастыру шаралары_____
Техникалық және физикалық қорғау_____
Анықталған өзекті қатерлерді бейтараптандыру мақсатында ақпаратты қорғау шараларын әзірлеу_____
Тарау бойынша қорытындылар_____

Негізгі ұсынылатын әдебиеттер:

1. "Ақпарат, ақпараттық технологиялар және ақпаратты қорғау туралы" 2006 жылғы 27 шілдедегі № 149-МЗ Мемлекеттік заң //[Электрондық ресурс], кіру режимі: http://www.consultant.kz/document/cons_doc_LAW _61798 /(өтініш берілген күні: 15.01.2020).
2. Чукарин А.В. Бизнес-процессы и информационные технологии в управлении современной инфокоммуникационной компанией / А.В. Чукарин. - М.: Альпина Паблишер, 2016. - 512 с.
3. Жидко Е.А. Информационные риски как аргумент безопасного и устойчивого развития организаций / Е.А. Жидко, Л.Г. Попова // Информация и безопасность, 2010. – №4. – С. 543–552.
4. "Дербес деректер туралы" МЗ: Қазақстан Республикасының 2006 жылғы 27 шілдедегі N 152-ФЗ Мемлекеттік заңы / / [Электрондық ресурс], кіру режимі: http://www.consultant. kz/document/cons_doc_LAW_61801 / (өтініш берген күні: 15.01.2020).

Жоба бойынша жобаның бөлімдеріне қатысты белгіленген кеңесшілер

Бөлімдері	Кеңесшілері	Мерзімі	Қолы
Ө.Т.Қ.Н.	Жандаулетова Ф.Р.	13.04.2020ж	
Негізгі бөлім	Шайкулова А.А.	03.03.2020ж	
Есептеу техникасы	Шайкулова А.А.	12.04.2020ж	
А.Қ.Т.Е.	Дмитриева М.В.	20.04.2020ж	
Нормабақылаушы	Альмуратова К.Б.	02.06.2020ж	

Диплом жобасын дайындау
КЕСТЕСІ

Бөлімдердің атауы, әзірленетін мәселелердің тізімі	Ғылыми жетекшіге ұсыну мерзімдері	Ескерту
1. Компанияның қызметі мен ұйымдық құрылымын зерттеу	25.02. 2020ж.	
2. “INFINITE VIP GROUP» компаниясының үй-жайлары мен техникалық архитектурасын талдау	25.02. 2020ж.	
3. Зерттеу тапсырмаларын қою	25.02. 2020ж.	
4. Қауіпсіздікті ықтимал бұзушының моделін әзірлеу	30.04. 2020ж.	
5. Тарау бойынша қорытындылар	30.04. 2020ж.	
6. Ұйымдастыру шаралары	30.04. 2020ж.	
7. Техникалық және физикалық қорғау	30.04. 2020ж.	
8. Анықталған өзекті қатерлерді бейтараптандыру мақсатында ақпаратты қорғау шараларын әзірлеу	30.04. 2020ж.	
9. Өміртіршілік қауіпсіздігі бөлімі	10.05. 2020ж.	
10. Есептеу бөлімі	10.05. 2020ж.	
11.А.Қ.Т.Е.	10.05. 2020ж.	
12. Қорытынды	20.05.2020ж.	

Тапсырманың берілген уақыты «25» ақпан 2020 ж.

Кафедра меңгерушісі: _____ (Бердибаев Рат Шиндалиевич)
(қолы) (аты-жөні)

Жобаның
ғылыми жетекшісі: _____ (Шайкулова Актоты Алиевна)
(қолы) (аты-жөні)

Орындалатын тапсырманы
қабылдаған студент: _____ (Омарова Гүлбану Бағдатқызы)
(қолы) (аты-жөні)

Аңдатпа

Бұл дипломдық жобада «INFINITE VIP GROUP» ЖШС-нің кеңсесіне бөгде енуден және бұзудан ақпараттық қорғауды әзірлеу жүргізілді. Жұмыста теориялық және жүйелік талдау әдістері, сондай-ақ аналитикалық модельдеу әдістері қолданылады. «INFINITE VIP GROUP» компаниясының үй-жайлары мен техникалық архитектурасы, өңделетін бағдарламалық архитектура және деректер талданды. Қауіпсіздікті ықтимал бұзушының, техникалық және физикалық қорғау моделі құрастырылды.

Анықталған өзекті қатерлерді бейтараптандыру мақсатында ақпаратты қорғау шаралары әзірленді. Жұмыстың практикалық маңыздылығы және оның нәтижелері толығымен қарастырылды.

Аннотация

В рамках данного дипломного проекта была разработана разработка средств защиты информации от вторжений и вторжения в офис ТОО «INFINITE VIP GROUP». В работе использованы методы теоретического и системного анализа, а также методы аналитического моделирования. Были проанализированы помещения и техническая архитектура, программная архитектура и данные компании «INFINITE VIP GROUP». Разработана модель технической и физической защиты потенциальных злоумышленников.

Меры информационной безопасности были разработаны для нейтрализации выявленных угроз. Практическая значимость работы и ее результаты были подробно рассмотрены.

Annotation

Within the framework of this diploma project, the development of means of protecting information from intrusions and intrusions into the office of «INFINITE VIP GROUP» LLP was developed. The methods of theoretical and system analysis, as well as methods of analytical modeling are used in the work. The facilities and technical architecture, software architecture and data of the «INFINITE VIP GROUP» company were analyzed. A model of technical and physical protection of potential attackers has been developed.

Information security measures have been developed to neutralize identified threats. The practical significance of the work and its results were examined in detail.

МАЗМҰНЫ

ТАПСЫРМА 2
БЕЛГІЛЕР МЕН ҚЫСҚАРТУЛАР 7
Кіріспе.....8
1 Компанияның қызметі мен ұйымдық құрылымын зерттеу 10
1.1 «INFINITE VIP GROUP» компаниясының үй-жайлары мен техникалық архитектурасын талдау 13
1.2 «INFINITE VIP GROUP» компаниясымен өңделетін бағдарламалық архитектураны және деректерді талдау 15
1.3 «INFINITE VIP GROUP» компаниясының үй-жайлары мен ақпараттық жүйелерін ақпараттық қорғаудың ағымдағы деңгейін бағалау. 20
1.4 Зерттеу тапсырмаларын қою 22
2 «INFINITE VIP GROUP» КОМПАНИЯСЫНЫҢ ҮЙ-ЖАЙЛАРЫ МЕН АҚПАРАТТЫҚ ЖҮЙЕЛЕРІНІҢ АҚПАРАТТЫҚ ҚАУІПСІЗДІГІН БҰЗУШЫНЫҢ ЖӘНЕ ӨЗЕКТІ ҚАУІПТЕРДІҢ ҮЛГІЛЕРІН ӘЗІРЛЕУ 23
2.1 Қауіпсіздікті ықтимал бұзушының моделін әзірлеу 23
2.2 «INFINITE VIP GROUP» компаниясының қауіпсіздік қатерлері мен осалдықтарын талдау 26
2.3 «INFINITE VIP GROUP» компаниясының ақпараттық қауіпсіздігі қатерлерінің өзектілігін бағалау.....31
2.4 «INFINITE VIP GROUP» компаниясының ақпараттық қорғалуын қамтамасыз ету принциптері 35
2.5 Тарау бойынша қорытындылар 36
3. «INFINITE VIP GROUP» КОМПАНИЯСЫНЫҢ ҮЙ-ЖАЙЛАРЫ МЕН АҚПАРАТТЫҚ ЖҮЙЕЛЕРІН АҚПАРАТТЫҚ ҚОРҒАУ ДЕҢГЕЙІН АРТТЫРУ БОЙЫНША ҰСЫНЫМДАРДЫ ӘЗІРЛЕУ 37
3.1Ұйымдастыру шаралары.....38
3.2Техникалық және физикалық қорғау….....
3.3 Анықталған өзекті қатерлерді бейтараптандыру мақсатында ақпаратты қорғау шараларын әзірлеу 44
3.4 Тарау бойынша қорытынды.....52
4 Өмір-тіршілік қауіпсіздігі.....55
5 Ақпараттық қауіпсіздік тәуекелдері.....63
5.1 Ақпараттық қауіпсіздік тәуекелдерін талдау 63
5.2 Есептеу бөлім 65
Қорытынды.....78
Әдебиеттер тізімі.....79
В қосымшасы.....82

БЕЛГІЛЕР МЕН ҚЫСҚАРТУЛАР

АЖО - автоматтандырылған жұмыс орны
ДҚ - деректер қоры
АҚ - ақпараттық қауіпсіздік
АЖ - ақпараттық жүйе
БА - бақыланатын аймақ
ЖЕЖ - жергілікті есептеу желісі
РК - рұқсатсыз кіру
ДД - дербес деректер
БҚЕ - бағдарламалық қамтамасыз ету
АҚЖ - ақпаратты қорғау жүйесі
АҚҚ - ақпаратты қорғау құралы
ТҚ - техникалық құралдар

Кіріспе

Қоғам дамуының қазіргі кезеңіне ақпараттандырудың және ақпараттық технологияларды жетілдірудің үздіксіз процесі тән. Адам өмірінің барлық салаларына ақпараттық технологияларды енгізумен ақпараттық қауіпсіздік мәселелері жыл сайын күрделі және көп қырлы болып келеді. Жаңа мүмкіншіліктерін ашу алдында адам жаңғырту әр түрлі процестерін, сондай-ақ жұмыс сапасы мен тиімділігін арттыру, ақпараттық инфрақұрылымға жүктеледі елеулі сақталуына және ақпарат қауіпсіздігі [3**Error! Reference source not found.**].

Бүгінгі таңда өзекті мәселелердің бірі – осындай инфрақұрылымдарды ақпараттық қорғаудың жан-жақты қамтамасыз етілуі. Ақпараттық қауіпсіздік қатерлерінің және оларды іске асыру тәсілдерінің саны үздіксіз өсуімен байланысты, ақпараттық қорғау деңгейін арттыру бойынша ұсынымдар әзірлеу өте қажетті іс-шара болып табылады [3].

Коммерциялық ұйымдар ерекшелік болып табылмайды. Осы коммерциялық инфрақұрылымдардың бүтіндігін бұзу, жойылуы немесе ұрлануы әр түрлі ауқымдағы залал келтіруге әкеп соқтыруы және қаржылық шығындар мен әкімшілік жауапкершілікпен ғана емес, сондай-ақ бедел үлесінің жоғалуына да қауіп төндіруі мүмкін. Осы жұмыс шеңберінде «INFINITE VIP GROUP» компаниясының үй-жайлары мен деректерді өңдеудің ақпараттық жүйелері басты қызығушылық тудырады, оның негізгі қызмет түрі тоғандар мен басқа да су қоймаларына қызмет көрсету үшін жабдықтарды іске асыру болып табылады [0].

Басқаша айтқанда, коммерциялық инфрақұрылымдардың қауіпсіздігін қамтамасыз ету шеңберінде «» компаниясының үй-жайлары мен ақпараттық жүйелері қауіпсіздігінің жеткілікті деңгейін, ұйымның үздіксіз жұмыс істеуін, сондай-ақ ішкі және сыртқы қауіптерді іске асырудан болатын тәуекел деңгейін төмендетуді қамтамасыз ететін ақпараттық қорғауды әзірлеу қажеттілігі туындайды [0].

Кілттік сөздер: ақпараттық қорғау, рұқсат етілмеген қол жеткізу, құпия ақпарат, дербес деректер, қауіпсіздік қатері.

Зерттеу объектісі «INFINITE VIP GROUP» компаниясының үй-жайлары мен ақпараттық жүйелері болып табылады.

Зерттеу пәні «INFINITE VIP GROUP» компаниясының үй-жайлары мен ақпараттық жүйелерін қорғаудың кешенді жүйесі болып табылады.

Жұмыстың мақсаты «INFINITE VIP GROUP» компаниясының үй-жайлары мен ақпараттық жүйелерін ақпараттық қорғау деңгейін арттыру болып табылады. Көрсетілген мақсатқа қол жеткізу үшін мынадай міндеттерді шешу болжанады:

1. Ақпараттық қорғау объектісі ретінде «INFINITE VIP GROUP» компаниясының қызметіне талдау жүргізу;
2. «INFINITE VIP GROUP» компаниясының үй-жайлары мен ақпараттық жүйелерін ақпараттық қорғаудың ағымдағы деңгейін зерттеу;

3. «INFINITE VIP GROUP» компаниясының үй-жайлары мен ақпараттық жүйелерінің қауіпсіздік қатерлері мен осалдықтарына талдау жүргізу;

4. «INFINITE VIP GROUP» компаниясының үй-жайлары мен ақпараттық жүйелері үшін тәртіп бұзушының және қауіпсіздіктің өзекті қатерлерінің үлгілерін әзірлеу;

5. «INFINITE VIP GROUP» компаниясының үй-жайлары мен ақпараттық жүйелерін ақпараттық қорғау деңгейін арттыру бойынша ұсыныстар әзірлеу.

Жұмыста теориялық және жүйкелік талдау әдістері, сондай-ақ аналитикалық модельдеу әдістері қолданылады.

Жұмыстың практикалық маңыздылығы оның нәтижелерін коммерциялық ұйымдардың коммерциялық инфрақұрылымдардың деректерін өңдеуге қатысты федералдық заңдар мен басқа да нормативтік құжаттардың талаптарын ескеретін ақпаратты қорғаудың қазіргі заманғы кешенді жүйелерін жобалау үшін пайдалануы мүмкін.

Жұмыс кіріспеден, үш тараудан және қорытындыдан тұрады. Бірінші тарау «INFINITE VIP GROUP» компаниясының қызметін ұйымның ақпараттық жүйелерінде өңделетін үй-жайлар мен деректерді нақтылауды есепке ала отырып жарықтандыруға арналған.

Екінші тарау «INFINITE VIP GROUP» компаниясының үй-жайлары мен ақпараттық жүйелері үшін тәртіп бұзушының модельдерін және қауіпсіздіктің өзекті қатерлерін әзірлеу туралы ақпаратты қамтиды.

Үшінші тарау ұйымдастыру шараларын, техникалық және физикалық қорғауды енгізу бөлігінде «INFINITE VIP GROUP» компаниясының үй-жайлары мен ақпараттық жүйелерін ақпараттық қорғау деңгейін арттыру бойынша ұсыныстарды әзірлеу туралы ақпаратты қамтиды.

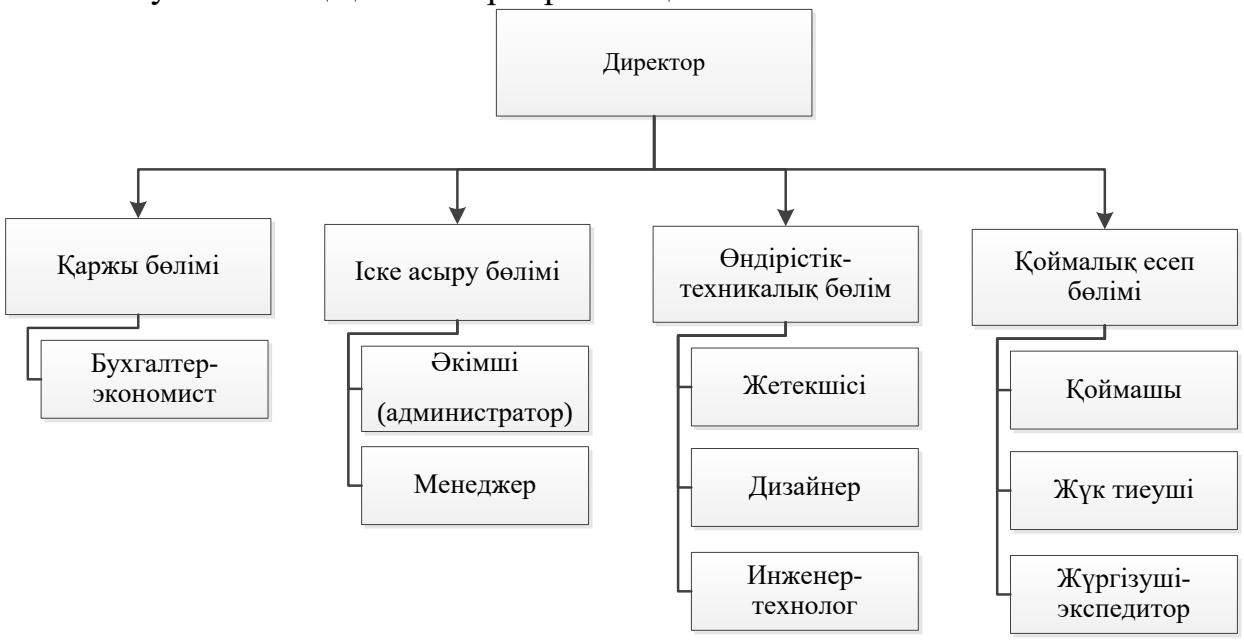
1.1 Компанияның қызметі мен ұйымдық құрылымын зерттеу

“INFINITE VIP GROUP» компаниясы 2005 жылы өндірістік-сауда ұйымы ретінде құрылған. Компания қызметінің негізгі түрі тоғандар мен басқа да су қоймаларына қызмет көрсетуге арналған жабдықтарды сату болып табылады. «INFINITE VIP GROUP» компаниясының қызметкерлері су ортасында: тоғандарда, жүзу және тірі балық су айдындарында, сондай-ақ бассейндерде күрделі техникалық шешімдерді іске асырады. «INFINITE VIP GROUP» компаниясының қызмет саласын келесі тізіммен сипаттауға болады:

1. Қажетті жабдықты жобалау, таңдау және құрастыру;
2. Тоғандар мен су айдындарын әзірлеу және салу;
3. Тоғандар мен су қоймаларына қызмет көрсету және күтім жасау;
4. Тоғандар мен су қоймаларын салу мен қызмет көрсетудің күрделі мәселелерін шешуге, сондай-ақ су құрылыстарында пайдалану шығындарын азайтуға мүмкіндік беретін жаңа өнімдерді, әдістемелер мен технологияларды әзірлеу (мысалы, тазалықты тұрақтандыруға мүмкіндік беретін су қоймаларын жетілдіру процесін жеделдетудің бірегей технологиясы);
5. Еуропадан Қазақстанға озық жабдықтарды импорттау.

«INFINITE VIP GROUP» компаниясы қызметкерлерінің жұмыс орындары ұйым аумағында орналасқан, мекен-жайы: Алматы қаласы, Клочков көшесі, 66 үй, ғимараттың бірінші қабатында жеке кіретін есігі бар.

«INFINITE VIP GROUP» компаниясының ұйымдық құрылымы бірқатар бөлімшелерден тұрады және 1-суретте көрсетілген. Жоғарыда көрсетілген мекен-жай бойынша қаржы және өндірістік-техникалық бөлімдер, сондай-ақ сату бөлімі, компания басшылығы және кеңсеге тікелей жақын орналасқан қоймадан тауар-материалдық құндылықтарды беруге жауап беретін қоймалық есепке алу бөлімінің қызметкері орналасқан.



1.1 сурет– «INFINITE VIP GROUP» компаниясының ұйымдық құрылымы

Қоймаларды есепке алу бөлімінің қалған қызметкерлері географиялық жағынан алыстағы ғимаратта, Алматы қаласы, Шемякин көшесі, 201 үй мекен-жайы бойынша орналасқан, онда «INFINITE VIP GROUP» компаниясының негізгі қоймасы орналасқан.

Компания клиенттерімен бастапқы өзара іс-қимыл менеджерінің немесе компания әкімшісінің күшімен жүзеге асырылады. Жобаларды әзірлеу және қажетті жабдықтарды талдау үшін бірнеше тапсырыс бере алатын дизайнер мен инженер-технолог жұмыс істейді. Дизайнер жобаларды үлгілеумен жұмыс істейді, ал инженер барлық өндірістік операциялармен айналысады – материалдар мен жабдықтарды дайындаудан бастап Тапсырыс берушінің объектісінде монтаждауға және орнатуға дейін.

Барлық материалдар мен бөлшектер сенімді жеткізушілерден, мердігерлерден, соның ішінде шетелдік материалдардан сатып алынатындығын атап өткен жөн. Персоналдың әрбір бөлімшенің тиісті функцияларын орындауды қамтамасыз етуге мүмкіндік беретін жұмысқа қажетті барлық құжаттары мен тиісті біліктілігі бар. «INFINITE VIP GROUP» компаниясының құрылымындағы негізгі кіші жүйелерді бөліп аламыз және олардың функцияларын 1.2-суретте сипаттаймыз.

Басшылық (директор)	•“INFINITE VIP GROUP” компаниясының қызметін ұйымдастыруды құрылымдық бөлімшелерді үйлестіру және ұйымдастыру. •Бюджетті қалыптастыру, “INFINITE VIP GROUP” компаниясының шоттарын төлеуді келісу. •Баға және тауар саясатын әзірлеу және енгізу.
Қаржы бөлімі (бухгалтер-экономист)	•Директордың сұрауы бойынша жоспарлы және қаржылық есептерді дайындау. •Директормен төлем шоттарын келісіп, мердігерлерге және мемлекеттік органдарға төлем жасау. •Банк және мемлекеттік мекемелермен жұмыс істеу. •Әкімші ұсынған деректер бойынша қызметкерлерге жалақыны есептеу және салу(жіберу).
Іске асыру бөлімі (әкімші, менеджер)	•Жұмыс уақыты табелін жүргізуді және қаржы бөліміне (әкімшіге) ақпарат беруді қоса алғанда, персоналды басқару. •Сатып алу үшін өндірістік-техникалық бөлім ұсынған ақпаратты жинақтау және талдау (әкімші). •Зергерлік бұйымдарды дайындау үшін материалдар мен жинақтаушылардың тапсырыстарын қалыптастыру, кейіннен шоттарды бухгалтерияға (әкімші) беру. •Клиентті қарсы алу, жобалар мен жабдық үлгілерін таңдауда көмек көрсету (менеджер). •“INFINITE VIP GROUP” (сату жөніндегі менеджер) компаниясының клиенттеріне тапсырыс қабылдау және қызмет көрсету. •Жобаны келісуді қоса алғанда, клиентпен мәміле жүргізудің толық циклын ұйымдастыру.
Өндірістік-техникалық бөлім (басшы, дизайнер, инженер-технолог)	•Заманауи жобаларды әзірлеу (дизайнер). •Өндірістік-техникалық қызметті үйлестіру (басшы). •Жабдықты нақты жобаның қажеттілігіне қарай өңдеу (инженер-технолог). •Әкімшіге және бухгалтер-экономистке жұмсалған материалдар мен жинақтаушылар (инженер-технолог) туралы есептер дайындау.
Қоймалық есепке алу бөлімі (қоймашы, жүк тиеуші, жүргізуші-экспедитор)	•Тауарлар мен жинақтаушылардың (жүк тиеуші) тиелуін / түсірілуін ұйымдастыру. •Жеткізілетін тауарлар мен жинақтаушылардың (қоймашы) тұтастығын, тауарлық түрін және сапасын өз деңгейінде бақылау. •Тауарларды және жинақтаушы заттарды жеткізу (жүргізуші-экспедитор).

1.2 сурет - «INFINITE VIP GROUP» компаниясы бөлімшелері функцияларының тізімі

1.2 «INFINITE VIP GROUP» компаниясының үй-жайлары мен техникалық архитектурасын талдау

Бас кеңсенің, “INFINITE VIP GROUP» компаниясының үй-жай схемасы 3.1-суретте көрсетілген.

Компанияның үй-жайлары өрт және күзет сигнализациясының техникалық құралдарымен жабдықталған. Бірінші қабаттағы кабинеттердің терезелерінде болат торлар бар. Түнгі уақытта “INFINITE VIP GROUP» компаниясының үй-жайлары кілтке жабылады және бөгде ұйымның күзет пультіне қосылған дабылға қойылады.

«INFINITE VIP GROUP» компаниясы қызметкерлерінің барлық автоматты жұмыс орындары (АЖО) Интернетке шығатын жергілікті желіге біріктірілген. Желі топологиясы 3.2-суретте көрсетілген. Бұл топология «INFINITE VIP GROUP» компаниясының желілік инфрақұрылымының негізгі құрылымдық элементтерін, соның ішінде алыстағы қойманың қоймашысының АЖО көрсетеді.

Ұйымның жергілікті желісінің құрамына 9 қызметкерлердің АЖО кіреді. Желіні басқару «INFINITE VIP GROUP» компаниясының өндірістік-техникалық бөлімінде орнатылған серверлік жабдықты (HP ProLiant ML30 Gen9) пайдалану арқылы жүзеге асырылады.

Басып шығару және сканерлеу функцияларын жүзеге асыру үшін ұйымның жергілікті желісінің құрамына 5 дана мөлшерінде КФҚ (Brother DCP-7057WR) кіреді. 1.1 кестеде «INFINITE VIP GROUP» компаниясы қызметкерлерінің АЖО тізімі және жергілікті желіге кіретін қосалқы жабдық ұсынылған.

1.1 кесте – «INFINITE VIP GROUP» компаниясы қызметкерлерінің жабдықтар тізімі

№	Белгісі	АЖО орналасуы	Қосымша жабдық
1	ДК1	Жетекшінің кабинеті	DVD-ROM, алмалы-салмалы қатты диск, USB қосқыштары
2	ДК2	Қаржы бөлімі	DVD-ROM, алмалы-салмалы қатты диск, USB қосқыштары
3	ДК3	Бас кеңсе қоймасы	Жоқ
4	ДК4	Іске асыру бөлімі	USB қосқыштары
5	ДК5	Іске асыру бөлімі	USB қосқыштары
6	ДК6	Өндірістік-техникалық бөлім	DVD-ROM, USB қосқыштары
7	ДК7	Өндірістік-техникалық бөлім	DVD-ROM, USB қосқыштары
8	ДК8	Өндірістік-техникалық бөлім	DVD-ROM, USB қосқыштары

1.1 кестенің жалғасы

9	ДК9	Өндірістік-техникалық бөлім	DVD-ROM, USB қосқыштары
10	ДК10	Қоймалық есеп бөлімі	Жоқ
11	КФҚ1	Жетекшінің кабинеті	ДК1-ге қосылған
12	КФҚ2	Қаржы бөлімі	ДК2-ге қосылған
13	КФҚ3	Бас кеңсе қоймасы	ДК4-ке қосылған
14	КФҚ4	Іске асыру бөлімі	ДК5-ке қосылған
15	КФҚ5	Өндірістік-техникалық бөлім	ДК6-ға қосылған
16	КФҚ6	Өндірістік-техникалық бөлім	ДК9-ға қосылған
17	КФҚ7	Қоймалық есеп бөлімі	ДК10-ға қосылған

«INFINITE VIP GROUP» компаниясының желілік ресурстарына қол жеткізу үшін қол жеткізу құқықтарын шектеу саясаты әзірленді және енгізілді. Әрбір қызметкердің компания желісінде бірегей аты, кіру үшін пароль, пайдаланушы мен әкімшіге қол жетімді жеке папка, ұйымның басқа қызметкерлерімен файл алмасу үшін жалпы папкаға кіру мүмкіндігі бар.

Қазіргі уақытта «INFINITE VIP GROUP» компаниясында заманауи техникалық құралдар қолданылады. «INFINITE VIP GROUP» компаниясының техникалық қамтамасыз ету кіші жүйесін келесі тізбемен анықтауға болады:

1. Ақпаратты жинау, тіркеу, жинақтау, өңдеу, бейнелеу, көбейту, жеткізу, сақтау және қауіпсіздігін қамтамасыз етудің техникалық құралдары;
2. Әр түрлі модельді компьютерлер, серверлік және желілік құрылғылар, оргтехника;
3. Телекоммуникациялық техника және байланыс құралдары;
4. Техникалық қамтамасыз ету бойынша мемлекеттік, салалық және корпоративтік стандарттарды қамтитын жалпы жүйелік құжаттама;
5. Техникалық және технологиялық құралдарды жобалаудың, әзірлеудің, енгізудің, сүйемелдеудің және қолданудың барлық кезеңдері бойынша әдістемелік материалдарды қамтитын мамандандырылған құжаттама;
6. Техникалық қамтамасыз етуді орындауға арналған нормативтік–анықтамалық құжаттама.

Аппараттық қамтамасыз етудің техникалық сипаттамалары «INFINITE VIP GROUP» компаниясы қызметкерлерінің функционалдық міндеттерін шешу кезіндегі қажеттіліктерін қанағаттандырады. Қолданылатын АЖО әртүрлі конфигурациясы бар, бірақ келесі ең төменгі параметрлермен шектелген:

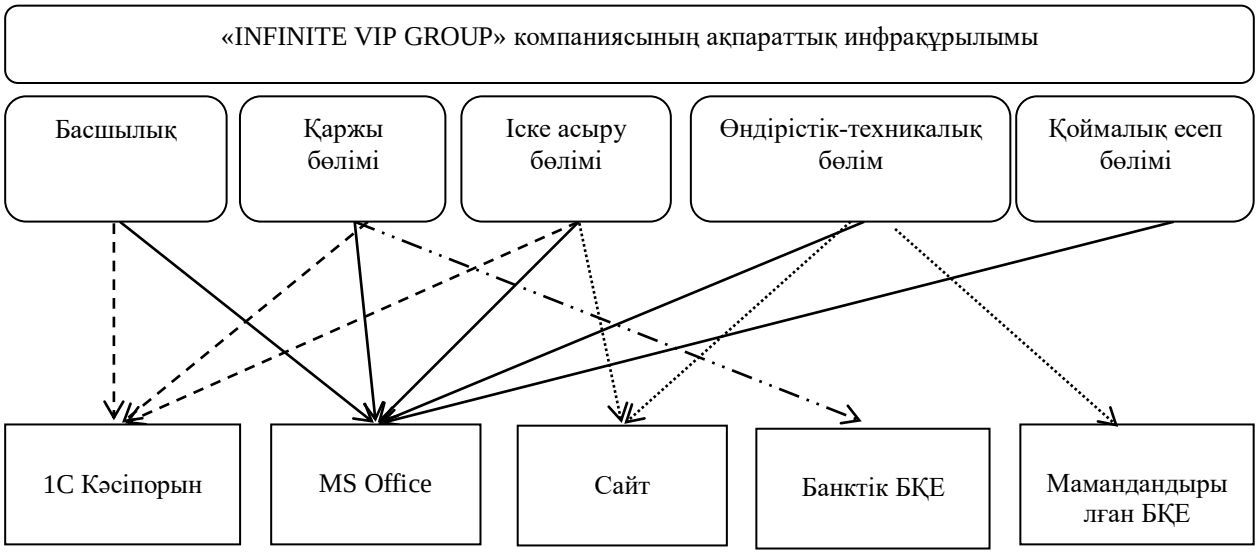
1. 2.8 ГГц кем емес тактілік жиілігі бар Процессор;
2. Жедел жады кемінде 4 Гигабайт;
3. 1024 Мбайттан кем емес бейне карта;
4. Монитордың рұқсаты кемінде 1600x1200 пикс;

5. Windows 7 операциялық жүйесі немесе одан кейінгі нұсқасы;
6. Желілік карта.

Кернеудің қысқа мерзімді іркілістерін өтеу мақсатында аппараттық қамтамасыз етуге электрді ажыратқаннан кейін 30 минут ішінде жүйемен жұмыс істеуге мүмкіндік беретін үздіксіз қоректендіру көздері кіреді. Студия желісінің жұмысын ұйымдастыру үшін switch типті бір концентратор қолданылады.

1.3 «INFINITE VIP GROUP» компаниясымен өңделетін бағдарламалық архитектураны және деректерді талдау

Сонымен қатар, осы жұмыс шеңберінде «INFINITE VIP GROUP» компаниясының қазіргі уақытта қолданылатын бағдарламалық өнімдер мен ақпараттық жүйелерді ескеру қажет. 1.3 суретте «INFINITE VIP GROUP» компаниясының ақпараттық инфрақұрылымының моделі көрсетілген, онда 1С Кәсіпорын бағдарламалық өнімдері (жалақы, Бухгалтерия, қойманы басқару), MS Office, банктік және ұйымның негізгі қызметін қамтамасыз ету үшін қажетті басқа да мамандандырылған бағдарламалық қамтамасыз ету бар. «INFINITE VIP GROUP» компаниясының сату бөлімінің қарамағында клиенттерге ұйымның қызметімен қашықтан танысуға мүмкіндік беретін бірнеше ақпараттық сайттар бар (олардың ішінде негізгі http://www.avangard-aqua.ru).



1.3 сурет - «INFINITE VIP GROUP» компаниясының ақпараттық инфрақұрылымының моделі

Бағдарламалық қамтамасыз ету жиынтығы «INFINITE VIP GROUP» компаниясы қызметінің ерекшелігіне негізделген. Әрбір жұмыс станциясы мен серверде белгілі бір бағдарламалық жасақтама орнатылған:

1. Microsoft Office стандартты бағдарламалары: Excel, Word, PowerPoint, Internet Explorer;

2. Антивирустық бағдарлама Dr.Web;

3. Mozilla Firefox.

Сонымен қатар, «INFINITE VIP GROUP» компаниясының сервері Windows Server 2012 операциялық жүйесімен жабдықталған. Бұл операциялық жүйе заманауи жабдықтармен компьютерлік желілерде серверлерді ұйымдастыруға арналған. Шексіз қосылымдарды қолдайды, жоғары функционалдығы, жылдамдығы және қауіпсіздігі бар.

«INFINITE VIP GROUP» компаниясында өңделетін деректердің жіктемесін келесі тізімге енгізуге болады:

1. Клиенттерге қызмет көрсетуге байланысты ақпарат;
2. «INFINITE VIP GROUP» компаниясының қызметін ұйымдастыру үшін қажетті ақпарат;
3. Жеткізушілермен және контрагенттермен байланысты ақпарат;
4. Компанияның әзірлемелері мен патенттеріне байланысты ақпарат.

Осылайша, «INFINITE VIP GROUP» компаниясының ақпараттық жүйелері жеке деректерді және коммерциялық құпияны қамтитын деректерді өңдейді. Егер коммерциялық құпияны қамтитын деректер салыстырмалы түрде оңай анықтаса («INFINITE VIP GROUP» компаниясында тікелей әзірленген және қолданылатын өнімдер, әдістемелер мен технологиялар), онда дербес деректерді анықтау және қорғауды қамтамасыз ету мәселесі едәуір күрделі.

Дербес деректер жеке тұлғаға (дербес деректер субъектісіне) осындай ақпараттың негізінде белгілі бір немесе анықталатын кез келген ақпаратты білдіреді [1]. «INFINITE VIP GROUP» компаниясында айналымдағы жеке деректерге неғұрлым толық талдау жүргіземіз.

Заңды тұлғалардың сатып алушыларының деректемелері көпшілікке қол жетімді болғандықтан, мұндай ақпаратты қорғау осы зерттеу аясында қарастырылмайды.

«INFINITE VIP GROUP» сату бөлімі мен қаржы бөлімінің функционалдық ерекшелігінің тізбесіне сүйене отырып (1.2 сурет), 1.2-кестеде клиенттердің дербес деректерінің тізбесін анықтаймыз:

1.2 кесте – «INFINITE VIP GROUP» компаниясы клиенттерінің жеке деректері

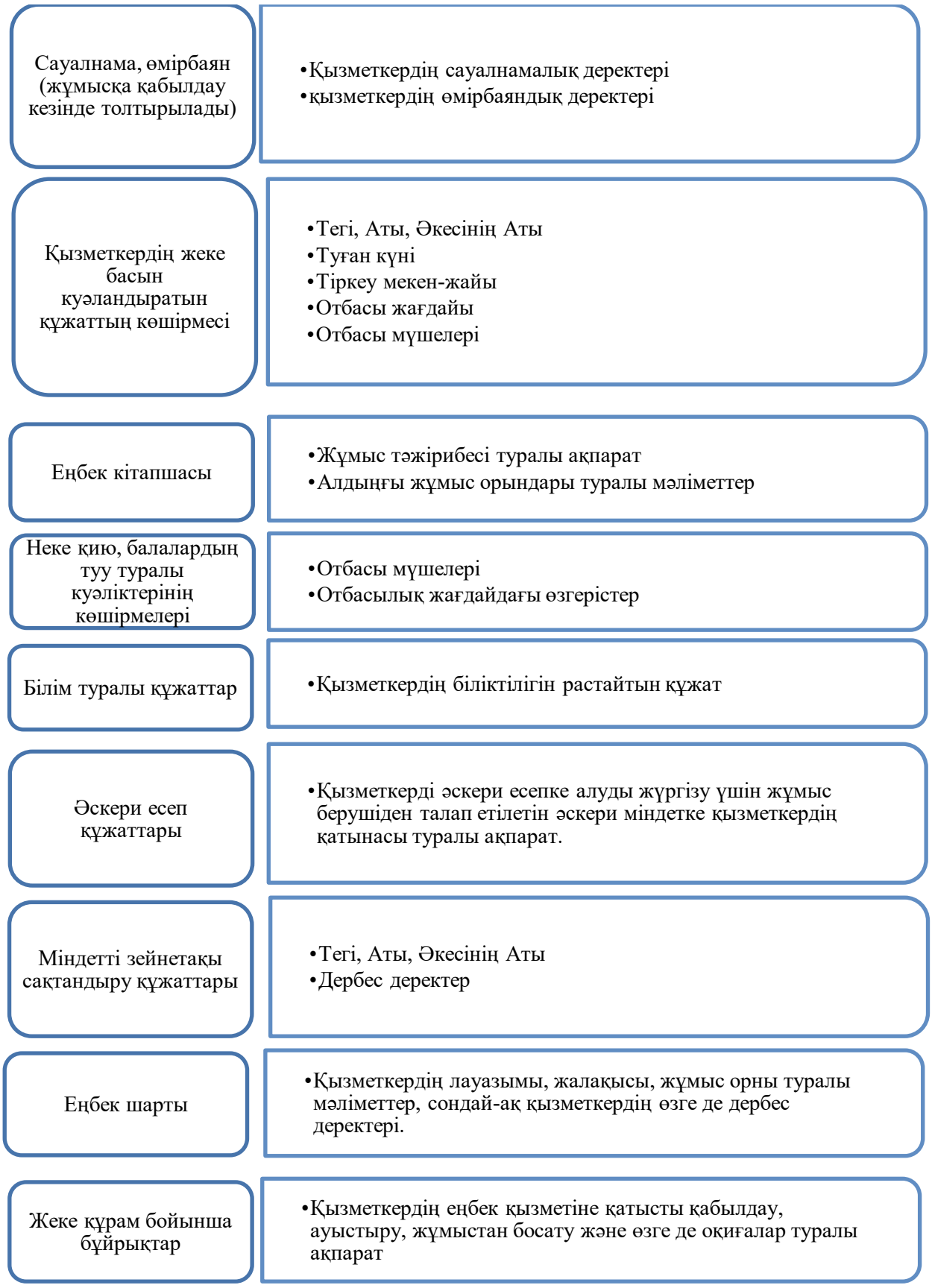
«INFINITE VIP GROUP» компаниясында өңделетін құжат	Дербес деректерді қамтитын мәліметтер
Жабдықты орнатуға клиенттің өтінімі	Тегі, Аты, Әкесінің Аты
	Объектінің тұрғылықты мекен-жайы
	Байланыс телефоны
Клиенттің тауарды жөнелтуге өтінімі	Тегі, Аты, Әкесінің Аты
	E-mail

1.2 кестенің жалғасы

	Байланыс телефоны
Клиенттің тұрақты клиенттің картасын алуға өтініші	Тегі, Аты, Әкесінің Аты
	Туған күні
	Паспорттық деректер (паспорттың сериясы, нөмірі, кім және қашан берген)
	Тұрғылықты мекен-жайы
	E-mail
	Байланыс телефоны

«INFINITE VIP GROUP» компаниясы қызметкерлерінің дербес деректері еңбек заңнамасы шеңберінде шарттық қатынастарды орнату үшін пайдаланылады.

Мұндай ақпарат жұмысқа қабылдау, еңбек шартын жасасу үшін қажет. Қаржы бөлімінің қызметі негізінде (1.2-сурет) біз «INFINITE VIP GROUP» компаниясының бухгалтериясында өңделген қызметкерлердің жеке мәліметтерінің тізімін, 1.4-суретте ұсынамыз.



1.4 сурет – «INFINITE VIP GROUP» компаниясының қызметкерлерінің дербес деректерінің тізімі.

Осылайша, «INFINITE VIP GROUP» компаниясының клиенттері мен қызметкерлерінің жеке деректерін өңдеу бойынша операцияларды келесі тізбемен анықтауға болады [1]:

1. Жинау;
2. Жазба;
3. Жүйелеу;
4. Жинақтау;
5. Сақтау;
6. Нақтылау (жаңарту, өзгерту);
7. Алу;
8. Қолдану;
9. Беру (тарату, ұсыну, қол жеткізу);
10. Бұғаттау;
11. Иесіздендіру;
12. Жою;
13. Дербес деректерді жою.

Қазақстан Республикасы 2012 жылғы 1 қарашадағы № 1119 қаулысымен бекітілген дербес деректердің ақпараттық жүйелерінде оларды өңдеу кезінде дербес деректерді қорғауға қойылатын талаптарды ескере отырып, ұйымда анықталған ақпаратты өңдейтін Ақпараттық жүйелер шеңберінде дербес деректердің төрт санаты бөлінеді [**Error! Reference source not found.**].

1.3-кесте – «INFINITE VIP GROUP» дербес деректерін талдау нәтижелері

Дербес деректердің талданатын құрамы	Дербес деректердің санаты
Тегі, аты, әкесінің аты (аты-жөніI)	3
Туған күні	4 (иесіздендірілген)
Паспорттық деректер	2
Тіркеу туралы деректер (тұрғылықты жері/тұрғылықты жері бойынша тіркелген күні мен орнын қамтиды)	3
Лауазымдық жағдайдағы өзгерістер туралы деректер	4 (иесіздендірілген)
ЖСН, сақтандыру медполис нөмірі	3
Қаржылық деректер	4 (иесіздендірілген)

Осылайша, «INFINITE VIP GROUP» компаниясында өңделетін дербес деректерге жүргізілген талдаудан шыға отырып, жұмыста барлық айналымдағы ақпарат санатталған.

Кеңсенен қашықтағы ғимараттағы қойма тек қашықтықтағы қойманың функцияларын орындайды, бұл қойма қорын тез толтыру үшін қажет (клиенттер оны жөнелту үшін келмейді), қашықтағы қоймадағы жеке деректерді қорғауды қамтамасыз ету жеке деректерді өңдеудің болмауына байланысты орынды болып көрінбейді.

«INFINITE VIP GROUP» компаниясының АЖДД-де дербес деректерді өңдеу режимі көп пайдаланушы болып табылады. Өңделетін (бір мезгілде) ДД

көлемі – «INFINITE VIP GROUP»компаниясының қызметкерлері болып табылатын ДД 100 000 субъектісінен кем.

«INFINITE VIP GROUP» компаниясының АЖДД барлық компоненттері бақыланатын аймақтың (БА) ішінде есептеуіш техниканың бір объектісінде орналасқан (3.1-сурет). «INFINITE VIP GROUP» компаниясының АЖДД қаралып отырған Жалпы пайдалану және халықаралық ақпарат алмасу желілеріне қосылмаған болады.

«INFINITE VIP GROUP» компаниясының АЖДД жұмысында келесі техникалық құралдар қолданылады:

1. Дербес деректерді өңдейтін сервер;
2. Автоматтандырылған жұмыс орындары (пайдаланушылардың жұмыс станциялары);
3. ДДАЖ ішінде жеке деректерді беруге қатысатын желілік жабдық;
4. Қосалқы техникалық құралдар мен жүйелер;
5. Принтерлер және көпфункционалды құрылғылар (жергілікті және желілік);
6. Алынатын (иеліктен шығарылатын) ақпарат тасығыштар;
7. Үздіксіз қоректендіру көздері (ҮҚК).

«INFINITE VIP GROUP» компаниясының АЖДД-де ақпаратты өңдеу қол жеткізу құқығын шектей отырып, бірнеше пайдаланушы режимде жүргізіледі. «INFINITE VIP GROUP» компаниясының АЖДД пайдаланушылары тек қана «INFINITE VIP GROUP» компаниясының қаржы бөлімі мен сату бөлімінің қызметкерлері болып табылады.

1.4 «INFINITE VIP GROUP» компаниясының үй-жайлары мен ақпараттық жүйелерін ақпараттық қорғаудың ағымдағы деңгейін бағалау.

Қорғанудың бастапқы деңгейі деп 2008 жылы Қазақстан Республикасы дербес деректердің ақпараттық жүйелерінде оларды өңдеу кезінде дербес деректердің қауіпсіздігінің өзекті қатерлерін анықтау әдістемесіне сәйкес ақпараттық жүйенің барлық техникалық және пайдалану сипаттамаларына байланысты жалпыланған көрсеткіш түсініледі [**Error! Reference source not found.**]. 1.4-кестеде «INFINITE VIP GROUP» компаниясының АЖДД үшін бастапқы қорғаныс деңгейінің сипаттамалары берілген.

1.4-кесте – «INFINITE VIP GROUP» компаниясының бастапқы қорғалу деңгейінің сипаттамасы

Техникалық және пайдалану сипаттамалары		Қорғалу деңгейі
Аумақтық орналастыру бойынша	Бір ғимарат шегінде орналасқан жергілікті АЖДД	Жоғары
Жалпы пайдалану желілерімен	Жалпыға қол жетімді емес АЖДД	Жоғары

1.4 кестенің жалғасы

қосылыстардың болуы бойынша		
Дербес деректер қорының жазбаларымен қоса салынған операциялар бойынша	Жазу, жою, сұрыптау	Орташа
Дербес деректерге қолжетімділікті шектеу бойынша	АЖДД иесі болып табылатын ұйымның қызметкерлері немесе дербес деректердің субъектеріне рұқсат беретін АЖДД	Орташа
Техникалық және пайдалану сипаттамалары		Қорғалу деңгейі
Ақпараттық жүйелерде өзге дербес деректердің басқа да дербес деректер базаларымен қосылыстардың болуы бойынша.	Дербес деректердің бір базасы қолданылатын АЖДД, онда осы АЖДД иесіне – ұйымға тиесілі.	Жоғары
ДД жинақтау (иесіздендіру) деңгейі бойынша	Пайдаланушыға ұсынылатын деректер иесіздендірілген болып табылатын (яғни ДД субъектісін сәйкестендіруге мүмкіндік беретін ақпарат бар) АЖДД.	Төмен
Үшінші тараптың АЖДД пайдаланушыларына алдын-ала өңдеусіз берілген жеке деректер тұрғысынан	Ешқандай ақпарат бермейтін АЖДД.	Жоғары

Қауіпсіздіктің бастапқы дәрежесі ақпарттық жүйелерде өңдеу кезінде жеке деректердің қауіпсіздігіне нақты қауіп-қатерлерді анықтау әдістемесіне сәйкес анықталады [**Error! Reference source not found.**]. Жүргізілген талдауға сүйене отырып, «INFINITE VIP GROUP» компаниясының АЖДД бастапқы қорғаныс деңгейінің "орташа" деңгейіне сәйкес келеді деген қорытынды жасауға болады.

Дербес деректердің қауіпсіздігін қамтамасыз ету үшін қажетті ұйымдастырушылық және техникалық қорғау шараларының кешені Қазақстан Республиксының заңнамасына сәйкес анықталады [**Error! Reference source not found.**,**Error! Reference source not found.**].

Бұл құжатта дербес деректердің қорғалуының төрт деңгейі анықталған, бұл ретте келесі көрсеткіштер ескеріледі:

1. Өзекті қауіптер түрі;
2. Өңделетін дербес деректердің санаты;
3. Ақпараттық жүйеде өңделетін дербес деректер субъектілерінің түрі;
4. Ақпараттық жүйеде өңделетін дербес деректер субъектілерінің саны.

Жоғарыда көрсетілген құжатқа сәйкес жүргізілген талдау нәтижесінде «INFINITE VIP GROUP» компаниясының АЖДД өңдеу кезінде дербес деректердің қорғалуының төртінші деңгейі анықталды.

Ағымдағы коммерциялық құпияны қамтитын деректер қауіпсіздігінің деңгейін қанағаттанарлықсыз деп бағалауға болады. Себебі, компанияда мұндай деректерге қол жеткізу тәртібі мен жария еткені үшін белгіленген жауапкершілік дәрежесі бойынша нақты құжаттама жоқ.

Сонымен қатар, «INFINITE VIP GROUP» компаниясының үй-жайлары қолжетімділікті басқаруды бақылау жүйесімен жабдықталмаған, бұл сондай-ақ персоналдың түрлі санаттарының (басқарушылық, әкімшілік және орындаушылық деңгейлердегі) қол жеткізуін қамтамасыз ету шеңберінде қолайсыз болып табылады.

1.5 Зерттеу тапсырмаларын қою

Осылайша, осы тарауда «INFINITE VIP GROUP» компаниясының қызметі мен ұйымдық құрылымына зерттеу жүргізілді, ол ұйым туралы жалпы ақпаратты зерделеуді, үй-жайларды және бағдарламалық-техникалық архитектураны, сондай-ақ «INFINITE VIP GROUP» компаниясы өңдейтін қолданыстағы ақпараттық жүйелер мен деректерді талдауды қамтиды.

Жүргізілген талдау нәтижелері бойынша «INFINITE VIP GROUP» компаниясының үй-жайлары мен ақпараттық жүйелерін ақпараттық қорғаудың ағымдағы деңгейіне бағалау жүргізілді. Алынған нәтижелер негізінде келесі міндеттерді шешу қажет:

1. «INFINITE VIP GROUP» компаниясының үй-жайлары мен ақпараттық жүйелерінің қауіпсіздік қатерлері мен осалдықтарына талдау жүргізу;
2. «INFINITE VIP GROUP» компаниясының үй-жайлары мен ақпараттық жүйелері үшін тәртіп бұзушының және қауіпсіздіктің өзекті қатерлерінің үлгілерін әзірлеу;
3. «INFINITE VIP GROUP»компаниясының үй-жайлары мен ақпараттық жүйелерін ақпараттық қорғау деңгейін арттыру бойынша ұсыныстар әзірлеу.

2 «INFINITE VIP GROUP» компаниясының үй-жайлары мен ақпараттық жүйелерінің ақпараттық қауіпсіздігін бұзушының және өзекті қауіптердің үлгілерін әзірлеу

2.1 Қауіпсіздікті ықтимал бұзушының моделін әзірлеу

Қауіпсіздік қатерін қауіп көзі мен деректер көзі арасында іске асыру арнасының пайда болуы нәтижесінде іске асырылуы мүмкін. «INFINITE VIP GROUP» компаниясының үй-жайлары мен ақпараттық жүйелеріне Заңды қол жеткізу тұрғысынан барлық тәртіп бұзушылар екі топқа бөлінеді:

1. Сыртқы тәртіп бұзушылар;
2. Ішкі тәртіп бұзушылар [**Error! Reference source not found.**].

Сыртқы зиянкестерге «INFINITE VIP GROUP» үй-жайлары мен ақпараттық жүйелеріне заңды қол жетімділігі жоқ және рұқсатсыз кіру (NSD) арқылы қауіп-қатерді жүзеге асыратын, мысалы, қоғамдық байланыс желілері немесе халықаралық ақпарат алмасу желілері арқылы кіретін тұлғалар жатады. «INFINITE VIP GROUP» компаниясы үшін:

1. Қылмыстық құрылымдар;
2. Зиянкестер немесе сыртқы субъектілер;
3. Бәсекелес ұйымдар;
4. Жосықсыз әзірлеушілер мен жеткізушілер;
5. Бұрынғы қызметкерлер.

Ішкі зиянкестерге «INFINITE VIP GROUP» компаниясының үй-жайлары мен ақпараттық жүйелеріне рұқсаты бар жеке тұлғалар, оның ішінде ұйым қызметкерлерінің өздері жатады. «INFINITE VIP GROUP» компаниясының ішкі зиянкестеріне жатуы мүмкін:

1. «INFINITE VIP GROUP» компаниясының ақпараттық жүйелерінің әкімшілері және қауіпсіздік әкімшілері;
2. «INFINITE VIP GROUP» компаниясының ақпараттық жүйелерін пайдаланушылар;
3. «INFINITE VIP GROUP» компаниясының ақпараттық инфрақұрылымының ресурстары орналасқан үй-жайларға ресми мақсатта рұқсаты бар, бірақ ресурстарға кіру құқығы жоқ қызметкерлер;
4. Қызмет көрсетуші персонал.

«INFINITE VIP GROUP» компаниясының барлық терезелерінде темір торлар бар болғандықтан, кеңсеге кіру заманауи сенімді есіктерді пайдалана отырып жабылады және барлық Үй-жайлар күзет кәсіпорнының пультіне қосылған сигнализациямен жабдықталған, кеңсеге физикалық енуді іске асыратын сыртқы зиянкестер осы жұмыс шеңберінде қызығушылық білдірмейді.

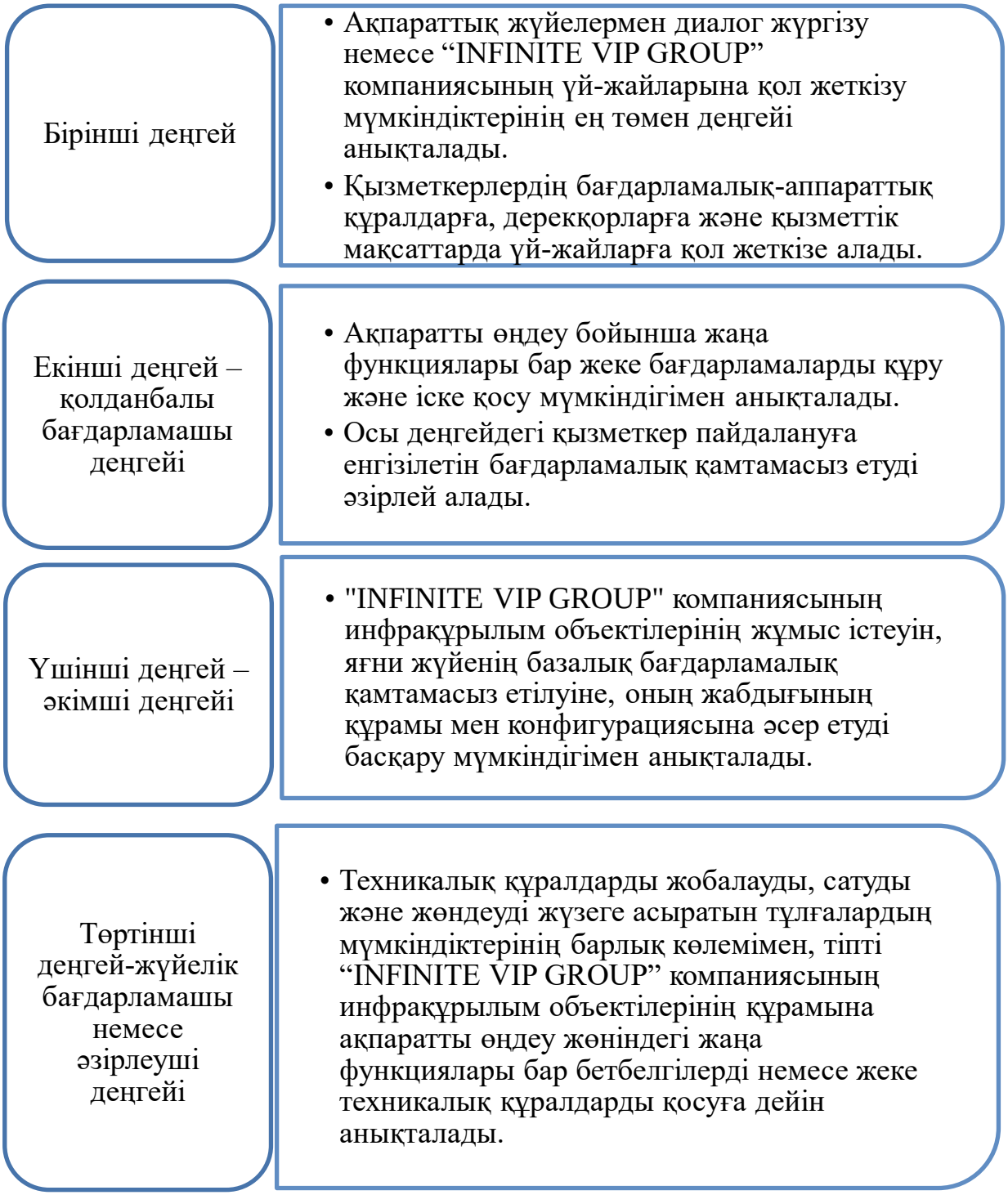
«INFINITE VIP GROUP» компаниясы қызметінің ерекшелігін ескере отырып, ішкі зиянкестерге ерекше назар аудару керек. Мысалы, «INFINITE VIP GROUP» компаниясының инсайдерлері озық әзірлемелерді немесе

қорғалған деректерді кейіннен шетелдік немесе бәсекелес кәсіпорындарға сату мақсатында зиянкестерге сата алады.

Басқаша айтқанда, «INFINITE VIP GROUP» компаниясының ішкі зиянкестері ұйымның өзінің барлық бизнес-процестерінің заңды қатысушылары болып табылады, мысалы, аппараттық-бағдарламалық кешендерге қызмет көрсететін немесе өзінің қызметтік міндеттеріне сәйкес оларға жіберілген персонал [8].

Зиян келтіру ықтималдығы неғұрлым жоғары болып, «INFINITE VIP GROUP» компаниясының қызметкерінің біліктілігі неғұрлым жоғары болса, ақпараттық немесе техникалық инфрақұрылымның иерархиясы соғұрлым жоғары болады және электронды ақпараттық ресурстарға немесе үй-жайларға қол жетімді болады [8].

Құқық бұзушыларды «INFINITE VIP GROUP» компаниясының ақпараттық инфрақұрылымы объектілері ұсынатын мүмкіндіктер деңгейіне қарай жіктеуге болады. Бұл мүмкіндіктердің төрт деңгейі анықталған (2.1-сурет). Жіктеу иерархиялық болып табылады, яғни әрбір келесі деңгей алдыңғы функционалдық мүмкіндіктерді қамтиды [**Error! Reference source not found.**].



2.1 сурет – өндірістік-техникалық бөлім жобаларын қамтамасыз етудің ақпараттық жүйесінің деректер базасының мәні мен атрибуттары.

Ішкі қаскүнем өзіне қоятын басты мақсат «INFINITE VIP GROUP» компаниясының электрондық ақпараттық ресурстарын, оның ішінде оларды өңдеу, сақтау және ұсыну құралдарын, оған ең жоғары қолжетімді деңгейде бақылау алу болып табылады. «INFINITE VIP GROUP» компаниясының ішкі қаскүнемінің жіктелуінің келесі белгілерін атап өтуге болады:

1. Кәсіби саладағы тәжірибе мен білім;
2. Қызметтік міндеттерді орындау үшін қажетті қолжетімді ресурстар;

3. Функционалдық қызмет саласы;
4. Іс-әрекет уәждемесінің болуы[6].

«INFINITE VIP GROUP» компаниясының ақпараттық инфрақұрылым объектілерінің әкімшілеріне және АҚ қауіп-қатерін әлеуетті іске асыра алатын қауіпсіздік әкімшілеріне ресурстар мен қорғау құралдарына тікелей қол жеткізу мүмкіндігін пайдалана отырып ерекше назар аудару керек. Аталған қызметкерлер «INFINITE VIP GROUP» компаниясының ақпараттық инфрақұрылым объектілерінің құрылымымен жақсы таныс. Бұл адамдар АҚ қатерлерін іске асыру үшін стандартты және жеңіл алынатын жабдықты ғана емес, сонымен қатар мамандандырылған жабдықтармен де пайдалана алады деп болжауда. «INFINITE VIP GROUP» компаниясы қызметкерлерінің ақпаратты қорғаудың бөлінген жүйесінде маңызды рөлінің салдарынан лауазымдық міндеттерді іріктеу, жұмысқа қабылдау және орындалуын бақылау бойынша елеулі тәсілге бағытталған техникалық және ұйымдастырушылық шаралар кешенін қолдану қажет [12].

Осылайша, зиянкестерге «INFINITE VIP GROUP»компаниясының үй-жайларына және бағдарламалық-аппараттық құралдарына әртүрлі рұқсаты бар бірінші, екінші және үшінші деңгейдегі қызметкерлер жатады деген қорытынды жасауға болады. Бұл ретте мұндай қызметкерлердің әлеуметтік және қаржылық деңгейі пайда табу мақсатында Заңды бұзуға итермелей алатынын ескеру қажет.

2.2 «INFINITE VIP GROUP» компаниясының қауіпсіздік қатерлері мен осалдықтарын талдау

Пайда болған қауіп-қатерлер, сондай-ақ ақпараттық ресурстарға дәстүрлі емес шабуылдар қауіп-қатерді бағалаудың және қауіп-қатерді төмендету бойынша күш-жігердің шектерін анықтады. Кейбір қауіптерді алдын-ала болжау мүмкін емес, және барлық ықтимал тәуекелдерді ең аз деңгейге дейін азайту әрқашан үнемді бола бермейді [12].

Сенімділік – тағы бір маңызды мәселе. Кез келген ұйымның ақпараттық инфрақұрылымы ақпаратқа сенімді қол жетімділікті қамтамасыз етуі керек және зиянды әрекеттерді уақытылы анықтау мәселесі әсіресе өзекті болып табылады.

Бүгінгі күні «INFINITE VIP GROUP»компаниясының үй-жайлары мен ақпараттық жүйелері қауіп-қатерінің әртүрлі түрлерінің едәуір санын бөліп көрсетуге болады. Табиғатта ықтимал қауіптер жиынтығының пайда болуы екі топқа бөлінеді: табиғи және жасанды [12].

Табиғи қауіп-қатерлер-бұл объективті, адамға тәуелді емес, жүйенің қауіпсіздігін бұзатын факторлар, ал жасанды қауіп-қатерлер, керісінше, адамның әдейі (қасақана қауіп-қатерлер) немесе әдейі емес (қасақана емес) қызметімен байланысты.

«INFINITE VIP GROUP» компаниясының үй-жайлары мен ақпараттық жүйелерінің ақпараттық қауіпсіздігіне қауіп-қатерді іске асыратын зиянкестердің мақсаттарын былайша анықтауға болады:

1. Жеке мәліметтер мен коммерциялық құпияны құрайтын мәліметтерді алу;

2. «INFINITE VIP GROUP» компаниясының үй-жайлары мен ақпараттық жүйелерінде айналымдағы кез келген басқа құпия ақпаратты алу;

3. «INFINITE VIP GROUP» компаниясының үй-жайлары мен ақпараттық жүйелеріндегі ақпараттың тұтастығы мен шынайылығының бұзылуы;

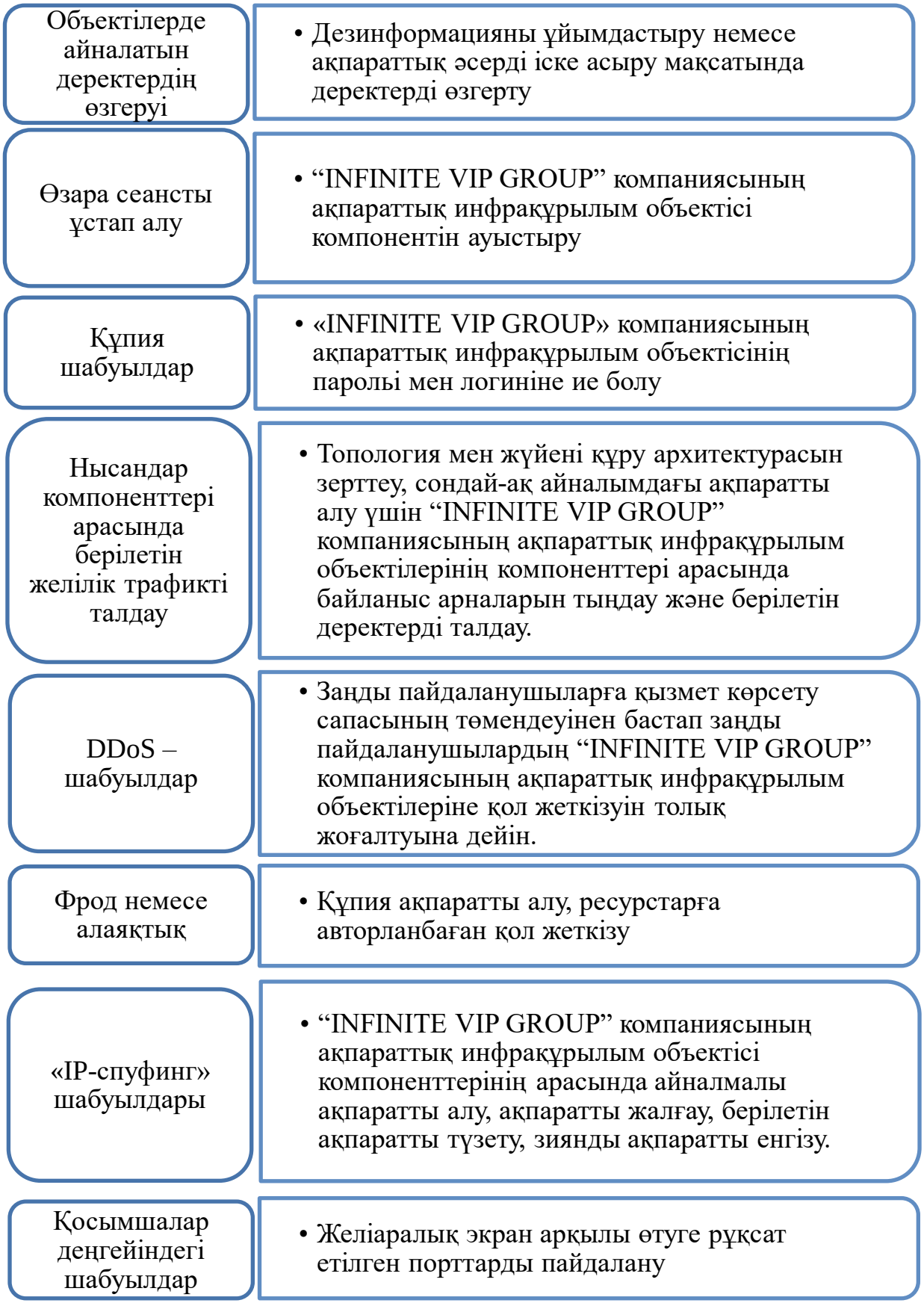
4. «INFINITE VIP GROUP» компаниясының барлық инфрақұрылымының немесе оның жекелеген компоненттерінің жұмысқа қабілеттілігінің бұзылуы.

Ұйымды тексерудің бірінші бөлімінде жүргізілген зерттеулерге сүйене отырып, қауіпсіздіктің негізгі проблемалары «INFINITE VIP GROUP» компаниясының ақпараттық инфрақұрылым объектілерінің әр түрлі құрамдауыштары мен құрамдас бөліктерінің таратылуымен және ашықтығымен байланысты екендігі туралы қорытынды жасауға болады.

Мысалы, мәліметтерді бұрмалау, хабарламалар көздерінің сипатты белгілерін анықтау, деректерді өңдеу және тораптарда сақтау процесінде көшіру, маршрутизаторлар конфигурациясының бұзылуы, жабдық пен т.б. байланыс сеанстарын орнату және жүргізу ережелерін бұзу қаупі бар.

Осылайша, осы зерттеу шеңберінде ақпараттық сипаттағы қауіп-қатерлерді талдау, яғни ашық стандарттарға байланысты және «INFINITE VIP GROUP» компаниясының ақпараттық инфрақұрылымының барлық деңгейлерінде көрініс табатын техникалық қауіп-қатерлер негізгі қызығушылық болып табылады.

«INFINITE VIP GROUP» компаниясының ақпараттық инфрақұрылым объектілерінің құрамына кіретін жабдықтың IP-хаттамаға негізделген кез келген шешімдерге тән осалдығы бар, сондықтан құрттар мен вирустардың, DDoS, спам және т. б. шабуылдарына ұшырайды. 2.2-суретте «INFINITE VIP GROUP» ақпараттық инфрақұрылымының компоненттеріне бағытталған желілік шабуылдардың ең ықтимал тізімін келтірейік [0,8,12].



2.2 сурет – «INFINITE VIP GROUP» компаниясы объектілерінің компоненттеріне бағытталған ең өзекті ықтимал желілік шабуылдар тізімі

1. «INFINITE VIP GROUP» компаниясының ақпараттық инфрақұрылым компоненттерінің арасында берілетін желілік трафикті талдау. Мұндай түрдегі шабуылдардың мақсаты байланыс арналарын тыңдау және топология мен инфрақұрылымды құру архитектурасын зерттеу, сондай-ақ айналымдағы ақпаратты алу үшін ақпараттық жүйелердің берілетін деректерін талдау болып табылады.

2. «INFINITE VIP GROUP» компаниясының ақпараттық инфрақұрылым объектілерінде айналымдағы деректердің өзгеруі. “INFINITE VIP GROUP» компаниясының ақпараттық инфрақұрылым компоненттерінің арасында берілетін деректерді оқуға мүмкіндік алған қаскүнем дезинформацияны ұйымдастыру немесе ақпараттық әсерді іске асыру мақсатында оларды өзгертуге мүмкіндігі бар.

3. Өзара әрекеттесу сеансын ұстап қалу (session hijacking). Аутентификациялаудың бастапқы рәсімі аяқталғаннан кейін «INFINITE VIP GROUP» компаниясының ақпараттық инфрақұрылым объектісінің заңды компонентімен белгіленген қосылысты қаскүнем жаңа хостқа ауыстырады, ал бастапқы компонентке қосылысты үзу командасы беріледі. Нәтижесінде легитимді пайдаланушының компоненті елеусіз өзгеріске ұшырайды. Осы шабуылды жүзеге асыратын шабуылдаушыны анықтау жіберушінің IP мекен-жайы жалған болуы мүмкін болғандықтан қиындайды, өйткені оған ақпаратты «INFINITE VIP GROUP» - жәбірленушіден алу қажет емес. Сонымен қатар, осы шабуылды сәтті жүргізу арқылы «INFINITE VIP GROUP» қызметкерлерін шабуылға тартуға мүмкіндік беретін вирустар мен басқа да зиянды бағдарламаларды (спаммен қоса) таратуға болады.

4. Пароль шабуылдары. Паролді шабуылдарды өткізудің мақсаты «INFINITE VIP GROUP» компаниясының ақпараттық инфрақұрылымының заңды компонентінің логині мен парольдерін иелену. Зиянкестер IP-мекенжайды ауыстыру, тыңдау (сниффинг), қарапайым аралықтар сияқты әдістерді пайдалана отырып, парольдік шабуылдарды жүргізе алады.

5. Қосымшалар деңгейіндегі шабуылдар бірнеше тәсілмен жүргізілуі мүмкін. Қолданбалы деңгейдегі шабуылдардың басты проблемасы - олар брандмауэр арқылы өтуге рұқсат етілген порттарды жиі пайдаланады. «INFINITE VIP GROUP» ақпараттық инфрақұрылым объектісі деңгейіндегі шабуылдарды толығымен жою мүмкін емес, өйткені әртүрлі қосымшалардың дамуы мен қосымшалардың осалдықтары бар.

6. Фрод немесе алаяқтық. Алаяқтықты сатудың мақсаттарының бірі - коммерциялық құпияны (немесе құпия ақпаратты) құрайтын ақпарат алу және оны кейіннен сату. Қаскүнемдер фродты ұйымдастыру үшін бір мезгілде бірнеше түрлі қол жеткізу тәсілдерін, мысалы, оптоталшық немесе радиоарнаны пайдалана алады. Фродты анықтау үшін «INFINITE VIP GROUP» компаниясының ақпараттық инфрақұрылымының барлық компоненттерінің арасында айналмалы деректерді тұрақты талдау қажет,бұл бүгінгі күні әр түрлі қызмет жеткізушілерінің түрлі жабдықтарының үйлесімділігіне байланысты мүмкін емес.

7. DOS-шабуылдар. «INFINITE VIP GROUP» компаниясының ақпараттық инфрақұрылым объектілері үшін DoS шабуыл ерекшелігін келесі тізбемен анықтауға болады:

– «INFINITE VIP GROUP» компаниясының ақпараттық инфрақұрылым объектілеріне DoS шабуылдары заңды пайдаланушыларға қызмет көрсету сапасының төмендеуінен бастап заңды пайдаланушыларға қолжетімділіктің толық жоғалуына дейін түрлі келеңсіз салдарға алып келеді. «INFINITE VIP GROUP» компаниясының ақпараттық инфрақұрылымының бір объектісі үшін dos шабуылды табысты іске асыру онымен шектес объектілерге теріс әсер етуі мүмкін.

– «INFINITE VIP GROUP» компаниясының ақпараттық инфрақұрылымы компоненттерінің біріне жасалған шабуыл желі учаскесі немесе компанияның барлық ақпараттық инфрақұрылымы үшін теріс салдары болуы мүмкін.

8. «IP-спуфинг» шабуылдары.

«INFINITE VIP GROUP» компаниясының ақпараттық инфрақұрылым компоненттерінің арасында деректерді алмасу үшін IP-адрестердің қолданылуына байланысты, IP-адресті (IP-spoofing) ауыстыру шабуылы қызығушылық тудырады. IP-спуфинг ұйым ішінде немесе одан тыс жерде зиянкестер заңды қолданушы болып көрінген кезде пайда болады.

"IP-спуфинг" шабуылын іске асыру үшін зиянкестер рұқсат етілген IP-адрестердің диапазоны шегінде орналасқан IP-адресті немесе «INFINITE VIP GROUP»компаниясының ақпараттық инфрақұрылым объектісіне қол жеткізуге рұқсат етілетін авторландырылған сыртқы мекенжайды пайдалануы тиіс. Қаскүнем сондай-ақ IP-пакеттерді «INFINITE VIP GROUP» компаниясының ақпараттық инфрақұрылымының кейбір құрауыштарынан шығатындай етіп қалыптастыратын арнайы бағдарламаларды пайдалана алады. Зиянкестер ауысымды IP-адресін алып, клиенттердің бірінің объектімен байланысын үзеді және қорғалатын ақпаратты қабылдау мүмкіндігін алады.

"IP-спуфингті" пайдалана отырып, шабуылды табысты іске асыратын қаскүнем «INFINITE VIP GROUP» компаниясына келесі тәсілдермен зиян келтіруі мүмкін:

– «INFINITE VIP GROUP» компаниясының ақпараттық инфрақұрылым компоненттерінің арасында айналмалы қорғалатын ақпаратты (оның ішінде коммерциялық құпияны, дербес деректерді) алу.

– Ақпаратты бұрмалау немесе түзету.

– «INFINITE VIP GROUP» компаниясының ақпараттық инфрақұрылым объектілеріне зиянды ақпаратты енгізу.

Осылайша, «INFINITE VIP GROUP» компаниясының ақпараттық инфрақұрылым объектілері ақпараттық қауіпсіздік қатерлерінің кең тізбесінің әсеріне ұшырағаны туралы қорытынды жасауға болады.

Одан әрі жұмыста зерттеу объектісіне қатысты ақпараттық қауіпсіздіктің өзекті қатерлерінің неғұрлым егжей-тегжейлі моделі әзірленетін

болады, алайда жүргізілген талдау негізінде «INFINITE VIP GROUP» компаниясының үй-жайлары мен ақпараттық жүйелерінің қауіпсіздігін қамтамасыз ету үшін ақпаратты қорғау әдістерінің тиімділігін арттыру және ұйымды қорғаудың тиімді жүйесін құру мақсатында ақпараттық қауіпсіздіктің талаптары мен қағидаттары нақты айқындалуы тиіс деген қорытынды жасауға болады.

2.3 «INFINITE VIP GROUP» компаниясының ақпараттық қауіпсіздігі қатерлерінің өзектілігін бағалау

«INFINITE VIP GROUP» компаниясының үй-жайлары мен ақпараттық жүйелерінде көбінесе дербес деректердің өңделуіне байланысты, «INFINITE VIP GROUP» компаниясының ақпараттық қауіпсіздігіне төнетін қауіп-қатерлердің өзектілігін дербес деректердің ақпараттық жүйелерінде оларды өңдеу кезінде қауіпсіздігінің өзекті қатерлерін анықтау әдістемесін пайдалана отырып бағалаймыз.

Қауіп – қатерді іске асыру ықтималдығы – «INFINITE VIP GROUP» компаниясы үшін қалыптасқан жағдайда дербес деректердің қауіпсіздігіне нақты қауіп-қатерді іске асыру қаншалықты ықтимал екендігін сипаттайтын сараптамалық жолмен анықталатын көрсеткіш. Әрбір қауіп үшін сараптамалық қауіптің іске асырылу коэффициенті мынадай формула бойынша есептеледі:

$$Y = \frac{Y_1 + Y_2}{20}, \qquad (1)$$

мұндағы Y_1 – АЖДД бастапқы қорғалу коэффициенті;
Y_2 – қауіпті жүзеге асыру ықтималдығының коэффициенті.

«Дербес деректердің ақпараттық жүйелерінде оларды өңдеу кезінде дербес деректердің қауіпсіздігіне өзекті қауіп-қатерлерді анықтау әдістемесіне» сәйкес қауіптердің туындау ықтималдығы 2.1-кестеде көрсетілген қауіптердің (Y_2) туындау ықтималдығының коэффициентімен анықталады [13]:

2.1 кесте - Дербес деректер қауіпсіздігі қатерінің өзектілігін бағалау

Категория	Сипаттамасы	Қауіптің туындау ықтималдығының коэффициенті
Екіталай	Қауіпті жүзеге асыру үшін объективті алғышарттар жоқ	0
Төмен ықтималдылық	Қауіп-қатерлерді іске асыру үшін объективті алғышарттар бар, бірақ қабылданған шаралар оны іске асыруды айтарлықтай қиындатады	2

2.1 кестенің жалғасы

Орташа ықтималдық	Қауіптерді іске асыру үшін объективті алғышарттар бар, бірақ құпия ақпараттың қауіпсіздігін қамтамасыз етудің қабылданған шаралары жеткіліксіз	5
Жоғары ықтималдылық	Қауіп-қатерлерді іске асыру үшін объективті алғышарттар бар және қауіпсіздікті қамтамасыз ету жөніндегі шаралар қабылданбаған	10

Y_1 коэффициенті 2.2-кестеге сәйкес анықталады.

2.2 кесте –ЖҚҚ АЖДД коэффициенті

ЖҚҚ АЖДД коэффициенті	Y1 коэффициентінің сандық көрінісі
Жоғары	0
Орташа	5
Төмен	10

Қауіптің іске асырылу коэффициентінің мәні бойынша Y қауіптің іске асырылуының вербалды интерпретациясы мынадай түрде қалыптасады:

1. Егер 0≤Y≤0,3 болса, онда қауіпті іске асыру төмен деп танылады.
2. Егер 0,3≤Y≤0,6 болса, онда қауіпті іске асыру орташа деп танылады.
3. Егер 0,6≤Y≤0,8 болса, онда қауіпті іске асыру жоғары деп танылады.
4. Егер Y≥0,8 болса, онда қауіпті іске асыру өте жоғары деп танылады.

Әрбір қауіптің қатері келесі вербалды көрсеткіштерді пайдалану арқылы бағаланады [13]:

1. Төмен қауіптілік (Дербес деректер субъектілері үшін болмашы теріс салдарлар);
2. Орташа қауіп (Дербес деректер субъектілері үшін теріс салдарлар);
3. Жоғары қауіп (Дербес деректер субъектілері үшін елеулі теріс салдарлар).

Содан кейін нақты қауіп-қатерлер төмендегі 2.3 кестеде көрсетілген ережелерге сәйкестіктің алдын-ала тізімі бойынша таңдалады:

2.3 кесте – Ақпарат қауіпсіздігіне қауіп-қатерді өзекті ақпаратқа жатқызу ережесі

Қауіпті іске асыру мүмкіндігі	Қауіптің қауіптілік көрсеткіші		
	Төмен	Орташа	Жоғары
Төмен	Өзексіз	Өзексіз	Өзекті
Орташа	Өзексіз	Өзекті	Өзекті
Жоғары	Өзекті	Өзекті	Өзекті
Өте жоғары	Өзекті	Өзекті	Өзекті

"Дербес деректер туралы" 2006 жылғы 27 шілдедегі №152-Қазақстан Республикасының заңының 19-бабына сәйкес, дербес деректерді заңсыз немесе кездейсоқ қол жеткізуден, сондай-ақ басқа да заңсыз әрекеттерден қорғауды қамтамасыз ету қажет [2]. «INFINITE VIP GROUP» компаниясында өңделетін деректердің қауіпсіздігін қамтамасыз етуге қойылатын талаптар тізбесін дайындау үшін келесі нормативтік-құқықтық құжаттар тізбесіне сәйкес іске асырылған қауіптердің жеке моделін әзірлеу қажет:

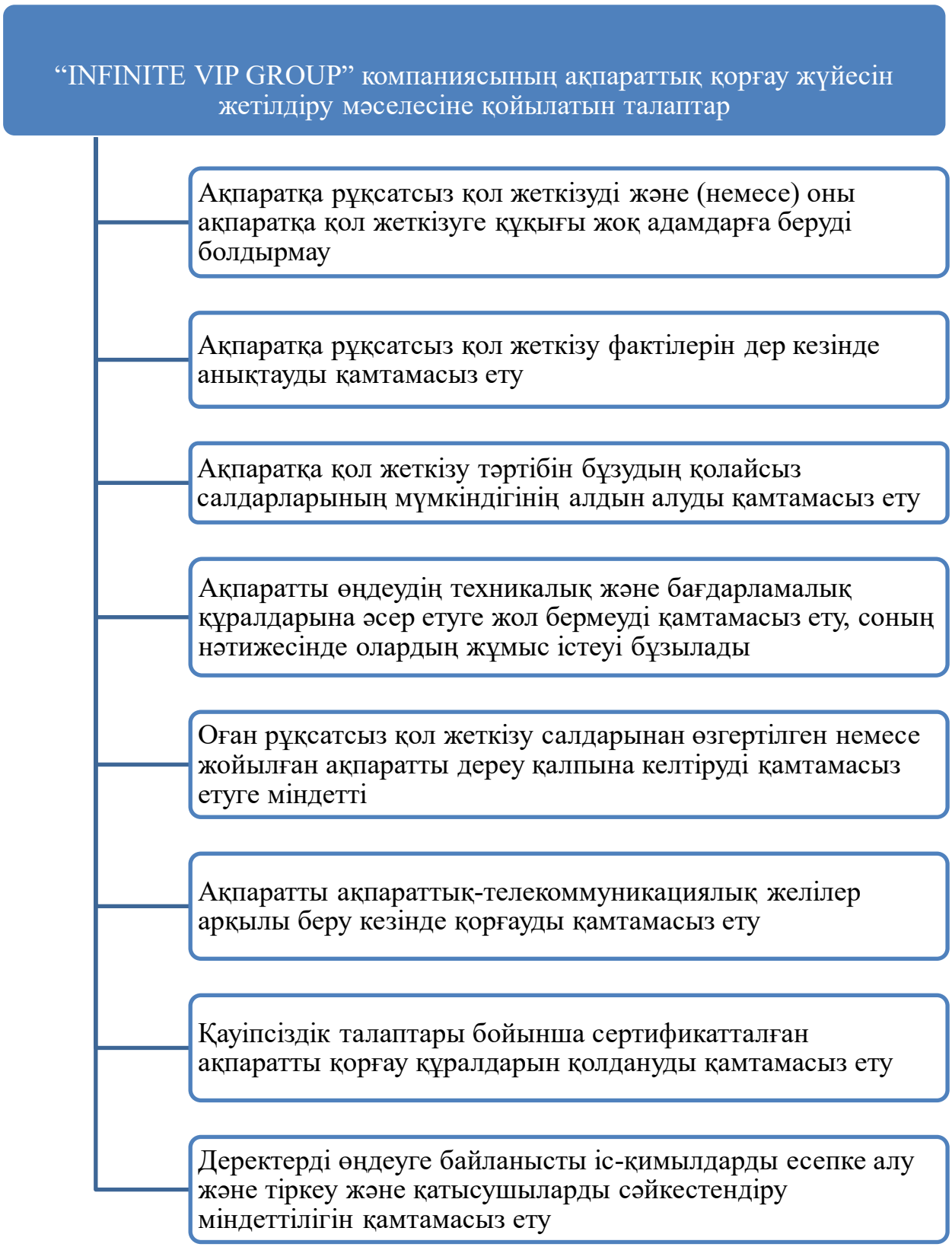
1. "Дербес деректер туралы" Республикалық заң.

2. "Дербес деректердің ақпараттық жүйелерінде өңдеу кезінде дербес деректердің қауіпсіздігіне өзекті қауіп-қатерлерді анықтау әдістемесі".

3. "Дербес деректердің ақпараттық жүйелерінде өңдеу кезіндегі жеке деректердің қауіпсіздігіне төнетін қауіп-қатердің базалық моделі" [2,13,14].

«INFINITE VIP GROUP» компаниясы үшін аса өзекті қауіптерді анықтаймыз, сондай-ақ «INFINITE VIP GROUP» компаниясының ақпаратты қорғау шаралары мен құрылымын ескере отырып, қауіптердің туындау ықтималдығына талдау жүргіземіз. Нәтижелерді В қосымшасының 1 кестесінде ұсынамыз.

«INFINITE VIP GROUP» компаниясының үй-жайлары мен ақпараттық жүйелерінің ақпараттық қауіпсіздік деңгейін арттыру мақсатында ақпараттық қорғау жүйесін жетілдіру мәселесіне қойылатын негізгі талаптарды бөліп көрсетеміз және оларды 3.1-суретте көрсетеміз.



2.3 сурет – «INFINITE VIP GROUP» компаниясының ақпараттық қорғау жүйесін жетілдіру мәселесіне қойылатын талаптар

2.4 «INFINITE VIP GROUP» компаниясының ақпараттық қорғалуын қамтамасыз ету принциптері

«INFINITE VIP GROUP» компаниясының ақпараттық инфрақұрылымының сенімді қорғалған объектілерін құру:

1. Байланыс арналары бойынша сақталатын, өңделетін және берілетін ақпараттың құпиялылығын қамтамасыз ету.
2. Сақталатын және берілетін ақпараттың тұтастығы мен сәйкестендірілуін қамтамасыз ету.
3. Пайдаланушылардың өкілеттіктеріне сәйкес «INFINITE VIP GROUP» компаниясының үй-жайлары мен ақпараттық ресурстарына қолжетімділікті бақылауды қамтамасыз ету.
4. «INFINITE VIP GROUP» компаниясының ақпараттық инфрақұрылым объектілерінде айналымдағы ақпараттың жылыстауын болдырмау.
5. Ақпаратқа рұқсатсыз қол жеткізуді болдырмау, сондай-ақ ақпаратты жоюды немесе бұрмалауды тудыратын бағдарламалық әсерлерді немесе олардың салдарларын болдырмау.
6. «INFINITE VIP GROUP» компаниясының ақпараттық қорғалуын қамтамасыз ету бойынша қажетті ұйымдастырушылық-техникалық шараларды іске асыру [11].

Қауіпсіздікті қамтамасыз ету құралдарын біріктіру үшін үздіксіз белсенділікті қамтамасыз ету фундаментін құрайтын жұмыс істеу процестерінің іргелі моделі және сенімді Инфрақұрылым талап етіледі. «INFINITE VIP GROUP» компаниясының желілік құрылымының барлық элементтері жүйенің жалпы жұмыс істеуінің маңызды аспектілері туралы ақпаратқа ие болуы, ал ақпараттық инфрақұрылым объектілерінің өздері мониторингтің және қауіпсіздік саясатын іске асырудың белсенді ортасы болуы қажет.

Басқаша айтқанда, белсенді қауіпсіздік тұтастай алғанда ақпараттық инфрақұрылым объектілері мен атап айтқанда ақпараттық жүйелер жұмысының маңызды сипаттамасына айналады, бұл «INFINITE VIP GROUP» компаниясының қауіпсіздігінде маңызды рөл атқарады. Қауіпсіздікті қамтамасыз ету бірінші кезекте реакция уақытының көрсеткіштерін және шабуылдарды басу тиімділігін жақсарта отырып, қазіргі осалдықтардың санын азайтып, дәстүрлі реактивті тәсілден кезең-кезеңмен проактивті тәсілге өту арқылы іске асырылуы тиіс [8].

«INFINITE VIP GROUP» компаниясының үй-жайлары мен ақпараттық жүйелерін ақпараттық қорғауды қамтамасыз ету жөніндегі осы зерттеу шеңберінде сондай-ақ ақпараттық қауіпсіздік қатерлерін бейтараптандырудың базалық қағидаттарын ескеру қажет:

1. Алдын алу (ақпараттық шабуылдарды болдырмау үшін басымдық). Белгілі қауіптердің алдын алу үшін белгілі қорғау шараларын іске асыру. Болдырмау құралдары жүйелік бағдарламалық қамтамасыз етудің стандартты

және күшейтілген бейнелерін енгізуді, желіаралық экрандарды немесе қолжетімділікті шектеудің өзге де технологияларын пайдалануды қамтиды.

2. Мониторинг. Белгілі осалдықтарды пайдаланумен байланысты ықтимал қауіпті әрекеттер мен әрекеттерді анықтау.

3. Агрегацияның негізгі нүктелерінде анықталған нақты қауіп-қатерлерді бөлу мақсатында «INFINITE VIP GROUP» компаниясы қызметкерлерінің әдепсіз іс-әрекеттері мен қаскүнемдің нақты іс-қимылдарын шектеу. Мұндай әрекеттерді анықтау үшін басып Кірулер мониторингі құралдарын өрістету әдістері, серверлер мен желіаралық экрандар журналдарына талдау жүргізу, сондай-ақ операциялық жүйе шақыруларының белсенді мониторингі қолданылады.

4. Жауап шаралары. Нақты уақыт режиміне жақын режиміндегі нақты қауіп-қатерді іске асыру залалын төмендету мақсатында алынған ақпарат негізінде әрекет ету қабілеті (мысалы, қолжетімділікті динамикалық шектеу, пакеттерді тастау, желілік құрылғының конфигурациясын өзгерту, жұмыс сеанстарын үзу және қате жүйелік шақыруларды бұғаттау) [8].

2.5 Тарау бойынша қорытындылар

Осылайша, осы тарауда «INFINITE VIP GROUP» компаниясының үй-жайлары мен ақпараттық жүйелері қауіпсіздігінің осалдықтары мен қатерлеріне талдау жүргізілді, сондай-ақ «INFINITE VIP GROUP» компаниясының үй-жайлары мен ақпараттық жүйелері үшін тәртіп бұзушының және қауіпсіздіктің өзекті қатерлерінің үлгілері әзірленді.

Одан әрі жұмыста алынған нәтижелер, ақпараттық қорғауды қамтамасыз етудің тұжырымдалған қағидаттары, федералдық заңдар мен басқарушы құжаттар негізінде ақпараттық қорғау деңгейін арттыру жөнінде нақты ұсыныстар әзірлеу қажет.

Мұндай ұсынымдарды ұйымдастыру шараларына, сондай-ақ ақпаратты қорғаудың бағдарламалық және техникалық құралдарына жіктеу қажет, олар «INFINITE VIP GROUP» компаниясының анықталған қауіпсіздік қатерінен ақпараттық қорғауды қамтамасыз етуге мүмкіндік береді.

3. «INFINITE VIP GROUP» компаниясының үй-жайлары мен ақпараттық жүйелерін ақпараттық қорғау деңгейін арттыру бойынша ұсынымдарды әзірлеу

«INFINITE VIP GROUP» компаниясының үй-жайлары мен ақпараттық жүйелерін ақпараттық қорғауды қамтамасыз ету жөніндегі шаралар 2 тарауда көрсетілген ақпарат қауіпсіздігіне төнетін қауіптерді бейтараптандыруға бағытталуы тиіс және келесі бағыттарға бөлінеді.

1. «INFINITE VIP GROUP» компаниясының үй-жайлары мен ақпараттық жүйелерін қорғау бойынша ұйымдастыру шаралары.

Ұйымдастыру шаралары ұйымның ақпараттық инфрақұрылым объектілерін қорғаудың сенімді тетігін құруда маңызды рөл атқарады. Бүгінгі күні ақпарат қауіпсіздігін ұйымдастыру және деректерді қорғау, қауіпсіз жұмыс ережелері, сондай-ақ штаттан тыс жағдайларда персоналдың іс-қимылдарын мерзімдік негізде пысықтау бөлігінде қызметкерлерді оқыту ұйымдастырылды. Сонымен қатар, персоналдың ақпарат қауіпсіздігіне төнетін қауіп туралы және қауіпсіз жұмыс ережелері туралы хабардар болуын бақылау жүзеге асырылады.

Алайда «INFINITE VIP GROUP» компаниясы басшылары мен қызметкерлерінің бөлімшелері мен лауазымдық нұсқаулықтары туралы ережелерде қолжетімділікті шектеу атрибуттарын, сондай-ақ коммерциялық құпияны құрайтын деректерді жария еткені, бергені немесе жоғалтқаны үшін жауапкершілік туралы тармақтар көзделмеген.

Сәйкестендірудің және аутентификацияның талап етілетін саясаты, қолжетімділікті басқару, ақпаратты машиналық тасымалдаушыларды қорғау, қауіпсіздік аудиті, антивирустық қорғау, тұтастық пен қол жетімділікті қамтамасыз ету, сондай-ақ басқа да қауіпсіздік саясаты кәсіпорында бүгінгі күні әзірленген.

«INFINITE VIP GROUP» компаниясының ақпараттық инфрақұрылым объектілерін қорғау жөніндегі ұйымдастыру шараларының арасында келесі бағыттарды егжей-тегжейлі пысықтау қажет:

1. Техникалық құралдарды орналастыру (әсіресе ақпаратты шығару құрылғыларын орналастыру бөлігінде, оны рұқсатсыз қарауды болдырмайтын).
2. Алынбалы ақпарат тасымалдаушылармен жұмыс істеу тәртібі.
3. Ақпаратты рұқсатсыз кіруден қорғау.
4. Қауіпсіздік әкімшісінің жұмыс тәртібі.
5. Пайдаланушылардың құпия сөздерін пайдалану тәртібі мен ережелері.

«INFINITE VIP GROUP» компаниясының үй-жайлары мен ақпараттық жүйелерін қорғау жөніндегі ұйымдастыру іс-шараларын реттейтін құжаттарды келесі тізбемен анықтауға болады:

1. Қандай да бір үй-жайға рұқсаты және қандай да бір ақпараттық жүйемен жұмыс істеуге рұқсаты бар қызметкерлердің тізбесі.

2. «INFINITE VIP GROUP» компаниясының ақпараттық инфрақұрылымын қорғау туралы ереже.

2. «INFINITE VIP GROUP» компаниясының үй-жайлары мен ақпараттық жүйелерін техникалық және физикалық қорғау.

Қазіргі уақытта тиісті қызметтердің бақылаудағы аймақтың қауіпсіздігін ұйымдастыруы толығымен жоқ. Ақпараттық жүйелер жұмыс істейтін «INFINITE VIP GROUP» компаниясы аумағының кіру / шығу және кіру / шығу нүктелері күзеттік хабарлау және бейнемониторинг жүйелерімен жабдықталған, бірақ турникеттер мен кіруді бақылау жүйесі жоқ.

Бұдан әрі «INFINITE VIP GROUP» компаниясы қызметкерлерінің функционалдық міндеттерін және үй-жайдың немесе ақпараттық жүйенің маңыздылығы санатын салыстыруға мүмкіндік беретін пәндік аймақтарды шектеуді көздейтін тәсілді әзірлеу ұсынылады.

Қауіпсіздік аудитін сондай-ақ мерзімдік негізде бөгде ұйым жүргізеді, оның шеңберінде ақпараттық ресурстарды түгендеу, қауіпсіздік оқиғаларын тіркеу, қауіпсіздік мониторингі жүргізіледі, сондай-ақ қауіпсіздік оқиғаларын тіркеу кезінде іркілістерге ден қою тексеріледі.

2-тарауда жүргізілген талдау нәтижелері бойынша сыни инфрақұрылымның маңызды объектілерінің талап етілетін бағдарламалық-аппараттық құралдарын келесі тізіммен атап өтеміз:

1. РК-ден ақпаратты қорғау құралы.
2. Вирусқа қарсы құрал.
3. Қорғауды талдау құралы.

«INFINITE VIP GROUP» компаниясының маңызды үй-жайлары мен ақпараттық жүйелерін қорғау бойынша техникалық іс-шараларды регламенттейтін құжаттарды келесі тізбемен анықтауға болады:

1. Ақпаратты қорғауды қамтамасыз ету жөніндегі іс-шаралар жоспары.
2. Штаттан тыс жағдайлардағы іс-қимыл жоспары.
3. Тасымалдаушыларды есепке алу және сақтау журналы.
4. Ақпаратты қорғау құралдарын орнату актісі.
5. Электрондық тасығыштарды есептен шығару және жою актісі.
6. Құжаттарды жою актісі.
7. Коммерциялық құпияны құрайтын ақпаратқа қол жеткізудің рұқсат беру жүйесі туралы ереже.

3.1 Ұйымдастыру шаралары

3.1.1 Техникалық құралдарды орналастыру бойынша ұйымдастыру шаралары

Осы жұмыста әзірленген «INFINITE VIP GROUP» компаниясында ақпараттық инфрақұрылымдар объектілері мен компоненттерін орналастыру бойынша ұйымдастыру шараларын атаймыз:

1. «INFINITE VIP GROUP» компаниясының ақпараттық инфрақұрылымының барлық объектілері мен компоненттері БА шегінде үй-жайларда орналасқан.

2. «INFINITE VIP GROUP» компаниясының ақпараттық инфрақұрылымының объектілері мен компоненттеріне рұқсатсыз кіруге кедергі келтіретін ұйымдастыру шаралары қарастырылған (үй-жайға кіру режимі, техникалық құралдармен жұмыс істеуге рұқсат беру тәртібі, үй-жайларды және перифериялық құрылғыларды негізгі техникалық өңдеу құралдарына қосу орындарын сүргі салу).

3. «INFINITE VIP GROUP» компаниясының ақпараттық инфрақұрылымының объектілері мен компоненттеріне рұқсатсыз кіруге кедергі келтіретін ұйымдастыру шаралары қарастырылған (үй-жайға кіру режимі, АЖО-мен жұмыс істеуге рұқсат беру тәртібі).

4. АҚҚ-ға рұқсатсыз кіруге кедергі келтіретін ұйымдастыру шаралары қарастырылған (АҚҚ-мен жұмыс істеуге рұқсат беру тәртібі анықталды, оларды пайдалану тәртібі анықталды).

5. АҚҚ пайдаланатын техникалық құралдарды орналастыру кезінде осы құралдарға ұсынымдар ескерілді.

6. Қорғалатын ақпаратты баспаға шығаруға арналған техникалық құралдарды орналастыру осы ақпаратқа рұқсаты жоқ тұлғалардың көзбен шолып көруінің барынша қиындықтарын ескере отырып іске асырылды.

3.1.2 Алмалы-салмалы ақпарат тасымалдаушылармен жұмыс жөніндегі ұйымдастыру шаралары

Сақтаудағы және айналыстағы барлық алмалы-салмалы тасығыштар тасығыштарды есепке алу журналында ескерілуі тиіс. Жазылған нөмірі бар әрбір баспа құралында алынбалы тасушы затбелгі мен мөртаңба көрсетілген жапсырма болуы керек.

«INFINITE VIP GROUP» компаниясының қызметкерлері жұмыстарды орындау үшін қауіпсіздік әкімшісінен есепке алынған алмалы-салмалы тасымалдаушыны алады. Алу кезінде есепке алу журналына тиісті жазбалар енгізіледі.

3.1.3 Қауіпсіздік әкімшісінің жұмысын ұйымдастыру

Қауіпсіздік әкімшісі «INFINITE VIP GROUP» компаниясының ақпараттық инфрақұрылымының объектілері мен құрауыштарына қолданылатын ақпаратты қорғау құралдарын олармен берілетін пайдалану құжаттамасына, сондай-ақ оларды пайдалану тәртібін айқындайтын қорытындылардың нұсқамалары мен көшірмелеріне сәйкес баптау және пайдалану жөніндегі ақпаратты меңгеруі тиіс.

Қауіпсіздік әкімшісі журналдарды жүргізуі тиіс:

1. Пайдаланушылардың жұмысын есепке алу және құжаттарды пайдаланушылардың мөрі.

2. «INFINITE VIP GROUP» компаниясының ақпараттық инфрақұрылым объектілері мен компоненттеріне пайдаланушылардың қол жеткізу сәйкестендіргіштері мен парольдерін есепке алу.

3. Техникалық құралдарға әкімшінің қол жетімділігінің сәйкестендіргіштері мен парольдерін есепке алу.

Қауіп-қатерлерді іске асыру әрекеттері мен ақауларын есепке алу.

Сонымен қатар, ақпараттық қауіпсіздік әкімшісі қауіпсіздік саясатының сақталуын және тиісті бұйрықтардың сақталуын, сондай-ақ ақпаратты қорғауды қамтамасыз ету жөніндегі іс-шаралардың орындалуын бақылауды, штаттық емес жағдайларда бағдарламалық қамтамасыз етуді резервтік көшіруді және қалпына келтіруді жүзеге асыруды бақылайды.

3.1.4 Пайдаланушылардың құпия сөздерін пайдалану тәртібі мен ережелері

«INFINITE VIP GROUP» компаниясының ақпараттық инфрақұрылым объектілеріне қол жеткізу үшін парольдерді пайдалану кезінде келесі ережелерді орындау қажет:

1. Парольдерді ұйымдастыру-өкімдік құжаттың талаптарына сәйкес белгіленген мерзімділікпен өзгерту қажет.
2. Парольде кемінде 6 таңба болуы және әріптік және сандық символдар болуы тиіс.
3. Жеке парольдерді міндетті түрде қолдану.
4. Топтық парольдерді қолдануға жол берілмейді.
5. Парольдерді қайта пайдалануды болдырмау үшін алдыңғы 12 айда есеп (жазба) жүргізу қажет.

Құпия сөзді пайдаланған кезде келесі әрекеттерге тыйым салу керек:

1. Құпия сөз ретінде сіздің аты-жөні, туған күні, иттің аты және т. б.
2. Құпия сөз ретінде оңай есептелетін таңбалардың үйлесімін, сондай-ақ жалпы қабылданған қысқартуларды пайдалану.

3.2 Техникалық және физикалық қорғау

«INFINITE VIP GROUP» компаниясының кіруін басқару жүйесі өзіне турникетті, науқанның әрбір үй-жайы үшін санауыштарды қамтуы тиіс, сондай-ақ қызметкердің функционалдық міндеттерін және қызметкер қол жеткізе алатын компанияның үй-жайларының немесе ақпараттық жүйелерінің мәнділік санатын салыстыруға мүмкіндік беретін бірқатар пәндік аймақтарды қамтуы тиіс. Есептік нысанға келесі аймақтарды қосу орынды:

-Іске асыру кезінде «INFINITE VIP GROUP» компаниясының үй-жайлары мен ақпараттық жүйелері пайдаланылатын қызметкердің штаттық функционалдық міндеттерінің аймағы (бекітілген лауазымдық нұсқаулыққа сәйкес).

-Аймағы өзгерістер мен толықтырулар енгізілген функционалдық міндеттері айқындалады.

Мұндай тәсіл «INFINITE VIP GROUP» компаниясының периметрін қорғауды толықтырып қана қоймай, сонымен қатар Үй-жайлар мен ақпараттық жүйелердің эшелондалған қорғалуын ұйымдастыруға мүмкіндік береді. Талдау аймақтардағы жазбалардың мазмұнын және қызметкерге белгілі индекстерді салыстырумен жүзеге асырылады, яғни сәйкессіздікті іздеу жүргізіледі.

Сонымен қатар, «INFINITE VIP GROUP» компаниясының ақпараттық инфрақұрылым объектілерін бағдарламалық-аппараттық қорғауды іске асыру қажет.

Пайдаланушыларды және олар бастамашылық жасайтын процестерді, құрылғыларды, сондай-ақ сәйкестендіру мен аутентификацияның басқа да аспектілерін сәйкестендіруді және аутентификациялауды ұйымдастыру мақсатында ақпаратты рұқсатсыз қол жеткізуден қорғау жүйесін пайдалану керек. Мұндай жүйе пайдаланушылардың есептік жазбаларын басқаруды, пайдаланушылардың өкілеттіктерін (рөлдерін) бөлуді, ең аз қажетті құқықтар мен артықшылықтарды тағайындауды және қолжетімділікті басқарудың басқа да аспектілерін қамтамасыз етуге мүмкіндік береді.

"Secret Net 7", "Dallas Lock 8.0 K" және "Блокхост-желі 2.0" РК-ден АҚҚ-ны салыстырмалы талдау әдістемесі төменде келтірілген. Осы жұмыста салыстырмалы талдау үшін өлшемдермен рұқсат етілмеген қол жеткізуден ақпаратты қорғау жүйелерінің мынадай техникалық сипаттамалары таңдалған:

1. Қорғалу класы.
2. Жарияланбаған мүмкіндіктер басқару жүйесі.
3. Автоматтандырылған жүйелер класы.
4. Қосымша жабдыққа қойылатын талаптар: АҚҚ орналастыру үшін қатты дискіде қажетті бос орын.
5. Қосымша аппараттық қолдау: бар немесе жоқ.
6. Лицензия құны.

МТЖ-дан таңдалған АҚҚ үшін көрсетілген техникалық сипаттамалар 3.1-кестеде келтірілген.

3.1 кесте – Салыстырмалы талдау ақпаратты рұқсатсыз қол жеткізуден қорғау жүйесі

Салыстыру критерийлері	Secret Net 7	Dallas Lock 8.0-K	АҚҚ «Блокхост-желі 2.0»
Қорғалу сыныбы	3 қауіпсіздік класы	4 қауіпсіздік класы	3 қауіпсіздік класы
Құжатталмаған мүмкіндіктер бойынша бақылау деңгейі	Бақылаудың 2 деңгейі	Бақылаудың 4 деңгейі	Бақылаудың 2 деңгейі
Автоматтандырылған жүйелер класы	1B класына дейін	1G класына дейін	1B класқа дейін

3.1 кестенің жалғасы

Қосымша аппараттық талаптар: қатты дискідегі бос орын	2,000 Гб	0,030 Гб	0,060 Гб
Қосымша аппараттық қолдау	Бар (Secret Net Card, ПАК "Соболь»)	Жоқ	Жоқ
Лицензия құны	44550 тг.	45000 тг.	31200 тг.

Жүргізілген талдау нәтижесінде "Блокхост-желі 2.0" рұқсат етілмеген қол жеткізуден ақпаратты қорғау жүйесі таңдалды. Мұндай таңдау салыстырмалы аз баға мен қолайлы техникалық сипаттамалардың себебінен жүзеге асырылды. "Блокхост-желі 2.0" АҚҚ-жергілікті желілерде және автономды автоматтандырылған ақпараттық жүйелерде рұқсатсыз қол жеткізуден ақпаратты кешенді қорғауға арналған.

«Блокхост-желі 2.0» санкцияланбаған кіруден ақпаратты қорғау жүйесі № ROSS RU.0001.01BI00 ақпараттық қауіпсіздік талаптары үшін ақпараттық қауіпсіздік құралдарын сертификаттау жүйесінде сертификатталған.

"Блокхост-желі 2.0" рұқсат етілмеген қатынауда АҚҚ кешені декларацияланбаған мүмкіндіктердің болмауын бақылаудың 3-деңгейі бойынша және ЕТҚ БӨ 3-классы бойынша басшылық құжаттардың талаптарына сәйкес келетінін, яғни «INFINITE VIP GROUP» компаниясының ақпараттық инфрақұрылымының қорғалатын объектілеріне сай келетінін куәландырады.

"Блокхост 2.0 желісі" АҚҚ қамтиды:

1. АҚҚ клиенттік және серверлік бөліктерінен тұратын мамандандырылған бағдарламалық кешен.

2. Пайдаланушының жүйеге кіруін идентификациялау және аутентификациялауды қолдаудың аппараттық бөлігі. Негізгі тасымалдаушылар eToken, Rutoken типті жеке идентификаторлар бола алады. Клиенттік бөліктер жұмыс станциясын ЖТС-дан ақпаратқа жергілікті қорғауды қамтамасыз етеді.

Вирусқа қарсы қорғау «INFINITE VIP GROUP» компаниясының ақпараттық инфрақұрылым объектілерінің өздерін, сондай-ақ электрондық поштаны, өзге де сервистерді қорғауды және зиянды компьютерлік бағдарламалар белгілерінің деректер базасын жаңартуды қамтамасыз етуі тиіс. Осы жұмыста антивирустық жүйелерді салыстырмалы талдау үшін өлшемдермен 3.2-кестеде ұсынылған техникалық сипаттамалар таңдалған.

3.2 кесте – Антивирустық шешімдерді салыстырмалы талдау.

Салыстыру критерийлері	Kaspersky Endpoint Security 10	Dr.Web Enterprise Security Suite	ESET NOD32 Secure Enterprise Pack
Файлдарды көшіру уақытын арттыру	29%	23%	24%
ДК жылдамдығының жалпы деңгейін төмендету	36%	12%	27%
Жүйені жүктеу уақытын арттыру	20%	26%	25%
Орнату/жою уақытын ұлғайту	59%	36%	30%
Атқаратын жедел жады көлемі	149 Мб	102 Мб	168 Мб
Сигнал базасы өлшемі	60 Мб	30 Мб	125 Мб
Тәулік ішіндегі желілік трафик	15 Мб	2 Мб	4 Мб

Қарастырылып отырған үш нұсқаның ішінен Dr.Web Enterprise Security Suite жүйенің жұмысына минималды әсер етеді, сонымен қатар антивирустық жүйені таңдауда басты артықшылық ретінде қызмет еткен желіге аз жүктеме береді.

Сонымен бірге, Dr.Web таңдау бойынша ұсыныс, көптеген бәсекелес шешімдерден айырмашылығы, Dr.Web бағдарламалық өнімдерінде Қазақстан Республикасының сәйкестік сертификаттары бар екендігіне байланысты. Сонымен қатар, "Доктор Веб" компаниясы Қазақстан Республикасының Қорғаныс министрлігінің ақпаратты қорғау құралдарын құру саласындағы қызметке лицензиясы бар. Белгілі бір бағдарламалық өнім ретінде Dr.Web Enterprise Security Suite таңдалды, ол Dr.Web өнімдерінің жиынтығы және корпоративті желінің барлық түйіндеріне арналған қауіпсіздік элементтері, сонымен қатар олардың көпшілігіне арналған бірыңғай басқару орталығы бар.

Сертификат куәландырылған, 27.01.2024 жылға дейін жарамды, бұл DrWeb Enterprise Security Suite декларацияланбаған мүмкіндіктердің болмауын бақылаудың 2 деңгейі бойынша басшылық құжаттардың талаптарына сәйкес келеді, яғни «INFINITE VIP GROUP» компаниясының ақпараттық инфрақұрылым объектілерін қорғау үшін қолайлы.

Компьютерлік шабуылдарды анықтаудың аппараттық-бағдарламалық кешені Компьютерлік инциденттерді анықтауды, компьютерлік инциденттер туралы талдауды және ақпараттандыруды, сондай-ақ «INFINITE VIP GROUP» компаниясындағы компьютерлік инциденттердің салдарын болдырмау және жою бойынша шаралар қабылдауды қамтамасыз етуі тиіс. Компьютерлік шабуылдарды анықтаудың аппараттық-бағдарламалық кешенін таңдау үшін негізгі критерий ретінде осы жұмыста АӨК құнын үнемдеуден алынатын

экономикалық тиімділік таңдалды. 3.3-кестеде салыстырмалы талдау көрсетілген.

3.3 кесте-АӨК салыстырмалы талдауы

Салыстыру критерийлері	Әзірлеуші ұйым	ТжЭББФҚ сертификаты	Бағасы, тг
Аргус, 1.5 нұсқасы	Арнайы Жүйелік Техника Орталығы	№ 2487	22000
Шабуыл детекторы «Континент»	ЖШҚ «Қауіпсіздік Коды»	№ 3008	38000
Форпост, 2.0 нұсқасы	РНН	№ 2845	27500

Осылайша, 1.5 нұсқадағы "Аргус" компьютерлік шабуылдарды анықтаудың аппараттық-бағдарламалық кешенін пайдалану ұсынылады. "Аргус" АӨК 1.5 нұсқасында АҚ оқиғаларын талдау, кешен операторлары мен әкімшілерінің есептерді дайындау үшін кіріктірілген пайдаланушы интерфейстері бар.

3.3 Анықталған өзекті қатерлерді бейтараптандыру мақсатында ақпаратты қорғау шараларын әзірлеу

3.4-кестеде «INFINITE VIP GROUP» компаниясының үй-жайлары мен ақпараттық жүйелерінің анықталған қатерлерін бейтараптандыру мақсатында ақпаратты қорғау шаралары келтірілген.

3.4-кесте – «INFINITE VIP GROUP» компаниясының үй-жайлары мен ақпараттық жүйелерінің анықталған қауіптерін бейтараптандыру мақсатында ақпаратты қорғау шаралары

Қатердің атауы	Қауіп-қатерге қарсы іс-қимыл шаралары	
	Техникалық және физикалық	Ұйымдастырушылық
Физикалық қол жеткізу жолымен «INFINITE VIP GROUP» компаниясының бөлме мен ақпараттық жүйелерінің қатері		
Ақпаратты ұрлау, түрлендіру, жою	АҚҚ РК «Блокхост-желі 2.0», кіруді басқару жүйесі	Персонал нұсқаулықтары, жария етпеу туралы міндеттеме, қауіпсіздік саясатына сәйкес ТҚ орналастыру, сыртқы тасымалдағыштарды пайдалануды шектеу, сертификатталған БҚЕ орнату.

3.4 кестенің жалғасы

Қорғау құралдарын рұқсатсыз өшіру	АҚҚ РК «Блокхост-желі 2.0», кіруді басқару жүйесі	АҚҚ-мен жұмыс істеуге қол жеткізу тәртібін сақтау және парольдерді пайдалану тәртібін сақтау.
Агенттерді жүйе персоналы қатарына енгізу қаупі	-	Қызметкерлерді бастапқы және мерзімді тексеру (қауіпсіздік аудиті)
Қолжетімділікті шектеу атрибуттарын жария ету, беру немесе жоғалту қаупі	-	Персоналға нұсқаулық, жарияламау туралы міндеттеме, парольдерді пайдалану тәртібін сақтау
Желінің жұмыс істеуін қамтамасыз ету кіші жүйелерінің(подсистем) қатардан шығу қаупі	Кіруді басқару жүйесі	Қызметкерлерге нұсқаулар
Желідегі жұмыс станциясының нөмірі, физикалық мекенжайы, байланыс жүйесіндегі мекенжайы, аппараттық сияқты бірегей физикалық сипаттамалары бар пайдаланушылардың терминалдарын рұқсатсыз пайдалану қаупі.	Кіруді басқару жүйесі	Персоналға нұсқаулықтар, жария етпеу туралы міндеттеме, қауіпсіздік саясатына сәйкес ТҚ орналастыру, пайдаланушыларды міндетті сәйкестендіру
Бағдарламалық және бағдарламалық-аппараттық құралдарды қолдана отырып, «INFINITE VIP GROUP» компаниясының ақпараттық жүйелерінің қауіптері		
Зиянды бағдарламалар болып табылатын «бет белгілер» мен «вирустар» бағдарламалық қамтамасыздандыруды енгізу қаупі.	АҚҚ РК «Блокхост-желі 2.0», ABC. Dr.Web Enterprise Security Suite 6.0, АПК «Аргус»	Қызметкерлерге нұсқаулық, сыртқы тасымалдағыштарды пайдалануды шектеу, тасымалдағыштарды есепке алу және интернет желісін пайдалану журналын жүргізу, сертификатталған БҚЕ (БЖ) орнату
Құпия сөздерді және одан әрі пайдалану арқылы қол	АҚҚ РК «Блокхост-желі	Қызметкерлерге нұсқаулық, парольдерді

жеткізуді басқарудың басқа бөлшектерін заңсыз алу	2.0», АПК «Аргус»	мезгіл-мезгіл ауыстыру, сыртқы

3.4 кестенің жалғасы

Қаупі		тасымалдағыштарды пайдалануды шектеу, сертификатталған БҚЕ орнату, парольдерді пайдалану тәртібін сақтау
Жасырын деректер каналын іске асыру қаупі	АҚҚ РК «Блокхост-желі 2.0»	ЖҚ
Желі арқылы құпия ақпаратты басып алу қаупі	АҚҚ РК «Блокхост-желі 2.0», АПК «Аргус»	Қызметкерлерге нұсқаулық.

Видеокамера – бұл бақыланатын объектінің оптикалық суретін белгілі бір стандарттың электр бейнесигналына түрлендіретін оптоэлектронды құрылғы (бейне / қабылдағыш беру процесін стандарттауға мүмкіндік беретін бейнесигнал компоненттерінің құрылымы мен сипатына қойылатын талаптар жиынтығы).

Видеокамера СОТ-тың ең маңызды элементі болып табылады, өйткені оның бастапқы ақпараты жүйеге келіп түседі және оның сипаттамалары жалпы кескіннің сапасын анықтайды.

СОТ тиімділігі екі негізгі қағиданы қолдана отырып, сыни аудандарға камераларды орналастыру арқылы қол жеткізіледі:

– кіру нүктелерінің мониторингі (есіктер, дәліздер, жүру жолдары);
– ең құнды мониторинг.

Кіру нүктелері - адамдар мен көліктер белгілі бір аумаққа кіру үшін өтуі керек учаскелер. Өткізу орындарына камераларды қою - бұл қорғалатын объектіге кіретіндердің барлығын қауіпсіздендірудің экономикалық мүмкіндігі.

Құндылық – бұл қауіпсіздік деңгейінің жоғарылауын талап ететін нақты объектілер, олардың маңыздылығы нақты клиенттің қажеттіліктері мен басымдықтарымен анықталады.

Материалдық құндылықтар, олардың орналасқан жерлері сияқты физикалық объектілер құндылықтардың мысалдары болып табылады; Сонымен қатар, бұл маңызды іс-шаралар өткізілетін орындар - мысалы, бақылау-кассалық машиналары бар орындар, көліктерге арналған тұрақ орындары немесе қабылдау алаңдары.

Бейнекамерадан алынған кескін сапасы бірқатар индикаторлармен анықталады, бірақ көп жағдайда белгілі бір жүйе үшін камераны таңдағанда келесі параметрлерге назар аудару жеткілікті.

Жасырын бейнебақылау мәселелерін шешу үшін, сондай-ақ бейнекамераға назар аудармау үшін көзге көрінбейтін жарықтандыру

қолданылады – инфрақызыл диапазондағы жарық. Инфрақызыл жарықтандырудың екі жағдайы бар.

1. Шашыраңқы немесе диффузиялық шағылысқан жарық ағынының көрінбейтіндігін қамтамасыз ету қажет, бірақ радиация көздерінен сәулеленуге жол беріледі. Толқын ұзындығы 920, 880 және тіпті 850 нм болатын эмитенттерді пайдалануға болады.

2. Эмитенттің көзге көрінбейтіндігін, оны жақын қашықтықтан тікелей бақылау арқылы қамтамасыз ету қажет. Бұл үшін толқын ұзындығы 940–950 нм болатын эмитенттер қолданылады.

Бейнебақылауға арналған барлық инфрақызыл жарық көздерін екі топқа бөлуге болады, олар мақсатына қарай ерекшеленеді, сондықтан сипаттамалары мен дизайны бойынша:

- радиатор ретінде ИҚ сәулелендіргіштер, фаралар және қыздыру шамдары;

- IR жартылай өткізгіш IR сәулелендіргіштер (жартылай өткізгішті дискретті элементтер мен алты элементті жарық диодты массивтерге негізделген ықшам эмиттерлер негізінде).

Ішкі пайдалану бейнебақылау камераларын қарастырайық. Мен 3 бейнебақылау камераларын таңдадым және олардың техникалық сипаттамаларын талдай отырып, ең қолайлы нұсқаны таңдаймыз (кесте.3.5).

3.5 кесте – Ішкі бейнекамералардың салыстырмалы сипаттамалары

HD Камера Blackview BL-63A 2mpx 3.6 1080P	HD Камера ADK ED-6615-7 1mpx 3.6 720P	HD Камера ADK ED-6617-9 1.3mpx 3.6 720P
		
Сипаттамалары:	**Сипаттамалары:**	**Сипаттамалары:**
Пайдалану температурасы: -10..+50°C	Пайдалану температурасы: -10..+50°C	Пайдалану температурасы: -10..+50°C
ИҚ жарық қашықтығы:15	ИҚ жарық қашықтығы: 15	ИҚ жарық қашықтығы:15
Матрицаның рұқсаты: 1080p (1920×1080)	Матрицаның рұқсаты: 720p (1280×720)	Матрицаның рұқсаты: 720p (1280×720)
Корпус түрі: күмбез	Корпус түрі: күмбез	Корпус түрі: күмбез
Объектив түрі: тұрақталған	Объектив түрі: тұрақталған	Объектив түрі: тұрақталған
Объектив: 3.6 мм/F2.0	Объектив: 3.6 мм/F2.0	Объектив: 3.6 мм/F2.0

Қорғау классы: IP55	Қорғау классы: IP55	Қорғау классы: IP55
ИҚ қашықтығы: 20-30 м	ИҚ қашықтығы: 20-30 м	ИҚ қашықтығы: 20-30 м

3.5 кестенің жалғасы

Қуат: Dc12v±10 %/ POE	Қуат: Dc12v±10 %/	Қуат: Dc12v±10 %/
Интерфейс хаттамасы: Onvif, IPC	Интерфейс хаттамасы: AHD 720, AHD-M	Интерфейс хаттамасы: AHD 720, AHD-M
Байланыс интерфейсі:1 ажыратқыш RJ45 10 м/100 м Ethernet	Байланыс интерфейсі:1 ажыратқыш BNC	Байланыс интерфейсі:1 ажыратқыш BNC
Бағасы: 20.000 тг.	Бағасы: 17.500 тг.	Бағасы: 18.500 тг.

Сондай-ақ, сыртқы пайдалану камераларын қарастырайық. Мен 3 көше камерасын таңдадым, олардың сипаттамаларына талдау жүргіземіз және ең қолайлы нұсқаны таңдаймыз.

3.6 кесте - Сыртқы бейнекамералардың салыстырмалы сипаттамалары.

IP Камера Smart SM-9092 2mpx 3.6 POE қуат	BW-202A Аналогтық Камера AHD 2mpx 3.6 1080P Blackview	IP Камера Smart SM-9011 2mpx 6mm
		
Сипаттамалары:	**Сипаттамалары:**	**Сипаттамалары:**
2 мегапиксельді CMOS Камера	2 мегапиксельді CMOS Камера	2 мегапиксельді CMOS Камера
Объектив: 3.6 мм/F2.0	Объектив: 3.6 мм/F2.0	Объектив: 6 мм/F2.0
Күндізгі және түнгі режим	Күндізгі және түнгі режим	Күндізгі және түнгі режим
Кадр жиілігі: 25fps (1280*960), (1280*720), (1980*1080)	Кадр жиілігі: 25fps (1280*1080), (1280*720)	Кадр жиілігі: 25fps (1920*1080), (1280*960), (1280*720)
Интерфейс хаттамасы: Onvif, IPC	Интерфейс хаттамасы: AHD 1080H, AHD-M	Интерфейс хаттамасы: Onvif, IPC
Байланыс интерфейсі:1 ажыратқыш RJ45 10 м/100 м Ethernet адаптивті порт	Байланыс интерфейсі: 1 ажыратқыш BNC	Байланыс интерфейсі: 1 ажыратқыш RJ45 10 м/100 м Ethernet адаптивті порт

Қуат:Dc12v±10 % POE	Қуат:Dc12v±10 %/	Қуат:Dc12v±10 %/
Қорғау классы: IP66	Қорғау классы: IP66	Қорғау классы: IP55
ИҚ қашықтығы: 20-30 м	ИҚ қашықтығы: 20-30 м	ИҚ қашықтығы: 20-30 м
Бағасы: 22.000 тг.	Бағасы: 20.000 тг.	Бағасы: 18.500 тг.

Бейнебақылау жүйесінің жабдығын таңдау кезінде мынадай факторлар, сипаттамалар мен міндеттер ескеріледі:

• берілетін сигнал түрі – сандық (IP) немесе аналогтық;

• тарату ортасы – сымды және оның сыртқы түрі немесе сымсыз;

• жабдықты электрмен қоректендіруді қамтамасыз ету;

• жүйенің масштабы – камералар саны, объект аумағы және т.б.;

• басқа әлсіз тогы бар жүйелермен байланыс – КБжБЖ, периметрді қорғау, күзет және өрт сигнализациясы және т. б.;

• аналитикалық функциялар-адамдарды, автомобиль нөмірлерін, сценарийлерді және әр түрлі оқиғаларды автоматты түрде тану (аналитика);

• Мұрағат өлшемі, жазу сапасы, ақпаратқа қол жеткізу және т.б.

Қауіпсіздікті қамтамасыз ету бойынша қойылған міндеттерге сүйене отырып.

"МедСнаб" ЖШС ішкі бақылау үшін қолайлы нұсқа камера болып табылады:

- HD Blackview BL-63A 2mpx 3.6 1080P.

Ал сырттай бақылау үшін камера қолайлы:

- IP Камера Smart SM-9092 2mpx 3.6 POE қуаты.

Бірінші қорғаныс желісін құру кезінде периметр пайдаланылатын жабдықтың техникалық сипаттамаларына байланысты ұзындығы 200 м аспайтын учаскелерге бөлінеді. Бұл бұзушылық болған периметрдің ауданын тез анықтауға және тиісті шаралар қабылдауға мүмкіндік береді.

Күзетілетін объектілердің көрші қараусыз қалған, қараусыз қалған ғимараттардан, сондай-ақ жеке үйлер мен азаматтардың пәтерлеріне төбелер, жертөлелер, балкондар және көрші пәтерлердің лоджиялары арқылы кіру жолдарын жабу қажет.

Ұялы байланыс құралдары визуалды бақылау үшін, сондай-ақ бұзушылықтардың сенімділігі мен сипатын арттыру үшін пайдаланылады, ал СКУД құралдары күзетілетін үй-жайларға және объектінің аумағына кіруді шектеу үшін пайдаланылады. Объектінің периметрі бойынша бейнекамералардың жұмысын қамтамасыз ету үшін ол қашықтықтан іске қосу басқарылатын: қолмен және автоматты сигналдық оттармен жабдықталуы тиіс.

Екінші қорғаныс желісі пассивті оптикалық-электрондық, ультрадыбыстық, аралас немесе радиотолқынды детекторлардың көмегімен үй-жайлардың ішкі көлемдерімен қорғалған.

Үшінші қорғаныс желісі тікелей құндылықтарды сақтау орындарымен және оларға кіреберістермен қорғалған. Ол үшін пассивті және белсенді оптикалық-электрондық немесе радиолқынды детекторлар қолданылады.

Объектілердің жергілікті немесе орталықтандырылған қауіпсіздік консольдеріне дабыл сигналдарын жіберуге арналған дабыл сигналдары болуы мүмкін. Осылайша, объектінің қауіпсіздік жүйесін таңдау мен құрудың күрделілігі мен әмбебаптығына қарамастан, оған қажетті барлық талаптар нақты айқындалуы және қалыптастырылуы тиіс.

GSM сигнализациясын және видеодомофондарды қарастырайық, талдау жүргіземіз және бізге ең қолайлы нұсқаларды таңдаймыз.

3.6 кесте – GSM сигнализациясының салыстырмалы сипаттамалары және видеодомофондар

GSM сигнализациясы «Сокол»	GSM сигнализациясы «Стражник»	GSM сигнализациясы «Страж Express»
		
Сипаттамасы: Телефон арқылы қашықтан бақылау мүмкіндігі. Пульттермен күзету және алу. Күзетке қою және шығару туралы СМС хабарлама. Алдын ала берілген телефон нөміріне автоматты қоңырау шалу.	**Сипаттамасы:** Рұқсатсыз басып кіру туралы хабарлау SMS және қоңырау арқылы жүргізіледі: датчиктер іске қосылған кезде сигнал беру пайдаланушы берген нөмірлерге SMS хабарлама жібереді, содан кейін іске қосылу туралы ақпарат пайдаланушы берген нөмірлерге қоңырау арқылы қайталанады.	**Сипаттамасы:** Дабыл режимінде сіз орнатылған микрофонмен кіріс шақыру кезінде күзетілетін объектіде болып жатқан жағдайды тыңдауға мүмкіндігіңіз бар. 220В желілік қуат жоғалған жағдайда, сигнал беру кіріктірілген аккумулятордың арқасында автономды режимде жұмысын жалғастырады. Бұл ретте бағдарламаланған нөмірге тиісті Ақпараттық хабарлама жіберіледі. 12 сымсыз аймақты құру мүмкіндігі, бұл күзетілетін объектіге қай бөлмеде болғанын білуге мүмкіндік береді.

Жұмыс температурасы: -20 С / + 55 С	Жұмыс температурасы: -10°С-тан 40°С-қа дейін	Жұмыс температурасы: -45 С-тан + 60С-қа дейін
GSM желісінің жиілігі: 900/1800 МГц	GSM желісінің жиілігі: 900/1800/1900 МГц;	Сымсыз жиілік: 315MHz/433MHz;
Радио датчиктер жиілігі: 433 * 0,5 МГц	Сымсыз датчиктер жиілігі: 433 МГц;	GSM жиілігі: 900/1800MHz

3.6 кестенің жалғасы

Жұмыс ылғалдылығы: 20 % — 95 %	Ылғалдылығы: 20 % - 95%;	Ылғалдылығы: ≤ 95%
Бағасы: 31.500 тг.	Бағасы: 25.000 тг.	Бағасы: 21.000 тг.

GSM сигнализациясын таңдағанда, ең алдымен келесі сипаттамаларға назар аудару керек:

1. датчиктер үшін кіру саны және түрі;
2. қашықтан басқару мүмкіндігі;
3. сыртқы құрылғыларды басқару үшін шығулардың болуы және түрі;
4. GSM Модулінің қуат тәсілі;
5. бағдарламалау және баптау тәртібі;
6. қосымша опциялар температура датчиктерін қосу мүмкіндігі сияқты және т. б.

Әрбір GSM сигнализациясының сипаттамаларын қарастыра және талдай отырып, сигнализацияның қандай да бір функцияларының құны мен қажеттілігіне назар аудару қажет. Біздің жағдайда ең қолайлы нұсқа "Страж Express" дабылы болып табылады.

Бұдан әрі бейнедомофондарды қарастырайық және ең қолайлы нұсқаны таңдаймыз (кесте.5).

3.7 кесте – Видеодомофондардың салыстырмалы сипаттамалары.

Optimus VM-7S (black)	JEJA TFT 725 LCD	JEJA TFT 801 LCD
		
Сипаттамалары:	**Сипаттамалары:**	**Сипаттамалары:**
Монитор диагоналі – 7 дюйм, TFT LCD.	Монитор диагоналі – 7 дюйм, LCD.	Монитор диагоналі – 8 дюйм, TFT LCD.
Сенсорлық басқару. Меню - орыс тілі.	Қатты дауыспен сөйлесу (Hands Free).	Қатты дауыспен сөйлесу (Hands Free).
Кірістірілген жады: 86 суретке дейін. SD карточкадағы фото	Кіріктірілген жадқа фотофиксациялау мүмкіндігі.	2 бейнекамераны қосу мүмкіндігі. Қашықтан басқару пультін

және бейнежазба мүмкіндігі.		басқару.
Есіктерді қашықтан ашу.	Түнгі көру үшін шақыру блогындағы камераға инфрақызыл жарық.	SD карточкаға фотофиксация және бейнефиксация мүмкіндігі.

3.7 кестенің жалғасы

32 Гб дейін SD жад карталарын қолдайды	Есіктерді қашықтан ашу.	Сыртқы мониторинг.
Параметрлер - дыбыс, контраст, жарықтық, әуен.	Параметрлер - дыбыс, контраст, жарықтық.	Түнгі көру үшін шақыру блогындағы камераға инфрақызыл жарық.
Бағасы: 38.000 тг.	Бағасы: 29.000 тг.	Бағасы: 35.000 тг.

Бейнедомофонды таңдау кезінде назар аудару керек негізгі сипаттамалары:

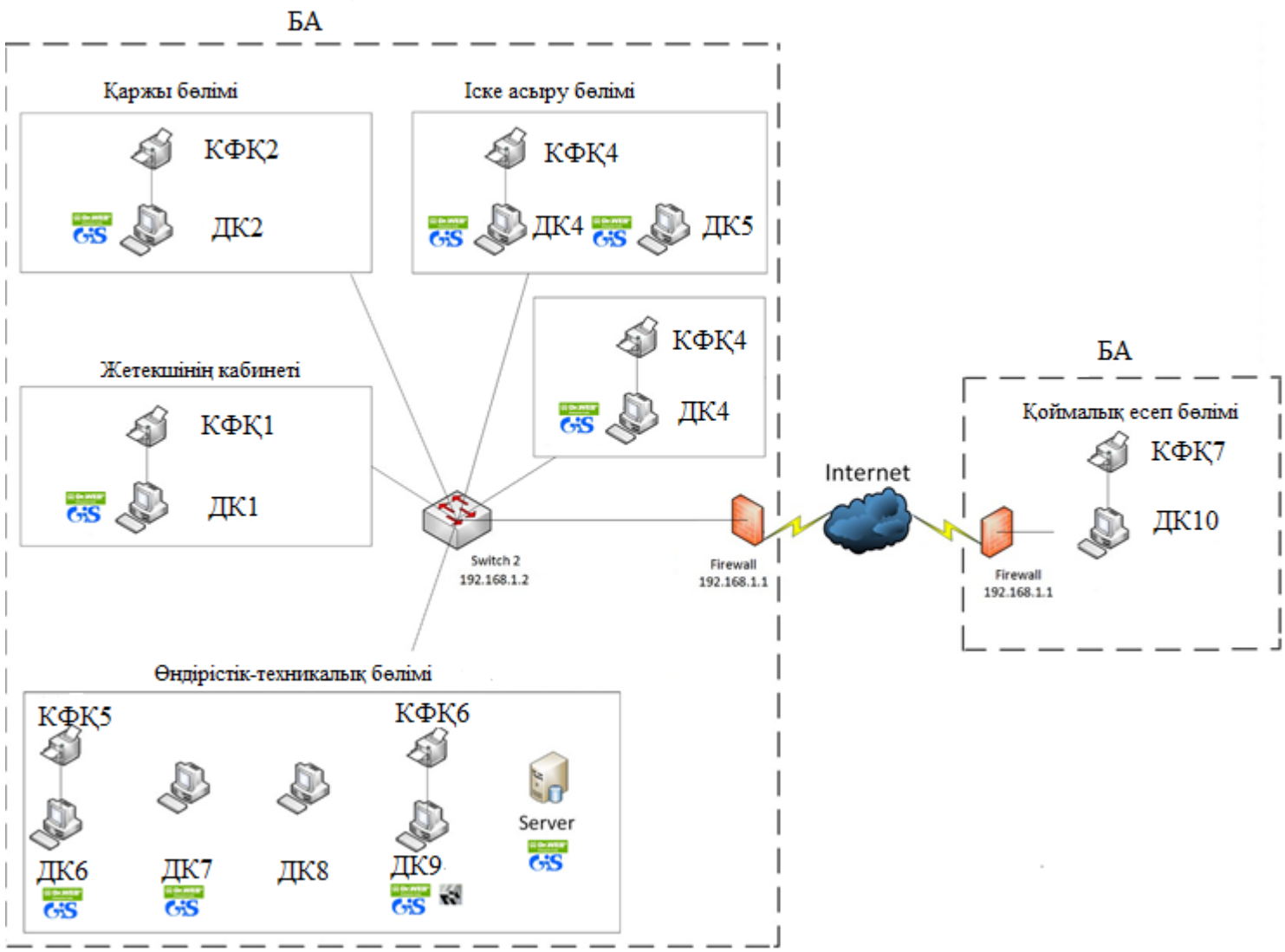
1. Бейнебақылау камераларын қосу;
2. Шақыру панельдерінің / камералардың болуы;
3. Экран;
4. Жарықтандыру;
5. Жады;
6. Интерфейстер;
7. Басқармасы;

Мұқият талдаудан кейін жоғарыда келтірілген критерийлерге, сондай-ақ Тапсырыс берушінің қажеттіліктеріне сүйене отырып, біз үшін ең қолайлы нұсқа "JEJA TFT 801 LCD" видеодомофоны болып табылады.

3.4 Тарау бойынша қорытынды

Осылайша, жұмыста жүргізілген талдаудың негізінде нақты ұйымдық-техникалық шаралар әзірленді және «INFINITE VIP GROUP» компаниясының үй-жайлары мен ақпараттық жүйелерінің анықталған өзекті қауіптерін бейтараптандыратын қорғаудың бағдарламалық-аппараттық бағыттары ұсынылды. Қорғау құралдарын 3.1-суретте көрсетілген. Және 3.2-суретте компания желісінің топологиясын көрсетіп кеттім.

3.1 сурет – «INFINITE VIP GROUP» компаниясының бас офисінің сызбасы



3.2 сурет – «INFINITE VIP GROUP» компаниясы желісінің топологиясы

4 Өмір-тіршілік қауіпсіздігі

4.1 Жұмыс орнындағы еңбек жағдайларын талдау

Жұмыстың мақсаты "INFINITE VIP GROUP" ЖШС-нің кеңсесіне бөгде енуден және бұзудан ақпараттық қорғау деңгейін арттыру болып табылады.

"INFINITE VIP GROUP" ЖШС-нің кеңсесінде, атап айтқанда IT бөлімінде жабдықтар мен жұмыс орындарынан басқа компьютерлер, серверлер, сорғыш және кондиционер бар. Бөлме жоспары 4.1-суретте көрсетілген. Төменде жұмыс кезінде қызметкерге не зақымдау келтіретінін айтамын:

– бөлмеде терезелер жоқ, бірақ бөлме сорғышпен және кондиционермен желдетіледі. Бірақ жұмыс кезінде сорғыш көп шу шығарады;

– бөлімнің барлық компьютерлерінде тыныш салқындатқыштар орнатылған. Бірақ серверде ыңғайсыздық тудыратын шулы салқындатқыш тұр, болашақта тыныш салқындатқышқа ауыстырады;

– барлық жарықтандыру құралдары (шамдары) төбеде орналасқан, осының арқасында олар жұмысшыға кедергі келтірмейді;

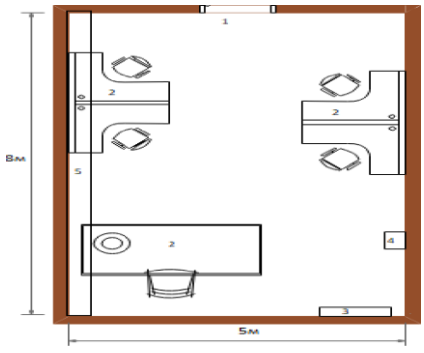
– электр жабдығымен дұрыс жұмыс істемегенде 220В токпен соққы алуға болады;

– компьютер алдында ұзақ жұмыс істеу салдарынан көз шаршайды және көру нашарлайды.

Антропогендік қауіптің әсері адамдардың қалыпты өмірін бұзады, төтенше жағдайларға (апаттық жағдайларға) және апаттарға, соның ішінде экологиялық апаттарға әкеледі. Қазіргі уақытта қауіпті табиғи құбылыстар мен процестердің зиянды әсерлерінің өсу үрдісі байқалуда. Нақты елдер мен өңірлердегі барлық нақты жағдайлар үшін олар халықтың өсуіне, оның шоғырлануына және салыстырмалы түрде шектеулі салалардағы материалдық байлықтарға, сондай-ақ дүлей зілзалалар генезисі сипатының өзгеруіне байланысты. Табиғатқа кірісе отырып және неғұрлым қуатты инженерлік кешендерді құра отырып, адамзат жаңа, өте күрделі жүйені қалыптастырады, оның даму заңдары әлі күнге дейін белгісіз [17].

Жұмыс орнының жоспары 4.1-суретте көрсетілген.

4.1 сурет – бөлме жоспары



1) Есік

2) Жұмыс орындары
3) Кондиционер
4) Сервер
5) Сорғыш.

Бөлменің өлшемдері: биіктігі – 3.2 м, ені – 5 м, ұзындығы – 8 м; Көрнекі еңбек жағдайлары үшін бөлме жарықтық жұмыс санатына жатады; - жасанды жарықтандыру - шамдар: жарықдиодты шамдар. ПК-мен жұмыс істеу кезінде қауіпті және зиянды факторлар пайда болады, және олардың әсері адам ағзасына зиян тигізіп, жарақат алуға әкеледі. Олардың шығу тегі мен нормалары бар негізгі факторлар ГОСТ 12.1.003-74/80 [18] және 4.1-кестеде келтірілген.

Ғылым ретінде өмір-тіршілік қауіпсіздігінің негізгі міндеті мен мақсаты - техносферадағы адамдарды антропогендік және табиғи шығу тегі зиянды әсерлерден қорғау, сонымен қатар жайлы және қауіпсіз өмір сүру жағдайларына қол жеткізу.

4.1-кесте — Негізгі қауіпті және зиянды факторлар

Фактордың атауы	Пайда болу орны	Шекті рұқсат етілген деңгей	Мүмкін салдары
Жоғары электр тізбегінің кернеу мәні	Әзірлеушінің жұмыс орны	ГОСТ 12.1.038-82 Uпр≤36В айнымалы токтың апаттық режимінде ұзақ әсер ету кезінде (LC артық).	Электр жарақаты
Электрлік доға	Тарату қалқаны	ГОСТ 12.2.007.3-75 ГОСТ 12.2.007.4-75 ГОСТ 12.1.004-85	Күйік, өрт
Жұмыс аймағының жеткіліксіз жарықтанды-рылуы	Бөлме	СНиП 23-05 Е=300 Лк	Шаршау, жарақаттану қаупі, көрудің нашарлау
Шудың жоғары деңгейі	Жұмыс орны	ГОСТ 12.1.003-88 жиілік жолақтары бойынша деңгей: 75 Дб-ден кем	Жүйке психикалық шамадан тыс жүктеме, есту мүшелерінің аурулары
Еңбек монотон-дылығы	Жұмыс орны	ГОСТ 12.1.003-80	Жүйке психикалық шамадан тыс жүктеме

4.2 Өрт қауіпсіздігі

Өртке қарсы су қондырғыларына қойылатын талаптар ҚР ҚНжЕ 2.02-05-2009 [19] құрылыс проект нормасымен анықталады. Электр тораптарына, соның ішінде электронды компьютерлерге қосылатын әртүрлі мақсаттағы құрылғылармен жұмыс істеу кезінде қадағаланды. Дұрыс жасалған құжат электрлік құрылғылармен жұмыс бөлмесінде сипаты дұрыс емес жағдайлардан туындайтын қауіпті жағдайларды болдырмауға көмектеседі.

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

Осыдан жұмыс компьютерлік кабинетінде мінез-құлық ережелерін сақтаңыз:

− тек таза, құрғақ қолдармен электр құрылғылармен қолдану;

− жұмыс аймағына кірмеңіз;

−ақаулы түрі бар электр сым ашасын розеткаға салуға тыйым салынады;

− жұмыс үдерісі кезінде сымның қыздыру дәрежесін бақылау қажет;

− қосқыштарды, қуат сымдарын, жерге тұйықтау құрылғыларын, монитордың артқы жағына түртуге тыйым салынады;

− жабдықты өзіңіз жөндеуге болмайды;

− электр лампаларының бетіне қағаз, шүберек және басқа да жанғыш материалдарды қоюға тыйым салынады;

− жоғарғы қуатты электр құрылғыларын бір розеткада қосуға болмайды;

− егер құрылыс кодекстерімен көзделмесе, сынып қа жиһаз және жабдықты қайта өңдеуді жүзеге асыруға тыйым салынады;

Егер ғимарат өртеле бастаған болса, қажет шаралар:

− барлық электронды жабдықты ажыратыңыз;

− өртті жою үшін сақтық шараларын қолданыңыз;

− мүмкіндігінше материалдық активтерді босату;

− тиісті қызметтерге өрт туралы есеп беру − кезекші, басқарушы бақылау пункті.

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

4.3 Электр қауіпсіздігі

Қоғамдық ғимараттардың электротехникалық құрылғылары Қазақстан Республикасының электр қондырғыларын орнату ережесіне, ҚР ҚНжЕ 2.04-01-2001 [20] талаптарына сәйкес жобаланады.

Электр қауіпсіздігі — адамдарды электр тогының, электр доғасының, электрлі магнит өрісінің және статикалық электрдің зиянды және қауіпті

әсерінен қорғанысын қамтамасыз ететін ұйымдастыру-техникалық шаралардың және құралдардың жүйесі.

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

Токтың келесі шектік мәндерін бөліп атауға болады:

− токты сезу шегі –ең аз сезілетін ток (0,5 -1,5мА);

− босатпайтын ток шегі –адам өз бетімен бұлшық еттері электродтармен қамтылған әрекеттен босана алмайтын ең аз ток мөлшері (6-10мА). Бұдан аз токтар босататын болып есептеледі;

− қаза ететін (100 мА және одан астам) ток.

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

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

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

Тиімді жерлендірген желілерде электр қауіпсіздігі қамтамасыз етілген деп жерлендіргіштегі φж потенциалы 10 кВ-тан аспайтын, ал жерлендіргіштің нәтижелі кедергісі жылдың кез-келген мерзімінде 0,5 Ом-нан аспайтын болып саналады.

4.4 Жарықтандыру жүйесі

Жарық беретін қондырғылардың жобалауы ҚР ҚНжЕ 2.04-05-2002 [21] нұсқаудағы қабылданған жалпы қағидаларға бағынады.

Жобаның жарық техника бөлімінде жарық сапасының көрсеткішін және жарықтандыру мағынасын, жүйесін, түрін және жарық әдістерін, жарық көздерімен жарық аспаптарын таңдауы орындалады.

Жарық аспаптарының түрі, қуаты және орналасуы жарық техникалық есептің нәтижесі бойынша таңдап алынады.

Жобалаудың тәжірибесінде жарық беретін қондырғылардың бірнеше нұсқаулары зерттелді. Нұсқаулар бір-бірінен бөлек немесе жиынтық сипаттамасының өзгешелігі (әртүрлі жарық жүйесі, әртүрлі шамдар мен жарық көздерінің типтері, шамдарды орнатудың әртүрлі биіктігі) арқылы ерекшеленеді.

Адамдардың қызмет етуіне жеткілікті табиғи және жасанды жарықтандыру атқарылатын жұмыстардың жоғары сапалылығын, қауіпсіздікті қамтамасыз етеді, еңбек жағдайларын жақсартып өнімділігін

арттырады, салдарынан, жұмыс жасаушылардың психологиялық күйіне әсер етеді. Жұмыс орнындағы жарықтың жеткіліксіздігі адам денсаулығына кері әсерін тигізеді, шаршап-шалдығу ұлғаяды, еңбек өнімділігі төмендейді, жарақат алу жиілеп, ауырлығы көбейеді. Жұмыс орындарын жарықтандыру сапасы көру жағдайы мен бағаланады да мына жағдайлармен сипатталады:

- үнемі жарықтандырылумен;
- кереғарлықтың болмауы;
- бетті және қоршаған кеңістікті жарықтандырудың жеткілікті және біркелкі таралған жарықтықтың болуы;
- көзді шағылдырмау;
- жарық түсетін беттерде айқын және терең көлеңкелердің болмауы.

Жасанды жарықтандыру үшін энергия үнемдейтін жарық көздерін пайдаланады. Тең қуаттылық кезінде, ұзақ мерзім қызмет атқаратын және ең көп жарық беретін жарық көздеріне жол беріледі. Жалпы қолданыстағы 100Вт және одан жоғары қуатты қызу лампаларын жарықтандыруға пайдалануға тыйым салынады.

4.5 Есептеу бөлімі

4.5.1 Жасанды жарықтандыру есептеу.

Есеп әдістемелік нұсқауларымен орындалды [22]. Пайдалану анализі әдісімен ІТ бөліміндегі жасанды жарықтандыруды есептеу. Есептеу бөлімі үшін жарықтандыруды, жарық көзін (жарық), көрсетілген облысқа немесе жұмыс офисіне шам түрін таңдаймыз. Жұмыс сыныптарын қалыпты жарықтандырумен қамтамасыз ету үшін қажетті жарықтандыруды орнату қуаты мен Емин қамтамасыз ету үшін шамдардың санын анықтаймыз. Бейнелеу жұмысын қалпына келтіру. Номиналды жарықтандыру-400 лк ғимарат, жер беті және басқа объектілер. LED шамдардың техникалық сипаттамалары 4.2 кестеде көрсетілген. Бұл ең гигиеналық және оны адамдар ұзақ уақыт болатын барлық бөлмелерде қолданамыз.

4.2 кесте-LED шамдардың техникалық сипаттамалары

Номиналды қуаты, Вт	LED типті шамдардың номиналды жарық ағыны	Шамдардың өлшемі, см	
		Диаметр	Қаңқалар бойынша ұзындығы
26	2880	19	4

Шам ретінде YUANFENG c129 - 2 26W / 2880 алынды. Шамның ұзындығы 1900 мм, ені 40 мм. Жасанды жарықтандыруды есептеу пайдалану коэффициентін қолдану арқылы жүзеге асырылады. Қабырға мен еден төбесінің көрініс коэффициенттері тең:

$$p\text{П}OT = 70\%;\ pCT = 50\%;\ \text{рПОЛ} = 30\%$$

Жұмыс бетінің үстінде шамды ілу биіктігін есептейміз:

$$\text{Н} = h - hP - hc, \qquad (4.1)$$

мұнда hc-шамнан жабынға дейінгі қашықтық, hc =0,11;
hp-жұмыс бетінің еденнен биіктігі;
hp=0,8 м. h-бөлме биіктігі, h=3.2 м

$$\text{Н} = 3{,}2 - 0{,}8 - 0{,}11 = 2{,}29\text{м}$$

Терезеден шамға дейінгі тиімді қашықтық:

$$L = \lambda \cdot \text{Н}, \qquad (4.2)$$

мұнда $\lambda = 1{,}2 \div 1{,}4$;

$$L = 1{,}2 \cdot 2{,}29 = 2{,}748\text{м}.$$

Қабырғадан жақын шамға дейінгі арақашықтықты қабырғада жұмыс жүргізілмейтін кезде мына формула бойынша анықтаймыз:

$$11 = (0{,}4 \div 0{,}5) \cdot L, \qquad (4.3)$$
$$11 = 0{,}4 \cdot 2{,}748 = 1{,}1\text{ м}.$$

Бөлме индексін анықтау:

$$i = l \cdot s/H(l + s), \quad (4.4)$$
$$i = 835 / 2{,}29(8 + 5) = 1{,}344$$

Бұл жағдайда пайдалану коэффициенті n = 49, қор коэффициенті КЗ=1,2 тең.

LED шамдардың санын мына формула бойынша анықтаймыз:

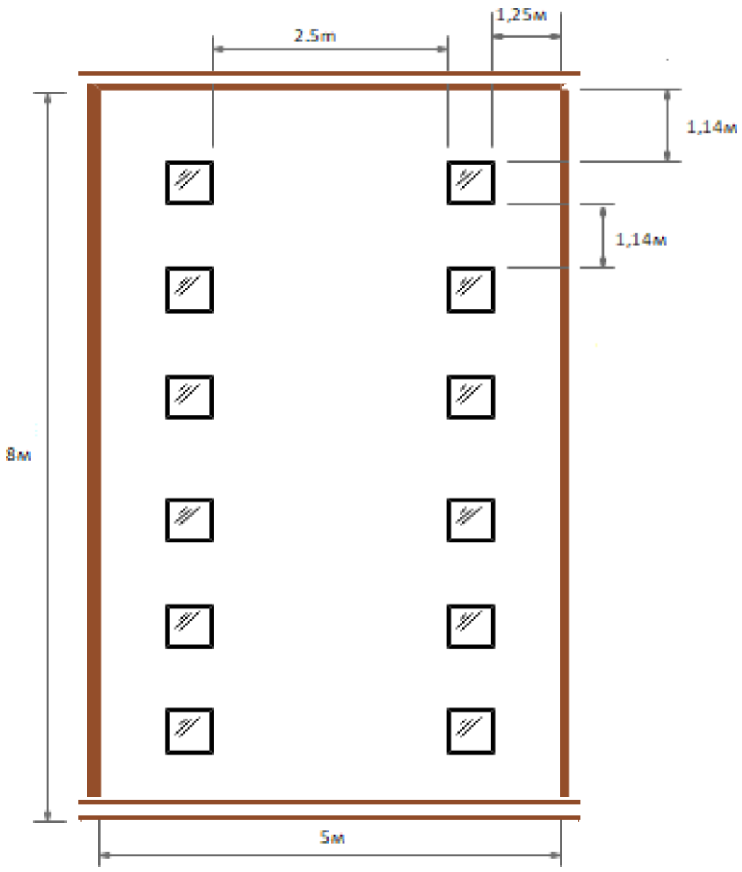
$$S = \frac{\text{Ен} \cdot \text{Кз} \cdot Z \cdot \text{Ат}}{m \cdot \text{Фл} \cdot n}, (4.5)$$

мұнда S- бөлме ауданы, 32 м^2;

Кз- қор коэффициенті;
Е- берілген ең аз жарық, Е=400 лк;
Z- жарықтандырудың біркелкі емес коэффициенті, Z=1,1;
m – арматурадағы шамдардың саны (количество ламп в светильнике);
Фл – таңдалған шамның жарық ағыны, Фл=2880 лм;
n – пайдалану коэффициенті, n = 410.

$$N = \frac{\text{Ен} \cdot S \cdot Z \cdot \text{Кз}}{N \cdot \text{Фл} \cdot n} = \frac{400 \cdot 32 \cdot 1{,}1 \cdot 1{,}2}{1 \cdot 2680 \cdot 0{,}49} \approx \frac{16896}{1411} \approx 12.$$

Жалпы алғанда, 400 люкс стандартты жарықтандыруды жасау үшін 12 арматура қажет, әр шамның қуаты 2 бВт болуы керек, демек, санитарлық нормаларға сәйкес келетін шамдардың санын көбейту немесе азайту қажет емес [19].



4.2 сурет – Шамдарды орналастыру жоспары

4.5.2 IT бөлімінің өрт қауіпсіздігін есептеу

Есеп әдістемелік нұсқауларымен орындалды [23]. ҚНжЕ 2.04-05-2002 [21] және РНТП-01-9 сәйкес, ғимарат өрттің даму қауіптілік дәрежесіне, жанғыш материалдардың функционалдық мақсатына және өрт жүктемесіне байланысты l-санаттағы топқа жатады. Өрт шығудың себебі:

– жабдық элементтерін тұтануы;

– өңдеу материалдарының ақаулы ажыратқыштардан, розеткалардан тұтануы;

– жабдықтың пайдалану шарттарын сақтамау, персоналдың дұрыс жұмыс істемеуі.

Өрт болған жағдайда тек бөлме ғана емес, сонымен қатар қымбат құрал-жабдықтар да зардап шегіп, бұл адам құрбандарына әкеледі. Сондықтан өрттерді анықтау және жою үшін шаралар қабылдануда. Оттың қайнар көздері компьютерлердің электр тізбегі, техникалық қызмет көрсету үшін пайдаланылатын құрылғылар, электр қондырғылары, кондиционерлер болады,

оларда қызып кететін элементтер әртүрлі бұзушылықтар нәтижесінде пайда болады және т.б. [20].

100 м^2-ге бір өрт сөндіргішті ескере отырып, ОU-5 отқа төзімді сөндіргіштер үшін сақтау бөлмелерінің өрт қауіпсіздігінің талаптарына сәйкес болады. Бөлменің жалпы ауданы 76,8 м^2 құрайды, сондықтан өрт сөндіргіш орнатылған. Өрт сөндіру құралы ретінде көмірқышқыл газы-хладонның аралас қоспасы қолданылады. Көлемді өрт сөндіру үшін md көміртек-хладон қос тотығының біріктірілген композициясының есептелген салмағы 5.6 формуласы шамасымен анықталады:

$$\mathrm{md} = \mathrm{k} \cdot \mathrm{gn} \cdot \mathrm{V}, (4.6)$$

мұнда k=1,2 – көмірқышқыл хладон құрамының ескерілмейтін шығындарын өтеу коэффициенті;

gn=0,04 көмірқышқыл-хладон құрамының нормативтік массалық концентрациясы.

V – бөлме көлемі 5.7 формуласы бойынша анықталады:

$$V = A \cdot \mathrm{B} \cdot \mathrm{H}, \qquad (4.7)$$

мұнда А = 8м – бөлменің ұзындығы;

В = 5м — бөлменің ені;

Н = 3,2м — бөлменің биіктігі.

Сонда:

$$V = 8 \cdot 5 \cdot 3{,}2 = 128 \text{ м}^3.$$

Демек

$$\mathrm{md} = 1{,}2 \cdot 0{,}04 \cdot 128 = 6{,}144 \text{ кг}.$$

х баллондарының есептік саны 12 литрлік 9.5 кг көмірқышқыл-хладон құрамының сыйымдылығы есебінен анықталады.

Магистральдық құбырдың ішкі диаметрі di(мм) 4.8 формуласы бойынша анықталады:

$$di = 12\ 32 = 17\text{мм}, \qquad (4.8)$$

12 магистральдық құбырдың эквивалентті ұзындығы 4.9 формула бойынша анықталады:

$$12 = k1 \cdot 1, (4.9)$$

мұнда k1=1,2 – жергілікті ысыраптарды ескермейтін өтем үшін құбыр ұзындығының ұлғаю коэффициенті;

l=3,2м – жоба бойынша құбырдың ұзындығы, сонда:

$$12 = 1{,}2 \cdot 3{,}2 = 3{,}84 \text{ м}.$$

Құбырдың эквивалентті ұзындығы мен диаметріне байланысты Q көмірқышқыл-хладон құрамының шығыны 1,4 кг/с тең.

Көмірқышқыл-хладон құрамын берудің есептік уақыты t, 4.10 формуласы бойынша анықталады:

$$t = \frac{md}{60 \cdot Q}, (4.10)$$

Сонда,

$$\mathrm{T} = \frac{6.144}{128 \cdot 1{,}4} = 0{,}0672\text{мин.}$$

Көмірқышқыл-хладон құрамының негізгі қорының массасы 4.11 формуласы бойынша анықталады:

$$\mathrm{M} = 1{,}1 \cdot \mathrm{md} \cdot (1 + \mathrm{k2} \cdot \mathrm{k1})$$

мұндағы к2 = 0,2-баллондар мен құбырлардағы көмірқышқыл-хладон құрамының қалдығын ескеретін коэффициент.

Сонда:

$$\mathrm{M} = 1{,}1 \cdot \mathrm{md} \cdot (1 + 0{,}2/1{,}2) = 4{,}72 \text{ кг.}$$

Осылайша, алынған нәтижелерден автоматты өрт сөндіру жүйесінің қалыпты жұмыс істеуін қамтамасыз ету үшін сыйымдылығы 12 литр көмірқышқыл-хладон құрамының 1 баллоны қажет, қоспаның салмағы 9.5 кг. Автоматты газды сөндіру қондырғыларында ГОСТ 12,4.009-83 [21] сәйкес автоматты іске қосуға арналған құрылғылар бар.

Өмір-тіршілігік қауіпсіздігіне талдау жүргізу нәтижесінде өрт ошағының пайда болуын болдырмауға мүмкіндік беретін қауіпсіздік жүйесі әзірленді.

5 Ақпараттық қауіпсіздік тәуекелдері

5.1 Ақпараттық қауіпсіздік тәуекелдерін талдау

Ақпараттық қауіпсіздік тәуекелі қауіпсіздік инциденттеріне байланысты қаржылық шығындардың (залалдың) және олардың іске асырылу ықтималдығының көбейтіндісі ретінде анықталады. Бұл анықтама ақпараттық жүйелердің әр түрлі архитектураларын қарау кезінде жарамды.

Ақпарат түрлі нысандарда болуы мүмкін. Ол қағазда жазылуы, электрондық түрде сақталуы, пошта арқылы немесе электрондық құралдарды пайдалану арқылы жіберілуі, экранда таратылуы немесе әңгімеде талқылануы мүмкін. Ақпарат қандай нысанда қабылданса да, ол әрқашан тиісті түрде қорғалуы тиіс.

Тәуекелдерді басқару тұрғысынан ақпараттық қауіпсіздік тәуекелдерін бағалау, ақпараттық жүйелер мен технологиялардың қазіргі әлсіздіктері мен қатерлерге жүйелі түрде ұшырайтын және ғылыми әдістермен және құралдармен талдау. Қатерлі оқиғалар туындаған кезде ықтимал залалды бағалау жүргізілді және ақпараттық қауіпсіздік тәуекелдерінің алдын-алу және басқару, сондай-ақ ақпараттың қауіпсіздігін барынша арттыратындай деңгейде қауіп-қатерлерді бақылау үшін қауіп-қатерге қарсы шаралар

ұсынылды. Ақпараттық қауіпсіздік тәуекелдерін бағалау үш негізгі кезеңнен тұрады: қауіптерді сәйкестендіру, осалдықтарды сәйкестендіру, активтерді сәйкестендіру [24] (5.1 сурет)

5.1 сурет – Ақпараттық қауіпсіздік тәуекелдерін бағалау элементтері

Ақпараттық қауіпсіздік тәуекелін бағалау процесі келесідей:

1) Ақпараттық активтерді анықтау, активтердің құндылығын белгілеу;

2) Қатерлерді талдау, қатерлердің ықтималдығын анықтау;

3) Ақпараттық активтердің осалдығын сәйкестендіру, осалдықтың дәрежесін анықтау;

4) Қауіптерді іске асыру (осалдықтарды пайдалану) бойынша оқиғаның басталу ықтималдығын есептеу);

5) Ақпараттық активтердің маңыздылығын және инциденттердің туындау мүмкіндігін үйлестіре отырып, ақпараттық актив үшін ақпараттық қауіпсіздік тәуекелінің мәнін есептеу орындалады.

Формуланың көмегімен тәуекелді есептеуді бейнелейміз:

$$Riskvalue = R(A, T, V) = R(L(T, V), F(Ca, Va)), \quad (1)$$

мұнда R — тәуекелді есептеу функциясы,

A — активтер,

T — қауіптер,

V — осалдықтар,

Ca — инцидент келтірген активтердің құны,

Va — осалдық дәрежесі,

L — осалдықтардың көмегімен инциденттерге келтіру қаупі,

F — қауіпсіздік оқиғаларынан туындаған шығындар.

Тәуекелдің мәнін анықтау тәуекелді бағалау нәтижелерімен және тәуекелді бақылау бойынша шараларды әзірлеумен байланысты, сондықтан бұл тәуекелді бағалау процесінде маңызды және күрделі кезең болып табылады. Бұл менің зерттеуімнің негізгі мәселесі.

Ұйым рұқсатсыз кіруді болдырмау мақсатында өз активтерін қорғау үшін түрлі қарсы өлшемдерді пайдаланады. Бірақ контрмерді қолдану және ақпараттық қауіпсіздікті басқару арқасында активтер бақылаудың жеткіліксіздігінен қауіптерден толық көлемде қорғалмаған.

Осылайша, тәуекелдерді бағалау ақпараттық қауіпсіздік тәуекелдерін басқарудағы маңызды қадамдардың бірі болып табылады. Іс жүзінде ақпараттық қауіпсіздік тәуекелдерін бағалау өте күрделі және толық белгісіздік процесс болып табылады [25]. Бағалау процесінде бар белгісіздік ақпараттық қауіпсіздік тәуекелін бағалау тиімділігіне әсер ететін негізгі фактор болып табылады. Сондықтан олар тәуекелдерді бағалау кезінде назарға алынуы тиіс. Алайда, бар тәсілдердің көпшілігі бағалау процесінде белгісіздікті өңдеу бойынша кейбір кемшіліктерге ие.

5.2 Есептеу бөлім

Бірінші кезекте ақпараттық қауіпсіздік тәуекелдерін есептеу үшін қорғалатын активтер анықталды, олар: операциялық жүйе, желілік инфрақұрылым және даму ортасы (PVS-Studio даму ортасына енеді және содан кейін ғана жұмыс жасай бастайды, осы дипломдық жобада Visual Studio даму ортасы ретінде қызмет етеді).

Ақпараттық қауіпсіздік тәуекелдері жұмыс тақырыбының ерекшеліктерін ескере отырып есептелген: осалдықтар мен БҚ бетбелгілерін анықтау үшін аспаптық құралдарды қолдану. Жоғарыда аталған активтер (қорғалмаған) үшін тәуекелдер есептелген. Осыдан кейін осы тәуекелдерді өңдеу шаралары ретінде осы жұмыста қаралған қорғау шаралары көрсетілді. Қалдық тәуекелдерді есептеу осы қорғау шараларын ескере отырып жүргізілді.

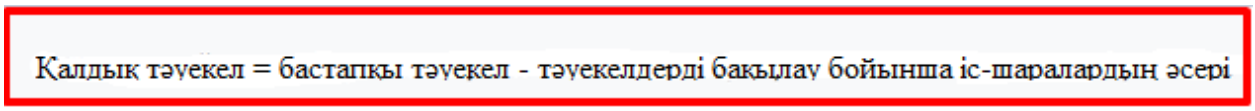
Тәуекелдерді талдау үшін ISO-27005 стандартынан алгоритмі таңдалды. Бірінші алгоритм бойынша есептеу (екі шкала бойынша) ISO-27005 стандартының Е қосымшасы негізінде жүргізіледі.

5.1 кесте – Активтердің құндылығы, қауіптер мен осалдықтар деңгейлері

Қауіптің туындау ықтималдығының дәрежесі		Төмен			Орташа			Жоғары		
Пайдалану оңайлығы		Н	С	В	Н	С	В	Н	С	В
Активтердің құндылығы	0	0	1	2	1	2	3	2	3	4
	1	1	2	3	2	3	4	3	4	5
	2	2	3	4	3	4	5	4	5	6
	3	3	4	5	4	5	6	5	6	7
	4	4	5	6	5	6	7	6	7	8

Қарапайым жалпы тәуекел рейтингі:
- төмен қауіп: 0-2;
- орташа қауіп: 3-5;
- жоғары қауіп: 6-8.

Қалдық тәуекел – бұл тәуекелдерді бақылау жөніндегі шаралардан кейін қалатын тәуекел. Қалдық тәуекелді есептеу 5.2-суретте ұсынылған формула бойынша жүзеге асырылады.



5.2 сурет – Қалдық тәуекелді есептеу формуласы

5.2 кесте – Ақпараттық қауіпсіздік тәуекелдерін талдау

№	Қауіптер	Осалдықтар	Тәуекелдің ең жоғары деңгейі	Тәуекелді өңдеу жөніндегі шаралар	Тәуекелдің қалдық деңгейі	Пікірлер, ресурстар, жауапты
Актив 1. Операциялық жүйе						
1	ОЖ жұмыс режимдері мен процесстерінің өзгеруі. Тергеу: бағдарламалардың қате жұмысы	Қорғаныс құралдарының дұрыс конфигурациясы	7	*Қорғау құралдары конфигурациясы; Операциялық жүйенің, әсіресе оның ішкі қорғау жүйесінің жұмыс істеуінің дұрыстығын тұрақты бақылау*	2	Жүйелік әкімші
2	Бағдарламалық өнімнің талданатын кодына рұқсатсыз кіру	Қауіпсіздік саясатын дұрыс орнатпау, жүйе әкімшісінің қателері	7	*Деректер конфигурациясы және ОЖ қауіпсіздік саясаты*	2	Жүйелік әкімші
3	Қаскүнеммен файлдық жүйені сканерлеу.Следствие: бағдарламаларды	Пайдаланушылар саясатының болмауы. Бағдарламалық	8	*Қауіпсіздіктің барабар саясатын ұйымдастыру және қолдау.*	3	Жүйелік әкімші

5.2 кестенің жалғасы

	көшіру немесе жою	қамтамасыз етудің қателіктері мен құжатталмаған мүмкіндіктері		*Барлық жүктелген файлдарды файл жүйесінде емес, деректер базасында сақтау.*		
4	Негізгі ақпаратты ұрлау. Салдары: кодты талдау алгоритмдерін түрлендіру	Салақтығы немесе немқұрайлылық қызметкерлердің. Болуы қорғау жүйесін айналып өтуге мүмкіндік беретін "қызметтік кіру"	8	*ОЖ-мен жұмыс істеу кезінде қауіпсіздік шараларын сақтау қажеттілігі туралы ОЖ пайдаланушыларын хабардар ету және осы шаралардың сақталуын бақылау*	3	Қауіпсіздік бөлімінің қызметкері
2 Актив. Желілік инфрақұрылым						
5	Берілетін деректерді бұрмалау	Берілетін трафикті жеткіліксіз қорғау, брандмауэрдің нашар конфигурациясы	6	Трафикті шифрлау, брандмауэр конфигурациясы	2	Желілік әкімші
6	Сниффер арқылы құпия ақпаратты (логин/парольдер) ұрлау	Брандмауэрдің нашар конфигурациясы, мәтіндік пішімде	6	Брандмауэр конфигурациясы, берілетін деректерді	2	Желілік әкімші

5.2кестенің жалғасы

		шифрланбаған деректерді жіберу	6	шифрлау және антисниффферлерді пайдалану	2	
7	Сессияны ұстап қалу және жалпы желілік ресурстарға қол жеткізу	Желілік қолжетімділікті бақылаудың болмауы	6	Сессияны компьютердің ір мекенжайына байланыстыру. Сессияны браузер агентіне байланыстыру. Сессияға берілетін параметрлерді шифрлау.	2	Желілік әкімші
8	Берілетін код фрагментін түрлендіру	Қорғалмаған сайтқа кіру	7	Трафикті сүзу. Сессияны браузер агентіне байланыстыру.	2	Желілік әкімші
3 Актив. Visual Studio даму ортасы						
9	Зиянды кодты енгізу	Вирусқа қарсы қорғаудың әлсіз шаралары және қолжетімділікті шектеу	6	Вирусқа қарсы қорғауды күшейту	1	Желілік әкімші
10	Бағдарламаға рұқсатсыз өзгерістер енгізу	Компанияның Интернет-порталы форумында пайдаланушылар	6	Атрибуттарды сүзгілеу; Қосымша деңгейіндегі	1	Желілік әкімші

5.2кестенің жалғасы

		қалдыратын хабарламалар мен түсініктемелерде атрибуттарды сүзудің болмауы, және осының салдарынан скрипт атрибуттары бар мәтінді енгізу мүмкіндігі		шабуылдардан қорғау		

Бастапқы бағалау кезінде тәуекелдер қолайсыз болып шықты (6-дан 8-ге дейін 8 балдық шкала бойынша), сондықтан барлық тәуекелдер үшін қорғау шаралары сипатталған. Тәуекелдерді өңдеу үшін шаралар енгізілгеннен кейін тәуекелдер қайта есептелді, қалдық тәуекелдер алынды. Қорғау шараларын ескере отырып, қайта есептеуден кейін қалған барлық тәуекелдер қолайлы болды (0-ден 2-ге дейін 8 балдық шкала бойынша).

Бұдан әрі CORAS бағдарламасында іске асырылған тәуекелдерді талдау компоненттерінің өзара байланысының әртүрлі диаграммалары ұсынылған (тәуекелдерді талдаудың жоғарыда көрсетілген кестесі негізінде).

5.2-суретте қорғалатын активтердің диаграммасы көрсетілген. Олар "жабдықтар мен аппаратура", "ақпараттық ресурстар" және "бағдарламалық құралдар"категорияларына бөлінген. Мысалы, "желілік инфрақұрылым" активі "жабдықтар мен аппаратура" және "ақпараттық ресурстар" санатына, "Операциялық жүйе" және "әзірлеу ортасы" активтері "ақпараттық ресурстар" және "бағдарламалық құралдар"санатына кіреді.

5.3-суретте қауіп моделінің диаграммасы көрсетілген. Диаграмма элементтері солдан оңға қарай: қауіптер көздері, осалдықтар, қауіп-қатерлерді іске асыру кезеңдері, қауіп-қатерлерді (инциденттерді) іске асырудан болған қауіп-қатерлерді (инциденттерді) іске асыру салдары, қауіп-қатерді іске асырудан болған активтер. Мысалы, "зиянкестер" қауіп көзі "брэндмауэрдің нашар конфигурациясы" осалдығын пайдалана отырып, "қниффер (логин/парольдер, талданатын кодтар) арқылы құпия деректерді ұрлауды" жүзеге асырады және жалпы желілік ресурсқа қол жеткізуге мүмкіндік алады. Осы қауіпті іске асырудың салдары "талданатын бағдарламалардың бастапқы кодтарын көшіру" Актив болуы мүмкін, оған қауіп – қатер бағытталған - "желілік инфрақұрылым" және "Операциялық жүйе".

5.4-суретте инциденттің туындау ықтималдығын есепке ала отырып, қауіптер моделінің диаграммасы көрсетілген. Оны 3-суретте көрсетілген диаграмма сияқты оқыған жөн, тек инциденттердің пайда болу ықтималдығы параметрі қосылған (жоғары, орташа, төмен). Мысалы, "талданатын бағдарламалардың бастапқы кодтарын түрлендіру" инцидентінің пайда болу ықтималдығы жоғары.

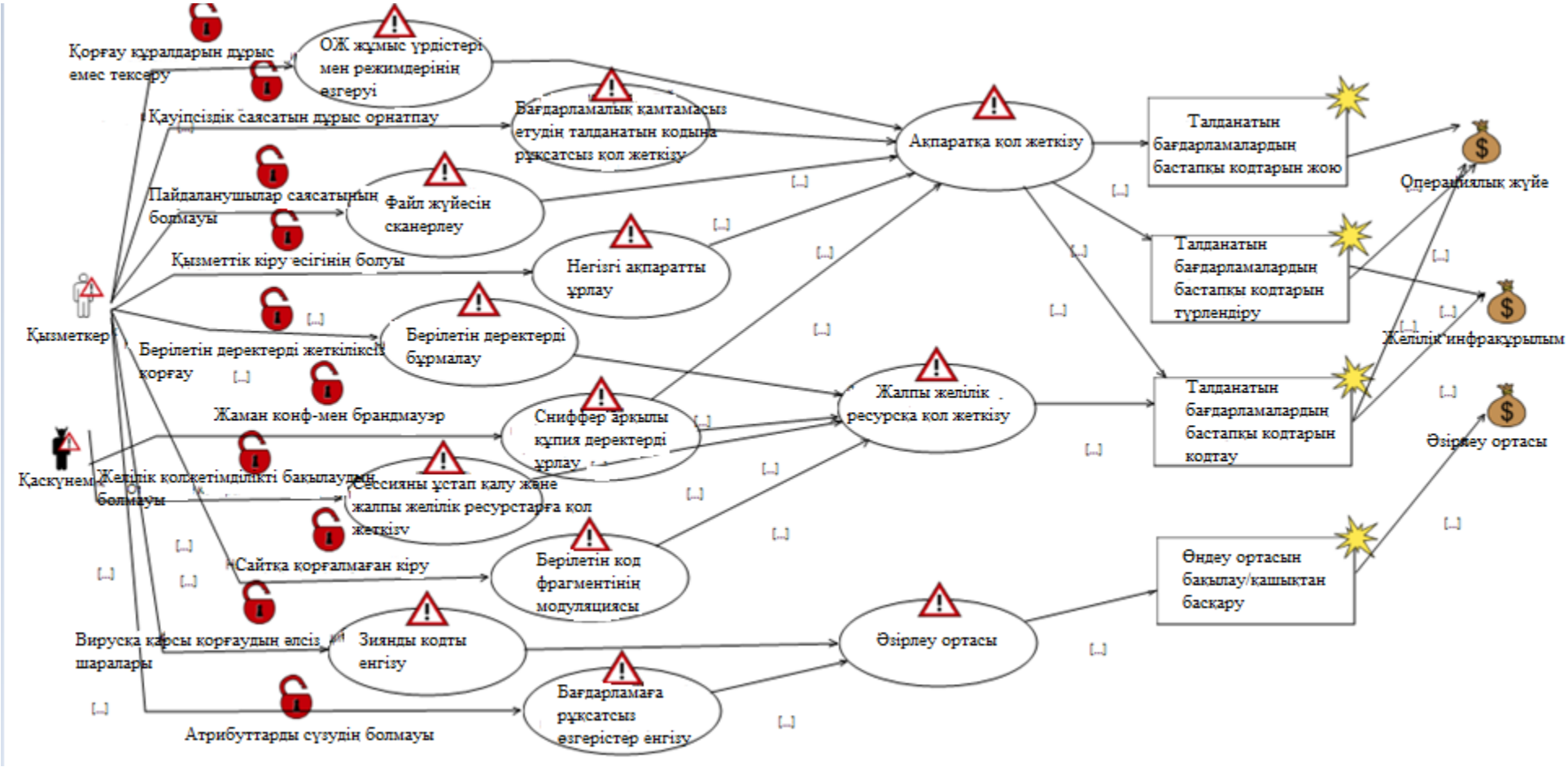
5.5-суретте қауіптердің әсер ету сипаттамалары бар тәуекелдер диаграммасы көрсетілген. Диаграмма элементтері солдан оңға қарай: қауіптер көздері, осалдықтар, қауіп-қатерлерді іске асыру тәсілдері, қауіп-қатерді іске асырудан активтерге залал шеккен қауіп-қатерлерді іске асырудың әсер ету дәрежесі. Мысалы, "қызметкер" "атрибуттарды сүзудің болмауы" осалдығын пайдалана отырып, "бағдарламаға рұқсатсыз өзгерістер енгізу" қаупін жүзеге асырады, бұл шабуылданатын активтерге – әзірлеу ортасына қатты әсер етті.

5.6-суретте қорғау шараларын ескере отырып, қауіптер моделінің диаграммасы көрсетілген. Оны 3-суретте көрсетілген диаграмма сияқты, жалғыз айырмашылығы бар оқу керек: осалдықтар мен қауіп-қатерлерді іске асыру тәсілдері арасында тәуекелдерді азайту үшін қорғау шаралары қосылды. Мысалы, "қызметтік кірулердің болуы" осалдығы үшін

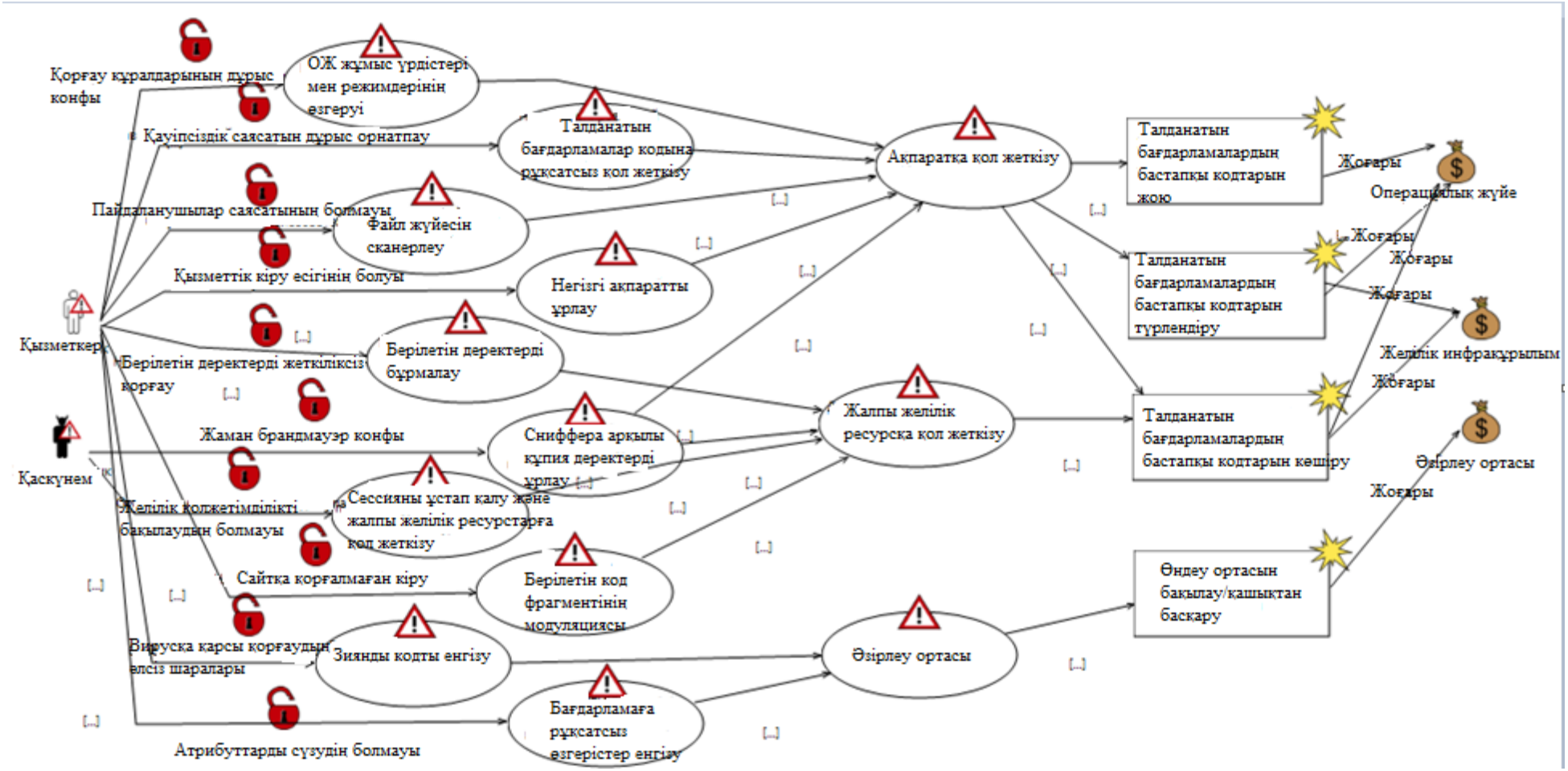
"сессиялардың қауіпсіздік шараларын, пайдаланушылар саясатын сақтау"қорғау шарасы енгізілді.

5.7-суретте жол берілмейтін тәуекелдер диаграммасы көрсетілген. Ол 5-суретте ұсынылған диаграмма базасында құрылған, алайда бұл диаграммада қауіп-қатерлердің жоғары дәрежелі әсер ететін тәуекелдер ғана көрсетілген.

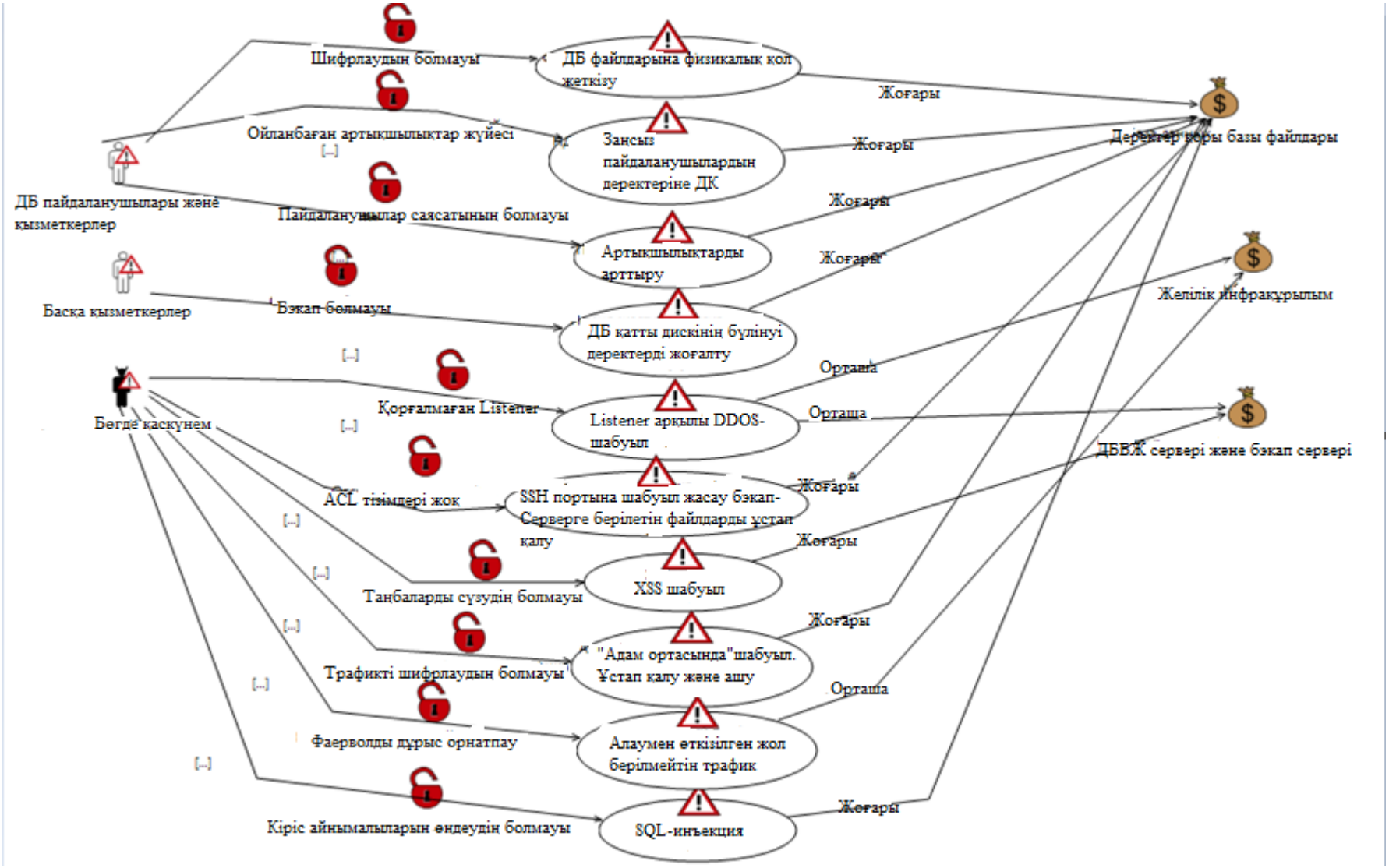
5.2 сурет – Активтер тізбесі



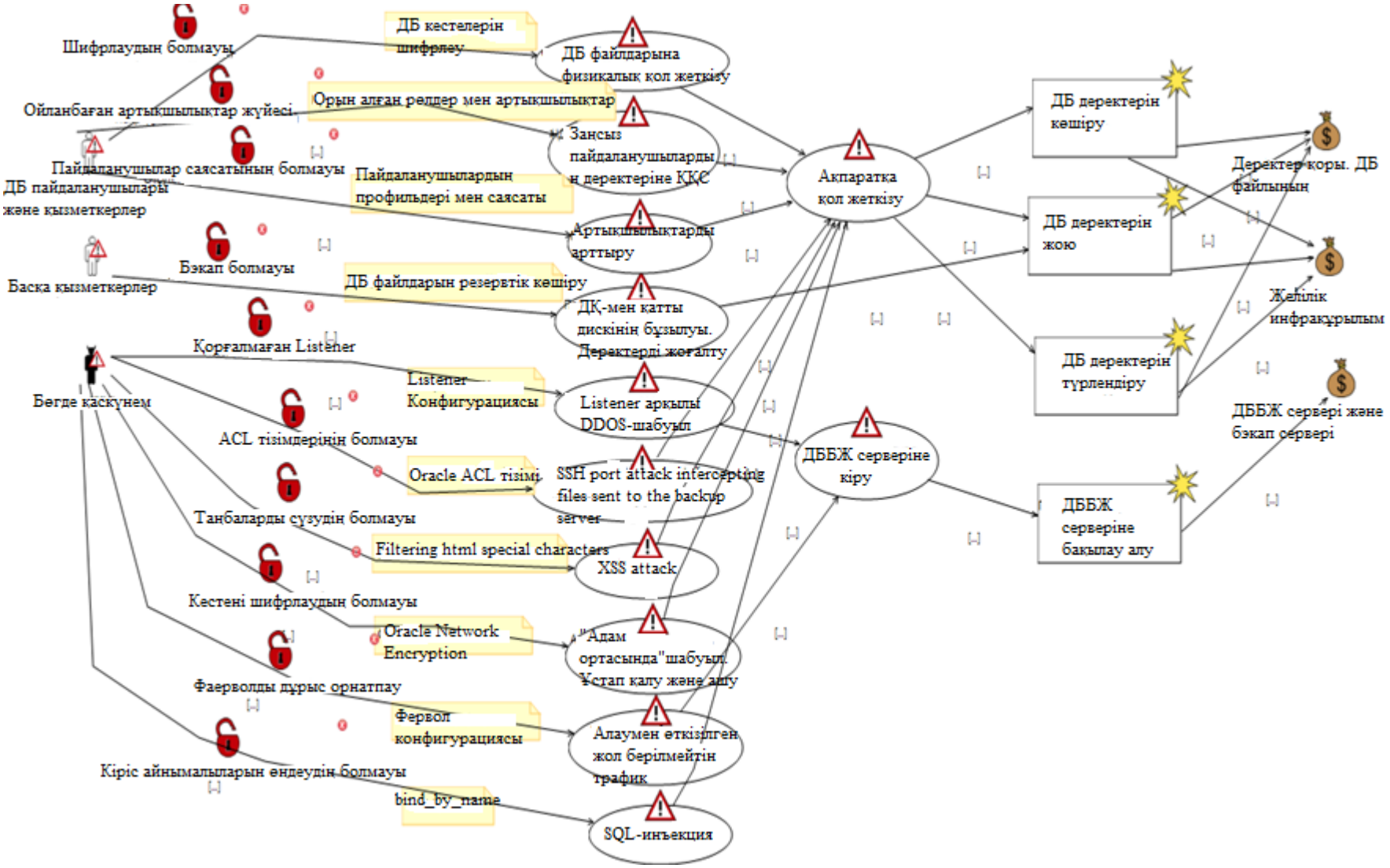
5.3 сурет – Қауіптер моделі



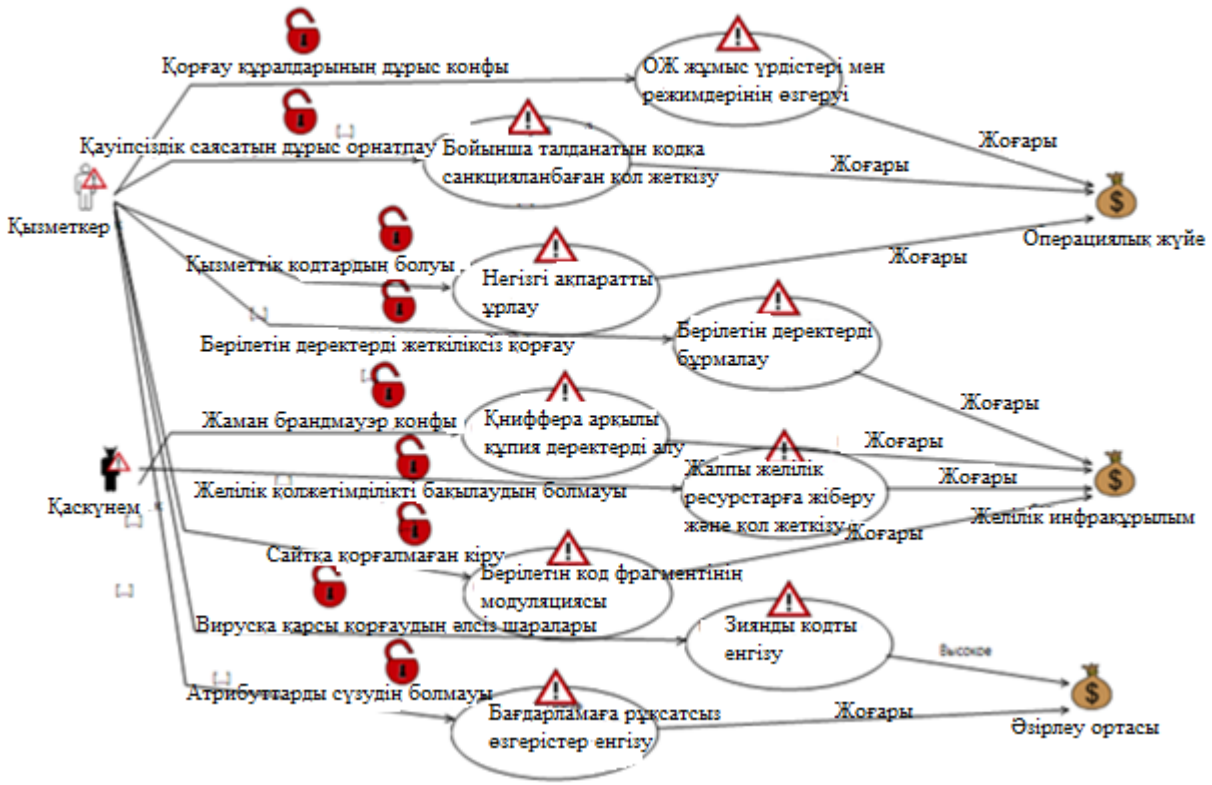
5.4 сурет – Инциденттің туындау ықтималдығын есепке ала отырып қауіптер моделі



5.5 сурет – Қауіптердің әсер ету сипаттамалары бар тәуекелдер диаграммасы



5.6 сурет – Қорғау шараларын ескере отырып қауіптер моделі



5.7 сурет – Жол берілмейтін тәуекелдер диаграммасы

Қорытынды: "Операциялық жүйе", "желілік инфрақұрылым" және "әзірлеу ортасы"қорғалмаған активтер үшін ақпараттық қауіпсіздіктің негізгі тәуекелдері сипатталып, есептелді. Есептеу нәтижесінде барлық тәуекелдер қолайсыз болып шықты (6-дан 8-ге дейін 8 балдық шкала бойынша), сондықтан барлық тәуекелдер үшін қорғау шаралары сипатталған. Тәуекелдерді өңдеу үшін шаралар енгізілгеннен кейін тәуекелдер қайта есептелді, қалдық тәуекелдер алынды. Қорғау шараларын ескере отырып, қайта есептеуден кейін қалған барлық тәуекелдер қолайлы болды (0-ден 2-ге дейін 8 балдық шкала бойынша). Тәуекелдерді өңдеу үшін шараларды енгізгеннен кейін "Операциялық жүйе" және "желілік инфрақұрылым" активтерінің тәуекелдері 3 есе азайтылды (орта есеппен), "әзірлеу ортасы" активтерінің тәуекелдері 6 есе азайды.

Қорытынды

Бұл жұмыста “INFINITE VIP GROUP» компаниясының қызметі мен ұйымдық құрылымына зерттеу жүргізілді, ол ұйым туралы жалпы ақпаратты зерделеуді, үй-жайларды және бағдарламалық-техникалық архитектураны, сондай-ақ «INFINITE VIP GROUP» компаниясы өңдейтін қолданыстағы ақпараттық жүйелер мен деректерді талдауды қамтиды.

Сонымен қатар жұмыста «INFINITE VIP GROUP» компаниясының үй-жайлары мен ақпараттық жүйелерінің қауіпсіздік қатерлері мен осалдықтарына талдау жүргізілді, сондай-ақ «INFINITE VIP GROUP» компаниясының үй-жайлары мен ақпараттық жүйелері үшін тәртіп бұзушының және қауіпсіздіктің өзекті қатерлерінің үлгілері әзірленді.

Алынған нәтижелер, ақпараттық қорғауды қамтамасыз етудің тұжырымдалған қағидаттары, мемлекеттік заңдар мен басқарушы құжаттар негізінде қорғаудың ұйымдық-құқықтық және инженерлік-техникалық бағыттары зерттелді, екінші тарауда айқындалған өзекті қатерлерді бейтараптандыру мақсатында ақпаратты қорғау шаралары іріктелді, сондай-ақ ақпаратты қорғау құралдарын орналастыру схемалары салынды.

Жұмыс нәтижесінде физикалық қол жеткізу жолымен де, бағдарламалық және бағдарламалық-аппараттық құралдарды қолдану жолымен де іске асырылатын қауіпсіздік қатерлеріне қарсы ақпараттық қорғау деңгейін арттыру бойынша нақты ұсыныстар ұсынылды.

Нәтижелерді мемлекеттік және коммерциялық ұйымдар ақпаратты қорғаудың заманауи интеграцияланған жүйелерін, сондай-ақ коммерциялық ұйымдарды деректерді өңдеуге қатысты басқа нормативтік құжаттарды жобалау үшін қолдана алады.

Әдебиеттер тізімі

1. "Ақпарат, ақпараттық технологиялар және ақпаратты қорғау туралы" 2006 жылғы 27 шілдедегі № 149-МЗ Мемлекеттік заң //[Электрондық ресурс], кіру режимі: http://www.consultant.kz/document/cons_doc_LAW _61798 /(өтініш берілген күні: 15.01.2020).

2. "Дербес деректер туралы" 2006 жылғы 27 шілдедегі №152-МЗ Мемлекеттік заң // [Электрондық ресурс], кіру режимі: http://www.consultant. kz /document/Cons_doc_LAW_61801 / (өтініш берген күні: 15.01.2020).

3. ГОСТ Р 50922-2006 "ақпаратты қорғау. Негізгі терминдер мен анықтамалар". М.: Стандартинформ, 2008. // [Электрондық ресурс] / Режим доступа: http://www.consultant. kz/cons/cgi/online.cgi?req=doc&base=EXP&n= 418509#06367720451532759 (Дата обращения: 15.01.2020).

4. Чукарин А.В. Бизнес-процессы и информационные технологии в управлении современной инфокоммуникационной компанией / А.В. Чукарин. - М.: Альпина Паблишер, 2016. - 512 с.

5. Жидко Е.А. Информационные риски как аргумент безопасного и устойчивого развития организаций / Е.А. Жидко, Л.Г. Попова // Информация и безопасность, 2010. – №4. – С. 543–552.

6. "Дербес деректер туралы" МЗ: Қазақстан Республикасының 2006 жылғы 27 шілдедегі N 152-ФЗ Мемлекеттік заңы / / [Электрондық ресурс], кіру режимі: http://www.consultant. kz/document/cons_doc_LAW_61801 / (өтініш берген күні: 15.01.2020).

7. Козин И.С. Метод определения опасности угрозы персональным данным при их обработке в информационной системе. 2017. С. 19-26.

8. Соловьев В.В. Улучшение защищенности распределенной информационной системы персональных данных на основе технологии VPN и терминального доступа // Информационные технологии и проблемы математического моделирования сложных систем. 2017. №18. С. 39-44.

9. Коломыцев М.В., Носок С.А. Маскирование таблиц базы данных с использованием технологии SQL // Защита информации. 2017. №19. С. 16-22.

10. Меликов У.А. Гражданско-правовая защита персональных данных // Вестник УрФО. Безопасность в информационной сфере. 2015. № 4 (18). С. 49-53.

11. Минбалеев А.В. Проблемные вопросы понятия и сущности персональных данных // Вестник УрФО. Безопасность в информационной сфере. 2012. № 2 (4). С. 4-9.

12. "Дербес деректердің ақпараттық жүйелерінде оларды өңдеу кезінде дербес деректерді қорғауға қойылатын талаптарды бекіту туралы" ҚР Үкіметінің 01.11.2012 №1119 Қаулысы // [Электрондық ресурс], қол жеткізу режимі: http://www.consultant.kz/document/cons_doc_LAW_137356/
(Өтініш берген күні: 15.01.2020).

12. Дербес деректердің ақпараттық жүйелерінде оларды өңдеу кезінде

олардың қауіпсіздігіне өзекті қауіп-қатерлерді анықтау әдістемесі. ҚР Фстэк, 2008 г.//[Электронды ресурс], кіру режимі:http://fstec.kz/component/attachments / download / 290 (жүгіну күні: 15.01.2020).

13. Дербес деректерді ақпараттық жүйелерде өңдеу кезінде дербес деректердің қауіпсіздігі тәуекелдерінің базалық моделі (Қазақстан ФСТЭК директорының орынбасары 2008 ж. 15 ақпанда бекіткен) / / [Электрондық ресурс], кіру режимі: https://fstec.kz/component/attachments/download/289 (өтініш берген күні: 15.01.2020).

14. СТО БР ИББС-1.0-2006 стандарты ҚР-ның банктік жүйесі ұйымдарының ақпараттық қауіпсіздігін қамтамасыз ету/ /[Электронды ресурс], қол жеткізу режимі: http://www.consultant.kz/document / cons_doc_LAW_69596 / (өтініш берілген күні: 15.01.2020).

15. Кудрявцев А.М. Киберустойчивость информационно-телекоммуникационной сети / М.А. Коцыняк, И.А. Кулешов, А.М. Кудрявцев, О.С. Лаутаи / СПб.: Бостон-спектр, 2015. – 150 с.

16. ГОСТ Р ИСО/МЭК 27002-2012 "Ақпараттық технология. Қауіпсіздікті қамтамасыз ету әдістері мен құралдары. Ақпараттық қауіпсіздік менеджменті нормалары мен ережелерінің жиынтығы " / / [Электронды ресурс], кіру режимі: http://protect.gost.kz/document.aspx?control=7&id=183918 (өтініш берген күні: 15.01.2020).

17. Ляшко В.Г. «Безопасность жинедеятельности», г. Тула, издательство Тульского государственного университета, 2015 – 236 с.

18. ГОСТ 12.1.003-74-80 «Система стандартов безопасности труда (ССБТ). Электробезопасность», ИПК Издательство стандартов, 2011 – 10 с.

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

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

21. ҚР ҚНжЕ 2.04-05-2002 – «Жасанды және табиғи жарықтандыру» - Сәулет, қала құрылысы және құрылыс саласындағы мемлекеттік нормативтер, Астана, 2002.

22. Абдимуратов Ж.С., Мананбаева С.Е. Безопасность жизнедеятельности. Методические указания к выполнению раздела «Расчет производственного освещения» Алматы: АИЭС, 2009. — 20с.

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

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

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

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

27. Bjorn, A.G. (January 2002). CORAS, A Platform for Risk Analysis on Security Critical Systems — Model-based Risk Analysis Targeting Security (***www.nr.no/coras***)

В қосымшасы

«INFINITE VIP GROUP» компаниясының АҚ қауіптерінің өзектілігін бағалау.

«INFINITE VIP GROUP» компаниясының қауіпсіздік қаупі	Қауіптің пайда болу ықтималдығы	Қауіпті жүзеге асыру ықтималдығы	Қауіпті жүзеге асыру қаупі	Қауіптің өзектілігі
Желі бойынша берілетін ақпаратты ұстаумен "желілік трафикті талдау" қаупі.	Төмен (2)	Орташа (0,35)	Төмен	Өзексіз
Парольдерді және басқа да деректемелерді оларды одан әрі пайдалана отырып, қолжетімділікті шектеудің заңсыз алу қаупі	Төмен (2)	Орташа (0,35)	Орташа	Өзекті
Қол жетімділікті шектеу атрибуттарын жария ету, беру немесе жоғалту қаупі	Төмен (2)	Орташа (0,35)	Орташа	Өзекті
Қолданбаларды қашықтан іске қосу қаупі	Төмен (2)	Орташа (0,35)	Төмен	Өзексіз
Желі бойынша құпия ақпаратты ұстап қалу қаупі	Төмен (2)	Орташа (0,35)	Орташа	Өзекті
Жедел жадтан және сыртқы есте сақтау құрылғыларынан қалдық ақпаратты оқу қаупі	Төмен (2)	Орташа (0,35)	Төмен	Өзексіз
Операциялық жүйе пайдаланатын жедел жады аймағынан ақпаратты оқу қаупі	Төмен (2)	Орташа (0,35)	Төмен	Өзексіз
Желідегі жұмыс станциясының нөмірі, физикалық мекенжайы, байланыс жүйесіндегі мекенжайы, аппараттық	Төмен (2)	Орташа (0,35)	Орташа	Өзекті

сияқты бірегей физикалық сипаттамалары бар пайдаланушылардың терминалдарын рұқсатсыз пайдалану қаупі.				
Криптографиялық шифрларды ашу қаупі	Төмен (2)	Орташа (0,35)	Төмен	Өзексіз
Жасырын деректерді беру арнасын іске асыру қаупі	Төмен (2)	Орташа (0,35)	Орташа	Өзекті
Заңды пайдаланушыны тікелей ауыстыру, кейіннен дезинформацияны енгізе отырып, жеке жолмен кіргеннен кейін ажырату мақсатында байланыс желілеріне заңсыз қосылу қаупі.	Төмен (2)	Орташа (0,35)	Төмен	Өзексіз
Бағдарламалық "бетбелгілерді" және "вирустарды"енгізу қаупі	Төмен (2)	Орташа (0,35)	Орташа	Өзекті
Аппараттық бетбелгілерді енгізу қаупі	Төмен (2)	Орташа (0,35)	Төмен	Өзексіз
Тыңдаушы құрылғыларды қолдану қаупі, қашықтықтан фото және бейне түсіру және т. б.	Төмен (2)	Орташа (0,35)	Төмен	Өзексіз
Агенттерді жүйе персоналы қатарына енгізу қаупі	Төмен (2)	Орташа (0,35)	Орташа	Өзекті
Желінің жұмыс істеуін қамтамасыз ету кіші жүйелерінің істен шығу қаупі	Орташа (5)	Орташа (0,35)	Орташа	Өзекті
Ақпаратты ұрлау, түрлендіру, жою	Орташа (5)	Орташа (0,35)	Орташа	Өзекті
Байланыс құрылғылары мен желілерінің жанама	Орташа (5)	Орташа (0,35)	Орташа	Өзекті

электромагниттік, акустикалық және басқа да сәулеленулерін, сондай-ақ ақпаратты өңдеуге тікелей қатыспайтын қосалқы техникалық құралдарға (телефон желілері, қоректендіру, жылыту және т.б. желілері) белсенді сәулеленудің нысаналарын ұстап қалу қаупі				
Қорғау құралдарын рұқсатсыз өшіру	Орташа(5)	Орташа (0,35)	Орташа	Өзекті
Жүйелік файлдар мен ақпаратты қорғау құралдарын қатардан шығару мақсатында модификациялау қаупі.	Төмен (2)	Орташа (0,35)	Төмен	Өзексіз
Бағдарламалық жасақтаманың және оның жұмыс істеу ортасының жұмыс жағдайлары бұзылған жағдайда жүйеде және қолданбалы БҚЕ-де осалдықтарды пайдалану негізінде ақпаратқа қол жеткізу қаупі	Төмен (2)	Орташа (0,35)	Төмен	Өзексіз
Қызметтік міндеттерін орындауға байланысты емес БҚЕ орнату	Төмен (2)	Орташа (0,35)	Төмен	Өзексіз
Байланыс арналарын абайсызда зақымдау қаупі	Төмен (2)	Орташа (0,35)	Төмен	Өзексіз
ДД қауіпсіздігіне қатер	Төмен (2)	Орташа (0,35)	Төмен	Өзексіз
Қызметкерлердің ақпаратты әдейі емес өзгерту (жою)	Төмен (2)	Орташа (0,35)	Төмен	Өзексіз
Қорғау құралдарын абайсызда ажырату	Төмен (2)	Орташа (0,35)	Төмен	Өзексіз

Электрмен жабдықтау жүйесінің істен шығуы	Төмен (2)	Орташа (0,35)	Төмен	Өзексіз
Табиғи апат.	Төмен (2)	Орташа (0,35)	Төмен	Өзексіз