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 Бердібаев Р. Ш.
(ғылыми дәрежесі, атағы, аты-жөні)
_____ «_____» _____2020ж.
(қолы)

ДИПЛОМДЫҚ ЖОБА

Тақырыбы: Университеттерде рұқсатты бақылау және басқару жүйесін жобалау

Мамандығы: 5В100200 – «Ақпараттық қауіпсіздік жүйелері»
Орындаған: Мұратбек Мұхаммед Батталұлы (аты-жөні) Тобы: СИБк-16-1

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)
_____ «_____» _____2020ж.
(қолы)

Тіршілік қауіпсіздігі бөлімі бойынша:
т.ғ.к доцент Жандаулетова Фарида Рустембековна
(ғылыми дәрежесі, атағы, аты-жөні)
_____ «_____» _____2020ж.
(қолы)

Мөлшер бақылаушы:
аға оқытушы Альмуратова Камшат Бимуратовна
(ғылыми дәрежесі, атағы, аты-жөні)
_____ «_____» _____2020ж.
(қолы)

Пікір беруші:
Төлеулиев Сырым Бимуратович
(ғылыми дәрежесі, атағы, аты-жөні)
_____ «_____» _____2020ж.
(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: Мұратбек Мұхаммед Батталұлы
(аты-жөні)

Жобаның тақырыбы: Университеттерде рұқсатты бақылау және басқару жүйесін жобалау

2019 ж. «11» қараша №146 университет бұйрығымен бекітілді.

Аяқталған жұмысты тапсыру мерзімі: «____» _____2020 ж.

Жобаға алғашқы деректер (талап етілетін зерттеу (жоба) нәтижелерінің параметрлері және зерттеу нысанының алғашқы деректері): "Castle" РББЖ және "Castle" БҚ бағдарламасы арқылы университетке рұқсатты бақылау және басқару жүйесі жобаланды. Университетке жабдықтардың толық қосылған жобасы, Windows 10 Pro, «Castle» РББЖ, БҚ «Castle», PHP кеңейтімі, Open Server бағдарламасы ДҚ-мен байланыс үшін, Sweet Home 3D бағдарламасы.

Диплом жобасындағы әзірленуі тиіс мәселелер тізімі немесе диплом жобасының қысқаша мазмұны: Мақсат: Рұқсатты бақылау және басқару жүйесі жайлы толық ақпарат беріп, РББЖ жүйесін университетке енгізу тиімділігін көрсету. Рұқсатты бақылау және басқару жүйесін Университетке енгізген жағдайда, қандай артықшылықтарға ие болатының және де қандай көмек тигізетіні жайлы қарастырылды.

Графикалық материалдардың (міндетті түрде дайындалатын сызбаларды көрсету) тізімі:
РББЖ жүйесінің зерттеу
Идентификация және аутентификация құралдарымен танысу

Қорғалатын объект пен жабдықтардың сипаттамаларымен танысу_____
Негізгі техникалық міндеттерді талдау_____

Castle РББЖ-ның сипаттамасы мен артықшылығын анализдеу_____
«Castle» бағдарламасының ерекшелігін талдау_____
Университет үшін РББЖ жүйесін жобалау_____
Жүйенің жабдықтарының орнатылуымен танысу_____
Бағдарламаны орнатуы мен жұмыс жасау принципімен танысу_____
Университет ғимаратына РББЖ орнатудың толық есебін талдау_____

Негізгі ұсынылатын әдебиеттер:

1. Тихонов В. А., Ворона В. А. Системы контроля и управления доступом, Москва, Горячая линия – Телеком, 2010_____
2. Castle. Система контроля и управления доступом. Руководство администратора, ООО «Агрегатор», 2020_____
3. Castle EP4, PRO4. Сетевые контроллеры. Инструкция по эксплуатации, ООО “Агрегатор”, 2016_____
4. Castle. Система контроля и управления доступом. Руководство пользователя, ООО «Агрегатор», 2020_____

Жоба бойынша жобаның бөлімдеріне қатысты белгіленген кеңесшілер

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

Диплом жобасын дайындау
КЕСТЕСІ

Бөлімдердің атауы, әзірленетін мәселелердің тізімі	Ғылыми жетекшіге ұсыну мерзімдері	Ескерту
1. РББЖ жүйесінің зерттеу	25.02. 2020ж.	
2. Castle РББЖ-ның сипаттамасы мен артықшылығын талдау	25.02. 2020ж.	
3. Жабдықтартың ерекшеліктерін талдау	25.02. 2020ж.	
4. «Castle» бағдарламасының ерекшелігін талдау	30.04. 2020ж.	
5.Университет үшін РББЖ жүйесін жобалау	30.04. 2020ж.	
6. Жүйенің жабдықтары мен бағдарламаның орнатылуы мен жұмыс жасау принципімен танысу	30.04.2020ж	
7. Деректер базасын сайтпен байланыстыру	30.04.2020ж	
8. РББЖ-ні орнатудың толық есебін талдау	30.04.2020ж	
9. АҚ тәуекелдерін талдау. Өмір-тіршілік қаіпсіздігі	10.05. 2020ж.	
10. Қорытынды	20.05.2020ж	

Тапсырманың берілген уақыты «25» ақпан 2020ж.

Кафедра меңгерушісі _____ (Бердибаев Рат Шиндалиевич)
(қолы)

Жобаның
ғылыми жетекшісі _____ (Шайкулова Актоты Алиевна)
(қолы)

Орындалатын тапсырманы
қабылдаған студент _____ (Мұратбек Мұхаммед Батталұлы)
(қолы)

Аңдатпа

Бұл дипломдық жобада "Castle" РББЖ және "Castle" БҚ бағдарламасы арқылы университетке рұқсатты бақылау және басқару жүйесі жобаланды. Жәнеде тек ақпараттық қауіпсіздік тұрғысынан ғана емес, сонымен қатар жалпы жұмыс жүйесі қандай артықшылықтарға ие болатының түсіндірілді. Осы мақсатта жобаланған жоспарға "Castle" жүйесі орнатылды және шығын бойынша есептер жүргізілді. Жүйенің жұмыс істеу принципі және оның бағдарламалық қамтамасыз етуі егжей-тегжейлі сипатталған.

Өмір-тіршілік қауіпсіздігі бөлімінде өрт сөндіру және жасанды жарықтандыру құралдарына есептеу жүргізілді, сонымен қатар администратордың еңбек жағдайларын, өрт кезіндегі әрекеттер, эргономикалық талаптар және электр қауіпсіздігі талданды.

Тәуекелдерді бағалау бөлімінде университетке РББЖ жүйесін орнатқаннан кейін туындайтын тәуекелдерді бағалаймыз. Жоба үшін екі параметр бойынша тәуекелдерді бағалау әдісі таңдалды. Кейін CORAS әдістемелерінің көмегімен тәуекелдерді талдаймыз.

Аннотация

В данном дипломном проекте была спроектирована система контроля и управления доступом в университет, с помощью СКУД «Castle» и программы ПО «Castle». И было объяснено какие преимущества и плюсы получит университет не только в плане информационной безопасности, но и в целом в рабочую систему. С этой целью, была установлена система «Castle» на спроектированный план, и проведены расчеты по затрате. Подробно был описан прицнип работы системы и его программного обеспечения.

В разделе Безопасность жизнедеятельности был проведен расчет на средства пожаротушения и искуственного освещения, также проанализированы условия труда администратора, поведение при пожаре, эргономические требования и электробезопасность.

В разделе Оценка рисков оцениваем риски, которые возникают после установления системы СКУД в университет. Для проекта был выбран метод оценки рисков по двум праматетрам. После, анализируем риски с помощью методологий CORAS.

Annotation

In this diploma project, a system for monitoring and controlling access to the University was designed using the "Castle" ACS and the "Castle" software program. And it was explained what advantages and advantages the University will get not only in terms of information security, but also in General in the working system. For this

purpose, the "Castle" system was installed on the designed plan, and cost calculations were made. The operating principle of the system and its software was described in detail.

In the section life Safety, a calculation was made for fire extinguishing and artificial lighting, as well as analyzed the working conditions of the administrator, fire behavior, ergonomic requirements and electrical safety.

In the section Risk Assessment, we assess the risks that arise after the establishment of the ACS system in the University. For the project, a risk assessment method was chosen based on two parameters. After that, we analyze the risks using CORAS methodologies.

Мазмұны

Кіріспе 8
1 Теориялық бөлім 9
1.1 РББЖ жүйесінің өзектілігі 9
1.2 РББЖ - ның ҚР бойынша стандарттары және заңдары 10
1.3 РББЖ - ның тарихы, алғаш пайда болған кезі 11
1.4 РББЖ-ның мақсаты, құрамы, міндеттері мен жіктелуі 15
1.5 Идентификация және аутентификация құралдары 18
1.6 Қорғалатын объект пен жабдықтардың сипаттамалары 31
2. Университет үшін РББЖ жүйесін әзірлеу 39
2.1 РББЖ жабдықтарың қосу 39
2.2 Бағдарламаны орнатуы мен толық сипаты 46
3 Университет ғимаратына РББЖ орнатудың толық есебі 67
4 Өмір-тіршілік қауіпсіздігі бөлімі 68
4.1 Жұмыс жағдайын талдау 68
4.2 Есептеу бөлімі 73
5 Ақпараттық қауіпсіздік тәуекелдері 78
5.1 Ақпараттық қауіпсіздік тәуекелдерін талдау 78
5.2 Есептеу бөлімі 79
Қорытынды 91
Әдебиеттер тізімі 92

Кіріспе

Осы дипломдық жұмыста рұқсатты бақылау және басқару жүйесін Университетке енгізген жағдайда, қандай артықшылықтарға ие болатының және де қандай көмек тигізетіні жайлы қарастырылды.

Заманауи техникалық құралдарды пайдалану арқылы, дұрыс ұйымдастырылған РББЖ жүйесі бірқатар міндеттерді шешуге мүмкіндік береді. Егер ең маңыздысын айтсақ:

- ұрлыққа қарсы әрекет;
- материалдық құндылықтарды зақымдауға қарсы әрекет;
- жұмыс уақытын есепке алу;
- студенттердің тәртібін (дисциплина) көтеру;
- қызметкерлер мен студенттердің уақытында келуін немесе кетуін бақылау;
- ақпараттың құпиялылығын қорғау;
- келушілердің ағынын реттеу;

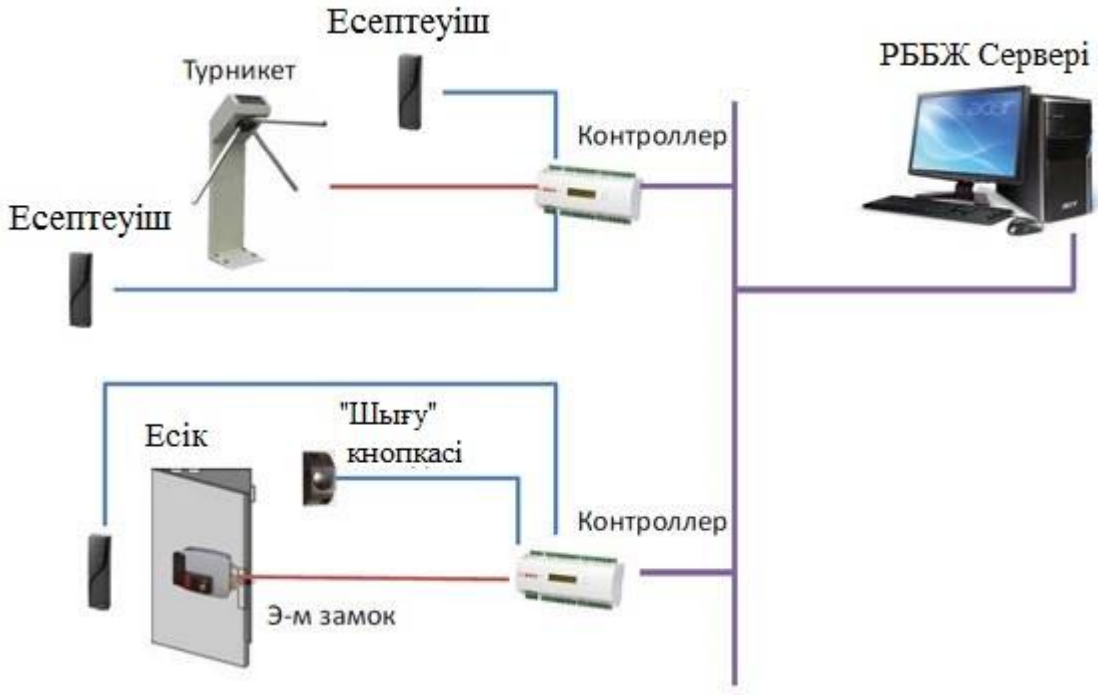
Жұмыстың басында жалпы рұқсатты бақылау және басқару жүйесі жайлы мәліметтер берілді. Яғни, қазіргі РББЖ-ның өзектілігі, қандай стандарт пен заңдарға жүгінетінің, қалай пайда болғаның, тарихы, оның мақсаттары, құрамы мен жіктелуі жайлы. Маңызды мәліметтерді қарастырып болған соң, университетке қандай жабдықтар мен бағдарламалар орнатылатының таңдап, олардың әр қайсысына жеке сипаттамалары айтылды. «Castle» жүйесін таңдау туралы шешім қабылданды.

Практикалық бөлімде, университетке «Castle» жабдықтарың орнату мен конфигурациялау жұмыстары сипатталумен басталады. Кейін «Castle» бағдарламасының компьютерге орнатылуы, серверлік пен клиенттік жұмыстарын қалай орындау және де қосылған барлық жабдықтарды бағдарламаға қалай тіркелетінің қарастырылды.

1 Теориялық бөлім

РББЖ (рұқсатты бақылау және басқару жүйесі) – бұл, белгілі бір объектіге зданияға, бөлмеге кіру уақытын тіркеу, сонымен қатар, оған қоса қауіпсіздікті қамтамасыз ету мақсатында кіру мен шығуды бақылауға бағытталған техникалық құралдардың жиынтығы болып саналады.

Идентификация жүйесінің көмегімен (карта, саусақ ізі, брелок, әмбебап код және тағы басқалары), бағдарлама, әрқайсысы үшін жеке оның жұмыс пен оқу кестесін, оқу уақытын, келу-кету уақытын, үзіліс мен түскі асқа жұмсалған уақытын деректер қорына сақтайды. Осының арқасында, мәліметтермен жұмыс жасауға жеңілденеді.



1.1 сурет– РББЖ жүйесі

1.1 РББЖ жүйесінің өзектілігі

Бүгінгі таңда, қорғалатын объектілерде қауіпсіз функцияланған жұмыс істеуін қамтамасыз ету мәселелері үлкен өзектілікке ие. Рұқсатты бақылау және басқару жүйелері (РББЖ), қауіпсіздікті қамтамасыз етудің интеграцияланған жүйелерінің ең міндетті элементі деп айтуға болады. Жүйе, рұқсатсыз басып кіруден тиімді қорғауға, объект бойынша адамдардың орын ауыстыруын немесе тіпті келмегенің байқауға жәнеде жалпы объектіде болып жатқан жағдайларды бақылауға зор мүмкіндік береді. Осы айтылған сөздерге негізделсек, РББЖ жүйесі объектіде адамдар мен көліктің кіруін бақылауды және тіркеуді тиімді

жүзеге асыру үшін жұмыс істейтін арнайы бағдарламалық және техникалық қамтамасыз ету кешені деп айтуға болады.

Дипломдық жұмысқа мен осы тақырыпты таңдаған себебім, университетке РББЖ жүйені дұрыс ойластырылып, орнатқан жағдайда қауіпсіздік пен қолжетімділікті арттырып және бақылап қана қоймай, жұмыс істеу жәнеде оқу үшін қандай қолайлы жағдайлар жасап, қандай плюстарға ие болатының көрсеткім келеді. Оған қоса, қазіргі таңда РББЖ жүйесі басқа да жүйелермен онай интеграцияланудың арқасында, өрт қауіпсіздігін бақылау және видеокамералармен нақты уақыт режимінде болып жатқан жағдайды бақылауға мүмкіндік береді.

1.2 РББЖ - ның ҚР бойынша стандарттары және заңдары

РББЖ бойынша Қазақстанда ҚР СТ 1699-2007 [13] стандарты 2007 жылдың 24 желтоқсанда бекітіліп қолданысқа енгізілді. Тексеру кезеңділігі әр 5 жыл.

Осы стандарт рұқсат етілген қол жеткізу және адамдарды, көлікті және өзге объектілерді ғимаратқа, үй-жайға, арнаулы аймақтар мен аумақтарға орналастыруды бақылайтын және басқаратын техникалық жүйелерге таратылады.

Осы стандартта сілтемелер мынадай стандарттарға пайдаланылды:

КР СТ 34.005-2002 Ақпараттық технология. Негізгі терминдер мен анықтамалар.

КР СТ 1174-2003 Объектілерді қорғауға арналған өрт сөндіру техникасы. Негізгі түрлері. Таратып улестіру және қызмет көрсету.

КР СТ 1201-2002 Ақпаратты қорғау құралдарын әзірлеу, келісу, бекіту және мемлекеттік тіркеу тәртібі.

КР СТ ИСО/МЭК 17799-2006. Ақпараттық технология. Қорғауды қамтамасыз ету әдістері. Корғалған ақпаратты басқару жөніндегі ережелер жинағы.

КР СТ ГОСТ Р 50571.22-2006 Ғимараттағы электроқондырғылар. 7-бөлім. Арнаулы электроқондырғыларға қойылатын талаптар. 707-бөлім. Ақпаратты өңдеу жабдықтарын жерге қосу.

КР СТ ГОСТ Р 50739-2006 Есептеу техникасы құралдары. Ақпаратты рұқсат етілмеген қол жеткізуден қорғау. Жалпы техникалық талаптар.

ГОСТ 2.601-2006 Конструкторлық құжаттаманың бірыңғай жүйесі. Пайдалану құжаттары.

ГОСТ 12.1.003-83 Еңбек қауіпсіздігі стандарттарының жүйесі. Шу. Жалпы қауіпсіздік талаптары.

ГОСТ 12.1.004-91 Еңбек қауіпсіздігі стандарттарының жүйесі. Өрт сөндіру қауіпсіздігі. Жалпы талаптар.

ГОСТ 12.1.006-84 Еңбек қауіпсіздігі стандарттарының жүйесі. Электромагнитті радиожиілік алаңдары. Жұмыс орындарында рұқсат етілген деңгейлер және бақылау өткізуге қойылатын талаптар.

ГОСТ 12.2.007.0-75 Еңбек қауіпсіздігі стандарттарының жүйесі. Электрлік техника бұйымдары. Жалпы қауіпсіздік талаптары.

ГОСТ 27.003-90 Техника сенімділігі. Сенімділік бойынша талап-міндеттердің құрамы мен жалпы ережесі.

ГОСТ 15150-69 Машиналар, құралдар және басқа техникалық бұйымдар. Әр турлі климаттық аудандарға арналған орындаулар. Сыртқы ортаның климаттық факторларының әсер етуі бөлігіндегі санаттар, пайдалану шарттары, сақтау және тасымалдау.

ГОСТ 28934-91 Электрмагнитті техникалық құралдар үйлесімділігі. Электрмагниттік үйлесімділік бөлігіндегі техникалық тапсырмалар бөлімінің мазмұны.

ГОСТ Р ИСО/МЭК ТО 10178-98* Ақпараттық технология. Жүйелер арасында мәліметтер беру және ақпаратпен алмасу. Жергілік есептеу желілеріндегі жергілікті топты басқару мекен-жайларының құрылымы және таңбалануы.

ГОСТ Р 51318.22-99 (СИСПР 22-97)* Электрмагнитті техникалық құралдар үйлесімділігі. Ақпараттық технология жабдықтарының өнеркәсіптік радиокедергілері. Сынау мөлшерлері мен әдістері.

1.3 РББЖ - ның тарихы, алғаш пайда болған кезі

Шамамен 20 жыл бұрын, байланыссыз қолжетімділік карталары, кеңінен қолданылған магниттік жолағы бар және Wiegand карталарының орнына, қауіпсіздік жүйелерінде алғаш рет қолданыла бастады [14].

Бүгінгі күнге дейін, жүздеген миллион пайдаланушылары бар HID Prox® деп аталатын алғашқы байланыссыз қол жетімділікті басқару технологиясы салалық стандартқа айналды. Бірнеше жылдан кейін Flexpass (Indala® компаниясынан) карталары шығарыла басталады. Олар HID Prox® сияқты бірдей жиілікті қолданады - 125 кГц және одан басқа жиіліктің орнына деректердің фазалық модуляциясын қолданатын карталар. Қол жетімділікті басқару жүйелерінде қолданылатын жиілігі 125 кГц болатын тағы бір танымал технология - бұл EM Microelectronics өндірушісінің амплитудалық модуляциясы бар EM-чиптеріне негізделген карталар.

Ең танымал 26 биттік ашық формат (кейде Wiegand деп аталады) болды, оны тіпті кез келген басқару тақтасы оқи алады. Екінші жағынан, ол ең аз қауіпсіздікті қамтамасыз етеді. Себебі, кез келген адам осы форматтағы карточкаларға тапсырыс бере алады және сіздің картаңыздың ерекше болатынына кепілдік жоқ.

Кейбір компаниялар жеке тапсырыстар үшін арнайы карта форматтарын шығара бастады, олардың бірегейлігі кепілдендірілді. Бұл карта форматтарында көбірек биттер қолданылады және олар бір жүйелік интеграторға немесе сатушыға арналған. Осылайша, үлкен түпкі пайдаланушылар физикалық және логикалық басқару деректерін толық бақылауға алады және болашақта олар өздері жеткізушілерін авторизациялай алады. Жақсы оқырмандар тек 26 битті емес, форматтары бар әртүрлі ұзындықтағы карталарды үздіксіз қабылдауы керек.

1.3.1 Смарт-картаның пайда болуы

13,56 МГцтік байланыссыз карталардың технологиясін (оларды смарт-карталар деп те атайды) пайда болуы карточкалардың көшірмелерін қорғауға деген нарықтық талаптардың артуымен байланысты болды.

Алғашқы байланыссыз смарт-карталар нарықта 1990-шы жылдардың соңында пайда болды және олар бұрынғыдан айтарлықтай ерекшеленді. Олар стандарттау жөніндегі халықаралық ұйымның (ISO) талаптарына сәйкес құрылды, әр түрлі криптографиялық механизмдерді қолдану арқылы қауіпсіз өзара әрекеттесу функциясын ие болды және картаның мазмұнын оқып қана қоймай, сонымен қатар ондағы ақпаратты сақтауға мүмкіндік берді. MIFARE® карталарын NXP Semiconductors тәуелсіз компаниясы (Philips негізін қалаған) қоғамдық көліктерге электрондық билеттер ретінде пайдалану үшін жасаған. ISO14443 байланыссыз карталар стандартына сәйкес келеді. Осы өндірушінің DESFire® деген кейінірек енгізілген карталары да ISO14443 стандарты бойынша жасалған, және ол қауіпсіздіктің жоғары деңгейін қамтамасыз етеді.

Тағы стандарт жайлы айта келсек, барлық ISO карталарда сериялық нөмір (CSN немесе UID) қолданылады. Бұл нөмір микропроцессорлық картада шифрланбаған жалғыз ақпарат болып табылады және оның негізгі міндеті карта мен оқырман арасында қауіпсіз өзара әрекеттесуді орнату болып табылады. Ол ешқашанда идентификация үшін қолдануға арналмаған. Алайда, оларды оқудың онайлығына және жайлығына байланысты оқырмандар оңай дайындалды. Бірақ, бұл өте қауіпті, себебі картаның сериялық нөмірі ерекше емес, сондықтан оны оңай жалғаның жасауға, не көшіруге болады. Оны қауіпсіздік жүйелері үшін пайдалануға тиімсіз.

1.3.2 Басқа тәсілді қарастып көру

13,56 МГц жиілігін қолданатын HID Global-дың iCLASS® деген карталары басынан бастап қауіпсіз қол жеткізуді басқару карталары ретінде қолданытың туралы ойлады. ISO15693 стандарттың арқасында ақпаратты үлкен қашықтықта оқуға мүмкіндік береді, бұл үздіксіз жұмыс жасауға және ыңғайлы қол жеткізуге ыңғайлы. Сондай-ақ, iCLASS® карталары ISO14443 стандартын қолдайтың

көптеген бағдарламаларды (мысалы, биометриялық деректерді сақтау, қолма-қол ақшасыз төлемдер саудасы және т.б.) оқуға немесе үлкен көлемді деректерді жазуға да қолданады. Стандарттар арасында қосылып жүру толығымен автоматтандырылған, яғни кез-келген операция үшін ең қолайлы стандартты таңдайды. iCLASS® карталары кез-келген қауіпсіз секторында шифрланған түрде сақталған форматты қол жеткізуді басқару үшін бағдарламаланған ақпаратымен жабдықталған.

Смарт-карталардың 125 кГц технологиялық карталардан түбегейлі айырмашылығы: деректерді оқырманға берер алдында бірқатар қауіпсіздік процестері жүреді, сол кезде карта мен оқырманның жарамдылығы тексеріледі жәнеде кодтау кілттері арасында ақпарат алмасу сессиясы өткізіледі. Осыдан кейін ғана деректер өзгертілген кілттермен шифрланады да, карта оларды жібереді.

Жетекші өндірушілер 125 кГц технологиясынан қауіпсіз 13,56 МГц технологиясына көшу үшін миграциялық шешімдерді ұсынады. Ол әр түрлі карта технологияларын бірдей оқи алатын көп форматты карталар мен оқырмандарды шығару болып табылады.

1.3.3 Көпдеңгейлік қорғау

Технологиялар бір орнында тұрмайды сол себептен қазіргі жаңа технология ертен ескіруі мүмкін. Осы мәселе РББЖ-ға да қатысы бар. HID Global уақыт сынағына жауап берді және идентификация саласындағы жаңа қауіпсіздік тұжырымдамасын жасады. Ол iCLASS SE® технологиясы.

iCLASS SE® технологиясы қауіпсіздікті көпдеңгейлі қорғаумен қамтамасыз етеді. Ол тамаша үйлесімділікке ие және осының арқасында ол Mifare®, DESFire® EV1, iCLASS®, HID Prox®, Indala®, EM Marin технологияларын қолдайды, оған қоса SIO™ (Secure Identity Object - қауіпсіз идентификация объектісі) жүйесі бар кез-келген тасымалдаушыны сенімді идентификация құралы ретінде пайдалануға мүмкіндік береді.

ICLASS SE® технологиясының негізгі идеясы - идентификация туралы мәліметтер (саусақ ізі, картадағы ақша, карта нөмірі) SIOTM-мен сенімді қорғалуы. SIO™ стандартты криптографиялық алгоритмдермен шифрланған (AES, 3DES, ...), цифрлық қолтаңбамен қол қойылған және тасымалдаушыда бекітілген.

iCLASS SE®-те қандай технологиялық жетістік бар:

1) РББЖ-да қолданылатын RFID-технологиясынан тәуелсіздік. Деректер SIOTM-мен қорғалуы маңызды.

2) Қауіпсіздікқа қауп туындаған жағдайда жабдықты ауыстырудың қажеті жоқ. iCLASS SE® технологиясы сізге РББЖ карталар мен оқырмандарды алмастырмай-ақ жаңартуға мүмкіндік береді.

3) SIOTM-ді түрлі тасылмалдаушы-картаға, NFC-телефонға және т.б. орнатуға болады.

1.3.4 Смартфондардың тағы бір ерекшелігі

HID Global компаниясы идентификация құралы ретінде NFC (Near Field Communication) смартфондарын қолданатын бірқатар пилоттық жобаларды жүзеге асырды. Жобалар HID департаментінің арнайы құралдарының көмегімен жүзеге асырылды, сол себептен ол коммерциялық мақсатта пайдалануға болмайды.

Қазіргі уақытта iCLASS SE® оқырмандарын iCLASS SE® карталарымен бірден сатып алуға және пайдалануға болады. NFC телефондарын идентификация құралы ретінде кейінірек қосуға болады. iCLASS SE® карталар мен оқырмандарды орнатуы және қолдануы дәл бұрынғы технологиялар сияқты. Тасымалдаушыға орнатылған деректердің қосымша қорғанысы сырттан көрінбейді. Карта мен оқырманның өзара әрекеттесу уақытына неғұрлым қуатты криптографиялық алгоритмдер әсер етпейді.

1.3.5 Одан әрі дамуы

Егер объектте әр түрлі технология карталары бар болғанмен, қазіргі қол жеткізу жүйесін пайдаланып жатқан клиент жана технологияларға көшуге қалап жатса, онда ол үшін ең тиімді таңдау - 125 кГц пен 13,56 МГц технология карталарын оқуға қабілеті бар multiCLASS SE® оқырмандары. Сонымен қатар бірнеше технологияларды біріктіретін карталар да бар.

Соңғы уақытта физикалық және логикалық қол жетімділік конвергенциясының қауіпсіздік жүйелерінде тұрақты үрдіс байқалды, былайша айтқанда – контактілі және контактісіз чипі бар бір картамен ғимаратқа / үй-жайға рұқсат және ақпараттық ресурстарға рұқсат. Мұндай шешім сізге жеке идентификацияларды құруға және басқаруға мүмкіндік береді, оны пайдалану транзакцияларды, коммуникацияларды және ақпаратқа қол жетімділікті қорғауды қамтамасыз етеді.

Карталарға суретті енгізу арқылы қамтамасыз етілетін визуалды қорғаудың қосымша мүмкіндіктерін туралы айтпау мүмкін емес. Бұл өтпелі суреттер, псевдоцветтер, нано-мәтін, тек ультракүлгін сәулемен көрінетін белгілер және т.б. Карталарды басып шығаруға және жекелендіруге арналған принтер саласы да қарқынды дамуда. Қазіргі заманғы ретрансферлік принтерлер жоғары сапалы суреттерді ұсынады және оны лазерлі гравюралық модульдермен, кодерлермен және ламинаттау модульдерімен толықтыруға болады.

1.4 РББЖ-ның мақсаты, құрамы, міндеттері мен жіктелуі

Қысқасы РББЖ дегеніміз ол кешендерге біріктірілген электрондық, механикалық, электротехникалық, аппараттық-бағдарламалық және тағы сондай сияқты құралдар белгілі бір тұлғалардың белгілі бір аймақтарға (аумақ, ғимарат, үй-жай) немесе белгілі бір аппаратура, техникалық құралдар мен заттарға (компьютер, автомобиль, сейф және тағы басқа) қол жеткізу мүмкіндігін қамтамасыз ететін немесе құқығы жоқ адамдарға қол жеткізуді шектейтін құралдар. Мұндай жүйелер күзетілетін объектінің аумағы бойынша адамдар мен көліктің орын ауыстыруын, персонал мен келушілердің қауіпсіздігін жүзеге асыра алады, сондай-ақ ұйымның материалдық және ақпараттық ресурстарының сақталуын қамтамасыз ете алады [30].

Мұндай жүйенің болуы ұйымның тиімді жұмысы үшін маңызды болғандықтан, қол жетімділікті бақылау және басқару жүйелеріне қызығушылық осы күнге дейін әлі артып келеді. Бақылау қауіпсіздік деңгейін тек арттырып қана қоймай, сондай-ақ персонал мен келушілердің мінез-құлқына жедел ден қоюға мүмкіндік береді. Көптеген ұйымдар үшін, әсіресе Университетке, маңызды міндет графикті бақылау және жұмыс немесе оқу уақытын есепке алу қажеттілігі болып табылады. Ұйымның барлық ерекшеліктерін ескере отырып, стандартты блоктардан қажетті конфигурацияларды құруға мүмкіндік беретін жүйелерге ерекше көңіл бөлінеді.

РББЖ жүйесінің міндеттері:

– дабыл қосылған жағдайда барлық есіктерді дереу бұғаттау;

– Қызметкерлер мен студенттердің жұмыс пен оқу уақытын есепке алуды автоматтандыру;

– Қызметкерлер мен студенттердің жұмыс немесе оқу орнында болуын автоматты тексеру;

– объектіге келушілердің орнын ауыстыруын бақылау.

Қазақстанның КР СТ ИСО/МЭК 17799 «Ақпараттық технология. Қорғауды қамтамасыз ету әдістері. Корғалған ақпаратты басқару жөніндегі ережелер жинағы» классификацияны, жалпы техникалық талаптарды мен сынау әдістерін белгілейтін стандарт РББЖ-ны былай бөледі:

– басқару тәсілі бойынша;

– бақыланатын кіру нүктелерінің саны;

– функционалдық сипаттамалары;

– бақылау объектілерінің түрі;

– рұқсат етілмеген қол жеткізуден жүйенің қорғалу деңгейі.

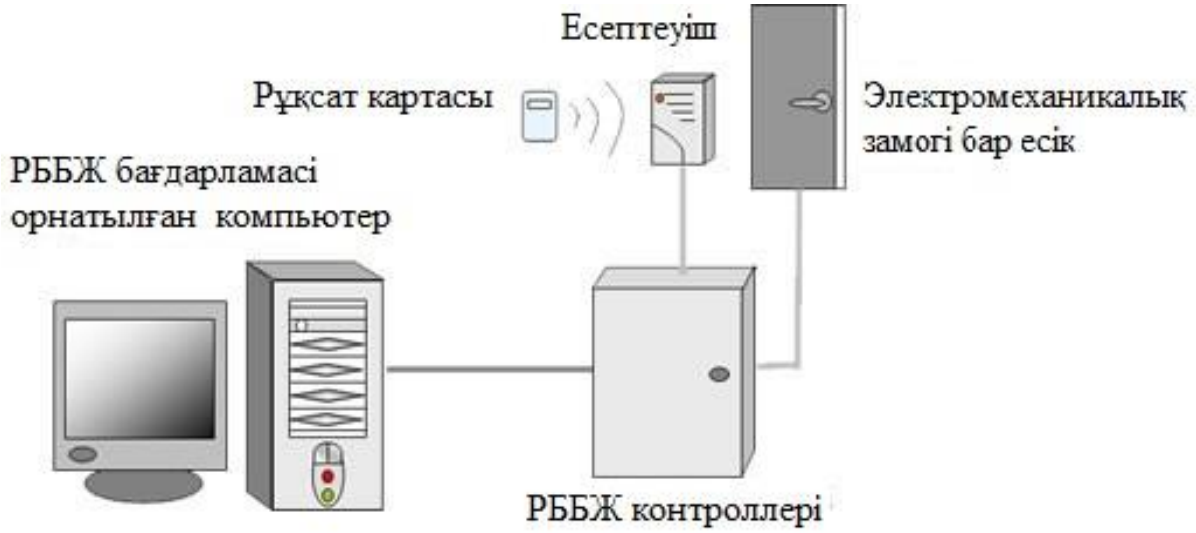
ҚР СТ 1699-2007 [13] стандартына сәйкес барлық РББЖ төрт классқа бөлінеді.

1-классты РББЖ- төмен функционалды және автономды режимде жұмыс істейтін және сәйкес идентификаторы бар барлық адамдарды қабылдайтын сыйымдылығы төмен жүйелер. Мұндай жүйемен қолмен немесе автоматты басқару элементтері бойынша жұмыс істеуге болады, сондай-ақ жарық және (немесе) дыбыстық дабылдар қолданылады.

2-ші класты РББЖ - көпфункционалды жүйелер. Олар бірдеңгейлі де, көпдеңгейлі де бола алады және автономдық пен желілік режимдерде де жұмыс жасай алады. Адам немесе адамдар тобына рұқсат күн, уақыт аралығы бойынша жүзеге асырылуы мүмкін. Жүйе оқиғаларды автоматты түрде тіркеуін және атқарушы құрылғыларды автоматты басқаруын қамтамасыз етуге қабілетті.

3-ші және 4-ші класстық РББЖ желілік болып табылады. Онда аса күрделі идентификаторлар және өзара желілік әрекеттесудің әртүрлі деңгейлері (клиент-сервер, Wigand немесе магниттік карталарды оқитын интерфейстер, мамандандырылған интерфейстер және тағы басқалар) қолданылады. Бүгінгі күні РББЖ-ның әртүрлі өндірушілердің түрлері, сондай-ақ оның компоненттері өте көп. Әрбір нақты өндірушінің РББЖ жүйесінің бірегейлігіне қарамастан, бәрі төрт негізгі элементтен тұрады: пайдаланушының идентификаторы (кілт немесе карта-пропуск), идентификация құрылғысы, басқарушы контроллер және атқарушы құрылғылар.

РББЖ-ның қысқаша схемасы 1.2-суретте көрсетілген. Барлық терминологияға, классификацияға және жалпы техникалық талаптарға байланысты негізгі ұғымдар мен анықтамалар ҚР СТ 1699-2007 стандартында көрсетілген [30].



1.2 сурет - РББЖ-ның қысқаша схемасы

Қол жеткізуді басқару және басқару жүйесінің жұмысын жеңілдетілген түрде былайша сипаттауға болады. Әрбір қызметкер немесе ұйымға тұрақты келуші идентификаторді (электронды кілт) алады ол пластикалық карта немесе

брелок болуы мүмкін жәнеде оның ішінде жеке коды болады. Электрондық кілттер аталған тұлғаларды тіркеу нәтижесінде жүйе құралдарының көмегімен беріледі. Паспорт мәліметтері, фотосуреттер (видео) және электрондық кілт иесі туралы басқа ақпарат жеке электрондық карточкаға енгізіледі. Иесінің жеке электрондық картасы және оның электрондық кілтінің коды бір-бірімен байланысты және арнайы ұйымдастырылған компьютерлік деректер базасына енгізілген.

Бақылауға жататын ғимаратқа немесе бөлмеге кіре берісте оқу құралдары орнатылады, олар карточкадан олардың жеке кодын және иесінің қол жеткізу құқығы туралы ақпаратты оқиды және кейін бұл ақпаратты жүйе контроллеріне жібереді.

Жүйеде әрбір кодқа карта иесінің құқықтары туралы ақпарат сәйкестікке қойылған. Осы ұсынылған ақпараттарды мен жағдайды ескере отырып салыстыру негізінде жүйе шешім қабылдайды: контроллер есікті (құлыптар, турникеттер) ашады немесе бұғаттайды, бөлмені күзет режиміне ауыстырады, дабыл белгісін қосады және тағы басқалар. Карточкаларды ұсынудың барлық фактілері мен оларға байланысты әрекеттері (өту жолдары, дабылдар және тағы басқалар) контроллерде тіркеледі және компьютерде сақталады. Карточкаларды ұсынудан туындаған оқиғалар туралы ақпарат одан әрі жұмыс уақытын есепке алу, еңбек тәртібін бұзулуы жайлы және тағы басқалары бойынша есепке алу үшін қажет. Ұйымдардағы қатынауды бақылаудың төрт негізгі нүктесін бөліп көрсетуге болады: өтулік(проходной), кеңсе бөлмелеры, аса маңызды бөлмелер және автокөліктің кіруі/шығуы.

Тексеру тәсіліне байланысты РББЖ-ны бірнеше түрге ажыратуды үсінді:

1) қолмен (ручной) (жеке тұлғаның түпнұсқалығын анықтауды иесінің фотосуреті бар ұсынылған рұқсаттама негізінде контролер жүзеге асырады);

2) механикаландырылған (ручнойға ұқсас автоматты сақтау және рұқсатнамаларды ұсыну элементтері бар тексеріс);

3) автоматтандырылған (пользовательдың идентификациясын мен жеке атрибуттарды тексеру электрондық автоматты түрде жүзеге асырылады, ал аутентификация мен рұқсат беру туралы шешімді КПП операторы қабылдайды)

4) Автоматты (барлық тексеру және шешім қабылдау процедурасы компьютермен жүзеге асырылады).

Кешенді жүйелермен орындалатын функциялар жиынтығы объектіде әртүрлі бақылау міндеттерін орындау үшін бақылау жүйесін пайдалануға мүмкіндік береді. Қойылған міндетке байланысты тиісті РББЖ-ны таңдауға болады. Шағын РББЖ қажетсіз адамдардың кіруін болдырмауға, ал қызметкерлерге тек қажет бөлмелерге қол жеткізуге құқығын көрсетуге мүмкіндік береді. Неғұрлым күрделі жүйе қолжетімділікті шектеуден басқа, әрбір қызметкерге жеке жұмыс кестесін тағайындауға, бір күн ішіндегі оқиғалар туралы ақпаратты сақтауға және қарауға мүмкіндік береді. Кешенді РББЖ

қауіпсіздік және тәртіп мәселелерін шешуге, кадрлық және бухгалтерлік есепті автоматтандыруға, күзетшінің автоматтандырылған жұмыс орнын құруға мүмкіндік береді. Жүйенің құрылымын және оның аппаратурасын таңдау кезінде оның сипаттамаларына мұқият назар аудару қажет. Олар:

– оның құны;
– жұмыс істеу(Функционирование) сенімділігі;
– жылдамдығы;
– пайдаланушыны тіркеу уақыты;
– жад сыйымдылығы;
– зұлымдық әрекеттерге төзімділігі;
– заңды пайдаланушыға қате шешім қабылдап кіргізбеу ықтималдығы (1-ші түрдегі қателер);
– заңсыз пайдаланушыға қолжетімділікті қате ұсыну ықтималдығы (2-ші түрдегі қателер)

1.5 Идентификация және аутентификация құралдары

Пайдаланушы идентификаторы - пайдаланушыны анықтайтын құрылғы немесе белгі. Идентификациялау үшін атрибутты және биометриялық идентификаторларды қолданылады. Атрибутты идентификаторлар ретінде рұқсат белгілерінің автономды тасымалдаушылары пайдаланылады: магниттік карточкалар, байланыссыз проксимит-карталар, "тамемори" брелкилары, түрлі радиобрелкилар, паайдаланушының көзі, саусақ іздері, алақан іздері, бет белгілері және басқа да көптеген физикалық белгілер. Әрбір идентификатор белгілі бір бірегей екілік кодпен сипатталады. РББЖ-ға әрбір кодқа иесінің құқықтары мен артықшылықтары туралы ақпарат қойылады [30].

Қазіргі уақытта мынандай идентификаторлар қолданылады:

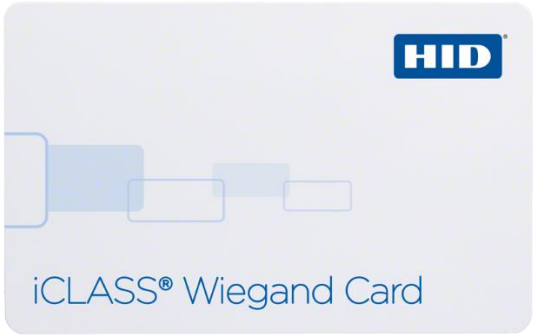
– байланыссыз радиожиілік проксимит-карталары (proximity) - қазіргі уақытта ең перспективтік карта түрі. Байланыссыз карточкалар қашықтықта жұмыс істейді және нақты позициялауды талап етпейді. Бұл олардың тұрақты жұмысын және пайдалану ыңғайлылығын, оған қоса жоғары өткізу қабілетін қамтамасыз етеді;

1.3 сурет - Байланыссыз радиожиілік проксимит-карталары

– магниттік карталар - ең кең таралған түрінің бірі. Төменэрцитивті және жоғарыэрцитивті магниттік жолағы бар және әр түрлі жолдарға жазылған карталарды айтады;

1.4 сурет - Магниттік карталар

– Виганда карталары (Wiegand) - тікбұрышты гистерезис циклі бар магнитті қорытпаны ашқан ғалымның аты бойынша аталған;



1.5 сурет - Виганда карталары (Wiegand)

– штрих-кодтық карталар - картаға штрих-код салыну арқылы жұмыс. Осыдан күрделірек нұсқасы бар - штрих-код тек инфрақызыл жарықта ғана көрінетін материалмен жабылады және оқу ИК-облысында жүреді;

1.6 сурет - Штрих-кодтық карталары

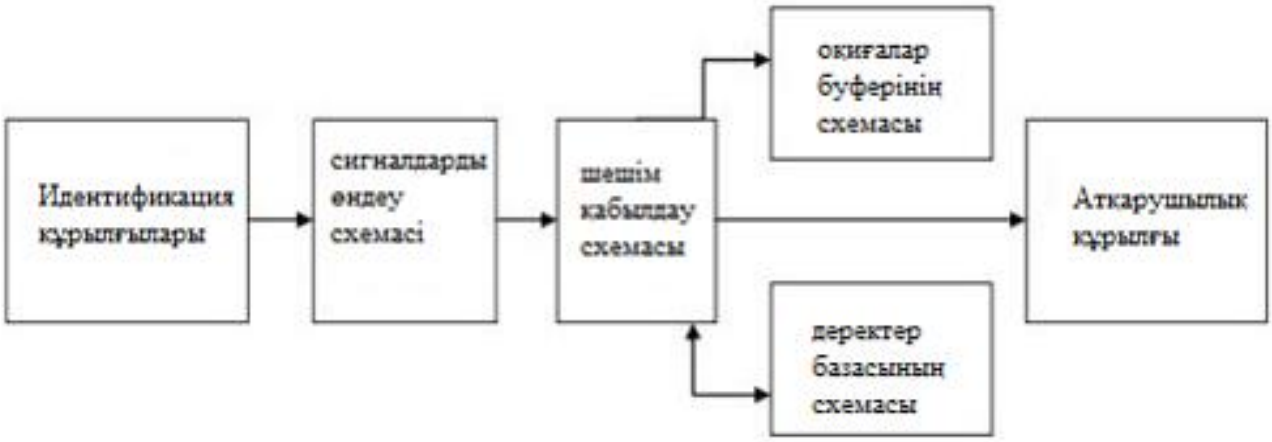
– кілт-брелок "тач-мемори" (touch-memory) - ішінде ПЗУ чипі орналасқан металлдан жасалған таблетка.

1.7 сурет - Кілт-брелок "тач-мемори"

1.5.1 Контроллерлер

Контроллерлер - идентификаторлық есептегіштерден ақпаратты өңдеуге, шешім қабылдауға және атқарушы құрылғыларды басқаруға арналған құрылғылар. Осы контроллерлердің арқасында өткізу пункттерінен өтуге рұқсат беріледі. Контроллерлер деректер базасының және оқиғалар буферінің сыйымдылығымен, қызмет көрсетілетін идентификация құрылғыларымен ерекшеленеді [30].

Кез келген РББЖ контроллері төрт негізгі бөліктен тұрады (1.2-сурет): есептеуіш, сигналдарды өңдеу схемасі, шешім қабылдау және оқиғалар буферінің схемасі.



1.8 сурет - РББЖ контроллерінің схемасы

Карта есептеуіші (идентификация құрылғысы) ақпаратты контроллердің сигналдарын өңдеу схемасына жібереді. Бұдан әрі сандық түрдегі ақпарат шешім қабылдау схемасына беріледі, ол оқиғалар буферінің схемасына өтуге әрекет ету фактісін енгізеді, деректер базасымен сәйкестендіріп, рұқсат сұрайды. Егер жауабы оң болған жағдайда атқарушы құрылғыны іске қосады. Шектеу шешілсе де, қол жеткізуді бақылау жүйесі әлі ақпаратты өңдеуді аяқтамады. Ол дәл осы адамның өту фактісің оқиға буферінің схемасына жазып алады. Басқару тәсілі бойынша РББЖ контроллерлері үш класқа бөлінеді: автономды, желілік және комбинированный (құрамдастырылған).

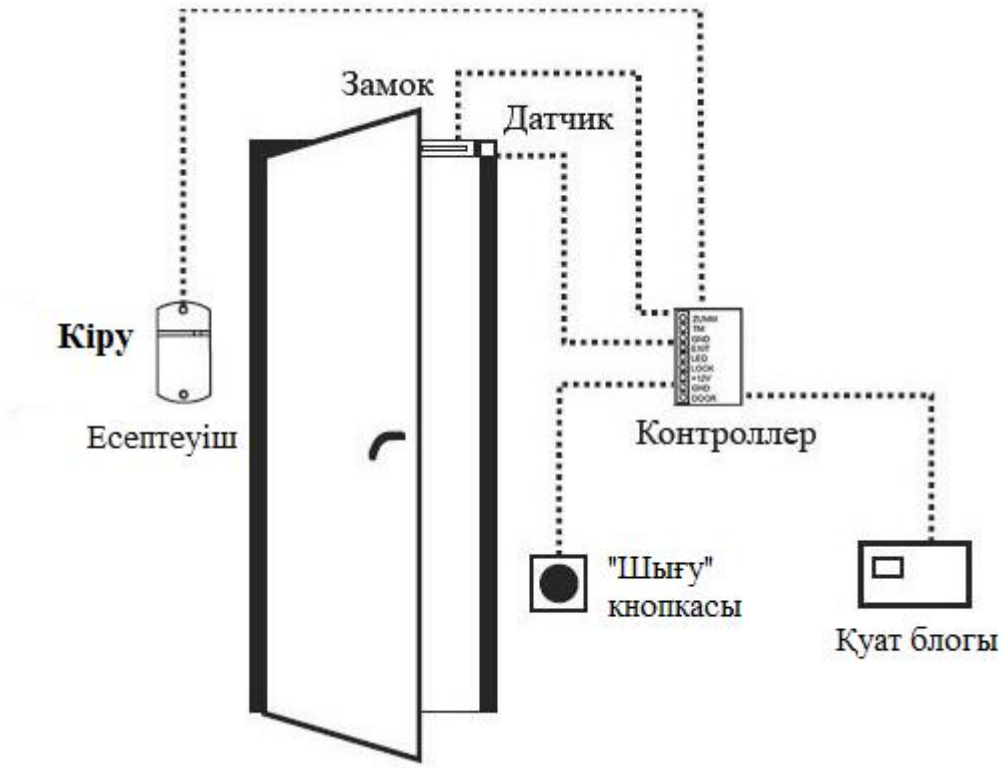
Қолданылатын оқырмандардың түріне қарамастан контроллерлер келесі кіру режимдерін қолдауы тиіс:

– бір карта және (немесе) ПИН-код бойынша;
– оператордың растауымен қол жеткізу;
– бөлмеде адамдардың санын бақылау(минимумын және максимумын).

Қазіргі заманғы РББЖ негізін автоматты және автоматтандырылған РББЖ-лар құрайды. Оларда тексеру процедурасы тексерілушіні бақылаушының мониторында видеопортретпен салыстыруды да қамтуы мүмкін. Қазіргі заманғы автоматты және автоматтандырылған РББЖ-лар басқару тәсіліне байланысты былай бөлінеді:

– автономды;
– желілік (орталықтанған);
– бөлінген (құрамдастырылған);

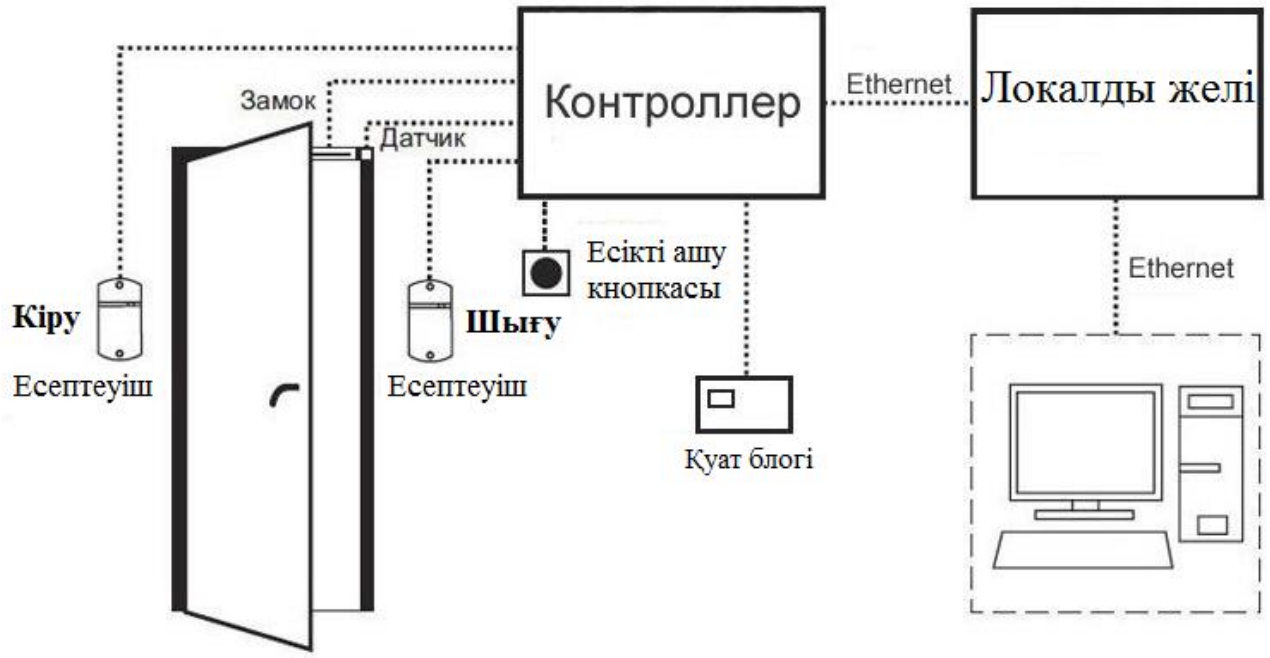
Автономды контроллерлер - бір өту нүктесіне қызмет көрсетуге арналған толық аяқталған құрылғылар. Басқа ұқсас контроллерлермен біріктіру мүмкіндігі қарастырылмаған. Мұндай құрылғылардың көптеген түрлері бар: есептеуішпен біріктірілген контроллерлер, электромагниттік құлыппен біріктірілген контроллерлер және тағы басқалары.



1.9 сурет - Автономды контроллер схемасы

Автономды контроллерлерде әртүрлі типтегі есептеуіштер қолданылады. Әдетте, автономды контроллерлер 500 адамнан аспайтын пайдаланушыларға қызмет көрсетуге арналған. Олар орталық күзет пунктіне ақпаратты жібермей және оператордың бақылауысыз бір атқарушы құрылғымен жұмыс істейді. Мұндай қолжетімділікті бақылау жүйесінің мысалы болып қарапайым "электромагниттік құлып + идентификатор карталарының есептеуіші" комбинациясы көрсете ете алады. Егер тек бір есікті бақылау қажет болса жәнеде болашақта қолжетімділікті бақылау жүйесін кеңейту жоспарланбаған болса, бұл оңтайлы және жеткілікті арзан шешімнің бірі.

Желілік контроллерлер - компьютер басқаруында желіде жұмыс істей алатын контроллерлер. Бұл жағдайда шешімді мамандандырылған және арнайы бағдарлама орнатылған компьютер қабылдайды. Желілік контроллерлерді кез келген күрделілік деңгейіндегі РББЖ-ны құру үшін қолданады. Жүйеде желілік бақылаушылар саны орталық күзет пунктімен ақпарат алмасу және бақылау, кезекші оператор тарапынан жүйені басқарумен бірге екіден, бірнеше жүзге дейін болуы мүмкін. Бұл жағдайда қолжетімділікті бақылау жүйесінің өлшемдері бақыланатын есіктердің саны бойынша емес, идентификация құрылғыларының саны бойынша бөлінеді. Себебі, бір есіктің өзіне қолданылатын өту технологиясына байланысты бірнеше құрылғы орнатылуы мүмкін.



1.10 сурет - Желілік контроллер схемасы

Желілік контроллерлерді пайдалана отырып, администратор қосымша мүмкіндіктерді алады:

– жұмыста қызметкерлердің болуы немесе болмауы туралы есеп алу;

– нақты қызметкердің орналасқан жерін анықтау;

– жұмыс уақытын есепке алу табелін жүргізу;

– кез келген уақыт аралығында қызметкерлердің орнын ауыстыру туралы есепті құру;

– қызметкерлерді өтудің уақытша кестесін қалыптастыру;

– қызметкерлердің деректер базасын (электрондық картотека) жүргізу.

– Желілік контроллерлер желімен біріктіріледі. Желілік контроллерлердің базалық сипаттамаларына:

– өту нүктелерінің саны;

– пайдаланушылардың деректер қорының көлемі;

– оқиғалар буферінің көлемі;

Өтетін нүктелердің саны. Бұл жағдайда оңтайлы шешім: бір желілік контроллер екі өту нүктесіне қойылу, себебі жалпы ресурстар (корпус, аккумулятормен қоректену көзі) аз мөлшерде талап етіледі. Көп мөлшердегі есіктерге қызмет көрсететін контроллерлер бар, бірақ олар келесі себептер бойынша аз:

– 4-5А қуат көзінің кесірінен артық құн шығуы;

– Контроллер мен есік арасындағы коммуникация құны артады. Сонымен қатар, егер есіктер бір-бірінен алыс орналасса, электркабелді төсеу қиынға соғады.

Пайдаланушылардың деректер қорының көлемі ең көп шиеленісті өту нүктесі арқылы өтетін адамдардың санымен анықталады.

Оқиғалар буферінің көлемін желі жүйесі сөндірілген (тоқтап қалған, жанып кеткен) компьютерде ақпаратты жоғалтпай қанша уақыт жұмыс істей алатынын анықтайды. Мысалы, қызметкерлер саны шамамен 20 адам болатын офис үшін 1000-ға тең оқиғалар буфері бір аптаға жетеді. Ал 3 мың адам өтетін жер үшін 10-мың оқиғаға арналған буфер бір тәуліктің өзіне қиын жетеді.

Комболанған контроллерлер желілік және автономды контроллердің функцияларын біріктіреді. Егер басқару компьютерімен (желіде) байланыс болса, контроллерлер желілік құрылғы ретінде жұмыс істейді, егер байланыс болмаса, онда автономды жұмыс істейді.

Контроллерлердің аралас функциялары. Біріншіден бұл күзет-өрт сигнализациясын қолдау, телеқадағалау кіші жүйелерімен интеграциялау және құлақтандыру мен өрт сөндірудің кейбір функцияларын басқару функциялары. Сонымен қатар, әр түрлі жұмыс станциялар, қол жеткізу мен интернет арқылы ақпарат беру құқықтары бар жергілікті компьютерлік желілерді қолдау мүмкін. Көпшілік жүйелерде бұл функциялар жоқ. Бірақ Apollo РББЖ-да осы мақсаттар үшін арнайы модульдері бар. Басқа жүйелерде өрт-күзеттік сигнализациясының функцияларын қолдау үшін үшінші өндірушілердің жабдықтарымен қосу есебінен қол жеткіздіруге болады.

1.5.2 Тұлғаны идентификациялау құрылғылары (есептеуіштер)

Жеке тұлғаны идентификациялау үшін заманауи жүйелері қолданушының қолданатын идентификаторының түріне байланысты бірнеше типті құрылғыларды пайдаланады. Рұқсат оның жеке басын идентификациялау және аутентификациялау процесінде пайдаланушымен тікелей "физикалық байланыс" кезінде жүзеге асырылады. Идентификация - объектіні (пайдаланушы адамды) ұсынылған идентификатор бойынша тану, жалпы және жеке белгілердің жиынтығы бойынша объектінің немесе жеке тұлғаның ұқсастығын анықтау рәсімі. Идентификацияға қарағанда аутентификация тексерілетін субъект өзі туралы мәліметтерді хабарлау негізінде жеке тұлғаның түпнұсқалығын анықтауды білдіреді. Мұндай мәліметтерді идентификациялық белгілер деп атайды [30].

Идентификация құрылғылары (есептеуіштер) карточкаларда немесе басқа үлгідегі кілттерде жазылған ақпаратты расшифровайтетіп, оны сандық реттілік түрінде контроллерге жібереді. Қол жеткізу карточкасының есептеуіші байланысты және байланыссыз болуы мүмкін. Белгілерді енгізу тәсілдері:

– қолмен енгізу - пернелерді басу, ауыстырып қосқыштарды бұру және тағы басқа тәсілдермен іске асады;

– байланысты енгізу - есептеуіш пен идентификатор арасындағы тікелей байланыс нәтижесінде іске асады;

– қашықтық (байланыссыз) - идентификаторды есептеуіш құралына белгілі бір қашықтыққа енгізу кезінде іске асады.

Адамның биологиялық белгілері туралы ақпаратты алу үшін арнайы биометриялық есептеуіштерді (терминалдар) пайдаланады, ал ПИН-кодты енгізу әртүрлі типтегі пернетақталармен жүзеге асырылады. Есептеуіштер барлық жүйенің сыртқы түрін және негізгі пайдалану сипаттамаларын анықтайды.

Кнопкалық пернетақталар. Жұмыс жасау принципі онай болып келеді. Егер пернетақтада терілген код дұрыс болса, онда қорғалып отқан аумаққа өту рұқсат етіледі. Кодтеруші құрылғылар кейде карта есептеуішімен бірге болатын кездер кездеседі, бұл жағдайда кодты картаның санкцияланған пайдалану фактісін растау үшін қолданады.

1.11 сурет - Кнопкалық пернетақталар

Штрих-код есептеуіші. Қазіргі уақытта штрих-код есептеуіштерді қолжетімділікті бақылау жүйесінде орнатылмайды, себебі рұқсаттаманы қолдан жасау өте онай. Қолында тек принтер немесе көшірме аппараты болса, жеткілікті.

Магниттік карта есептеуіші. Магнитофонға ұқсас магнитті бас(магнитная головка) магниттік карта есептеуіштің негізгі элементі болып табылады. Идентификация коды магниттік жолаққа картаны өткізгенде есептеледі.

1.12 сурет - Магниттік карта есептеуіші

Мұндай идентификаторлардың негізгі артықшылықтары:

– есептеуіштер және магниттік карталардың құны өте төмен;

– кодтаушы арқылы магниттік карта кодын өзгертуге болады.

Негізгі кемшіліктер:

– рұқсатсыз қолжеткізуден қорғалу жеткілікті емес, себебі қаскүнем бөтен картамен ие болып, өте шектеулі уақыттың өзінде қажет дубликаттарды жасай алады;

– магниттік карта есептеуіштері эксплуатацияға ыңғайсыз. Уақыт өте келе магниттік бастары бітеліп, ығысады;

– қолжетімділікті бақылау жүйесінің төмен өткізу қабілеті, осының себебінен көбінесе магниттік картаны бірнеше рет идентификациялауға тура келеді;

– магниттік жолағы бар карталар өте ұқыпты сақтауды талап етеді және электромагниттік өрістердің әсерінен аулақ болу қажет.

Байланыссыз карта есептеуіші (Виганда интерфейсі). Есептеуіш пластикалық немесе металл корпуста орналасқан екі магнитті индукциялық катушка болып келеді жәнеде толық герметика үшін арнайы оқшаулағыш материалымен құйылады. Пластикалық картаны есептеуіштен жүргізген кезде қолжетімділікті бақылау жүйесі картаның бинарлық кодын алады. Есептеу байланыссыз индукция әдісімен жүргізіледі.

Негізгі артықшылықтары:

– құрылғының қарапайымдылығының арқасында жоғары сенімділік;

– пластикалық картаның құрылымы туралы ақпарат жоқ болған соң оны жалған жолмен жасау мүмкін емес;

– пластикалық картаның сыртқы әсерлерге деген жоғары тұрақтылығы;

Проксимит-карталар есептеуіші. Мұндай карталар тұлғаны қашықтан идентификациялауға мүмкіндік береді. Есептеуіштің ішінде тарату-қабылдау антеннасы және сигналдарды өңдейтін электрондық плата орналасқан.

"Тач-мемори" кілтің есептеуіші. "Тач-мемори" есептеуіші жұмыс жасау бойынша өте қарапайым және арнайы кілттердің жанасуына арналған нақты байланыс алаңын білдіреді. "Тач-мемори" кілті тот баспайтын болаттан жасалған цилиндрлік корпуста орналасқан арнайы микросхеманы білдіреді.

1.13 сурет - Тач-мемори" кілтің есептеуіші

Биометриялық есептеуіштер. Идентификаторлардың қолдан жалған жасалу немесе ұрланған жағдайды болдырмау мәселелері: адамның жеке белгілері мен нақты биометриялық идентификаторларды пайдалану жолымен шешіледі. Олар: саусақтардың іздері, алақанның геометриясы, көз торының қабығы, қан тамырларының суреті, беттің жылы бейнесі, қол қою динамикасы, сөйлеудің спектраль сипаттамалары [29].

1.14 сурет – Есептеуіштердің РББЖ жүйесіндегі орны

Осы жаңа технологияларды пайдалана отырып, мына проблемаларды шешуге болады:

– құжаттарды, карталарды, парольдерді ұрлау немесе қолдан жалған жасау есебінен, қаскүнемдерді күзетілетін аумақтарға немесе бөлмелерге кіруінің алдын алу;

– ақпаратқа қолжеткізуді шектеу және оның сақталуына жеке жауапкершілікті қамтамасыз ету;

– жауапты объектілерге тек сертификатталған мамандарды өткізуді қамтамасыз ету;

– қолжетімділікті бақылау жүйелерін пайдалануға байланысты шығындарды болдырмау;

– кілттердің, карталардың, парольдердің жоғалуына, бүлінуіне немесе ұмытылуына байланысты қолайсыздықтарды болдырмау;

– қызметкерлер және студенттердің кіруін және сабаққа қатысуын есепке алуды ұйымдастыру.

Қазіргі уақытта саусақ іздері, бет белгілері, көздің қабығы, дауыс және басқа да сипаттамалары бойынша тұлғаны идентификациялау үшін, қауіпсіздік жүйелерінде бірқатар технологиялар белгілі.

1.15 сурет – Биометриялық және карталық есептеуіш

Барлық биометриялық технологиялардың идентификациялау жұмысының тәсілдері бір-бірімен бірдей деп айтуға болады. Бірақ, олардың барлығы, қолдану ыңғайлығымен және нәтижелердің дәлдігімен ерекшеленеді. Кез келген биометриялық технология кезең-кезеңмен қолданылады:

– объектіні сканерлеу;
– жеке ақпаратты алу;
– үлгіні қалыптастыру;
– алынған үлгіні деректер базасымен салыстыру.

Қолжетімділікті бақылауындағы биометриялық жүйесінің өткізу қабілетінің мәселесі өте маңызды болып тұр. Есептеуішпен талданатын деректер көлемі өте үлкен болғандықтан, ол өте ұзақ уақыт бойы жұмыс істейді. Талдау уақытын азайту үшін, биометриялық есептеуіштер, пайдаланушының жеке қолжеткізу кодына қосымша кірістірілген пернетақтаға ие болады. Осыдан кейін ғана, биометриялық идентификациялау процесіне кіріседі. Биометриялық қолжетімділікті бақылау жүйесінің тағы бір артықшылығы, ол затпен емес ("тач-мемори" кілті, проксимит-карта), адамның өзімен идентификация жүргізеді. Осының арқасында, қолданылатын сипаттама, онымен тығыз байланысты, себебі "биометриялық паспортты" жоғалту, беру немесе ұмыту мүмкін емес [29].

1.5.3 Атқарушы құрылғылар

Қолжетімділікті бақылаудың атқарушы құрылғыларының арасында келесі бөгет құрылғылары таралған: құлыптар, ілмектер, турникеттер (белдік, толықбиіктік, "билеттік", жылжымалы, үш немесе төртштангты айналатын) және шлюздік кабиналар (тамбурлық типті, ротанттар, шлагбаумдар), Автоматты қақпалар (қозғалатын қақпалар, жиналатын қақпалар, рулеттік қақпалар),

лифтілер. Қазіргі заманғы РББЖ-да негізінен электромагниттік және электромеханикалық құлыптар қолданылады [30].

Есік құлыптары мен ілмектер. Электрмеханикалық құлыптар мен ілмектерде қолданылатын жұмыс принципі өте қарапайым: олардың арнайы түйіспелі клеммасына кернеу берген кезде (әдетте 9-16 В диапазонында) электромагниттік реле механикалық құрылғының тоқтатқышын тартып, есікті ашуға мүмкіндік береді.

1.16 сурет – РББЖ жүйесінің құлыбы

Шлюз кабиналары. Шлюздік кабиналарды құрылғысы, өткізу қабілеті мен бағасына байланысты екі негізгі түрге бөлуге болады: тамбурлық және ротант-шлюздер.

1.17 сурет - Шлюз кабиналары

Тамбур типті шлюз кабинасы екі тәуелді есіктің жабық жүйесі болып табылады. Кез келген шлюз кабинасының негізгі қасиеті кез келген уақытта екі есіктің біреуі ғана ашық болуы.

Өткізу қабілетін арттыру үшін ротант-шлюздерді қолданады. Олардың әрекет ету принципі тамбур типтегі шлюздерге ұқсас, бірақ екі есіктің орнына турникет сияқты бір бұрылмалы есік болады. Шлюз-ротанттың өткізу қабілеті минутына 18-ден 22 адамға дейін жетеді.

Қаскүнемдерден неғұрлым сенімді қорғалу үшін кабинаның ішіндегі адамдардың санын қосымша бақылау үшін өлшеу жүйелерімен және металл детекторлармен жинақталады. Кабинаның қабырғалары болаттан немесе бронестеклодан жасалады.

Турникеттер. Бақылау жүйелерінің турникеттерін екі түрге бөлуге болады: белдік және толықбиікті. Турникеттің жұмыс істеу принципі: егер қолжеткізуге сұраныс заңды болса, механикалық жүйе бұрылып, күзетілетін аумаққа өту рұқсат береді.

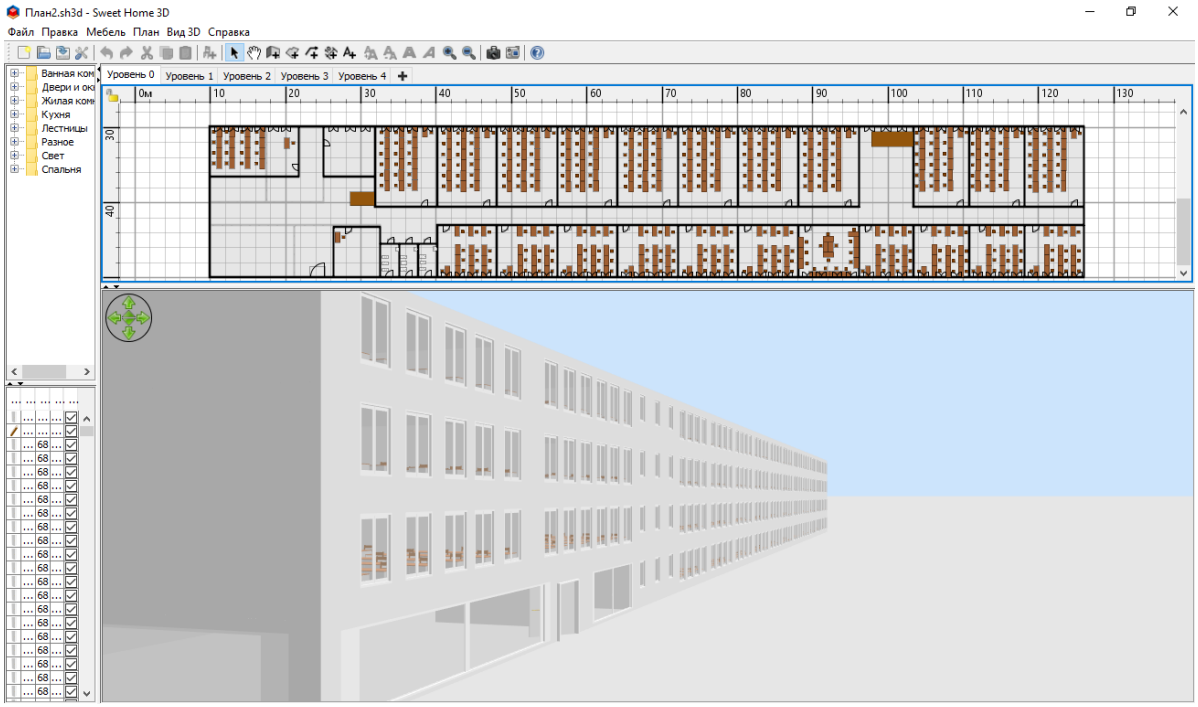
1.18 сурет - Турникет

Автоматты шлагбаумдар және қақпаға арналған автоматика. Көлік құралына атрибутты идентификатор ретінде машинаның мемлекеттік нөмірі, жүргізушінің және жүкті тасымалдауға жауапты адамның тегі көрсетіледі. Жүргізуші мен жолаушылардың идентификаторлары олардын пропусктары болып табылады.

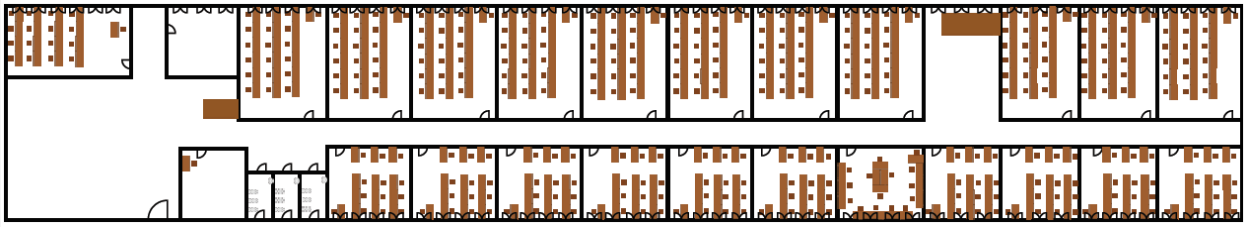
1.6 Қорғалатын объект пен жабдықтардың сипаттамалары

Объектке жоғары оқу орнының бір ғимаратын аламыз. Объектінің аумағына кіру, рұқсатты бақылау жүйесімен жабдықталған, автоматты қақпалары орнатылған 4 бақылау-өткізу пункттері арқылы жүзеге асырылады. Ғимаратқа кіру рұқсатты бақылау жүйесімен жабдықталған 2 турникет арқылы жүзеге асырылады. Ғимаратта 100-ге тең оқу бөлмелер мен аудиториялар қорғалады.

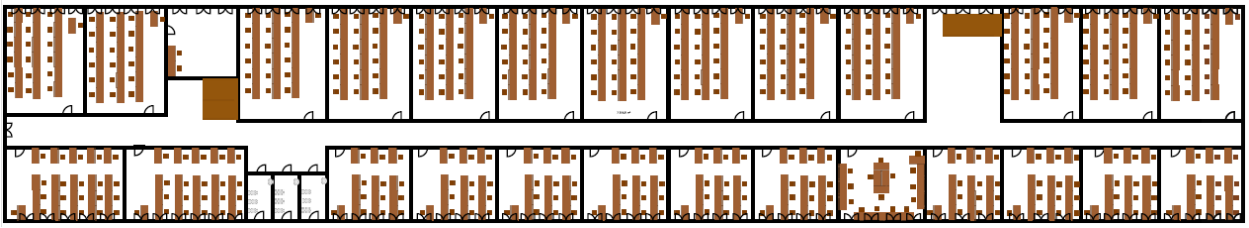
Sweet Home 3D бағдарламасының көмегімен ғимараттың жобасы сызылды.



1.19 сурет – Университет ғимаратының жобасы



1.20 сурет – Университет ғимаратының бірінші қабаттың жобасы



1.21 сурет – Университет ғимаратының екінші, үшінші және төртінші қабатттардың жобасы

1.6.1 Негізгі техникалық міндеттер

Мына техникалық шешімдер, объектіде орнатылатын аппаратуралық талаптарды ескере отырып, қабылданған жәнеде объекті қорғаудың кешенді тәсіліне негізделген.

Объекті нормативтік құжаттаманың барлық талаптарын орындайтын қорғауды қамтамасыз ету үшін жобада Castle РББЖ жабдықтарын қолдану көзделген:

– Castle EP - Желілік контроллер. Турникетті, екі есікті, қақпаны немесе шлагбаумды басқару үшін.

– Castle EP4 - Желілік контроллер. Төрт есікті басқару үшін.

– Matrix-2-EH - EM-Marine және HID форматты карталарын бақылау есептеуіші.

– ОМА-26.461_/1 - Турникет-трипод

– ИО 102-5 - Есікке магнитті-контактілі датчик

– TRD-1086C - соленоидты электромеханикалық құлып.

– TS-MAGIC – Шығу кнопкасы

– ББП-20 - Үздіксіз қоректендіру блогы

– АКБ 7А/сағ - Аккумулятор 7А/сағ

– «Castle» - Castle бағдарламасы

1.6.2 Castle РББЖ-ның сипаттамасы мен артықшылығы

"Castle" РББЖ жүйесі бөлмелер, ғимараттар немесе ғимараттар топтарында шектелмеген қызметкерлер мен студенттерді бақылап, шексіз есіктер пен турникеттер арқылы кіруді бақылауға керемет мүмкіндік береді. Бұл жүйе контроллерлердің кең ассортимент пен қосымша бағдарламалық қамтамасыз етуден тұратын аппараттық-бағдарламалық комплекс болып табылады. РББЖ жүйесі кең интеграциялық мүмкіндіктерге ие, бұл деген оның көптеген жүйелермен онай интеграциялауды жүзеге асыруға мүмкіндік береді. Бүгінгі күні "Castle" жүйесі жекелеген және аумақтық алыстатылған объектілері үшін классикалық және биометриялық РББЖ-ны құруды қамтамасыз етеді жәнеде деректер базасын синхронизациялау технологиясы бар бірегей шешім.

"Castle" жүйесі адам факторының әсерін өткізу режиміне толығымен жоққа шығарады, өйткені бақылау толық жабдыққа жүктеледі. Оған қоса "Castle" кіруді белгілі бір қызметкерге немесе студенттерге шектеуге, яғни арнайы бөлмелерге ғана өтуге рұқсат беруді мүмкіндік береді.

Жүйе кабинеттерды күзеттен алып тастауға және оларды күзетке қоюға мүмкіндік береді. Штаттан тыс жағдай туындаған жағдайда дабыл сигналы беріледі. Барлық оқиғалар, дабылдар, күзеттен қою/шығару жағдайлары оқиғалар журналында тіркеледі, жәнеде оған қоса жүйе мен контроллерлердің жадында ұзақ уақытқа сақталады.

Жүйе қызметкерлер мен студенттердің кабинетке өту күні мен уақытын белгілеуге, пайдаланған карта иесінің түпнұсқа фотосуретімен визуалды салыстыруға, күзетілетін объект бойынша қызметкерлер мен студенттердің орын

ауыстыруын бақылауды жүзеге асыруға, жүйенің көмегімен карточканы басқа тұлғаға беруден қорғауды қамтамасыз етуге мүмкіндік береді.

РББЖ мереке және демалыс күндері студенттерге өтуге тыйым салуға, сондай-ақ күн аяқталғаннан кейін әрбір оқытушы немесе студент үшін деректер базасын ұйымдастыруға, нақты уақытта әртүрлі штаттан тыс және мазасыз жағдайлар туралы ақпарат алуға мүмкіндік береді.

"Castle" РББЖ жүесінің бейнебақылау жүйелері мен ОПС-пен интеграцияланып, объектідегі жағдайды автоматты режимде толық бақылауды жүзеге асыруға мүмкіндік береді.

1.6.3 Жабдықтартың ерекшеліктері

Кез келген қол жетімділікті бақылау жүйесі бағдарлама мен оған қосылған әр түрлі атқарушы құрылғылардың (есептеуіштер, құлыптар, турникеттер және т.б.) жұмысына жауап беретін контроллерлерден тұрады. Жалпы, барлық контроллерлер базалық функционалдылық бойынша бір-біріне ұқсас болып келеді. Олар қолданушылар мен оқиғалардың деректер базасының орындалуы, көлемі мен мөлшерімен ерекшеленеді. Осының арқасында объектінің ерекшеліктеріне сәйкес РББЖ-ның аппараттық бөлігін оптимизациялауға мүмкіндік береді. Барлық мәліметтер мен параметрлерді автоматты түрде сақтай отырып, жүйенің жұмысын тоқтатпай тез және ыңғайлы жаңартуға болады. Контроллерлер:

1.22 сурет - Castle RD2.2 / RD4

Телекоммуникациялық шкафқа арналған 1U кәсіби IP-контроллері. IT мамандарға контроллермен жұмыс істеуі түсінікті болу үшін арналған. Айрықша ерекшеліктері - жобалау жеңілдігі және СКС технологиясының арқасында өте жылдам орнату. Құрылғыларда өзінің қуат көзімен АКБ-сі бар жәнеде кейбір модельдерде Linux сервері бар.

1.23 сурет - Castle EP2 / EP / EP4 / ES

Жабдықталған кіру нүктелері аймағына орнатуға арналған IP-контроллері. Олар индикаторлармен жабдықталған, металл корпустағы микропроцессорлық плата болып табылады. РББЖ контроллері ең көп таралған «есіктің үстіне» деген тәсілі бойынша орнатылады. Бөлек қуат көзін қосу қажет.

1.24 сурет - Castle PRO / RS

485-интерфейсті контроллерлер. Контроллерге қажетті ұзындығы 100 метр немесе одан көп болатын кабельдік объектілерге арналған. Мұндай типтегі контроллерлер IP-инфрақұрылымын құру тиімсіз жерлерде, яғни қақпалар мен шлагбаумдарды басқару тапсырмаларын орындау үшін қолданылады.

Castle РББЖ контроллерлерінің барлық модельдері бағдарламаның әрекетісіз автономдық режимінде жұмыс істейді. Контроллер қабылданған сигналды өңдеп, энергияға тәуелді жадында сақталатын идентификаторлар (карталар, кілттер) мен қолжеткізу режимдерінің дерекқорына сүйене отырып, команданы атқарушы құрылғыға жібереді. Мұндай алгоритм Castle жүйесінің басқаларымен салыстырғанда тезірек жұмыс істейтінің көрсетеді.

Сонымен қатар, электр қуатының үзілгенде немесе сервермен байланыс жоғалған жағдайдың өзінде деректердің жоғалып кетпеуін қамтамасыз етеді. Байланыс қалпына келтірілген кезде жинақталған деректер автоматты түрде АБЖ серверіне жіберіледі.

Контроллерлердің барлық үлгілерінде төртдеңгейлі грозозащита қорғанысы бар. Барлық кіріс және шығыс интерфейстері өз өзін қалпына келтірумен сақталған.

1.6.4 «Castle» бағдарламасының ерекшелігі

"Castle" РББЖ жүйесі компьютерге орнатылатын жүйені баптау үшін қызмет етуге арналған бағдарламамен бірге беріледі. Ол күзетілетін кабинеттердың және кіру нүктелердін (есіктер, қақпалар және тағы басқалары) графикалық жоспарларын шығаруға мүмкіндік береді. Компьютер мониторында күзет қызметкерлері адамдардың орналасқан жерін және кез келген есіктің жағдайын (ашық немесе жабық) қадағалайды. Адам есік арқылы өткенде, күзет экранында оның фотосуреті пайда болады. Күзетші есіктерді қашықтықтан ашуға мүмкіндігі бар. Оған қоса компьютердің жесткий дискіна жазылатын оқиғалар протоколы жүргізіледі. Бағдарлама келу және кету уақытын белгілеуге, сондай-ақ қызметкерлердің жұмыс уақытын есептеуге мүмкіндік береді. Қосымша ол автодиагностика және қажетті мерзімділікпен деректер базасын автоматты резервтеу функцияларына ие жәнеде жүйе компоненттерінің арасындағы байланыстың жоғалғаны туралы SMS-хабарлама жіберу мүмкіндігі қарастырылған.

"Castle" бағдарламаның функционалдық мүмкіндіктері:

– Контроллерлер арасындағы байланыс жағдайын және жүйе серверінің компоненттерінің жағдайын бақылау.

– Жүйе операторлары үшін қолжеткізу құқықтарының настройкасы.

– "Castle" контроллерлерді қашықтан басқару (блоктау, блоктан шығару, автономды жадты басқару).

– Кәсіпорын қызметкерлерінің тізімін беру. Кіру нүктелері, бағыт және уақыт (режимдер) бойынша рұқсат шектеулерін беру.

– Кез келген уақытта жасалған өту әрекеттері жайлы есептерді алу, персонал тізімін мен олардың режимін MS Excel-ге экспорттау немесе MS Excel-ден персонал тізімін импорттау.

– Үшінші тұлғаларға (AntiPassBack) рұқсат беруді болдырмау.

Әрбір объект үшін уақыт аралықтарын сипаттайтын еркін кіру режимдерін жасау. Жәнеде кіруге немесе шығуға рұқсат етілген немесе мүлдем тыйым салынған кіру нүктелерінің тізімін жасау.

– Рұқсаттың күрделі режимдерін құру мүмкіндігі (тәулігіне үш рет, көп ауысымды графиктер және тағы сондай сияқты).

– Ерекше жағдайлар үшін рұқсатты реттеу(мереке күндері, жоспардан тыс жұмыстар және тағы басқалары).

1.6.5 Castle EP4 контроллерлерінің толық сипаттамасы

Castle EP4 контроллері Castle желілік жүйесінің құрамында және оған қосылған атқарушы құрылғылармен жұмыс істеуге арналған. Атқарушы құрылғыларға: электромагниттік және(немесе) электромеханикалық құлыптармен немесе ілмектермен жабдықталған есіктер. Есіктерді контроллерден 50м-ге дейінгі қашықтықта орналастыруға болады.

Castle EP4 контроллері сервермен байланысы болмаса да, кілттер базасы мен рұқсат режимдерінің негізінде қолжеткізуге рұқсат беру немесе тыйым салу туралы шешімді өзі қабылдайды. Оқиғаның күні мен уақыты контроллердің өзінде бекітілген сағат бойынша тіркеледі. Оқиға серверімен байланыста болса, РББЖ серверіне оқиғалар автоматты түрде жіберіледі. Контроллерлердің серверден тәуелсіздігі мен болып жатқан оқиғаларға реакцияның жылдамдығының арқасында жоғары сенімділікті қамтамасыз етеді.

Идентификация құрылғысы ретінде контроллерге шығыс интерфейсін қолдайтын Wiegand немесе Touch Memory деген төрт есептеуіштерге дейін қосылуы мүмкін. IP-желісіне қосылу үшін белсенді желілік жабдық қажет.

Сипаттама:

Байланыс интерфейсі: Ethernet

Басқаратын құрылғылар саны: Төрт есік (бір жақты)

Энергияға тәуелді жады: 7000 кілт, 500 уақытша аймақ, 40000 оқиға

Есептеуіш интерфейсі: әртүрлі биттік Wiegand (w26, w34, w37, w40, w42) Dallas Touch Memory

Температурасы: 0°C бастап + 45°C дейін

1.6.6 «Castle» ПО-ның негізгі сипаттамалары

Castle ПО серверін орнату Windows операциялық жүйесінің (32 және 64 биттік) басқаруындағы компьютерлерге жүргізіледі: Windows 7 SP1, Windows Server 2008 R2 SP1 және одан да жаңа версиялар, сондай-ақ Linux Debian-ға (32 және 64 биттік) да орнатуға болады. Castle ПО-ның клиенттік бөлікті орнату Windows операциялық жүйесінің (32 және 64 биттік) басқаруындағы компьютерлерге жүргізіледі: Widows XP SP3, 2003 Server SP2 және одан да жаңа

версиялар, сондай-ақ Linux Debian (32 және 64 биттік). Әр түрлі ОС комбинацияларымен жұмыс мүмкідігі бар. Мысалы, сервер Linux-та, клиенттердің бір бөлігі Linux-та, ал басқа бөлігі Windows-та. Қолданылатын операциялық жүйенің түріне қарамастан, оған шығарылған соңғы жаңартуларды(обновление) орнату қажет.

Сервер конфигурациясы:

– Процессор: Intel Core i3 немесе одан жоғары.

– Жады: кем дегенде 2 ГБ.

– Жесткий дискідегі бос орын: жүйені орнату үшін 300 МБ және дерек базасы үшін қосымша орын. Деректер базасының мөлшері жұмысшылар санына, фотосуреттердің көлеміне және жүйенің уақытына байланысты болады. Уақыт өте келе жүйелік оқиғалар, жаңа қолжеткізу режимдері және тағы басқалыры туралы ақпарат жинақталады. Жесткий дискідегі деректердің болжамды мөлшері 1 000 000 оқиғаларға 120 МБ құрайды.

– Кемінде бір бос USB порты болу керек.

– Байланыс интерфейсі бар үздіксіз қуат көзі (USB немесе RS232).

– Монитор: кемінде 1280*1024.

– Үлкен деректер базасымен жұмыс істеу кезінде (ондаған миллион немесе одан да көп) - жоғары жылдамдықты жесткий диск (SSD немесе RAID массиві).

Castle-дің бетті тану мүмкіндігін пайдалану кезіндегі қосымша талаптар:

– Процессор: Intel Core i7 немесе одан жоғары.

– Жады: кем дегенде 8 ГБ

Бетті тану функциясы жұмыс істеу үшін серверден айтарлықтай күшті қуатты қажет етеді. Мысалы: Intel Core i5-7260U@2.2GHz процессордың бір ядросында бір кадрды өңдеу шамамен 150 мс алады (яғни, төрт ядролы процессорда секундына 26 кадр).

Клиенттік орынға конфигурация:

– Процессор: кемінде 1 ГГц.

– Жады: кем дегенде 2 ГБ.

– Жесткий дискідегі бос орын: жүйені орнату үшін кемінде 300 МБ бос орын болу қажет.

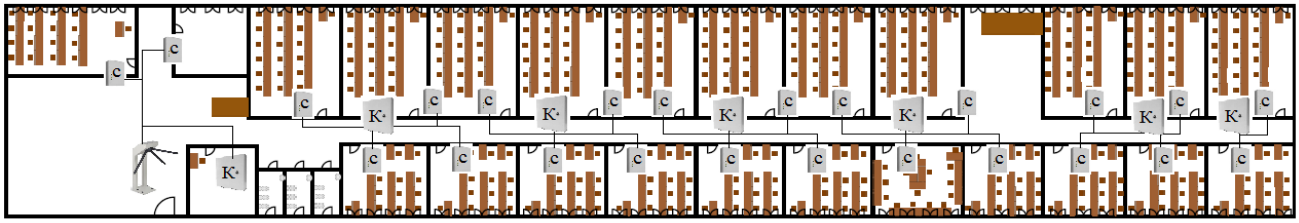
– Монитор: кемінде 1280*1024.

Клиент және сервер бағдарламасын бір компьютерге орнатуға болады. Бырақ, сервер үшін ұсынылған конфигурацияға жүгіну керек.

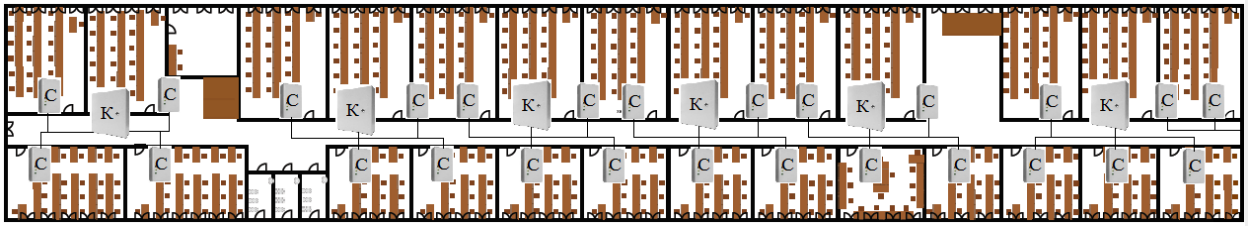
2. Университет үшін РББЖ жүйесін әзірлеу

2.1 РББЖ жабдықтарын қосу

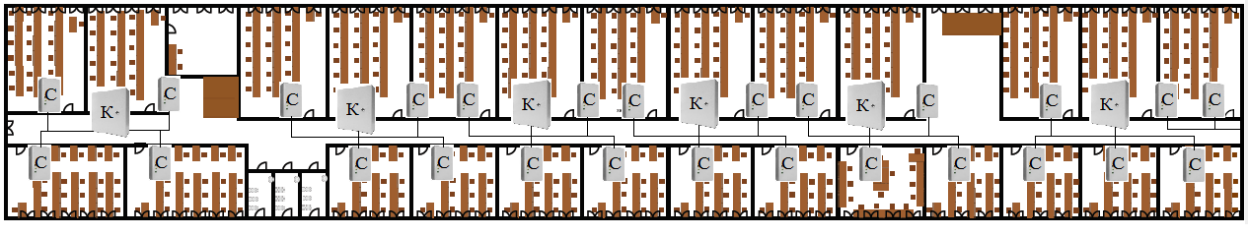
Нормативтік құжаттаманың барлық талаптарын орындайтын қорғауды қамтамасыз етілген Castle РББЖ жабдықтарын сызылған жобаға енгіздіреміз.



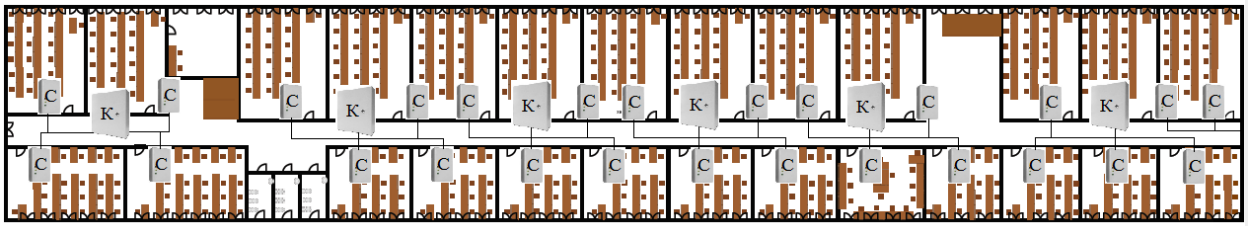
2.1 сурет – Университет ғимаратының бірінші қабатына орнатылған жабдықтардың жобасы



2.2 сурет – Университет ғимаратының екінші қабатына орнатылған жабдықтардың жобасы

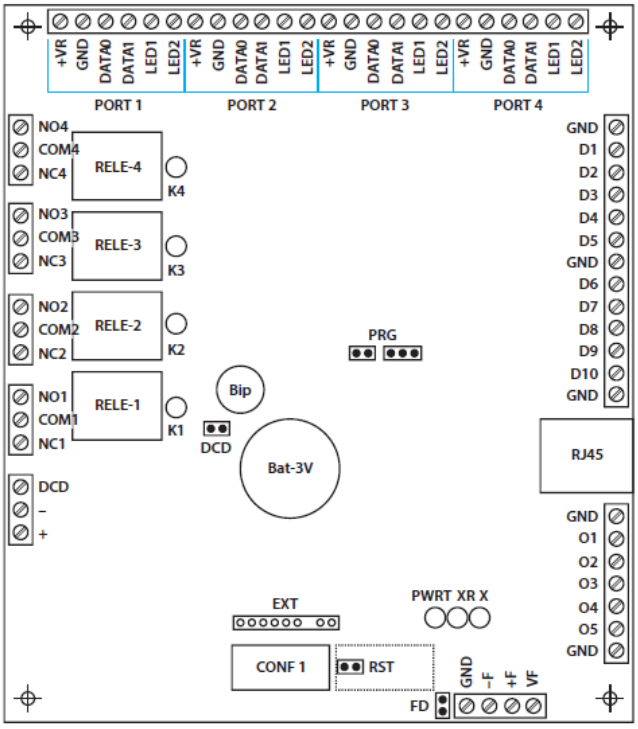


2.3 сурет – Университет ғимаратының үшінші қабатына орнатылған жабдықтардың жобасы



2.4 сурет – Университет ғимаратының төртінші қабатына орнатылған жабдықтардың жобасы

2.1.1 Контроллер элементтерінің белгіленуі



2.5 сурет - EP4 контроллерінің платасында негізгі элементтердің орналасу схемасы

Кесте 1 – 2.5 сурет элементтерінің белгіленуі [31].

Элементі	Сипаты
CONF 1	Контроллердің конфигурациясын таңдау дип-блогі.
RST	Контроллердің IP-настройкаларын қалпына келтіру перемычкасы.
K1	1-ші реле қосу индикаторы.
K2	2-ші реле қосу индикаторы.
K3	3-ші реле қосу индикаторы.
K4	4-ші реле қосу индикаторы.
PWR	Контроллер қуат күйінің индикаторы (жасыл).
RX	Деректерді қабылдау индикаторы (сары).
TX	Деректерді жіберу индикаторы (қызыл).
DCD	Қоректендіруші кернеу түрін анықтауды сөндіру перемычкасы.
FD	Өрт сигнализациясының кірісін

	сөндіру перемычкасы.
RJ45	Ethernet разъёмы

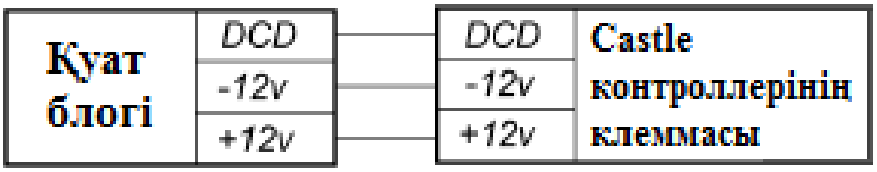
2.1.2 Контроллердің қуаты

Контроллер 9,9-17,8В тұрақты кернеумен қуат алады. Контроллер тұтынатын ток 160 мА-дан аспайды [31].

БП-дан қуат беру кезінде контроллерді кез келген ыңғайлы жерге орнатады. Тұрақты токтың кернеуін 12В жәнеде ток кемінде 200 мА-ді қамтамасыз ететін БП-ға орнату керек.

БП тек контроллерді қуаттандыруға ғана емес, сонымен қатар есептеуіштер, құлыптар және басқа сыртқы құрылғыларды шамамен 20% ток күші бар қуатпен қамтамасыз ету керек.

Төтенше жағдайлар туындаған кезде контроллердің қорғаныс тізбектері шамадан тыс жүктелген немесе замкнутый желінің қуатын өшіреді.



2.6 сурет - Қуатты контроллерге қосу.

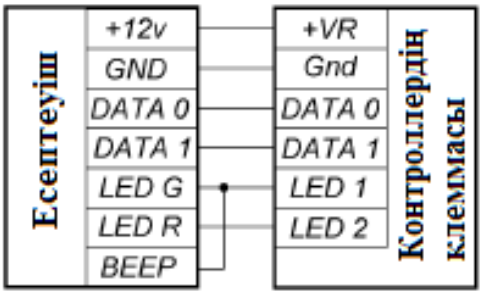
Қосылу үшін кем дегенде 0,75 мм² аспайтын кез келген кабельді пайдаланады.

DCD желісін, контроллер, қуат көзі кернеуінің күйін диагностикалау үшін қолданатын қосымша кіріс болып келеді. DCD кірісін басқаруы минус қуат көзіне тұйықтау арқылы немесе төмен логикалық деңгейдегі кернеуді беру арқылы жүзеге асырылады (0 ... 0,5 В). Бұл кірісті логикалық деңгеймен басқарған кезде, оның ең жоғарғы кернеуі 3,3В аспауы керек.

2.1.3 Есептеуіштер мен байланыстырушыларды байланыстыру

Wiegand-26 шығу интерфейсін стандартты қолдайтын төрт есептеуішті контроллерге қосуға болады. Есептеуіш интерфейсінің түрлері контроллерге кернеу берген кезде автоматты түрде анықталады [31].

Әр есептеуіш PORT 1, PORT 2, PORT 3 және PORT 4 деген платада көрсетілген бірдей клемм блогына қосылады.



2.7 сурет – Есептеуішті контроллерге қосудың мысалы.

+ VR - плюс қуаты, GND – жалпы сым, DATA0, DATA1 - Wiegand-26 интерфейсінің мәліметтерін тарату желілері, LED1, LED2 – есептеуіштін индикациясын басқару желісі. LED G – есептеуіштін жасыл жарықдиоды, R - есептеуіштін қызыл жарықдиоды.

2.1.4 Байланыс желісін қосу және контроллердін настройкасы

Контроллер Ethernet-желісіне стандартты жолмен қосылады, оның бір разъемы контроллердын RJ45 разъемына, ал екіншісі – Ethernet-жабдығының белсенді разъемына (хаб, свич және тағы басқалары) қосылады [31].

Контроллердің қалыпты жұмысы үшін оны конфигурациялау қажет.:

– IP мекенжайын;

– Желілік маскасын;

– «шлюз по умочанию»-сын.

– Параметрлерге қол жеткізудің құпия сөзі - «castle». Парольді конфигурация кезінде өзгертуге болады.

– Контроллерді конфигурациялау үшін:

– оны жергілікті желідегі еркін портқа қосу;

– Қуат қосу;

– Castle жүйесінің серверлік бағдарламасын компьютерлердің біріне орнату;

– «Программы управления сервером» көмегімен қажетті параметрлерді орнату.

Брандмауэрларды IP-желісінде қолданған кезде, оған 3303 және 3305 порттарындағы сервер мен жүйелік контроллер арасында UDP мәліметтерінің еркін алмасуына мүмкіндік енгізу қажет.

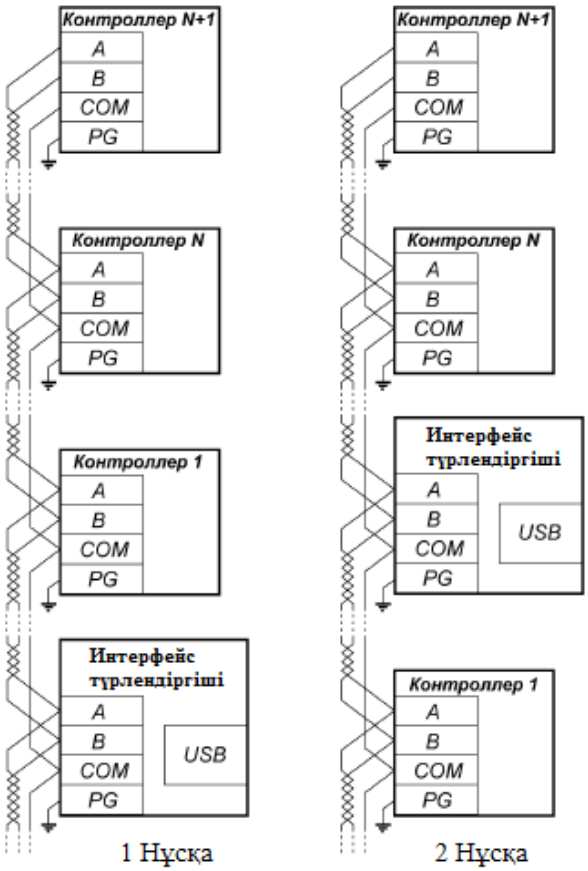
2.1.5 RS-485 байланыс желісін қосу

RS-485 байланыс желісі "шина" типті топологиямен өнеркәсіптік желі болып табылады, яғни осы сызықпен біріктірілетін барлық құрылғыларды қосу бірінен кейін бірі ретімен жүргізіледі [31].

RS-485 интерфейсінің электрлік сипаттамалары монтаждау ережелерін сақтау кезінде 1200 м дейін байланыс желісін құруға мүмкіндік береді. Байланыс желісі UTP 5 кабельмен салынады.

Соңғы контроллерде "RT", "PA" және "PB" перемычкалары орнатылуы тиіс.

Байланыс желісі "A", "B" және "COM" клеммаларына қосылады. «Заземление» "PG" клеммасына қосылады.



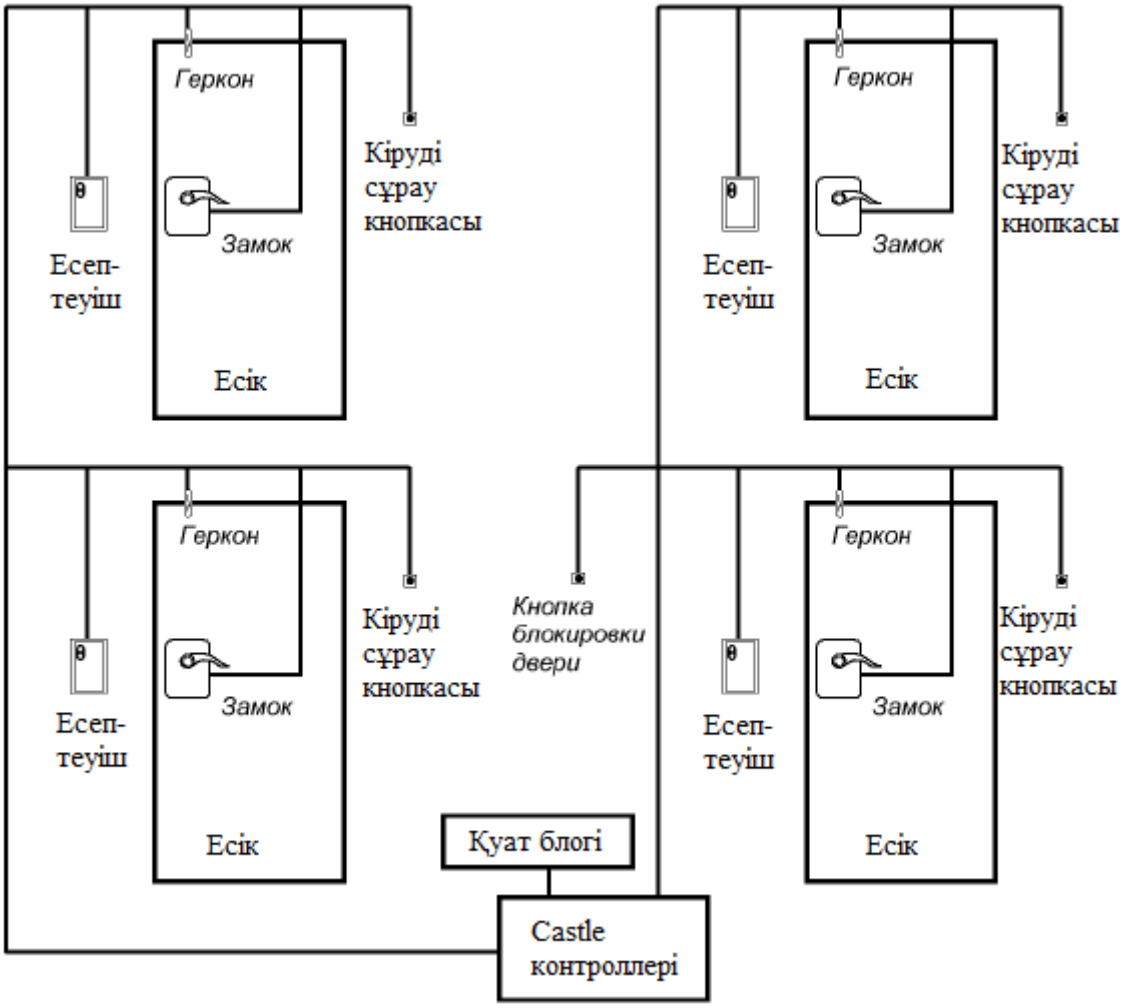
2.8 сурет - Байланыс желісін қосу мысалы.

2.1.6 Есіктерді қосу

Контроллер электромагниттік немесе электромеханикалық құлыптармен немесе ілмектермен жабдықталған, бірден төртке дейінгі есіккермен бір мезгілде басқара алады [31].

Әрбір есік үшін:

– Құлып;
– Геркон;
– Есептеуіш;
– Өту сұрауының кнопкасы орнатылады.



2.9 сурет - Жабдықты қосу үлгісі.

2.1.7 Есікке құлыптарды қосу

Құлыптар контроллер платасында орналасқан төрт реле арқылы басқарылады (RELE-1 - RELE-4). Әр реледе ауысып қосылуға жұмыс істейтін контактілер тобы бар. Олар COM - жалпы контакт, NC - қалыпты түрде жабық, NO - қалыпты түрде ашық [31].

Әр түрлі модельдерді қолдау үшін екі құлыптау режимі қолданылады: потенциалды және импульсті.

Потенциалды режимде, құлыптау релесі қалыпты (құлыпталған) күйде қосулы болады, ал ашқан соң, біраз уақытқа өшірулі болады. Бұл режим электромагниттік құлыптарды басқаруға мүмкіндік береді.

Импульстік режимде, құлыптау релесі қалыпты (құлыпталған) күйде жұмыс істемейді. Ал құлыптан босатылған кезде ол аздап іске қосылады. Бұл режим электромеханикалық құлыптарды басқаруға мүмкіндік береді.

Электрмагниттік құлыптарды қосу. Контроллер электромагниттік құлыптардың кез келген түрін басқаруға мүмкіндік береді. Электромагниттік құлыптар, әдетте оларға кернеу берген кезде құлыпталады немесе ашылады.

Электромагниттік құлыптарды басқару үшін контроллер құлыптарды ықтимал басқару режиміне қосылуы керек («CONF 1» блогының №2 ауыстырғышын OFF күйіне).

2.10 сурет - Кернеумен бекітілетін электромагниттік құлыпты жалғаудың схемасы

Мұндағы, VD1 - Контроллермен бірге берілетін 1N4007 қорғаныс диоды.

Vp - құлыптау қуатының кернеуі

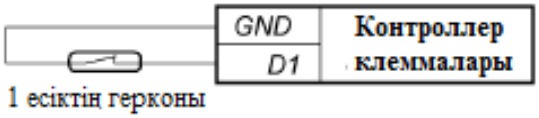
Электромеханикалық құлыптарды қосу. Контроллер электромеханикалық құлыптардың кез келген түрін басқаруға мүмкіндік береді.

Электромеханикалық құлыптармен жұмыс істеу үшін контроллерді құлыптарды импульсті басқару режиміне ауыстыру керек («CONF 1» блогының №2 ауыстырғышын ON күйіне).

2.11 сурет - Электромеханикалық құлыпты жалғаудың схемасы

2.1.8 Есік ашылу датчиктерін қосу

Есік ашылу сенсоры өту немесе есікке бұру фактісін тіркеу үшін қолданылады. Сенсор ретінде геркон датчигі қолданылады (магнитпен басқарылатын герметикалық контакті) [31].



2.12 сурет - Есік ашылу датчикгін қосу схемасы

Мұндағы, D1 – D4 – есіктердің датчигі

2.1.9 Контроллерді іске қосу

Контроллерге қуат берген кезінде [31]:

1.CONF 1 дип-блогынан конфигурацияны оқиды және оның дұрыстығын тексереді. Конфигурация қате болған жағдайда, контроллер сигнал береді.

2. Ethernet интерфейсі бар EP4 контроллері CONF 2 дип-блогының бірінші переключательдың күйін оқиды. Егер переключатель ON күйінде болса, контроллер IP-конфигурациясын «по умолчанию» күйге келтіреді.

3. Берілген конфигурацияға сәйкес атқарушы құрылғылар мен датчик желілерін іске қосады.

4. Барлық қосылған атқарушы құрылғыларды құлыптайды.

2.13 сурет – Жабдықтардың толық қосылған жобасы

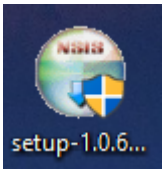
2.2 Бағдарламаны орнатуы мен толық сипаты

Серверлік бағдарлама деректер базасының серверінен және Castle жүйесінің серверлік модулінен тұрады. Сервердің деректер базасы жалпы деректер базасына жүйенің компоненттеріне рұқсат ұсынады. Серверлік модуль байланыс желісі бойынша жүйенің контроллерлерімен ақпараттық алмасуды қамтамасыз етеді [32].

Жүйе бойынша серверлік бағдарлама орнатылған кезде, сервердің екі компоненті Windows қызметтері (сервистері) ретінде тіркеледі және операциялық жүйені қосқан кезінде автоматты түрде іске қосылады.

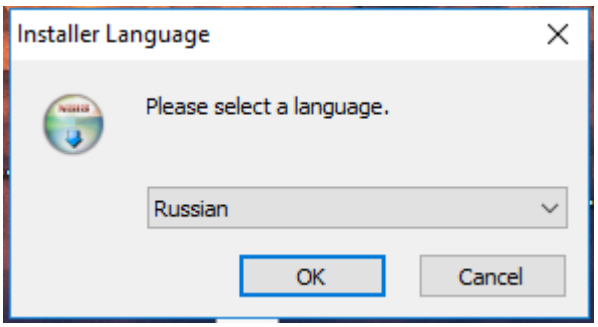
Сервер компоненттерін басқару үшін " Программа управления сервером" қолданылады. Сондай-ақ, стандартты Windows қызмет утилитасын да қолдануға болады. Қызметтердің атауы: Castle database server және Castle service module.

Castle жүйесінің бағдарламасын орнату үшін администратор құқықтары бар жүйеге кіріп, setup.exe файлын іске қосу керек.

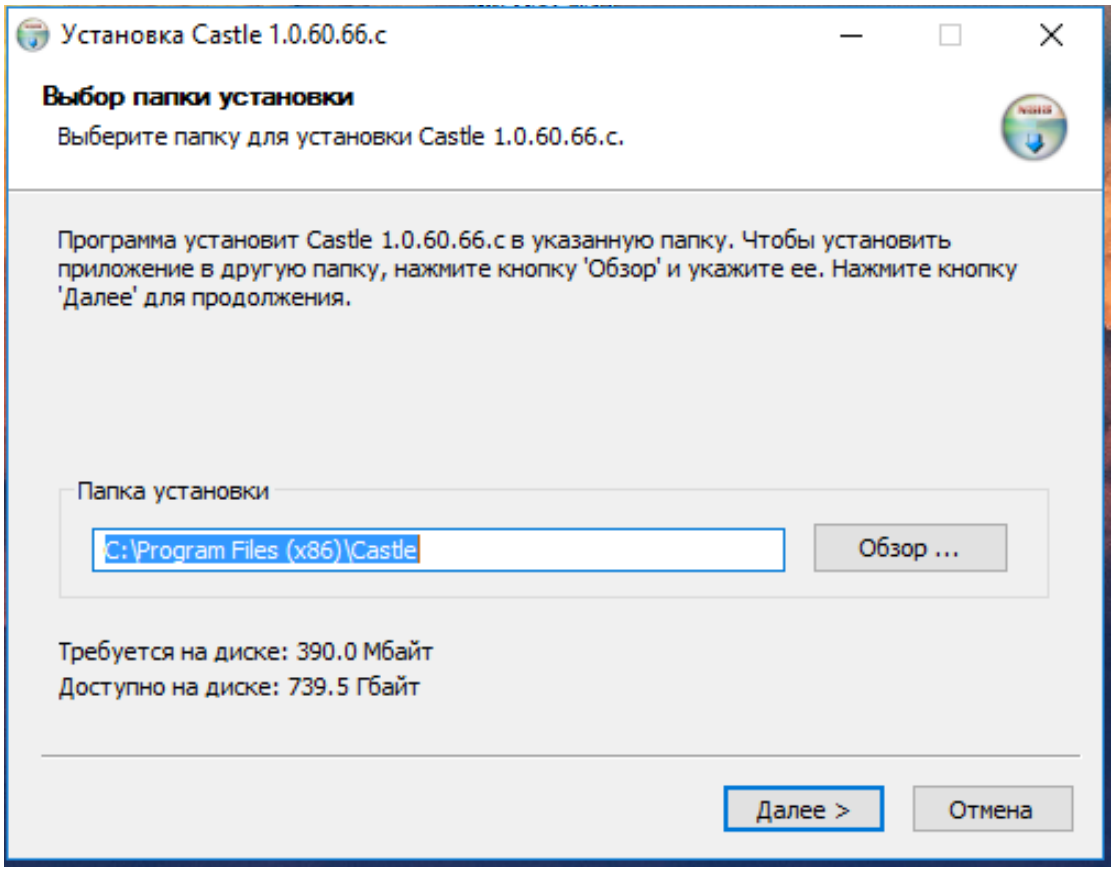


2.14 сурет - setup.exe файлы

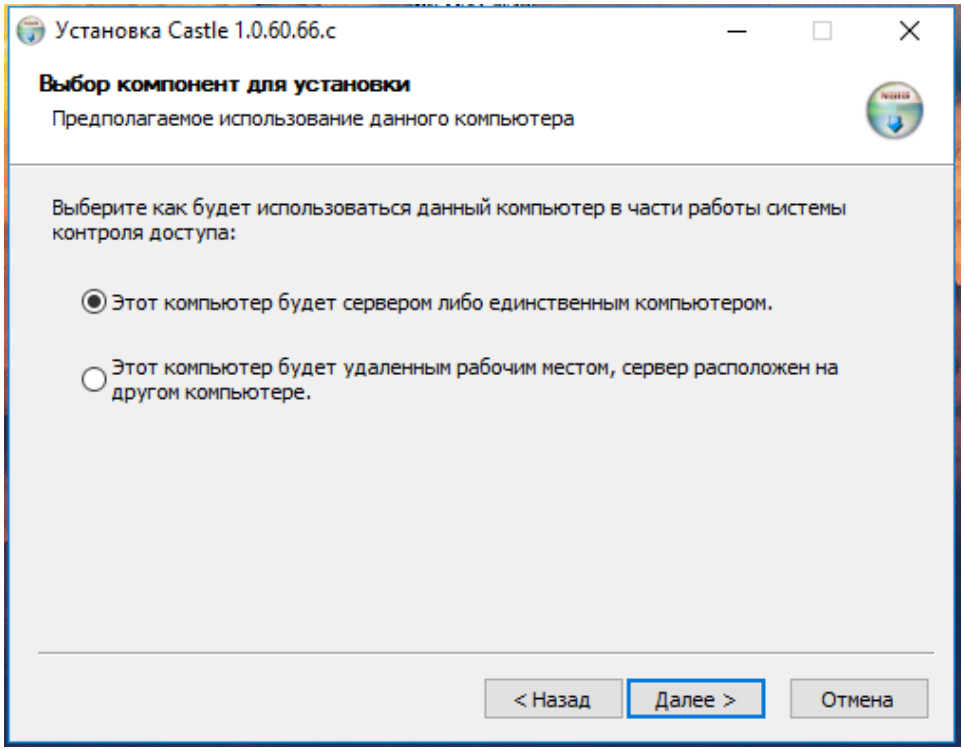
Кейін таңдау терезелері шығады:



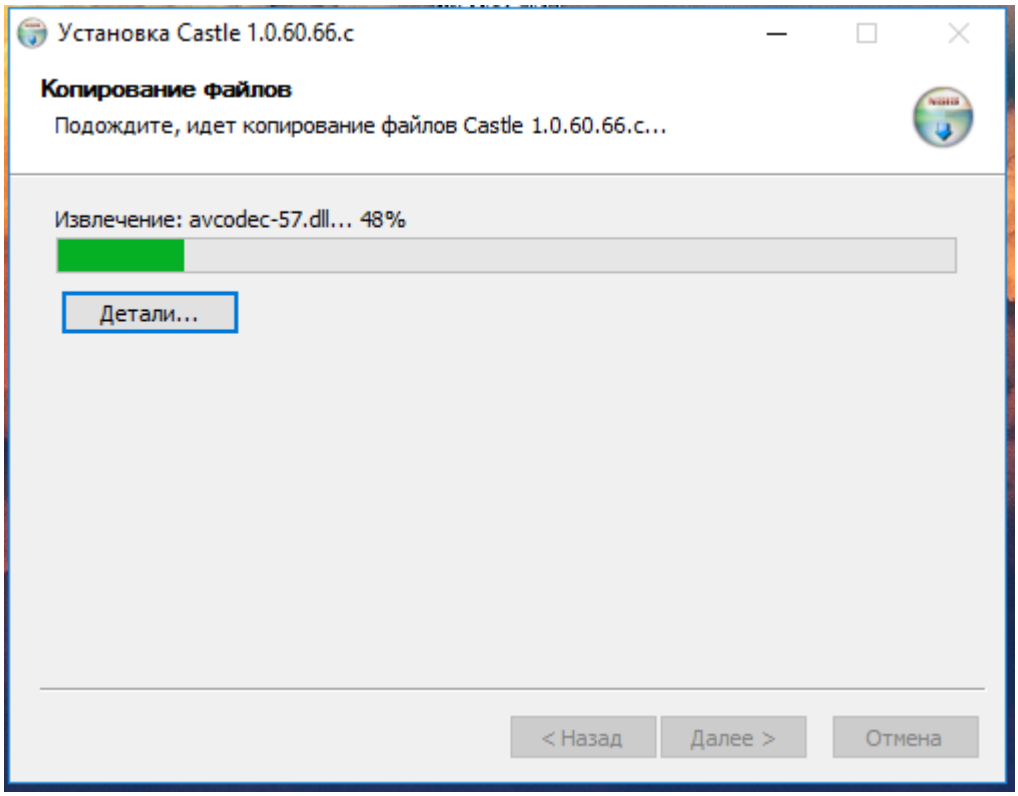
2.15 сурет – Тілді таңдау терезесі



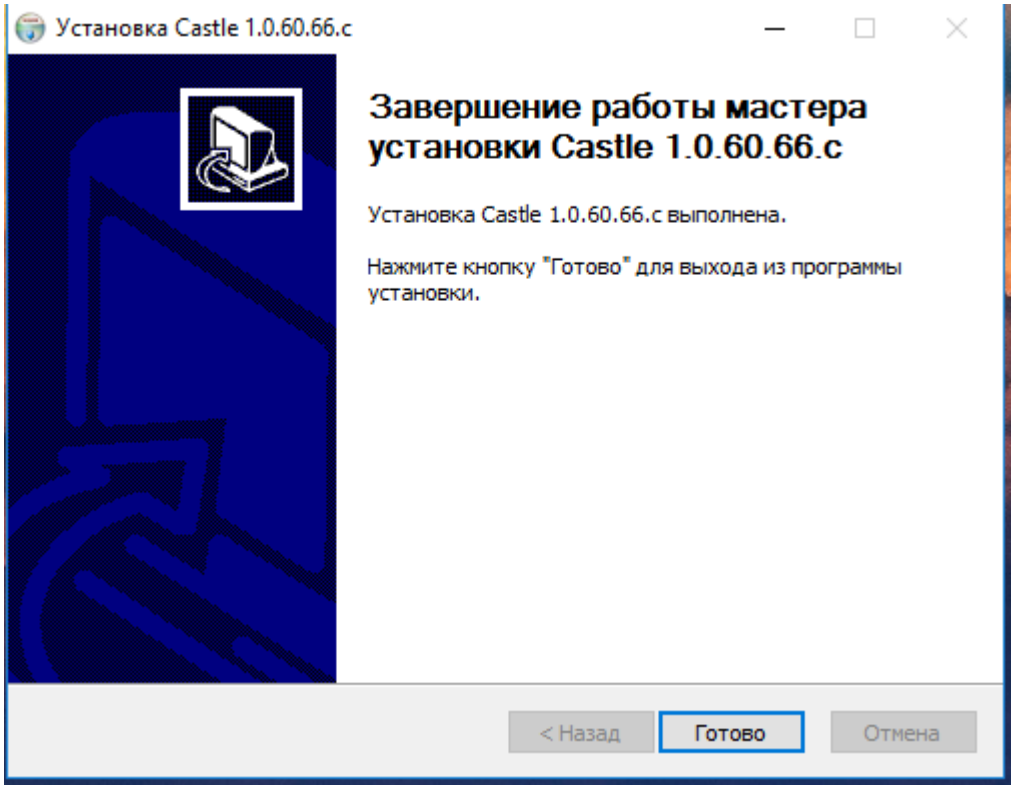
2.16 сурет – Бағдарламаның орнату жолы



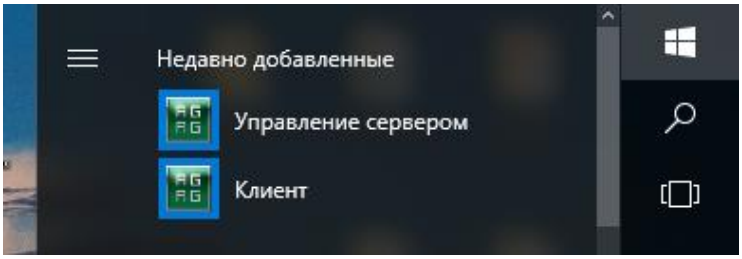
2.17 сурет – Орнатылып жатқан компьютер серверлік екенің таңдау



2.18 сурет – Орнатылу процесі



2.19 сурет – Бағдарлама компьютерге сәтті орнатылды

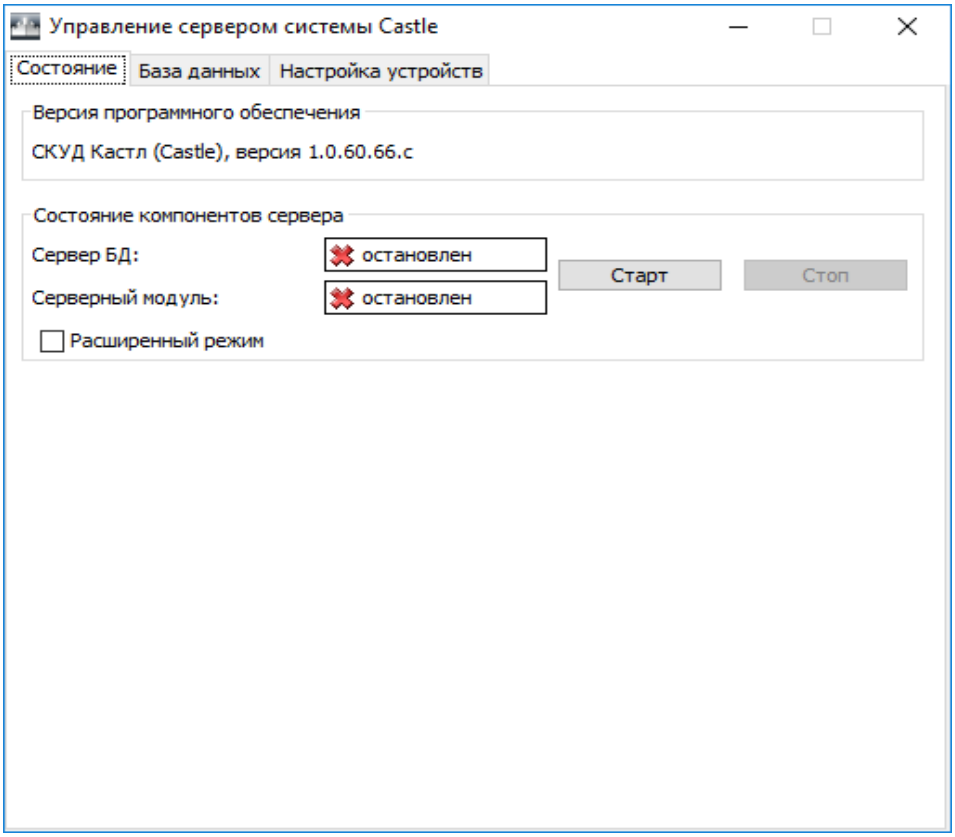


2.20 сурет – Жоғарыда айтып өткенімдей серверлік және клиенттік бағдарлама бірдей орнатылады.

Серверді басқару бағдарламасы сервер компоненттерінің жағдайын бақылауға, деректер базасының резервтеу настройкасы, жүйеге жаңа IP-контроллерлерді қосуға және тағы басқа жұмыстарға арналған.

2.2.2 Серверлік бағдарламаның толық сипаттамасы

Бағдарламаның басты терезесі пайдаланушыға Castle жүйесінің серверін басқару және оның компоненттерінің күйін бақылау үшін барлық құралдарды ұсынады [32].



2.21 сурет – Бағдарламаның басты терезесі

РББЖ Серверін басқару функциялары: «Состояние», «База данных» және «Настройка устройств» вкладкалар бойынша бөлінген.

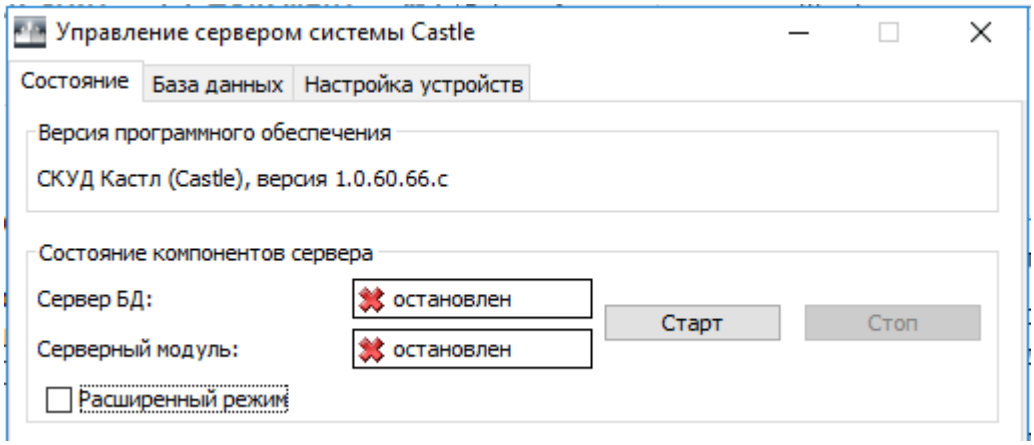
«Состояние» вкладкасында сервер компоненттерін іске қосуға, тоқтатуға және олардың күйін бақылауға болады.

Басқару режимін ауыстыру үшін «Расширенный режим» функциясын қолданады.

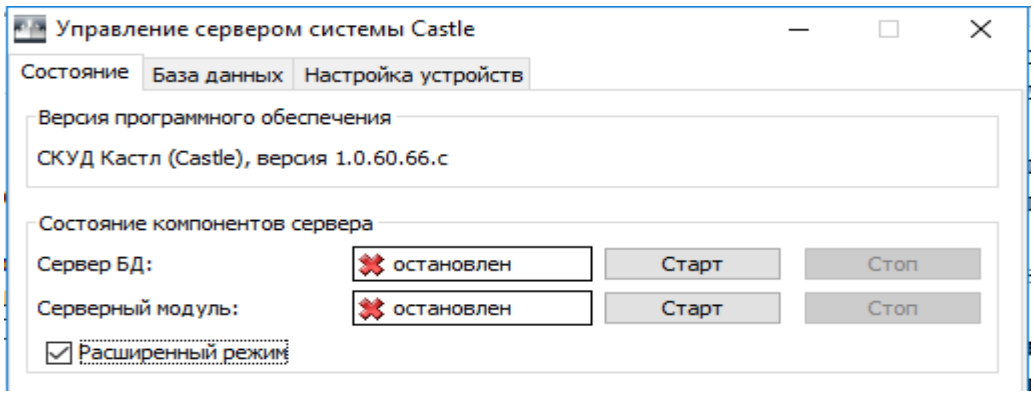
Кеңейтілген режим өшірілген кезде, екі компонентті бірдей қосуға болады. Қосылған кезде - бөлек.

Компоненттерді іске қосу "Старт" батырмасымен жүзеге асырылады.

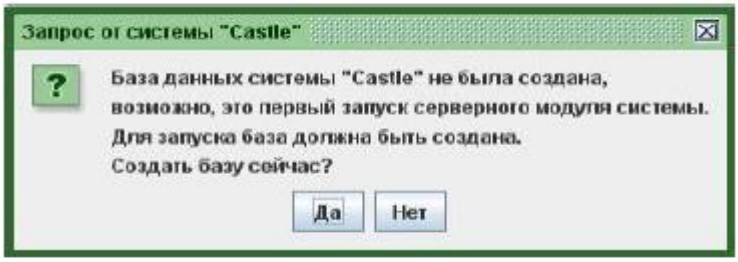
Компоненттерді тоқтату "Стоп" батырмасымен жүзеге асырылады.



2.22 сурет – «Расширенный режим» функциясы өшірілген кезде

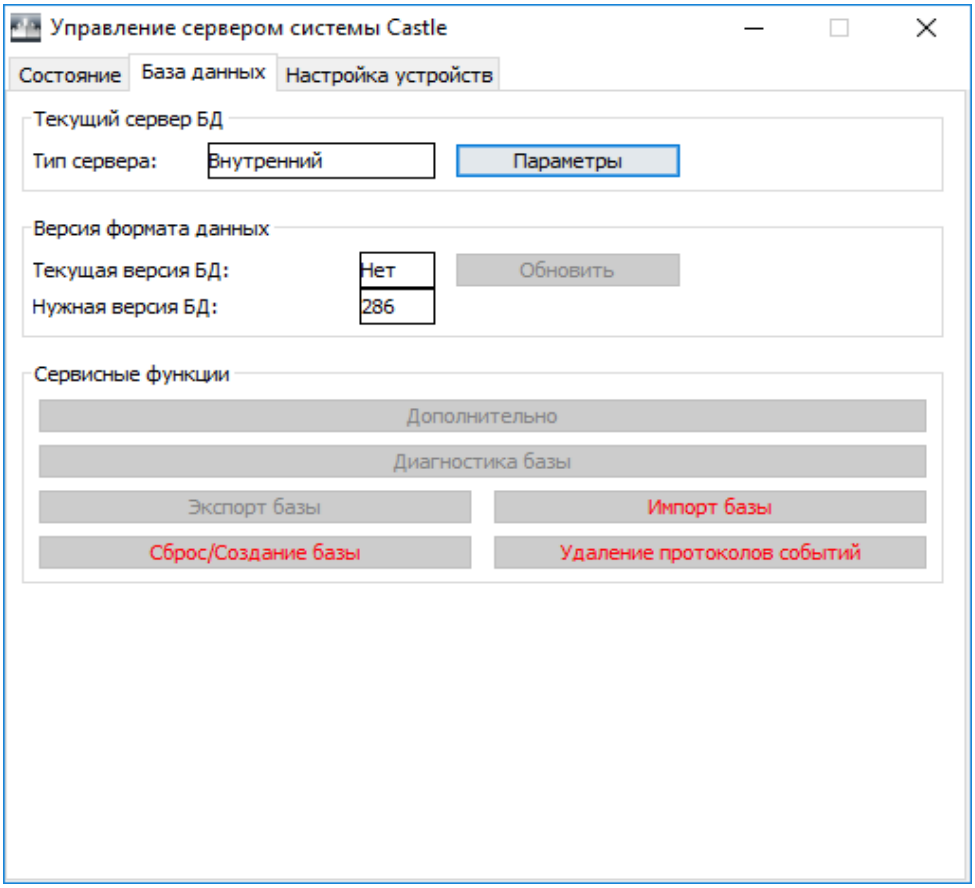


2.23 сурет – «Расширенный режим» функциясы қосылған кезде



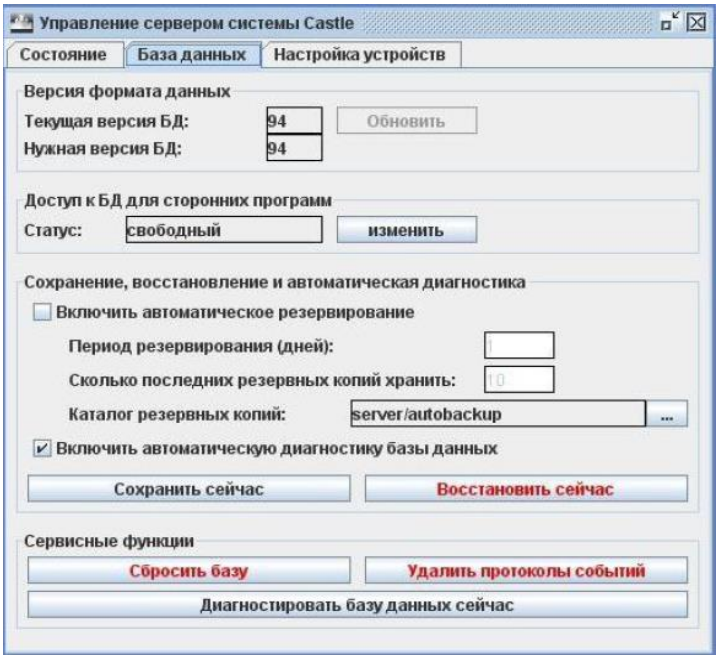
2.24 сурет – Деректер базасын құру туралы сұрау терезесі

"База данных" вкладкасы Castle РББЖ деректер базасымен мүмкін болатын барлық операцияларға арналған.



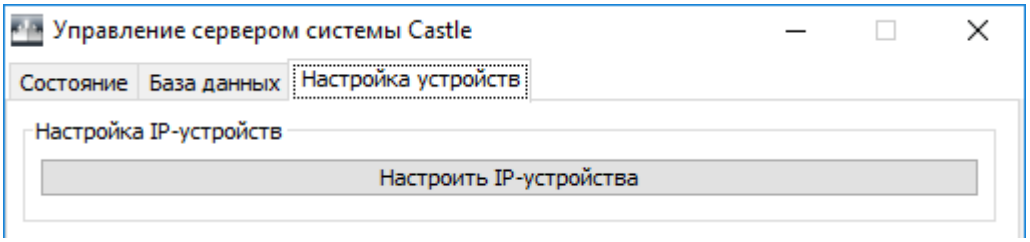
2.25 сурет - "База данных" вкладкасының терезесі

Менің орнатқан бағдарламам тегін болғандықтан, қол жетімді операциялар аз болып келеді.



2.26 сурет – Толық версияның терезесі

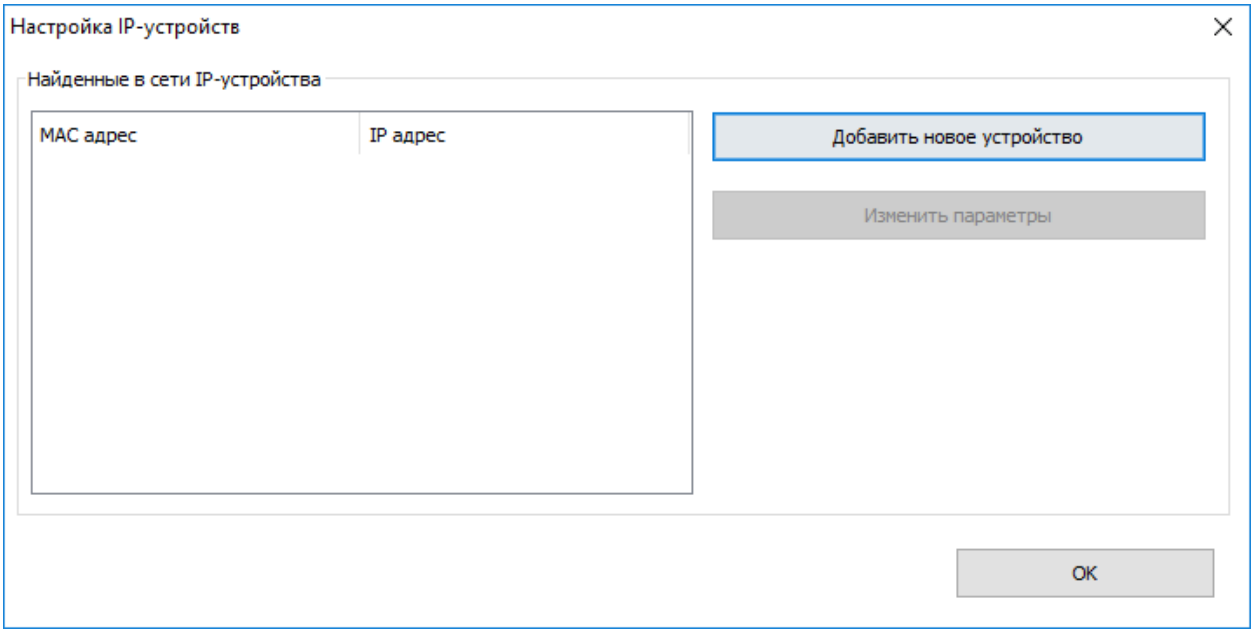
"Настройка устройств" вкладкасында Castle контроллерлерін қосуға немесе конфигурациялауға, сондай-ақ желідегі қазіргі уақытта қосулы тұрған құрылғылар тізімін көруге болады.



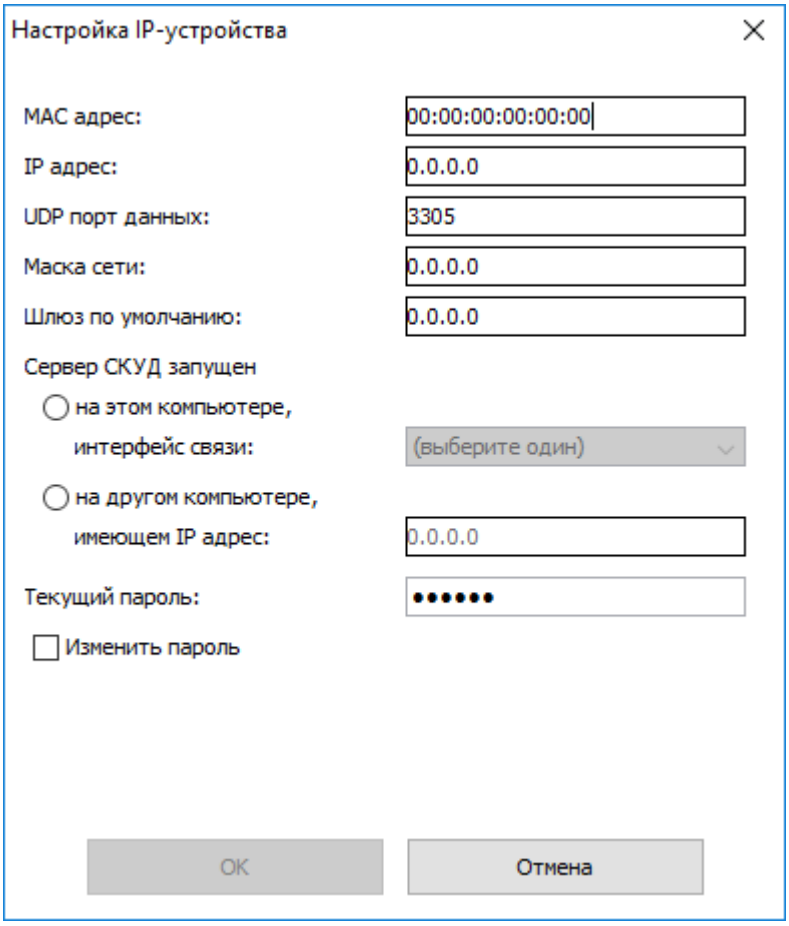
2.27 сурет – "Настройка устройств" вкладкасы

Жаңа Castle РББЖ құрылғысын қосу немесе қосылған құрылғының IP-параметрлерін өзгерту үшін Castle серверін басқару бағдарламасында "Настроить IP-устройства" таңдау керек.

Ашылған терезеде орнатылған IP параметрлері бар құрылғылар тізімі болады, сонымен бірге " Добавить новое устройство " және " Изменить параметры " кнопкалары бар.



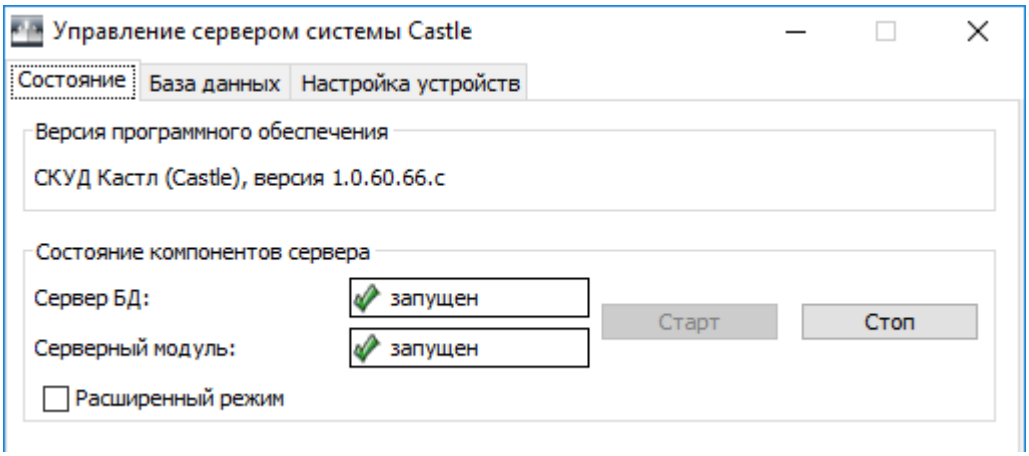
2.28 сурет - "Настроить IP-устройства" терезесі



2.29 сурет – Жаңа контроллерлерді қосқым келген кездегі менюсі

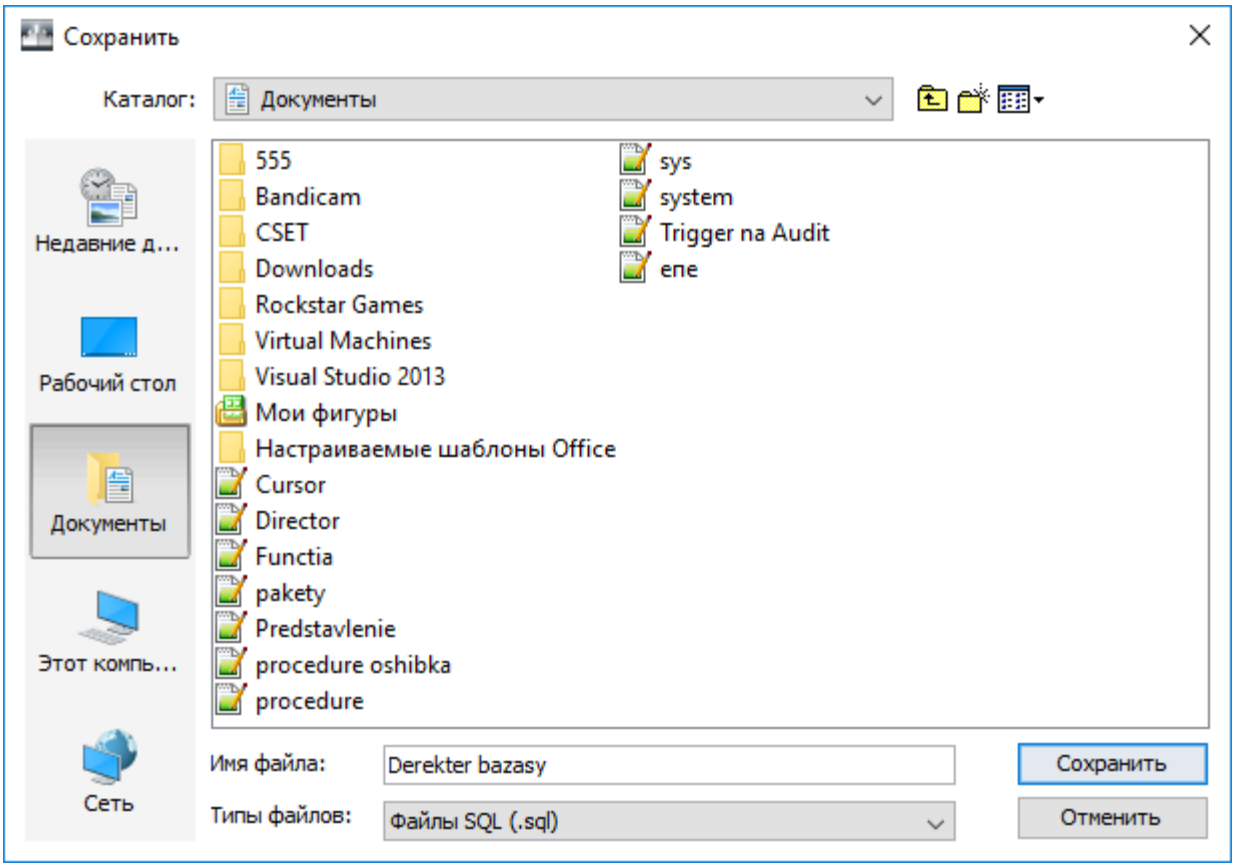
2.2.1 Деректер базасын сайтпен байланыстыру

Біріншіден, деректер базасын құраймыз.



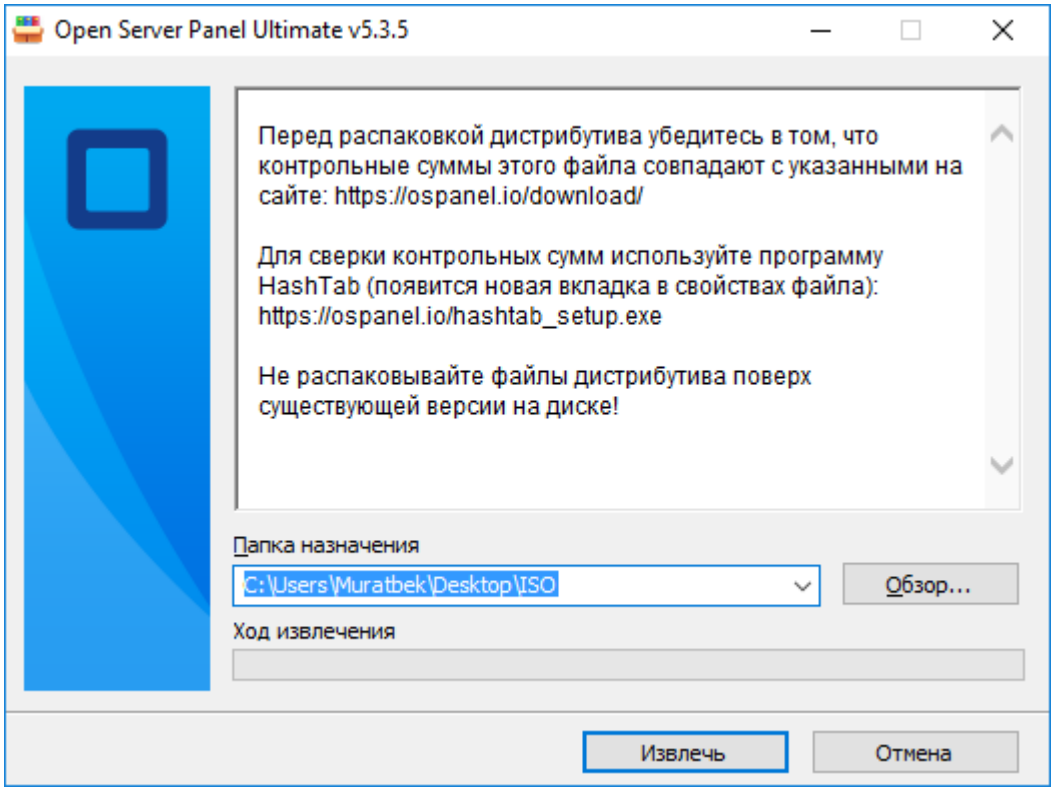
2.30 Сурет – Деректер базасының құрылуы

Содан кейін, клиенттік бағдарламада керек деректердің барлығы қосылғаннан кейін, деректер базасын тиісті папкаға экспорттаймыз. Біздің жағдайда, «Документы» деген папкада «Derekter bazasy» деген атымен.



2.31 сурет – Деректер базасының сақталу жолын таңдау

Сайттың өзінің серверлік бағдарламасы болады. Байланысу жолын көрсету үшін мен OpenServer деген бағдарламаны таңдадым. Себебі ол қолдануға ыңғайлы, әрі түсінікті. Алдымен, оны орнатып, іске қосамыз.

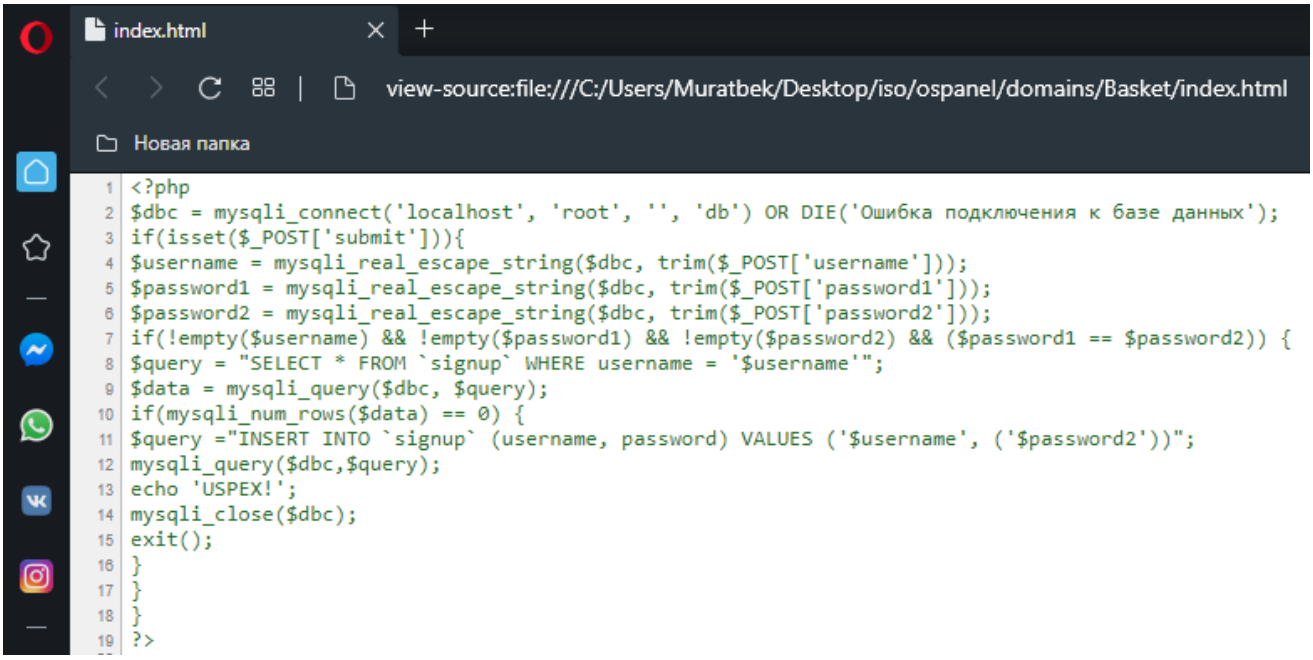


2.32 сурет – OpenServer – дың сақталу жолын таңдау

Содан соң, OpenServer бағдарламасы мен сайттың арасындағы байланысты орнатамыз. Ол төмендегі PHP коды арқылы жүзеге асады.

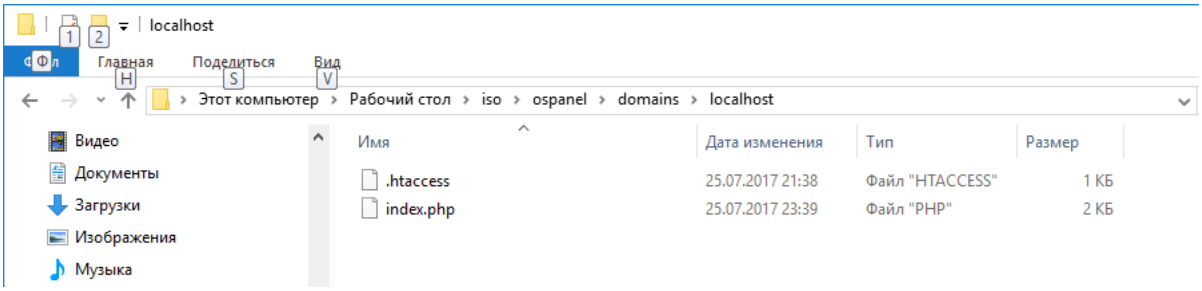
```
<?php
$dbc = mysqli_connect('localhost', 'root', '', 'db') OR DIE('Ошибка подключения к базе данных');
if(isset($_POST['submit'])){
$username = mysqli_real_escape_string($dbc, trim($_POST['username']));
$password1 = mysqli_real_escape_string($dbc, trim($_POST['password1']));
$password2 = mysqli_real_escape_string($dbc, trim($_POST['password2']));
if(!empty($username) && !empty($password1) && !empty($password2) && ($password1 == $password2)) {
$query = "SELECT * FROM `signup` WHERE username = '$username'";
$data = mysqli_query($dbc, $query);
if(mysqli_num_rows($data) == 0) {
$query ="INSERT INTO `signup` (username, password) VALUES ('$username', ('$password2'))";
mysqli_query($dbc,$query);
echo 'USPEX!';
mysqli_close($dbc);
exit();
}}}
```

?>



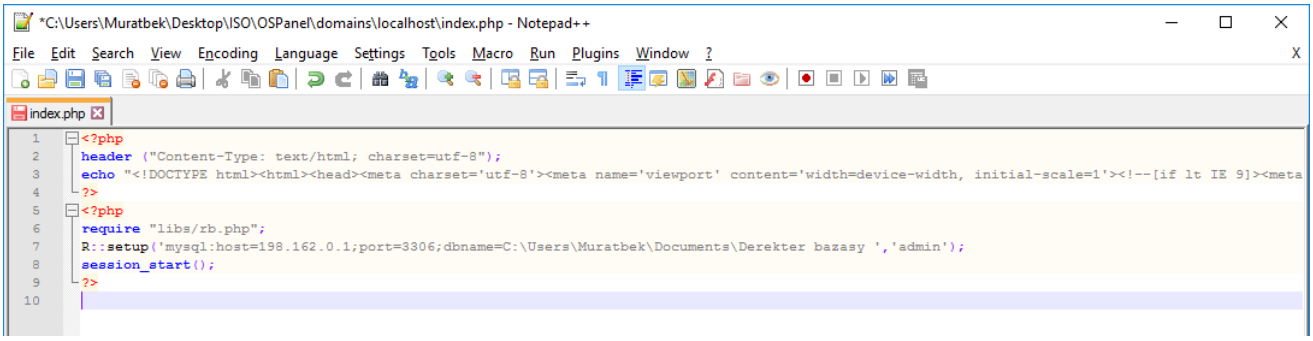
2.33 сурет - PHP код

Сайт пен бағдарлама арасында байланыс пайда болған соң, деректер базасы мен сайтты байланыстырамыз. Ол үшін бізге index.php деген файлға кіріп, төмендегі кодты енгіздіреміз.



2.34 сурет – index.php файлі

<?php
require "libs/rb.php";
R::setup('mysql:host=198.162.0.1;port=3306;dbname=C:\Users\Muratbek\Documents\Derekter bazasy ','admin');
session_start();
?>

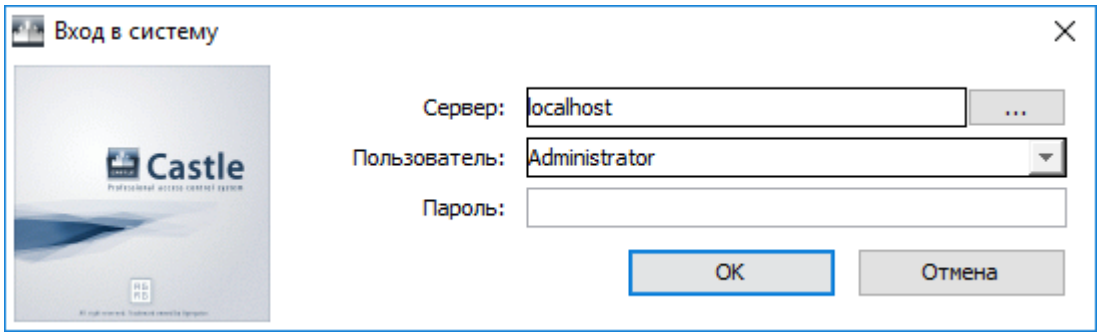


2.35 сурет – index.php файлға терілген код

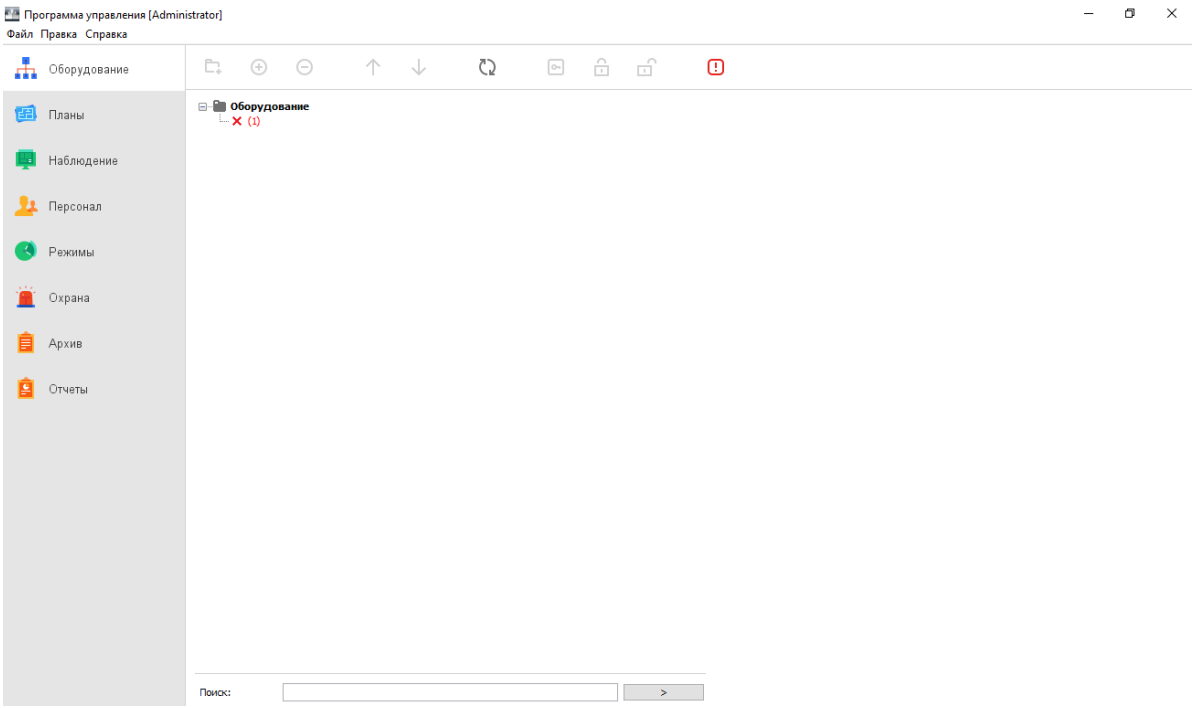
Барлық байланыс құрылып болған соң, сайтты қосқан жағдайда ДБ-ға енгізілген барлық деректер шығып тұрады. Әр күні, жұмыстың соңында администратор ДБ-ны экспорттаған сайын, сайттағы деректер жаңарып, жаңа деректер қосылады. Яғни, оқытушыларға студенттердің бар-жоғын енгіздіру қажет болмайды.

2.2.3 Клиенттік бағдарламаның толық сипаттамасы

Клиенттік ПО "Castle РББЖ клиенті" бағдарламасынан тұрады. Оны TCP хаттамасы бойынша, сервермен қосылған желіден кез келген компьютерге орнатуға болады. Сонымен қатар, клиенттік ПО-ны тікелей Castle РББЖ серверін өзіне де орнатуға болады [33].



2.36 сурет – Клиенттік ПО қосқандағы терезесі

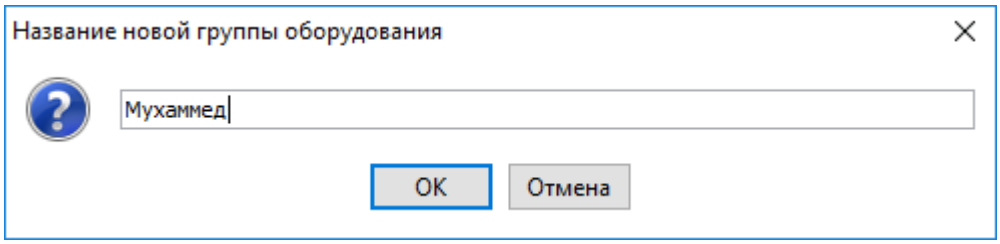


2.37 сурет – Клиенттік бағдарламаның басты терезесі

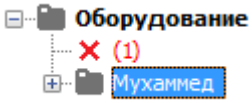
Барлық Castle РББЖ қолжеткізу нүктелерін (ТД) настройкалау және басқару үшін "Оборудование" вкладкасы арналған.

2.38 сурет – Қолжеткізу нүктелерінің тізімін басқару түймелері

Жаңа топты немесе кіру нүктесін қосу үшін тиісті батырманы басу жеткілікті, содан кейін топ үшін оның атауын енгізу қажет.

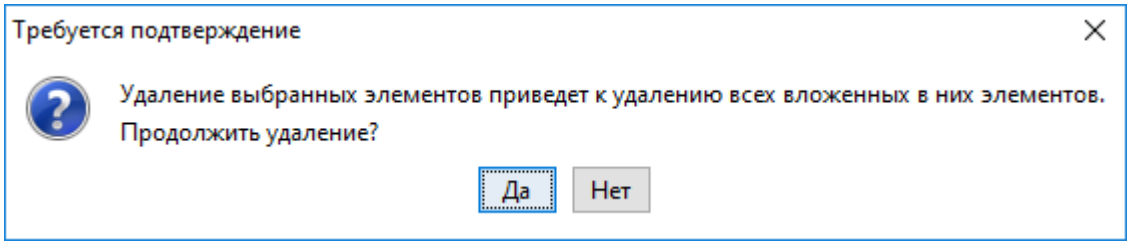


2.39 сурет – Жаңа топты қосу

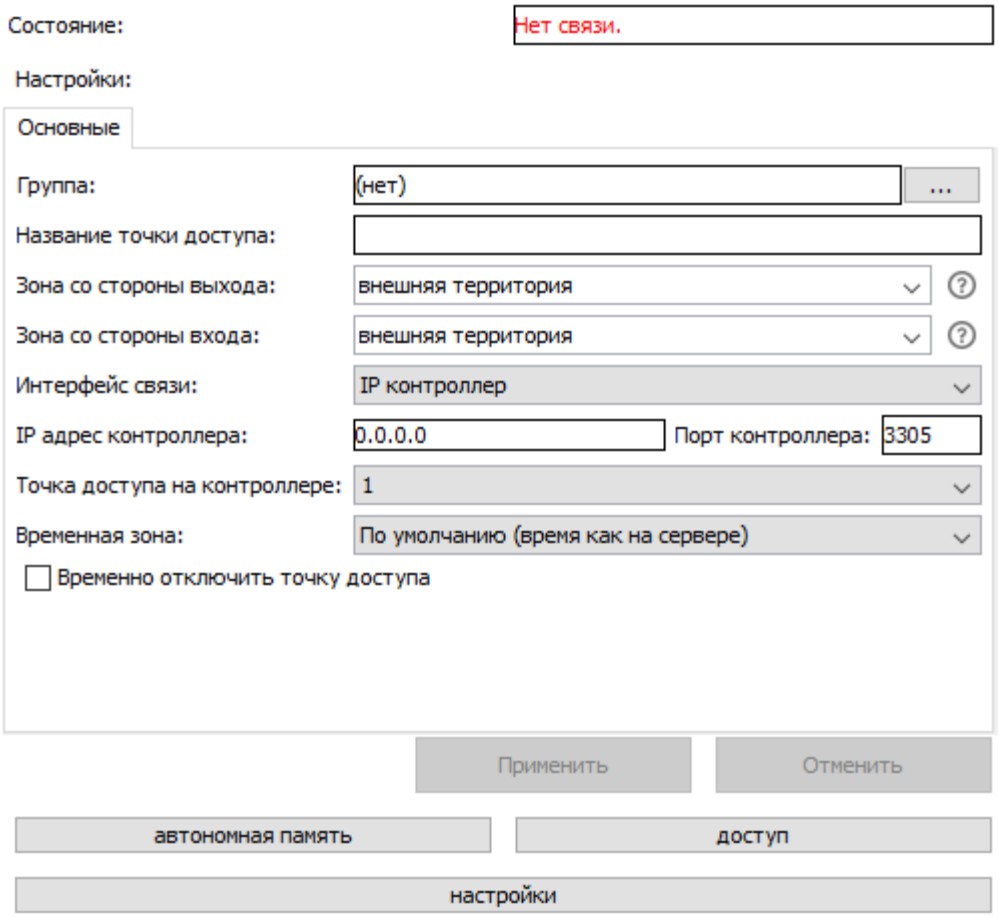


2.40 сурет – Жаңа топтың пайда болуы

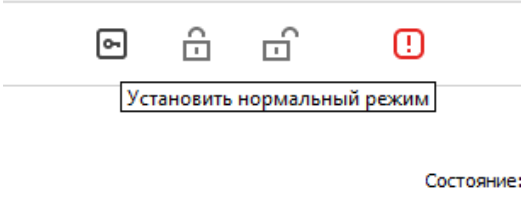
Топты немесе ТД-ны жою үшін оны тізімде бөлектеп алып, "Удалить выбранные элементы" батырмасын басу керек, содан кейін жоюды растау қажет.



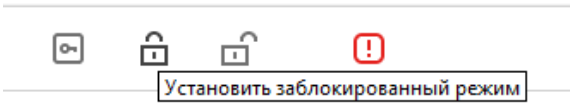
2.41 сурет – Топты жою



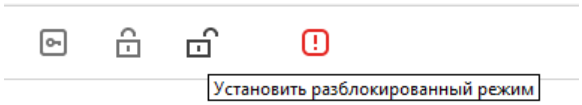
2.42 сурет – Топ немесе ТД-ның жалпы сипаттамасы



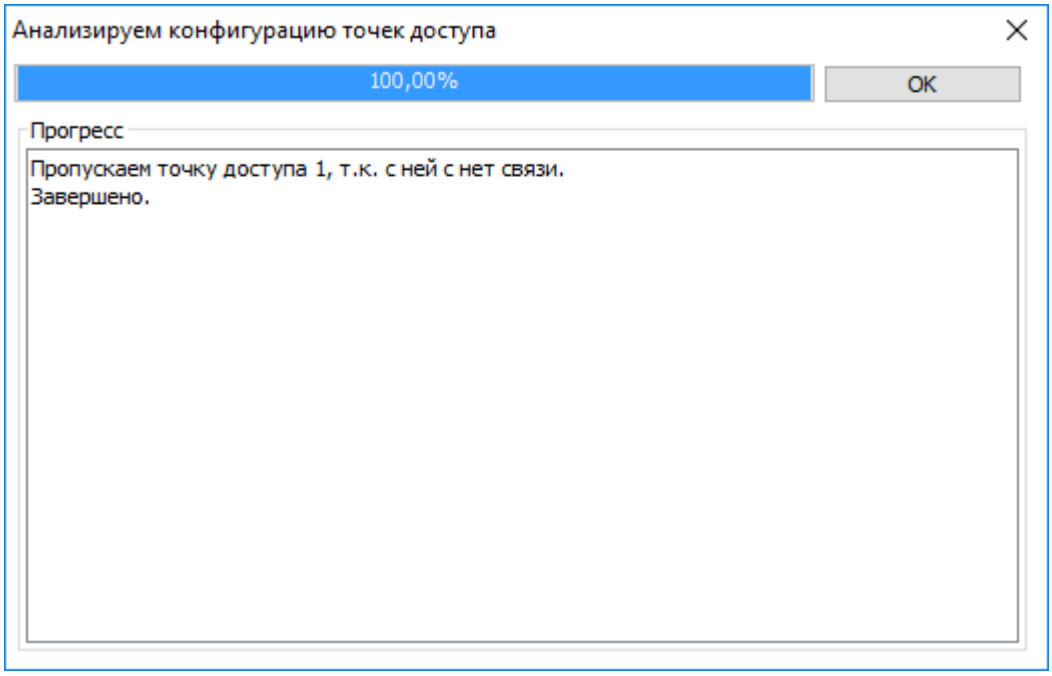
2.43 сурет – Қалыпты жағдайға қосу кнопкасы



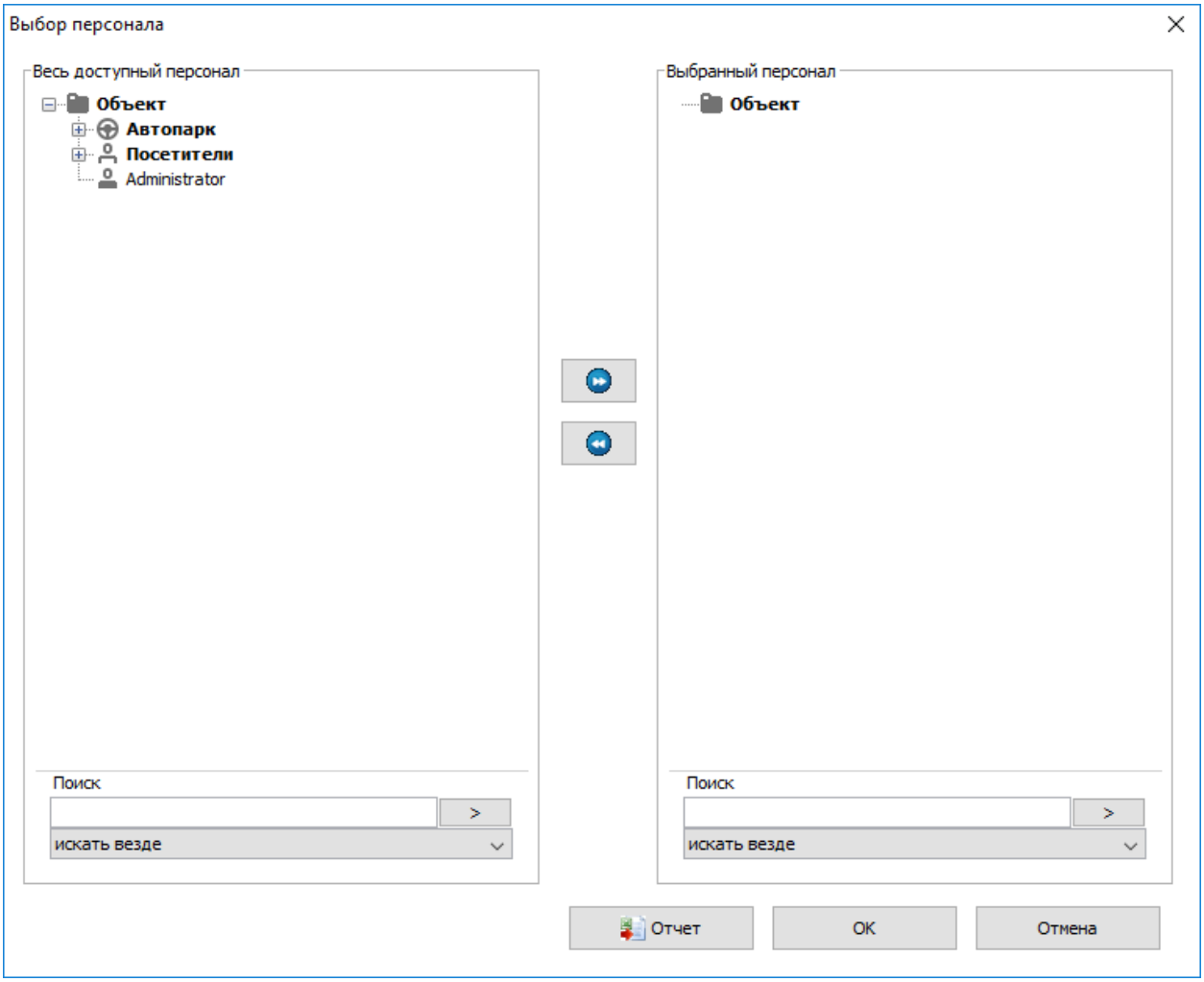
2.44 сурет – Блок жағдайға қосу кнопкасы



2.45 сурет – Блок емес жағдайға қосу кнопкасы

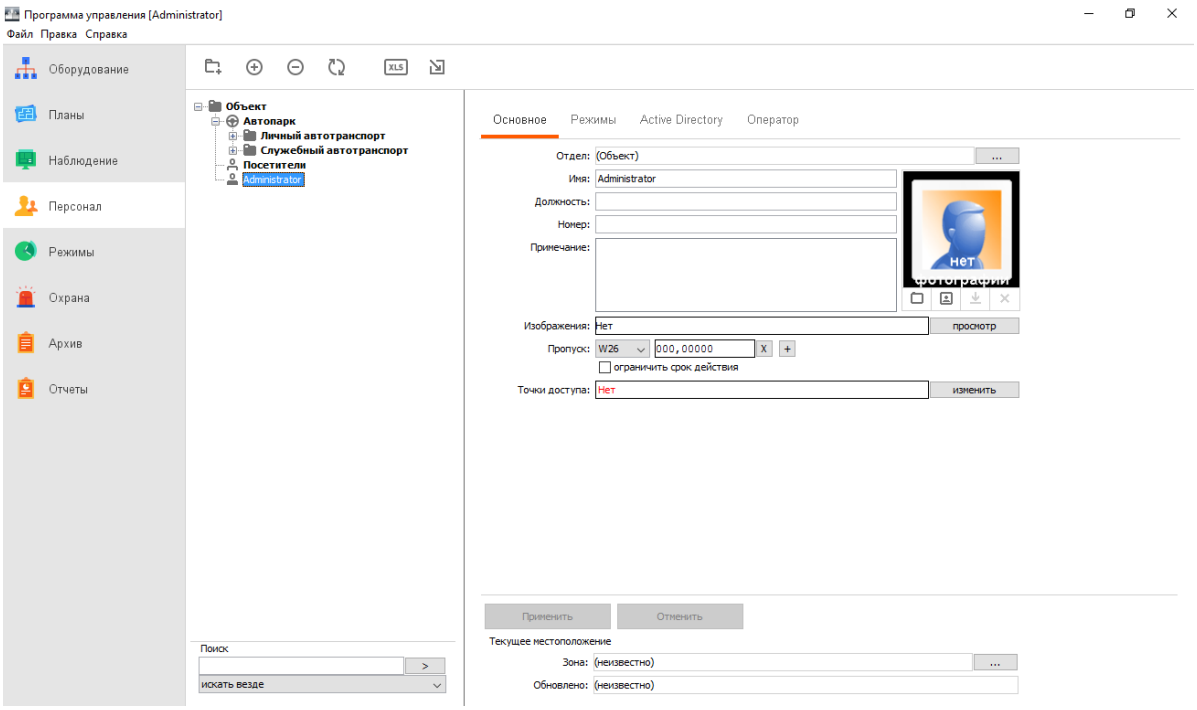


2.46 сурет – «Автономная память» кнопкасын басқан кезде ТД конфигурациялық анализын жасайды



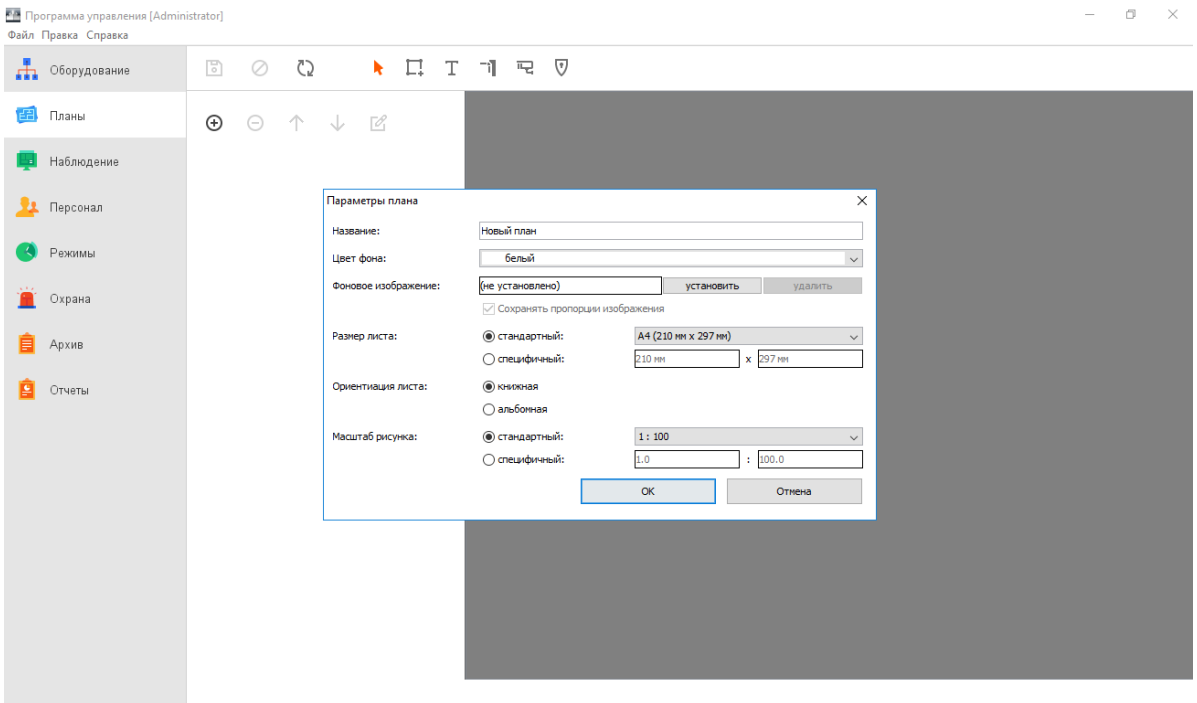
2.47 сурет – рұқсатты реттеу терезесі

Жүйенің қолжетімділік объектілерінің тізімін басқару үшін "Персонал" вкладкасы арналған. Қызметкерлерді қосу және жою, бөлімдер мен кіші бөлімдерді құру, қолжеткізу нүктелері бойынша қолжетімділікті шектеу, қол жеткізу режимдерін беру және тағы басқалары.



2.48 сурет – "Персонал" вкладкасының менюсі

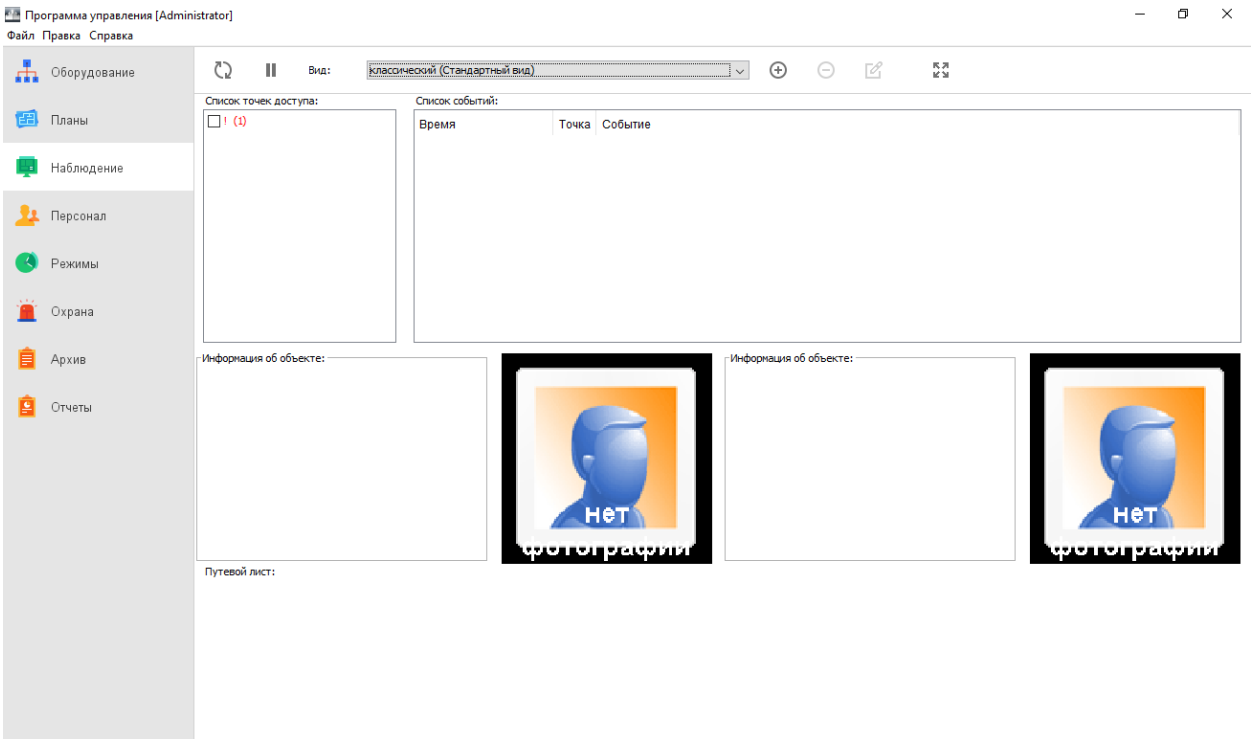
Помещениялардың жоспарларын жасап, оларға РББЖ нүктелерін және бейнекамералардың орналасуын көрсету үшін "Планы" вкладкасы арналған. Оны пайдалану объект схемасында көрсетілген нақты уақыттағы оқиғаларды ыңғайлы және көрнекі бақылауға, сондай-ақ кіру нүктелерін жедел басқаруға мүмкіндік береді.



2.49 сурет – " Планы" вкладкасының менюсі

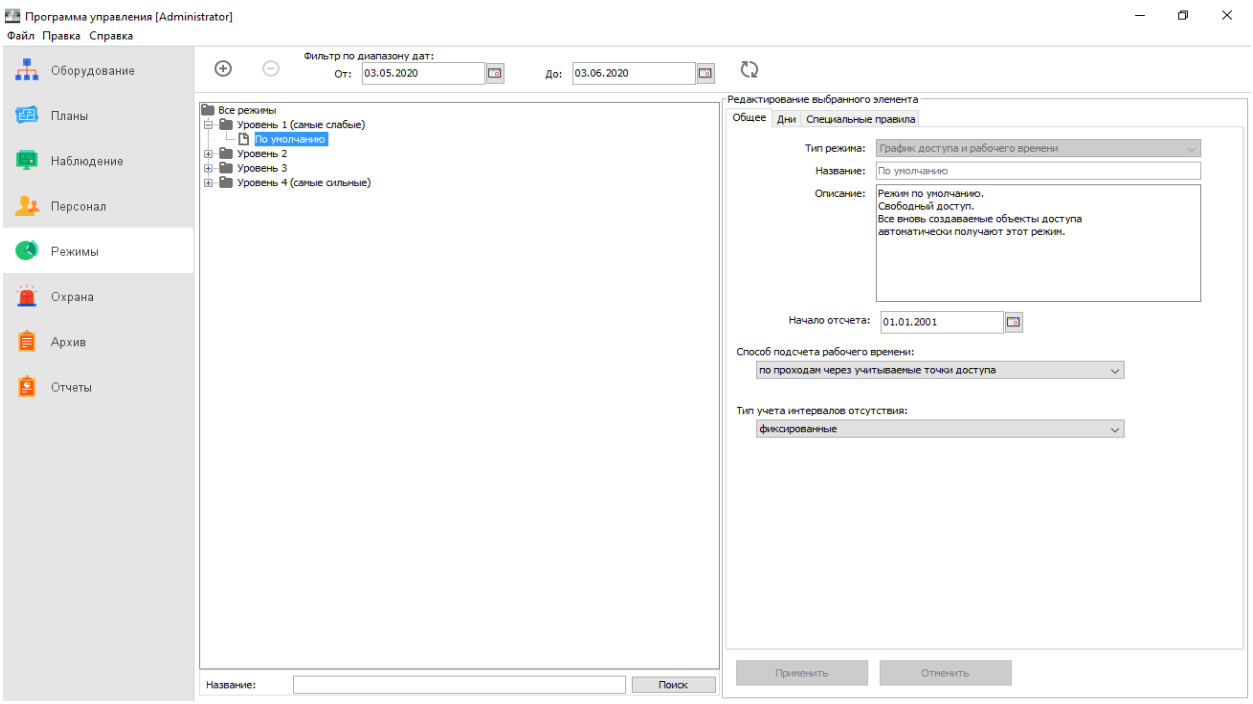
"Наблюдение" қойындысы жүйенің оқиғаларын нақты уақытта қарауға және келесі функцияларды жүзеге асыруға арналған:

– Жүйенің қолжеткізуіне рұқсат беру немесе тыйым салу себептерін.
– Өтетін адамдардың фотосуреттер мен учетный данныйларын көру .
– Бейнебақылау және IP-камералар жүйелерімен тірі бейне көру.
– Күзет санкциясынан қолжеткізу функциясын қамтамасыз ету .
– Қолжеткізу нүктелерімен байланыстың болуын бақылау.



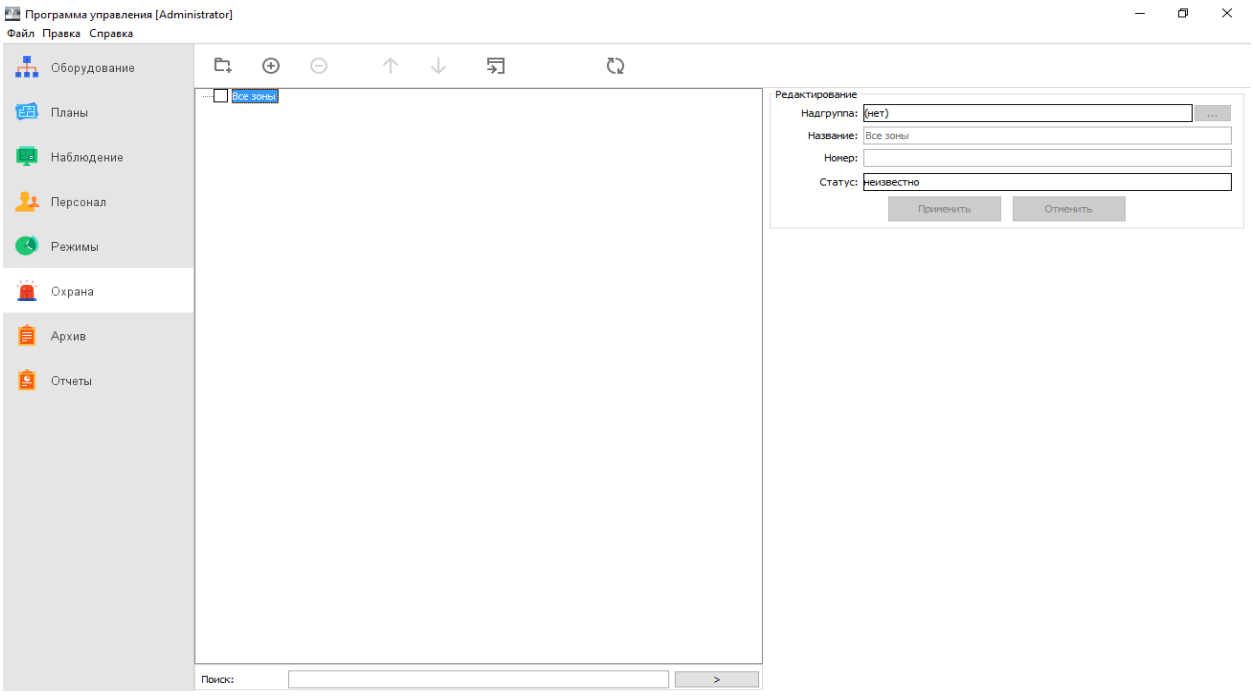
2.50 сурет – "Наблюдение" вкладкасының менюсі

"Режимы" вкладкасы режимдерді, ерекшеліктер мен бұйрықтарды жасау, өңдеу және жою үшін арналған.



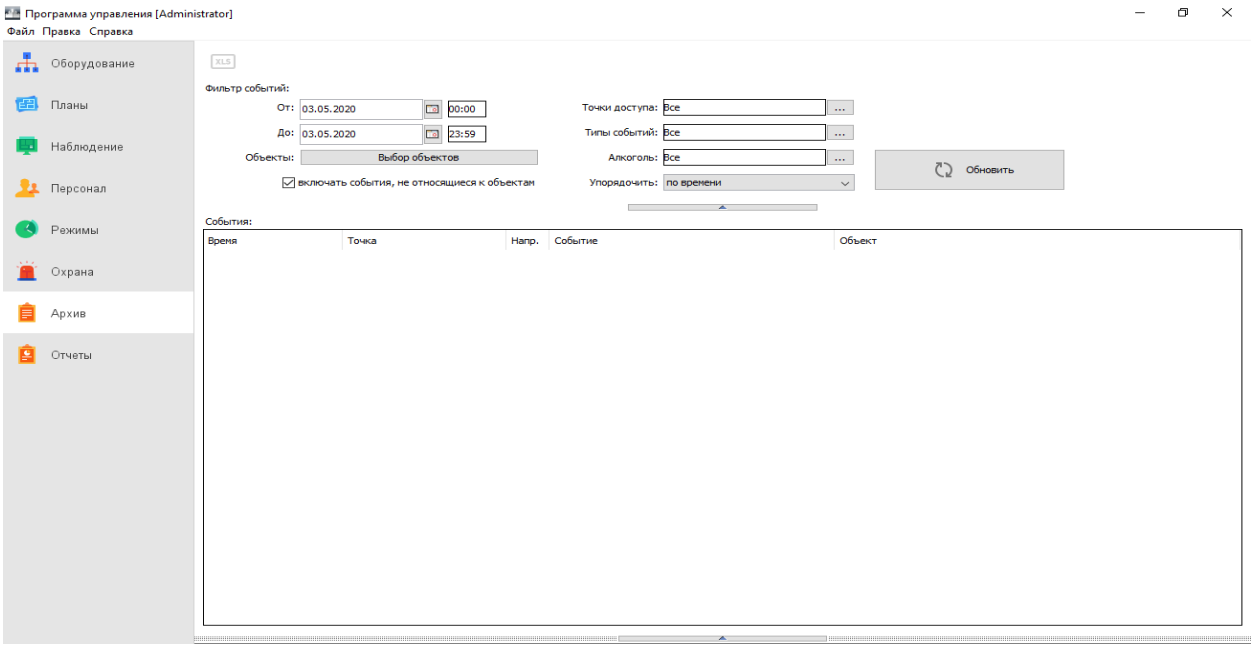
2.51 сурет – " Режимы" вкладкасының менюсі

Күзет (өрт) аймақтарының конфигурациясын басқару және бақылау "Охрана" вкладкасында жүреді. Жеке иерархиялық тізім жасауға, күзет аймағын немесе аймақтар тобын қосуға немесе жоюға, басқа аймақ конфигурациясын импорттауға, аймақтар топтарының жағдайын бақылауға және оларды басқару деген жұмыстар атқарылады.



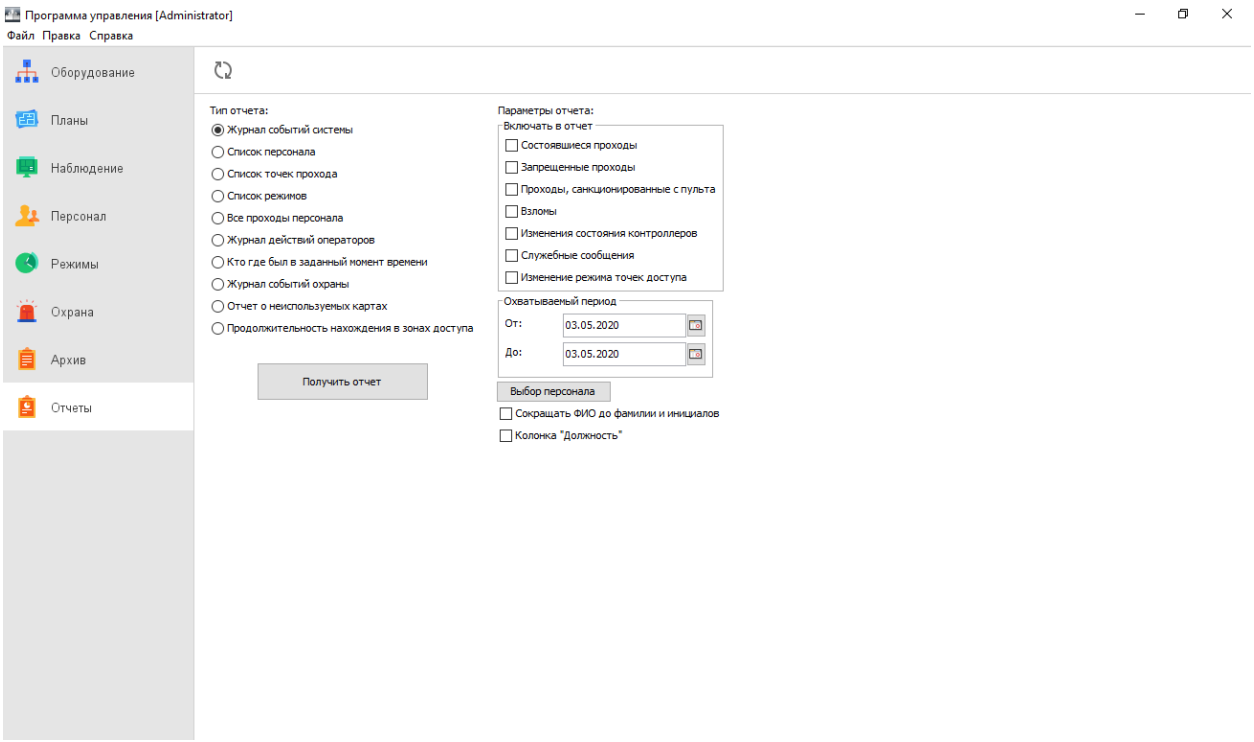
2.52 сурет – "Охрана " вкладкасының терезесі

Берілген уақыт аралығында жүйеде болған қолжеткізу нүктелері мен персоналдың оқиғалары туралы ақпаратты алу үшін "Архив" вкладкасына жүгінеміз. Бұл вкладка операторға қажетті ақпаратты тез алуға мүмкіндік береді.



2.53 сурет – "Архив" вкладкасы

Castle РББЖ-да барлық уақытта тіркелген жүйенің режимдері мен қызметкерлері жайлы оқиғаларды алу үшін "Отчеты" вкладкасын қолданамыз.



2.54 сурет – "Отчеты" вкладкасы беті

3 Университет ғимаратына РББЖ орнатудың толық есебі

РББЖ жабдықтары	**Сипаты**	**Штук саны**	**Бағасы, тг**	**Жалпы құны, тг**
Castle EP4 Желілік контроллері	Есіккерді басқару жұмысын атқарады	25	120000	3000000
Castle EP Желілік контроллері	Турникетті, екі есікті, қақпаны немесе шлагбаумды басқару үшін.	2	110000	220000
Matrix-2-EH	Карта есептеуіші	104	10000	1040000
TS-MAGIC	Шығу кнопкасы	100	5000	500000
OMA-26.461_/1	Турникет-трипод	2	290000	580000
TRD-1086C	Есікке арналған соленоидтық электромеханикалық құлып	100	18000	1800000
ИО 102-5	Өткен адам саның санайтын магнитті-контактілі датчик	100	900	90000
ББП-20	Үздіксіз қоректендіру блогы	27	7500	202500
SF 1207	Аккумулятор 7А/сағ	27	3400	91800
Castle Em-Marine	Байланыссыз карта			Универдегі адам санына байланысты
ПО Castle	Castle-дің толық бағдарламасы	1	300000	300000
Қорытынды				7 824 300 тг

4 Өмір-тіршілік қауіпсіздігі бөлімі

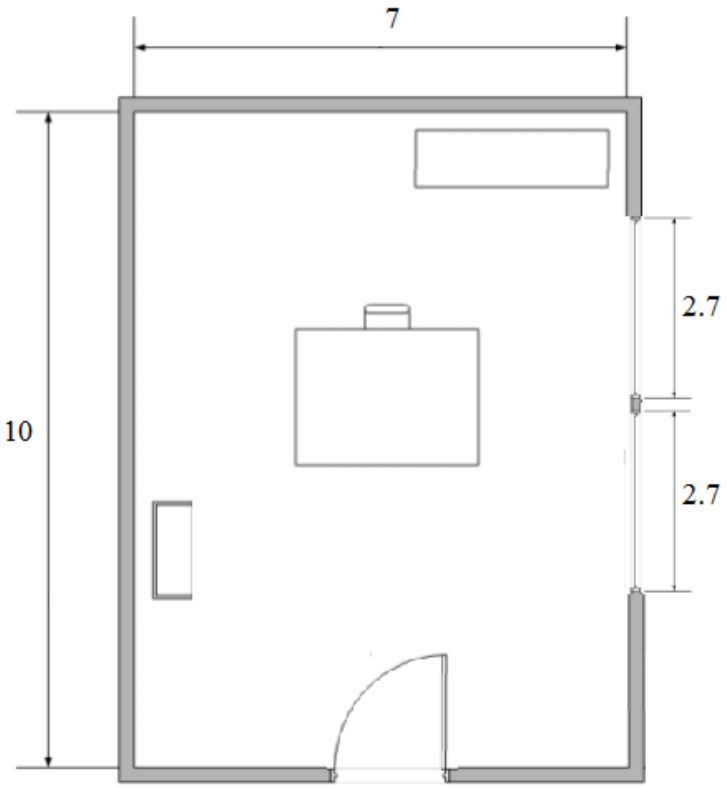
4.1 Жұмыс жағдайын талдау

Дипломдық жоба "Университеттерде рұқсатты бақылау және басқару жүйесін жобалау» бойынша жүйені орнатқаннан кейін бағдарламамен жұмыс жасайтын администратордың бөлмесінде өмір-тіршілік қауіпсіздігін қарастырдым.

Бөлмеде администатордың жұмысы үшін 1 персоналды компьютер орналасқан. Ғаламторға RJ-45 кабелі арқылы модеммен жалғанып, байланысады. Администратор үшін таңдалған бөлмеде, қауіпті және зиянды өндірістік көрсеткіштердің деңгейі, бақылау бөлмелерінде және әр қашықтағы жұмыс орнында белгіленген нормадан өтпейді, администраторға орындалатын жұмыстың күрделілік дәрежесіне байланысты мүмкіндігінше ыңғайлы. Тек жарықтандыру жүйесін дұрыстау керек болды. Сондықтан, бөлменің жарықтандыру жүйесін есептеп, администраторға жұмыс жасауға қолайлы жағдай жасалу туралы шешім қабылданды.

Администратор бөлмесінің ұзындығы 7 метр, ені 10 метр, биіктігі 3 метр. Бір қабырғада пердесі бар екі терезе орналасқан. Әрқайсысының биіктігі 1,8 метр және ені 1,5 метр.

4.1 суретте бөлмеде: 2 терезе, шкаф, жұмыс орны, есік, ауаны баптау.



4.1 сурет − Бөлме жоспары

Еңбек жағдайлары негізінен администрацияға, өндіріс технологиясына, оны ұйымдастыру, еңбек ағымы және айналадағы санитарлық-гигиеналық жағдайға байланысты. Автоматты және өздігінен жұмыс жасайтын өндіріс әдістері, жергілікті жабдықтарды басқару және техногендік процестерді енгізу мүмкіндігі де ерекше емес.

Администатордің негізгі міндеттері - жабдықтың күйін бақылау және оның конфигурациясын жасау, ақпаратты өңдеу, оны жүйеге енгізу және оны әрі қарай зерттеу үшін бағдарламалық жасақтамада нақты көрсету мүмкіндігі.

Жұмыс кестесі 5/2, яғни жұмыс күндері. Демалыс күндері демалады, одан кейін әрі қарай жұмыс жасайды. Негізгі үзіліс - түскі ас. Негізгі үзілістен әрқайсысы 20 минутқа тең тағы екі қосымша енгізілді.

Компьютердің алдында жұмыс уақыты орташа, яғни қажет болған жағдайда ғана отырады, оған қоса администратор әр сағат сайын дерекқордың күйін тексеріп отырады.

Құзыретті және үздіксіз жұмыс үшін қажетті ұйымдық жабдық сервер орнатылған коммутациялық шкафына администратор үшін оңай қол жетімді болатындай етіп ұйымдастырылған.

Жұмыстың жайлылығына әсер ететін маңызды сәттердің бірі - жарықтандыру. Жарық жағдайлары денеге жалпы пайдалы әсер етеді, сонымен қатар адамның жұмысы мен белсенділігіне әсер етеді. Бөлмедегі жұмыс күн сайын болатындығына байланысты біз жасанды жарықтандыруды есептейміз.

Жылы мезгілде бөлме температурасы, оның қозғалғыштығы мен ылғалдылығына тиісінше 23 - 25 Цельсии бойынша градусқа тең, 0,1 - 0,2 метр/сек, 60 - 70% құрайды.

Кондиционер тәулік бойы және автоматты жаңарту үшін оңтайлы шектерде ауытқиды. Сондай-ақ, бөлменің ішіндегі администраторлық бөлмеде орнатылған басқару панелінің арқасында ауаны реттеу мүмкіндігі қарастырылған.

Байланыс торабы администраторлық бөлмеде болғандықтан, біз міндетті түрде автоматты газбен өрт сөндіруді қарастыруымыз керек. Жүйенің өзі негізінен автономды жұмысқа бапталған, сондықтан адамның қатысуы тек оған қызмет көрсетуге және тоқсан сайынғы профилактикалық жұмыстарға байланысты.

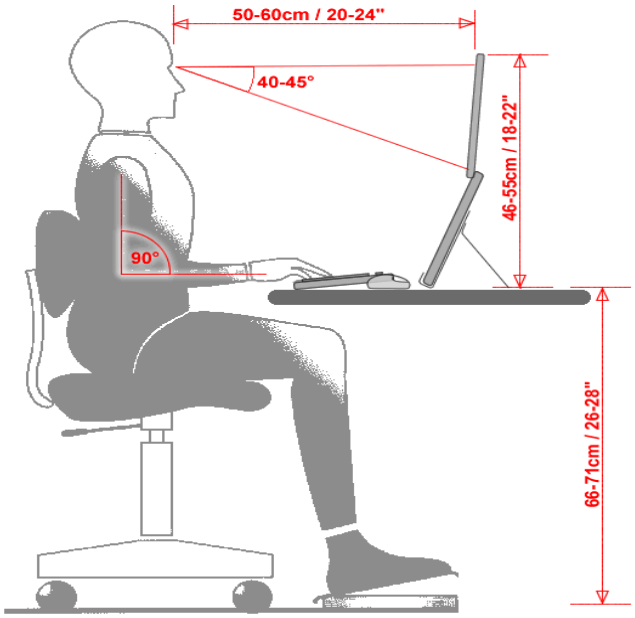
4.1.1 Жұмыс орнының эргономикалық талаптары.

Эргономика - қазіргі заманғы өндіріс жағдайында адам немесе адамдар тобының қызметін және олардың жұмыс құралдары мен еңбек үрдісін оңтайландыру мақсатында, зерттейтін ғылым. Адамның еңбекке деген белсенділігі көбінесе ол жұмыс істеп отырған қызмет шарттарымен анықталады. Оларға жұмыс орны мен жұмыс істеу кеңістігі жатады. Жұмыс кеңістігі мен

жұмыс орнын эргономикалық жобалау кезінде келесідей ең жақсы деген жұмыс жағдайларын құру керек:

- технологиялық процесстің талаптарына сәйкес жұмыс істейтін адамның еңбек қозғалысы мен еркін қозғалу мүмкіндігін орналастыру;
- жұмыс ерекшелігіне қарай және ең оңтайлы еңбек тәсілін пайдалана отырып, ыңғайлы жұмыс күйінде негізгі және қосымша операцияларды орындау;
- басқару құралдарының адам қозғалысы кеңістігінің оңтайлы шегінде орналасуы;
- жұмыс күйі мен жұмыс қалыпын ауыстырған жағдайда визуалды ақпарат көзін оңтайлы шолудың сақталуы;
- жабдықтарды ұтымды үлестіру, қызметкерлердің қауіпсіздігі.

Бұл бөлімде қарастырып отырған жұмыс сипаты, отырықшы және ПК қатысуымен болғандықтан, ең алдымен компьютер алдында отыру нормаларын анықтаймыз. СаНПИН 2.2.4.548-96/03 [1] бойынша монитор экраны пайдаланушы 60-70 см қашықтықта орналасу керек, бірақ 50 см ден төмен емес.



4.2 сурет - Эрганомикалық талапқа сай отыру күйі

Монитор экраны 60 см қашықтықта орналасқан, яғни нормаға сәйкес.

Отырықшы қалпында жұмыс кезінде келесідей жұмыс кеңістігі ұсынылады:

- ені 70 смден кем емес;
- тереңдігі 40 смден кем емес;
- еденмен жұмыс үстелінің беті арасындағы биік 70-75 см.

Жұмыс үстелінің оңтайлы көлемі:

- биіктігі 71 см;
- үстел ұзындығы 130 см;
- үстел ені 65 м.

Администратор үшін маңызды элементтің бірі жұмыс орындығы. Оңтайлы орындық болу үшін адам физикалық қозғалу мүмкіндігі болуы қажет және жұмыс кеңістігінде еркін қозғалуы керек. ПК алдында дұрыс отыру қалыпы 4.2 суретте көрсетілген.

4.1.2 Электр қауіпсіздігі

Электр қауіпсіздігі дегеніміз – адамдарды зиянды және қауіпті электр тогының, электр доғасының, электромагниттік өрістің және тұрақты токтың әсерінен қорғауды қамтамасыз ететін ұйымдастырушылық және техникалық қызмет түрлері мен құралдары. Біздің қарастырып отырған бөлмеде ЭЕМ жабдықтары, яғни компьютерлер және оның қосымша перифериялық жабдықтары орналасқан.

Электрлік құралдарға жататын барлық дерлік ЭЕМ жабдықтары, эксплуатация процесі кезінде немесе профилактикалық жұмыстарды орындау кезінде адамға қауіп төндіруі мүмкін, себебі жоғарға кернеулі күйде тұрған бөлігіне адам денесі тиіп кету мүмкін.

Мысалы, электр тогымен зақымдану немесе өрт қауіпі немесе ЭЕМ жұмыс істеу кезінде төтенше жағдайларды болдырмау үшін келесідей талаптарды орындау керек:

- СанПиН 2.2.2/2.4.1340-03 «Гигиенические требования к персональным электронно-вычислительным машинам и организации работы» [2] стандарты бойынша ЭЕМ орналасқан жұмыс орны бар бөлмелерде, жабдықтарды эксплуатацияға жібермей тұрып, қорғайтын жерге тұйықтаумен техникалық талаптарға сай жабдықтау керек. Жерге тұйықтау дегеніміз - кернеу астында болуы мүмкін металды жанды элементтерінің қорғаныс өткізгіштер қасақана электр байланысы;
- ЭЕМ пайдаланушыларының жұмыс орындарын күштік ЭЕМ жұмысына кедергі келтіретін кабельдерден, жоғарғы вольтті трансформаторлардан алшақ орналастыру керек.

Әдетте, компьютердің электр энергиясына қосылуы тиісті үшжолды ашасы мен электр желісі бар жерге розетка жоғары жиілікті кедергі арқылы айналып әзірленген желілік сүзгі конденсаторлар бар қоректену блогы арқылы жүзеге асырылады. Бұл жағдайда, ашаға үш сым қосылуы керек: бірі- фазалық, екіншісі - нөлдік жұмыс сымы және үшіншісі - нөлдік қорғаныс сымы (НҚС). Егерде НҚС еш жерге қоспағанда, жүйелік блоктың корпусында 110 В айнымалы тоқтың кернеуі пайда болуы мүмкін. Бұл жағдай сүзгі конденсаторының кернеуді сыйымдылықтық бөлу ретінде жұмыс істегеннен болады. Конденсатор

сыйымдылықтары бірдей мән иеленгендіктен, желі кернеуі 220 В екіге теңдей бөлінеді. Егерде адам денесінің орташа кедергісі 1000 Ом екендігін, ал еденнің және аяқ киімінің кедергісі 330 Ом ескерсек, адам денесінен өтетін тоқ 83 мА құрайды. Бұл жағдайда, демалу параличі ұстауы мүмкін. Келесіде ЭЕМ іске қосу кезінде мынадай ұсыныстарды сақтауға тиіс:

- әрдайым үшсымды ашалар қосылу байланысының сенімділігін тексеріп отыру;
- жүйелік блокты НҚС ға қосымша қосу, мысалға көрек көзіне сымды бекіту;
- дисплейді келістірілген құрал арқылы қосу ұсынылады. Онымен қатар желілік сүзгілер және барлық сымдар оператордың жұмыс орнынынан алшық тұруы қажет;
- жүйелік блокты жоғары ылғалды және жоғары шаңды жер аймағы мен оператор аяғының астына және еденге қоюға болмайды;
- бір уақытта монитор экранына және пернетақтаға қол тигізуге болмайды(жоғары электростатикалық потенциал болуы мүмкін);
- электр тогымен зақымдануды алдын алу үшін қосылып тұрған компьютердің артқы жүйелік блок панеліне қол тигізіп, перифериялық және басқа құрылғылардың разьемдарын ауыстыруға болмайды;
- ЭЕМ ді және оның пернетақтасын тұрақты тоқ жиналатын бетке қоймау керек(органикалық әйнек және жылтыраған лакты беткей);
- бөлмедегі температура 20-25 °С мәнінде рұқсат етіледі, салыстырмалы ылғалдылық 75 %;
- шектен шыққан шаңдану рұқсат етілмейді, (1 мг/м кем емес);
- күнделікті ылғалды тазарту жұмыстарын жүргізу керек.

4.1.3 Өрт кезінде адамдарды қауіпсіз эвакуациялауды қамтамасыз ету

Өрт кезіндегі негізгі міндет адамдар үшін қауіпсіз аймақ құру болып табылады. Объектіде қалған адамның сақталуын қамтамасыз етудің ең басты және маңызды әдісі оны эвакуациялау болып табылады.

Қауіпсіздік аймағы - адамдар денсаулығы үшін зиянды факторлар мен сәттерден қорғалған орын.

Эвакуацияның қажетті уақыты - өрт қауіпті факторлардың әсерінен пайда болған кезден бастап адамдардың өмірі мен денсаулығына зиян тигізбей қауіпсіз аймаққа эвакуацияланған уақыты.

Университетті қоса алғанда, адамдар көп болатын қоғамдық ғимараттарда СКУД орнатылған эвакуациялық (апаттық) шығу есіктері апаттық ашылатын құрылғылармен жабдықталуы керек [4].

Эвакуациялық есіктерді шұғыл ашу құрылғылары бір әрекетпен қосылуы тиіс, яғни көлденең жолақты жай ғана басу арқылы. Ол есік төсемінің ішкі

бетінде орнатылған, яғни есік блогының енінде орналасқан штангаға немесе штанга- рейкаға басу арқылы кілтсіз және басқа тетіктерсіз ашылады.

Адамдар жиі болатын бөлмелерде өрт шыққан кезде адамдар үшін қауіпсіз аймаққа қол жеткізу сызбалары ғимараттың барлық қабаттарына шығу алдында және одан кейін орнатылуы керек, онда кез-келген әрекеттерді орындау стандарттары көрсетіледі.

Өрт кезінде қызметшілердің орындау нормативтерін анықтайтын ережелер жинағы қызметкерлердің өз бетінше шығу, сондай-ақ эвакуациялауға қабілетсіз адамдарды эвакуациялау үшін тәртіптің реттелген тізімін қамтиды.

Адамдар көп уақыт бойы бөлмелерде отыратын жағдайда хабарлау және адамдарды эвакуациялауды басқару жүйесімен жабдықталуы тиіс. Оны пайдаланудың дәлдігі өрт кезінде адам өмірін сақтауға жауапты басшылықтың өз қызметкерлеріне қаншалықты жақсы жеткізгеніне байланысты болады. Алғашқы өртке қарсы оқу-жаттығулар кезінде жүйелер үшін жауапты қызметкерлер осы құрылғылардың әрекет ету принципін, қол өрт хабарландырушыларының орналасқан жерін, сондай-ақ осындай жағымсыз жағдайлар кезіндегі іс-қимыл регламентін қызметкерлерге жеткіздіреді.

Басшылық жарты жылда кемінде бір рет, ал егер бұл адамдар жиі жиналатын жер болса, онда тоқсанына кемінде бір рет адамдардың және төтенше қызметтердің хабарлауына жауап беретін жүйенің жұмыс қабілеттілігін тексере отырып, өрт кезінде олардың регламенттік іс-қимылдары бойынша қызметшілерге оқу-жаттығуларды өткізуге міндетті.

Диспетчерлік үй-жай хабарлау жүйесіне арналған телефон-аппараттық рупормен жарақтандырылатын бөлмеде орналасады.

Эвакуациялық шығуларды жобалау және әзірлеу кезінде қозғалысты жеңілдететін жүйелер ескерілуі тиіс жәнеде оның ішінде жарықтандыру да кіреді.

4.2 Есептеу бөлімі

4.2.1 Табиғи жарықтандыру есебі

Есеп әдістемелік нұсқауларымен орындалды [6]. Жарық беретін қондырғылардың жобалауы ҚР ҚНжЕ 2.04.-05.2002 [3] бойынша қабылданған жалпы қағидаларға бағынады.

Администратор бөлмесінің ұзындығы 7 метр, ені 10 метр, биіктігі 3 метр. Бір қабырғада пердесі бар екі терезе орналасқан. Әрқайсысының биіктігі 1,8 метр және ені 1,5 метр. Бұл жағдайда, егер, ҚР ҚНжЕ-ге сүйенетін болсақ, онда бүйірлік жарықпен жарықтандыру коэффициенті 1,2% құрайды, Алматыдағы жел климаты 0,65 құрайды. Осы бөлме үшін, ТЖК-ның нормаланған маңыздылығын табамыз:

$$en = e_{\text{Н}} * m_{\text{п}}, \%$$

мұндағы N – табиғи жарықпен қамтамасыз ету тобының нөмірі;
e_H – табиғи жарықтандыру коэффициенті (ТЖК);
m_n – жарық климатының коэффициенті;

$$en = 1{,}2 * 0{,}65 = 0{,}78\%$$

Есептеу, бүйірлік жарықтандыру кезінде жарық ойықтарының ауданын алдын ала анықтау болып табылады:

$$S_0 = \frac{e_n * K_3 * \eta_0 * K_{3d} * S_{\text{п}}}{\tau_0 * r_1 * 100}, \text{ м}^2$$

мұндағы $S_{\text{п}}$ – еденнің ауданы;
S_0 – Жарық ойықтарының ауданы;
K_3 – қор коэффициенті;
η_0 – терезенің жарық сипаттамасы;
K_{3d} – терезелерді қараңғылау коэффициенті;
r_1 – бүйірлік жарықтандыру кезінде ТЖК жоғарылату коэффициенті;
τ_0 – жарық өткізу;

$$\tau_0 = \tau_1 * \tau_2 * \tau_3 * \tau_4 * \tau_5$$

мұндағы τ_1 – материалдың жарық өткізу коэффициенті
τ_2 – жарықтың түптеуіндегі жарықтың жоғалуын ескеретін коэффициент
τ_3 – көтергіш конструкциялардағы жарықтың жоғалуын ескеретін коэффициент
τ_4 – күннен қорғайтын құрылғылардағы жарықтың жоғалуын ескеретін коэффициент
τ_5 – қорғаныс торындағы жарықтың жоғалуын ескеретін коэффициент.

Жарық ауданы $S_0 = 5{,}04$ м2 тең. Еден ауданы $S_{\text{п}} = 70$ м2 құрайды. Қор коэффициенті 1,2 тең. Қауіпсіздік коэффициенті - 1,2. Жарық сипаттамасы бөлме мен терезе өлшемінің қатынасына тең, $\eta 0 = 20$. Қараңғылау коэффициенті $K3\text{d} = 1{,}25$. Бөлме бетінен шағылысқан және ғимаратқа іргелес жатқан төсеніш қабатының арқасында бүйірлік жарықтандыру кезінде ТЖК көтерілуін ескеретін коэффициент $r_1 = 2$. Стеклопакеттері бар терезелер үшін жарық өткізу коэффициенті τ_2=0,75. Стеклопакеттері бар терезелер болғандықтан τ_2=0,75. $\tau_3 = 1$ бүйір жарық кезінде. Күн қорғанысы ретінде сыртқа реттелетін жалюздер қолданылады, сондықтан $\tau_4 = 1$.

$$\tau_0 = 0{,}85 * 0{,}75 * 1 * 1 * 0{,}8 = 0{,}51$$

2 формуласына мәндерді қойып, аламыз:

$$S_0 = \frac{0{,}78 * 1{,}2 * 20 * 1{,}25 * 5{,}04}{0{,}51 * 2 * 100} = 14{,}33 \text{ м}_2$$

Қорытынды: Есептеу есебінен алынған деректер бойынша бір терезе алаңы кемінде 14,33 м2 болуы тиіс. Администратор бөлмесінде екі терезе бар, әрқайсысының ауданы 2,7 м2 тең.

4.2.2 Өрт қауіпсіздігінің есебі

Есеп әдістемелік нұсқауларымен орындалды [6]. ҚНжЕ 2.04-05-2002 [7] стандарты бойынша, өрттің даму қауіптілік дәрежесіне, жанғыш материалдардың функционалдық мақсатына және өрт жүктемесіне байланысты біздің бөлмеміз 1-санаттағы топқа жатады.

Өрт шығудың себебі:

- ақаулы ажыратқыштар мен розеткалардың тұтануы;
- Сұйық тиюден;
- жабдық элементтерін тұтануы;
- жабдық тазалығын сақтамау;
- жабдықтың пайдалану шарттарын сақтамау;
- персоналдың дұрыс жұмыс істемеуі.

Өрт болған жағдайда тек бөлме зардап шектейді, сонымен қатар қымбат құрал-жабдықтар да зақымданады, бұл адам құрбандарына әкеледі. Сондықтан өрттерді анықтау және жою үшін шараларды қолданамыз. Оттың қайнар көздері: техникалық қызмет көрсету үшін пайдаланылатын құрылғылар, компьютерлердің электр тізбегі, кондиционерлер, электр қондырғылары болады, оларда қызып кететін элементтері бар болғандықтан, әртүрлі бұзушылықтар нәтижесінде пайда болады және тағы басқалары.

100 м^2-ге бір өрт сөндіргішті келетінің ескере отырып, ОУ-5 отқа төзімді сөндіргіштер үшін сақтау бөлмелерінің өрт қауіпсіздігінің талаптарына сәйкес болады. Бөлменің жалпы ауданы 70 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 мына формуламен анықталады:

$$md = k \cdot gn \cdot V$$

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

gn=0,04 көмірқышқыл-хладон құрамының нормативтік массалық

концентрациясы.

V – бөлме көлемі:

$$V = A \cdot \text{B} \cdot \text{H}$$

Мұнда, A = 7м – бөлменің ұзындығы;
B = 10м — бөлменің ені;
H = 3м — бөлменің биіктігі.

Сонда:

$$V = 7 \cdot 10 \cdot 3 = 210 \text{ м}^3$$

Демек:

$$\text{md} = 1{,}2 \cdot 0{,}04 \cdot 210 = 10{,}08 \text{ кг.}$$

х баллондарының есептік саны 12 литрлік 10,08 кг көмірқышқыл-хладон құрамының сыйымдылығы есебінен анықталады.

Магистральдық құбырдың ішкі диаметрі di(мм) мына формула бойынша анықталады:

$$di = 12\,32 = 17 \text{ мм.}$$

12 магистральдық құбырдың эквивалентті ұзындығы мына формула бойынша анықталады:

$$12 = k1 \cdot 1$$

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:

$$t = \frac{md}{V \cdot Q}$$

Сонда,

$$t = \frac{10.08}{210 \cdot 1{,}4} = 0{,}0343 \text{ мин.}$$

Көмірқышқыл-хладон құрамының негізгі қорының массасы келесі формула бойынша анықталады:

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

Мұндағы, к2 = 0,2 - баллондар мен құбырлардағы көмірқышқыл-хладон

құрамының қалдығын ескеретін коэффициент.

Сонда:

$$M = 1{,}1 \cdot 10{,}08 \cdot (1 + 0{,}2 \cdot 1{,}2) = 13{,}7 \text{ кг.}$$

Осылайша, алынған нәтижелерден автоматты өрт сөндіру жүйесінің қалыпты жұмыс істеуін қамтамасыз ету үшін сыйымдылығы 12 литр көмірқышқыл-хладон құрамының 1 баллоны қажет, қоспаның салмағы 10,08 кг. ГОСТ 12,4.009-83 [8] стандартына сәйкес автоматты газды сөндіру қондырғыларында 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

Дипломдық жұмыстың осы бөлігінде біз университетке РББЖ жүйесін орнатқаннан кейін туындайтын тәуекелдерді бағалаймыз.

ISO 27005 стандарты, ақпараттық тәуекел тұжырымдамасын: активтерге, қауіп-қатерлерге, осалдықтарға және залалдарға бөледі. ISO 27005 стандартына сәйкес: Ақпараттық қауіпсіздік тәуекелі - бұл ұйымға залал келтірудің нақты қауіп-қатері ретінде актив немесе активтер тобының осалдығын пайдалану мүмкіндігі [11]. Іс жүзінде, әрбір тәуекел қандай да бір түрдегі залал әкеледі. Залал мәнін анықтау үшін тәуекел қауіп-қатері ұғымы енгізілді. Тәуекелдерді есептеу үшін екі параметр бойынша тәуекелді бағалау әдістемесі қолданылды.

РББЖ талдауы: атқарушы құжаттарды зерделеу, объектіні тексеру (егер ол болмаса) және бағдарламалауды тексеру негізінде жүзеге асырылады. Тексеру бірден екі бағытта жүзеге асырылады: инженерлік-техникалық және ұйымдастырушылық-өкімдік қорғау шаралары.

РББЖ құрамына: басқарылатын бөгет құрылғылары, белгілерді идентификациялауға арналған енгізу құрылғылары, контроллерлер мен жүйенің бағдарламасы кіреді. Бейнебақылау және уақытты бақылау жүйелері де кіреді (орнатылған жағдайда). Оларды жиі тексеру керек, бірақ көбінесе бұл жекелеген оқиғалардың бөлігі ретінде жүреді [12].

5.1.1 Активтер

Ақпараттық қауіпсіздік тәуекелін талдау процесі активтерді анықтаудан басталады. Себебі, ол адам үшін немесе ұйым үшін маңызды, сондықтан жақсы қорғауды қажет етеді. Ұйымдастырушылық құндылықтан басқа, активтер заңды міндеттемелерді орындалуына да көмектесе алады.

Ақпараттық қауіпсіздік жүйесінде активтер осы түрлерде болады:

а) аппараттық, бағдарламалық және коммуникациялық компоненттер;

б) олардың арасындағы коммуникациялық байланыстар;

с) жүйенің жұмысын басқаратын, оны өндіретін және / немесе тұтынатын немесе оған енгізілетін деректер;

d) жүйе қолданылатын физикалық және ұйымдастырушылық инфрақұрылым;

е) жүйемен өзара әрекеттесетін және оның жұмысына әсер ете алатын адам агенттері (мысалы, пайдаланушылар, администраторлар және тағы басқалары).

Активтер 5.1-кестеде көрсетілген, ал олардың мазмұны былайша көрінеді:

– Сервер - университет туралы ақпаратты енгізуге жауапты актив;

– LAN – РББЖ жүйесінің жабдықтарын жалғау үшін;

– ПО "Castle" - студенттер, оқытушылар жәнеде аудиториялар туралы мәліметтерді ДБ-ға енгізу үшін;

– РББЖ-ның барлық жабдықтары - жүйені толық қосу үшін қажет;

– "Castle" бағдарламасын орнату үшін Windows 10 Pro операциялық жүйесі.

Кесте 5.1 – Активтер тізбесі

Активтің №	Активтің атауы	Саны	Актив коды
1	Сервер - университет туралы ақпаратты енгізуге жауапты актив	1	ser
2	LAN – РББЖ жүйесінің жабдықтарын жалғау үшін	1	lan
3	ПО "Castle" - студенттер, оқытушылар жәнеде аудиториялар туралы мәліметтерді ДБ-ға енгізу үшін;	1	dba
4	РББЖ-ның барлық жабдықтары - жүйені толық қосу үшін қажет	480	oser
5	"Castle" бағдарламасын орнату үшін Windows 10 Pro операциялық жүйесі	1	win

5.2 Есептеу бөлімі

5.2.1 Екі параметр бойынша тәуекелдерді бағалау

Дипломдық жоба үшін екі параметр бойынша тәуекелдерді бағалау әдісі таңдалды. Екі параметр бойынша тәуекелді бағалау әдісі өзіне:

– қауіптің туындау ықтималдығын бағалау;

– ықтимал залалды бағалау.

Осы әдістеме бойынша тәуекел: пайда болу ықтималдығын, залалды бағалауға көбейту кезінде анықталады.

Бұл әдіс бірнеше кезеңнен тұрады. Яғни, біріншіден, біз тәуекелдердің бастапқы есебін жасауымыз керек, әрі қарай қолайсыз тәуекелдерге арналған шараларды анықтау керек, кейін қайтадан есептейміз. Тәуекелдердің бастапқы есебі, қауіптің туындау ықтималдығын және ықтимал залалды анықтау үшін қажет. Ол үшін, біз 5.2 кестені пайдалануымыз керек. Онда есептеу үшін қауіптің туындау ықтималдығының мәні және оның уақытқа арақатынасы сипатталған.

Кесте 5.2 – Қауіптің туындау ықтималдығының мәні

Қауіптердің туындау ықтималдығының шкаласы	
Ықтималдылық деңгейі	Қауіптің туындау ықтималдығы
0 – өте төмен	Шамамен 2-3 рет 7 жылда
1 - төмен	Шамамен 5 жылда бірнеше рет немесе одан сирек
2 - орташа	Шамамен жылына бірнеше рет
3 - жоғары	Айына шамамен 1 рет
4 – өте жоғары	Шамамен айына бірнеше рет

Залалды анықтау үшін 5.3-кестені пайдалану қажет. Онда есептеу үшін залалдың мәні және оның ақшалай эквиваленттегі арақатынасы сипатталған.

Кесте 5.3 – Залалдың мәні және оның ақшалай эквиваленттегі арақатынасы

Залал көлемінің шкаласы	
Деңгейі	Мәні
0 - өте төмен	құны 5 000 теңгеге дейін
1 - төмен	құны 9 000 теңгеге дейін
2 - орташа	құны 13 000 теңгеге дейін
3 - жоғары	құны 20 000 теңгеге дейін
4 - өте жоғары	құны 50 000 теңгеге дейін

Тәуекелдерді бағалаудың нәтижелері (Кесте 5.4):

№	Қауіп-қатерлер	Осалдықтар	Тәуекелдің ең жоғары деңгейі	Тәуекелді өңдеу жөніндегі шаралар	Тәуекелдің қалдық деңгейі
1. Сервер - университет туралы ақпаратты енгізуге жауапты актив;					
1.1	Серверге басып кіру немесе бұзу арқылы қол жеткізу	Қауіпсіздік осалдығын хабарлау үшін рәсімдердің жетіспеушілігі	6	Рұқсатты шектеу, көпфакторлы аутентификация	3
1.2	Жабдықты өшіруге бағытталған вирустық немесе хакерлік шабуылдар	Конфигурацияның өзгеруінің тиімді басқарудағы кемшіліктері	6	Резервтік көшірме	3
1.3	Серверді басқару үшін рұқсатсыз кіру	Бақылауды үнемі тексерудің жетіспеуі	6	Рұқсатты шектеу, көпфакторлы аутентификация	3
2. LAN – РББЖ жүйесінің жабдықтарын жалғау үшін;					
2.1	Әдейі буферді толтыру	Қорғау параметрі дұрыс емес орнатылған	1	Керек емес	1
2.2	Хакерлік ұстау бағдарламалары арқылы шабуыл жасау	Қорғалмаған және сезімтал трафик	1	Керек емес	1
2.3	Жүйенің бағдарламасына қол жеткізу	Жіберуші мен алушының идентификация және аутентификацияның кемшіліктері	2	Керек емес	2
3. ПО "Castle" - студенттер, оқытушылар және де аудиториялар туралы мәліметтерді ДБ-ға енгізу үшін;					
3.1	Деректер базасына рұқсаты жоқ адамдардың қолжетуі	Қауіпсіздік осалдығын хабарлау үшін рәсімдердің жетіспеушілігі	6	Рұқсатты шектеу, парольмен қорғау	3
3.2	Хакерлік атаканың көмегімен	Қорғалмаған сақтау	6	Деректерді шифрлау	3

	ұрлық жасау				
3.3	Деректерді өзгерту немесе бүлдіру	Қолжетімділікті шектеудің болмауы немесе дұрыс болмауы	6	Рұқсатты шектеу, парольмен қорғау	3
4. РББЖ-ның барлық жабдықтары - жүйені толық қосу үшін қажет;					
4.1	Жабдықтың жұмысын істен шығару	Өзгерістер енгізуді бақылау рәсімдерінің кемшіліктері	6	Резервтік көшірме жасау жүйелері, Құлыптар, Сигнализация	3
4.2	Жабдық арасындағы барлық ақпараттық процестердің жұмыс істеу қабілеттілігінің бұзу	Сервистік қызмет көрсету келісімі бұзылған немесе жеткіліксіз	6	Резервтік көшірме жасау жүйелері, Құлыптар, Сигнализация	3
4.3	Процестер мен жұмыс режимдерін өзгерту және конфигурацияны қалпына келтіру	Қорғалмаған жабдық	6	Құлыптар, Сигнализация	3
5. "Castle" бағдарламасын орнату үшін Windows 10 Pro операциялық жүйесі.					
5.1	ОЖ процестері мен жұмыс режимдерін өзгерту	Обновление мен антивирустық қорғаудың болмауы	1	Керек емес	1
5.2	Компьютердегі ақпараттық процестерді тоқтату	Қате конфигурация, резервтік көшірме жоқ	2	Керек емес	2
5.3	ОЖ процестерінің жұмысын бұрмалау	Рұқсат құқықтарының дұрыс бөлінбеуі	1	Керек емес	1

5.2.2 CORAS методологиясын қолдана отырып, ақпараттық қауіпсіздік тәуекелдерін талдау

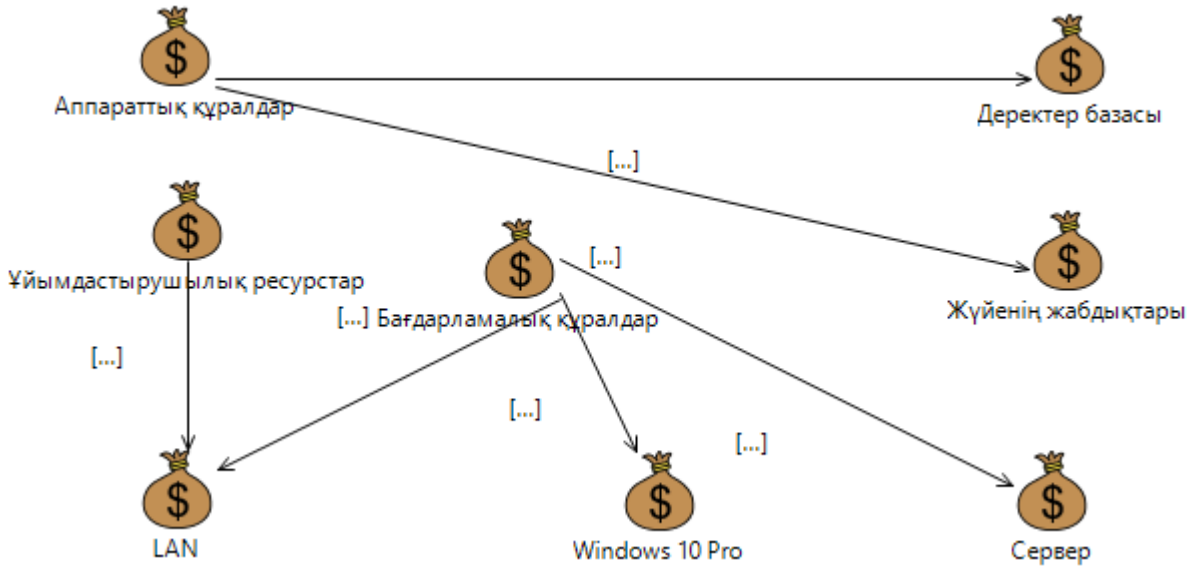
CORAS методологиясы [9] Information Society Technologies бағдарламасының аясында жасалды. Оның мәні - Event-Tree-Analysis, Марков тізбегі, HazOp және FMECA сияқты тәуекел талдауларын бейімдеу, нақтылау және біріктіру болып келеді [10].

CORAS UML технологиясын қолданады және австралиялық / жаңазеландиялық AS / NZS 4360:1999 Risk Management және ISO / IEC 17799-1: 2000 Code of Practice for Information Security Management стандарттарына негізделген. Бұл стандартта ISO / IEC TR 13335-1: 2001 Guidelines for the Management of IT Security және IEC 61508:2000 Functional Safety of Electrical/Electronic/Programmable Safety Related рекомендациялары ескерілген.

CORAS-қа сәйкес ақпараттық жүйелер тек қолданылатын технологиялар тұрғысынан ғана емес, сонымен қатар, бірнеше жағынан қарастырылады, атап айтқанда, адам факторы да ескерілетін күрделі кешен ретінде. Бұл методологияның ережелері Windows және Java-бағдарламаларының түрінде жүзеге асырылды.

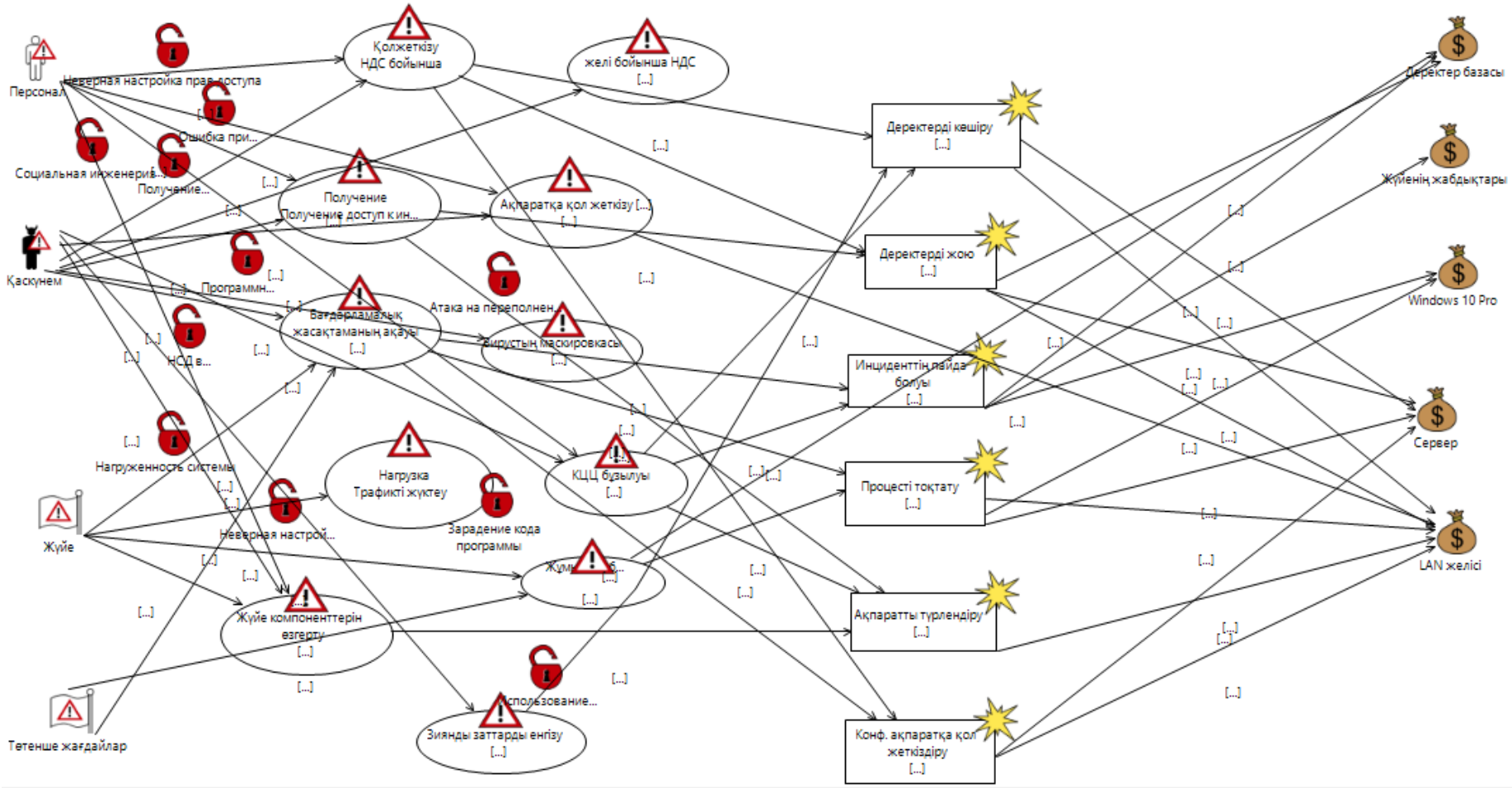
Алдымен, біз бағдарламаның көмегімен активтер моделін жасауымыз керек.

5.1-суретте активтер моделі көрсетілген. Активтер үш санаттарға бөлінген. Олар: Аппараттық құралдар, оған: Деректер базасы және Жүйенің жабдықтары кіреді, Ұйымдастырушылық ресурстар, оған: LAN кіреді жәнеде Бағдарламалық құралдар, оған: Сервер, LAN және Windows 10 Pro кіреді.



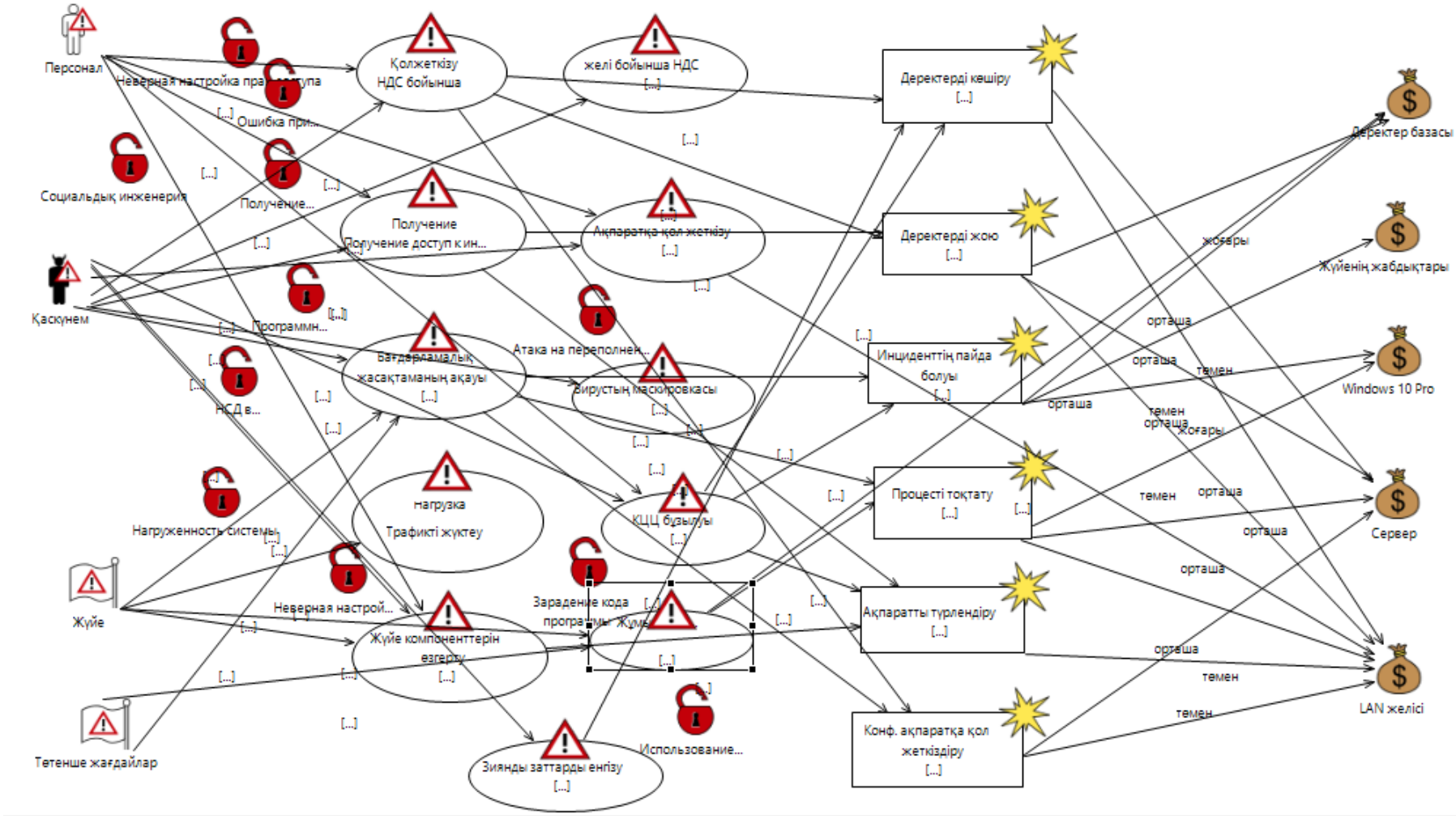
5.1 сурет – Активтер

Алынған активтер моделіндегі кестені қолдана отырып, жағымсыз оқиғалардың сценарийінің ықтималдығын енгіземіз. Нәтижесінде, біз 5.2 суретте келтірілген қауіп моделін аламыз. Яғни, басында бізде қауіп-қатердің қайнар көздері (қызметкерлер, шабуылдаушы, жүйе және күтпеген жағдайлар) орналысқан, олар осалдықтардың көмегімен белгілі бір активке, қандай да бір салдар туғызатын қауіпті туғыздырады. Мысалы, вирустық бағдарламалық жасақтаманың көмегімен шабуылшы ақпаратқа қол жеткізіп алады. Ол серверде деректердің жойылуына әкеледі.



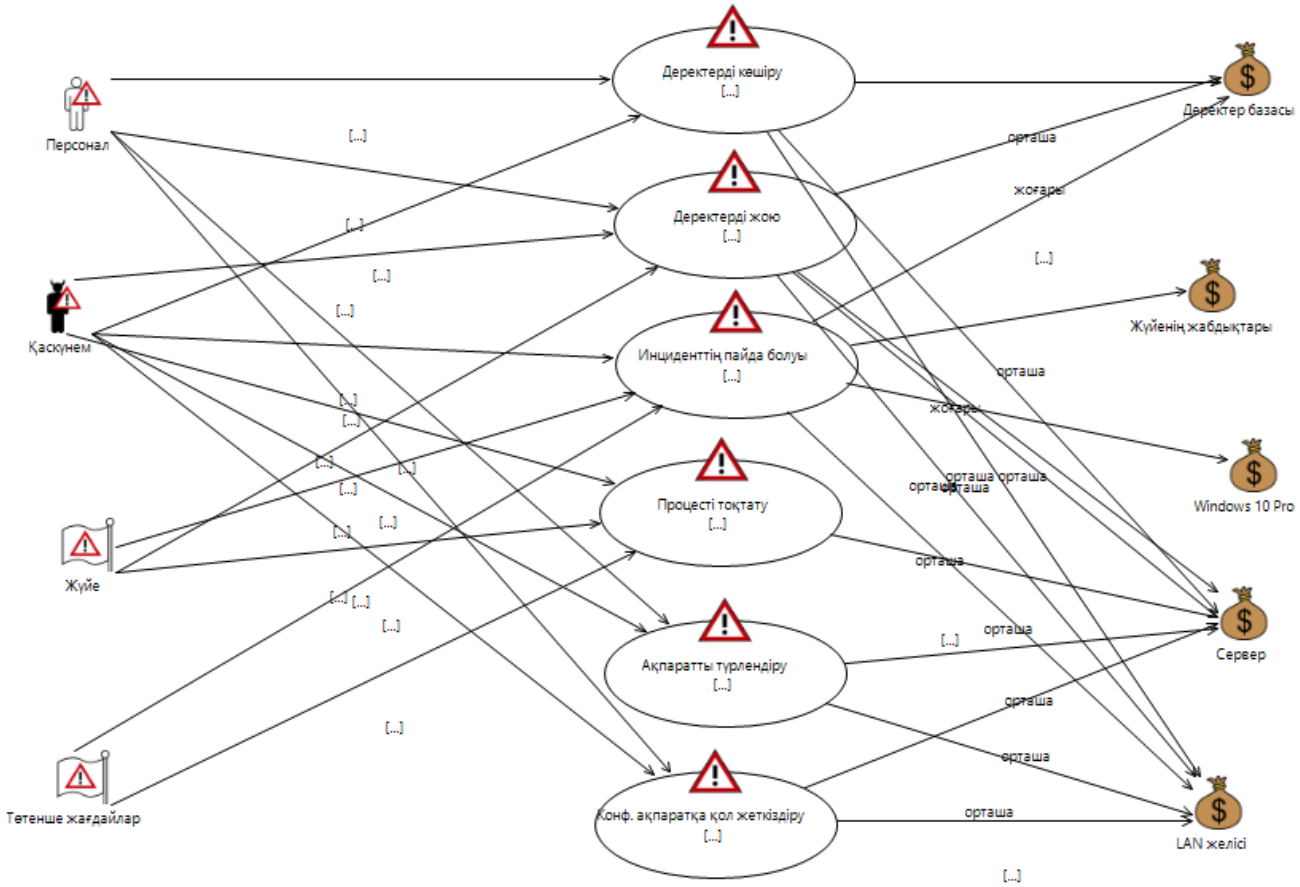
5.2 сурет – Қауіп моделі

Әрі қарай, біз инциденттың болу ықтималдығы ескерілген қауіп-қатер диаграммасын жасаймыз. Мұны істеу үшін, біз әрбір актив үшін инцидент ықтималдығын жоғарыдан төменге дейінгі аралығында жазып тастауымыз керек.



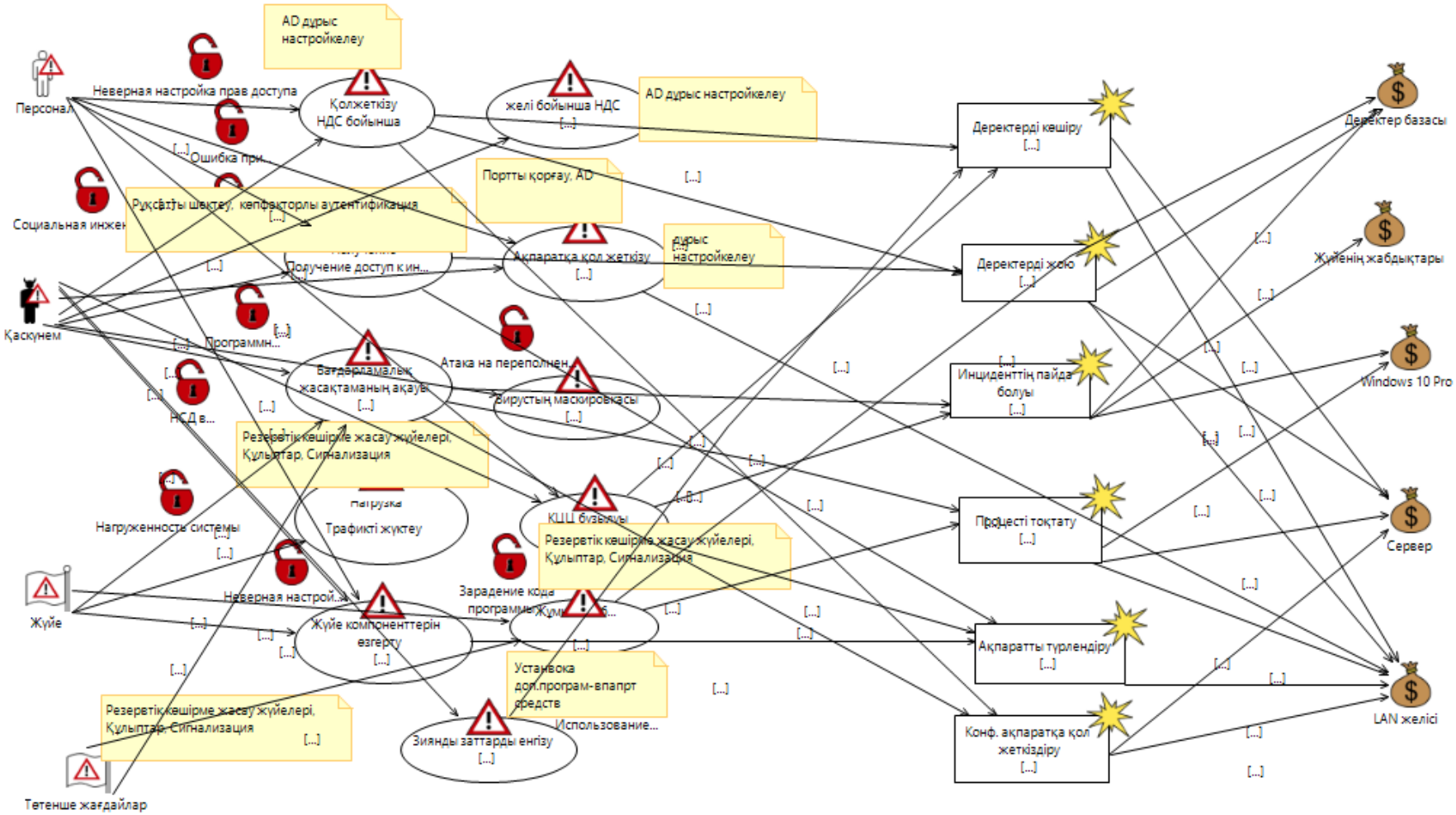
5.3 сурет – Қауіп-қатер диаграммасы

Енді әрбір тәуекел бойынша, әр актив үшін осы тәуекел жүзеге асырылған жағдайдағы салдарды анықтаймыз.



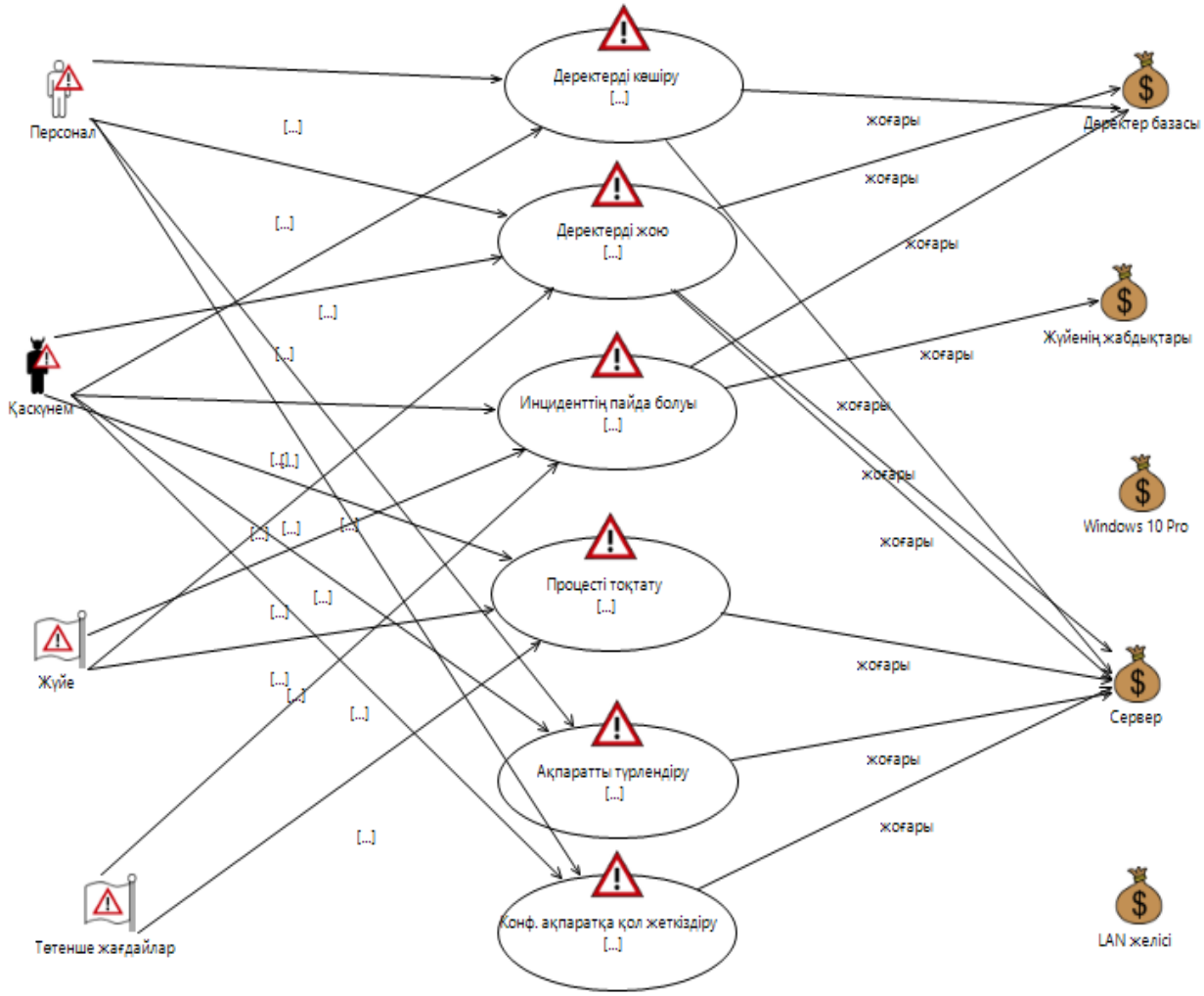
5.4 сурет – Қауіпті жүзеге асыру салдарының сипаттамасы бар тәуекелдер диаграммасы

Кейін, біздің активтерімізге тәуекелдерді азайту үшін шараларді қолданамыз. Басқаша айтқанда, осалдықтар мен қауіп-қатерлерді іске асыру тәсілдері арасында тәуекелдерді азайту үшін қорғау шаралары қосылды.



5.5 сурет – Қорғау шараларын қосқаннан кейінгі қауіп-қатер диаграммасы

5.6 суретте қолайсыз тәуекелдердің диаграммасы көрсетілген. Диаграммада тек жоғары әсер ету дәрежесі бар тәуекелдер ғана көрсетілген.



5.6 сурет – Қолайсыз тәуекелдердің диаграммасы

Қорытынды жасай отырып, дипломдық жобаның осы бөлімінде біз ақпараттық жүйенің осалдығын анықтау, ал кейін оларды жою мақсатында тәуекелдердің есебін жүргіздік. Тәуекелдерді есептеу екі параметр бойынша тәуекелдерді бағалау әдісі негізінде болды. Мұнда, есептеулер нәтижелері ақпараттық жүйенің ағымдағы жағдайын көрнекі көруге мүмкіндік береді. Содан соң, қорғаудағы кемшіліктерді ескере отырып, параметрдің көмегімен есептелген тәуекелдерді азайтуға бағытталған қорғау шараларын орындауға ұсынылды. Кейін, тәуекелдерге сол әдіс бойынша қайта есептеу жүргізілді. Қайта есептеу нәтижесінде, біз, ақпараттық жүйесіне енгізуге ұсынылған қорғау шараларының арқасында, тәуекелдер қолайлы деңгейге дейін төмендегенің көре аламыз. Яғни, 6-дан 3-ке дейін. Осының арқасында, тәуекелдерді есептеудің осы әдісі шынымен пайдалы деген қорытынды жасауға болады, өйткені шығындарды болдырмауға мүмкіндік береді. Есептік бөліктің екінші бөлігінде CORAS-тің көмегімен тәуекелдерге талдау жүргізілді. Онда UML-диаграммалары салынған суреттер көрсетілген. Олар:

активтердің идентификациясы, қауіптер мен осалдықтардың моделі, сондай-ақ шаралар енгізілгеннен кейінгі модель.

Қорытынды

Бұл дипломдық жұмыста рұқсатты бақылау және басқару жүйесін университетке қойған жағдайдағы мәселені зерттедім. Рұқсатты бақылау және басқару жүйесі енді дамып келе жатқан сала болып келеді жәнеде қауіпсіздікті ғана қамтамасыз етпей, дамып, басқа да салаларды жаулап алуға потенциалы бар деп ойлаймын. Осыған көзімді жеткізу үшін, біріншіден, мен толық РББЖ жүйесінің тарихын мен жұмыс істеу принципін зерттедім. Кейін, практикалық жұмыста оның орнатуын мен программалық жұмысын қарастырдым. Осы практикалық жұмыстың арқасында университетке орнатылған жүйе оның қауіпсіздігін ғана жақсартпай, уақыт тиімділігін арттыра түсетінің байқауға болады. Яғни:

1) 100 есікке 100 кілт арнағанша, бір-ақ карта жеткілікті болады. Осының арқасында кілтті іздеу қажет болмайды. Ал егер, оқытушы карточканы жоғалтқан кезде, оған уақытша карточка беріледі (Егер алдын-ала ескерткен жағдайда) немесе старостаның карточкасымен рұқсат сұрайды.

2) Коридорда кабинетке кире алмай отқан, жолды жауып тұрған студенттер болмайды. Себебі, оқытушының рұқсатымен старостаға есікті ашуға рұқсат беріледі немесе оқытушының өзі, кілт іздемей, лезде келіп, кабинетті ашады.

3) Студенттердің бар-жоғын тексермей, бірден сабаққа көшу. Себебі, есікте орнатылған датчиктін арқасында кім өткенінің бәрі оқиғаға жазылады. Сосын жұмыстың соңында оқытушыға жіберіледі.

4) Оқытушыға, оқу кестесі бойынша, тек сабағы бар болатын есіктерге ғана рұқсат алады. Ол қажет емес аудиторияға кіріп кетуден немесе шатасып кіріп кетуден сақтайды

5) Әр оқытушы тек өзінің кафедрасына кіре алады.

6) Универ қонақтарына бөлек «Гость» деген карточка арналады.

7) Студенттің кітапханаларға кіруы және одан кітап алуы оның базасында жазылады.

8) Университеттің ақпараттық және материалдық қауіпсіздігі артады.

Оның үстіне РББЖ-ны университетке орнатқанда, айтылып өткен артықшылықтарға тағы университеттің басқа университеттерге қарағанда статусы арта түсуі мүмкін. Себебі, басқаларға қарағанда ерекше және байыпты болып, келген қонақтар мен жаңа студедеттерді таң қалдырады.

Қорытындылай келсек, алдыма қойылған міндеттерді орындадым. Жәнеде рұқсатты бақылау және басқару жүйесін университеттерге орнату өте актуалді жәнеде бір-қатар ерекшеліктерге ие болады деп айтуға болады.

Әдебиеттер тізімі

1. СаНПИН 2.2.4.548-96/03 - «Гигиенические требования к микроклимату производственных помещений» - Ресей Госкомсанэпиднадзоры, 1996.
2. СанПиН 2.2.2/2.4.1340-03 «Гигиенические требования к персональным электронно-вычислительным машинам и организации работы» - Ресей Федерациясы, 2003
3. ҚР СНиП 2.04.-05.2002 (Табиғи және жасанды жарық. Құрылыс, қала құрылысы және архитектура саласындағы мемлекеттік нормативтері) - Астана, 2003.
4. Системы контроля и управления доступом (СКУД). Особые требования пожарной безопасности при эксплуатации эвакуационных выходов. // gpnrostov.ru URL: https://gpnrostov.ru/01pusk/?p=5679
5. Жандаулетова, Ф. Р. Охрана труда : учебник для вузов / Ф.Р. Жандаулетова, Т.Е. Хакимжанов, Т.С. Санатова; МОН РК, НАО АУЭС. - Алматы : АУЭС, 2019. - 399 с.
6. Абдимуратов Ж.С., Мананбаева С.Е. Безопасность жизнедеятельности. Методические указания к выполнению раздела «Расчет производственного освещения» Алматы: АИЭС, 2009. — 20с.
7. 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.
8. ҚР ҚНжЕ 2.02-05-2009 – «Ғимараттар мен имараттардың өрт қауіпсіздігі» - Сәулет, қала құрылысы және құрылыс саласындағы мемлекеттік нормативтер, Астана, 2010.
9. Методологии управления ИТ-рисками. // www.osp.ru URL: https://www.osp.ru/os/2006/08/3584582/
10. 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***)
11. Понятие риска // анализ-риска.рф URL:http://анализ-риска.рф/content/ponyatie-riska
12. Анализ СКУД: как проверить систему контроля и управления доступом на эффективность // www.terra-security.ru URL: https://www.terra-security.ru/blog/analiz-skud-kak-proverit-sistemu-kontrolya-i-upravleniya-dostupom-na-effektivnost
13. ҚР СТ 1699-2007 – «Қол жеткізуді бақылау және басқару жүйесі» - Астана, 2009
14. История развития технологий, повышающих надежность использования идентификаторов в СКУД. // www.techportal.ru URL: http://www.techportal.ru/189719

15. Карты контроля доступа. // www.techportal.ru URL: http://www.techportal.ru/glossary/karti-kontrolya-dostupa.html

16. Система контроля и управления доступом. // ru.wikipedia.org URL:https://ru.wikipedia.org/wiki/Система_контроля_и_управления_доступом

17. Тихонов В А., Райх В. В. Информационная безопасность: концептуальные, правовые, организационные и технические аспекты: Уч. пособие. М.: Гелиос АРВ, 2006.

18. 6. Абалмазов Э. И. Энциклопедия безопасности. Справочник каталог, 1997. Тарасов Ю Контрольно-пропускной режим на предприятии. Защита информации // Конфидент, 2002. № 1. С. 55-61.

19. 8. Сабынин В. Н. Организация пропускного режима первый шаг к обеспечению безопасности и конфиденциальности информации // Информост - радиоэлектроники и телекоммуникации, 2001. № 3 (16).

20. 9. Татарченко И. В., Соловьев Д. С. Концепция интеграции унифицированных систем безопасности // Системы безопасности. № 1 (73). С. 86-89.

21. Мащенов Р. Г. Системы охранной сигнализации: основы теории и принципы построения: учебное пособие. М.: Горячая линия - Телеком, 2004

22. Горлицин И. Контроль и управление доступом - просто и надежно КТЦ «Охранные системы», 2002.

23. Абрамов А. М., Никулин О. Ю, Петрушин А. И. Системы управления доступом. М.: «Оберег-РБ», 1998.

24. Предтеченский В И , Рыжухин Д. В , Сергеев М. С. Анализ возможности использования кодонаборных устройств (клавиатур) в системах контроля и управления доступом высокого уровня безопасности. М.: МГИФИ, 2005.

25. Филипп Х. Уокер Электронные системы охраны. Наилучшие способы предотвращения преступлений / Пер. с англ. М.: «За и против», 1991

26. Флорен М. В. Организация управления доступом // Защита информации «Конфидент», 1995. № 5. С. 87-93.

27. Крахмалев А. К. Средства и системы контроля и управления доступом. Учебное пособие. М.: НИЦ «Охрана» ГУВО МВД России. 2003.

28. Гинце А. А. Особенности СКУД систем доступа крупных распределенных объектов. ААМ Системз, 2005.

29. Кондратьев Д. Р. Биометрические устройства для СКУД // Системы безопасности, 2004. № 1.

30. Тихонов В. А., Ворона В. А. Системы контроля и управления доступом, Москва, Горячая линия – Телеком, 2010

31. Castle EP4, PRO4. Сетевые контроллеры. Инструкция по эксплуатации, ООО “Агрегатор”, 2016

32. Castle. Система контроля и управления доступом. Руководство администратора, ООО «Агрегатор», 2020

33. Castle. Система контроля и управления доступом. Руководство пользователя, ООО «Агрегатор», 2020