**Семинар 2. Ақылды үй шлюзі бар антропологиялық деректерді қашықтан бейнебақылауы мен тануы бар электрондық құлыптың принципті схемасы. Саусақ ізінің кодын танитын электрондық құлыптың прототипін жобалау және сынау.**

I. Электронды құлып және оның түрлері.

Электронды құлып - бұл рұқсат етілмеген адамдардың бөлмеге кіруіне жол бермеуге немесе керісінше бөлмеден шығуды шектеуге арналған электрондық құрылғы. Адамдар бөлмесіне кіру туралы шешім әр түрлі сенсорлардың сигналдары негізінде қабылданады: магниттік карта оқу құрылғылары, штрих -кодтар, байланыс жады сенсорлары, биометриялық датчиктер, теру тақтасы, комбинаторлық флуоресцентті молекулалық датчиктер, қашықтан басқару пульті және т.б. электронды басқару жүйесіне қатынау, кейде одан бөлінбейді. Жетектер ретінде электромеханикалық және электромагниттік құлыптау құрылғылары қолданылады.

Электронды құлыптардың бірнеше түрлері бар. Ашу және бұғаттау жолымен олар бөлінеді:

1. Электромагниттік құлып;

2. Электромеханикалық құлып.

Электронды құлыптар кілт түріне қарай ажыратылады:

1. Физикалық кілті бар құлып (мысалы, таблеткаға арналған кілт);

2. Ақылды құлып (смартфонның кілті немесе радио пернелері);

3. Кодты құлыптау;

4. Биометриялық құлып.

Электронды (ең алдымен электромеханикалық) құлыптардың маңызды ерекшелігі - оларды қашықтан басқаруға болады. Бұл функция ақылды үй технологиялары таралған кезде жиі қолданылады. Мұндай құлыптар әдетте ақылды үй жүйесінің жалпы бөлігі болып табылады, ол әдетте иесінің смартфонына байланған, қажет болған жағдайда құлыпты ашу және жабу арқылы смартфоннан құлыпты қашықтан басқаруға мүмкіндік береді.

II. Қол жеткізуді басқару және басқару жүйесі

Қатынауды басқару жүйесі, ACS (Физикалық қатынауды басқару жүйесі, PACS) - «өткізу пункттері» арқылы белгілі бір аймаққа объектілердің (адамдардың, көліктердің) кіруі мен шығуын шектеуге және тіркеуге бағытталған бағдарламалық және аппараттық техникалық бақылау мен бақылаудың жиынтығы. «: Есіктер, қақпалар, бақылау бекеті.

Негізгі міндет - берілген аумаққа кіруді бақылау (кімге, қай уақытта және қандай аумаққа рұқсат етілуі керек), оның ішінде: берілген аумаққа кіруді шектеу және берілген аумаққа кіруге рұқсаты бар адамды анықтау.

Қосымша тапсырмалар:

• жұмыс уақытын есепке алу;

• қызметкерлер / келушілер базасын қолдау;

• қауіпсіздік жүйесімен интеграция, мысалы:

• жүйелік оқиғалар мұрағаттарын біріктіру үшін бейнебақылау жүйесімен

• бейнебақылау жүйесіне жазуды бастау қажеттілігі туралы хабарламаларды жіберу, жазылған күдікті оқиғаның салдарын жазу үшін камераны бұру;

• ұрлық дабыл жүйесімен (SOS), мысалы, қарулы үй -жайларға кіруді шектеу немесе үй -жайларды автоматты түрде қарусыздандыру және қаруландыру.

• өрт детекторларының күйі, эвакуациялық шығулардың автоматты түрде оқшаулануы және өрт дабылы болған кезде өртке қарсы есіктердің жабылуы туралы ақпарат алуға арналған өрт сигнализациясының (СПС) көмегімен.

Әсіресе маңызды объектілерде АБЖ құрылғыларының желісі физикалық түрде басқа ақпараттық желілерге қосылмаған.

Желілік жүйеде барлық контроллерлер компьютерге қосылған, ол ірі кәсіпорындар үшін көптеген артықшылықтар береді, бірақ «бір есікті» АБЖ үшін мүлде қажет емес. Желілік жүйелер үлкен объектілерге ыңғайлы (кеңселер, өндіріс орындары), өйткені автономды жүйелер орнатылған ондаған есіктерді басқару өте қиынға соғады. Желілік жүйелер келесі жағдайларда қажет:

• егер әр түрлі артықшылықтары бар қызметкерлер тобын кәсіпорынның әр түрлі аймақтарына қабылдаудың күрделі алгоритмдерін енгізу қажет болса және оларды тез өзгерте алса;

• егер кіру нүктелерінің үлкен саны немесе қызметкерлердің көптігі үшін бос орындарды (белгілерді) іріктеп алып тастау немесе құру қажет болса (ауысымның жоғары болуы және өтудің жоғалуы);

• егер сізге алдыңғы оқиғалар туралы ақпарат қажет болса (оқиғалар мұрағаты) немесе сізге нақты уақытта қосымша бақылау қажет. Мысалы, желілік жүйеде фотосуретті тексеру функциясы бар: бақылау -өткізу пунктінде, кіруші оқырманға идентификаторды әкелгенде, қызметкер (күзетші, күзетші) монитор экранында адамның суретін көре алады. дерекқорда осы идентификатор тағайындалады және оны басқа адамдарға карталарды беруден сақтандыратын, өтіп бара жатқан адамның сыртқы келбетімен салыстырады;

• егер жұмыс уақытын есепке алуды және еңбек тәртібін бақылауды ұйымдастыру қажет болса;

• егер басқа қауіпсіздік ішкі жүйелерімен өзара әрекеттесуді (интеграциялауды) қамтамасыз ету қажет болса, мысалы, бейнебақылау немесе өрт дабылы).

Желілік жүйеде сіз бір жерден қорғалатын аймақтағы оқиғаларды бақылап қана қоймай, сонымен қатар пайдаланушылардың құқықтарын орталықтан басқара аласыз, мәліметтер қорын жүргізе аласыз. Желілік жүйелер басқару функцияларын әр түрлі қызметкерлер мен кәсіпорын қызметтері арасында бөлу арқылы бірнеше жұмыс орнын ұйымдастыруға мүмкіндік береді.

Желілік қатынауды басқару жүйелерінде радиоарналар деп аталатын сымсыз технологияларды қолдануға болады. Сымсыз желілерді пайдалану көбінесе нақты жағдайлармен анықталады: объектілер арасында сымды байланыс орнату қиын немесе мүмкін емес, кіру нүктесін орнатуға қаржылық шығындарды азайту және т.б. Радиоарналардың көптеген нұсқалары бар, бірақ тек олардың кейбіреулері АБЖ -де қолданылады.

• Блютуз. Сымсыз деректерді беру құрылғысының бұл түрі Ethernet -ке ұқсас. Оның ерекшелігі RS-485 интерфейсін пайдалану кезінде компоненттерді біріктіру үшін параллель байланыс орнатудың қажеті жоқтығында.

• Сымсыз дәлдiк. Бұл радиоарнаның басты артықшылығы - оның ұзақ байланыс диапазоны, бірнеше жүз метрге жетуге қабілетті. Бұл әсіресе алыс қашықтықтағы объектілерді қосу үшін қажет. Сонымен қатар, көше коммуникацияларын жүргізуге уақыт та, қаржылық шығын да азаяды.

• ZigBee. Бастапқыда бұл радиоарнаның ауқымы қауіпсіздік пен өрт дабылы болды. Технологиялар бір орында тұрмайды және белсенді дамуда, сондықтан ZigBee қатынауды басқару жүйелерінде қолданыла алады. Бұл сымсыз технология лицензияланбаған 2,45 ГГц диапазонында жұмыс істейді.

• GSM. Бұл сымсыз байланыс арнасын қолданудың артықшылығы - толық қамту. Қарастырылатын желіде ақпаратты берудің негізгі әдістеріне GPRS, SMS және дауыстық арна жатады.

Соңғы бірнеше жылда мобильді қосымшалар мен құрылғыларды бейнебақылау жүйесіне кірудің бір әдісі ретінде қолданушылардың саны артып келеді. Алайда, қашықтан қатынауды ұйымдастыру бүкіл жүйенің қауіпсіздігіне қауіп төндіреді және желілік жабдықтың күрделі конфигурациясын қажет етеді.

Біздің статистика көрсеткендей, барлық бейнебақылау жүйелерінің 70 -ке жуығы қашықтықтан қарау мүмкіндігіне ие.

Бейнебақылау үшін қашықтан қатынауды құрудың 5 жалпы нұсқасы бар

• Портты қайта бағыттау

• Әмбебап қосылу және ойнату (UPnP)

• Динамикалық DNS

• Бұлтты қызметтер

• Виртуалды жеке желілер (VPN)

Толыққанды қауіпсіздік жүйесін орнату тапсырманы шешу үшін негізсіз қымбатқа түсуі мүмкін жағдайлар жиі кездеседі. Мұндай жағдайларда ең жақсы шешім-кіру нүктесімен жабдықталуы қажет әрбір кіру нүктесінде дербес контроллерді орнату.

ACS қолдану аймағы әр түрлі:

• компания кеңселері, бизнес орталықтары, банктер;

• оқу орындары (мектептер, техникумдар, жоғары оқу орындары);

• өнеркәсіптік кәсіпорындар, ерекше қорғалатын табиғи аумақтар;

• автотұрақтар, автотұрақтар, көлік құралдары өтетін орындар;

• жеке үйлер, тұрғын үй кешендері, коттедждер;

• қонақүйлер, қоғамдық мекемелер (спорт кешендері, мұражайлар, метро және т.б.)