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

ЭжсР кафедрасы

«ҚОРҒАУҒА ЖІБЕРІЛДІ»

Кафедра меңгерушісі т.ғ.к., доцент Жиланбаев Т.Д
(ғылыми дәрежесі, атағы, Т.А.Ж.)

_____ «____» _____201___ж.
(қолы)

ДИПЛОМДЫҚ ЖОБА

Тақырыбы: Қол жеткіншідің биометрилық бақылау және басқару жүйесін әзірлеу

Мамандығы 5В071600 Аспап жасау

Орындаған Орынбасаров Бақытбек Оразалыұлы (Т.А.Ж.) Тобы ПСк-15-1

Ғылыми жетекшісі Доктор PhD., доцент Балбаев Г.К.
(ғылыми дәрежесі, атағы, Т.А.Ж.)

Кеңесшілер:

экономикалық бөлім бойынша:

Аға оқытушы Тулегенова С.К.
(ғылыми дәрежесі, атағы, Т.А.Ж.)

_____ «29» 05 2019 ж.
(қолы)

өміртіршілігі қауіпсіздігі бойынша:

Аға оқытушы Байдакова С.М.
(ғылыми дәрежесі, атағы, Т.А.Ж.)

_____ «30» 05 2019 ж.
(қолы)

есептеу техникасын қолдану бойынша:

Доктор PhD., доцент Балбаев Г.К.
(ғылыми дәрежесі, атағы, Т.А.Ж.)

_____ «31» 05 2019 ж.
(қолы)

_____
(ғылыми дәрежесі, атағы, Т.А.Ж.)

_____ «____» _____201___ж.
(қолы)

Нормобақылаушы: т.ғ.к., доцент Жиланбаев Т.Д.
(ғылыми дәрежесі, атағы, Т.А.Ж.)

_____ «31» 05 2019 ж.
(қолы)

Пікір беруші: т.ғ.к., доцент Илманбекова Тоқтабуби Жұмадиловна
(ғылыми дәрежесі, атағы, Т.А.Ж.)

_____ «____» _____201___ж.
(қолы)

Алматы 2019

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

Ғарыштық техника және телекоммуникация институты

Электроника және робот техникасы кафедрасы

Мамандығы 5В071600 Аспап жасау

Дипломдық жобаны орындауға берілген
ТАПСЫРМА

Студент Орынбасаров Бақытбек Орازامұлы
(Т.А.Ж.)

Жобаның тақырыбы қол жеткізуді биометриялық бақылау және бақылау жүйесін әзірлеу

201___ ж. «__» _____ №_____ университет бұйрығымен бекітілді.

Аяқталған жобаны тапсыру мерзімі «_____»_____201___ж.

Жобаға алғашқы деректер (талап етілетін зерттеу (жоба) нәтижелерінің параметрлері және зерттеу нысанының алғашқы деректері):

1. Arduino платформасы

Диплом жобасындағы әзірленуі тиіс мәселелер тізімі немесе диплом жобасының қысқаша мазмұны:

1. Биометриялық кіруді қарастыру
2. Микроконтроллер таңдау
3. Бағдарламасын құру
4. Бағдарламаға блок-сызба құру
5. Бағдарламаны тестілеу

Графикалық материалдардың (міндетті түрде дайындалатын сызбаларды көрсету) тізімі:

(1. Arduino платформасы)

1. Титулдық бет
2. Өзектілік пен мақсаты
3. Биометриялық кірудің артықшылықтары мен кемшіліктері.
4. Қосылу сызбасы
5. Қажетті жабдықтардың сипаттамалары
6. Өміртіршілік қауіпсіздік бөлімі
7. Экономикалық бөлім.

Негізгі ұсынылатын әдебиеттер:

1) Вороня В.А., Системы контроля и управления доступом – М.: Горячая линия – Телеком, 2013. – 272 с.

2) Старовойтов В.В. Биометрические системы контроля доступа по отпечаткам пальцев. Информатика. 2015, (1): 26-28 с.

3) Биометрические методы защиты информации: учеб.- метод. пособие/ А.М. Прудников, (П.В) Г.А. Рощупкин.- Минск: БГУИР, 2014. - 123 с.

Жоба бойынша жобаның бөлімдеріне қатысты белгіленген кеңесшілер

Бөлімдері	Кеңесшілері	Мерзімі	Қолы
Экономикалық бөлім.	Аға оқытушы Тулегенова С.К.	29.05.19	
Өміртіршілік қауіпсіздік	Аға оқытушы Байдакова С.М.	30.05.19	

Диплом жобасы дайындау
КЕСТЕСІ

Бөлімдердің атауы, әзірленетін мәселелердің тізімі	Ғылыми жетекшіге ұсыну мерзімдері	Ескерту
1. Теориялық бөлім	3.10.2018	
2. Техникалық бөлім	15.10.2018	
3. Бағдарламалық бөлім	14.11.2018	
4. Өміртіршілік қауіпсіздік бөлімі	30.05.2019	
5. Экономикалық бөлімі	29.05.2019	

Тапсырманың берілген уақыты «___» _____ 201___ж.

Кафедра меңгерушісі _____ (Балбаев Б.О.)
(қолы) (Т.А.Ж.)

Жобаның
ғылыми жетекшісі _____ (Балбаев Г.К.)
(қолы) (Т.А.Ж.)

Орындалатын тапсырманы
қабылдаған студент _____ (Орынбасаров Б.О)
(қолы) (Т.А.Ж.)

Аңдатпа

Бұл дипломдық жобаның тақырыбы қол жеткізудің биометриялық бақылау және басқару жүйесін әзірлеу болатын. Ол үшін база ретінде Arduino Uno тақтасын және сонымен қоса саусақ ізі ZFM60 V1.4 сканерін пайдаландым. Оларға қажетті алгоритмді Arduino IDE бағдарламалық ортасында жасалынды. Өмір тіршілік қауіпсіздігі бөлімінде саусақ ізі ZFM60 V1.4 сканерінің адам өміріне зиянсыз екені дәлелденді. Экономикалық бөлімінде, жобаға жұмсалатын шығындар есептелінді.

Аннотация

Тема данного дипломного проекта заключалась в разработке биометрической системы контроля и управления доступом. В качестве базы для этого служит панель Arduino Uno а также сканер отпечатка пальцев ZFM60 V1.4. Алгоритм был разработан в программной среде Arduino IDE. Сканер отпечатка пальцев ZFM60 V1.4 в части безопасности жизнедеятельности был доказан, что он безвреден для жизни человека. В экономической части рассчитаны затраты на проект.

Annotation

The theme of this diploma project was to develop a system of biometric control and access control. As a base for this is the Arduino Uno panel and fingerprint scanner ZFM60 V1.4. The algorithm was developed in the Arduino IDE software environment. Zfm60 V1 fingerprint scanner.4 in terms of life safety, it has been proved that it is harmless to human life. In the economic part of the calculated costs of the project.

Мазмұны

Кіріспе 8
1 Теориялық бөлім 9
1.1 Биометриялық технологиялар 9
1.2 Биометриялық сәйкестендіру негіздері 10
1.3 Аутентификация әдістері 12
1.3.1 Саусақ іздері 14
1.3.2 Бет геометриясы 16
1.3.3 Қол геометриясы 16
1.3.4 Көздің торлы қабығы 17
1.3.5 Көз торы 17
1.3.6 Дауыс және сөйлеу 17
1.3.7 Қолы 18
1.4 Биометриялық параметрлердің артықшылықтары мен кемшіліктері 19
1.4.1 Саусақ ізімен сәйкестендіру 19
1.4.2 Тұлға(лицо) 20
1.4.3 Дауысы 21
1.4.4 Қол 23
1.4.5 Қолы 23
1.4.6 Биометрия ұмтылысы 24
1.5 Биометриялық мифтер және қате көріністер 26
2 Техникалық бөлім 29
2.1 Fritzing бағдарламасы арқылы жобамыздың сұлбасын құру 29
2.2 Arduino микроконтроллерін таңдау 29
2.3 Жобамызға қажетті қосымша бөлшектер 36
2.3.1 Саусақ ізі сканері ZFM60 V1.4 36
2.3.2 Сервожетек SG-90 37
2.3.3 Буззер(динамик) 39
2.3.4 Bluetooth модуль JDY-10 39
2.3.5 Жарық диоды 40
2.3.6 10кОм-дық резистор 41
2.4 Жобамыздың құрылымдық және блок-сұлбасы 43
3 Бағдарламалық бөлім 44
3.1 Жобамызға қолданылатын бағдарлама 44
3.2 Arduino UNO-ға жүктелетін бағдарлама листингі 45
4 Өміртіршілік қауіпсіздік бөлімі 51
4.1 Оптикалық әдіс 51
4.2 Samsung Galaxy S8 және S8+ смартфондары көздің биометриясымен салыстыру 51

4.3 Qualcomm компаниясының ультрадыбыстық саусақ ізі сенсорымен (3D Sonic Sensor) салыстыру 53
5 Экономикалық есептеу бөлімі 57
5.1 Жұмыстың сипаттамасы мен қажеттілігінің негіздемесі 57
5.2 Сканерді арқылы кіруді есептеу мен құрастыруға кететін шығындарды анықтау 58
5.3 Жобаны есептеу мен құрастырудың еңбек сыйымдылығы мен ұзақтығын есептеу 58
5.4 Жобаны есептеу мен құрастыруға кеткен қызметкерлердің төлемақысын есептеу 59
5.5 Әлеуметтік аударым есебі 60
5.6 Материалдарға кеткен шығын көлемін есептеу 62
5.7 Амортизациялық аударымдар 63
5.8 Жұмыстың болжамдалған құнын есептеу 64
5.9 Жұмыстың тиімділігін бағалау 65
Қорытынды 66
Әдебиеттер тізімі 67
А қосымша. Arduino Uno-ның қағидаттық сұлбасы 71

Кіріспе

Қол жетімділікті бақылау және басқару жүйесі - бұл берілген аумақта «өту нүктелері» (есіктер, қақпалар және т.б.) арқылы адамдар мен көліктің кіруін шектеу, тіркеу және бақылау жүйесін ұйымдастыруға арналған арнайы жабдықтар мен бағдарламалық қамтамасыз етудің жиынтығы.

Қол жетімділікті бақылау мен басқарудың биометриялық жүйесі адамдарды олардың физикалық жеке ерекшеліктері бойынша тануға мүмкіндік береді (саусақтардың немесе алақанның іздері, көздің торлы қабығы, дауыс, бет белгілері, қол білезігінің пішіні, ДНҚ және т.б.). Осылайша, жүйенің бақылау және қауіпсіздік сапасы айтарлықтай артады, жүйенің рұқсатсыз ену және алдау тәуекелі төмендейді.

Қазіргі уақытта қолжетімділікті бақылаудың биометриялық жүйелері сатып алушылар өте қажет, бұл өндірушілердің сала мен технологияларды дамытуға, жабдықтардың номенклатурасы мен сипаттамаларын кеңейтуге дайындығына әсер етті. Қазіргі заманғы технологиялар оны іс жүзінде қолданыстағы кіруді бақылау және басқару жүйесінің кез келген жүйесіне біріктіруге мүмкіндік береді. Жабдықтың өзі функционалдық, жеңіл, ықшам, пайдалануға ыңғайлы және құны бойынша қолжетімді болды. Бірнеше жыл бұрын мұндай жүйені орнатуды тек ірі кәсіпорындар ғана бере алады, қазір тапсырыстар спектрі жергілікті жүйелерден (бір есікке), аумақтық-бөлінген объектілердің ірі желілік құрылымдарына дейін кеңейді. Жабдықтар тек банктер мен ерекше қорғалатын мекемелерде ғана емес, сонымен қатар қарапайым кеңселерде, мектептерде, ауруханаларда, санаторийлерде, тұрғын үйлерде (жеке және көп пәтерлі) және т. б. кеңінен қолданыла бастады.

Биометриялық бақылау жүйесі, барлық жабдықтары сияқты, берілген аумаққа кіруді басқаруға арналған:

- материалдық құндылықтарды, ақпаратты, мүлікті, жабдықтарды қорғау;
- қызметкерлер мен келушілердің қауіпсіздігі;
- объектіге кіруді бақылау, есепке алу және басқару (тұлғаны сәйкестендіру, қол жеткізу аймағы мен уақытын анықтау, есіктерді, турникеттерді, шлагбаумдарды ашу және т. б.);
- персоналды тиімді басқару (тиісті БҚ-мен интеграциялау кезінде).

1 Теориялық бөлім

1.1 Биометриялық технологиялар

Компьютерлік желілердің дамуына және автоматтандыру салаларының кеңеюіне қарай ақпараттың құндылығы ұдайы өсуде. Мемлекеттік құпиялар,ғылымды қажетсінетін ноу-хау, коммерциялық, заңды және дәрігерлік құпиялар әдетте жергілікті және корпоративтік желілерге қосылған компьютерге жиі сенім артады. Бір жағынан, ғаламдық ғаламтор желісінің танымалдығы электрондық коммерция үшін үлкен мүмкіндіктер ашады, бірақ екінші жағынан, корпоративтік деректерді сырттан қол жеткізуден қорғау үшін қауіпсіз құралдарға деген қажеттілікті тудырады. Қазіргі уақытта көптеген компаниялар өз жүйелеріне рұқсатсыз қол жеткізуді болдырмау және электрондық бизнестегі транзакцияларды қорғау қажеттілігімен бетпе-бет келеді [1].

90 жылдардың соңына дейін пайдаланушыны дербестендірудің негізгі тәсілі оның желілік аты мен паролін көрсету болды. Әділдік үшін мұндай тәсілді көптеген мекемелер мен ұйымдарда бұрынғысынша ұстанады. Құпия сөзді пайдалануға байланысты қауіптер жақсы белгілі: құпия сөздерді ұмытады, дұрыс емес жерде сақтайды, ақырында, олар жай ғана ұрлана алады. Кейбір пайдаланушылар паролді қағазға жазып, осы жазбаларды жұмыс станцияларының жанында ұстайды. Көптеген компаниялардың ақпараттық технологиялар тобының хабарлауынша, қолдау қызметіне қоңырау шалудың басым бөлігі ұмытылған немесе күші жойылған парольдермен байланысты [2].

Жүйені басқаның атымен елестетіп алдауға болады. Ол үшін қауіпсіздік жүйесі тұрғысынан бір ғана адамға ие болатын кейбір идентификациялық ақпаратты білу қажет. Қаскүнем компания қызметкері үшін өзін бере отырып, осы пайдаланушыға оның өкілеттіктері мен лауазымдық міндеттеріне сәйкес қол жетімді барлық ресурстарды өз иелігіне алады. Нәтижесінде ақпаратты ұрлаудан бастап барлық ақпараттық кешеннің істен шығуына дейінгі түрлі құқыққа қарсы әрекеттер болуы мүмкін.

Дәстүрлі идентификация құрылғыларын әзірлеушілер стандартты әдістер көп жағдайда ескірген. Мәселе, атап айтқанда, физикалық қол жеткізуді бақылау және Ақпаратқа қол жеткізуді бақылау әдістерін жалпы қабылданған бөлу дәрменсіз. Өйткені серверге қол жеткізу үшін кейде ол тұрған бөлмеге кіру міндетті емес. Оның себебі - клиент-сервер және ғаламтор технологиясын біріктіретін, бөлінген есептеулердің түгел қамтитын тұжырымдамасы. Бұл мәселені шешу үшін жаңа идеологияға негізделген

түбегейлі жаңа әдістер қажет. Жүргізілген зерттеулер көрсеткендей, аталған компанияларға рұқсатсыз қол жеткізу жағдайында шығын миллиондаған долларды құрауы мүмкін.

Бұл жағдай шығу амалы бар ма? Бар және бұрыннан бар. Тек жүйеге кіру үшін оларды тасымалдаушыдан тыс жұмыс істемейтін идентификациялау әдістерін қолдану қажет. Бұл талапқа адам ағзасының биометриялық сипаттамалары жауап береді. Қазіргі биометриялық технологиялар жеке тұлғаны физиологиялық және психологиялық белгілері бойынша сәйкестендіруге мүмкіндік береді. Айтпақшы, биометрия адамзатқа бұрыннан белгілі - ежелгі мысырлықтар өсу бойынша сәйкестендіруді қолданды [3].

1.2 Биометриялық сәйкестендіру негіздері

Биометриялық сәйкестендірудің негізгі мақсаты заңды пайдаланушыларға қол жеткізуден өте сирек бас тартатын және сонымен бірге компьютерлік деректер қоймаларына рұқсатсыз қол жеткізуді толық болдырмайтын тіркеу жүйесін құру болып табылады. Құпия сөздер мен карталармен салыстырғанда, мұндай жүйе әлдеқайда сенімді қорғауды қамтамасыз етеді: өз денесін ұмытуға да, жоғалтуға да болмайды. Объектіні биометриялық тану осы объектінің физиологиялық немесе психологиялық сипаттамаларын жүйенің деректер базасында сақталатын оның сипаттамаларымен салыстыруға негізделген. Бұл процесс үнемі адамның миында жүреді, мысалы, олардың жақындарын білуге және оларды бейтаныс адамдардан ажыратуға мүмкіндік береді [12].

Биометриялық технологияларды екі үлкен санатқа бөлуге болады - физиологиялық және психологиялық (мінез-құлық). Бірінші жағдайда бет белгілері, көздің құрылымы (торлы немесе радужка), саусақтар (папиллярлы сызықтар, топография, буындардың ұзындығы және т.б.), алақан (мөр немесе топография), қолдың формасы, қолдың білезігіндегі немесе термалды бейнедегі Венаның суреттері сияқты сипаттамалар қарастырылады. Психологиялық сипаттамалар - адам дауысы, оның қол қою ерекшеліктері, жазу динамикалық параметрлері және пернетақтадан мәтінді енгізу ерекшеліктері [8].

Бұл жағдайда ең қолайлы әдісті таңдауға бірқатар факторлар әсер етеді. Ұсынылған технологиялар үнемділігімен ерекшеленеді, ал олардың құны көп жағдайда сенімділік деңгейіне тікелей пропорционалды. Осылайша, мамандандырылған жабдықты қолдану әрбір жұмыс орнының құнын мың долларға ұлғайтады.

Саусақтың папиллярлы өрнегі, алақанның геометриясы немесе көздің торлы қабығының суреті (үлгісі) сияқты физиологиялық ерекшеліктер -

адамның тұрақты физикалық сипаттамалары. Бұл өлшеу түрі (верификация) физиологиялық сипаттамалар сияқты іс жүзінде өзгермейді. Пернетақтаның қолы, дауысы немесе жазуы сияқты мінез-құлық сипаттамалары бақыланатын іс-қимылдарға да, аз бақыланатын психологиялық факторларға да байланысты. Мінез-құлық сипаттамалары уақыт өте келе өзгеруі мүмкін болғандықтан, тіркелген биометриялық үлгі әрбір пайдалану кезінде жаңартылуы тиіс. Мінез-құлық сипаттамаларына негізделген Биометрия арзанырақ және пайдаланушылар үшін аз қауіп төндіреді; алайда физиологиялық белгілері бойынша сәйкестендіру неғұрлым дәл болып табылады және үлкен қауіпсіздікті қамтамасыз етеді. Кез келген жағдайда, екі әдіс пароль немесе картаға қарағанда айтарлықтай жоғары сәйкестендіру деңгейін қамтамасыз етеді [4].

Аутентификацияның барлық биометриялық құралдары жеке адамның белгілі бір қасиеттерінің статистикалық қасиеттерін қандай да бір нысанда пайдаланатынын атап өткен жөн. Бұл дегеніміз, оларды қолдану нәтижелері ықтимал болып табылады және уақыт өзгереді. Сонымен қатар, барлық осындай құралдар аутентификация қателігінен сақтандырылмаған. Екі түрі бар қателер: жалған ауытқуы және төзімділік. Бұл тақырып ықтималдық теориясында радар әзірлеу кезінен бастап жақсы зерттелді. Аутентификация процесіне қателердің әсері жалған оң және жалған оң орта ықтималдықтарды салыстыру жолымен бағаланады. Тәжірибе көрсетіп отырғандай, бұл екі ықтималдықтар кері тәуелділікпен байланысты, яғни басқаруды созу әрекеттерінде жүйеге жібермеу ықтималдығы артады және керісінше артады. Осылайша, әрбір нақты жағдайда ымыраға келу керек. Алайда, тіпті ең пессимистік сараптамалық бағалаулар бойынша, биометрия барлық салыстырулардан ұтады, өйткені ол аутентификацияның басқа қолданыстағы әдістеріне қарағанда әлдеқайда сенімді.

Тиімділік пен бағадан басқа, компаниялар сондай-ақ қызметкерлердің биометриялық құралдарға реакциясын ескеруі тиіс. Мінсіз жүйе пайдалану оңай, жылдам, нәзік, ыңғайлы және әлеуметтік қолайлы болуы тиіс. Бірақ табиғатта ешнәрсе жасалмаған және әзірленген технологиялардың әрқайсысы талаптардың барлық жиынтығына ішінара жауап береді. Бірақ тіпті ең ыңғайсыз және тұрақты емес құралдар (мысалы, пайдаланушылар өз көздерін қорғай отырып, аулақ болуға тырысатын тор көзіндегі идентификация) жұмыс берушіге күмәнсіз пайда әкеледі: олар компанияның қауіпсіздік мәселелеріне тиісті назарын көрсетеді.

Биометриялық құрылғылардың дамуы бірнеше бағытта жүріп жатыр, бірақ олар үшін қауіпсіздіктің бірегей деңгейі, парольді және карточкалық

қорғаныс жүйелерінің дәстүрлі кемшіліктерінің болмауы және жоғары сенімділік болып табылады. Биометриялық технологиялардың табысы осы уақытқа дейін негізінен олар бұйрық бойынша енгізілетін ұйымдармен байланысты, мысалы, күзетілетін аумақтарға қол жеткізуді бақылау үшін немесе Құқық қорғау органдарының назарын аударған адамдарды анықтау үшін. Корпоративтік пайдаланушылар биометрия әлеуетін толық түсіне алмады. Компания басшылары жиі биометриялық жүйелерді өрістетуге қауіп төндірмейді, себебі өлшеулердегі мүмкін қателіктердің салдарынан пайдаланушыларға құқықтары бар қол жеткізуден бас тартылады деп қауіптеніп. Дегенмен, жаңа технологиялар корпоративтік нарыққа көбірек енеді. Бүгінде ондаған мың компьютерлендірілген орындар, сақтау орындары, зерттеу зертханалары, қан банктері, банкоматтар, әскери құрылыстар бар, оларға қол жеткізу жеке тұлғаның бірегей физиологиялық немесе мінез-құлық сипаттамаларын сканерлейтін құрылғылармен бақыланатын.

1.3 Аутентификация әдістері

Белгілі болғандай, аутентификация субъектіде тек адам ғана емес, бағдарламалық процесс болуы мүмкін шынайылығын тексеруді білдіреді. Жалпы айтқанда, индивидтердің аутентификациясы әр түрлі формада сақталған ақпаратты ұсыну есебінен мүмкін болады. Бұл мүмкін:

- пароль, жеке нөмір, криптографиялық кілт, желідегі компьютердің желілік мекенжайы;
- смарт-карта, электрондық кілт;
- көздің сыртқы келбеті, дауысы, көздің тор қабығының суреті, саусақ іздері және пайдаланушының басқа да биометриялық сипаттамалары [13].

Аутентификация жалпы пайдаланудағы ақпаратқа қол жеткізу құқығын негізді және дұрыс ажыратуға мүмкіндік береді. Алайда, екінші жағынан, бұл ақпараттың тұтастығы мен дұрыстығын қамтамасыз ету проблемасы туындайды. Пайдаланушы сенімді көзден ақпаратқа қол жеткізуге және осы ақпараттың тиісті санкцияларсыз өзгермегеніне сенімді болуы тиіс.

«Жалғыз» (бір атрибут бойынша) сәйкестігін іздеу верификация деп аталады. Бұл әдіс жоғары жылдамдықпен ерекшеленеді және компьютердің есептеу қуатына ең аз талаптар қояды. Бірақ іздеу көп деп аталады идентификация. Мұндай алгоритмді жүзеге асыру әдетте қиын ғана емес, қымбат. Бүгінде компьютер пайдаланушыларды анықтау және сәйкестендіру үшін адамның саусақ іздері, бет белгілері, көздің мөлдір қабығы және торлы қабығы, алақанның пішіні, дауыс, сөйлеу және қол қою ерекшеліктері сияқты жеке сипаттамаларын пайдаланатын биометриялық құрылғылар нарыққа шығады. Тестілеу және тәжірибелік пайдалану сатысында беттің жылу өрісі,

қолдың қан тамырларының суреті, дененің иісі, терінің температурасы және тіпті құлақтың пішіні бойынша пайдаланушылардың аутентификациясын орындауға мүмкіндік беретін жүйелер болады.

Кез келген биометриялық жүйе белгілі бір үлгіні тануға және пайдаланушының нақты физиологиялық немесе мінез-құлық сипаттамаларының түпнұсқалығын орнатуға мүмкіндік береді. Логикалық биометриялық жүйені екі модульге бөлуге болады: тіркеу модулі және сәйкестендіру модулі. Біріншісі жүйені анықтау үшін жауап береді. Тіркеу кезеңінде биометриялық датчиктер адамның қажетті физиологиялық немесе мінез-құлық сипаттамаларын сканерлейді және олардың сандық көрінісін жасайды. Арнайы модуль бұл көрініс өзіне тән ерекшеліктерді бөліп, шаблон деп аталатын ықшам және мәнерлі көрініс генерациялау үшін өңдейді. Бет бейнесі үшін көздің, мұрын мен ауыздың мөлшері мен салыстырмалы орналасуы осындай тән ерекшеліктер болуы мүмкін. Әрбір пайдаланушы үшін үлгі биометриялық жүйенің деректер базасында сақталады.

Идентификация модулі адамды тану үшін жауап береді. Идентификация кезеңінде биометриялық датчик идентификациялау қажет адамның сипаттамасын алып, осы сипаттамаларды шаблон сақталатын сандық форматқа түрлендіреді. Алынған үлгі бір-біріне сәйкес келетіндігін анықтау үшін сақталған үлгімен салыстырылады.

Мысалы, Microsoft Windows жүйесінде пайдаланушы аутентификациясы үшін екі нысан қажет - пайдаланушы аты мен құпия сөз. Саусақ іздерін аутентификациялау барысында пайдаланғанда, пайдаланушы аты тіркелу үшін енгізіледі, ал саусақ ізі құпия сөзді ауыстырады (1.1 сурет). Бұл технология пайдаланушының тіркелгісін алу үшін және таңбаны тіркеу кезінде саналған үлгінің және пайдаланушының осы атына бұрын сақталған үлгінің арасында «бір - біріне» сәйкестігін тексеру үшін пайдаланушы атын көрсеткіш ретінде пайдаланады. Екінші жағдайда тіркеу кезінде енгізілген үлгі саусақ ізін сақталған үлгілердің барлық жиынтығымен салыстыру қажет.

1.1 Сурет - Саусақ іздері бойынша аутентификация процесі

Аутентификация әдісін таңдағанда бірнеше негізгі факторларды ескеру керек:

- ақпараттың құндылығы;
- аппараттық және бағдарламалық аутентификация құны;
- жүйенің өнімділігі;
- қолданушылардың қолданылатын аутентификация әдістеріне қатынасы;
- қорғалатын ақпараттық кешеннің ерекшелігі (мақсаты).

Аутентификация құралдарының құны, яғни сапасы мен сенімділігі ақпараттың маңыздылығымен тікелей байланысты болуы тиіс. Сонымен қатар, кешеннің өнімділігін арттыру, әдетте, оның қымбаттауына ілесе жүреді.

1.3.1 Саусақ іздері

Соңғы жылдары, саусақ іздері бойынша сәйкестендіру процесі болашақта кеңінен қолданылатын биометриялық технология ретінде назар аударды. Gartner Group мәліметтері бойынша http://www.gartnergroup.com), бұл технология корпоративтік нарықта басым және жақын болашақта Iris бойынша тану технологиясымен ғана бәсекелесе алады [14].

Бүкіл әлемдегі азаматтық қоғамның Үкіметі мен ұйымдары саусақтардың іздерін сәйкестендірудің негізгі әдісі ретінде бұрыннан пайдаланады. Сонымен қатар, саусақ іздері сәйкестендірудің компьютерлік жүйесінде қолдану үшін ең дәл, ыңғайлы және үнемді биометриялық сипаттама болып табылады. Бұл технология АҚШ-та, мысалы, Штаттардың бірнеше әкімшіліктерінің Көлік ведомстволарында, MasterCard, Федералдық тергеу бюросы, құпия қызметте, Ұлттық қауіпсіздік агенттігінде, қаржы және қорғаныс Министрлігінде және т. б. қолданылады. Пайдаланушылар үшін

құпия сөз қажеттілігін жоя отырып, саусақ іздері технологиясы қолдау қызметіне қоңырау шалу санын қысқартады және желіні басқару шығындарын төмендетеді.

Әдетте саусақ іздерін тану жүйелері екі түрге бөлінеді: сәйкестендіру үшін - AFIS (Automatic Fingerprint Identification Systems) және верификациялау үшін. Бірінші жағдайда барлық он саусақтың іздері қолданылады. Мұндай жүйелер сот жүйесінде кеңінен қолданылады. Верификация құрылғысы әдетте бірнеше саусақ іздері туралы ақпаратпен жұмыс істейді. Сканерлеу құрылғылары әдетте үш түрі бар: оптикалық, ультрадыбыстық және микрочиптер негізінде.

Саусақ іздері бойынша қол жеткізу артықшылықтары пайдалану қарапайымдылығы, ыңғайлылығы және сенімділігі болып табылады. Саусақ іздерін анықтаудың екі негізгі алгоритмі бар: жеке бөлшектер бойынша (тән нүктелер) және саусақтың барлық бетінің бедері бойынша. Тиісінше, бірінші жағдайда, құрылғы нақты таңба үшін бірегей кейбір жерлерді ғана тіркейді және олардың өзара орналасуын анықтайды. Екінші жағдайда барлық бедерлердің бейнесі өңделеді. Қазіргі заманғы жүйелерде осы екі әдістің үйлесімі жиі қолданылады. Бұл екі кемшіліктерді болдырмау және сәйкестендіру дәлдігін арттырады. Бір рет тіркеу адамның саусақ ізін оптикалық сканерде біраз уақыт алады. Жеке құрылғы түрінде жасалған немесе пернетақтаға салынған кішкентай зарядтау байланысы бар аспап камера саусақтың ізін түсіреді. Содан кейін, арнайы алгоритмдердің көмегімен алынған сурет бірегей - бұл сызықтардың үзілуі мен қиылысуы анықталатын баспа микроточкасының картасы болып табылады. Бұл үлгі (саусақ ізінің өзі емес) шифрланады және желі пайдаланушыларының түпнұсқалығын тексеру үшін Деректер базасына жазылады. Бір үлгіде бірнеше ондаған-жүздеген микроточкаға дейін сақталады. Сонымен қатар, пайдаланушылар өзінің жеке өмірінің құпиялылығы туралы алаңдатты болмауы мүмкін, себебі саусақ іздерінің өзі сақталмайды және микроточки қайта жасалуы мүмкін емес.

Ультрадыбыстық сканерлеу артықшылығы лас саусақтарда және тіпті жұқа резеңке қолғаптар арқылы қажетті сипаттамаларды анықтау мүмкіндігі болып табылады. Қазіргі заманғы тану жүйелері тіпті жаңа кесілген саусақтарды алдай алмайды (микрочип терінің физикалық параметрлерін өлшейді). Мұндай жүйелерді әзірлеумен 50-ден астам түрлі өндірушілер айналысады.

Тұлғаны сәйкестендіру үшін саусақ іздерін пайдалану барлық биометриялық әдістердің ең ыңғайлы болып табылады. Пайдаланушыны

идентификациялаудағы қатенің ықтималдығы биометрияның басқа әдістерімен салыстырғанда айтарлықтай төмен. Саусақ ізін тану сапасы және оны алгоритммен дұрыс өңдеу мүмкіндігі саусақ бетінің жай-күйіне және оның сканерлеу элементіне қатысты жағдайына қатты байланысты. Әр түрлі жүйелер осы екі параметрге әр түрлі талаптар қояды. Талаптар сипаты, атап айтқанда, қолданылатын алгоритмге байланысты. Мысалы, сипатты нүктелер бойынша тану саусақтың беті нашар болған кезде қатты шу береді. Барлық бетінде тану бұл кемшілік жоқ, бірақ сканерлейтін элементке саусақты өте дәл орналастыруды талап етеді. Саусақ іздерін идентификациялау құрылғысы көп орынды талап етпейді және индекстік манипуляторға (тінтуірге) немесе пернетақтаға орнатылуы мүмкін.

1.3.2 Бет геометриясы.

Адамды кәдімгі өмірде сәйкестендіру - танудың ең көп таралған тәсілі. Оның техникалық іске асырылуына келетін болсақ, ол саусақ іздерін танудан гөрі күрделі (математикалық тұрғыдан) міндет болып табылады және одан басқа, қымбат тұратын аппаратураны талап етеді (сандық бейне - немесе фотокамера және бейнені басып алу ақысы қажет). Бұл әдіс бір маңызды плюс бар: сәйкестендіру үлгісінің бір үлгісі туралы деректерді сақтау үшін өте аз жады қажет. Өйткені, адамның беті барлық адамдарда өзгермейтін учаскелердің аз мөлшерін бөлшектеуге болады. Мысалы, нақты адамға сәйкес келетін бірегей үлгіні есептеу үшін тек 12-ден 40-қа дейін тән учаскелер қажет.

Әдетте камера объектіден бірнеше ондаған сантиметр қашықтықта орнатылады. Суретті алып, жүйе беттің әр түрлі параметрлерін талдайды (мысалы, көз мен мұрын арасындағы қашықтық). Көптеген алгоритмдер зерттелетін индивидте көзілдіріктердің, шляпалар мен сақалдардың болуын өтеуге мүмкіндік береді. Бұл мақсат үшін әдетте инфрақызыл ауқымда бетті сканерлеу қолданылады. Мұндай жүйелер өте дәл нәтиже береді деп болжауға болар еді. Осыған қарамастан, бірқатар елдерде олар кассирлерді және депозиттік сейфтерді пайдаланушыларды верификациялау үшін өте табысты пайдаланылады.

1.3.3 Қол геометриясы.

Бет геометриясын бағалауға арналған жүйелермен қатар қолдың алақандарын тануға арналған жабдық бар. Қазіргі уақытта қолданушыларды қол геометриясы бойынша сәйкестендіру заңнамалық органдарда, халықаралық әуежайларда, ауруханаларда, иммиграциялық қызметтерде және т. б. қолданылады. Алақанның геометриясы бойынша идентификацияның артықшылықтары сенімділік мәселесіндегі саусақ ізі бойынша

идентификацияның плюстерімен салыстыруға болады, бірақ алақанның іздерін оқуға арналған құрылғы көбірек орын алады.

1.3.4 Көздің торлы қабығы.

Жеткілікті сенімді тану адам көзінің торлы қабықшасының суретін талдайтын жүйелерді қамтамасыз етеді. Өйткені, бұл сипаттама жеткілікті тұрақты, адамның бүкіл өмір бойы іс жүзінде өзгермейді, ластану мен жарақаттарға сезімтал емес. Сондай-ақ, сол және оң көздің торлы қабығы, сурет айтарлықтай ерекшеленеді.

Әдетте танудың белсенді және пассивті жүйелері бар. Бірінші типті жүйелерде пайдаланушы камераны дәл көзбен көру үшін жылжыта отырып, өзі баптауы тиіс. Пассивті жүйелер пайдалану оңай, себебі камера автоматты түрде реттеледі. Бұл жабдықтың жоғары сенімділігі оны тіпті түзету мекемелерінде пайдалануға мүмкіндік береді.

Торлы қабықшасының сканерлерінің артықшылығы - олар пайдаланушыдан мақсатқа назар аудару үшін талап етпейді, себебі үлгісі торлы қабықшасында көз бетінде орналасқан дақ. Шын мәнінде, көздің бейнені тіпті бір метрден кем қашықтықта сканерлеуге болады, сондықтан торлы қабығы сканерлері банкоматтар үшін қолайлы.

1.3.5 Көз торы.

Көз торының сәйкестендіру әдісі салыстырмалы түрде жақында - 50-ші жылдардың ортасында өткен XX ғасырдың өзінде іс жүзінде қолдануға ие болды. Сол кезде егіздердің тіпті тордың қан тамырларының суреті сәйкес келмейді. Арнайы құрылғыда тіркелу үшін камераның көзіне бір минуттан кем қарау жеткілікті. Осы уақыт ішінде жүйе тор көзді жарықтандыруға және көрсетілген сигнал алуға үлгереді. Торды сканерлеу үшін көздің артқы қабырғасындағы қан тамырларына қарашық арқылы бағытталған төмен қарқындылық инфрақызыл сәуле қолданылады. Алынған сигналдан ақпарат орташаланатын және кодталған файлда сақталатын бірнеше жүздеген бастапқы сипаттық нүктелер бөлінеді. Мұндай жүйелердің кемшіліктеріне бірінші кезекте психологиялық факторды жатқызуға болады: кез келген адам көзге жарық беретін белгісіз қараңғы тесікке қарауға ұмтылмайды. Сонымен қатар, тесікке қатысты көздің жағдайын қадағалау керек, себебі мұндай жүйелер торлы қабаттың дұрыс емес бағдарына сезімтал. Көз торына арналған сканерлер аса құпия жүйелерге қолжетімділікті ұйымдастыру кезінде үлкен таралған, өйткені тіркелген пайдаланушылардың қол жетімділігінен бас тартудың ең төмен пайыздарының бірі мен қателердің нөлдік пайызына дерлік кепілдік береді.

1.3.6 Дауыс және сөйлеу.

Көптеген фирмалар адамды дауыспен сәйкестендіруге қабілетті бағдарламалық жасақтаманы шығарады. Сыртқы көріністі танудан айырмашылығы, бұл әдіс қымбат тұратын аппаратураны талап етпейді - тек дыбыстық ақы мен микрофон жеткілікті.

Дауыс бойынша сәйкестендіру ыңғайлы, бірақ басқа биометриялық әдістер сияқты сенімді әдіс емес. Дауыс физиологиялық және мінез-құлық факторларының комбинациясынан қалыптасады, сондықтан осы биометриялық тәсілге байланысты негізгі мәселе-сәйкестендіру дәлдігі. Қазіргі уақытта дауысты идентификациялау қауіпсіздік дәрежесі орташа үй-жайға кіруді басқару үшін қолданылады.

1.3.7 Қолы.

Оның айтуынша, қол - адамның физиологиялық сипаттамалары сияқты бірегей атрибуты. Сонымен қатар, бұл кез-келген адам үшін әдеттегі сәйкестендіру әдісі, өйткені ол саусақ іздерін алып тастағандықтан, қылмыстық саламен байланысты емес. Аутентификацияның перспективті технологияларының бірі жазу кезінде адам қолының қозғалысының биометриялық сипаттамаларының бірегейлігіне негізделген. Әдетте қол қою туралы деректерді өңдеудің екі жолы бар: үлгімен қарапайым салыстыру және динамикалық верификация. Біріншісі өте сенімсіз, өйткені деректер базасында сақталған графикалық үлгілермен енгізілген қолтаңбаны әдеттегі салыстыруға негізделген. Өйткені қол әрқашан бірдей болуы мүмкін емес, бұл әдіс қателердің үлкен пайызын береді. Динамикалық верификация әдісі әлдеқайда күрделі есептеулерді талап етеді және қолдың әр түрлі учаскелердегі қозғалыс жылдамдығы, қысым күші және қолдың әр түрлі кезеңдерінің ұзақтығы сияқты қол қою процесінің параметрлерін нақты уақытта бекітуге мүмкіндік береді. Бұл қолтаңбаны тәжірибелі графологтың да қолдан жасай алмайтындығына кепілдік береді, себебі ешкім қол иесінің қолын дәл көшіре алмайды [11].

Пайдаланушы стандартты дигитайзер мен қаламды пайдалана отырып, өзінің әдеттегі қолтаңбасын имитациялайды, ал жүйе қозғалыс параметрлерін оқиды және оларды деректер базасына алдын ала енгізілгендермен салыстырады. Қол қою үлгісі эталонмен сәйкес келген кезде жүйе қол қойылатын құжатқа пайдаланушының атын, оның электрондық почтасының мекенжайын, лауазымын, ағымдағы уақыты мен күнін, қозғалыс динамикасының бірнеше ондаған сипаттамасынан (бағыты, жылдамдығы, үдеуі) тұратын қол қою параметрлерін және басқаларын қамтитын ақпаратты қоса тіркейді. Бұл деректер шифрленеді, содан кейін олар үшін бақылау

сомасы есептеледі және одан әрі мұның барлығы биометрикалық белгі ретінде құрылып, тағы да шифрленеді. Жүйені теңшеу үшін жаңадан тіркелген пайдаланушы құжатқа қол қою рәсімін бес реттен он ретке дейін орындайды, бұл орташаланған көрсеткіштер мен сенімді интервалдарды алуға мүмкіндік береді. Бұл технологияны алғаш рет PenOp компаниясы пайдаланды.

Қол қою идентификациясын барлық жерде қолдануға болмайды - атап айтқанда, бұл әдіс үй-жайға кіруді шектеу үшін немесе компьютерлік желіге кіру үшін қолайлы емес. Алайда, кейбір салаларда, мысалы, банк саласында, сондай-ақ маңызды құжаттарды ресімдеу жүргізілетін барлық жерде қолдың дұрыстығын тексеру неғұрлым тиімді, ал ең бастысы-ауыртпалықсыз және елеусіз тәсілмен болуы мүмкін.

1.4 Биометриялық параметрлердің артықшылықтары мен кемшіліктері

Объективті және субъективті бағалау нүктесінен нақты қосымша үшін жақсы келетін бірнеше биометриялық параметрлер болуы мүмкін. Әрбір биометриялық параметр белгілі бір оң және теріс қасиеттерге ие, ол белгілі бір қосымша үшін параметрді таңдағанда ескерілуі керек. Әрбір алты дәстүрлі биометриялық параметрлердің оң және теріс жақтары ұқсас [7].

1.4.1 Саусақ іздері.

Биометриялық параметрдің артықшылықтары:

- саусақ басып шығару жеке тұлғаны криминалистикада сәйкестендіру үшін бұрыннан қолданылып келеді. Дегенмен жақында таңбаларды талдаудың қолданыстағы әдістерінің дәлдігіне күмән келтіретін жаңа мәліметтер табылды;

- саусақ іздерінің үлкен деректер базасы бар,бірақ онда негізінен қылмыскерлер тіркелген.Сонымен қатар, Калифорния, Колорадо, Флорида және Техас көлік департаменттері жүргізуші құқықтары мен деректер жазбаларында саусақ іздерін пайдалану тәжірибесін енгізу үшін жұмыс істейді;

- саусақ іздері сотта сараптама жасау үшін қолайлы, мысалы, саусақтардың латентті іздерін зерттеу әдісі кең таралған.

Қылмыскерлер қылмыс орнында жиі саусақ іздерін (машиналарда,есік тұтқаларында,шыныларда,қаруларда) қалдырады:

- саусақ іздерінің үлгілерін қарапайым құралдарды пайдалана отырып, оңай алуға болады;саусақ іздерін оқитын құрылғылардың мөлшері мен бағасы төмендеуді жалғастырады. Сандық бейнелерді түрлендіру оңай, сапалы және арзан болады. Қазір баға бойынша қол жетімді саусақ іздері бар. Олар көптеген қол жетімділікті бақылау қосымшаларында қолданылады.

Биометриялық параметрдің кемшіліктері:

- саусақ ізімен тұрақты әлеуметтік ақыл-ой байланысты, кейбір елдер адамдарының санасында олар қылмыстық қылмыстармен байланысты. Бұл қауымдастық кейбір жағдайларда артықшылығы болуы мүмкін, бірақ жиі саусақ іздерін биометриялық параметр ретінде қолдану аясын кеңейтуге кедергі келтіреді;

- кейбір мәдениеттерде саусақ іздері әлі күнге дейін қол қою орнына пайдаланатын өршіксіз адамдармен байланысты;

- саусақ іздерінің сапасы қарсылығына, қолдың ластануына, саусақ ұшының жоғалуына байланысты әртүрлі болуы мүмкін, сонымен қатар саусақ ампутациялануы мүмкін, яғни адамның өмір сүру салты мен оның саусақ іздерінің сапасы арасындағы байланысты ескеру қажет;

- сурет алу үшін саусақ ізін оқу құрылғысының бетіне саусақпен басу керек. Бұл техникалық қиындықтарға және сенсор тазалығы мен гигиена мәселелеріне әкеледі;

- кейде саусақтары жоқ адамдар кездеседі. Әлбетте, бұл адамдардан үлгілер алу мүмкін емес.

1.4.2 Тұлға.

Биометриялық параметрдің артықшылықтары:

- адамдардың бейнелері паспорттар мен жүргізуші куәліктерінде кеңінен қолданылады-меншік негізінде аутентификациялық хаттаманың мүмкіндіктерін кеңейту үшін; сондықтан қоғам тұлғаны биометриялық сәйкестендіргіш ретінде пайдалану тәжірибесін оңай қабылдайды;

- адамдарды тану жүйесі үлгіні алған кезде өте аз көрінеді, олар физикалық байланысты да, объектінің хабардарлығын да талап етпейді;

- адамдарды тану үшін фотосуреттердің, бейнекассеталардың немесе басқа да тасымалдаушылардың қолданыстағы деректер базасы пайдаланылуы мүмкін;

- адамды тану, кем дегенде теориялық жағынан, олардың қалауынсыз және нақты уақытта топтарда адамдарды сұрыптау жұмыстары жүргізілуі мүмкін;

- бұл биометриялық идентификатор адамдардың шағын топтарымен жұмыс істейтін верифициялық қосымшалар үшін тамаша.

Биометриялық параметрдің кемшіліктері:

- автоматтандырылған аутентификациялық жүйелер үшін биометриялық үлгілерді алу кезінде тұлға бақыланатын жарық көздерімен жақсы жарықтандырылуы тиіс. Бұл техникалық қиындықтардың ұзын тізіміндегі бірінші мәселе;

- биометриялық параметр ретінде бет таза идентификациялық хаттама үшін жаман. Бұл параметр нәтижесі өте жоғары дәлдікті қажет етпеген кезде верификациялау үшін қолданылады;

- тану жүйесін бүркемелеу арқылы алдауға болады, ол сұрыптау қосымшаларында жалған теріске шығаруға себеп болады, яғни, қалаусыз жасырын тұлға сәйкестендірілмейді;

- қылмыстық әлеммен кейбір жағымсыз қауымдастықтар да бар, өйткені адамдардың бейнесі қылмыскерлердің картотекасын жасау кезінде ұзақ уақыт бойы қолданылады. Дегенмен, адамның бейнесі дәстүрлі түрде паспорттар, билеттер және т. б. үшін қолданылады.

1.4.3 Дауысы.

Биометриялық параметрдің артықшылықтары:

- адам сияқты, дауыс табиғи биометриялық параметр болып табылады;

- адамдар бір-бірін сәйкестендіру үшін қолданатын адамдардың бірі; белгілі бір жағдайларда (телефон байланысы), машинамен қабылданатын шешімдер салыстырмалы түрде біліксіз оператормен тексерілуі мүмкін;

- дауыс үлгілері, бет бейнесі сияқты, мүлдем көрінбеуі мүмкін;

- қоғам биометриялық идентификатор ретінде дауысты оңай қабылдайды, оның табиғатына байланысты сағат, ішінара қылмыстық әлеммен байланысты емес;

- дауысты өңдеу үшін қымбат жабдықтар қажет емес, онымен барлық жерде таралған телекоммуникациялық инфрақұрылымды пайдалана отырып, жұмыс істеу оңай, сондықтан дауыс қауіпсіздік жүйесіне жақсы;

- дауыс инкременттік аутентификациялық хаттамаларды пайдалануға мүмкіндік береді. Мысалы, хаттама құпиялылықтың жоғары деңгейін талап еткенде дауыстық ақпаратты көбірек алуды ұйғаруы мүмкін;

- дауыс биометриялық идентификатор ретінде дәл және қатты жұмыс істейді, білім арқылы верификациямен үйлеседі, аутентификациялық протоколда бұл ауызекі биометрикалық параметрлер деп аталады;

- дауыс кейбір уақыт кезеңінде жеке тұлғаны тексеруді жүргізуге мүмкіндік береді, яғни дауысты бүкіл сөйлесу барысында тұтынушы қалауға болады.

Биометриялық параметрдің кемшіліктері:

- кәсіби алаяқтың дауысын имитациялау мүмкіндігі бар. Бұл мәселе әлі жақсы зерттелген жоқ, дауыс үшін қол қоюға қарағанда нақты зиянкестерді зерттеуге арналған тест жоқ;

- сөйлеудің жасанды синтезі құрылғыларының жақсаруына қарай машиналық дауыспен жоқ тұлғаларды құру мүмкін болады (тіркеу мен

аутентификация қашықтықта болған кезде). Сөйлеу синтезінің оқыту құрылғылары берілген мәтінді сөйлейтін нақты адамның дауысын имитациялайтын автоматты жүйені құруға мүмкіндік береді;

- дауысты тану дыбыс сигналының сапасына байланысты. Сөйлеушінің ұқсас жүйелері фондық шуға, арналық шуға (шу - телефон желілері, радиотолқындар немесе компрессиялар) және микрофондармен жасалатын бұрмалауларға сезімтал емес;

- кейбір адамдар ауру, дене жетпейтіндер немесе психикалық бұзылулар, кереңдік себебінен, сондай - ақ дауысты уақытша жоғалтудан сөйлесе алмайды.

Биометриялық параметрдің артықшылықтары:

- тор қабығы қазір ең дәл биометриялық параметр болып саналады, әсіресе жеке пайда есептелген кезде. Торлы қабығын өңдеу кезінде өте аз жалған қол жеткізу жағдайлары бар, сондықтан ол таза сәйкестендіру үшін жақсы;

- торлы қабықшасының үлгісін алу камералардың көмегімен қашықтықта байқалмайды, оқу физикалық байланыссыз және пайдаланушы үшін ерекше қолайсыздықтарсыз жүзеге асырылады;

- жағымсыз қауымдастықтарға байланысты емес, оны пайдаланушыларды мақұлдаудың жоғары дәрежесі ерекшелендіреді. Сонымен қатар, ол сот сараптауында ешқашан пайдаланылмады;

- сатушылар торды тану жүйесін оқыту үлкен шығынды талап етпейді. Жоғарыда атап өткендей, тіркеу-бұл жүйенің жаттығуының негізгі бөлігі болса да, ол ие болуы тиіс артықшылықтарға ие емес.

Биометриялық параметрдің кемшіліктері:

- өте аз жұмыс істейтін торлы қабықшаларының деректер базасы бар.Қазіргі уақытта аутентификация жүйесін құру үшін қажетті инфрақұрылым жоқ болғандықтан, мұндай жоба өте үлкен ақшалай салымдарды талап етеді. Көз торын сәйкестендіру үшін жақсы биометриялық параметр болуы мүмкін болса да, осы саладағы ірі масштабты зерттеулер тестілік деректер базасының болмауына байланысты қиын;

- торлы қабығы кішкентай болғандықтан, оны алу үшін тұрған жабдықтар жағынан көп күш қажет;

- көзілдіріктер немесе контактілі линзалар салдарынан торлы қабығын аутентификациялауды жүргізу қиын болуы мүмкін; объект оларды алып тастауы тиіс;

- бір немесе екі көзін жоғалтқан адамдар, сондай-ақ өздерінің моторлы реакцияларын бақылай алмайтын адамдар бар, сондықтан олар осындай жүйеде тіркеле алмайды.

1.4.4 Қол.

Биометриялық параметрдің артықшылықтары:

- бұл параметр қазірдің өзінде мойындалған сияқты, өйткені ол - Диснейворлдта, АҚШ-тың иммиграция және натурализация қызметінде, сондай-ақ, Джорджия университетінде түрлі университеттерде верификация үшін пайдаланады;

- қол геометриясын өлшеу қарапайым операция болып саналады; - биометриялық параметр ретінде қол геометриясын кем дегенде бір сценарийлік бағалау жүргізілді , оның нәтижелері: ол верификация үшін қолайлы биометриялық параметр болып табылады. Бұл параметрге тән қателер коэффициенттері туралы өте аз белгілі;

- қол геометриясы, салыстырмалы түрде әлсіз биометриялық пармет-ром бола отырып, аса күшті параметрлер пайдаланушыларға артық қолайсыздық тудыруы мүмкін жағдайларда верификациялау үшін пайдаланылуы мүмкін.

Биометриялық параметрдің кемшіліктері:

- саусақ іздері сияқты үлгілерді алу үшін сенсордың бетіне қол қою керек (басқа да тәсілдер бар болса да). Бұл әдіс гигиена бойынша қауіп тудыруы мүмкін;

- биометриялық параметр ретінде қол геометриясының тек бір сценарийлік бағасы бар. Ғалымдар қол геометриясы биометрикалық параметрлер болып табылады ма деген пікірде;

- кейбір адамдар түрлі себептермен қолын немесе саусақтарын жоғалтып алды.

1.4.5 Қолы.

Биометриялық параметрдің артықшылықтары:

- қолтаңба адам жасаған биометриялық параметрлер болып табылады; оны қолдан жасау әдістері жақсы зерттелген, сондықтан оны тәжірибелі алаяқ жасаған кезде де жасанды анықтауға болады;

- тіркеу сатысында жалған қолтаңбаны анықтау мүмкіндігі бар;

- оқыту тез жүреді және адамдар түсінеді (т.б. сөз тану технологияларындағы сияқты), жүйе оқытылуы тиіс, жалған қол жеткізу үшін қалай тіркелу қажет екенін интуитивті түсінеді: қол қою верификациясы тез өтеді, шаблондарды сақтау үшін аз орын қажет;

- қолтаңбаның верификациясына объект айтқан тіл әсер етпейді;

- қолтаңбаны, шын мәнінде, ақпарат пен биометриялық параметрдің комбинациясы болып табылады, ақпараттық компонент (не жазылғандай) пайдаланушы өзгертуі мүмкін;

- қатты қысу қолтаңба үлгісінің сапасына әсер етпейді (тіпті 100-150 байт мөлшерінде).

Биометриялық параметрдің кемшіліктері:

- құжаттарға қол қою тәжірибесі бүкіл әлемде кеңінен таралған. Бұл қол қою әуежайларды қорғау үшін жеткіліксіз сенімді параметр болып табылады және т. б.;

- қолдардың жеке ерекшеліктері жақсы зерттелген, соның ішінде сапалы қолдан жасау негізінде. Өкінішке орай, қолтаңбаны тану жүйелерін тестілеу жеткіліксіз ұқыпты жүргізіледі және олардың нәтижелері қолдың биометриялық параметр ретінде ауқымдылығы туралы қорытынды жасауға мүмкіндік бермейді;

- қалаған дәлдікке қол жеткізу үшін қысым мен көлбеу бұрышын бекітетін бес өлшемді кеңістікте жазу қаламды қолдану қажет. Бұл қымбат жабдық. Технологиялардың бүгінгі жағдайы кезінде қол жеткізуді бақылау үшін қолтаңбаны пайдалану тиімділігі зерттелмеген;

- кейбір адамдар салдан зардап шегеді, ал басқалары хатты үйлестіру үшін жақсы моторлы реакциялары жоқ.

1.4.6 Биометрия ұмтылысы.

Сонымен қатар, биометриялық жүйелер аутентификацияның басқа да аппараттық құралдарымен, мысалы смарт-карталармен үйлескен жүйелерді қорғаудың барынша тиімділігін қамтамасыз ететінін атап өткім келеді. Биометриялық және аппараттық аутентификациялаудың әр түрлі тәсілдерін біріктіре отырып, өте сенімді қорғаныс жүйесін алуға болады (бұл осы технологияларға жетекші өндірушілер көрсететін үлкен қызығушылықпен жанама түрде расталады) [32].

Смарт-карталар пайдаланушыларға арналған электрондық өнімдер нарығының ең ірі және тез өсетін сегменттерінің бірін құрайды. Dataquest фирмасының болжамы бойынша http://www.dataquest.com), келесі жылға қарай смарт-карталарды сату көлемі жарты миллиард доллардан асады. Смарт-карталарды қолдану әрбір жұмыс орнында компьютерге қосылған арнайы оқу (терминалдық) құрылғысының болуын талап етеді, ол пайдаланушыны карта мен аутентификация серверінің өзара іс-қимыл процесіне тарту қажеттілігін болдырмайды. Ақылды карта аутентификацияның екі деңгейін қамтамасыз етеді. Жүйе іске қосу үшін пайдаланушы смарт картасын оқу құрылғысына салып, жеке сәйкестендіру

нөмірін дұрыс енгізуі керек. Ресей нарығында саусақ іздері бойынша сәйкестендіруді және смарт-карталарды пайдалануды үйлестіретін кешенді шешімдер, мысалы, Compaq (http://www.compaq.ru) және Fujitsu-Siemens (http://www.fujitsu-siemens.ru).

1.2 сурет - Сканері және смарт-картасы бар құрамдастырылған жүйе

Fujitsu-Siemens, Motorola, Sony, Unisys сияқты ірі компьютерлік компаниялардан басқа, биометриялық технологияларды әзірлеумен қазіргі уақытта Биометрия бойынша консорциумға - Biometric Consortium (Biometric Consortium) бірікті шағын жеке компаниялар айналысады .http://www.biometrics.org). Биометрия IT-индустриясының негізгі арнасына құйылатынын неғұрлым үміт артатын куәліктердің бірі-BioAPI (Biometrics API) қолданбалы бағдарламалау интерфейсін құру. Бұл әзірлеменің артында 1998 жылы құрылған өндірушілер консорциумы тұр. Compaq, IBM, Identicator Technology, Microsoft, Miros және Novell корпорацияларымен операциялық жүйелер мен қолданбалы БҚ-ға енгізуге болатын қолданыстағы биометриялық технологияларды қолдайтын стандартталған ерекшелікті әзірлеу үшін арнайы. BioAPI консорциумына бүгінде 78 ірі мемлекеттік және жеке компаниялар кіреді.

Енді корпоративтік клиенттер биометриялық өнімдерді стандартты компьютерлік және желілік технологиялар шеңберінде пайдалана алады. Стандартты API биометриялық құрылғылар мен бағдарламалық өнімдердің кең спектріне қол жеткізуге мүмкіндік береді, сондай-ақ бірнеше жеткізушілердің өнімдерін бірлесіп қолдануға мүмкіндік береді.

Биылғы жылы АҚШ үкіметі мемлекеттік мекемелерде BioAPI ашық стандартын енгізуді жариялады. Онда бірнеше миллион әскери және азаматтық қызметкерлер үшін саусақ іздері мен иесінің қолының үлгісін сақтайтын жаңа смарт-карталарды енгізу көзделіп отыр.

Бірқатар талдаушылардың пікірінше, биометриялық технологиялар әлі баяу дамып келеді,алайда тек үстелдік және портативті компьютерлер ғана

емес, сонымен қатар ұялы телефондар да осындай аутентификация құралдарынсыз ойластырылмайды. Microsoft Windows операциялық жүйесінің болашағы зор биометриялық технологияларды қолдаумен байланысты.

Биометриялық технологиялар үнемі дами береді. Дауысты тану алгоритмдері жақсарады, сканерлер аз және дәлірек, ал биометрияны пайдаланатын жүйелер сенімді және жылдамырақ болады. Биометриялық сипаттамалардың бірегейлігі және олардың адамнан ажыратылмауы ақпараттық қауіпсіздік саласындағы мамандар үшін де қызығушылық тудырады. Биометриялық технологияларды пайдалану жүйені пайдаланушылардың қателіктеріне неғұрлым төзімді етуге мүмкіндік береді, өйткені құпия сөзді ұмытып немесе күнделікке жазып алуға болады, ол жерден зиянкестер, смарт-карта жоғалады, ал өз саусақтарыңыз немесе көздеріңіз үйде қалдыра алмайды немесе жоғала алмайды. Қазіргі заманғы сканерлердің дәлдігі қателердің төмен деңгейін және жоғары сенімділігін қамтамасыз етеді, бұл қорғауға қойылатын жоғары талаптар бар жүйелер үшін өте маңызды. Бірнеше кемшіліктерге қарамастан, биометриялық технологияларды пайдалану жүйелердің қорғалуына оң әсер етеді және ақпараттық қауіпсіздік саласындағы білетін кәсіби биометриялық технологияларды жоспарлау, кірістіру және пайдалану, тұрақты өсіп келе жатқан және өзгеретін қорғаныс құралдарының бір бөлігі ретінде зерделенуі тиіс.

1.5 Биометриялық мифтер және қате көріністер

Төменде қарсыластардың да, биометрияның жақтастарының да арқасында таралуы мүмкін кейбір ең көп таралған мифтер мен қате көріністер тізімі келтірілген.

Биометриялық х параметрі кез келген қосымшалар үшін ең жақсы болып табылады. Барлық жағдайларға сәйкес келетін бір параметр жоқ. Әрбір қолданба немесе сценарийдің бағасы, дәлдігі, қолайлылығы және пайдаланушыларды мақұлдауын қоса алғанда, көптеген сипаттамалары бар.

Биометриялық х параметрі әрбір адам үшін бірегей. Биометриялық параметрлер деп аталатын адам денесінің ерекше ерекшеліктері тұқым қуалаушылыққа және даму процесіндегі өзгерістерге байланысты. Әрбір генетикалық айнымалының вариация саны немесе даму ерекшеліктері бір биометриялық параметрден екіншісіне өзгереді, жеке ерекшеліктердің мұндай кездейсоқ дамуы, егер оларды жеткілікті негізді зерттесе, оларды бірегей деп айтуға мүмкіндік береді. [17].

Бірдей биометриялық репрезентациясы бар екі адамды табу мүмкін емес, сондай - ақ бір адамның биометрикалық параметрлерінің екі үлгісінен

бірдей репрезентация алынады. Бұл мәселе «толеранттылық» көмегімен шешіледі, бұл шуды немесе нақты өзгерістерді өлшеудің орнына биометриялық параметрлерді қоюға мүмкіндік береді, бірақ бір мезгілде және биометриялық параметрлердің төмендігі түсінігін нивелирдей отырып, түрлі адамдардың биометрлік репрезентацияларының сәйкес келу мүмкіндігін арттырады.

Жүйенің нақты жұмыс дәлдігін болжауға болады. Жүйе жұмыс істейтін жағдайларда пайдаланушылардың нақты популяциясынан алынған деректер жүйесін оқыту жақсы. Жүйе жұмысының дәлдігін болжау үшін пайдаланушылар мен қоршаған орта популяциясының дәл үлгісін жасау қажет еді. Мұндай модельдер қол жетімді деректер базасының негізінде жасалуы мүмкін емес және тіпті тестілік эксплуатация жүйенің жұмыс істеу процесінде пайда болуы мүмкін барлық жағдайларды кодтауға мүмкіндік бермейді.

Бірнеше биометриялық параметрлер біреуге қарағанда жақсы. Адамның биометриялық идентификациясы сәйкестендіру процесінде көптеген биометриялық параметрлер мен үлгілерді пайдаланудан әлеуетті ұтуы мүмкін деп есептеледі. Шын мәнінде, бұл жүйенің жылдамдығын / бағасын / дәлдігін жақсартады.

Адамдарды тану терроризмнің алдын алады. Қазіргі уақытта бетті тану технологиясы әлі жеткілікті әзірленбеген. Жолаушыларды «іздестіріліп жатқан қылмыскерлердің» тізімімен салыстыру жалған тану жағдайларының көп болуына алып келеді. АҚШ-тағы әуежайлар мен басқа да көпшілік орындарда адамдарды тану үшін бірнеше тест жүргізілді, бұл технологиялар одан әрі зерттеуді талап ететінін көрсетті. Биометриялық параметрлерді пайдалану 100 пайыздық қауіпсіздікті білдіреді. Қарапайым биометриялық мәтчерлер жетілмеген, және бұл статистикалық түрде енгізілген қолдан жасалғандар саны көп болған кезде жүйенің кейбіреулерін жіберіп алмайтынына кепілдік береді. Бірде-бір жүйе 100% қорғалмаған, әсіресе,егер әлеуметтік инженерия, сөз байласу және мәжбүрлеу сияқты түрлі әдістерді қолданатын кәсіби зиянкестер жасайтын шабуылдардың ықтималдығын ескерсе.Биометриялық жүйелер құпиялыққа қауіп төндірмейді. Құпиялылықты технологиямен ұстап тұру мүмкін, бірақ ол кепілдік бермейді. Құпияны сақтау жүйенің мінез - құлық стратегиясына байланысты. Бұл биометриялық параметрлерді пайдалану құпия ақпаратты қорғауға ықпал ете алмайды дегенді білдірмейді. Жақсы әзірленген биометриялық жүйе шын мәнінде пайдаланушыларды қорғайтын ойластырылған рәсімдер негізінде жұмыс істейді.

Биометриялық жүйелер құпиялылықты бұзады. Көптеген адамдар идеалды сәйкестендіруге уәде беретін биометрия шын мәнінде олардың құпиялыққа құқығын бұзады деп қорқады. Биометриялық жүйелер шын мәнінде тоталитарлық қоғамдарда пайдаланылуы мүмкін, біреуі - нақты биометриялық жүйеден, ел саясаты мен заңнамаларға сәйкестендіру рәсімдері құпиялылықты қаншалықты бұзатынына байланысты болады. Практикада биометриялық технологиялар құпия ақпаратты қорғау үшін, мысалы денсаулық жағдайы туралы ақпаратты қорғаудың қосымша тәсілдерін пайдалану жолымен немесе жеке деректерді ашпай аутентификация жүргізу жолымен қолданылуы мүмкін. Бұл тәсілдер әлеуметтік сақтандыру нөмірі, анасының қыз тегі немесе жүргізуші куәлігі бойынша бірдейлендірудің кең таралған әдістеріне қарағанда құпиялылықты сақтауға мүмкіндік береді (бұл мекен - жайға және туған күніне қосымша рұқсат береді).Биометриялық сенсорлар өте қауіпті немесе тіпті зиянды**.** Көптеген биометриялық сенсорлар физикалық байланысты талап етеді, бірақ олармен жанасу ақша, пернетақта, есік тұтқалары және т. б. байланысына қарағанда гигиена тұрғысынан қарағанда аса қауіпті емес.

Биометриялық аутентификация қандай қауіп бар?

1) Техниканың жетілмегендігі. Қандай да бір биометриялық параметрді тексеру үшін «ұсыну» әдетте қарапайым смартфонның көмегімен, ал олардың сапасы әртүрлі болғандықтан, жалған теріс нәтиже болуы мүмкін. Жүйе тіркелгінің шынайы иесінің шынайылығын танудан бас тарта алады — мысалы, саусақтағы кесіндіге байланысты бұл таңбаны «бөтен»деп санайды. Жағдайда пайдаланылады мультифакторная аутентификация және биометриялық деректері қызмет етеді тек бір ғана оның компоненттерін сәйкестендіру алады. Егер 2FA нұсқасы қолданылса, онда бір реттік парольдер емес, атап айтқанда биометрия екінші фактор болып табылады, онда пайдаланушы осы жалған іске қосылудан тіркелгіге кіре алмайды.

2) Техникалық прогрестің жемісін тек заңға бағынушы азаматтар ғана емес. Зиянкестер соңғы технологиялық жаңалықтарды тез меңгеруде. Мысалы, бірнеше жыл бұрын нақты уақыт режимінде адамның фотосуреттерінен бейнеге виртуалды бейнелерді салуға мүмкіндік беретін бағдарлама пайда болды. Оның көмегімен сканерге кіру жүзеге асырылатын объектінің статикалық фотосуретін ғана емес, динамикалық, қозғалыстағы клонды ұсынуға болады. Саусақ ізімен-сол қайғы. Олар көлемді латекс соқырларын немесе қолғапты жасау оңай. Бастапқы үлгі үшін әлеуетті құрбанның алақанының тіпті фотосуреттері жеткілікті.

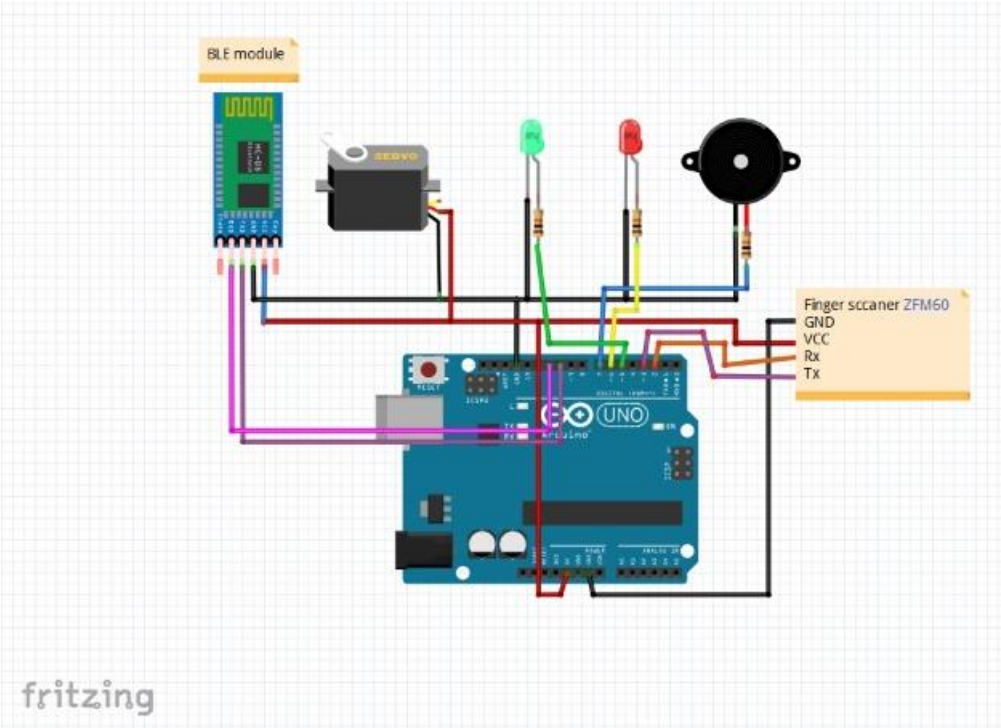
3) Компрометирленген деректерді қалпына келтіру өте қиын. Егер құпия сөз ұстап қалса, оны бірнеше минут ішінде өзгертуге болады. Ұрланған несие немесе OTP токен қалпына келтіру сәл ұзағырақ болады, бірақ мүмкін. Адамға туғаннан тән биометриялық параметрлер бұзылған жағдайда, іс жүзінде жеке басын ұрлау орын алады. Ал оны құпия сөз немесе электрондық карта сияқты оңай өзгертпесің.

2 Техникалық бөлім

2.1 Fritzing бағдарламасы арқылы жобамыздың сұлбасын құру

Fritzing – электр тізбектерін, сұлбаларды және электрондық жабдықтарды виртуалды модельдеу үшін ашық коды бар бағдарламалық қамтамасыз ету. Потсдамда қолданбалы ғылымдар университетінде жасалған.

Fritzing дамуына Processing бағдарламалау тілі мен Arduino жүйесі әсер етті. Бағдарлама арқылы Arduino негізіндегі прототипді сериялық жасау үшін баспа платасының топологиясына түрлендіруге болады. Сондай-ақ, бағдарлама макеттік платалардың көмегімен схемаларды баптауды жеңілдетеді. Қосымша Qt графикалық стекін қолданумен C++ тілінде жазылған.



2.1 сурет - Fritzing бағдарламасы арқылы құрастырылған сұлба

2.2 Arduino микроконтроллерін таңдау

Arduino тақталарының негізгі үлгілері келесі моделдермен көрсетілген:

а) Due – Cortex-M3 ARM SAM3U4E микропроцессоры 32-битті ARM базасының негізінде құрастырылған тақта;

б) Leonardo – ATmega32U4 микроконтроллері негізінде жасалынған тақта;

в) Uno – ATmega328 Arduino базалық платформасының ішіндегі өте танымал нұсқасы;

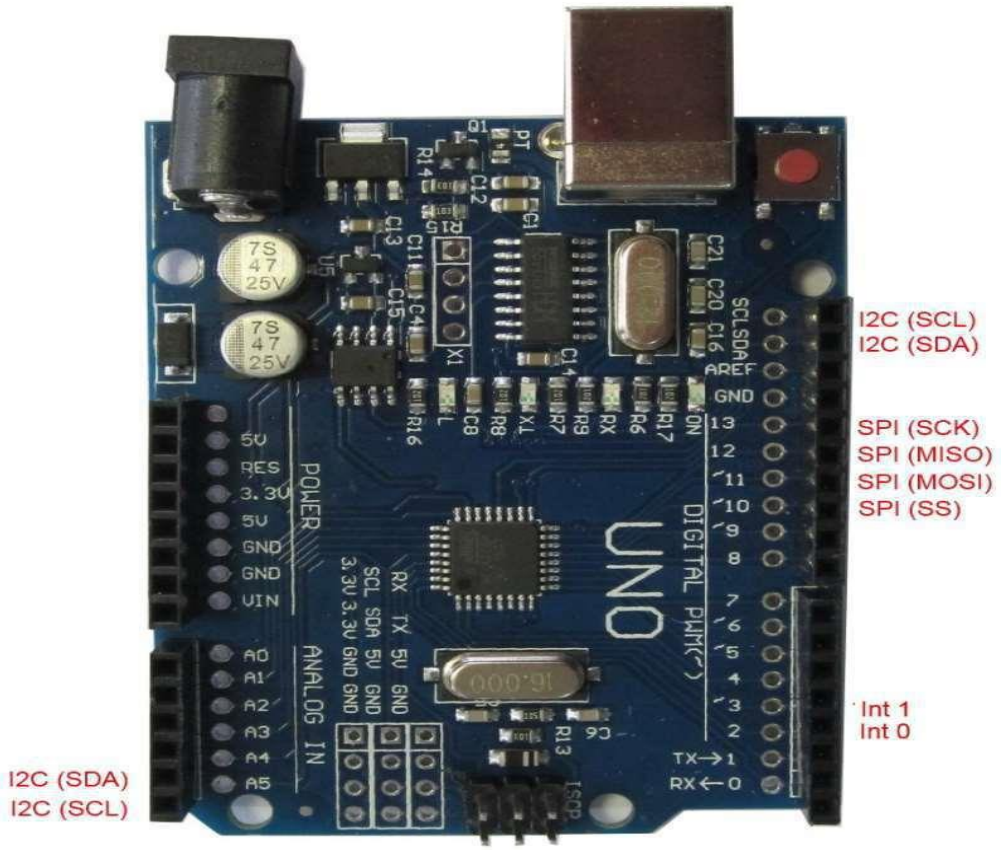
г) Duemilanove – ATmega168 немесе ATmega328 микроконтроллер негізіндегі тақта;

д) Nano – макет түрінде қолданылатын шағын платформа болып табылады;

ж) Mega2560 – негізі ATmega2560 микроконтроллері болып табылатын тақта;

и) Pro – тәжірибелі қолданушыларға арналған платформа.

Мен өз жобамда Arduino Uno ATmega328 микроконтроллерін пайдаландым.

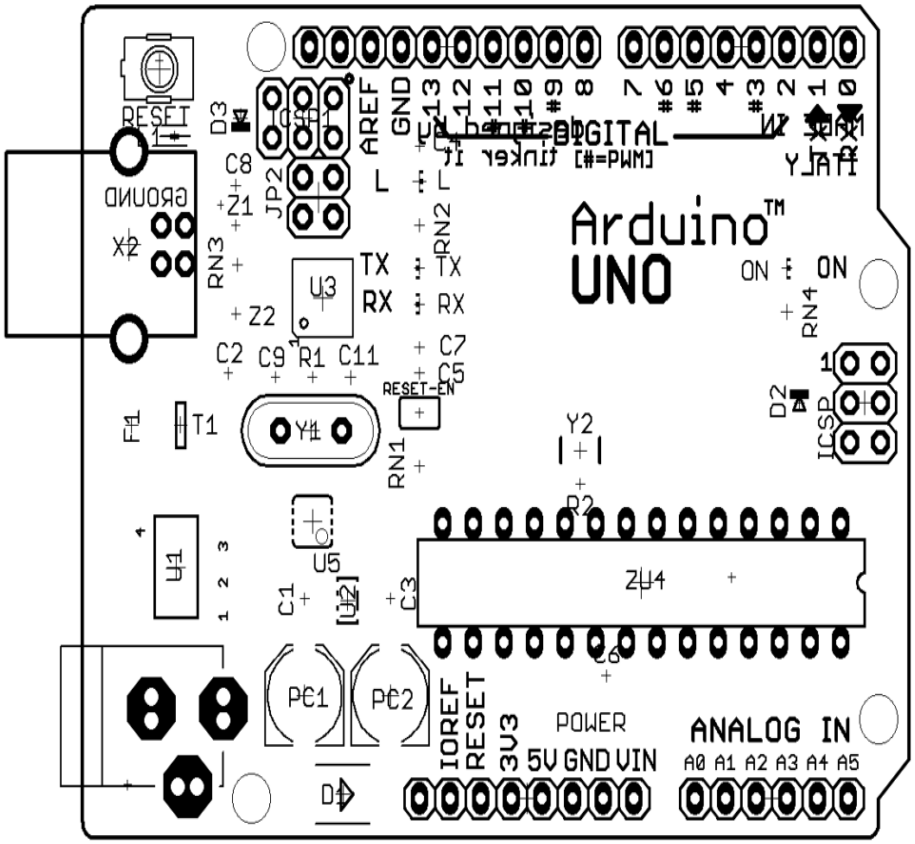


2.2 сурет - Arduino Uno көрінісі

Arduino Uno – бұл микроконтроллерлердің негізгі және ең танымал нұсқасы. Ол кез келген жобалар үшін жеткілікті қуатқа ие. Ол «мама»сияқты бір қатарлы коннекторлар арқылы жұмыс істеу өте ыңғайлы. Әдетте бұл төлем жобаларды прототиплеу үшін пайдаланылады, ал Arduino Nano және Arduino pro сияқты ардуино ұсақ платаларының базасында дайын құрылғыны жинайды. Бұл оңай, себебі тігістер үйлесімді және көп жағдайларда пин нөмірлері әр түрлі емес. Arduino Uno үшін Ethernet shield, motor shield, servo shield және т.б. сияқты көптеген кеңейту платалары бар**.**

2.1 к е с т е – Arduino Uno платасының сипаттамасы

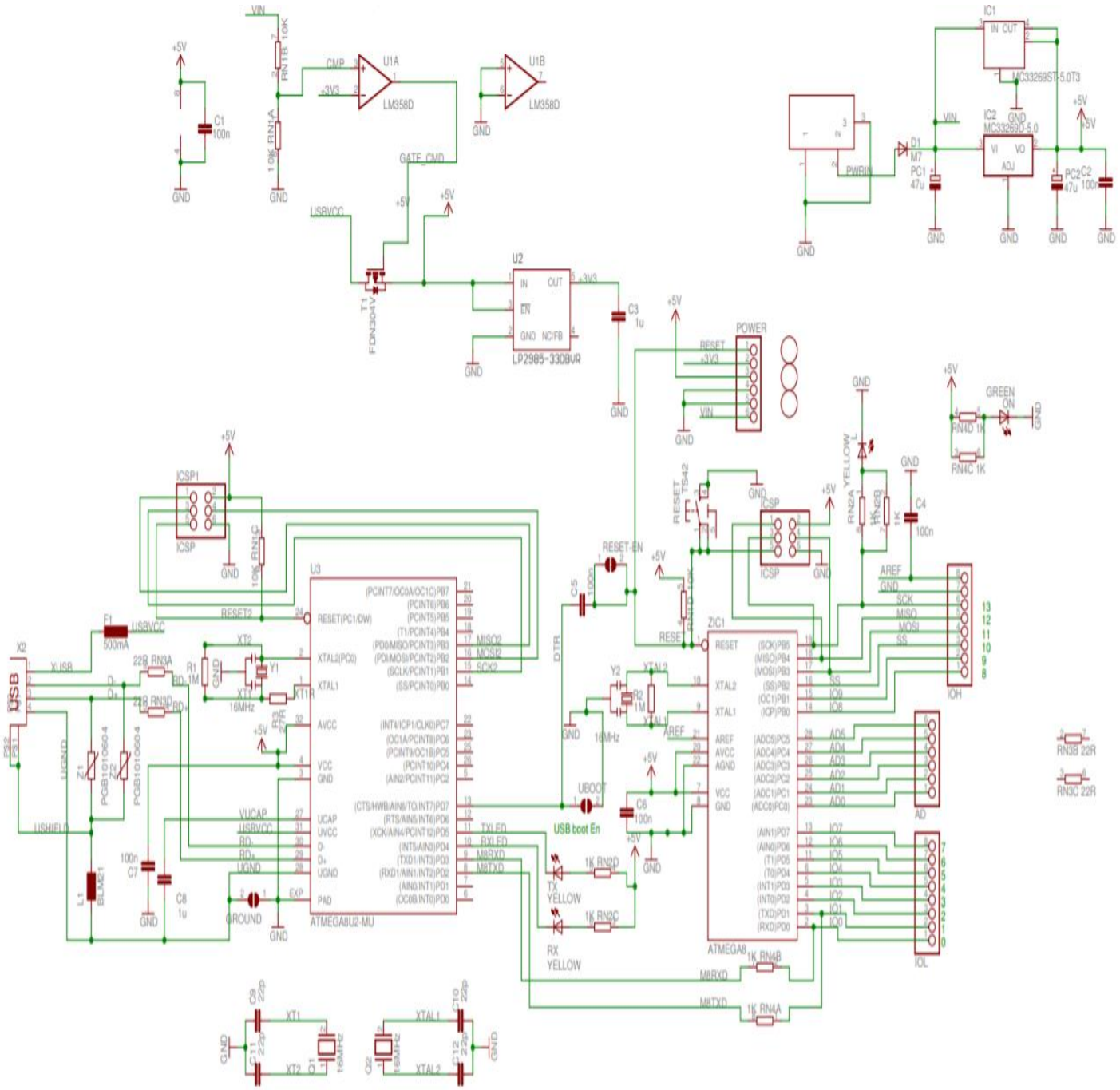
Микроконтроллер	ATmega328
Жұмыс кернеуі	5-20 В
Сыртқы қоректендіру көзі (ұсынылатын)	7-12 В
Ендік-импульстік модуляция	6 цифрлық пин Ендік-импульстік модуляция тұжырымы ретінде пайдаланылуы мүмкін
Сандық кіріс/шығыстары	14
Аналогтық шығыс саны	6
Максималды тоқ күші	бір шығыстан 40 мА және барлық шығыстардан 500 мА.
Flash жады	32 кб
SRAM	2 кб
EEPROM	1 кб
Тактілік жиілік	16 МГц



2.3 сурет - Arduino Uno-ның монтаждық сұлбасы

Arduino Uno платформасында компьютермен, басқа Arduino құрылғыларымен немесе микроконтроллермен байланысу үшін бірнеше құрылғылар орнатылған. ATmega328 0 (RX) және 1 (TX) терминалдары арқылы орындалатын UART TTL (5 V) сериялық интерфейсін қолдайды. Тақтаға орнатылған микросхемалар бұл интерфейсті USB арқылы басқарады, компьютер жағынан бағдарламалар виртуалды COM порты арқылы «байланысады».

Arduino Uno компьютеріңіздің USB порттарын асқын және қысқа тұйықталудан қорғайтын сақтандырғыш бар. Көптеген компьютерлерде өз қорғаныс құралдары бар болса да, сақтандырғыш қосымша сенімділік береді. USB портына 500 мА-ден артық болса, жағдай қалпына келтірілсе, оны қалпына келтіреді.



2.4 сурет - Arduino Uno-ның қағидаттық сұлбасы «(А қосымша)»

Қорек көзі – Arduino Uno USB байланысы немесе сыртқы қуат көзі арқылы қуат ала алады. Қуат көзі автоматты түрде таңдалады.Сыртқы қуат (USB емес) AC/DC кернеу түрлендіргіші (қуат блогы) немесе аккумуляторлық батарея арқылы берілуі мүмкін. Кернеу түрлендіргіш орталық оң полюсті 2.1 мм коннекторы арқылы қосылады. Батареядан сымдар GND және Vin қуат қосқышы шығыстарына қосылады.

Қорек кернеуі 7 В-тан төмен болғанда 5V шығару 5 В-тан кем бере алады, бұл ретте платформа тұрақсыз жұмыс істей алады. 12 В жоғары

кернеуді пайдалану кезінде кернеу реттегіші қызып, ақыға зақым келтіруі мүмкін. Ұсынылған диапазон 7 В бастап 12 В дейін.

Қорек көзінің қорытындылары:

- VIN. Кіріс сыртқы көзден қуат беру үшін пайдаланылады (USB қосқышынан немесе басқа реттелетін қуат көзінен 5 В болмаса). Қуат кернеуін беру осы шығару арқылы жүзеге асырылады.

- 5V. Микроконтроллерді және платадағы компоненттерді қоректендіру үшін қолданылатын реттелетін кернеу көзі. Қуат VIN шығысынан кернеу реттегіші арқылы, немесе USB қосқышынан, немесе басқа реттелетін 5 В кернеу көзінен берілуі мүмкін.

- 3V3. 3.3 в шығысындағы кернеу платада орнатылған реттеуішпен генерацияланатын. Максималды ток тұтыну 50 мА.

- GND. Жерге тұйықтау шықпалары.

Жады – ATmega328 микроконтроллерінде 32 кБ флэш жады бар, оның ішінде 0.5 кБ жүктеушіні сақтау үшін қолданылады, сондай-ақ 2 кБ ОЗУ (SRAM) және 1 Кб EEPROM.(EEPROM кітапханасының көмегімен оқылатын және жазылған).

Кіріс және Шығысы – Uno 14 сандық қорытындылар әрбір pinMode (), digitalWrite (), және digitalRead () мүмкіндіктерін пайдалана отырып, кіріс немесе шығыс ретінде теңшеуге болады . Әрбір қорытынды жүктеме резисторы бар (әдепкі бойынша ажыратылған) 20-50 кОм және 40 мА дейін өткізе алады. Кейбір қорытындылар ерекше функцияларға ие:

Тізбекті шина: 0 (RX) және 1 (TX). Қорытынды TTL деректерін алу (RX) және беру (TX) үшін қолданылады. Бұл тұжырымдар ATmega8U2 USB-to-TTL тізбекті шинасының микросхемасына сәйкес қосылған.

Сыртқы үзіліс: 2 және 3. Бұл қорытындылар үзу шақыруына немесе кіші мәнде, не алдыңғы немесе артқы фронтта немесе мән өзгергенде теңшеуге болады. Толық ақпарат attachInterrupt () функциясының сипаттамасында.

Ендік-импульстік модуляция: 3, 5, 6, 9, 10, және 11. Кез келген тұжырымдар 8 бит ажыратымдылығымен analogWrite () функциясының көмегімен тігуді қамтамасыз етеді.

SPI: 10 (SS), 11 (MOSI), 12 (MISO), 13 (SCK). Бұл тұжырымдар арқылы SPI байланысы жүзеге асырылады, ол үшін SPI кітапханасы қолданылады.

LED: 13. Сандық шығаруға қосылған кіріктірілген жарық диоды 13. Егер қорытындыда жоғары әлеуетке ие болса, онда LED жанып тұрады.

Uno платформасында 6 аналогтық кіріс орнатылған (A0 ретінде белгіленген A5), әрбір 10 бит (яғни, 1024 түрлі мәндерді қабылдай алады). Стандартты қорытындылар жерге қатысты өлшеу диапазоны 5 В дейін

болады, дегенмен AREF шығару және analogReference () функциясы арқылы жоғарғы шегін өзгерту мүмкіндігі бар. Кейбір қорытындылар қосымша функциялар бар:

- I2C: 4 (SDA) және 5 (SCL). Қорытынды арқылы I2C (TWI) байланысы жүзеге асырылады, оны жасау үшін Wire кітапханасы қолданылады.

Платформа шықпаларының қосымша жұбы:

- AREF. Аналогтық кіру үшін тірек кернеуі. AnalogReference () функциясы бар.

- Reset. Шығыс сигналының төмен деңгейі микроконтроллерді қайта жүктейді. Әдетте, Arduino платасындағы батырмаға кіруді жабатын кеңейту платасындағы қайта жүктеу түймесін қосу үшін қолданылады.

Arduino шығысы мен ATmega328 порттары арасындағы байланысқа назар аударыңыз.

Байланыс - Arduino Uno платформасында компьютермен, басқа Arduino құрылғыларымен немесе микроконтроллерлермен байланыс үшін бірнеше құрылғы орнатылған. ATmega328 0 (RX) және 1 (TX) қорытындыларымен жүзеге асырылатын UART TTL (5 В) тізбекті интерфейсін қолдайды. Atmega8u2 микросхемасында орнатылған бұл интерфейсті USB арқылы, компьютер жағындағы бағдарламалар Виртуалды COM порты арқылы төлеммен «қарым-қатынас» арқылы жібереді. ATmega8U2 құрылғысы стандартты USB COM драйверін пайдаланады, ешқандай бөгде драйверлер қажет емес, бірақ Windows-та қосылу үшін ArduinoUNO файлын қажет етеді.inf. Arduino бағдарламасының сериялық Шина (Serial Monitor) мониторингі платформаға қосылған кезде мәтіндік деректерді жіберуге және алуға мүмкіндік береді. Платформадағы RX және TX жарық диодтары деректерді FTDI немесе USB жалғау микросхемасы арқылы тасымалдаған кезде жыпылықтайды (бірақ 0 және 1 қорытындылар арқылы тізбекті жіберуді пайдаланғанда емес).

SoftwareSerial кітапханасымен кез келген Uno сандық қорытындылар арқылы деректерді жүйелі жіберуді жасауға болады.

ATmega328 I2C (TWI) және SPI интерфейстерін қолдайды. Arduino I2C шинасын пайдалану үшін Wire кітапханасы қосылған.

USB қосқышын ток қорғанысы-Arduino Uno-да компьютердің USB портын қысқа тұйықталу токтарынан және аса токтардан қорғайтын өздігінен тоқтайтын сақтандырғыш (автомат) орнатылған. Барлық компьютерлердің осындай қорғауы болса да, бұл сақтандырғыш қосымша кедергіні қамтамасыз етеді. Сақтандырғыш 500 мА астам ток USB порты арқылы өткен кезде іске

қосылады және тізбекті токтың қалыпты мәндері қалпына келтірілгенге дейін ажыратады.

Физикалық сипаттамалары-Arduino Uno келесі өлшемдері бар: ұзындығы 69 мм және ені 53 мм. Arduino Uno салмағы 25 грамм. Платада 4 тесік бар, оны бекіту үшін бетінде. 7 және 8 шығыстардан басқа, Шығыс арасындағы қашықтық 2,5 мм тең. Олардың арасында 4 мм.

2.3 Жобамызға қажетті қосымша бөлшектер

2.3.1 Саусақ ізі сканері ZFM60 V1.4.

Қолдану: саусақ іздерінің есік құлыптары, сейфтер, қару, қаржылық және басқа да қауіпсіздік аймақтары.

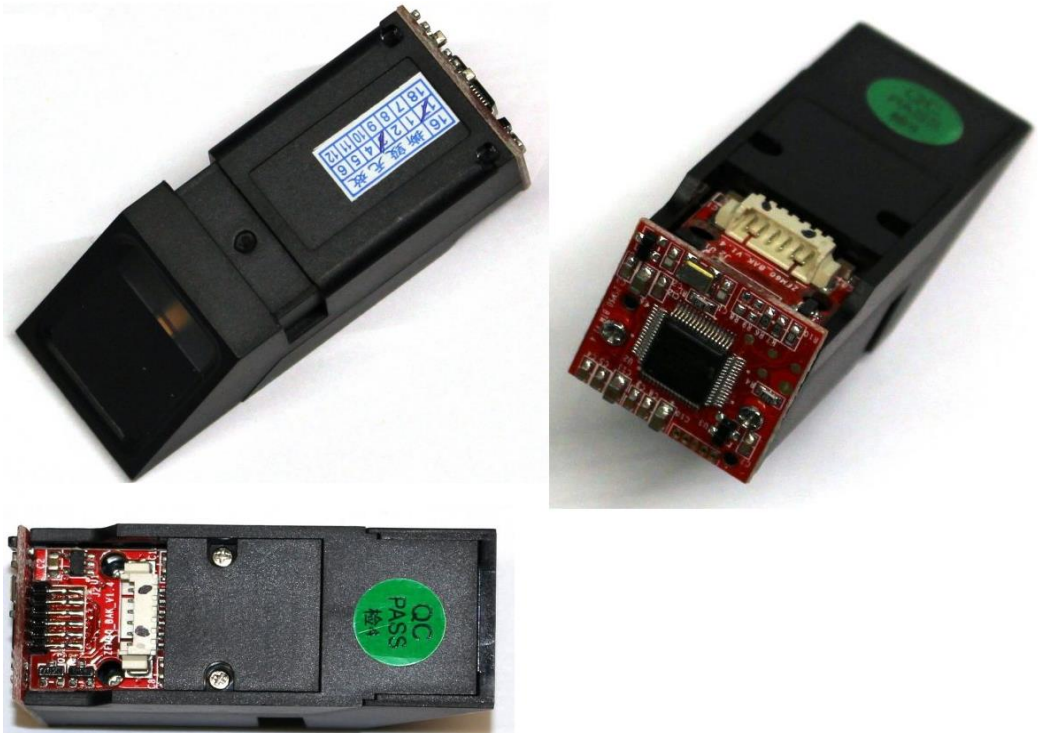
Кіруді бақылау жүйелері, өнеркәсіптік компьютерлер, POS машиналар, жүргізуге оқыту, қатысу және басқа да ұқсас салаларю .Жеке меншік клубтар, басқару үшін бағдарламалық қамтамасыз ету, лицензиялау және басқа басқару салалары.Медициналық қызмет алушылар, зейнеткерлер саусақ іздерін және басқа да қаржы облыстарын алады, төлейді.

Қосылымдар:

- Pin #2 сенсорында (жасыл сым);
- Pin #3 arduino (ақ сым);
- 5 В қосылу датчигіне (қызыл сым);
- GND connect sensor (қара сым).

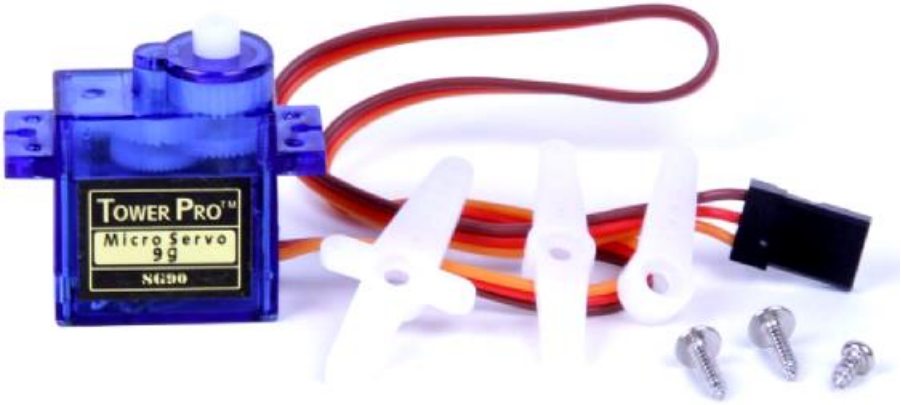
2.2 к е с т е – Саусақ ізі сканері ZFM60 V1.4 негізгі сипаттамалары

Қуат кернеуі	3,8-7В
Саусақ іздерін енгізу уақыты	<0,5 секунд
Терезе ауданы	15 × 17 мм
Іздеу уақыты	<240 MS (орташа 1: 220)
Хост интерфейсі	UART (TTL логикалық деңгейі)
Деректер жылдамдығы (UART)	(9600 × N) bps, мұнда N = 1 ~ 12 (әдепкі бойынша N = 6, іе 57600bps)
Іздеу әдісі	(1: N)
Тән Файл	384 байт
Үлгі файлы	786 байт
Тиісті әдіс	салыстыру әдісі (1: 1)
жұмыс тогы	<60мА
Жалған қабылдау коэффициенті (FAR)	<0.001% (қауіпсіздік деңгейі 3)
Бас тарту коэффициенті (FRR)	<1.0% (қауіпсіздік деңгейі 3)



2.5 сурет - Саусақ ізі сканері ZFM60 V1.4 көрінісі

2.3.2 Сервожетек SG-90.



2.6 сурет - Сервожетек SG-90 көрінісі

2.3 к е с т е – Сервожетек SG-90 негізгі техникалық сипаттамалары:

Редуктор матералы	Нейлон
Қуат кернеуі	3-5 В
Білікке(вал) күш	1.2 кг / см (4.8 В); 1.6 кг / см (6.0 В)
Өлі импульс ені	2 мс
Өлшемі	Микро (22 мм х 11.5 мм х 27мм)
Салмағы	9 грамм
Бұрылу бұрышы	160°

Сервожетек (лат. Servus – құл, көмекші, жұм), немесе қадағалаушы жетек-сырттан берілген параметрлерге сәйкес ішкі теріс кері байланыс арқылы күйін автоматты түзетумен механикалық жетек.

Сервожетек құрамында датчигі (жағдайы, жылдамдығы, күші және т.б.) және жетекті басқару блогы (электрондық схема немесе тарту механикалық жүйесі) бар, берілген сыртқы мәнге (басқару тұтқасының жағдайы немесе басқа жүйелерден сандық мәні) сәйкес датчикте (және тиісінше құрылғыда) қажетті параметрлерді автоматты түрде қолдайтын механикалық жетектің (құрылғының, жұмыс органының) кез келген түрі болып табылады.

Басқаша айтқанда, сервопривод болып табылады «автоматты дәл орындаушы» – получая кіру мәні басқарушы параметр (нақты уақыт режимінде), ол «өз күшімен» (негізге ала отырып, көрсеткіштер датчик) ұмтылады құру және қолдау, бұл мәні шығу атқарушы элемент.

Сервожетектерге санатына сияқты, кері байланысы теріс түрлі реттеуіштер мен күшейткіштер жатады, мысалы, басқару элементтерінің қол жетегінің гидро , электр , пневмоусилаторлары (атап айтқанда, тракторлар мен автомобильдердегі рульдік басқару және тежегіш жүйесі), алайда «сервожетек» термині көбінесе (және осы бапта) басқару элементтері мен жұмыс органдарын жетекке арналған автоматты жүйелерде қолданылатын жағдай бойынша кері байланысы бар электр жетегін белгілеу үшін пайдаланылады.

Сервожетектер қазіргі уақытта мынадай салалардың жоғары өнімді жабдықтарында қолданылады: машина жасау; автоматты өндіріс желілері: сусындар, буып - түю, құрылыс материалдары, электроника және т. б., көтергіш-көлік техникасы; полиграфия; ағаш өңдеу, тамақ өнеркәсібі.

Сервоприводты қосу схемасы:

- қоңыр сым - жер (Ground, Arduino платасында GND шинасынақосылады;
- қызыл сым - қуат + 5 V (Arduino платасында 5V шинасына қосылады);

- сары сым басқару сигналы (Arduino сандық пинасына қосылады).

2.3.3 Буззер (динамик).

Буззер немесе дыбыс сигналы-механикалық, электромеханикалық немесе пьезоэлектрлік (қысқа пьезо) болуы мүмкін дыбыстық сигнал құрылғысы. Буззерлер мен beepers-тің типтік пайдасы дабыл сигналын, уақыт белгілерін, және тышқанды басу немесе пернені басу ретінде тұтынушының кіріс сигналын растауды қамтиды.

2.7 сурет - Буззер көрінісі мен сұлбасы

2.4 к е с т е- Буззер негізгі сипаттамалары

Жұмыс кернеуі	5В
MAX. номиналды ток	10мА
Тональдылығы	Біртоналды
Жұмыс температурасы	-10 бастап +70°С дейін
Салмағы	3 грамм

2.3.4 Bluetooth модуль JDY-10.

JDY-10 ашық тарату модулі Bluetooth 4,0 стандарты негізінде, жұмыс жиіліктік диапазоны 2,4 ГГц диапазоны, gfsk модуляция режимі, максималды тарату қуаты 8 дБ құрайды, максималды тарату қашықтығы 80 м құрайды,

төмен энергия тұтыну, аз өлшемді, күшті сигнал, тұрақты деректер беру және басқа да сипаттамалар.

2.8 сурет - Bluetooth модуль JDY-10 көрінісі

Жұмыс кернеуі 1,9-3,6 В.
Жұмыс температурасы: - 40-85 °C.
Максималды тарату қуаты: + 8 дБм.
Антенналар: PCB орнатылған антенна.
Сезімталдықты алу: - 92dbm.
Wake режимі: 9MA.
Суспензиялар режимі: 30-800 мкА.
Терең ұйқы режимі: 5 МБ.

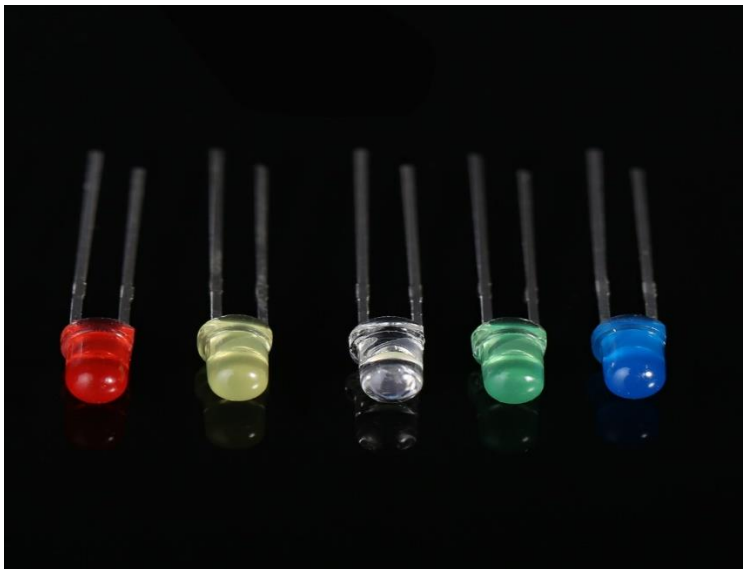
2.5 к е с т е- Bluetooth модуль JDY-10 негізгі сипаттамалары

Жұмыс кернеуі	1,9-3,6 В
Жұмыс температурасы	- 40-85 °C
Максималды тарату қуаты	+ 8 дБм
Антенналар	PCB орнатылған антенна
Сезімталдықты алу	- 92дБм
Wake режимі	9MA
Суспензиялар режимі	30-800 мкА
Терең ұйқы режимі	5 МБ

2.3.5 Жарық диоды.

- төмен жылу, энергия үнемдеу, төмен энергия тұтыну, ұзақ қызмет ету мерзімі;
- дәстүрлі жарық көздері үшін үздік ауыстыру;

- жарық әшекейлері, алаулар, ойыншықтар мен сыйлықтар, автомобиль әшекейлері, жарнаманың жарық қорабы, сигнал индикаторы және т. б.;
- саны: 2.
- түсі: жасыл, қызыл.
- өлшемі: 3 мм.
- қуыс ұзындығы: 17 мм-19 мм.
- бұрылу бұрышы: 120 °.
- ток: 20mA.
- кернеу: 3 В.



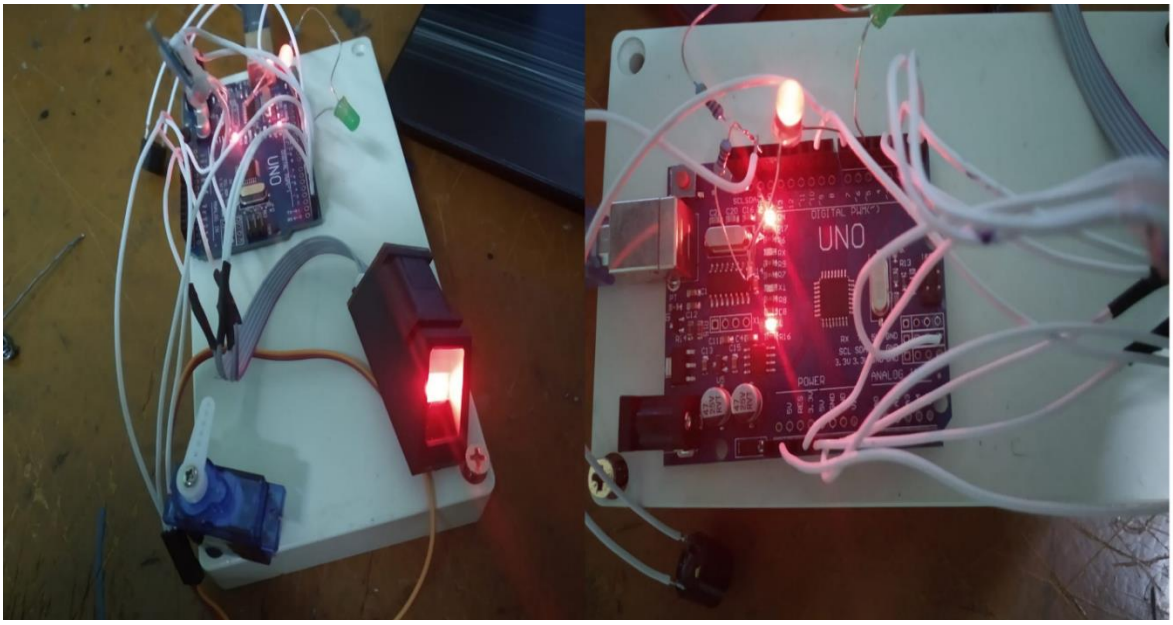
2.9 сурет - Жарық диодының көрінісі

2.3.6 10 кОм-дық резистор.

2.6 кесте-Резистор сипаттамасы

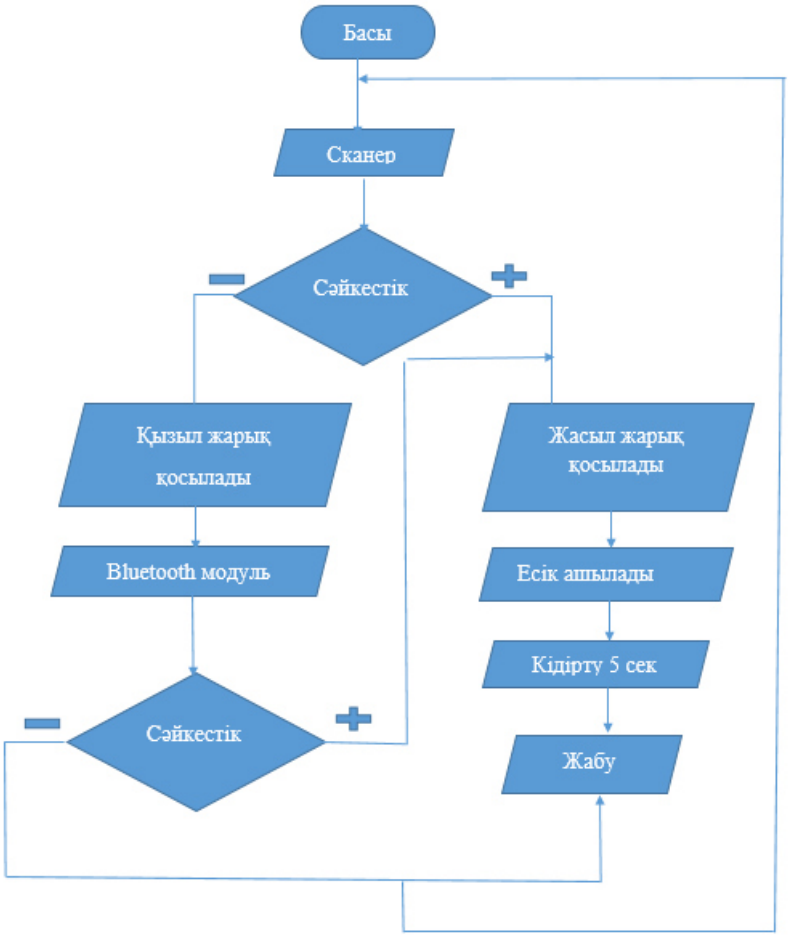
Кедергісі	10 кОм
Рұқсат беру	1%
Сәлемдеме(посылка)	Осьтік
Номиналды қуаты	1Вт
Түрі	Метал резистор

2.10 сурет - Резистордың көрінісі

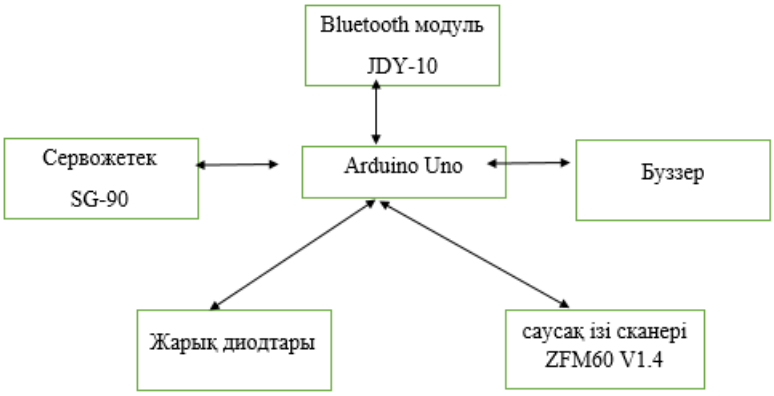


2.11 сурет - Fritzing бағдарламасы арқылы құрастырылған сұлбаны жинау барысында

2.4 Жобамыздың құрылымдық және блок-сұлбасы



2.12 сурет - Жобамыздың блок-сұлбасы



2.13 сурет - Жобамыздың құрылымдық сұлбасы

3 Бағдарламалық бөлім

3.1 Жобамызға қолданылатын бағдарлама

Arduino IDE - Arduino платформасы үшін өз бағдарламаларын жазуға мүмкіндік беретін пайдаланушылар үшін бағдарламалық жасақтама.

3.1 сурет - Бағдарламаның интерейсі

Бағдарлама интерфейсі осылай көрінеді. Бағдарламаларды Ардуино үшін арнайы әзірленген C AVR оңайлатылған тілде жазуға болады, шын мәнінде бұл Wiring деп аталатын кітапханалардың жиынтығы, сондай-ақ таза C AVR. Оны пайдалану кодты жеңілдетеді және оның жұмысын тездетеді.Терезенің жоғарғы жағында әдеттегі мәзір бар, онда файлды ашуға, баптауларды таңдауға, сіз жұмыс істейтін төлемді (Uno, Nano және көптеген басқа) таңдауға және дайын код үлгілері бар жобаларды ашуға болады. Төменде тігіспен жұмыс істеу үшін түймелер жиынтығы орналасқан, пернелердің тағайындалуы төменде суретте көресіз.

3.2 сурет - Бағдарламаның баптаулары

Терезенің төменгі бөлігінде-жоба туралы, кодтың жай-күйі, тігістер және қателердің болуы туралы ақпаратты шығару аймағы.

3.2 Arduino UNO-ға жүктелетін бағдарлама листингі

```
#include <Adafruit_Fingerprint.h>
#include <SoftwareSerial.h>
#include <Servo.h>
int getFingerprintIDez();
Servo myservo;
SoftwareSerial mySerial(2, 3);
SoftwareSerial BSerial(12, 13); // RX, TX
bool f=false;
int pop=0;
Adafruit_Fingerprint finger = Adafruit_Fingerprint(&mySerial);
String input_string = «»;
```

```
void setup()
{
while (!Serial);  // For Yun/Leo/Micro/Zero/...
Serial.begin(9600);
BSerial.begin(9600);
Serial.println(«Adafruit finger detect test»);
// set the data rate for the sensor serial port
finger.begin(57600);
if (finger.verifyPassword()) {
Serial.println(«Found fingerprint sensor!»);
} else {
Serial.println(«Did not find fingerprint sensor :(«);
while (1);
}
Serial.println(«Waiting for valid finger...»);
pinMode(7,OUTPUT); //buz
pinMode(0,OUTPUT);  //red
pinMode(1,OUTPUT); //green
myservo.attach(9);
myservo.write(65);
digitalWrite(4,0);  //green LED
digitalWrite(5,1);
}
void loop() // run over and over again
{
getFingerprintID();
if(f==true){
while (BSerial.available() > 0) {
char c = BSerial.read();
if (c == '\n') {
Serial.print(«Input_string is: «);
Serial.println(input_string);
input_string = «««;
} else { input_string += c;}
if(input_string==«open»){   // open the door
digitalWrite(4,1);  //green LED
digitalWrite(5,0);  //red LED
myservo.write(40);
```

```
digitalWrite(7,1);
delay(1000);
digitalWrite(7,0);
delay(3000);
digitalWrite(4,0);  //green LED
digitalWrite(5,1);  //red LED
myservo.write(70);
}
if(input_string==«AccesFingerOpen»){
mySerial.listen();
digitalWrite(7,1);
delay(50);
digitalWrite(7,0);
delay(50);
digitalWrite(7,1);
delay(50);
digitalWrite(7,0);
delay(50);
digitalWrite(7,1);
delay(50);
digitalWrite(7,0);
delay(50);
digitalWrite(7,1);
delay(50);
digitalWrite(7,0);
}
if(input_string==«AccesFingerClose»){
BSerial.listen();
}
}
}
}
uint8_t getFingerprintID() {
uint8_t p = finger.getImage();
switch (p) {
case FINGERPRINT_OK:
Serial.println(«Image taken»);
break;
```

```
case FINGERPRINT_NOFINGER:
//Serial.println(«No finger detected»);
return p;
case FINGERPRINT_PACKETRECIEVEERR:
Serial.println(«Communication error»);
return p;
case FINGERPRINT_IMAGEFAIL:
Serial.println(«Imaging error»);
return p;
default:
Serial.println(«Unknown error»);
return p;
}
// OK success!
p = finger.image2Tz();
switch (p) {
case FINGERPRINT_OK:
Serial.println(«Image converted»);
break;
case FINGERPRINT_IMAGEMESS:
Serial.println(«Image too messy»);
return p;
case FINGERPRINT_PACKETRECIEVEERR:
Serial.println(«Communication error»);
return p;
case FINGERPRINT_FEATUREFAIL:
Serial.println(«Could not find fingerprint features»);
return p;
case FINGERPRINT_INVALIDIMAGE:
Serial.println(«Could not find fingerprint features»);
return p;
default:
Serial.println(«Unknown error»);
return p;
}
// OK converted!
p = finger.fingerFastSearch();
if (p == FINGERPRINT_OK) {
```

```
Serial.println(«Found a print match!»);
} else if (p == FINGERPRINT_PACKETRECIEVEERR) {
Serial.println(«Communication error»);
return p;
} else if (p == FINGERPRINT_NOTFOUND) {
Serial.println(«Did not find a match»);
/**/
digitalWrite(7,1);
delay(200);
digitalWrite(7,0);
delay(200);
digitalWrite(7,1);
delay(200);
digitalWrite(7,0);
if(pop>2){
digitalWrite(7,1);
delay(500);
digitalWrite(7,0);
f=true;
BSerial.listen();
Serial.println(«Use BLE please»);
pop=0;
}else
{pop++;}
Serial.print(«popitka # «);
Serial.println(pop);
/**/
return p;
} else {
Serial.println(«Unknown error»);
return p;
}
// found a match!
Serial.print(«Found ID #»); Serial.print(finger.fingerID);
Serial.print(« with confidence of «); Serial.println(finger.confidence);
/**/
if(finger.fingerID==1){
pop=0;
```

```
digitalWrite(4,1);  //green LED
digitalWrite(5,0);  //red LED
myservo.write(40);
digitalWrite(7,1);
delay(1000);
digitalWrite(7,0);
delay(3000);
digitalWrite(4,0);  //green LED
digitalWrite(5,1);  //red LED
myservo.write(65);}
}
// returns -1 if failed, otherwise returns ID #
int getFingerprintIDez() {
uint8_t p = finger.getImage();
if (p != FINGERPRINT_OK)  return -1;
p = finger.image2Tz();
if (p != FINGERPRINT_OK)  return -1;
p = finger.fingerFastSearch();
if (p != FINGERPRINT_OK)  return -1;
// found a match!
Serial.print(«Found ID #»); Serial.print(finger.fingerID);
Serial.print(« with confidence of «); Serial.println(finger.confidence);
return finger.fingerID;
}
```

4 Өміртіршілік қауіпсіздік бөлімі

Мақсаты: Мен өз дипломдық жобамда оптикалық ZFM60 V1.4 саусақ ізі сканерін пайдаландым.Мен өміртіршілік қауіпсіздік бөлімінде оптикалық саусақ ізі сканерінің адам өміріне қауіпсіз екенін дәлелдеймін.

4.1 Оптикалық әдіс

Бұл әдіс бұзылған толық ішкі шағылысу әсерін пайдаланады (Frusted Total Internal Reflection). Екі ортадағы бөлім шекарасына жарық түскен кезде жарық энергиясы екі бөлікке бөлінеді-біреуі шекарадан көрінеді, екіншісі шекара арқылы екінші ортаға өтеді. Көрсетілген энергияның үлесі жарық ағынының құлау бұрышына байланысты. Осы бұрыштың кейбір шамасынан бастап, барлық жарық энергиясы бөлім шекарасынан көрінеді.

Бұл құбылыс толық ішкі көрініс деп аталады. Жарық шоғырының толық ішкі шағылысу нүктесінде тығыз емес оптикалық орта (саусақтың беті) жанасқан жағдайда осы шекара арқылы өтеді. Осылайша, шекарадан толық ішкі көрінудің белгілі бір нүктелеріне түскен, саусақтың папиллярлы өрнегі жоқ жарық шоғыры ғана көрінеді. Саусақтың бетінің алынған жарық суретін басып алу үшін арнайы сурет датчигі қолданылады.

Оптикалық сканерлер нарықта бірінші болып пайда болды. Ол басып алғаннан кейін жадында бар үлгімен ерекше алгоритмдерді пайдалана отырып салыстырылатын іздердің өзіндік суретіне негізделген. Тән ерекшеліктер анықталған жағдайда таңбаның сәйкес келуі немесе сәйкес келмеуі туралы шешім қабылданады.

Яғни, бұл әдіс - саусақ ізін тек суретке түсіріп алады. Сондақтанда оптикалық ZFM60 V1.4 саусақ ізі сканеріміз адам өміріне зиян емес екенін дәлелденді.

4.2 Samsung Galaxy S8 және S8+ смартфондары көздің биометриясымен салыстыру

Ал бұл әдіспен салыстыруға 2017 жылдың сәуір айында шығарылған Samsung Galaxy S8 және S8+ смартфондары көздің биометриясы арқылы мобильді құрылғының құлпын ашуға мүмкіндік беретін көздің торлы қабығының кіріктірілген сканерімен жабдықталған. Дегенмен, тақырыптық форумдардағы пікірлерді талдасаңыз, онда осы мобильді құрылғылардың көптеген пайдаланушылары флагмандарды сатып алғаннан кейін көрудің маңызды проблемаларының пайда болуына шағымданады.Galaxy S8 және S8+ бірнеше жүздеген иелерінің хабарламалары бойынша көздің торлы қабығының биометриялық сканерін қолдану ыңғайсыздық пен көру органдарының тітіркенуін тудырады. Кейбір пайдаланушылар Samsung Pay арқылы құрылғыны

құлпын ашу және сатып алу төлеу осы әдісін пайдалана бастағаннан кейін бірнеше аптадан кейін, жаңа модульді пайдаланғаннан кейін көз ауыруы мен бас айналуы туралы шағымдана бастады.Нәтижесінде, көрудің пайда болған проблемаларына шағымданатын барлық адамдар көздің торлы қабығының сканерін пайдаланудан бас тартып, өзінің таңдауын дәстүрлі сәйкестендіру тәсіліне – дактилоскопиялық модуль арқылы тоқтады. Samsung компаниясы бұл жағдайға түсініктеме беруден бас тартады, бірақ ол өз көз арқылы құрылғыны құлпын ашу технологиясы мүлдем қауіпсіз екенін айтады. Зерттеушілердің тобы жүргізілген тексерулерден кейін Samsung Galaxy S8 және S8+ смартфондарына кіріктірілген инфрақызыл сәуле шығаратын көздің мөлдір қабығының сканері көру органдарын тітіркендіруге ұшыратады – басты ақуыз қатты зардап шегеді деген қорытындыға келді. Көруі бар генетикалық проблемаларға ұшырайтын барлық адамдар қымбат смартфонды осындай тәсілмен блоктан шығару кезінде ыңғайсыздық сезіне бастайды.Galaxy S8 немесе S8+ көз қабықшасының сканерін үнемі пайдаланатын адам айтарлықтай жарақат алуы мүмкін, содан кейін катаракта өседі. Көз бұршағына теріс әсер ететін ИҚ-сәуленің кінәсі. Егер көзіңізді сақтағыңыз келсе, құрылғыны қорғау әдісін қолданудан бас тарту керек.

Инфрақызыл сәуленуден келетін зиян: адамның ми тіні инфрақызыл қысқа толқындардың әсеріне ұшыраса, әсер басқаша болады. Бұл жағдайда күн сәулесі сияқты құбылыс бар. Бұл өзін-өзі сезінудің нашарлауынан көрінеді: адамда ауырсынуға, бастың айналуына, Пульс пен тыныс алудың жиілеуіне, көздегі қараңғылыққа шағымданады, ал аса ауыр жағдайларда талу орын алуы мүмкін. Егер адам одан әрі сәулеленуге ұшыраса, онда денені жеңуге күш жетпей қалады. Нәтижесінде ми тіндері мен қабығының ісінуі пайда болады, энцефалит пен менингит белгілері пайда болады. Мұның бәрі адамның өмір сүру сапасын айтарлықтай нашарлатады.Әсіресе инфрақызыл қысқа толқындар көзге теріс әсер етеді. Егер бұл әсер тым ұзақ болса, инфрақызыл катаракты дамыту қаупі бар. Инфрақызыл толқындар жүрек-қантамыр жүйесіне де зиян келтіруі мүмкін. Бұл әсіресе инфрақызыл сәулеленудің жоғары көрсеткіштері бар үй-жайларда жұмыс істейтін ыстық цех қызметкерлерінің жұмысына қатысты. Ақыр соңында бұл жүрек және ас қорыту органдары ауруларының дамуына әкеледі.Статистикаға сәйкес, металлургия өнеркәсібіндегі адамдар шамамен 23,6% - да жүрек ауруына байланысты мүгедек болады. Ыстық цехтарда бір жыл жұмыс иммундық жүйенің айтарлықтай әлсіреуі үшін жеткілікті. Сондықтан осы кезеңнен кейін көптеген жұмысшылар суық тию белгілері пайда болады.

4.3 Qualcomm компаниясының ультрадыбыстық саусақ ізі сенсорымен (3D Sonic Sensor) салыстыру

Тағыда бір әдісті салыстыра кетсек: ол Qualcomm компаниясынан ультрадыбыстық саусақ ізінің сенсоры (3D Sonic Sensor).

Ультрадыбыстық адам ағзасына әсері**:** Ультрадыбыстың әсері үшін жүйке жүйесінің зақымдануы тән. Ұзақ уақыт бойы ультрадыбыстық жабдыққа қызмет көрсететін тұлғалар бас ауруына, жалпы әлсіздікке, ұйқының бұзылуына, тітіркенгіштікке, жадының нашарлауына, дыбыстарға сезімталдықтың жоғарылауына, құлаққа салыну сезіміне, кейде аяқ-қолдың суық болуына, бозаруы ұстамаларына немесе керісінше, бет қызаруына, талуға шағымданады. Диспепсиялық сипаттағы шағымдар жиі кездеседі. Клиникалық зерттеуде астениялық немесе астеновегетативті синдром байқалады. Кейде диэнцефальды бұзылулар байқалады (арықтау, субфебрилитет, висцералды криз, галлюцинация түріндегі пароксизмальді ұстамалар)

Ультрадыбыстың әсерінен болатын өзгерістердің 3 сатысы бар:

- бастапқы (нерв жүйесінің функционалдық өзгерістері, эндокриндік қозғалыстар, вестибулярлық бұзылулар, вегетативті полиневрит - барлық өзгерістер жарамсыз);

- орташа айқын білінетін (айқын білінетін түрдегі сол өзгерістер, диэнцефалдық емес дәрежедегі бұзылулар);

- айқын (диэнцефальды криздер, орталық нерв жүйесінің органикалық зақымдануының жеңіл шашыраңқы симптоматикасы).

Жаңа ғылыми зерттеу жүкті әйелдерде жүргізілетін ультрадыбыстық тексеру ұрықтың ми жасушаларының дамуына кедергі келтіруі мүмкін екенін көрсетті. Зерттеу осы зерттеудің тамаша беделіне ие болды. Йель университетінің ғалымдары ультрадыбыстық толқындар тумаған балаға, атап айтқанда, оның жүйке жасушаларына теріс әсер ететінін дәлелдеді, деп хабарлайды «die Zeit» - неміс газеті.

Топ беделді нейробиологтың басшылығымен жүкті тышқандарды жүктіліктің соңғы үш күні ішінде әр түрлі ұзындықтағы ультрадыбыстық тексеруге ұшыратты - әдетте адамдарды ультрадыбыстық тексеру үшін пайдаланылатын аспаптың көмегімен. Содан кейін жаңа туған тінтуір миында ғалымдар үш күн бойы туар алдында әдетте мидың белгілі бір бөлігіне қозғалатын таңбаланған нейрондарды іздеген.

Жалпы, жаңа туған мишат миы ешқандай айқын ауытқулар болған жоқ, оның өлшемдері стандартты болды. Бірақ туар алдында 30 минут және одан да көп ультрадыбыстық тексеруге ұшыраған барлық жануарларда, туғаннан

кейін Е16 нейрондар деп аталатын бас миының қабығының тиісті орнына ауыспады. Олар сұр заттың терең қабаттарында «адасқан» сияқты. «Адасқан» жасушалардың саны ультрадыбыстық жүктемемен бірге өсті, кейбір нейрондар кейінірек төменгі орналасқан ақ затта да табылды. Бұл жасушаларда дұрыс позицияланған нейрондардың белгілі бір химиялық сипаттамалары жоқ, ал мұндай жүйке жасушалары табиғатқа арналған функцияны орындай алмайды.

Шын мәнінде, ДНҚ деформациясы бар жасушалардың толық мутациясы бар.

Ультрадыбыстық зерттеу жоғары жиіліктегі дыбыстық толқындарды пайдаланады, олар сұйық орта арқылы өтеді, тығыз объектіден, бұл жағдайда — бала. Көрсетілген толқындар датчиктермен түрлендіріледі және сурет-қаңқасы және баланың ішкі органдары-монитордың экранында пайда болады. ультрадыбыстық зерттеу жүкті әйелдің арнайы даярлығын талап етпейді. Тек ерте кезеңдерде, әлі де аз болса, әйел қуық толтырылған зерттеуге келуді сұрайды, сурет жеткілікті анық болуы үшін. Әйел кушеткаға жатады, ішті жалаңаштайды, оны дыбыс өткізгіш гельмен майлайды және аспаптың датчигімен жүргізеді. Барлық рәсім он минутқа созылады. Анамның қалауы бойынша, ол экранға көре алады, бірақ жақсы маманның түсіндірмесіз экранда не бейнеленгенін түсіну өте қиын.

Ана құрсағындағы балалар қарқынды қозғалыспен жауап бере отырып , бұл тексеруге қатты жауап бергенін ешкім айтпайды. Бұл ерекшелігі тіпті көптеген «ақылдылар» жүктілік кезінде сынақ ретінде пайдаланылады, анасы кенеттен оның баласы ұзақ қозғалмайды деп қорқады. Ультрадыбыстық зерттеу ұрықтың қозғалысын ынталандырады және оның жүрек соғуын жеделдетеді.

Бала жағымсыз әсерді сезінеді және қорғануға тырысып, сәулеге рефлекторлық жауап береді. Әуесқойлық-баланы күмәнді мақсаттарда, мысалы, баланың жынысын тану үшін ықтимал қауіп төндіру үшін маңызды себеп жеткіліксіз.

АҚШ-та ұлттық денсаулық институты барлық жүкті әйелдер үшін міндетті ультрадыбыстық зерттеу мақұлдамады. Зерттеу жүргізген: Гаряева П. П.

Генотип бойынша соққы. Зиянсыз деп саналған ультрадыбыс генетикалық аппаратты зақымдауы мүмкін . Ресей Ғылым академиясының теориялық мәселелер бөлімінің аға ғылыми қызметкері Петр Петрович Гаряевтің жетекшілігімен Мәскеу зерттеушілері осындай қорытындыға келді.

Мойындау керек, - дейді Гаряев, - бұрын біз генетиканың заңдарын адамдарға зиян келтіруде қолдануға болатынынан қорқатынбыз. Ал бұл баяғыда дәрігерлер. Олар адамның генетикалық аппаратына әсер етеді. Қазір адамдарға қатысты осы кең ауқымды эксперименттің алыс салдарын елестету қиын.

Көзқарас жақында басталды. Биология ғылымдарының кандидаты Петр Петрович Гаряев және физика-математика ғылымдарының кандидаты Андрей Александрович Березин өз алдына мақсат қойды: ағзаның дамуын басқаратын қасиетті тірі материя — толқындық генге ену. Табиғат болашақ ұрпақ үшін тұқым қуалаушылық бағдарламаларды сақтау үшін кез келген шабуылдан геномды қорғайды. Бірақ ғалымдар оларға өз түзетулерін енгізуді — «ДНҚ мәтініне»жаңа ақпаратты енгізуді шешті.

Жасушалардан бөлінген ДНҚ молекулалары әртүрлі сигналдарды шығарады. Бұл ДНҚ командасы бойынша дамитын барлық тіндердің, органдар мен жүйелердің «әуендері» бар, мүмкін, өмірдің нақты симфониясы. Бірақ ғалымдар әзірге осы акустикалық тербелістердің спектрін анықтай алады. Олар соншалықты көп және олар соншалықты әлсіз, оларды ажыратуға аса сезімтал аппаратура ғана қабілетті.

Лазердің Гелий-неон сәулесі ДНҚ тербелмелі молекулаларына бағыттайды-олардан көрініс табады, Жарық шашырайды және оның спектрі сезімтал аспапты жазады. Мұндай өлшеу жүйесі фотондар корреляциясының спектроскопиясын орнату деп аталады.

Гаряев пен Березин кюветке ДНҚ молекулаларының сулы ерітіндісін салып, оны ультрадыбыс генераторымен өңдеді. Олар акустикалық тербелістердің жиілігін атаудан бас тартты, тек кейбір обертон жұқа ысқырық сияқты құлақты естуге болатынын байқады. Бірақ зерттеушілер эксперимент нәтижелерін жасырмайды-керісінше, олар туралы көптеген адамдар туралы айтып беруді өз парызы деп санайды.

Генератормен әсер еткенге дейін ДНҚ молекулалары кең диапазонда дыбыстар шығарған: бірліктерден жүздеген герц дейін. Ал кейін-молекулалар ерекше күшпен бір жиілікте: 10 герц. Ол бірнеше апта бойы сақталады. Және тербеліс амплитудасы азаймайды. Бейнелі айтқанда, өмір симфониясында бір пронзительная нота басым болды.

ДНҚ жұмысын, - деп түсіндіреді Гаряев, - тез жұмыс істейтін компьютермен салыстыруға болады, ол бірден көп шешім қабылдайды. Бірақ компьютер арқылы кувалдамен соғылғанын елестетіп көріңізші, нәтижесінде барлық сұрақтарға ол бірдей жауап береді. Біз оны ультрадыбыстық деп

атаған кезде осындай нәрсе толқын геномда болды. Оның толқындық матрицалары бір жиілік күрт күшейе түсті.

Ультрадыбыстық құрылғылармен тұрақты өзара әрекеттесетін ультрадыбыстың зиянды әсер ету қаупі аймағына кіреді.

Бірінші кезекте қауіпті жиіліктер ОЖЖ-ны зақымдайды.

ОЖЖ-ның ультрадыбыспен зақымдануы бүкіл ағзаның жұмысында бұзылуларға әкеледі, ультрадыбыстық жиіліктердің зиянды әсері әртүрлі органдар мен жүйелердің жұмысында бұзылулармен көрінеді.

Аппаратқа қызмет көрсететін қызметкерлер осындай проблемаларға тап болуы мүмкін:

- әлсіздік және шаршау;
- тітіркендіргіш;
- құлақтың бітелуі;
- жаман ұйқы;
- бас ауруы;
- дыбысқа сезімталдықты арттыру;
- бозғылт немесе қызған адам;
- жадтың нашарлауы;
- суық аяқтар мен қолдар;
- талу.

Кейде диспепсиялық табиғаттың шағымдары, яғни асқазанның қалыпты қызметінің бұзылуы (абдоминальды ауырсыну, ауырлық сезімі немесе ерте қанығу).

Сондай-ақ, диэнцефалдық бұзылудың симптомдары да мүмкін, ол арықтау, галлюцинация,дене қызуының шамалы артуы (37-37, 5 градус), висцералды криз түріндегі пароксималдық ұстамалармен көрінеді.

Жиі бүйрек үсті қабығының, жыныс және қалқанша безінің бұзылуы бар. Вестибулярлық қозу айтарлықтай төмендейді. Емделушілерде жоғары және төмен тондарға реакцияның төмендеуі байқалады. Ультрадыбыс вегето-сезімтал немесе вегетативті полиневрит тудырады. Оның негізгі белгілері болып табылады:

- қол саусақтарының сезімталдығын төмендету.
- терінің көк түсі (цианоз).
- терінің шамадан тыс немесе жеткіліксіз қабыршақтануы (гиперкератоз).
- терінің ісінуі (пастоздық).
- жүрек-тамыр жүйесі жұмысының бұзылуы жиі кездеседі.

Ультрадыбыстық жиіліктер мұндай симптомдарды тудыруы мүмкін:

- жүректегі;
- гипотонияны;
- брадикардия;
- брадисистолия.

5 Экономикалық есептеу бөлімі

5.1 Жұмыстың сипаттамасы мен қажеттілігінің негіздемесі

Бұл дипломдық жобаның тақырыбы биометриялық бақылау жүйесін және кіруді бақылауды жобалау болатын.

Саусақ іздерін тану адам идентификациясының биометриялық жүйелерінде қолданылады.Сканерлеу сенімділігі сенсорға ғана байланысты емес. Алынған деректерді одан әрі өңдеу — ізді сәтті тану кілті.

Оптикалық сезімтал элементі бар саусақ іздері сканерінде, шын мәнінде монохромды матрицамен сурет түрінде түседі.

Қарапайым сканерлерде сурет эталонмен салыстырылады. Жиі одан әрі өңдеу бірнеше үлгімен жұмыс істейді.

Сканерден алынған сандық код желілік жылу датчигі бар жүйеде әр түрлі үлгі. Саусақ ізі әрқашан әртүрлі, тану сапасы саусақтың астында болған бұрышқа, саусақтың ылғалдылығына немесе сканердің бетіне байланысты. Мұндай сканермен берілетін деректер-нақты нүктелер жиынтығы. Сканердің бетіне саусақтың жатуы сияқты маңызды емес, бұл нүктелер әрдайым сызықтардың бірдей бүгілуі болады.

Таңбаларды кез келген сенсорлар мен алгоритмдер түрінде тану кезінде қателер сөзсіз. Қателер әдетте 2 түрге бөлінеді — дұрыс таңбаны тану және дұрыс емес таңбаны дұрыс деп тану.

Саусақ ізі сканері бар құлыптардың негізгі артықшылығы деректерді бұрмалау мүмкіндігін толық жою болып табылады. Өйткені, әр адамның саусақ іздері жеке және зақымданудан кейін де, уақыт өте келе де өзгертілмейді.

Сканерлер сенімді және қарапайым, ал бұл технологияның әмбебаптығы бұл құрылғыларды әртүрлі міндеттерді шешу үшін қолдануға мүмкіндік береді.

Аппарат терминалдың түрі бар: ол саусақ іздерін оқу үшін арнайы сканермен жабдықталған берік корпуста немесе байланыссыз карталардан шығарылады.

Саусақ іздерін анықтау кәсіпорын иелеріне кең ауқымды мүмкіндіктер береді:

- қызметкерлердің қызметін бақылауды жүзеге асыру;
- қызметкерлердің белгілі бір үй-жайларға кіруін шектеу;
- қажетті объектілерге жылдам қол жеткізуді қамтамасыз етеді;
- жалпы кіру басқару орталығынан белгілі бір өткізу пункттерін орталықтандырып басқаруға мүмкіндік береді.

Дипломдық жобаның мақсаты – саусақ ізі арқылы кіретін кіруді қарастыру және оны құрастыру.

Жобамыздың есептелуі мен құрастырылуының жалпы міндетінде келесі жағдайларды қарастырамыз:
- жоба туралы түсінік;
- сканерді арқылы кіруді есептеу мен құрастыруға кететін шығындарды анықтау;
- жобаны есептеу мен құрастырудың еңбек сыйымдылығы мен ұзақтығын есептеу;
- есептеу мен құрастыруға кеткен қызметкерлердің төлемақысын есептеу;
- әлеуметтік аударым есебі;
- материалдарға кеткен шығын көлемін есептеу;
- амортизациялық аударымдар;
- жұмыстың болжамдалған құнын есептеу;
- жұмыстың тиімділігін бағалау.

5.2 Сканерді арқылы кіруді есептеу мен құрастыруға кететін шығындарды анықтау

Есептеу және құрастыру жұмыстарын өткізудің өзіндік бағасын анықтау үшін келесі шығындарды есептеу қажет:
- негізгі қызметкерлердің төлемақысы (яғни жұмысқа тікелей қатысатын қызметкерлер үшін);
- қосымша төлемақы;
- еңбек қорына төлем;
- еңбек қоры төлемінен әлеуметтік салыққа түсетін аударым көлемі;
- амортизациялық аударым көлемі;
- коммуналдық төлемақылармен бірге жалдауға кеткен төлемақы құны;
- материалдарға кеткен шығын көлемі;
- сертификаттау мен лицензияға кеткен шығын көлемі;
- сатып алушыны іздеу мен жарнамаға кеткен шығын көлемі;
- салықтар көлемі (транспорт, жол және т.б.);
- үстеме шығындар көлемі.

5.3 Жобаны есептеу мен құрастырудың еңбек сыйымдылығы мен ұзақтығын есептеу

Бұл дипломдық жобада саусақ ізі арқылы кіретін кіруді есептеу мен құрастыру келесі сатылардан тұрады:
- оптикалық сканер таңдау;

- қосымша құралдары таңдау және сұлбасын сызу;
- жобаны құрастыру;
- бағдарламасын жазу;
- құрылғыны сынақтан өткізу.

Жобаны жасауға 2 қызметкер қатысады. Олар: құрастырушы инженер және бағдарламашы.

Құрастырушы инженер жобаны қиындығын бағалап, оған сәйкес сұлбасын сызып, сол сұлба бойынша құрастыру.Ал бағдарламашының міндеті белгілі бір алгорим бойынша жұмыс істейтін С++ тілінде бағдарламалық код жазып,оны микроконтроллерге енгізу.

5.1 к е с т е –Жобаны құрастыру бойынша еңбек сыйымдылығын есептеу

№	Жұмыс мазмұны	Орындаушылар	Ұзақтығы, күн
1	Оптикалық сканер таңдау	Инженер Бағдарламашы	3 0
2	Қосымша құралдары таңдау және сұлбасын сызу	Инженер Бағдарламашы	2 0
3	Жобаны құрастыру	Инженер Бағдарламашы	2 1
4	Бағдарламасын құрастыру	Инженер Бағдарламашы	0 4
5	Сынақтан өткізу	Инженер Бағдарламашы	3 2
6	Микроконтроллерге енгізу	Инженер Бағдарламашы	1 1
Барлығы			19

Жоба бойынша жасалған жұмыстың еңбек сыйымдылығы:

-Инженер– 11 адам-күн;

-Бағдарламашы– 8 адам-күн.

5.4 Жобаны есептеу мен құрастыруға кеткен қызметкерлердің төлемақысын есептеу

Қызметкерлердің негізгі жалақысы мына өрнек бойынша есептеледі:

$$Ж_{нег} = Ж_{орт} * T, \qquad (5.4.1)$$

мұндағы $Ж_{нег}$ – қызметкерлердің негізгі жалақысы (тг.);

$Ж_{орт}$ – қызметкердің бір күнгі орташа жалақысы (тг.);

T – еңбек сыйымдылығы (17 адам-күн).

Инженер үшін негізгі жалақы құны:

$$Ж_{нег} = 6000 * 11 = 66\,000 \text{ тг.}$$

Бағдарламашы үшін негізгі жалақы құны:

$$Ж_{нег} = 7000 * 8 = 56\,000 \text{ тг.}$$

Айлық 21 жұмыс күні үшін есептелген. Негізгі жалақы есебін 5.2 кестеде көрсетілген.

5.2 к е с т е – Негізгі жалақы есебі

Қызметкерлер	Айлық, тг/ай.	Қызметақы тг/күн.	Еңбек сыйымдылығы, адам-күн.	Сомасы, тг.
Инженер	126000	6000	11	66 000
Бағдарламашы	147000	7000	8	56 000
Қызметкерлердің негізгі жалақы $Ж_{нег}$				122 000

Қызметкерлердің демалыс пен ауырғанына кеткен шығындарды есептеу келесі өрнекпен анықталады, яғни қызметкерлердің қосымша жалақысы (орташа есеппен алғанда негізгі жалақыдан 10 %-бен есептелінеді):

$$Ж_{қос} = 0{,}1 * Ж_{нег}, \quad (5.4.2)$$

Инженер үшін қосымша жалақы құны:

$$Ж_{қос} = 0{,}1 * 66000 = 6600 \text{ тг.}$$

Бағдарламашы үшін қосымша жалақы құны:

$$Ж_{қос} = 0{,}1 * 56000 = 5600 \text{ тг.}$$

5.5 Әлеуметтік аударым есебі

Әлеуметтік салық Қазақстан Республикасының Салық туралы кодексы бойынша еңбекақы қорынан (ЕАҚ) 9,5 %-ды құрайды. Ал зейнетақы қорысының (ЗАҚ) төлемі ЕАҚ 10 %-ын құрайды. Зейнетақы қорынан әлеуметтік салық алынбайды.

Еңбекақы қорын келесі өрнек арқылы есептеуге болады:

$$ЕАҚ = Ж_{нег} + Ж_{қос}, \quad (5.5.1)$$

мұндағы $Ж_{нег}$ – негізгі жалақы;

$Ж_{қос}$ – қосымша жалақы;

Инженер үшін еңбекақы қорының көлемі:

$$ЕАҚ_1 = 66000 + 6600 = 72\,600 \text{ тг.}$$

Бағдарламашы үшін еңбекақы қорының көлемі:

$$ЕАҚ_2 = 56000 + 5600 = 61\ 600 \text{ тг.}$$

Еңбекақы қорының жалпы сомасы:

$$\sum ЕАҚ = 72\ 600 + 61\ 600 = 134\ 200 \text{ тг.}$$

Зейнетақы қорына (ЗАҚ) аударылым көлемі келесі өрнекпен есептеледі:

$$ЗАҚ = ЕАҚ * 0{,}1\ , \qquad (5.5.2)$$

мұндағы, ЕАҚ – еңбекақы қоры.

Инженер үшін зейнетақы қорына аударылым көлемі:

$$ЗАҚ_1 = 72600 * 0{,}1 = 7260 \text{ тг.}$$

Бағдарламашы үшін зейнетақы қорына аударылым көлемі:

$$ЗАҚ_2 = 61600 * 0{,}1 = 6160 \text{ тг.}$$

Зейнетақы қорының жалпы сомасы:

$$\sum ЗАҚ = 7260 + 6160 = 13420 \text{ тг.}$$

Әлеуметтік салыққа аударым көлемін келесі өрнекпен анықтаймыз:

$$С_{әлеу} = (ЕАҚ - ЗАҚ) * 0{,}095\ , \qquad (5.5.3)$$

Инженер үшін әлеуметтік салыққа аударым көлемі:

$$С_{әлеу1} = (72600 - 7260) * 0{,}095 = 6207 \text{ тг.}$$

Бағдарламашы үшін зейнетақы қорына аударылым көлемі:

$$С_{әлеу2} = (61600 - 6160) * 0{,}095 = 5267 \text{ тг.}$$

Әлеуметтік аударымдардың жалпы сомасы:

$$\sum С_{әлеу} = 6207 + 5267 = 11\ 474 \text{ тг.}$$

Қызметкерлерге байланысты әлеуметтік аударымдар 5.3 кестеде көрсетілген:

5.3 к е с т е – Әлеуметтік аударымдар көлемі

	Еңбекақы қоры, тг.	Зейнетақы қоры, тг.	Әлеуметтік салық, тг.
Инженер	72 600	7260	6207
Бағдарламашы	61 600	6160	5267
Барлығы: $\sum$ЕАҚ, $\sum$ЗАҚ, $\sum С_{әлеу}$	134 200	13420	11 474

5.6 Материалдарға кеткен шығын көлемін есептеу

Материалдық шығындарға кеткен сомма көлемін келесі өрнекпен анықтауға болады:

$$З_м = \sum P_i \times Ц_{i,} \quad (5.6.1)$$

мұндағы P_i – і түрлі материалды ресурсқа кеткен шығын, натурал сандар;

$Ц_i$ – і түрлі материалды ресурстың данасының бағасы, тг;

і – материалдық ресурстың түрі;

n – материалдық ресурстар түрлерінің саны.

Материалдық ресурстарға кеткен шығын көлемінің есептеулері 5.4 кестеде көрсетілген.

5.4 к е с т е – Материалдық ресурстарға және құрастыруға кеткен шығын көлемі.

Материалдың атауы	Маркасы	Өлшем бірлігі	Саны	1 дана үшін бағасы, тг.	Соммасы, тг.
Arduino Uno	R3	Дана	1	9700	9700
Bluetooth модуль	JDY-10	Дана	1	2100	2100
Сервожетек	SG-90	Дана	1	1500	1500
Саусақ ізі сканер	ZMF60 V1.4	Дана	1	15500	15500
Буззер(динамик)	-	Дана	1	500	500
Жарық диодтары	-	Дана	2	30	60
Резисторлар	-	Түтік	2	50	100
Arduino үшін негізгі жинақ	-	Дана	1	12000	12000
Изолента	-	Дана	1	200	200
Корпус	ПВХ	Дана	1	2700	2700
Барлығы				44 280	44 360

Жүк тасымалдауға кететін шығын материалдардың жалпы сомасынан 10%-ды құрайды. Ол келесі өрнекпен анықталады:

$$С_м = З_м \times 0,1. \quad (5.6.2)$$

Жүк тасымалдауға кететін шығын көлемі:

$$С_м = 44360 \times 0,1 = 4\ 436 \text{ тг.}$$

Жобаны толықтай жасап шығару үшін 19 күн уақыт қажет. Соған байланысты кеңселік ғимарат жалға алынады. Алматы қаласы бойынша кеңселік ғимаратты жалға алу сомасы 90000 теңге көлемінде (1 айға) болады. Жобаны жасау бойынша жалдауға кеткен жалпы сома көлемі 57 000 теңге болады. Осы соманың ішінде 24 шаршы метрге тең жұмыс аймағының:

- электр энергиясы;
- суық және ыстық су;
- жылыту жүйесі;
- қарауыл қызметі;
- интернет желісі сияқты шығындар жатады.

5.7 Амортизациялық аударымдар

Амортизациялық аударымдар $С_а$ келесі өрнекпен анықталады:

$$C_a = Н \times Ф, \quad (5.7.1)$$

мұндағы Н – орташа жылдық амортизация нормасы, %;

Ф – құрылғының бастапқы бағасы, тг.

Қазақстан Республикасының салық кодексының 25.12.2017 N 120-VI ЗРК «Салықтар және бюджетке түсетін басқа төлемдер туралы» бөлімі бойынша автокөлік және құрылғылар (II топ) үшін амортизацияның шектік нормасы 25 %-ды құрайды.

Құрылғы үшін амортизациялық аударым көлемі:

$$С_а = 44\ 360 \times 0,25 = 11090 \text{ тг.}$$

Жобаның әр кезеңіндегі шығындар құны 5.5 кестеде көрсетілген:

5.5 к е с т е – Жобаны жасауға кеткен шығындардың сметасы

Жобаның жасалу кезеңдеріндегі шығындар	Сомасы, тг.
Еңбекақы қорының жалпы сомасы	134 200
Әлеуметтік аударымдар	11 474
Материалдық ресурстарға және құрастыруға кеткен шығын	44 360
Жалдауға және коммуналдық қызметтерге кеткен шығын	57 000
Амортизациялық аударымдар	11090
Тасымалдауға кеткен шығын	4436
Барлығы	262 560

5.8 Жұмыстың болжамдалған құнын есептеу

Жобаның ықтимал құнының көлемі өнімділіктің, қасиеттернің және уақытысында орындалуы орындаушы мен сатып алушының қаржылық қызығушылығының дейгейіне жауап беретіндей қылып орнатылады.

Жобаның келісілген бағасы келесі өрнекпен есептеледі:

$$Ц_{oi} = С_{жоба} \times \left(1 + \frac{Р}{100}\right) + ҚҚС\ , \qquad (5.8.1)$$

мұндағы $Ц_{oi}$ – жобаның келісілген бағасы, тг;

$С_{жоба}$ – жобаны жасауға кеткен шығын, тг;

Р – рентабельділіктің орташа деңгейі, 10 %;

ҚҚС – қолданбалы құнның салығы, 12 %.

Қолданбалы құнның салығын есептемеген кездегі құн:

$$С_{ҚҚС-сыз} = 262\ 560 \times \left(1 + \frac{Р}{100}\right) = 288\ 816.$$

Жобаның қосымша бағасынан қосылатын құнның салық ставкасы келесі өрнекпен есептеледі:

$$ҚҚС = 288\ 816\ \times 0{,}12 = 34\ 657{,}92 \text{ тг.}$$

Жобаның келісілген бағасының көлемі:

$$Ц_{oi} = 288\ 816 + 34\ 657{,}92 = 323\ 473{,}92 \text{ тг.}$$

5.9 Жұмыстың тиімділігін бағалау

Ғылыми-зерттеу жұмыстарының басты ғылыми әсерінің көрсеткіштері жұмыс жаңашылдығы, теориялық пысықталуының дәрежесі, болашағы, нәтижелерінің таралу дәрежесі және іске асыру ықтималдылығы болып табылады. Ғылыми-зерттеу жұмыстарының ғылыми әсерін екі көрсеткішпен мінездеуге болады: ғылыми жаңашылдығының дәрежесі және теориялық пысықталуының деңгейі.

Ғылыми әсерді мінездейтін көрсеткіш келесі өрнекпен анықталады:

$$Э_{н} = 0{,}6k_{нов} + 0{,}4k_{теор}\ , \qquad (5.9.1)$$

мұндағы $k_{нов}$, $k_{теор}$ - ғылыми жаңашылдығының дәрежесі мен теориялық пысықталуының деңгейінің көрсеткіштері;

0,6; 0,4 – ғылыми жаңашылдығының дәрежесі мен теориялық пысықталуының деңгейінің көрсеткіштерінің коэффициенттері.

Ғылыми жаңашылдығының дәрежесі бойынша осы жұмыс біршама жаңа болып табылады. Өйткені бұл технология тек шетелде ғана бар, ал ҚР әлі қолданыста жоқ. А қосымшасы бойынша жобаның ғылыми жаңашылдығының дәрежесі 4 баллға тең. Ал теориялық пысықталуының деңгейі бойынша Б қосымшасында көрсетілгендей 6 баллға тең.

Осы көрсеткіштерге байланысты жобаның ғылыми әсері келесідей болады:

$$Э_{н} = 0{,}6 \times 4 + 0{,}4 \times 6 = 4{,}8.$$

Жобаны толықтай жасап шығару үшін 323 473,92 теңге көлемінде шығын кетті. Ал ғылыми әсерінің бағасы 4,8 балды құрайды. Жұмыс ғылыми жаңашылдығының дәрежесі мен теориялық пысықталуының деңгейіне байланысты біршама жаңа болып табылады. Менің жобам болашақта үлкен сұранысқа ие болатынына мен сенімдімін, себебі бағасы өте қол жетімді әрі адамға өте пайдалы.

Қорытынды

Бұл дипломдық жобада адамдың биометриялық деректері арқылы кіру және оны жоба ретінде жасау мәселесі қарастырылды.Жұмыс барысынды келесідей құрал-жабдықтар таңдалынды:

- жұмысқа қажетті құрал-жабдықтар таңдалынды;
- жоба Arduino Uno тақтасынды жұмыс құрастырылды және де Arduino IDE бағдарламалау ортасында бағдарлама жасалынды;
- жасалынған бағдарламаға сәйкестендірілген блок-сұлба құрастырылды;
- жобаны жасауға кеткен жалпы шығын анықталды,және ол 323 473,92 теңгені құрады;
- дипломдық жобада өмір тіршілік қауіпсіздік бөлімінде жобада қолданылған оптикалық ZFM60 V1.4 саусақ ізі сканерінің адам өміріне зиянсыз екені дәлелденді.

Жасалынған дипломдық жоба білім беру мекемелерін,өндірістік кәсіпорындарында және т.б. мекелерінде жұмыс сапасын арттыруға пайдалануға болады.

Қолданылған әдебиеттер тізімі

1 Старовойтов В.В. Биометрические системы контроля доступа по отпечаткам палцев.Информатика. 2015, (1): 26-38 с.

2 Т. И. Лапина, Н. Н. Епишев, Д. В. Лапин, Способ биометрической аутентификации пользователя в компьютеризованных системах контроля доступа, Тр. СПИИРАН, 2013, выпуск 27, 189–199 с.

3 Вороня В.А., Тихонов В.А. Системы контроля и управления доступом. – М.: Горячая линия– Телеком, 2013. – 272 с.

4 Аутентификация. Теория и практика обеспечения безопасного доступа к информационным ресурсам. - Москва: Мир, 2012. - 552 с.

5 Научная статья- Современные системы идентификации личности для развития национальной информационной инфраструктуры социалистической Республики Вьетнама // Выпуск №6-1(37), 2015год. Страница 83 - 85.

6 Волхонский В.В. Системы контроля и управления доступом. – СПб: Университет ИТМО, 2015. – 200 с. Рис. 96. Библ. 6.

7 Биометрические методы защиты информации : учеб.-метод.пособие/А.М. Прудник, Г.А.Рощупкин. - Минск:БГУИР,2014.-123с.

8 Бадиков А.В., Бондарев П.В. Системы контроля и управления доступом. Лабораторный практикум. – М.: НИЯУ МИФИ, 2010. – 128 с.

9 Татарченко Н. В., Тимошенко С. В. Биометрическая идентификация в интегрированных системах безопасности // Специальная техника. 2002. № 2.

10 Технические средства охраны : системы контроля и управления доступом : учеб. пособие / В. П. Бугаков, А. В. Тельный; Владим. гос. ун-т. – Владимир : Изд-во Владим. гос. ун-та, 2007. – 148 с. (Комплексная защита объектов информатизации. Кн. 14 / под ред. М.Ю. Монахова).

11 Современные операционные системы. 4-е изд. — СПб.: Питер, 2015. — 1120 с.: ил. — (Серия «Классика computer science»).

12 Гоева А.А. Технологии авторизации по биометрическим данным в мобильном приложении на операционной системе IOS // Научное сообщество студентов: Междисциплинарные исследованиясб. ст. по мат. XLI междунар. студ. науч.-практ. конф. № 6(41). URL: https://sibac.info/archive/meghdis/6(41).pdf (дата обращения: 27.02.2019).

13 Защита информации. Техника защиты информации. Требования к средствам высоконадежной биометрической аутентификации/ Цели и принципы стандартизации в Российской Федерации установлены Федеральным законом от 27 декабря 2002 г. № 184-ФЗ «О техническом регулировании», а правила применения национальных стандартов Российской Федерации — ГОСТ Р 1.0—2004 «Стандартизация в Российской Федерации. Основные положения».

14 Пересыпкин И. П., Мартынова Л. Е., Назарова К. Е., Белозёрова А. А., Попков С. М. Принципы работы и уязвимости биометрических систем аутентификации // Молодой ученый.(часть 1) — 2016. — №30. — С. 86-88.

15 Первая миля-научно-технический журнал:Высоконадежная биометрическая аутентификация пользователя // А.Иванов, А.Малыгин. 2007 Выпуск № 7 .

16 Купцов Р.Р. Анализ современных методов биометрической идентификации скуд // Студенческий: электрон. научн. журн. 2018. № 8(28).

17 Газета «Securitynews» / Биометрические технологии в СКУД: актуальный доклад Андрея Васильева . URL: http://www.secnews.ru/events/21265.htm#ixzz5fyIVveYV (дата обращения:22.12.2014).

18 Александр Дрёмин - Биометрические системы контроля и управления доступом: шаг в будущее// журнал «современные технологии автоматизации» 2006г Выпуск №4 стр. 26.

19 Биометрия в СКУД.Взляд не постороннего // журнал «Алгоритм безопасности» издание для профессионалов. Выпуск № 1, 2017 год.

20 Биометрические системы контроля и управления доступом//Инженерная компания «Электрет-2001». URL:http://electret2001.ru (дата обращения:19.02.2019 17:35).

21 Барсуков В. С. Биоключ - путь к безопасности // Специальная техника. — 2003. — № 2.

22 Биометрическая и системная безопасность: обзор сквозной системы безопасности//Научно-технический журнал «Communicationsofthe IIMA» 2006 г том 6 Выпуск 2.

23 Контроль управление доступом // Инженерная компания «Прософт-Биометрикс» URL:http://www.bio-smart.ru/about (дата обращения:26.02.2019г 10:57).

24 Виды скуд // Компания ООО «Квантек-СТ» Ссылка:http://www.quantech.ru/about/ (дата: 26.02.2019г 11:34).

25 Научная работа сотрудников Индийского инстиута информационных технологии Читтур :Yash Mittal,Aishwary Varshney,Prachi Aggarw al,Kapil Mataniand V. K. Mittal URL:https://www.researchgate.net/profile/Vinay_Mittal2 (дата обращения: 26.02.2019 12:00).

26 Система контроля и управления доступа: Куда идем? // журнал «Алгоритм безопасности» издание для профессионалов. 2011г Выпуск №4 Авторы: И. Раков, П.Шмелев, Ю.Суконщиков, О.Батманов.

27 Как выбрать биометрическую скуд параметры параметры выбора и эксплуатации // журнал «Алгоритм безопасности» издание для профессионалов. 2011г Выпуск №4. Автор: К. Новиков.

28 Биометрические технологии в СКУД//журнал «Алгоритм безопасности» издание для профессионалов. 2011г Выпуск №4. Автор:К. Грибачев.

29 Волхонский В.В. Системы контроля и управления доступом. – СПб: Университет ИТМО, 2015. – 105 с. Рис. 96. Библ. 6.

30 Тампель И.Б., Карпов А.А. АВТОМАТИЧЕСКОЕ РАСПОЗНАВАНИЕ РЕЧИ. Учебное пособие. − СПб: Университет ИТМО, 2016. – 138 с.

31 Молдовян А.А., Молдовян Д.Н., Левина А.Б. Протоколы аутентификации с нулевым разглашением секрета. – СПб: Университет ИТМО, 2016. – 55 с.

32 Щеглов А.Ю., Щеглов К.А.Математические модели и методы формального проектирования систем защиты информационных систем. Учебное пособие.– СПб: Университет ИТМО, 2015. – 93с.

33 Щеглов А.Ю. Модели, методы и средства контроля доступа к ресурсам вычислительных систем. Учебное пособие.– СПб: Университет ИТМО, 2014. – 95с.

34 Волхонский В. В. Системы контроля и управления доступом. Штриховые коды. – СПб: Университет ИТМО, 2015. – 53 с. Рис. 30. Библ. 15.

35 Биометрические системы контроля и управления доступом в задачах защиты информации: учебно-метод. Пособие / В.В. Вихман, А.А. Якименко.- Новосибирмк: Изд-во НГТУ, 2016.-54 с.

36 Биометрия сегодня и завтра. Мнение экспертов // Опубликовано: Журнал «Системы безопасности» Выпуск #5, 2018
Автор: Константин Кравченко.

37 Биометрические идентификаторы в СКУД на практике // Опубликовано: Журнал «Системы безопасности» Выпуск #5, 2018
Автор: Иван Царев, Тихон Григоренко

38 СКУД на 360°Мнения экспертов // Опубликовано: Журнал «Системы безопасности» Выпуск #5, 2018
Автор: Вячеслав Тесаков, Вадим Борисов .

39 Интеграция IdM и СКУД // Опубликовано: Журнал «Системы безопасности» Выпуск #6, 2018
Автор: Евгений Мельников.

40 Биометрическая идентификация . Биометрия. СпецВыпуск#1 (4), 2017.

41 Биометрические технологии в системах управления доступом // Опубликовано: Журнал «Системы безопасности» Выпуск #7, 2002
Автор:А.А.Гинце .

42 Биометрия в системах контроля и управления доступом: вызовы времени и новые возможности // Научно-промышленная компания »Секьюрити Центр С&Т»
URL:http://www.scct.ru/o-kompanii (дата обращения:26.02.2019 14:30).

43 Чистяков М. В. Методы идентификации пропусков и основные требования к системе контроля и управления доступом и безопасностью учреждения // Молодой ученый. — 2016. — №11. — С. 241-243.

44 Разработка метода биологической идентификаии повышенной надежности на основе атомно-силовой микроскопии // журнал «Известия южного федерального университета. Технические Науки»Раздел V. Биомедицинские нанотехнологии.

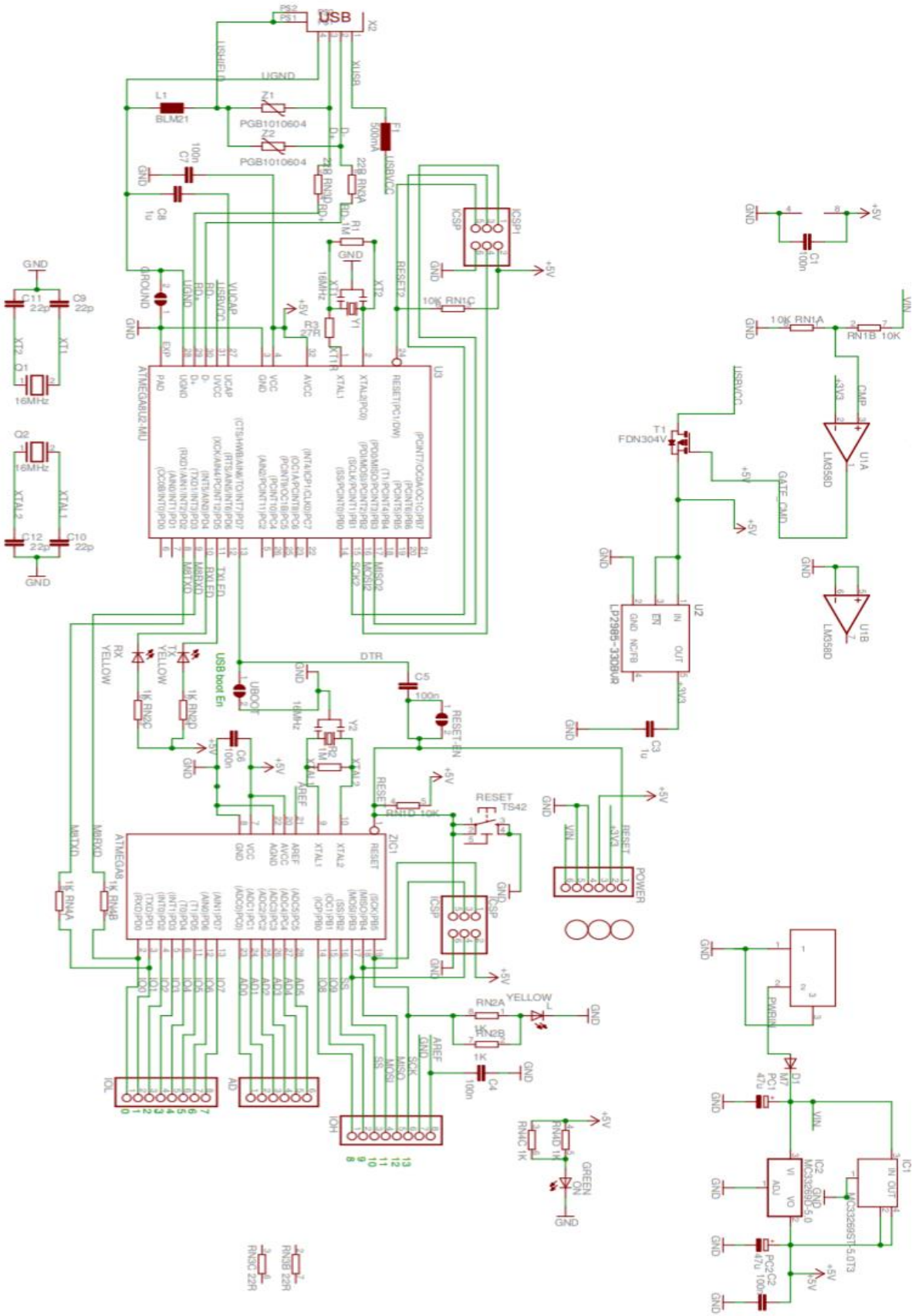
45 Биометрические технологии идентификации в системах технологии идентификации в системах контроля и управления доступом // журнал «Computationalnanotechnology« 2016г Выпуск №3.

46 Биометрические технологии в антитеррористической деятельности правохранительных органов: Перспективы и проблемы использования // журнал «Вестник Московского университета МВД России«Специальный выпуск №10, 2014г Посвященный научным трудам Московского областного филиала Московского университета МВД России им. В.Я. Кикотя.

47 Биометрическая идентификация человека // Научный журнал КубГАУ, №109(05), 2015 года.

48 Методы распознавания в системах биометрической идентификации// Компания Вокорд
URL:http://old.vocord.ru/press-center/reviews/biometricheskaya-identifikatsiya-fantastika-i-realnost (дата: 26.02.2019 16:36).

49 Биометрические технологии // Журнал «Бестселлеры ИТ-рынка» выпуск №10 (39), октябрь 2001
Автор: Андрев Борзенко .

50 Крылова И. Ю., Рудакова О. С. Биометрические технологии как механизм обеспечения информационной безопасности в цифровой экономике // Молодой ученый. — 2018. — №45. — С. 74-79.

А қосымша
Arduino Uno-ның қағидаттық сұлбасы