

ҚАЗАҚСТАН РЕСПУБЛИКАСЫНЫҢ ҒЫЛЫМ ЖӘНЕ ЖОҒАРЫ БІЛІМ
МИНИСТРЛІГІ

Қ.И. Сәтбаев атындағы Қазақ ұлттық техникалық зерттеу университеті

Автоматика және ақпараттық технологиялар институты

Электроника, телекоммуникация және ғарыштық технологиялар кафедрасы

Тұрланұлы Мейрамбек

«Arduino негізінде IoT арқылы жекеменшік мүлікті қорғау жүйесін жасау»

ДИПЛОМДЫҚ ЖҰМЫС

6B06201 «Телекоммуникация» білім беру бағдарламасы

Алматы 2025 ж.

ҚАЗАҚСТАН РЕСПУБЛИКАСЫНЫҢ ҒЫЛЫМ ЖӘНЕ ЖОҒАРЫ БІЛІМ
МИНИСТРЛІГІ

Қ.И. Сәтбаев атындағы Қазақ ұлттық техникалық зерттеу университеті

Автоматика және ақпараттық технологиялар институты

Электроника, телекоммуникация және ғарыштық технологиялар кафедрасы

ҚОРҒАУҒА ЖІБЕРІЛДІ

Кафедра меңгерушісі

Е.Таштай

20 / 05 2025 ж.

ДИПЛОМДЫҚ ЖҰМЫС

Тақырыбы: Arduino негізінде IoT арқылы жекеменшік мүлікті қорғау жүйесін
жасау

6B06201 Телекоммуникация білім беру бағдарламасы

Орындаған: М. Тұрланұлы

Пікір беруші

М.Тынышбаев атындағы АЛТ
университеті, PhD, АКТ
кафедрасының ассистент
профессоры

Мәдібайұлы Ж.

20 / 05 2025 ж.

Ғылыми жетекші

ҚазҰТЗУ, PhD, Электроника,
телекоммуникация және ғарыштық
технологиялар кафедрасының
Қауымдастырылған профессоры

Хабай А.

20 / 05 2025 ж.

Алматы 2025 ж.

ҚАЗАҚСТАН РЕСПУБЛИКАСЫ ҒЫЛЫМ ЖӘНЕ ЖОҒАРЫ БІЛІМ
МИНИСТРЛІГІ

Қ.И. Сәтбаев атындағы Қазақ ұлттық техникалық зерттеу университеті

Автоматика және ақпараттық технологиялар институты

Электроника, телекоммуникация және ғарыштық технологиялар кафедрасы

6B06201 Телекоммуникация

БЕКІТЕМІН

Кафедра меңгерушісі

Е. Таптай

31 01 2025 ж.

**Дипломдық жұмыс орындауға
ТАПСЫРМА**

Білім алушы Тұрланұлы Мейрамбек

Тақырыбы *Arduino негізінде IoT арқылы жекеменшік мүлікті қорғау жүйесін жасау*

Университет ректорының 29 қаңтар 2025 ж. №26 П/Ө бұйрығымен бекітілген.

Аяқталған жұмысты тапсыру мерзімі 30 мамыр 2025 ж.

Дипломдық жұмыстың бастапқы берілістері: 1) Негізгі платформа: *Arduino* (ұсынылатын модель: *Arduino Mega* немесе *Uno*). 2) Датчиктер: Қозғалыс сенсоры (*PIR Motion Sensor*), Есіктің ашылуын бақылау сенсоры (*Reed Switch*), Дыбыс сенсоры (*Sound Detection Module*). 3) Дабылдық сигнал (*Buzzer* немесе динамик). 5) *GSM* модулі (*SIM800L* немесе аналогы) мүлік иесіне хабар жіберу үшін. 6) *Wi-Fi* модулі (*ESP8266*) деректерді қашықтан бақылау үшін. 7) Қуат көзі: *5V* тұрақты ток көзі немесе литий-ионды аккумулятор. 8) Желіге қосылу *GSM* арқылы.

Дипломдық жұмыста қарастырылатын мәселелер тізімі: а) Жекеменшік мүлікті қорғау жүйелерінің қазіргі жағдайын талдау. б) *Arduino* негізінде қорғау жүйесін жобалау және құрастыру. в) Қауіпсіздік сенсорларын таңдау, қосу және олардың жұмысын тексеру. г) *IoT* технологияларын пайдаланып, деректерді қашықтан бақылау және сақтау мүмкіндігін қамтамасыз ету. д) *GSM* модулі арқылы дабылдық хабарламаларды жіберу алгоритмін әзірлеу. е) Жүйенің қауіпсіздігі мен тиімділігін тәжірибелік сынақ арқылы бағалау.

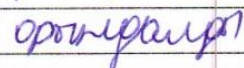
Сызбалық материалдар тізімі (міндетті сызбалар дәл көрсетілуі тиіс):

Ұсынылатын негізгі әдебиеттер: 1) *Chikara, S. Jain, M. Fatima, and M. Luthra, Review on Implementing Smart Water Grid for Smart Cities in India: Challenges and Solutions, 2019 5th International Conference on Advanced Computing & Communication Systems (ICACCS), Coimbatore, India, pp. 216-219, 2019.* 2)

Anand R. Padwalkar, Prajakta Pande, "Internet of Things -A Future of Internet: A Survey," *International Journal of Advance Research in Computer Science and Management Studies*, Volume 2, Issue 2, February 2014. 3) Pharmasetiawan and R. Rediana, Designing a business model for smart water management system with the smart metering system as a core technology: Case study: Indonesian drinking water utilities, 2017 *International Conference on ICT For Smart Society (ICISS)*, Tangerang, pp. 1-6, 2017 doi: 10.1109/ICTSS.2017.8288862.

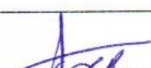
дипломдық жұмысты (жобаны) дайындау

КЕСТЕСІ

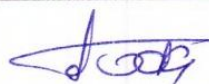
Бөлімдер атауы, карастырылатын мәселелер тізімі	Ғылыми жетекшіге және кеңесшілерге көрсету мерзімі	Ескерту
Диплом жұмысының тақырыбын талдау	04.01.2025 - 01.02.2025	
Теориялық ақпарат	01.02.2025 - 01.03.2025	
Жабдықтар жұмысының есебі және жұмысты рәсімдеу	01.03.2025 - 30.05.2025	

Дипломдық жұмыс (жоба) бөлімдерінің кеңесшілері мен
норма бақылаушының аяқталған жұмысқа(жобаға) қойған

қолтаңбалары

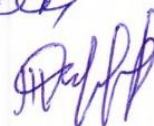
Бөлімдер атауы	Кеңесшілер (аты, әкесінің аты, тегі, ғылыми дәрежесі, атағы)	Қол қойылған күні	Қолы
Диплом жұмысының тақырыбын талдау	Хабай А. ЭТжҒТ каф. қауым.профессоры, PhD	13.03.2025	
Теориялық ақпарат	Хабай А. ЭТжҒТ каф. қауым.профессоры, PhD	29.04.2025	
Норма бақылау	Досбаев Ж.М. ЭТжҒТ каф.аға оқытушысы, PhD	19.05.2025	

Ғылыми жетекшісі



Хабай А.

Тапсырманы орындауға алған білім алушы



Тұрланұлы М.

Күні 02 ақпан 2025 ж.

АНДАТПА

Бұл дипломдық жұмыста Arduino негізінде IoT технологиялары арқылы жекеменшік мүлікті қорғау жүйесін жасау мәселесі қарастырылады. Жүйе түрлі сенсорлар кешенін және микроконтроллерді пайдалана отырып, тұрғын үйдің қауіпсіздігін арттыруға бағытталған. Жоба барысында қозғалысты, газдың концентрациясын, температура мен ылғалдылықты бақылайтын сенсорлар қолданылды және деректерді өңдеп, қауіп туындаған жағдайда дабыл жүйесін іске қосу қарастырылды. Жүйенің негізгі ерекшелігі — интернет желісі арқылы қашықтықтан бақылау және басқару мүмкіндігі. Зерттеу нәтижелері көрсеткендей, жасалған жүйе тиімді, сенімді және шығындары төмен, бұл оны тұрғын үйлердің қауіпсіздігін қамтамасыз етуде қолдануға мүмкіндік береді.

АННОТАЦИЯ

В данной выпускной работе рассматривается разработка системы защиты частной собственности с использованием технологий IoT на базе Arduino. Система направлена на повышение безопасности жилых помещений посредством применения комплекса различных датчиков и микроконтроллера. В ходе проекта использовались датчики для контроля движения, концентрации газа, температуры и влажности, а также предусматривалась обработка данных и активация сигнализации при возникновении опасности. Основной особенностью системы является возможность удалённого мониторинга и управления через интернет-сеть. Результаты исследования показали, что разработанная система эффективна, надёжна и экономична, что делает её применимой для обеспечения безопасности жилых объектов.

ABSTRACT

This thesis explores the development of a private property protection system using IoT technologies based on Arduino. The system is aimed at enhancing the security of residential premises by utilizing a set of various sensors and a microcontroller. During the project, sensors were employed to monitor motion, gas concentration, temperature, and humidity, with data processing and the activation of an alarm system in case of potential threats. A key feature of the system is the ability for remote monitoring and control via the Internet. The research results demonstrate that the developed system is effective, reliable, and cost-efficient, making it suitable for ensuring the security of residential properties.

МАЗМҰНЫ

Кіріспе	7
1 Интернет заттары технологиясын қолданатын жобаларға шолу	8
1.1 Интернет заттармен байланысты технологиялардың тұжырымдамасы	8
1.2 Интернет заттары жүйелерін стандарттау	16
1.3 Интернет заттарымен жұмыс істейтін қолданыстағы жүйелерді талдау	22
2 Arduino негізінде IoT қауіпсіздік жүйесін құру	30
2.1 IoT негізіндегі қауіпсіздік тұжырымдамасы	30
2.2 Қауіпсіздік жүйесіндегі IoT-қа шолу	30
2.3 IoT қауіпсіздік жүйесінің құрылымы	31
2.4 Қауіпсіздік жүйесі бойынша қолданыстағы IoT жүйелерін талдау	35
3 Arduino негізінде жасалған үй қауіпсіздігіне арналған смарт жүйе	37
3.1 Arduino негізінде IoT арқылы жекеменшік мүлікті қорғау жүйесін талдау	37
3.2 Arduino негізінде IoT арқылы жекеменшік мүлікті қорғау ағыны	39
3.3 Arduino негізінде IoT арқылы жекеменшік мүлікті қорғау жүйесінің жалпы құрылымы	42
3.4 Arduino негізінде IoT арқылы жекеменшік мүлікті қорғау жүйесінің аппараттық және бағдарламалық бөлігін жобалау	45
3.5 Негізгі компоненттердің таңдалу негіздемесі	47
3.6 Деректерді өңдеу және жіберу есебі	48
Қорытынды	50
Пайдаланылған әдебиеттер тізімі	51
Қосымша А	53

КІРІСПЕ

XXI ғасырда ақпараттық технологиялардың және интернеттің қарқынды дамуы адам өмірінің көптеген салаларына елеулі өзгерістер әкелді. Соның бірі — тұрғын үйлер мен жеке меншікті қорғауға арналған интеллектуалды қауіпсіздік жүйелерінің кеңінен таралуы. Әсіресе IoT (Internet of Things) технологияларының дамуы үйді автоматтандыруды және қауіпсіздікті жаңа деңгейге көтерді.

Бұл дипломдық жұмыста Arduino микроконтроллерін және әртүрлі сенсорларды пайдалану арқылы IoT негізінде жекеменшік мүлікті қорғау жүйесін жасау қарастырылады. Жүйенің басты мақсаты — үй ішінде орын алған қозғалысты, газдың ағып шығуын немесе температура мен ылғалдылықтағы қалыптан тыс өзгерістерді анықтап, пайдаланушыға дер кезінде хабарлау.

Жобада Wi-Fi арқылы интернет желісіне қосылатын модуль қолданылды. Сымсыз байланыс үшін статикалық IP мекенжай орнатылып, қашықтан басқару мен бақылау мүмкіндігі қамтамасыз етілді. Пайдаланушы жүйені Google Assistant арқылы дауыс командаларымен немесе арнайы әзірленген веб-қосымша арқылы басқара алады.

Жұмыстың өзектілігі — тұрғын үйлердің қауіпсіздігін арттырудың қолжетімді, тиімді және үнемді жолдарын іздестіру болып табылады. Дипломдық жұмыс барысында жүйенің жобалау, іске асыру және тестілеу кезеңдері қарастырылып, алынған нәтижелер бойынша қорытындылар жасалды.

1 Интернет заттары технологиясын қолданатын жобаларға шолу

1.1 Интернет заттармен байланысты технологиялардың тұжырымдамасы

«Смарт үй» жүйесінің тұжырымдамасы - үйдегі өмірді ұйымдастырудың жаңа тәсілі, мұнда жоғары технологиялық жабдықтар кешенінің негізінде барлық өмірді қамтамасыз ету жүйелерінің жұмысын едәуір тиімді және сенімді қылатын бірыңғай автоматтандырылған басқару жүйесі құрылады [1].

«Смарт үй» - бұл барлық пайдаланушылар үшін қауіпсіздікті, ресурстарды үнемдеуді және жайлылықты қамтамасыз ететін жүйе. Ең қарапайым жағдайда жүйе ғимаратта болып жатқан нақты жағдайларды тани алуы және оларға сәйкес әрекет етуі тиіс: оның ішкі жүйелерінің бірі басқа жүйелердің жұмысын алдын ала белгіленген алгоритмдерге сәйкес басқара алады. Бұдан бөлек, бірнеше ішкі жүйені автоматтандыру арқылы бүкіл кешен үшін синергетикалық әсерге қол жеткізіледі.

«Смарт үй» дегеніміз - адамның тұрғын кеңістікпен өзара әрекеттесуінің мұндай тұжырымдамасы, мұнда барлық инженерлік жүйелер мен электр құрылғыларының жұмысы алдын ала белгіленген параметрлерге сәйкес бірыңғай орталықтан автоматты түрде реттеледі. Мұндай жүйе пайдаланушыларға бірнеше артықшылық береді: жайлылық, қауіпсіздік және ресурстарды үнемдеу. Жүйе жылыту және кондиционерлеу жүйелерінің үйлесімді жұмысын, сондай-ақ аталған жүйелерді қосу немесе өшіруге әсер ететін факторларды бақылауды көздейді. Басқаша айтқанда, автоматтандырылған режимде сыртқы және ішкі жағдайларға байланысты барлық инженерлік жүйелер мен электр құрылғыларының жұмыс режимдері орнатылады және бақыланады [2].

Дамыған елдерде «Смарт үй» экологиялық тұрақтылық тұжырымдамасымен ұштасады, өйткені бұл технология шектеулі табиғи ресурстарды ұтымды пайдалануға, қоршаған ортаға теріс әсерді азайтуға және адамдардың әл-ауқатын арттыруға көмектеседі. "Смарт үйдің" негізгі мақсаты - тұрғындардың жайлылығын арттыру және күнделікті өмірді жеңілдету [2].

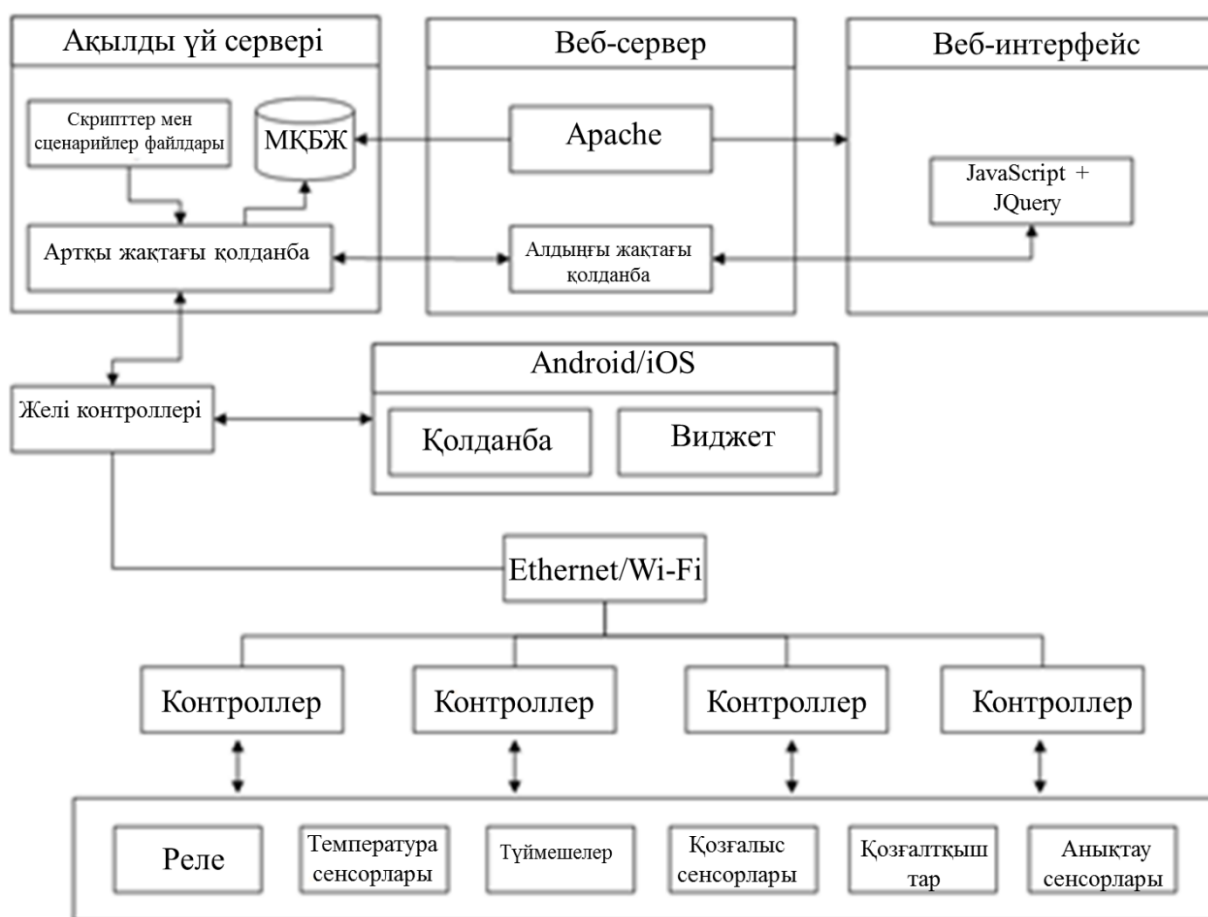
«Смарт үй» технологиясының даму тарихы өткен ғасырда басталды. «Смарт үй» ұғымы алғаш рет 1970 жылдары Вашингтон штатындағы Интеллектуалды ғимараттар институтында пайда болды: «Жұмыс кеңістігін тиімді және өнімді пайдалануды қамтамасыз ететін ғимарат...»; онда бір сым арқылы әртүрлі ақпарат түрлерін беру мүмкіндігін қарастыратын, өз уақытында революциялық болған жобалар әзірленді, бұл әртүрлі құрылғыларды басқаруға мүмкіндік берді [3].

Бұл технологияның дамуының тағы бір мысалы - Монсанто компаниясының «Болашақ үйі» (1957 жылғы аттракцион). «Монсанто» компаниясы Массачусетс технологиялық институтына жаңа типтегі тұрғын үйді бірлесіп жасау ұсынысын білдірді: толығымен пластиктен жасалған үй. Пластиктің басты артықшылығы - жеңілдігі, бұл үйдегі барлық жүйелерді

автоматтандыруды оңайлатты. Монсанто үйінде ультрадыбыстық ыдыс жуғыш машина, еденге орнатылған кондиционерлеу жүйесі, дауыс зорайтқышпен жабдықталған телефон, асүй төбесіне жасырылған сөрелер және адамның бойына бейімделетін автоматтандырылған раковина орнатылған еді.

«Смарт үй» тұжырымдамасының танымал болуы 1990 жылдардың соңында басталды. Мысалы, 1999 жылы Disney студиясы «Смарт үй» атты фильм шығарды, онда робот-қызметші басқаратын автоматтандырылған үй туралы баяндалған. Жаңа мыңжылдықта бұл тақырып кино мен баспасөзде жиі көтеріле бастады.

«Смарт үй» - бұл үйдегі электр құрылғылар мен тұрмыстық техникаларды біртұтас экожүйеге біріктіру арқылы тұрмысты автоматтандыру [4]. «Смарт үйдің» шамамен архитектурасын қарастырайық (1.1-сурет). Қашықтықтан басқару жүйесін әзірлеу кезінде әдетте мынадай негізгі құрамдастар бөлінеді: пайдаланушыға арналған қолданба, веб-сервер, "Смарт үй" сервері және сенсорлар мен датчиктерді басқаратын контроллер.



1.1-сурет – Смарт Үй технологияларының құрылымы

«Смарт үй» жүйесі өзіне мынадай компоненттерді қамтиды:

1. Мобильді қосымша немесе веб-браузер – «Смарт үй» құрылғыларын қашықтан басқару үшін қажет. Бұл компонент арқылы командалар бұлтты серверге жіберіледі және датчиктердің күйі туралы ақпарат алынады [2].

2. Веб-сервер - датчиктер мен құрылғылардың күйі туралы мәліметтерді дерекқорда сақтау үшін арналған. Сонымен қатар ол қашықтан басқару құрылғылары мен «Смарт үй» сервері арасында делдал қызметін атқарады. Бұл функция, мысалы, мобильді құрылғылардан бұлтқа командаларды жіберу және оларды өңдеп үй серверіне жеткізу арқылы жүзеге асырылады.

3. «Смарт үй» сервері - веб-серверден командаларды қабылдап, оларды әрі қарай контроллерлерге жіберуге, сондай-ақ контроллерден келген датчиктердің мәліметтерін кері бағытта жіберуге арналған.

4. Контроллер – «Смарт үй» элементтерін біртұтас жүйеге біріктіретін құрылғы [5]. Контроллер қосылған датчиктерді басқарады, серверден командалар қабылдайды және датчиктің күйі өзгерген кезде оған ақпарат жібереді. Барлық құрылғылар орталық контроллерге тіркеледі, ол веб-интерфейсті, сценарийлерді және құрылғылар арасындағы командалардың алмасуын қамтамасыз етеді.

5. Датчиктер - қоршаған орта мен тұрмыстық техниканың күйі туралы ақпарат жинайтын және оны контроллерге жіберетін құрылғылар [2]. Мысал ретінде, үйдегі температураға байланысты жылытқышты немесе кондиционерді қосатын термодатчикті атауға болады.

6. Актуаторлар - командаларды тікелей орындайтын атқарушы құрылғылар. Бұл топқа Смарт қосқыштар, Смарт розеткалар, сиреналар, климаттық бақылау құрылғылары және т.б. кіреді.

7. «Смарт үй» құрылғысы - контроллерден, датчиктен және тұрмыстық құрылғыдан тұратын құрылғы (мысалы, тоңазытқыш, термометр, перде). Олар «Интернет заттар» немесе IoT құрылғылары деп аталады.

Интернет заттар (ағылш. Internet of Things, IoT) - бұл интернетке қосылып, басқа IoT-қосымшалармен, қосылған құрылғылармен, өндірістік машиналармен және тағы басқалармен деректер алмасатын заттардың орасан зор желісі. Интернетке қосылған құрылғылар орнатылған датчиктер арқылы деректер жинап, кейбір жағдайларда оларға әсер етеді. Интернет заттар қолдану мысалдары: жылыту мен жарықты автоматты түрде реттейтін Смарт үйлерден бастап, өндірістік машиналарды қадағалап, ақауларды анықтап, автоматты түрде реттеуге қабілетті Смарт зауыттарға дейін [2].

Интернет заттар тұжырымдамасы - машиналар арасындағы өзара байланыс принципіне негізделген: адам араласуынсыз электронды құрылғылар бір-бірімен "сөйлеседі". Бұл автоматтандырудың жана, жоғары деңгейі. "Смарт үйден" айырмашылығы, мұнда жүйе түйіндері ғаламтор арқылы TCP/IP протоколдары арқылы деректермен алмасады. "Ғимараттың желілік басқару кешенінің архитектурасы IoT құрылғылары негізінде" атты мақалада [3] интеллектуалды ғимараттарды басқаруға арналған киберфизикалық жүйелерді жобалау мәселесі қарастырылған.

Интернет заттар - интернетке қосылған және басқа құрылғылармен өзін сәйкестендіре алатын физикалық нысандар желісі. Дұрыс ойластырылған IoT-қосымша энергия тұтынуды азайтып, ғимараттар мен қалалардағы қауіпсіздікті арттырып, бөлмелердегі жайлылықты жақсартып алады [4].

Интернет заттар ұйымдарға қашықтан орындалатын операцияларды басқарудың және мониторинг жүргізудің жаңа жолдарын ұсынады. Бұл технология қашықтағы объектілерді толық бақылауға мүмкіндік береді және қосымшалар мен деректер сақтау жүйелеріне үздіксіз ақпарат жеткізіп отырады.

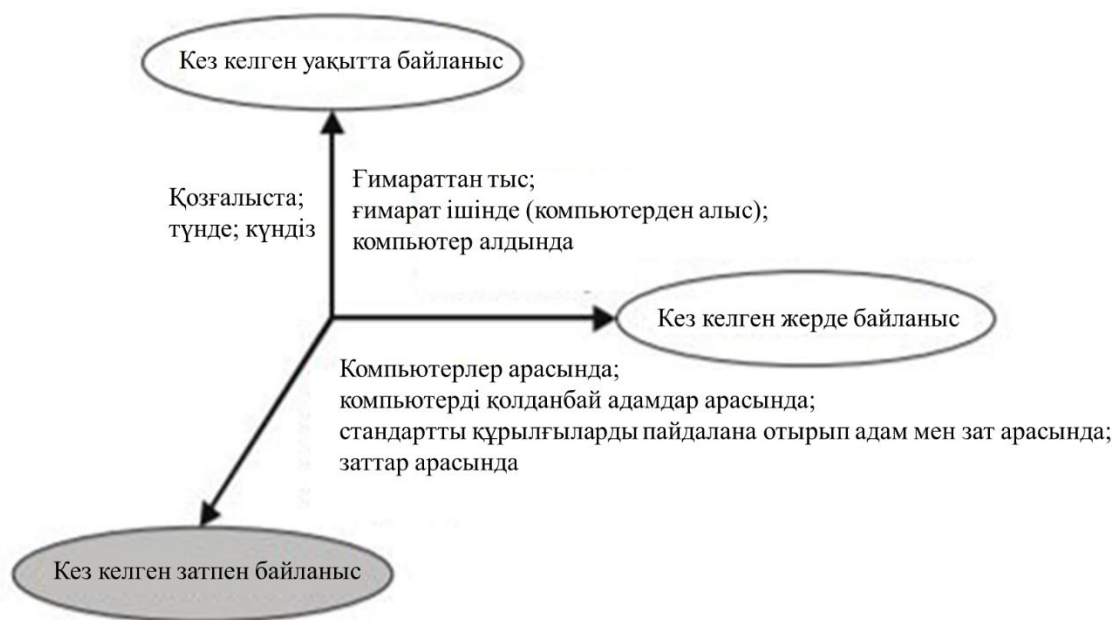
Халықаралық электр байланыс одағының (МСЭ, ағылш. International Telecommunication Union) Стандарттау бөлімшесі Интернет заттарға қатысты Y.2060 ұсынысын жариялады, ол "Интернет заттарға шолу" (Overview of the Internet of Things) деп аталады [11]. Бұл құжатта Интернет заттардың аясын сипаттайтын келесі анықтамалар берілген:

1. Интернет заттар - ақпараттық қоғам үшін жаһандық инфрақұрылым, ол физикалық және виртуалды заттарды қолданыстағы және дамып келе жатқан ақпараттық-коммуникациялық технологиялар негізінде өзара байланыстырып, неғұрлым күрделі қызметтерді ұсынуға мүмкіндік береді.

2. Зат - Интернет заттар контекстінде байланыс желілеріне біріктірілуі және сәйкестендірілетін физикалық (нақты) немесе ақпараттық әлемдегі (виртуалды) объектіні білдіреді.

3. Құрылғы - Интернет заттар контекстінде міндетті байланыс функцияларымен және қосымша түрде өлшеу, іске қосу, деректерді енгізу, сақтау және өңдеу мүмкіндіктерімен жабдықталған құрылғы элементін білдіреді.

1.2-суретте көрсетілгендей, Интернет заттар технологиясында қазіргі уақытта "кез келген уақытта" және "кез келген жерде" байланыс мүмкіндігін қамтамасыз ететін ақпараттық-коммуникациялық технологиялар енді "кез келген затпен байланыс" жаңа аспектісіне ие болды.



1.2-сурет – Интернет заттарындағы пайда болған жаңа өлшем

IoT контекстінде "заттар" - бұл физикалық әлемдегі (физикалық заттар) немесе ақпараттық әлемдегі (виртуалды заттар) объектілер, олар байланыс желілеріне біріктіріле алады және сәйкестендіріледі. Заттарда олармен

байланысты ақпарат болады, ол статикалық немесе динамикалық болуы мүмкін. Физикалық заттар физикалық әлемде өмір сүреді, оларды өлшеуге, әрекетке келтіруге және қосуға болады. Физикалық заттардың мысалдарына қоршаған орта элементтері, өнеркәсіптік роботтар, тауарлар мен электр жабдықтары жатады. Виртуалды заттар ақпараттық әлемде болады және оларды сақтау, өңдеу және оларға қол жеткізу мүмкіндігі бар. Виртуалды заттардың мысалдарына мультимедиялық контент пен қолданбалық бағдарламалық қамтамасыз ету жатады [2].

Зерттеушілер әртүрлі елдердің үкіметтері интернет заттар технологиясына қызығушылық танытып, оны енгізумен және дамытуымен айналысатын ғалымдар мен кәсіпорындарды қолдайтынын атап өтеді. Ресейде Интернет заттар баяу дамуда, бірақ өсу байқалады: 2019 жылы өсу көрсеткіші 9% болды. Қазіргі уақытта өнеркәсіп шығындарының 20%-ы дәл өнеркәсіптік Интернет заттарды (IIoT) енгізу мен қызмет көрсетуге тиесілі. 2019 жылы "Ростех" компаниясы IIoT-тың ресейлік экономика үшін пайдасы 5,5 трлн рубль деп бағаланатынын жариялады. Ең көп пайда IIoT пайдалы қазбаларды өндіру және шикізаттық емес өнеркәсіп салаларында береді, сонымен бірге ол ауыл шаруашылығында, энергетикада және логистикада тиімді қолданылады [4].

Алайда, бұл технологияның кемшіліктері де бар. Интернет заттарды қолдану бірқатар мәселелерге әкелуі мүмкін. Ең алдымен - бұл қауіпсіздік мәселелері. Компаниялар құпия деректердің сақталуына көңіл бөлуі керек. Сонымен қатар, пайдаланылатын құрылғылардың хакерлік шабуылдардан қорғалуына назар аудару қажет. Интернет заттар технологиясын дамытудың екінші елеулі кедергісі - әртүрлі протоколдардың көптігі және жалпыға ортақ стандарттардың жоқтығы [3].

Интернет заттардың негізгі мәселесі - біріктірілген автоматтандырылған жүйелерді құру үшін нақты және келісілген архитектуралардың болмауы. Бір жарық қосқышында деректерді шифрлау бір алгоритммен жүргізілуі мүмкін, ал қашықтан басқару пультінде басқа шифрлау алгоритмдері қолданылуы мүмкін. Сымсыз байланыс протоколдары да әртүрлі болуы мүмкін: бір құрылғы ZigBee қолданса, басқалары Bluetooth немесе Wi-Fi-ға сүйенеді [9]. Барлық осы параметрлер бойынша қосылу көпірлері қайталанып отырады. Тіпті тәуелсіз жүйелер қауіпсіз болса да, олар бірге сыртқы әсерлерге осал желі құруы мүмкін.

Тұрмыстық салада интернет заттардың қауіпсіздігі аса күрделі мәселе емес. Смарт үй құрылғылары интернетке қарапайым арналар арқылы қосылады. Олар жіберетін ақпарат вирустар мен киберқатерлерден негізгі қорғаныс талап етеді. Тіпті жаппай кибершабуыл болған жағдайда да бұл үлкен апатқа әкелмейді. Бұдан бөлек, үй құрылғылары әдетте жаппай өндіріледі, ал артықша қорғау олардың бағасын күрт арттырып жіберуі мүмкін, бұл сұранысты төмендетеді [8].

Ал бизнес пен өнеркәсіпте жағдай әлдеқайда күрделі - зиянкестер Смарт құрылғыларға қол жеткізуге тырысуы мүмкін, бұл миллиондаған шығынға немесе өндірістік апаттарға алып келуі ықтимал. Сондықтан IoT желілерінде қауіпсіздікке ерекше назар аударылады [9].

Қорғау үшін келесі әдістер қолданылады:

1. Интернеттен оқшаулау - құрылғылар тек кеңсе немесе зауыт ішіндегі желіде жұмыс істейді.
2. Өнеркәсіптік деректерді шифрлау, мысалы, AES-256 алгоритмімен. Бұл шифрды бұзу үшін 256 биттік кілтті табу керек, ал тіпті заманауи суперкомпьютерге бұл үшін біздің ғаламшардың жасынан да көп уақыт қажет болады [4].
3. Бағдарламалық қамтамасыз ету мен операциялық жүйелерді қорғау.
4. Бұзушылықтарды анықтау және алдын алу жүйелері - бұл жүйелер бөгде адамдар жүйеге қол жеткізуге әрекет жасаған кезде ескерту береді [4].

Қазіргі уақытта бизнестегі процестерді цифрландыру жаһандық деңгейде жүріп жатыр, бұл еңбек өнімділігін арттыру, жұмыстардың сапасын жақсарту және өндіріс қауіпсіздігін қамтамасыз ету мақсатында жүзеге асуда. Цифрландыру - заманауи үрдіс, жұмыс кеңістігін жетілдіру және автоматтандыру қарқынды жүріп жатыр. Цифрландыру ұғымы цифрлық технологияларға негізделген. "Интернет заттар" - бұл интернет пен сыртқы әлеммен байланысқан физикалық және виртуалды объектілер желісі, олар бір-біріне деректерді беріп, сол деректер негізінде басқару жүйесін, экономиканы, бизнесті және әлеуметтік саланы дамыту үшін түрлі әрекеттер орындайды [1].

Смарт офис - бұл жарықтандыруды, жылыту жүйесін, желдетуді, сумен жабдықтауды, қауіпсіздікті, аудио/бейне жабдықтарды және басқа да инженерлік жүйелерді басқаруға арналған автоматтандырылған жүйе. Бұл жүйе иесінің қалауы бойынша оңай бейімделіп, өзгертілуі мүмкін. Смарт офис әртүрлі ішкі жүйелерді біріктіріп, олардың үйлесімді жұмысын және кешеннің жоғары функционалдығын қамтамасыз етеді [15]. Бұл ішкі жүйелер арасында жұмыс істеу барысында қайшылықтардың туындауын болдырмауға және олардың үйлесімді әрекетін қамтамасыз етуге мүмкіндік береді. Мысалы, кондиционер жылыту жүйесі жұмыс істеп тұрған кезде салқындатуды бастамайды.

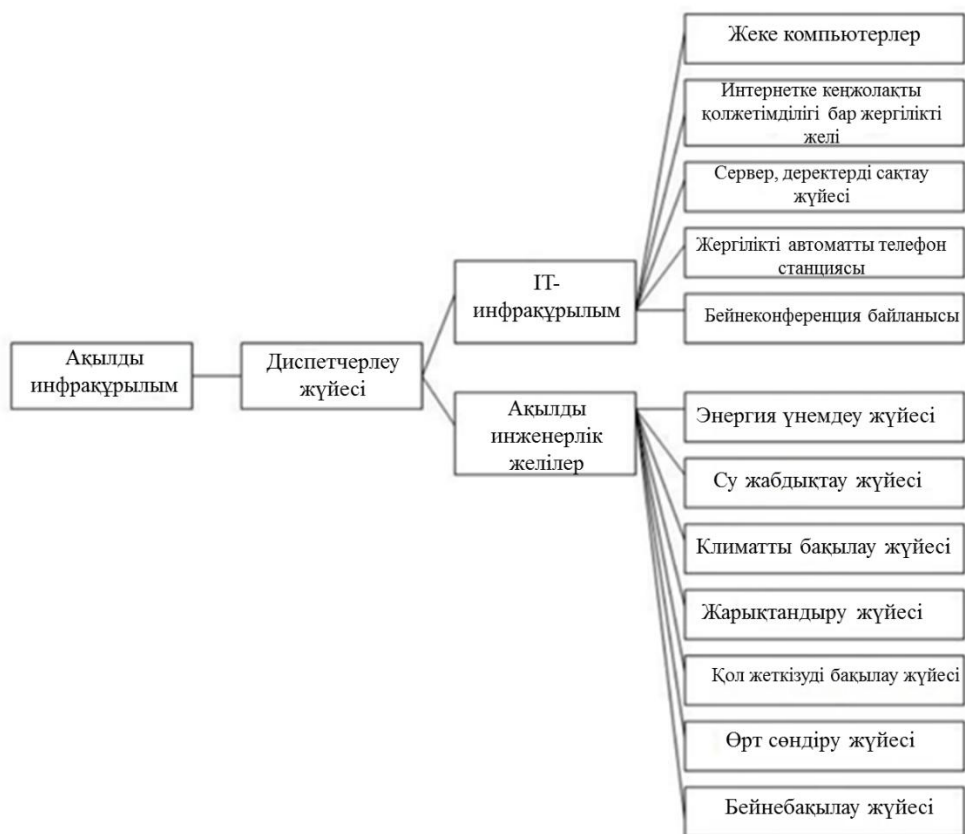
Аталған технологияларды біріктіру ғимарат ішіндегі жайлылықты қамтамасыз етеді. Барлық кешеннің параметрлерін басқаруды Смарт офис өз қолына алады. Қажет болған жағдайда Смарт офис жарықтандыруды, перделерді, кондиционерді, жылы еденді, бейне жабдықты және басқа құрылғыларды басқарады [5].

Қазіргі уақытта Ресейдегі Смарт технологиялар нарығы үшін келесі үрдістер тән:

1. Интеллектуалды офистерге арналған шешімдердің басым болуы, олардың енгізілуі сарапшылардың пікірінше қызмет нәтижелілігін едәуір арттырады және уақыт өте келе өзін ақтайды.
2. Офистік ғимараттарды салу кезінде Смарт технологияларды енгізу тәжірибесінің артуы: дайын шешімдердің кешенділігі, олардың модульділігі және жеке конфигурациялаудың мүмкіндігі [1].

Жалпы алғанда, ғимараттың Смарт инфрақұрылымы екі компоненттен тұрады:

ИТ-инфрақұрылым және смарт инженерлік жүйелер (1.3-сурет). ИТ-инфрақұрылым - бұл белгілі бір ұйым немесе компания қолданатын барлық ақпараттық технологиялар мен ресурстардың жиынтығы. Ал Смарт инженерлік жүйелер - бұл ғимараттың немесе бөлменің өмірді қамтамасыз етуге, технологиялық процестерді орындауға, жайлылықты сақтауға, энергия мен ресурстарды үнемдеуге, сондай-ақ қауіпсіздікті қамтамасыз етуге арналған жүйелері.



1.3-сурет – Интеллектуалды ғимараттың инфрақұрылымы [2]

Смарт инфрақұрылым клиентке қажетті қызметті қауіпсіздік талаптарын сақтай отырып, қызмет көрсетушіге тікелей жүгінбей-ақ алуға мүмкіндік береді.

Жүйені енгізудің негізгі артықшылықтары:

1. Офисті ұстауға кететін шығындарды азайту: Смарт офис жүйесі электр энергиясына жұмсалатын шығындарды екі есе азайтуға және су мен жылумен жабдықтауға үнемдеуге мүмкіндік береді. Осылайша, жалдау бағасы мен пайдалану шығындары төмендейді [6].

2. Өнімділікті арттыру: мысалы, келіссөз бөлмелерін іздеу және брондау сияқты күнделікті жұмыстарды жеңілдету арқылы жұмысқа қатысы жоқ әрекеттерге жұмсалатын уақыт азаяды.

3. Жайлылық: жүйе үй-жайда жұмысқа қолайлы жағдай жасайды, мысалы, температураны, ылғалдылықты және таза ауаның ішкі және сыртқы айналымын қолдайды.

4. Қауіпсіздік: Смарт офис қауіпсіздік жүйесі жайлылықты қамтамасыз ету үшін бірқатар функцияларды қамтиды: күзет және өрт дабылы жүйелері, кіруді бақылау, инженерлік қосалқы жүйелердің күйін бақылау және бейнебақылау [2].

5. Офис алаңын тиімді пайдалану: Смарт шешімдер жұмыс кеңістігін оңтайландыру арқылы оны босатуға көмектеседі.

1.2 Интернет заттары жүйелерін стандарттау

Интернет заттар жүйелері ең жоғары танымалдыққа 2010–2017 жылдары ие болды, сол кезде терминалдық құрылғылар арзандап, деректерді қауіпсіз әрі жылдам тасымалдауға арналған технологиялар пайда болды және Интернет пен өзара әрекеттесу протоколдары қарқынды дамыды. Бұл факторлар арзан әрі қарапайым терминалдық құрылғылардың көптеп шығуына оң әсерін тигізді, олардан қысқа мерзімде дайын шешімдер жинауға мүмкіндік болды. Қарапайым шешімдермен қатар нарықта күрделі әрі тармақталған логикасы бар кәсіби жүйелер де пайда бола бастады. Мұндай жүйелерді қалыптастыруға тұтас компаниялар мен халықаралық комитеттер (мысалы, Industry 4.0 тұжырымдамасы және Industrial Internet Consortium, Өнеркәсіптік Интернет Консорциумы) үлес қосты.

Интернет заттар жүйелерін таңдау және құру мәселелері шетелдік әдебиеттерде кеңінен сипатталған. Бұл саладағы негізгі зерттеулер арасында [2-4] еңбектерін атап өтуге болады. Ресейде Интернет заттар жүйелерін әзірлеу мәселелері мен осы технологияның теориялық негіздері [4, 5] еңбектерінде қарастырылған, ал технологияның даму перспективалары мен стандарттау, адрестеу және желілік коммуникациялар мәселелері [5] еңбегінде қозғалған. Кейбір зерттеушілер Интернет заттар қолданбалары үшін бірыңғай бағдарламалық архитектура стандарты болуы мүмкін емес деген пікірге келеді, себебі терминнің өзі алдын ала жобалық шешімдер қабылдау үшін жеткілікті контексті ұсынбайды [6].

Дегенмен, 2015 жылы Өнеркәсіптік Интернет Консорциумы өнеркәсіптік Интернет заттар жүйелеріне қатысты жобалауды қолдау құралын әзірлеу әдістемесін жасады. Бұл әдістеме әртүрлі типтегі Интернет заттар жүйелерін жобалауға арналған. Жарияланған құжаттар арасында [6] стандартын атап өтуге болады – ол құрылым деңгейлерін, күрделілік дәрежесін, техникалық ерекшеліктер мен өнеркәсіпте мұндай жүйелерді енгізу ерекшеліктерін регламенттейді. Мұндай жүйелер күрделі бағдарламалық архитектура мен логикаға ие, бұл оларға бір уақытта көптеген күрделі құрылғылардан деректерді қабылдауға және оларды басқаруға мүмкіндік береді, сонымен қатар кеңейту мен нақты уақытта өзара әрекеттесу мүмкіндігін сақтайды. Бұл құжатты көптеген батыс компаниялары өнеркәсіптік Интернет заттар жүйелерін әзірлеу кезінде басшылыққа алды, және әдістеменің практикалық тұрғыда жоғары тиімділігін дәлелдеді [3].

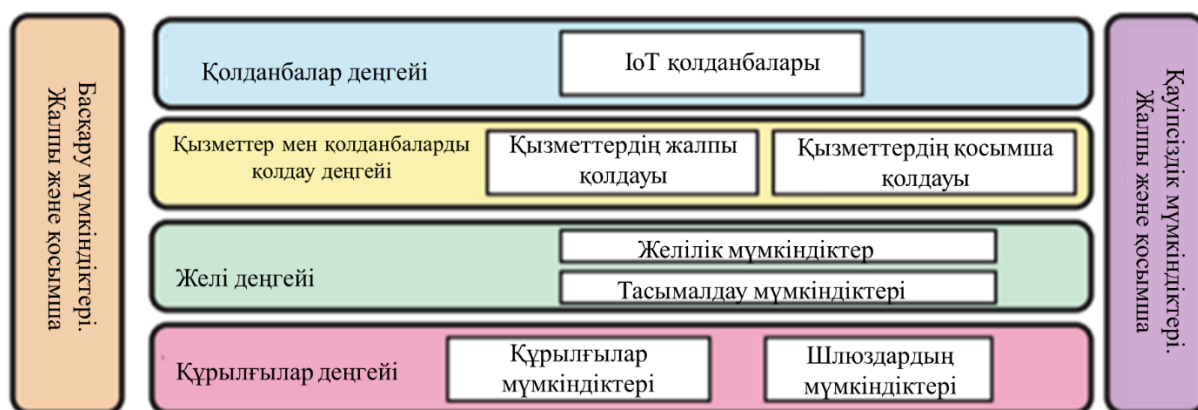
Интеллектуалды ғимараттың ерекшеліктері келесідей сипатталады [3]:

- Инженерлік жүйелердің динамикалық дамуының мүмкіндігі - жүйелерді толықтыру және өзгерту мүмкіндігі;
- Ғимараттың жағдайы туралы жедел ақпарат жинау үшін көптеген датчиктердің болуы [5];
- Жүйенің бағдарламалық және аппараттық элементтері бір өндірушіге тәуелді болмауы керек;
- Типтік құрылғыларды қолдану - контроллерлер, байланыс шиналары, енгізу-шығару модульдері және ақпаратты көрсету жүйелері [7].

Осы қасиеттерден шығатыны: интеллектуалды ғимараттағы барлық қауіпсіздік жүйелері мен инженерлік жүйелер бірыңғай ақпараттық жүйе - ғимаратты автоматтандырылған басқару жүйесі негізінде біріктірілуі керек.

МСЭ-нің Y.2060 ұсынысында IoT үшін үлгілік модель де берілген, ол NGN моделіне өте ұқсас және төрт негізгі көлденең деңгейден тұрады (1.4-суретте көрсетілген):

- IoT қолданбалар деңгейі;
- Қызметтер мен қолданбаларды қолдау деңгейі;
- Желілік деңгей;
- Құрылғылар деңгейі.



1.4-сурет – IoT үлгілік моделі

Сонымен қатар екі тік деңгей бар – басқару деңгейі және қауіпсіздік деңгейі, олар барлық төрт көлденең деңгейлерді қамтиды.

IoT қолданбалар деңгейі Y.2060 ұсынысында егжей-тегжейлі қарастырылмаған.

Қызметтер мен қолданбаларды қолдау деңгейі әртүрлі IoT объектілері үшін деректерді өңдеу және сақтау мүмкіндіктерін біріктіреді. Желілік деңгей – бұл желілердің мүмкіндіктерін қамтитын деңгей (қолжетімділік желісінің және көлік желісінің ресурстарын басқару функциялары, мобильділікті басқару, авторизация, аутентификация және есептеу функциялары).

Соңында, құрылғылар деңгейі – құрылғылар мен шлюздардың мүмкіндіктерін қамтиды.

Құрылғының функционалдығы байланыс желісімен тікелей алмасуды, шлюз арқылы алмасуды, сымсыз динамикалық adhoc-желі арқылы алмасуды, сондай-ақ энергия үнемдеу үшін құрылғының жұмысын уақытша тоқтату және қайта қосу мүмкіндіктерін қамтиды.

Шлюз мүмкіндіктері мыналарды көздейді:

- құрылғылар үшін әртүрлі интерфейстерді қолдау (мысалы, CAN-шина, ZigBee, Bluetooth, WiFi);
- қатынау желілері мен көлік желілері үшін қолдау (мысалы, 2G/3G, LTE, DSL);
- егер құрылғы интерфейстерінің және желі интерфейстерінің протоколдары әртүрлі болса, протоколдарды түрлендіру мүмкіндігін қамтамасыз ету [5].

ҚР ҚН (Құрылыс Нормалары) 4.02-23-2009 "Ғимараттар мен имараттарды автоматтандыру" Бұл нормативтік құжат ғимарат ішіндегі инженерлік жүйелерді (жылу, желдету, жарықтандыру, қауіпсіздік, сумен жабдықтау) автоматтандыру талаптарын белгілейді.

ҚР ҚН 4.02-06-2012 "Интеллектуалды ғимараттар. Жалпы талаптар"

"Ақылды ғимарат" жүйелері үшін міндетті базалық талаптар:

- Автоматтандырылған бақылау және басқару
- Энергия тиімділігі
- Қауіпсіздік жүйелері (өрт дабылы, бейнебақылау, рұқсатты басқару)
- Пайдаланушылардың қолайлылығы үшін жүйелердің интеграциясы

Ресей Федерациясында ISO 16484 (Ғимаратты автоматтандыру және басқару жүйелері) стандарты негізінде әзірленген СТО НП «АВОК» стандарттар кешені бар.

Бұл стандарттарда автоматтандырудың үш деңгейі бөлінеді, оларды автоматтандырылған басқару жүйесі қолдайды. Бұл деңгейлер келесілерді қамтамасыз етеді:

- жүйе мен персонал арасындағы өзара әрекеттестікті адам-машина интерфейсі арқылы ұйымдастыру;
- инженерлік жүйелерді контроллерлер арқылы басқару;
- перифериялық құрылғыларды басқару.

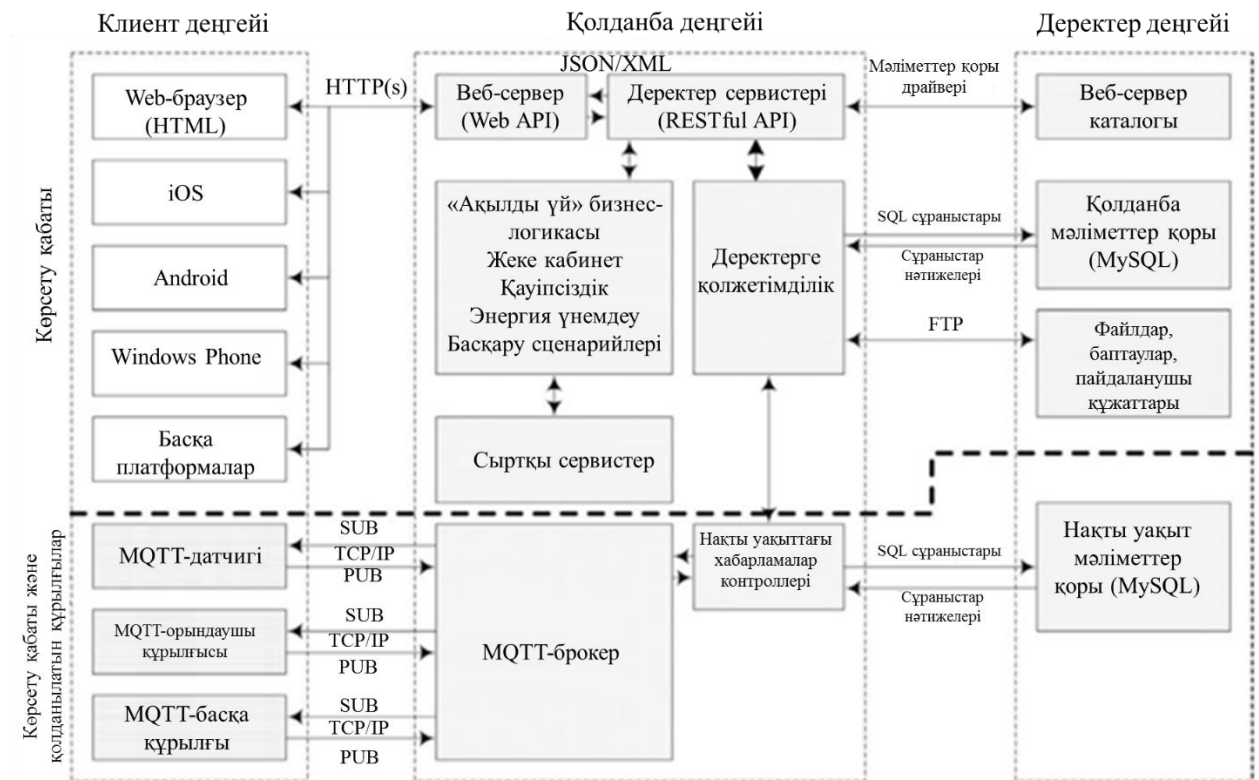
Д.В. Байғозин, Д.Н. Первухин, Г.Б. Захарова өз еңбектерінде "Смарт үй" жүйесіндегі ғимараттың инженерлік жабдықтарын басқаруға арналған бағдарламалық-аппараттық кешенді құру принциптерін тұжырымдады. Олар үш басқару деңгейін бөле отырып, келесілерді ұсынды:

- стандартты жабдықты пайдалану;
- ашық деректерді беру протоколдарын қолдану;
- қашықтан басқару мүмкіндігі бар таралған білім базасын қолдану.

О.Л. Викентьева, А.В. Кычкин, А.И. Дерябин, Л.В. Шестакова өз еңбектерінде интеллектуалды ғимаратты басқару ақпараттық жүйесінің архитектурасында үш компонент деңгейін бөліп көрсетеді (1.5-сурет):

- клиент деңгейі;

- қолданба деңгейі;
- деректер деңгейі.



1.5-сурет – Басқару ақпараттық жүйесінің архитектурасы

Клиент деңгейі – датчиктер мен атқарушы механизмдердің болуын (атқарушы құрылғылар қабаты), сондай-ақ басқару субъектісі тарапынан басқару және бақылау функцияларын жүзеге асыратын құрылғылар мен бағдарламалық камтамасыз етуді (ұсыну қабаты) қамтиды.

Қолданба деңгейі – датчиктерден ақпарат жинау және өңдеу құралдарын, сондай-ақ атқарушы механизмдерді басқаруға арналған контроллерді (атқарушы құрылғылар қабаты) қамтиды. Қолданба деңгейінің ұсыну қабаты пайдаланушының (басқару субъектісінің) ақпараттық жүйемен интернет арқылы өзара әрекеттесуін қамтамасыз ететін серверді және интеллектуалды ғимараттың бизнес-логикасын іске асыру үшін қажетті сыртқы сервистерді (пайдаланушының жеке кабинеті, авторизация және тіркеу механизмдері) қамтиды.

Деректер қорында сақталған ақпаратқа қол жеткізу үшін әртүрлі қолжетімділік механизмдері жүзеге асырылған.

Деректер деңгейі – веб-парақтарда көрсетілетін ақпарат сақталатын сервер каталогын, басқару жүйесінің жұмысын сипаттайтын деректер қорын және контроллер өңдейтін ақпарат сақталатын деректер қорын (нақты уақыт режиміндегі деректер қоры жүйесін) қамтиды [12].

Ұсынылған архитектурада екі ақпараттық модельді бөліп көрсетуге болады:

- Біріншісі – датчиктер мен атқарушы механизмдер деңгейінің моделі (датчиктер, контроллер, контроллер өңдейтін ақпаратты сақтау үшін арналған деректер қоры). Бұл модель контроллер арқылы автоматтандырылған режимде басқаруды қамтамасыз етеді. Контроллер датчиктерден ақпарат жинап, алынған параметр мәндерін белгіленген нормалардың шекті мәндерімен салыстырады және қажет болған жағдайда көрсеткіштерді түзету үшін басқару командасын датчикке жібереді. Датчиктерден алынған ақпарат нақты уақыт режиміндегі деректер қорында сақталады.

- Екіншісі – интеллектуалды ғимарат логикасының моделі, оған интерфейс, ғимараттың бизнес-логикасы, деректер қоры және коммуникациялық элементтер кіреді. Бұл модель пайдаланушы мен құрылғылар арасындағы өзара әрекеттесуді ұйымдастырады.

Датчиктер мен құрылғылардан келетін ақпаратты көрсету және бақылау үшін әртүрлі веб-сервистер мен SCADA-жүйелер (Supervisory Control And Data Acquisition) қолданылады.

Бұл деректерді серверге жіберу үшін арнайы протоколдар қажет. Қазіргі уақытта қолданыстағы HTTP негізіндегі протоколдар Интернет заттар мен машинааралық өзара әрекеттесу (Machine-to-Machine, M2M) концепциясына сай келмейді. Осы мақсатта жаңа протокол – MQTT (Message Queue Telemetry Transport) әзірленді [8].

MQTT немесе Message Queueing Telemetry Transport – ашық деректер алмасу протоколы. Брокер көптеген түйіндерден деректер жинап, оларды серверге жібереді. MQTT жариялаушы-подписчик моделіне негізделген және аралық сервер – брокер арқылы жұмыс істейді. Деректерді тасымалдау үшін TCP протоколы қолданылады [5].

MQTT протоколы міндетті түрде деректер брокерінің болуын талап етеді. Бұл – технологияның негізгі идеясы: барлық құрылғылар деректерді тек брокерге жібереді және тек брокерден алады. Брокер – TCP-сервер функцияларын орындайтын және динамикалық деректер қорымен жұмыс істейтін бағдарлама [6].

MQTT протоколы ашықтықты, қарапайымдылықты, аз ресурстарды қажет етуді және оңай енгізуді қамтамасыз ету үшін жасалған. MQTT TCP/IP желісінің үстінде жұмыс істейді және «клиент/сервер» моделін қолданады, мұнда әрбір датчик клиент ретінде әрекет етеді және брокерге қосылады. Брокер деректерді жазылушылар арасында таратады. Барлық құрылғылар немесе актуаторлар тек брокерге деректер жібереді және тек одан деректер алады [7].

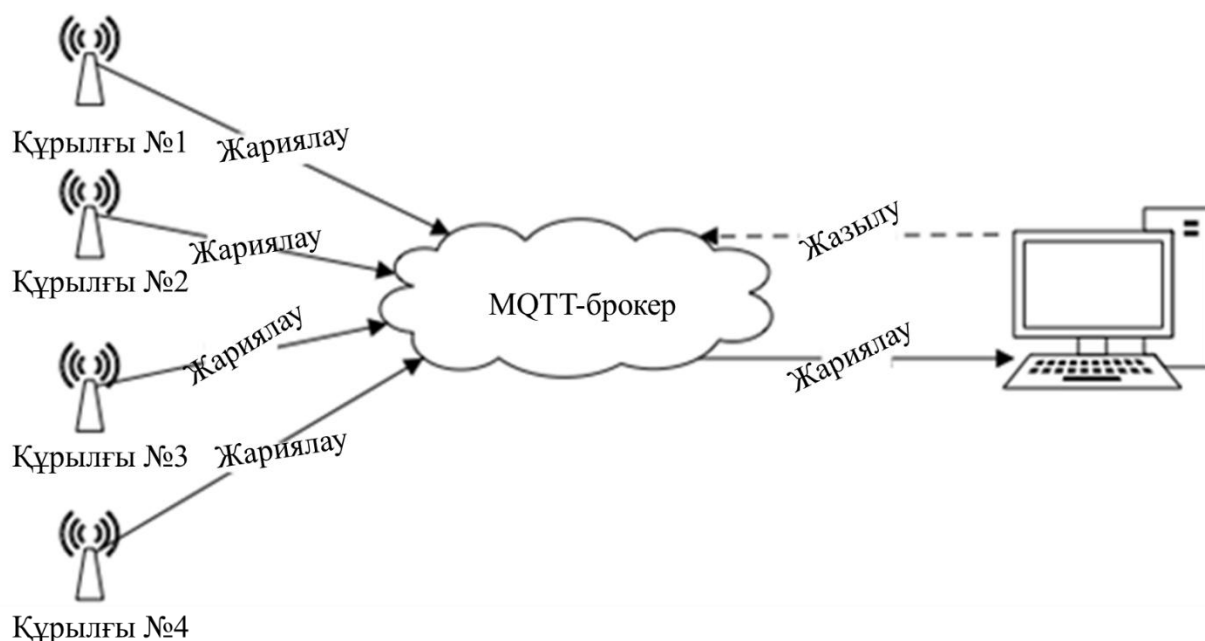
MQTT протоколы негізіндегі желіде келесі объектілер ажыратылады:

1. Жариялаушы (Publisher) – MQTT-клиент, белгілі бір оқиға туындаған кезде сол туралы ақпаратты брокерге жібереді және сәйкес топиктерді жариялайды.

2. Брокер (Broker) – MQTT-сервер, жариялаушылардан ақпарат қабылдайды және оны тиісті жазылушыларға таратады. Күрделі жүйелерде брокер алынған деректерді өңдеу мен талдауды да жүзеге асыруы мүмкін. Өртүрлі брокерлер бір-бірімен қосыла алады, егер олар бір-бірінің хабарламаларына жазылған болса.

3. Жазылушы (Subscriber) – MQTT-клиент, ол брокерге жазылғаннан кейін көп уақыт бойы оны «тындап» тұрады және брокерден қажетті топиктер бойынша келетін хабарламаларды қабылдауға және өңдеуге дайын болады [6].

Жариялаушы, жазылушы және брокер арасындағы қарапайым өзара әрекеттесу сұлбасы 1.6-суретте көрсетілген.



1.6-сурет – MQTT брокерінің жұмыс құрылымы

Температура датчиктері «жариялаушылар» болып табылады, өйткені олар тек өздерінің күйі туралы деректерді бере алады және ешқандай басқару командаларын қабылдай алмайды. Ал компьютер «жазылушы» ретінде әрекет етеді, өйткені ол MQTT брокерінен датчиктердің күйі туралы деректерді қабылдайды.

Уақыттық қатарлар – аналитикалық тәжірибеде жиі кездесетін деректер түрінің бірі.

Уақыттық қатар – бұл бір құбылыс немесе процестің қандай да бір параметріне қатысты белгілі бір уақыт ішінде жүргізілген бақылау нәтижелерінің статистикасы. Әр өлшеу нәтижесіне оны орындаған уақыт немесе уақыт шкаласындағы реттік нөмір сәйкес келеді [14].

InfluxDB – уақыттық қатарлар мен метрикаларды сақтау үшін арнайы әзірленген кластерленетін деректер қоры.

InfluxDB толықтай Go тілінде жазылған және сыртқы тәуелділіктерсіз бір ғана орындалатын файлға компиляцияланады. Пайдаланушылар деректерді жазуға және командалық жол арқылы сұраныстар жіберуге мүмкіндік алады [9].

InfluxDB артықшылықтары:

- сыртқы тәуелділіктердің болмауы;
- кластерлік режимде жұмыс істеу мүмкіндігі;
- миллиардтаған өлшеу нүктелерін сақтау мүмкіндігі;
- деректерді тегтер бойынша топтастыру арқылы жылдам және тиімді іріктеу мүмкіндігі;
- көптеген бағдарламалау тілдері үшін кітапханалардың болуы;
- SQL-ге ұқсас сұраныс тілі арқылы уақыттық қатарлармен әртүрлі операцияларды орындау мүмкіндігі.

InfluxDB DevOps мониторинг метрикаларын, сенсор деректерін (sensor data), және уақыттық қатарлар бойынша онлайн аналитика деректерін сақтау үшін арналған.

InfluxDB-де деректер уақыттық қатарлар түрінде сақталады, олардың ішінде өлшенген мәндер орналасқан. Қатар – белгілі бір уақыт мезетінде алынған мәндер жинағы (points).

Point құрылымы келесі өрістерден тұрады:

- time – уақыт белгісі (timestamp);
- measurement – қатардың атауы (мәтін түрінде);
- fields – негізгі мәндер (кілт-мағына форматында);
- tags – мән туралы метадеректер (кілт-мағына форматында).

Концептуалды түрде measurement SQL-дегі кестеге ұқсайды, онда басты индекс – уақыт, ал tags және fields кестенің бағандарына сәйкес келеді. «Tags» индекстелген, ал «Fields» индекстелмеген. InfluxDB-де миллиондаған өлшеулерді алдын ала схема анықтамай-ақ жазуға болады. Деректер InfluxDB-ге сызықтық протоколды пайдалану арқылы жазылады.

1.3 Интернет заттарымен жұмыс істейтін қолданыстағы жүйелерді талдау

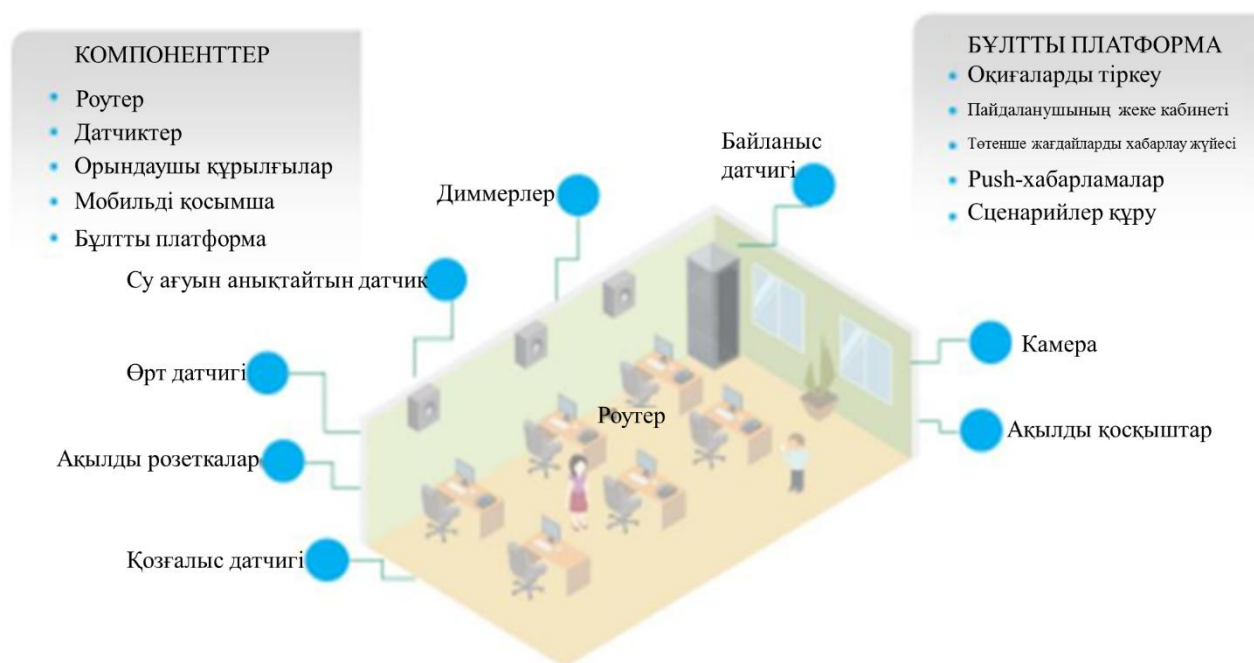
«Смарт офис» ұғымын сарапшылар екі бөлікке бөледі - технологиялық және концептуалдық.

Технологиялық жағынан «Смарт офис» «Смарт үйден» көп ерекшеленбейді [4]. Қазіргі заманғы шешімдер бизнес-орталықтың барлық инженерлік инфрақұрылымын біріктірілген басқару жүйесіне біріктіруге мүмкіндік береді. Бұл жүйе қызметкерлердің, келушілердің және автокөліктердің аумаққа кіруін, энергиямен жабдықтау, жылумен жабдықтау, сумен жабдықтау және өрт дабылы жүйелерінің жұмысын бақылайды.

Кеңсе жылжымайтын мүлкін жалға алушылар немесе сатып алушылар үшін пайдалану тәсілі екінші орында тұрады. Оларды ең алдымен кеңсенің күтіп

ұстау шығындары және оларды қалай азайту мәселесі қызықтырады. "Смарт офис" жүйесі электр энергиясына жұмсалатын шығындарды екі есе және сумен, жылумен жабдықтауға кететін шығындарды 30–40% азайтуға мүмкіндік береді. Бұл, өз кезегінде, жалдау құнын және пайдалану шығындарын төмендетеді [3].

«Смарт офис» - жүйелер мен құрылғыларды автоматты түрде басқаруға арналған бағдарламалық - аппараттық кешен. Бұл кешенде пайдаланушы Смартфон, планшет немесе веб-браузер арқылы басқаратын «Смарт офис» контроллері қолданылған, ол абоненттік құрылғыларға біріктірілген. (1.7-суретте көрсетілген).



1.7-сурет – «Смарт офис» шешімінің құрамы

"Смарт офис" жүйесінің мүмкіндіктері:

1. Ғимараттағы қауіпсіздікті қамтамасыз ету - Wi-Fi камерасы арқылы ғимараттың жағдайын қашықтан бақылау жүйесі.

2. Датчиктер жүйесінің күйін қашықтан бақылау және басқару үшін орнатылған қосымшаға хабарламалар жіберу мүмкіндігі:

- есіктердің рұқсатсыз ашылғаны туралы хабарлама;
- су ағуы туралы хабарлама;
- түтін анықталғаны туралы хабарлама;
- қозғалыс датчиктерінен хабарлама.

3. Жайлылық пен ыңғайлылықты барынша қамтамасыз ету үшін барлық жабдықты қажетті режимге сәйкес, уақыт пен күнді көрсете отырып, тізбекті немесе бір мезгілде жұмыс істеуге бағдарламалауға болады.

4. Ресурстарды ұтымды пайдалану үшін жүйеде тұтыну мөлшерін есептейтін арнайы есептеуіш датчиктер бар.

Қосымша мүмкіндіктер:

1. Микроклиматты басқару - бөлмедегі температура мен ылғалдылық деңгейін реттеуге мүмкіндік береді. Оптималды микроклиматқа жеткенде, жылытқыштар мен кондиционерлердің қуаты автоматты түрде төмендейді.

2. Жарықтандыру және электр құрылғыларын басқару: бөлмедегі табиғи жарық деңгейі жеткілікті болған жағдайда, жарық автоматты түрде өшіріледі.

"Смарт офис" шешімі ұйымдарда қауіпсіздікті қамтамасыз етудегі маңызды міндеттерді шешуге мүмкіндік береді. Енді "Смарт офис" жүйесін қолданудың артықшылықтарына тоқталайық.

- Су ағуын бақылау: бұл құрал құбырларда күтпеген жарықтар пайда болған жағдайда қолданылады. Егер су датчикке тисе, ол иесінің Смартфонына хабарлама жібереді және дыбыстық немесе жарықтық сигнал береді. Алдағы уақытта апатты жағдайларда судың берілуін автоматты түрде тоқтата алатын су ағуын жоятын датчиктер шығарылады.

- Жаңа үйлерде мұндай датчиктер су және жылу есептегіштерін бақылап, көрсеткіштерді Смартфонға жүктейді және орташа айлық нормадан асқан кезде ескерту береді.

- Қауіпсіздіктің жаңа деңгейі: есік пен терезеге орнатылатын ашылу датчигі олардың ашылғанын немесе жабық екенін бақылайды. Бұл датчик офис қауіпсіздігі үшін тиімді: егер бөгде адам кірсе, ол Смартфонға хабарлама жібереді, қатты сирена қосады немесе қауіп туралы күзет агенттігіне сигнал береді.

- Ашылу датчигі сонымен қатар бөлмедегі температура мен жарық деңгейін де бақылайды.

- Қозғалыс датчигі - көрінбейтін құрылғы, сіздің жоқ кезіңізде үйде біреу бар екенін хабарлайды. "Смарт офис" сізге ескерту жібереді, бақылау камераларын қосады және жағдайды бағалауға көмектеседі.

- Түтін датчигі дыбыстық сигнал береді және иесінің Смартфонымен байланысады [9].

- Сыртқы және ішкі бейнебақылау: камера кез келген жерде оңай орнатылады, бұл қауіпсіздікті арттырады. Бейнеағынды Смартфондағы қосымша арқылы немесе компьютердегі жеке кабинеттен көруге болады.

- Камера түсірген барлық материалдар "Ростелекомның" бұлтты сақтау қоймасында сақталады.

"Смарт үй" экожүйесінің жүрегі - контроллер. Ол кеңседегі барлық датчиктерді, камераларды және шамдарды байланыстырады және оларды басқарады. Контроллер көмегімен құрылғылар арасындағы өзара әрекет сценарийлерін жазуға болады.

Microsoft Technology Center (Майкрософт Технологиялық Орталығы) 2009 жылы Мәскеуде ашылған және әлем бойынша жұмыс істейтін 35 орталықтың бірі болып табылады.

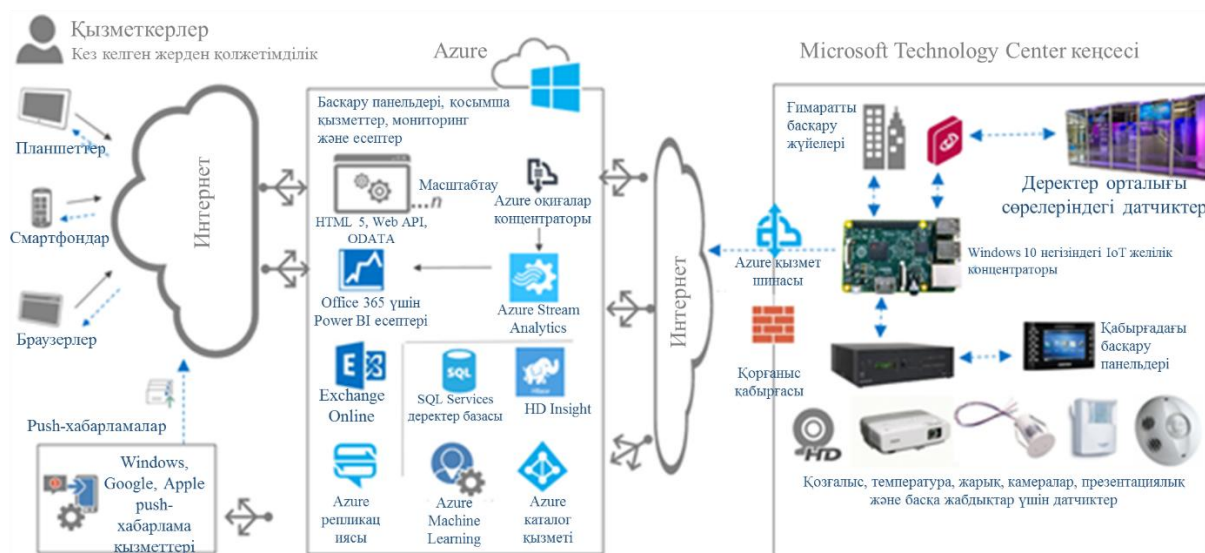
Орталықтың мақсаты - Microsoft өнімдерін енгізу сценарийлерін тестілеу, серіктестер үшін оқу семинарлары мен брифингтер өткізу, сондай-ақ конференциялар мен презентациялар ұйымдастыру.

Microsoft Technology Center шешімдері IoT архитектурасында, Microsoft Azure IoT Suite қызметіне негізделген.

Microsoft Azure - бұлтты платформа, ол IaaS (серверлер, деректер қоймалары, желілер, операциялық жүйелер) шешімдерін де, сондай-ақ бұлтты қосымшаларды әзірлеу мен орналастыруды жеңілдететін құралдар мен сервистерді (PaaS) біріктіреді.

Бұл шешімдер әзірлеушілерге нақты ұйымдардың қажеттіліктеріне бейімделген ірі масштабты қосымшаларды тез әзірлеуге, орналастыруға және басқаруға мүмкіндік береді.

Microsoft Azure қызметтері тапсырыс берушілерге қолданыстағы жабдықтарды ауыстыру, негізгі инфрақұрылымды басқару сияқты қиындықтар мен қосымша шығындардан аулақ болуға көмектеседі, осылайша IT-бюджетті тиімді басқаруды қамтамасыз етеді: пайдаланушылар тек қажетті ресурстар үшін ғана төлейді [9].



1.8-сурет – Microsoft Technology Center архитектурасы

Инфрақұрылым жұмысы жүздеген датчиктер мен атқарушы механизмдер арқылы бақыланады. Ақпарат жеткізушілер болып табылатын сенсор көздері келесілерге бөлінеді:

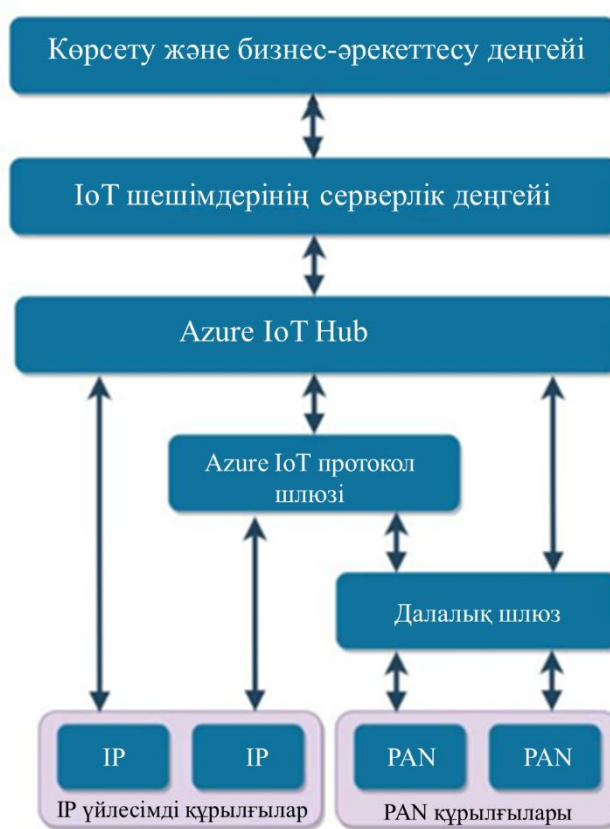
- Server Display Room датчиктері (температура, ылғалдылық, электрмен жабдықтау параметрлері, салқындату жүйесі, бейнебақылау және т.б.);
- Жарықты басқару;
- Аудио-видео және презентациялық жабдықтарды басқару;
- Бөлмелердің кестесін, конфигурациясын және жүктемесін басқару;
- Климатты басқару;
- Кіруді басқару;
- Бизнес-өнімділікті арттыру және біріктірілген коммуникацияларды басқару.

2015 жылдың 16 наурызында Microsoft корпорациясы Azure IoT Suite деп аталатын бұлтты шешімді таныстырды. Бұл шешім корпоративтік пайдаланушыларға танымал бола бастаған "Интернет заттарға" бейімделуге көмектесу үшін әзірленген болатын.

Azure IoT Suite - бұл Azure ортасымен интеграцияланған бұлтты сервистер жиынтығы, ол кез келген компанияға өздерінің IoT жобаларын іске қосуға мүмкіндік береді.

Azure IoT Suite арқылы әртүрлі желілік функциялары бар электрондық құрылғыларды Microsoft Azure бұлтына қосуға, олардан басқаруға, сақтауға және талдауға болатын деректерді алуға болады.

Бұл деректер кейін маңызды бизнес шешімдер қабылдау және процестерді автоматтандыру үшін қолданылады.



1.9-сурет – Azure IoT өнімінің жалпы архитектурасы

Microsoft Azure IoT жинағы - бұл кәсіпорын деңгейіндегі шешім, ол кеңейтілетін және алдын ала бапталған шешімдер жиынтығы арқылы жылдам жұмыс бастауға мүмкіндік береді. Бұл шешімдер Интернет заттар үшін кең таралған сценарийлерге, мысалы, қашықтан мониторинг және болжамды (алдын ала) қызмет көрсету үшін ыңғайлы.

Алдын ала бапталған шешімдер толыққанды жұмыс істейтін кешенді шешімдер болып табылады және келесілерді қамтиды:

- жұмыс бастау үшін қажетті виртуалды құрылғылар;
- алдын ала бапталған Azure қызметтері;

- нақты шешімге арналған басқару консолі.

Алдын ала бапталған шешімдер тексерілген және дайын кодпен келеді, оны нақты IoT сценарийлеріне бейімдеп өзгертуге және кеңейтуге болады.

Azure IoT Suite пакеті негізінде Azure IoT Hub қызметі жатыр. Бұл қызмет құрылғылар мен бұлт арасында хабар алмасу мүмкіндігін қамтамасыз етеді және бұлт пен басқа да маңызды IoT қызметтері үшін шлюз рөлін атқарады. Қызмет құрылғылардан нақты уақыт режимінде хабарлар алуға және оларға командалар жіберуге мүмкіндік береді. Сондай-ақ құрылғыларды басқару функцияларын да атқарады.

Azure Stream Analytics деректерді жылдам талдау мүмкіндігін қамтамасыз етеді: телеметрия деректерінің келіп түсуін өңдеу, деректерді жинақтау және оқиғаларды анықтау.

Алдын ала бапталған шешімдер Stream Analytics-ті ақпараттық хабарламаларды (мысалы, метадеректер немесе құрылғылардан келген командаларға жауаптар) өңдеу үшін пайдаланады және бұл хабарламаларды басқа қызметтерге жеткізеді.

Деректерді сақтау мүмкіндігі Azure DocumentDB қызметі арқылы жүзеге асырылады.

Телеметрия деректерін сақтау және оларды талдауға дайындау үшін алдын ала бапталған шешімдер BLOB-объектілерді сақтау қоймасын пайдаланады. DocumentDB құрылғының метадеректерін сақтауға арналған және құрылғыларды басқару мүмкіндіктерін ұсынады.

Деректерді визуализациялау мүмкіндігі Microsoft Power BI веб-қосымшасы арқылы қамтамасыз етіледі. Power BI икемділігі IoT Suite деректері негізінде интерактивті бақылау тақталарын жылдам құруға мүмкіндік береді.

Интернет заттарымен жұмыс істеуге арналған тағы бір платформа - AWS IoT Core. Бұл басқарыладыратын бұлтты платформа қосылған құрылғылардың бұлтты қосымшалармен және басқа құрылғылармен қарапайым әрі қауіпсіз өзара әрекеттесуін қамтамасыз етеді.

AWS IoT Core мүмкіндіктері:

1. AWS IoT Core миллиардтаған құрылғылармен және триллиондаған хабарламалармен жұмыс істеуді қолдайды.

2. Платформа құрылғыларды бұлтпен немесе бір-бірімен оңай байланыстыруға мүмкіндік береді.

3. AWS қолданушыға операциялық жүйені, бағдарламалау тілін, интернет-қосымша платформасын, дерекқорларды және басқа да қажетті сервистерді таңдауға мүмкіндік береді.

4. AWS IoT Core құрылғылардың деректерін сүзуге және оларды өңдеуге мүмкіндік береді.

5. Жүйе құрылғының соңғы күйін сақтап, кез келген сәтте оны оқу немесе жаңадан орнатуға мүмкіндік береді.

6. AWS қауіпсіздікті күшейту үшін кешенді әдісті қолданады: физикалық, операциялық және бағдарламалық қорғау құралдарын қамтиды.

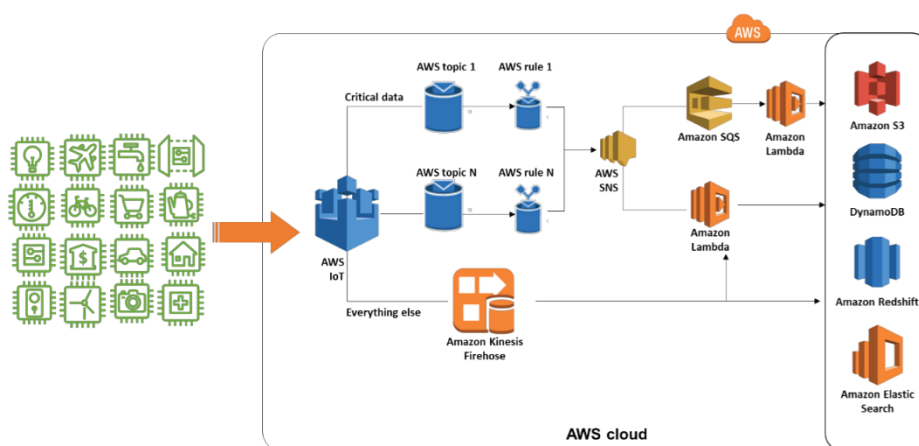
AWS IoT Core - IoT құрылғыларды серверлерді бөлу немесе оларды басқару қажеттілігінсіз AWS Cloud-қа қосуды қамтамасыз етеді. AWS IoT Core миллиардтаған құрылғылармен және триллиондаған хабарламалармен сенімді әрі қауіпсіз жұмыс істеуді қамтамасыз етеді, хабарламаларды AWS-тің өзге қызметтеріне немесе басқа құрылғыларға бағыттайды.

AWS IoT Core көмегімен қосымшалар барлық құрылғыларды үздіксіз бақылап, олармен өзара әрекеттесе алады, тіпті құрылғылар оффлайн режимде болғанда да.

AWS IoT Core сондай-ақ келесі AWS және Amazon қызметтерімен жұмысты жеңілдетеді:

- AWS Lambda;
- Amazon Kinesis;
- Amazon S3;
- Amazon SageMaker;
- Amazon DynamoDB;
- Amazon CloudWatch;
- AWS CloudTrail;
- Amazon QuickSight;
- Alexa Voice Service.

Сонымен бірге, AWS IoT Core құрылғылардан алынатын деректерді жинау, өңдеу және талдау үшін IoT қосымшаларын оңай жасауға мүмкіндік береді, әрі бұл үшін қандай да бір инфрақұрылымды басқару қажет болмайды.



1.10-сурет – AWS IoT Core архитектурасы

AWS IoT Core әртүрлі IoT құрылғыларын қосу және оларды басқару үшін нақты қолдану мысалдарына ең қолайлы қосылу протоколын таңдауға мүмкіндік береді.

AWS IoT Core келесі протоколдарды қолдайды:

- MQTT (хабарлама кезегі және телеметриялық деректерді жеткізу);
- HTTPS (қолданушы қауіпсіздігін күшейткен гипермәтіндік тасымалдау протоколы);

- MQTT арқылы WSS (қауіпсіз WebSockets арқылы байланыс);
- LoRaWAN (энергияны үнемдейтін әрі алыс қашықтыққа арналған сымсыз желі).

Құрылғы шлюзі - IoT құрылғылары үшін AWS-ке қосылу нүктесі ретінде қызмет етеді.

Құрылғы шлюзі барлық белсенді құрылғы қосылымдарын басқарады және әртүрлі протоколдардың семантикасын іске асырып, құрылғылардың AWS IoT Core-пен сенімді әрі тиімді байланысын қамтамасыз етеді. Қазіргі уақытта құрылғы шлюзі келесі протоколдарды қолдайды:

- MQTT,
- WebSockets,
- HTTP 1.1.

MQTT немесе WebSockets арқылы қосылған құрылғылар үшін құрылғы шлюзі ұзақ мерзімді екіжақты қосылымды қолдайды, бұл құрылғыларға кез келген уақытта аз кідіріс арқылы хабарлама жіберуге және қабылдауға мүмкіндік береді.

Құрылғы шлюзі толықтай басқарылады және автоматты түрде масштабталады, миллиардтан астам құрылғыны қолдай алады және пайдаланушылардан қандай да бір инфрақұрылымды басқаруды талап етпейді. AWS IoT қызметіне деректерді көшіруді қалайтын клиенттер үшін құрылғы шлюзі инфрақұрылымдарды аз әсермен көшіру мүмкіндігін ұсынады, осылайша қолданыстағы архитектура мен IoT құрылғыларына әсер етуді барынша азайтады.

2 Arduino негізінде IoT қауіпсіздік жүйесін құру

2.1 IoT негізіндегі қауіпсіздік тұжырымдамасы

Интернет заттар (IoT) - интернет арқылы интернетке қосылған физикалық құрылғыларды басқаруға/бақылауға арналған дамып келе жатқан технология.

Негізгі тұжырымдамасы - Смарт датчиктердің бір-бірімен тікелей, адамның араласуынсыз өзара әрекеттесуі арқылы жаңа қолданбалар класының кең таралуына жағдай жасау.

IoT пайдаланушыларға интернет арқылы ыңғайлы графикалық интерфейс көмегімен сандық құрылғылар жиынтығын оңай басқаруға мүмкіндік береді. Бұл бөлімде Интернет заттар концепциясына негізделген, заманауи IoT құралдарын қолданатын қауіпсіздік жүйесінің схемасы сипатталады.

Бұл бөлімде сипатталған қауіпсіздік жүйесін құру үшін Arduino Uno тақшасын қолдану ұсынылады.

Контроллерге адамның қозғалысын анықтайтын ультрадыбыстық датчик қосылады, ол қозғалыс анықталған кезде пьезодинамикке басқару сигналы беріледі.

Сонымен қатар, Arduino-ға GSM модулін қосуға болады, ол қозғалысты анықтаған кезде хабарлама жіберу және қабылдау үшін қолданылады.

Төтенше жағдай орын алғанда, динамик арнайы тонда дабыл сигналы шығарады және қорғалатын аймақ иесіне дабыл хабарламасын жібереді.

Бұдан бөлек, Wi-Fi модулі арқылы интернетке қосылып, деректерді жіберу және қабылдау мүмкіндігі қарастырылады.

Алынған деректер бұлтты серверлік мониторинг панелінде проекцияланып, объектідегі бұзушының қозғалыс үлгісі жасалады.

Деректерді сақтау үшін ThingSpeak деп аталатын бұлтты сақтау жүйесі қолданылады.

2.2 Қауіпсіздік жүйесіндегі IoT-қа шолу

IoT ұғымын алғаш рет 2000 жылдардың басында Кевин Эштон ойлап тапты [1], ол бизнес жүргізу кезінде деректерді интернет арқылы беру үшін RFID технологиясын қолданды.

Бұл бастаманы Procter & Gamble компаниялары қолдады.

Тұжырымдама қарапайым, бірақ әсерлі болды: күнделікті өмірдегі заттарды сәйкестендіру құралдарымен және сымсыз байланыспен жабдықтау арқылы оларды бір-бірімен байланыстыру және компьютерлер арқылы басқару мүмкін болды.

IoT физикалық құрылғыларды интернетке сымды немесе сымсыз желілер арқылы қосуды білдіреді. Бұл датчиктер әртүрлі жергілікті байланыс түрлерін қолдана алады, мысалы:

- RFID,

- NFC,
- Wi-Fi,
- Bluetooth және т.б.

Датчиктер кең ауқымда GSM, GPRS, 3G және LTE сияқты технологиялар арқылы да өзара әрекеттесе алады.

IoT-тың үш негізгі құрамдас бөлігі:

1. Коммуникация:

IoT-тың басты мақсаты - физикалық құрылғылар, жүйелер және адамдар арасындағы байланысты қамтамасыз ету. Мысал ретінде: медицина саласында пациент туралы маңызды ақпаратты жылдам жіберу арқылы шұғыл шаралар қабылдауға болады. Тасымалдау саласында орналасу құрылғысы арқылы кемеңіз қозғалысын бақылауға болады. Барлық жағдайда коммуникация негізгі рөл атқарады.

2. Басқару және автоматтандыру: Бүгінгі күні тұтынушылар IoT арқылы құрылғыларды тікелей немесе қашықтан басқара алады. Мысалы, автокөлікті құлыптан ашу немесе кір жуғыш машинаны қашықтан қосу мүмкіндігі. Сол сияқты, қозғалысты анықтайтын датчик орнату арқылы белгілі бір аймақты бақылауға болады.

3. Құндылық: IoT технологиясының негізгі пайдасы - шығындарды азайту мүмкіндігі. Датчиктерден алынған жаңа ақпараттың көмегімен компаниялар құрал-жабдықтың істен шығуынан болатын тоқтап қалуды азайта отырып, техникалық қызмет көрсету шығындарын төмендете алады. Датчиктер сонымен қатар басқару үлгілерін немесе өмір салты параметрлерін өлшеп, отын шығынын азайтуға немесе жайлы өмір сүру жағдайларын ұсынуға мүмкіндік береді.

2.3 IoT қауіпсіздік жүйесінің құрылымы

Бүгінгі тез өзгеріп жатқан әлемде қауіпсіздік жүйелеріне деген сұраныс артып келеді.

Адамның араласуынсыз жұмыс істейтін IoT технологиясы негізінде құрылған Смарт жүйелерге сұраныс жоғары.

IoT - интернет арқылы интернетке қосылған физикалық құрылғыларды басқару/бақылау үшін қолданылатын дамып келе жатқан технология (2.1-сурет).

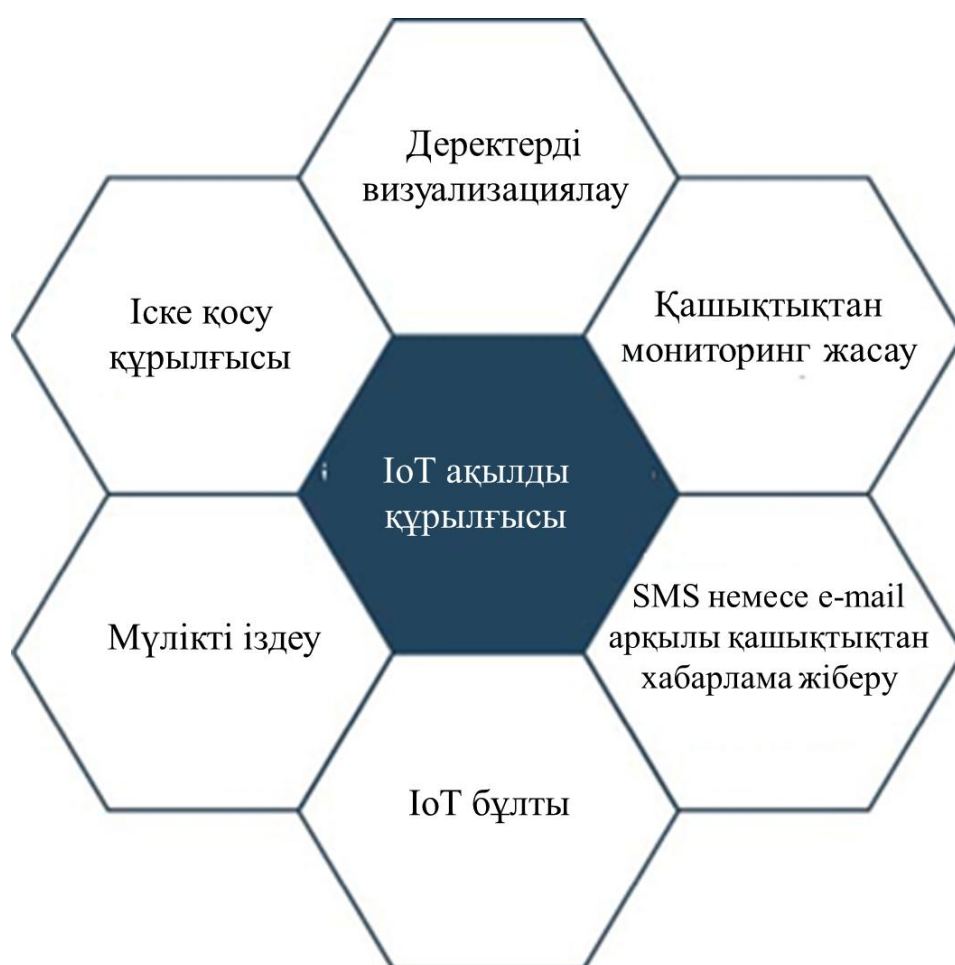
Бұл жұмысыта зерттеудің негізі болып табылатын Arduino Uno тақшасын қолдану қарастырылған. Arduino тақшасы бастапқыда ATmega8 микроконтроллері негізіндегі қымбат тақшаларды арзандату мақсатында жасалған [2, 3]. Arduino - бұл ашық бастапқы кодты электрондық платформа [4], оның құрамына аппараттық қамтамасыз ету (тақша) және оны бағдарламалауға арналған бағдарламалық жасақтама кіреді. Arduino әртүрлі кәсіби емес пайдаланушыларға - суретшілерге, дизайнерлерге, әуесқойларға және интерактивті объектілер мен орталарды жасағысы келетін кез келген адамға арналған.

Arduino тақшасын алдын ала жиналған түрде сатып алуға немесе оны қолмен жинауға болады.

Қолданушылар тақшаны өз қажеттіліктеріне бейімдеп, өз нұсқаларын жасап тарата алады.

Arduino тақшасы құрамында микроконтроллер бар, ол Arduino бағдарламалау тілінде бағдарламаланады. Бұл тіл негізінен C/C++ тілінің жеңілдетілген нұсқасы болып табылады [5] және «эскиздер» (sketches) түрінде негізгі бағдарламалық құрылымдарды, айнымалыларды және функцияларды қолданады.

Кейін олар толыққанды C++ бағдарламасына түрленеді.



Сурет 2.1-IoT жүйесінің макеті

Деректерді жіберу және қабылдау үшін Arduino тақшасы ультрадыбыстық датчикпен қосылған және мәліметтерді тікелей мониторға шығару үшін реттік интерфейсті пайдаланады.

Ультрадыбыстық датчиктер [6] - дыбыс ауқымынан жоғары жиіліктердегі (шамамен 40 кГц) акустикалық толқындардың қасиеттерін өлшеуге негізделген құрылғылар.

Олар жоғары жиілікті дыбыстық импульс шығарып, кейін эхо-сигналдың қасиеттерін қабылдап, бағалау арқылы жұмыс істейді.

Қазіргі уақытта нарықта әртүрлі ультрадыбыстық датчиктер кең таралған [7].

Arduino тақшасын датчикпен қосу үшін макет тақшасы қолданылады [8].

Осы жинаққа дабыл құрылғысы да қосылған: егер бұзушы қорғалатын аймаққа кіріп, ультрадыбыстық датчиктің әрекет ету аймағына түссе, ол дыбыстық дабыл береді.

Дыбыстық сигнал шығаратын бұл құрылғы пьезо-динамик деп аталады [9].

Пьезо-динамиктер үзілісті дыбыстық сигналдар, тондық дыбыстар және дабыл дыбыстарын жасау үшін қолданылады.

Бұл шағын, бірақ қатты дыбыс шығаратын құрылғы тік бұрышты пішіндегі (3–30 В аралығында) электрлік импульспен басқарылады.

Оны пайдалану үшін бір ұшын жерге қосып, екінші ұшын таймер немесе микроконтроллерден келген тік бұрышты толқын сигналына қосу керек.

Ең қатты дыбыс шығару үшін шамамен 4 кГц жиілік орнату ұсынылады, бірақ құрылғы 2–10 кГц диапазонында да жақсы жұмыс істейді.

Дыбысты күшейту үшін екі шығысты да микроконтроллерге қосып, сигналды ауыстырып, дыбысты екі еселеуге болады.

Осы Arduino жинағы ультрадыбыстық датчикпен және зуммермен бірге қосымша түрде GSM [10] немесе GPRS(Global Packet Radio Service) модульдерімен де өзара әрекеттесе алады.

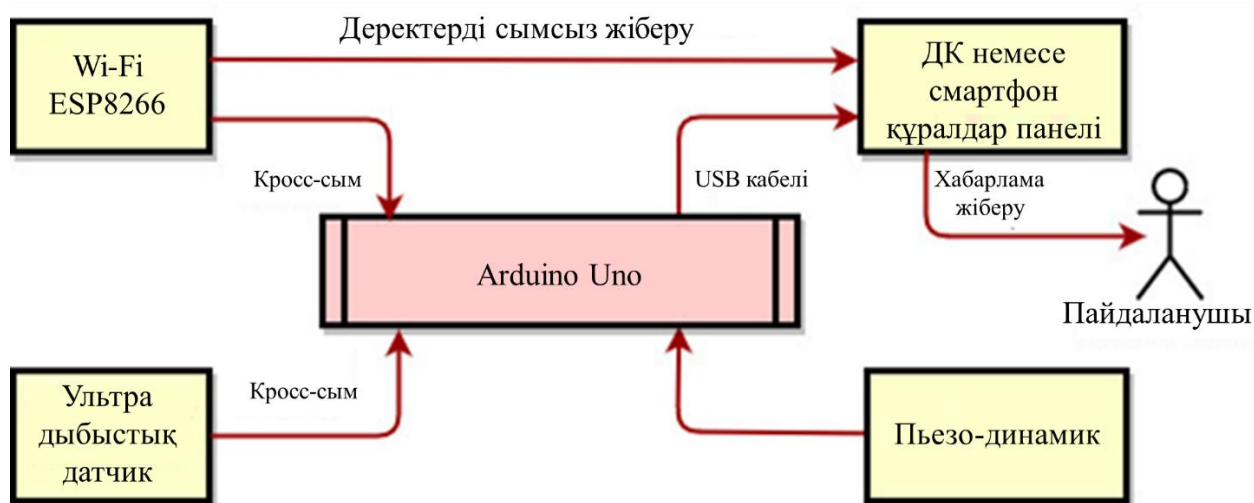
Кесте 2.1 – Қажетті компоненттер тізімі

Компонент	Модель атауы	Үйлесімділік	Жұмыс істеу мерзімі
Arduino	Arduino UNO	-	6 ай
Датчик	Ультрадыбыстық датчик	Кез келген Arduino нұсқасымен үйлесімді	8 ай
GSM модулі	SIMCom 900	Тек Arduino Uno үшін үйлесімді	1 жыл
Wi-Fi модулі	ESP8266/32	Тек Arduino Uno үшін үйлесімді	1 жыл
Сирена	Пьезо-датчик	Кез келген Arduino нұсқасымен үйлесімді	6 ай
Кроссовер сымы	Тікелей	Кез келген Arduino нұсқасымен үйлесімді	Бұзылғанға дейін

IoT қолдану мысалдары:

1. Смарт автотұрақ - қаладағы бос автотұрақ орындарын бақылау;
2. Ғимараттардың тұтастығын бақылау - ғимараттардың, көпірлердің және тарихи ескерткіштердің дірілін және материалдық күйін қадағалау;
3. Қалалық шу карталары - нақты уақыт режимінде шудың деңгейін бақылау;

4. Смартфондарды анықтау - Wi-Fi немесе Bluetooth интерфейстері арқылы жұмыс істейтін құрылғыларды табу (iPhone, Android);
5. Электромагниттік өріс деңгейі - ұялы байланыс станциялары мен Wi-Fi маршрутизаторларынан шығатын энергияны өлшеу;
6. Көлік кептелістері - көлік және жаяу жүргінші қозғалысын бақылау, қозғалысты оңтайландыру үшін;
7. Смарт жарықтандыру - ауа райы жағдайына бейімделген көше жарықтандыруы;
8. Ауыз суды бақылау - қаладағы су сапасын бақылау;
9. Өзенге төгілулерді анықтау - зауыттардан өзенге ағызылған қалдықтарды немесе судың ағуын анықтау.



2.2-сурет – Қауіпсіздікті қамтамасыз ету жүйесінің архитектурасы

Қолданыстағы жүйе адамдарды, заттарды, технологияларды және қауіпсіздік жүйелерін қолданады, бірақ олардың сенімділігі төмен.

Камералар белгілі бір жерлерге тұрақты түрде орнатылады және оқиғалар ағынын бақылайды.

Барлық камералардан алынған бейне ақпарат орталық жүйеге жіберіледі, ол адам тарапынан үнемі мониторингті қажет етеді.

Қолданыстағы жүйенің негізгі кемшіліктері:

- Нақты уақыттағы хабарламалар жоқ;
- Толық қауіпсіздіктің кепілдігі жоқ;
- Түнде немесе жарықсыз уақытта жүйе жұмыс істемейді;
- Полицияның жедел араласуы қарастырылмаған.

Сонымен қатар, жарық жетіспейтін немесе энергия тапшылығы бар жерлерде жүйенің сенімділігі төмен. Электр энергиясы өшкен кезде жүйе толық өшеді және қайта іске қосу керек болады, бұл қауіпті және адамның араласуын талап етеді.

Қызмет көрсету құны жоғары болғандықтан, бұл жүйе орта таптағы және төмен кірісті адамдар үшін қолжетімді емес.

2.4 Қауіпсіздік жүйесі бойынша қолданыстағы IoT жүйелерін талдау

Ұсынылған жүйе автоматтандырылған қауіпсіздік жүйесі болады.

Бұл жүйе қауіп туралы сигнал беріп, иесіне және бұлтты серверге ақпарат жібереді (кейінгі талдау үшін).

Жүйенің автоматтандырылуы үшін Arduino Uno тақшасы қолданылады, ол көптеген физикалық құрылғылармен үйлесімді.

Осы жоғарыда сипатталған компоненттерді пайдалана отырып құрылған жүйе (2.2-суретті қараңыз) адамның бақылауынсыз кез келген қозғалысты немесе әрекетті анықтап, бұл ақпаратты бақылау панеліне жеткізеді.

Қозғалыс анықталған кезде дабыл сигналы GSM модулі арқылы тіркелген мобильді телефонға жіберіледі және Wi-Fi модулі көмегімен бұзушының қозғалыс үлгісі бақылау панелінің экранына шығарылады.

GSM модулі тіркелген пайдаланушыға хабарлама жіберу үшін арналған. Бұл үшін SIMCOM-900 модулін қолдану ұсынылады, ол мобильді телефоннан хабарлама жіберуге және қабылдауға мүмкіндік береді.

GSM қолданудың негізгі мақсаты - пайдаланушы интернетке қосылмаған болса да, оған қолжетімділікті қамтамасыз ету.

GSM модулінің жұмысын тексеру үшін Arduino IDE қабығындағы арнайы терезеде хабарлама жіберіп, қабылданғанын тексеруге болады.

Wi-Fi модулі ультрадыбыстық датчиктен алынған ақпаратты бұлтқа жіберу үшін орнатылады, ол кейінгі талдау үшін қолданылады.

Егер деректерді үнемі GSM модулі арқылы жіберетін болсақ, онда байланыс шығындары жоғары болуы мүмкін.

Оның орнына Wi-Fi модулін пайдалану ұсынылады, ол Arduino мен бұлттық сервер арасында байланыс орнату үшін Wi-Fi маршрутизаторына қосылады.

Бұл схема үшін ESP8266/32 Wi-Fi модулін қолдану ұсынылады.

GSM модулі - GSM модемінен, қуат беру тізбегінен және компьютермен байланыс интерфейстерінен (RS-232, USB және т.б.) тұрады.

Бұлттық сервер ретінде ThingSpeak сервері ұсынылады [11]. ThingSpeak - тек қана IoT-қосымшаларды жасауға арналған платформа.

ThingSpeak келесі мүмкіндіктерді ұсынады:

- нақты уақытта деректерді жинау;
- жиналған деректерді диаграммалар түрінде визуализациялау;
- веб-сервистермен, әлеуметтік желілермен және басқа да API-мен жұмыс істеуге арналған плагиндер мен қосымшаларды құру.

ThingSpeak-тің негізгі элементі - ThingSpeak каналы. Ол келесіден тұрады:

- 8 деректер сақтау өрісі - кез келген типтегі деректерді (датчиктен немесе басқа құрылғыдан) сақтау үшін қолданылады;

- 3 орналасу өрісі - ендік, бойлық және биіктік мәліметтерін сақтау үшін;

- 1 күй өрісі - арнада сақталған деректерді сипаттайтын қысқа хабарлама.

ThingSpeak қолдану үшін алдымен тіркеліп, арна құру керек. Содан кейін деректер жіберуге және оларды өңдеп, қайта алуға болады.

Функционалдық жүйеге қойылатын талаптар

Аппараттық талаптар:

- Arduino Uno;
- ультрадыбыстық датчик;
- GSM модулі;
- Wi-Fi модулі ESP8266/32;
- пьезо-динамик;
- макет тақшасы;
- кроссовер сым.

Бағдарламалық талаптар:

- Arduino IDE интеграцияланған әзірлеу ортасы;
- деректерді сақтау үшін бұлттық сервер;
- IoT симуляция платформасы (ThingSpeak);
- деректерді талдау үшін бақылау панелі.

Ультрадыбыстық датчиктен келіп түсетін деректер негізінде Arduino тақшасы кез келген күдікті қозғалысты анықтаған кезде дабыл сигналын қосады және бір мезгілде меншік иесінің телефон нөміріне хабарлама жібереді.

Сонымен қатар, датчик деректері Wi-Fi модулі арқылы ThingSpeak серверіне жіберіледі.

Бұл жұмыстың қолдану саласы - үй қауіпсіздігі жүйелерінен бастап көлік қауіпсіздік жүйелеріне дейін, супермаркеттерді бақылау және деректерді талдау.

Адам араласуынсыз қауіпсіздікті IoT технологиясы арқылы қамтамасыз етуге болады.

Бұл жүйе кез келген басып кіруді автоматты түрде анықтап, құрылғының жұмыс істеп тұрғанын немесе істемей қалғанын тексеру үшін бұлтқа жіберілген ақпаратты пайдаланады.

Жиналған ақпарат құрылғыны қызмет көрсету үшін немесе тіркелген пайдаланушыға ескерту хабарламаларын жіберу үшін қолданылуы мүмкін.

Осылайша, бұл жүйе үй автоматтандыру, офис қауіпсіздігі жүйелері сияқты көптеген салаларда қолданылуы мүмкін.

3 Arduino негізінде жасалған үй қауіпсіздігіне арналған смарт жүйе

Технологияның қарқынды дамуы тұрғын үйлердің қауіпсіздігі мен қорғанысын арттыруға арналған үй қауіпсіздік жүйелеріне деген қызығушылықты күшейтті.

Жүйе сенсорлар жиынтығы мен Arduino микроконтроллерін пайдалана отырып, ықтимал бұзушыларды анықтайды және дабылды дереу іске қосады.

Бұл зерттеу тиімділікті, сенімділікті және үнемділікті көрсетеді, сондықтан оны үй қауіпсіздігін қамтамасыз етуде қолдануға болады.

Дипломдық жұмыста IoT қосымшасы ретінде Arduino пайдалана отырып, үйге арналған дабыл жүйесін жобалау және іске асыру баяндалады.

Бұл жүйеге арналған интернет байланыс модулі үй желісінің орталық қуат көзіне қосылады және интернет арқылы қолжетімді болады.

Сымсыз байланыс үшін статикалық IP мекенжай қолданылады.

Үйді автоматтандыру әртүрлі қосымшаларға негізделеді, оларды Google Assistant немесе пайдаланушының веб-қосымшасындағы дауыс тану командалары арқылы басқаруға болады.

3.1 Arduino негізінде IoT арқылы жекеменшік мүлікті қорғау жүйесін талдау

Интернет заттар (IoT) - электронды компоненттері бар физикалық құрылғылар желісі, олар өзара немесе нақты уақыттағы ортамен әрекеттесе алады.

Соңғы бірнеше жылда IoT әдістемесі адамдардың күнделікті өмір салтын өзгертіп, озық қызметтер ұсынды.

Медицина, электроника, гендік терапия, ауыл шаруашылығы, Смарт қалалар және Смарт үйлер сияқты салаларда Интернет заттардың кеңінен орныққаны байқалады [1].

Бүгінгі күні үйге арналған дабыл жүйесіне деген қажеттілік өте өзекті.

Қылмыстың күн санап артып келе жатқанын ескере отырып, қауіпсіздікті қамтамасыз ететін бір жүйе қажет.

Қазіргі заманда нарықта қолжетімді дамыған қауіпсіздік жүйелері бар болғанымен, олар барлығына бірдей қолжетімді емес [2].

Сондықтан біз бұзушының қозғалысын тыңдап, дабыл қосатын пайдалы электрондық құрылғы жасауды мақсат етеміз.

Осы жұмыстың басты идеясы - барлық материалдардың құрамында адамның көзіне көрінбейтін инфрақызыл жарық түрінде белгілі бір жылу энергиясы бар.

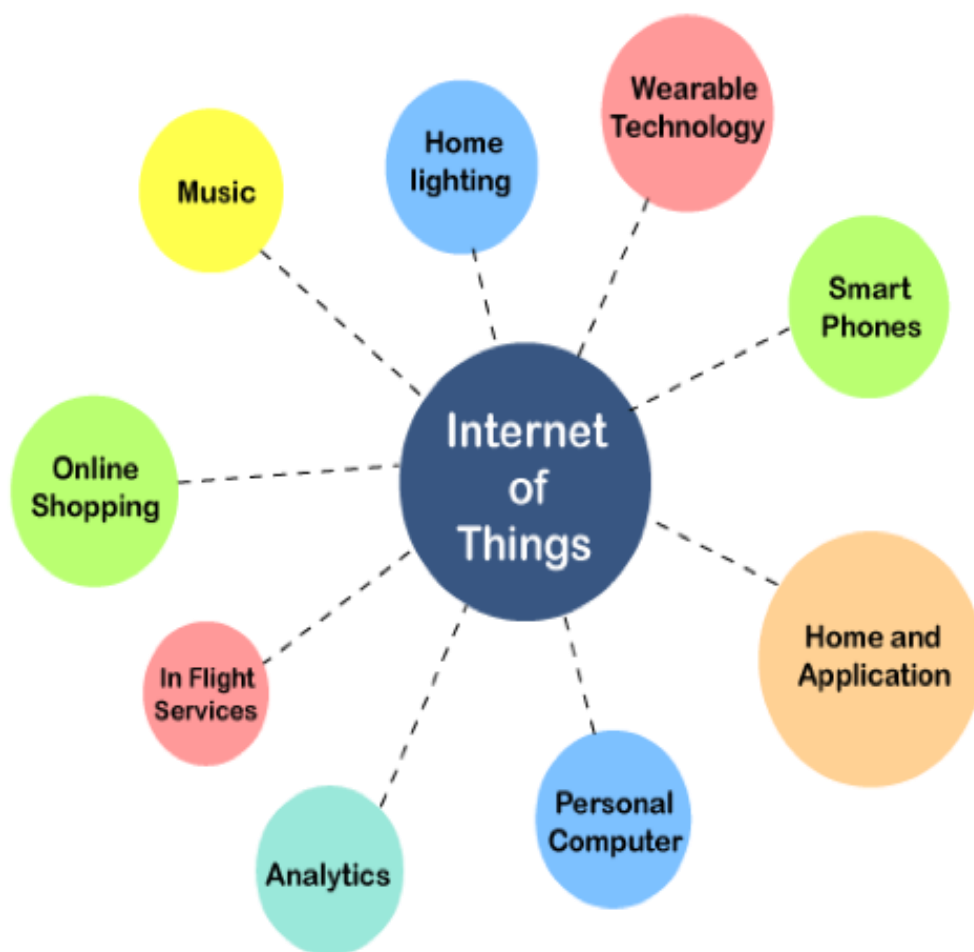
Алайда, оны арнайы электрондық құрылғылар арқылы анықтауға болады.

Бұл бөлімде Arduino тақшасы, қозғалыс сенсоры, дыбыстық зуммер, LCD дисплей және негізгі бағдарламалар қолданылған.

Сенсор өз аймағында қозғалысты анықтап, дабылды іске қосады [3].

Сонымен қатар, сенсор Arduino тақшасына сигнал жібереді, ал Arduino бұл сигналды өңдеп, дабыл қосады және экранға хабарлама шығарады.

Осы жүйенің көмегімен үйімізде бұзушылардың алдын алу үшін оңай қауіпсіздік дабылын орнатуға болады [4].



3.1-сурет – IoT қолданбалары

IoT пен үй қауіпсіздігі ұғымдарының үйлесімі үйіңізді әлемнің кез келген жерінен бақылап, қорғауға мүмкіндік береді.

Интернет заттар (IoT) - адамның араласуынсыз ақпарат алмасуға және байланысуға қабілетті өзара байланысқан физикалық құрылғылар желісін білдіреді [5].

Оны «ақпараттық қоғам жүйесі» деп атайды, өйткені Интернет заттар технологиясы адамдардан, жануарлардан, көліктерден, тұрмыстық техникалардан және жолдағы кез келген нәрседен ақпарат жинауға мүмкіндік береді.

Демек, физикалық әлемде бар барлық объектілерді әртүрлі электрондық құрылғылармен (мысалы, датчиктермен, бағдарламалық қамтамасыз етумен, желілік құрылғылармен) жабдықтауға немесе біріктіруге болады және оларды желі арқылы ақпарат беру үшін IP мекенжаймен қамтамасыз етуге болады [6].

Интернет заттар жай ғана интернетпен шектелмейді, ол тек интернет бұлтын құрылғыларды біріктіру және интерфейстеу үшін қолданады.

IoT қолданбалары мен жобаларының ауқымы 200 миллиард рупийден асып, бұл салада өзгеріс пен өсу жалғасуда [7].

IoT пен үй қауіпсіздігін біріктірудің кейбір мысалдары:

- газ немесе түтінді анықтайтын детекторлар орнату және адамдар үйде болмаған кезде ескерту жіберу;
- үй немесе көлік камераларын бақылау арқылы қашықтан үйді бақылау;
- орталықтандырылған құлыптау жүйесі және басқа да көптеген қосымшалар [8].

IoT технологиясының үнемі дамуы мен жаңашылдығының арқасында, IoT қолданбалары өміріміздің барлық салаларында пайда болуда. IoT арқасында компаниялар да, тұтынушылар да пайда көруде [9].

Өндірушілер мен тұтынушылардың пайдасы:

- Өндірушілер өз өнімдерінің нақты уақыттағы қолданылуын жақсы түсініп, қосымша қызметтерді ұсынып, табыстарын арттырады, сондай-ақ өнімдері мен қызметтерінің өмірлік циклін ұзартады [10].
- Ал тұтынушылар бірнеше құрылғыны бір құрылғы арқылы біріктіріп басқара алады, бұл олардың құрылғыларды тиімді пайдалануына және тұтынушы тәжірибесін жақсартуға мүмкіндік береді.

3.2 Arduino негізінде IoT арқылы жекеменшік мүлікті қорғау ағыны

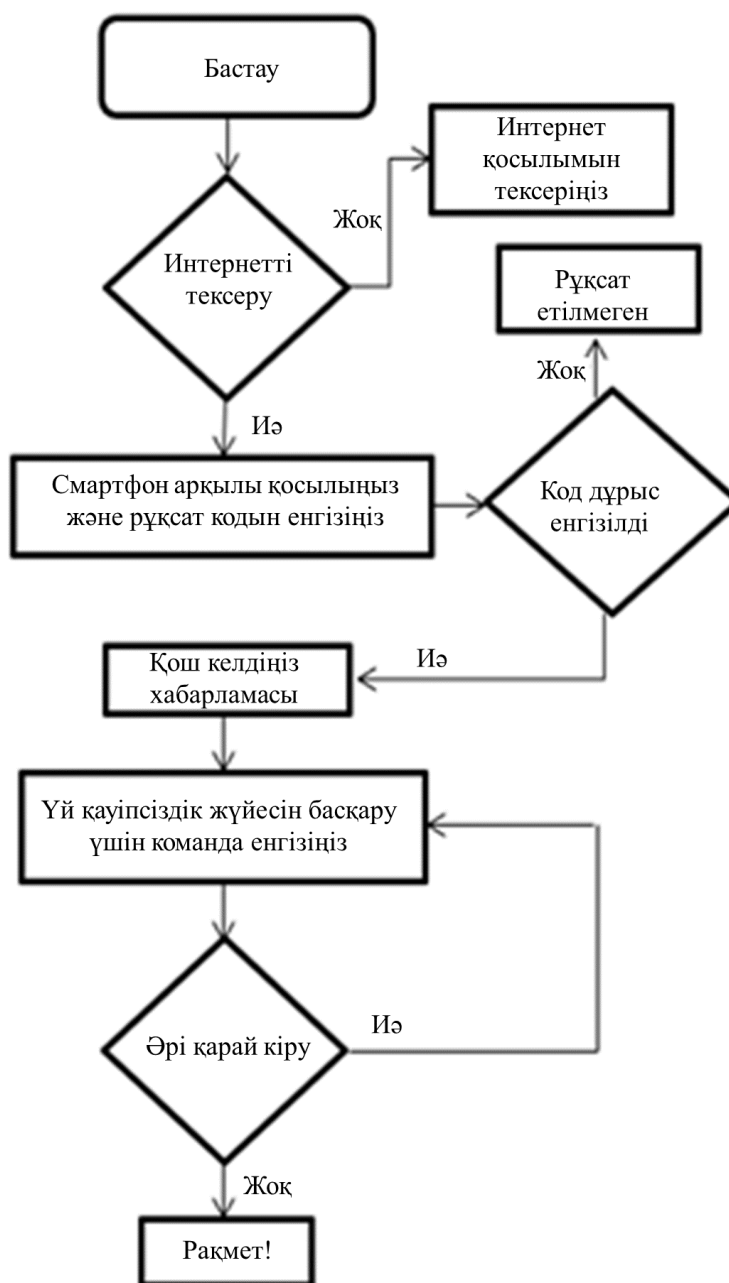
Бұл жобалау процесі бағдарламалық және аппараттық құралдардың үйлесімі арқылы жүзеге асырылды. Сондықтан ұсынылған әдістер аппараттық және бағдарламалық бөліктер үшін әртүрлі.

3.2-суретте көрсетілген жобалау ағыны үйге арналған қауіпсіздік дабыл жүйесін жобалау және әзірлеу барысында орындалатын негізгі қадамдарды көрсетеді.

Жобалау ағыны келесі элементтерді қамтиды:

- PIR (Пассив инфрақызыл) қозғалыс сенсорлары,
- газ/түтін детекторлары,
- және басқа қажетті сенсорлар.

Сондай-ақ, осы бөлімде Arduino микроконтроллерін бағдарламалау және жүйені басқару үшін жүзеге асырылған логика қарастырылады.



3.2-сурет – Үй қауіпсіздігіне арналған Смарт жүйенің блок-схемасы

Ең алдымен, пассив инфрақызыл сенсор (PIR сенсоры) қолданылады.

PIR сенсоры - бұл көрінетін диапазондағы объектілерден шығатын инфрақызыл (IR) сәулені өлшейтін электронды сенсор.

Олар көбінесе PIR негізіндегі қозғалысты анықтау үшін пайдаланылады.

PIR сенсорлары әдетте қауіпсіздік дабыл жүйелерінде және автоматты жарықтандыруда қолданылады.

PIR сенсорлары кеңістіктегі қозғалысты анықтайды, бірақ кімнің немесе ненің қозғалғаны туралы ақпарат бермейді [11].

Ол үшін инфрақызыл кескінді түсіретін сенсор қажет.

PIR сенсорларын кейде жай ғана PIR немесе PID (Passive Infrared Detector - пассив инфрақызыл детектор) деп те атайды.

Рассив сөзі PIR құрылғысының қозғалысты анықтау үшін энергия шығармайтынын білдіреді.

Олар тек объектілер шығаратын немесе шағылыстыратын инфрақызыл сәулеленуді (жылулық сәулені) анықтау арқылы жұмыс істейді.

Жалын сенсоры - өрт немесе жалын пайда болғанын анықтауға және оған жауап беруге арналған жабдық түрі.

Жалын детекторының реакциясы оның конфигурациясына байланысты өзгеруі мүмкін.

Дабыл жүйесіне табиғи газ құбырлары, пропан, өрт сөндіргіштер кіреді.

Бұл сенсор өнеркәсіптік салада қолданылады және негізгі міндеті - қазандықтың дұрыс жұмыс істеуін қамтамасыз ету.

Жалынды анықтау әдісі жылу/түтін детекторларымен салыстырғанда жылдамырақ әрі дәл жауап береді [12].

Жалын сенсорының пин сипаттамасы:

- Pin1 (VCC): Қоректену кернеуі 3,3 В–5,3 В аралығында.
- Pin2 (GND): Жерге қосу (нөлдік) пин.
- Pin3 (AOUT): Аналогтық шығыс пині (MCU.IO).
- Pin4 (DOUT): Сандық шығыс пині (MCU.IO).

MQ2 газ сенсоры - ауадан сұйытылған мұнай газы, пропан, метан, сутегі, алкоголь, түтін және көмірқышқыл газы сияқты газдардың концентрациясын анықтауға арналған электронды сенсор.

MQ2 газ сенсорлары химиялық резисторлар деп те аталады.

Олар маймен байланысқан кезде қарсыласу қасиетін өзгертпейді.

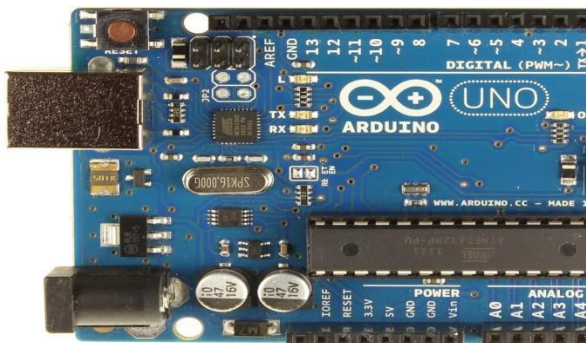
MQ2 - метал оксиді негізіндегі жартылай өткізгіш газ сенсоры, ол қарсыласу мәнінің өзгерісі арқылы газдың бар екенін анықтайды.

Майдағы концентрацияны сенсордағы электр тогының таралуы арқылы өлшейді.

Бұл сенсор 5V тұрақты токпен (DC) жұмыс істейді және газдарды 200–10000 ppm концентрация диапазонында анықтай алады [13].

Бұл сенсорлар ауадан метан, бутан, LPG және түтінді анықтай алады, бірақ газдардың нақты түрін ажырата алмайды.

Яғни, олар газ бар екенін анықтайды, бірақ оның қандай газ екенін айта алмайды [14].



3.2-сурет – Arduino тақшасы

Макет тақшалары (breadboard), дәнекерлеусіз макет тақшалары немесе прототиптеу тақшалары - электрондық схемалардың жартылай тұрақты прототиптерін жасауға арналған құрылғылар.

Perfboard-пен салыстырғанда, макет тақшаларын дәнекерлеудің немесе бөлшектеудің қажеті жоқ, сондықтан оларды қайта-қайта пайдалануға болады.

Осы себепті макет тақшалары студенттер мен білім беру саласында өте танымал.

Макет тақшалары:

- шағын электроникалық құрылғылардан бастап,
- толық орталық процессорларға (CPU) дейінгі әртүрлі электрондық жүйелерді модельдеу үшін қолданылады.

Бүгінгі замандағы дәнекерлеусіз макет тақшалары қалайы қапталған фосфорлы қола өткізгіштері бар перфорацияланған пластикалық қаптамамен жабдықталған.

Пьезоэлектрлік зуммер дыбысты пьезоэлектрлік эффектінің қайтарылуына негізделген түрде шығарады.

Бұл үшін пьезоэлектрлік материалдың потенциалын пайдаланып қысым немесе кернеу жасау қажет [15].

Пьезо-зуммер дыбыстық ескертулерге арналған, мысалы:

- іс-әрекеттің өзгеруіне,
- қарсы сигналдарға,
- сенсордан келетін кіріс мәліметтерге пайдаланылуы мүмкін.

Сондай-ақ, олар дабыл схемаларында да қолданылады. Кілт қалай ауысса да, зуммер бірдей дыбыс шығарады. Пьезоэлектрлік кристалл екі өткізгіштің арасында орналасқан. Кристаллға потенциал қолданылғанда бір өткізгішті итеріп, екіншісін тартады. Бұл итеру және тарту қозғалыстары дыбыс толқындарын тудырады. Көптеген зуммерлер 2-ден 4 кГц аралығында дыбыс шығарады. Қызыл сым кіріс сигналына, қара сым жерге қосылады.

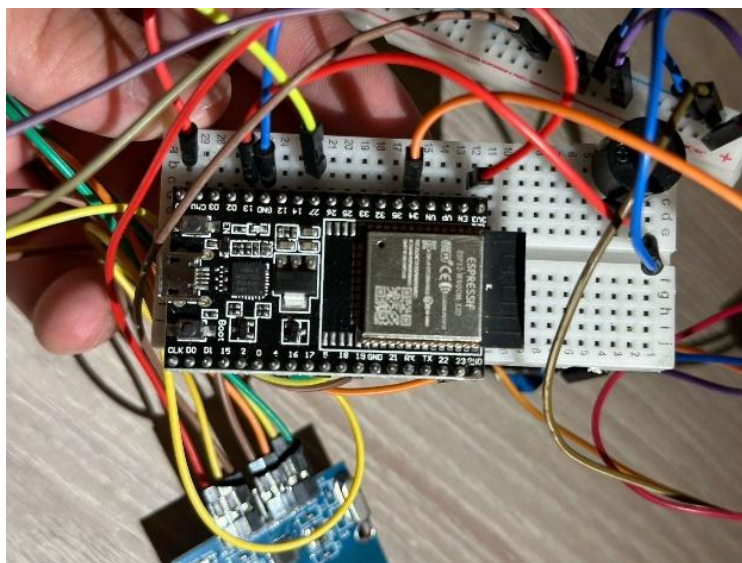
3.3 Arduino негізінде IoT арқылы жекеменшік мүлікті қорғау жүйесінің жалпы құрылымы

Ұсынылып отырған жоба - «Arduino негізінде IoT арқылы жекеменшік мүлікті қорғау жүйесін жасау» - жекеменшік ғимараттар мен мүліктердің қауіпсіздігін арттыру мақсатында әзірленген. Жүйенің негізі ретінде ESP32 микроконтроллері таңдалып, оған түрлі сенсорлар мен модульдер қосылған. Жүйе қорғалатын аумақта қозғалыс, газдың ағып шығуы немесе температураның қалыптан ауытқуы сияқты төтенше жағдайларды анықтап, иесіне хабарлама жіберуге мүмкіндік береді.

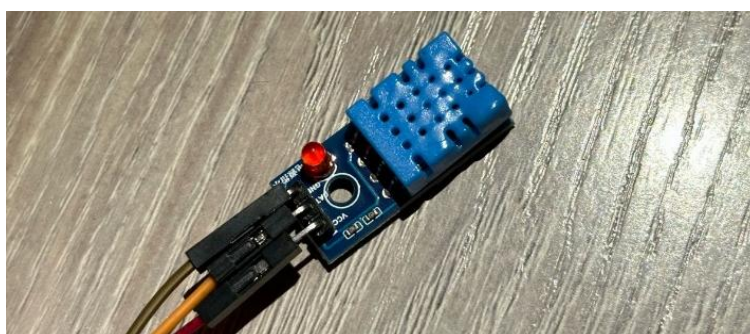
Жүйенің негізгі функциялары:

- Қозғалысты анықтау
- RFID арқылы рұқсатты тексеру
- Температура мен ылғалдылықты бақылау

- Газдың концентрациясын анықтау
 - Желі арқылы IoT серверіне немесе қолданбаға деректерді жіберу
- Проекте қолданылған компоненттер



3.3-сурет – ESP 32



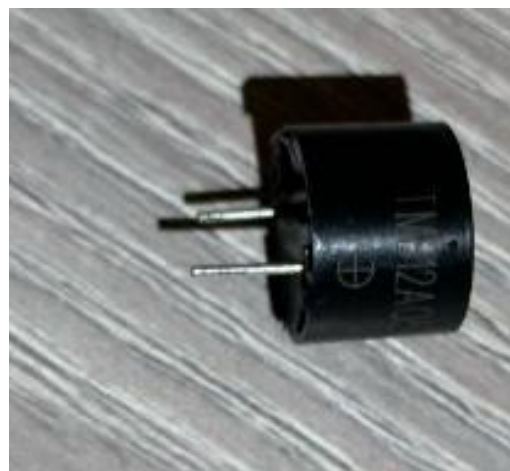
3.4-сурет – Dht11 sensor



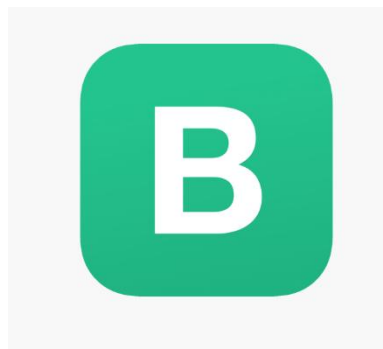
3.5-сурет – MQ-2 sensor



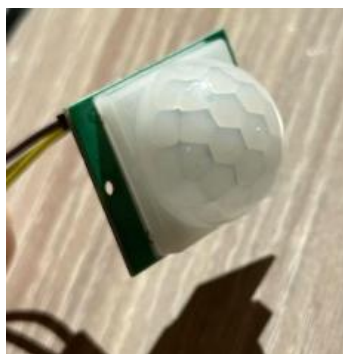
3.6-сypeт – RFID sensor



3.7-сypeт – Buzzer



3.8-сypeт – Notifications (blynk)



3.9-сурет – PIR sensor

3.4 Arduino негізінде IoT арқылы жекеменшік мүлікті қорғау жүйесінің аппараттық және бағдарламалық бөлігін жобалау

Аппараттық бөлік төмендегі негізгі компоненттерден тұрады:

Кесте 3.1 – Аппараттық бөліктің негізгі компоненті

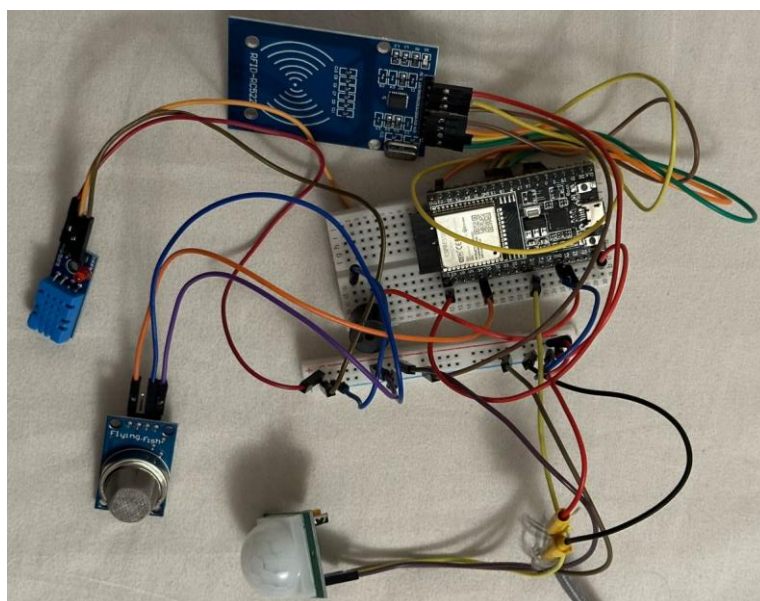
№	Компонент атауы	Мақсаты
1	ESP32 микроконтроллері	Барлық құрылғыларды басқару және желіге қосылу
2	RFID модулі (RC522)	Қол жеткізуді тексеру (карта немесе брелок арқылы)
3	RFID карта және кілт	Рұқсат етілген пайдаланушылар үшін
4	DHT11 сенсоры	Температура және ылғалдылықты өлшеу
5	PIR қозғалыс сенсоры	Қозғалысты анықтау
6	Газ сенсоры (MQ-2)	Газдың ағып шығуын анықтау
7	Breadboard және сымдар	Құрылғыларды қосу

Жүйе қосылған кезде, ESP32 барлық сенсорлардан деректер жинайды және оқиғалар орын алған жағдайда (мысалы, қозғалыс анықталса немесе газ концентрациясы асып кетсе) ескерту жібереді.

Барлық ақпарат Blynk қосымшасы арқылы көрсетіліп бақыланады.



3.10-сурет – Blynk қосымшасында деректердің көрсетілуі



3.11-сурет – Arduino негізінде IoT арқылы жекеменшік мүлікті қорғау жүйесі

Бағдарламалық қамтамасыз ету Arduino IDE ортасында әзірленді. ESP32 арқылы сенсорлардан деректер оқылады, талданады және қажет болған жағдайда хабарлама немесе дерек IoT серверіне жіберіледі. Кодтық тізбек А қосымшасында көрсетілген.

Бағдарлама логикасы келесідей:

1. Жүйе іске қосылғанда Wi-Fi желісіне қосылады.

2. RFID модулі арқылы рұқсат тексеріледі.
3. DHT11 сенсорынан температура мен ылғалдылық мәндері өлшенеді.
4. PIR сенсоры қозғалысты анықтайды.
5. MQ-2 сенсоры газ концентрациясын бақылайды.

Егер қозғалыс немесе газдың қауіпті деңгейі анықталса, иесіне Blynk қосымшасы арқылы хабарлама жіберіледі.

Жүйенің жұмыс алгоритмі төмендегідей:

1. Жүйе Wi-Fi желісіне қосылады.
2. RFID картасы сканерленеді. Егер карта рұқсат етілген болса, жүйе актив режимге өтеді.
3. Сенсорлар арқылы орта бақылауға алынады.
4. Егер қозғалыс анықталса → хабарлама жіберіледі.
5. Егер газдың концентрациясы қауіпті деңгейге жетсе → хабарлама жіберіледі.
6. Температура мен ылғалдылық туралы мәліметтер серверге жіберіледі.
7. Барлық мәліметтер IoT серверде тіркеледі немесе қолданбаға көрсетіледі.

Жүйенің қауіпсіздігін қамтамасыз ету үшін:

1. RFID арқылы тек тіркелген пайдаланушыларға қолжетімділік беріледі.
2. Желіге қосылу кезінде шифрланған байланыс пайдаланылады (WPA2).
3. IoT серверге деректерді жіберу кезінде қауіпсіз протоколдар (MQTT over TLS) қолданылады.

3.5 Негізгі компоненттердің таңдалу негіздемесі

ESP32 микроконтроллері: Wi-Fi және Bluetooth модульдері бар, жоғары өнімділікті 32-биттік микроконтроллер. Жад көлемі үлкен (520 KB SRAM), сондықтан бір уақытта бірнеше сенсорлармен жұмыс істей алады.

RFID RC522: 13.56 MHz жиілікте жұмыс істейтін стандартты RFID модулі. Энергияны аз тұтынады (13-26 mA).

DHT11 сенсоры: Қарапайым температура мен ылғалдылық сенсоры. Нақты жұмыс шегі:

- Температура диапазоны: 0°C–50°C
- Ылғалдылық диапазоны: 20%–90% RH

PIR сенсоры: Қозғалысты анықтайды, төмен ток тұтынуымен (50 μ A күту режимінде) жұмыс істейді.

MQ-2 газ сенсоры: Пропан, метан сияқты газдарды анықтайды. Газ концентрациясын аналогты түрде шығарады.

3.5.1 Ток тұтыну есебі

Кесте 3.2 Әр құрылғының ток тұтынуы

Құрылғы	Ток тұтынуы (мА)
ESP32	80–240
RFID модулі (RC522)	13–26
DHT11 сенсоры	0.5
PIR сенсоры	50
Газ сенсоры (MQ-2)	150

Максималды ток тұтынуды есептейміз:

$$I_{total} = I_{ESP32} + I_{RC522} + I_{DHT11} + I_{PIR} + I_{MQ-2}$$

Орташа мәндерді аламыз:

$$I_{total} = 150 + 20 + 0.5 + 50 + 150 = 370.5\text{мА}$$

Жүйенің максималды ток тұтынуы шамамен 370–400 мА.

Егер ESP32 USB арқылы қоректенсе (5V, 500 мА), онда бұл тұтынуды толық жаба алады. Бірақ сенсорлардың саны көбейсе немесе жүйе тәуелсіз аккумулятордан жұмыс істесе, қуатты аккумулятор керек.

3.5.2 Аккумулятор таңдау есебі (егер тәуелсіз қоректену керек болса)

Жүйе 8 сағат жұмыс істеуі керек. Керек сыйымдылық:

$$C = I_{total} \times t$$

Мұндағы:

$$I_{total} = 400\text{мА} = 0.4\text{А}$$

$$t = 8\text{сағат}$$

Есептейміз:

$$C = 0.4 \times 8 = 3.2\text{Асағ} = 3200\text{мАсағ}$$

Бір тәулік бойы жұмыс істеу үшін кем дегенде 3200 мАсағ сыйымдылығы бар аккумулятор қажет.

Қауіпсіздік коэффициентін (20%) ескеріп:

$$C_{final} = 3200 \times 1.2 = 3840 \text{ мАсағ}$$

Яғни, 4000 мАсағ литий-ионды аккумулятор қолдану ұсынылады.

3.6 Деректерді өңдеу және жіберу есебі

ESP32 Wi-Fi арқылы IoT серверіне мәліметтерді жіберген кезде қуат тұтыну артады.

Желіге қосылған кездегі ток тұтыну:

- Қалыпты күту режимі: 80 мА

- Берілген кезде: 240 мА

Әрбір деректі жіберу уақыты шамамен 1 секунд.

Егер әр 2 минут сайын бір пакет жіберілсе:

1 сағатта:

$$\frac{60}{2} = 30 \text{ пакет}$$

1 күнде:

$$30 \times 24 = 720 \text{ пакет}$$

Желіге қосылу кезінде аккумулятор тезірек отырады, сондықтан Wi-Fi уақытша қосылып, деректер жіберілгеннен кейін қайта өшірілуі керек (deep sleep режимі ұсынылады).

Газ сенсорының калибровкасы

MQ-2 сенсорының аналогты мәні 0–1023 аралығында болады (ESP32-де 12-бит ADC бар).

Газ концентрациясы:

$$PPM = \frac{A_{analog}}{1023} \times 1000$$

Мысалы, егер аналогты мән 500 болса:

$$PPM = \frac{500}{1023} \times 1000 \approx 488 PPM$$

Бұл мән қауіпті шекке жеткенін көрсетсе (мысалы, > 300 PPM болса), дереу ескерту беріледі.

ҚОРЫТЫНДЫ

Бұл дипломдық жұмыста Arduino платформасы мен IoT технологияларын пайдалану арқылы жекеменшік мүлікті қорғауға арналған тиімді қауіпсіздік жүйесі жасалды. Жүйе түрлі сенсорлардан деректер жинап, деректерді өңдеп, қауіпті жағдайлар туындаған кезде дабыл жүйесін іске қосады және пайдаланушыға қашықтықтан хабар береді.

Жоба барысында қозғалыс сенсоры, газ сенсоры, температура мен ылғалдылық сенсоры және RFID модулі сәтті интеграцияланды. Жүйенің интернет арқылы қолжетімділігі қамтамасыз етіліп, пайдаланушы кез келген жерден өзінің мүлкін бақылауға мүмкіндік алды.

Эксперименттік тестілеу нәтижелері жүйенің жоғары сенімділігі мен тұрақты жұмысын көрсетті. Бұл шешім арзан бағасы, жеңіл жобалануы және икемділігі арқасында тұрғын үйлердің қауіпсіздігін қамтамасыз етудің тиімді жолдарының бірі бола алатынын дәлелдеді.

Болашақта жүйені әрі қарай жетілдіру үшін:

- Қосымша сенсорлар мен қауіпсіздік деңгейлерін енгізу;
- Бейнебақылау мүмкіндіктерін қосу;
- Көпқабатты хабарлау жүйелерін әзірлеу ұсынылады.

Осылайша, жасалған жүйе үй қауіпсіздігін қамтамасыз етуде IoT технологияларының қолданылу тиімділігін толық көрсетті.

ПАЙДАЛАНЫЛҒАН ӘДЕБИЕТТЕР ТІЗІМІ

- 1 Chikara, S. Jain, M. Fatima, and M. Luthra, "Review on Implementing Smart Water Grid for Smart Cities in India: Challenges and Solutions," 2019 5th International Conference on Advanced Computing & Communication Systems (ICACCS), Coimbatore, India, pp. 216-219, 2019.
- 2 Anand R. Padwalkar, Prajakta Pande, "Internet of Things -A Future of Internet: A Survey," International Journal of Advance Research in Computer Science and Management Studies, Volume 2, Issue 2, February 2014.
- 3 Pharmasetiawan and R. Rediana, "Designing a business model for smart water management system with the smart metering system as a core technology: Case study: Indonesian drinking water utilities," 2017 International Conference on ICT For Smart Society (ICISS), Tangerang, pp. 1-6, 2017 doi: 10.1109/ICTSS.2017.8288862.
- 4 Global Sustainable Development Report: "Building the Common Future We Want". United Nations Department of Economic and Social Affairs. September 2013.
- 5 Khalifa, T.; Naik, K.; Nayak, A. A survey of communication protocols for automatic meter reading applications. IEEE Commun. Surv. Tutorials 2011, 13, 168–182.
- 6 M. Elkahout, M. M. Abu-Saqr, A. F. Aldaour, A. Issa and M. Debeljak, "IoT-Based Healthcare and Monitoring Systems for the Elderly: A Literature Survey Study," 2020 International Conference on Assistive and Rehabilitation Technologies (iCareTech), Gaza, Palestine, 2020, pp. 92-96, doi: 10.1109/iCareTech49914.2020.00025.
- 7 M. M. Bautista-Villalon, J. M. Gutierrez-Villalobos and E. A. Rivas-Araiza, "IoT-Based System to Monitor and Control Household Lighting and Appliance Power Consumption and Water Demand," 2018 7th International Conference on Renewable Energy Research and Applications (ICRERA), Paris, France, 2018, pp. 785-790, doi: 10.1109/ICRERA.2018.8566816.
- 8 Michele Mutchek, Eric Williams, "Moving Towards Sustainable and Resilient Smart Water Grids," in Challenges 2014, March 2014.
- 9 Perera, A. Zaslavsky, P. Christen, and D. Georgakopoulos, "Sensing as a service model for smart cities supported by internet of things," Transactions on Emerging Telecommunications Technologies (ETT), vol. 25, no. 1, pp. 81–93, 2014.
- 10 S. K. Vishwakarma, P. Upadhyaya, B. Kumari and A. K. Mishra, "Smart Energy Efficient Home Automation System Using IoT," 2019 4th International Conference on Internet of Things: Smart Innovation and Usages (IoT-SIU), Ghaziabad, India, 2019.
- 11 S. Mathavan, A. Kumar, K. Kamal, M. O. Arshad, T. Vadamala, "Smart Irrigation Using Low-Cost Moisture Sensors and XBee-based Communication," in IEEE 2014 Global Humanitarian Technology Conference, 2014.
- 12 Sharma, Vatsala, and Kamal Nayanam, "A survey on Smart Railway Track Fault Detection Using IOT", IOSR Journal of Engineering 11 (08), pp. 38-42, 2021.

- 13 Sharma, Vatsala, and Kamal Nayanam. "Arduino based Smart Water Management." *International Journal of Engineering Research & Technology (IJERT)* 9 (2020): 652-656.
- 14 U. Muthukumar, M. Suresh, and J. Chandapillai, "A novel smart water-meter based on IoT and smartphone app for city distribution management," 2017 IEEE Region 10 Symposium (TENSYP), Cochin, pp. 1-5, 2017. doi:10.1109/TENCONSpring.2017.8070088.
- 15 Vatsala Sharma, Mansi Agarwal, Sukreeti and Kamal Nayanam, "IOT based Smart Robot using Arduino" *Gujarat Agricultural University Research Journal*, Vol. 46 (1), ISSN 0250-5193, NAAS rating 2.72, January 2021.

ҚОСЫМША А

```
#define BLYNK_PRINT Serial
#define BLYNK_TEMPLATE_ID "TMPL4gJYqI3og"
#define BLYNK_TEMPLATE_NAME "Esp32 home"
#define BLYNK_AUTH_TOKEN "trZb4m7W04Gdo6Ws4znEvPBWJerfJkL9"

#include <WiFi.h>
#include <BlynkSimpleEsp32.h>
#include <MFRC522.h>
#include <SPI.h>
#include <DHT.h>

#define WIFI_SSID "Sak"
#define WIFI_PASS "Alem2023"

#define SS_PIN 5 // RC522 SS (SDA)
#define RST_PIN 0 // RC522 RST
#define BUZZER 13 // Пин зуммера
#define PIR_PIN 27 // PIR сенсор
#define MQ2_PIN 34 // MQ-2 датчик
#define DHT_PIN 4 // DHT11 датчик
#define DHT_TYPE DHT11

DHT dht(DHT_PIN, DHT_TYPE);
MFRC522 mfrc522(SS_PIN, RST_PIN);
BlynkTimer timer;

const String validCardUID = "9FE04F1C"; // UID разрешённой карты
bool accessGranted = false; // Флаг доступа
bool motionSensorEnabled = true; // Включён ли PIR-сенсор

void setup() {
  Serial.begin(115200);
  WiFi.begin(WIFI_SSID, WIFI_PASS);
  Blynk.begin(BLYNK_AUTH_TOKEN, WIFI_SSID, WIFI_PASS);

  SPI.begin();
  mfrc522.PCD_Init();
  dht.begin();

  pinMode(BUZZER, OUTPUT);
```

```

    pinMode(PIR_PIN, INPUT);
    pinMode(MQ2_PIN, INPUT);

    timer.setInterval(2000L, sendSensorData);
}

void loop() {
    Blynk.run();
    timer.run();

    checkRFID();
    if (motionSensorEnabled) {
        checkPIR();
    }
    checkMQ2();
}

void checkRFID() {
    if (!mfrc522.PICC_IsNewCardPresent() || !mfrc522.PICC_ReadCardSerial())
    {
        return;
    }

    String cardID = "";
    for (byte i = 0; i < mfrc522.uid.size; i++) {
        cardID += String(mfrc522.uid.uidByte[i], HEX);
    }
    cardID.toUpperCase();

    Serial.println("RFID Card: " + cardID);
    mfrc522.PICC_HaltA();

    if (cardID == validCardUID) {
        if (!accessGranted) {
            Serial.println("□ Доступ разрешен! PIR выключен.");
            Blynk.logEvent("access_granted", "Добро пожаловать!");
            Blynk.virtualWrite(V3, "Добро пожаловать!");
            accessGranted = true;
            motionSensorEnabled = false; // Отключаем PIR-сенсор
            digitalWrite(BUZZER, LOW);
        } else {
            Serial.println("□ Выход. PIR снова включен.");
            Blynk.logEvent("access_revoked", "До свидания!");
            Blynk.virtualWrite(V3, "До свидания!");
        }
    }
}

```

```

        accessGranted = false;
        motionSensorEnabled = true; // Включаем PIR-сенсор
    }
} else {
    Serial.println("□ Доступ запрещен!");
    Blynk.logEvent("access_denied", "Попытка входа: " + cardID);
    digitalWrite(BUZZER, HIGH);
    delay(2000);
    digitalWrite(BUZZER, LOW);
}
}

void checkPIR() {
    if (digitalRead(PIR_PIN) == HIGH && !accessGranted) {
        Serial.println("Движение обнаружено!");
        Blynk.logEvent("motion_detected", "Движение зафиксировано!");
        Blynk.virtualWrite(V4, "Движение обнаружено!");
        digitalWrite(BUZZER, HIGH);
        delay(1000);
        digitalWrite(BUZZER, LOW);
    }
}

void checkMQ2() {
    int gasLevel = analogRead(MQ2_PIN);
    Serial.println("Газовый уровень: " + String(gasLevel));
    Blynk.virtualWrite(V5, gasLevel); // Отображение данных датчика газа в
Blynk

    if (gasLevel > 2000) {
        Serial.println("△□ Обнаружен дым!");
        Blynk.logEvent("smoke_detected", "Внимание! Обнаружен дым!");
        Blynk.virtualWrite(V6, "Обнаружен дым!");
        digitalWrite(BUZZER, HIGH);
        delay(3000);
        digitalWrite(BUZZER, LOW);
    }
}

void sendSensorData() {
    float temperature = dht.readTemperature();
    float humidity = dht.readHumidity();

    if (!isnan(temperature) && !isnan(humidity)) {

```

```

Blynk.virtualWrite(V1, temperature);
Blynk.virtualWrite(V2, humidity);
Serial.println("Температура: " + String(temperature) + "C");
Serial.println("Влажность: " + String(humidity) + "%");

if (temperature > 40) {
  Serial.println("⚠ Внимание! Высокая температура! ⚠");
  Blynk.logEvent("high_temperature", "Температура выше 40°C!");
  Blynk.virtualWrite(V7, "Высокая температура!");
  digitalWrite(BUZZER, HIGH);
  delay(3000);
  digitalWrite(BUZZER, LOW);
}
} else {
  Serial.println("Ошибка чтения DHT11");
}
}

```

Дипломдық жоба (жұмыс) бойынша

РЕЦЕНЗИЯ

Тұрланұлы Мейрамбек

6B06201 «Телекоммуникация» білім беру бағдарламасы

Тақырыбы: Arduino негізінде IoT арқылы жекеменшік мүлікті қорғау жүйесін жасау

Орындалды:

- а) Графикалық бөлім 3 парақтарда
б) түсіндірме жазба 74 беттерінде

ЖҰМЫСҚА ЕСКЕРТУЛЕР

Жұмыстың өзектілігі.

Қазіргі кезде тұрғын үйлер мен жеке нысандардың қауіпсіздігін арттыру өзекті мәселе болып отыр. Осы тұрғыда Arduino және IoT технологияларын біріктіріп тиімді шешім ұсыну — ғылыми және тәжірибелік тұрғыда жоғары сұранысқа ие тақырып.

Құрылымы мен мазмұны.

Дипломдық жұмыс кіріспеден, үш мазмұнды тараудан, қорытынды мен қосымшалардан тұрады. Жұмыста теориялық талдау, жүйенің жобалануы, бағдарламалық және аппараттық қамтамасыз ету егжей-тегжейлі қарастырылған. ESP32, RFID, PIR, DHT11 және газ сенсорларын біріктіре отырып, нақты жұмыс істейтін жүйе жасалған.

Практикалық маңыздылығы.

Ұсынылған жүйе нақты құрылғылар негізінде жасалып, IoT арқылы қауіпсіздік мәселесін қашықтан басқаруға мүмкіндік береді. GSM және Wi-Fi арқылы деректерді жіберу, Blynk платформасы арқылы пайдаланушымен өзара әрекет жасау – практикалық тұрғыдан өте құнды шешім.

Орфографиялық және стилистикалық сәйкестік.

Жұмыста академиялық тіл нормалары мен техникалық терминдер дұрыс қолданылған. Грамматикалық және стилистикалық қателер аз, мәтін түсінікті жазылған.

Жұмысты бағалау

Жалпы, дипломдық жұмысқа «өте жақсы» (95%) деген баға, ал студент Тұрланұлы Мейрамбекті 6B06201 – Телекоммуникация білім беру бағдарламасы бойынша «Ақпараттық коммуникациялық технологиялар бакалавры» дәрежесіне ұсынамын.

Рецензент

М.Тынышбаев атындағы
АЛТ университеті, PhD,
«АКТ» кафедрасының
ассистент профессоры

Мәдібайұлы Ж.
«20» 05 2025 ж.



Дипломдық жобаға (жұмысқа)

ҒЫЛЫМИ ЖЕТЕКШІНІҢ ПІКІРІ

Тұрланұлы Мейрамбек

6B06201 «Телекоммуникация» білім беру бағдарламасы

Тақырыбы: Arduino негізінде IoT арқылы жекеменшік мүлікті қорғау жүйесін жасау

Диплом жұмысының негізгі мақсаты – Arduino микроконтроллері мен ESP32 платформасы негізінде түрлі сенсорлар (қозғалыс, газ, температура мен ылғалдылық, RFID модульдері) арқылы жекеменшік мүлікті қорғаудың интеллектуалды жүйесін жобалау және жүзеге асыру болып табылады.

Мейрамбек жұмыстың барлық кезеңдерінде белсенділік танытып, қойылған міндеттерді өз бетінше орындап шықты. Ол қажетті теориялық негізді терең меңгеріп, қолданылатын компоненттердің сипаттамалары мен өзара байланысын дұрыс анықтай алды. Жүйенің практикалық іске асырылуы, оның ішінде аппараттық бөліктерді қосу, бағдарламалау, мәліметтерді өңдеу және бұлтқа жіберу сияқты бөлімдер тиянақты орындалған.

Студент IoT-тың ThingSpeak және Blynk сияқты платформаларын пайдалану арқылы деректерді визуализациялау мен нақты уақыттағы мониторинг жүргізуді жүзеге асырды. Бұл жұмыс тек теориямен шектеліп қалмай, нақты жұмыс істейтін жүйе ретінде сәтті модельденіп, бірнеше тестілеуден өтті.

Жұмыстың мазмұны толық, құрылымы жүйелі. Тілдік және стильдік жағынан жұмыс академиялық талаптарға сай орындалған. Қолданылған әдебиеттер мен дереккөздер де заманауи талаптарға сай, халықаралық және отандық еңбектерге негізделген.

Студент, Тұрланұлы Мейрамбек дипломдық жұмысты жазу барысында жетекші нұсқаулығымен өз бетінше жұмыс істеу қабілетін көрсетті. Дипломдық жұмыс «95/А/ өте жақсы» деп бағаланды, ал Тұрланұлы Мейрамбекті 6B06201 «Телекоммуникация» білім беру бағдарламасы бойынша «Ақпараттық коммуникациялық технологиялар» бакалавры академиялық дәрежесіне ұсынамын.

Ғылыми жетекші
ЭТЖҒТ каф. қауымдастырылған
профессор, PhD

Хабай А.

«20» 05 2025 ж.

Протокол

о проверке на наличие неавторизованных заимствований (плагиата)

Автор: Тұрланұлы Мейрамбек

Соавтор (если имеется):

Тип работы: Дипломная работа

Название работы: Arduino негізінде IoT арқылы жекеменшік мүлікті қорғау жүйесін жасау

Научный руководитель: Сұңғат Марксұлы

Коэффициент Подобия 1: 4.2

Коэффициент Подобия 2: 2.3

Микропробелы: 0

Знаки из других алфавитов: 2

Интервалы: 0

Белые Знаки: 0

После проверки Отчета Подобия было сделано следующее заключение:

☒ Заимствования, выявленные в работе, является законным и не является плагиатом. Уровень подобия не превышает допустимого предела. Таким образом работа независима и принимается.

☐ Заимствование не является плагиатом, но превышено пороговое значение уровня подобия. Таким образом работа возвращается на доработку.

☐ Выявлены заимствования и плагиат или преднамеренные текстовые искажения (манипуляции), как предполагаемые попытки укрытия плагиата, которые делают работу противоречащей требованиям приложения 5 приказа 595 МОН РК, закону об авторских и смежных правах РК, а также кодексу этики и процедурам. Таким образом работа не принимается.

☐ Обоснование:

2025-04-29

Дата



Заведующий кафедрой



**Университеттің жүйе администраторы мен Академиялық мәселелер департаменті
директорының ұқсастық есебіне талдау хаттамасы**

Жүйе администраторы мен Академиялық мәселелер департаментінің директоры көрсетілген еңбекке қатысты дайындалған Плагиаттың алдын алу және анықтау жүйесінің толық ұқсастық есебімен танысқанын мәлімдейді:

Автор: Тұрланұлы Мейрамбек

Тақырыбы: Arduino негізінде IoT арқылы жекеменшік мүлікті қорғау жүйесін жасау

Жетекшісі: Сұңғат Марксұлы

1-ұқсастық коэффициенті (30): 4.2

2-ұқсастық коэффициенті (5): 2.3

Дәйексөз (35): 2.4

Әріптерді ауыстыру: 2

Аралықтар: 0

Шағын кеңістіктер: 0

Ақ белгілер: 0

Ұқсастық есебін талдай отырып, Жүйе администраторы мен Академиялық мәселелер департаментінің директоры келесі шешімдерді мәлімдейді :

☒ Ғылыми еңбекте табылған ұқсастықтар плагиат болып есептелмейді. Осыған байланысты жұмыс өз бетінше жазылған болып санала отырып, қорғауға жіберіледі.

☐ Осы жұмыстағы ұқсастықтар плагиат болып есептелмейді, бірақ олардың шамадан тыс көптігі еңбектің құндылығына және автордың ғылыми жұмысты өзі жазғанына қатысты күмән тудырады. Осыған байланысты ұқсастықтарды шектеу мақсатында жұмыс қайта өңдеуге жіберілсін.

☐ Еңбекте анықталған ұқсастықтар жосықсыз және плагиаттың белгілері болып саналады немесе мәтіндері қасақана бұрмаланып плагиат белгілері жасырылған. Осыған байланысты жұмыс қорғауға жіберілмейді.

Негіздеме:

2025-04-29

Күні



Кафедра меңгерушісі



Протокол

о проверке на наличие неавторизованных заимствований (плагиата)

Автор: Тұрланұлы Мейрамбек

Соавтор (если имеется):

Тип работы: Дипломная работа

Название работы: Arduino негізінде IoT арқылы жекеменшік мүлікті қорғау жүйесін жасау

Научный руководитель: Сұңғат Марқсұлы

Коэффициент Подобия 1: 4.2

Коэффициент Подобия 2: 2.3

Микропробелы: 0

Знаки из других алфавитов: 2

Интервалы: 0

Белые Знаки: 0

После проверки Отчета Подобия было сделано следующее заключение:

☒ Заимствования, выявленные в работе, является законным и не является плагиатом. Уровень подобия не превышает допустимого предела. Таким образом работа независима и принимается.

☐ Заимствование не является плагиатом, но превышено пороговое значение уровня подобия. Таким образом работа возвращается на доработку.

☐ Выявлены заимствования и плагиат или преднамеренные текстовые искажения (манипуляции), как предполагаемые попытки укрытия плагиата, которые делают работу противоречащей требованиям приложения 5 приказа 595 МОН РК, закону об авторских и смежных правах РК, а также кодексу этики и процедурам. Таким образом работа не принимается.

☐ Обоснование:

2025-04-29

Дата



Сұңғат Марқсұлы

проверяющий эксперт