ҚАЗАҚСТАН РЕСПУБЛИКАСЫ БІЛІМ ЖӘНЕ ҒЫЛЫМ МИНИСТРЛІГІ

Қ.И. Сәтбаев атындағы Қазақ ұлттық техникалық зерттеу университеті

Бүркітбаев ат.өндірістік автоматтандыру және цифрландыру институты

Электроника, телекоммуникация және ғарыштық технологиялар кафедрасы

Нүкетаев Жандос

«"Smart home" жүйесінің қауіпсіздік қатерлерін талдау»

ДИПЛОМДЫҚ ЖҰМЫС

5В071900 – Радиотехника, электроника және телекоммуникация мамандығы

Алматы 2020

ҚАЗАҚСТАН РЕСПУБЛИКАСЫ БІЛІМ ЖӘНЕ ҒЫЛЫМ МИНИСТРЛІГІ

Қ.И. Сәтбаев атындағы Қазақ ұлттық техникалық зерттеу университеті

Бүркітбаев ат.өндірістік автоматтандыру және цифрландыру институты

Электроника, телекоммуникация және ғарыштық технологиялар кафедрасы

ҚОРҒАУҒА ЖІБЕРІЛДІ
Кафедра меңгерушісі
_____И.Сыргабаев
«____» _____2020 ж.

ДИПЛОМДЫҚ ЖҰМЫС

Тақырыбы «"Smart home" жүйесінің қауіпсіздік қатерлерін талдау»

5В071900 – Радиотехника, электроника және телекоммуникация мамандығы

Орындаған: Ж.Нукетаев

Пікір беруші
техн.ғыл.канд.,
АУЭС доценті
_____ А.О.Касимов
«_02_» ___06_____ 2020 ж.

Ғылыми жетекші
ассистент-профессор
_____ А.А.Абдыкадыров
«_02_» __06___2020 ж.

Алматы 2020

ҚАЗАҚСТАН РЕСПУБЛИКАСЫ БІЛІМ ЖӘНЕ ҒЫЛЫМ МИНИСТРЛІГІ

Қ.И. Сәтбаев атындағы Қазақ ұлттық техникалық зерттеу университеті

Бүркітбаев ат.өндірістік автоматтандыру және цифрландыру институты

Электроника, телекоммуникация және ғарыштық технологиялар кафедрасы

5В071900 – Радиотехника, электроника және телекоммуникация

БЕКІТЕМІН
Кафедра меңгерушісі
_____И.Сыргабаев
«____» _____2020 ж.

Дипломдық жұмыс орындауға
ТАПСЫРМА

Білім алушы *Нүкетаев Жандос*

Тақырыбы *«*"Smart home" жүйесінің қауіпсіздік қатерлерін талдау*»*

Университет ректорының «27*» қаңтар 2020 ж. №762-б бұйрығымен бекітілген.*

Аяқталған жұмысты тапсыру мерзімі *«21» сәуір 2020 ж.*

Дипломдық жұмыстың бастапқы берілістері:

1) "Smart home" жүйелеріндегі желілік өзара іс-қимыл кезінде қолжетімділікті басқарудың контекстік моделін қолдана отырып, компрометирленген құрылғылардан қорғауды қамтамасыз ету. 2) Қадағалаушы жүйені құруға қажетті микроконтроллер және датчиктер т.б құралдардың техникалық сипаттамасы мен бағдарламалық мәліметтер.

Кадрлері мен пакеттерінің құрылымдары.

Дипломдық жұмыста қарастырылатын мәселелер тізімі:

а) Архитектураны, қауіпсіздік тетіктерін, "Smart home" жүйелеріндегі желілік хаттамаларды талдау, қауіп моделін жасау.

ә) "Smart home" жүйелеріне қолжетімділікті басқару үшін контексттік модельдердің қолданылуын талдау.

б) Контексттік қолжетімділікті басқарудың моделіне негізделген "Smart home" қауіпсіздік жүйесін жобалау.

в) Әзірленген қолжетімділікті басқару моделін тәжірибелік тексеру үшін "Smart home" жүйесінің бағдарламалық моделін құру.

Сызбалық материалдар тізімі (міндетті сызбалар дәл көрсетілуі тиіс):

1. Ұсынылатын негізгі әдебиет: Снегуров А. В., Ткаченко Е. А., Кравченко А. Д. Риски информационной безопасности систем, построенных по технологии” Умный дом” //Восточно-Европейский журнал передовых

технологий. – 2011. – Т. 4. –№. 3 (52)
2. Smirnov A. et al. Context-based access control model for smart space //Cyber Conflict (CyCon), 2013 5th International Conference on. – IEEE, 2013. – С. 1-15.
3. RTLS | Технологии | Сетевая инфраструктура системы РТЛС // RTSL URL: http.

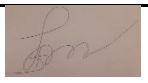
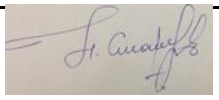
дипломдық жұмысты (жобаны) дайындау

КЕСТЕСІ

Бөлімдер атауы, қарастырылатын мәселелер тізімі	Ғылыми жетекшіге және кеңесшілерге көрсету мерзімі	Ескерту
Диплом жұмысының тақырыбын талдау	04.01.2020 -25.01.2020	орындалды
Теориялық ақпарат	20.01.2020 -25.02.2020	орындалды
Жабдықтар жұмысының есебі	25.02.2020 – 01.04.2020	орындалды

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	А.А.Абдыкадыров, ЭТжҒТ каф. ассистент-профессоры	02.06.2020	
Теориялық ақпарат	А.А.Абдыкадыров, ЭТжҒТ каф. ассистент-профессоры	02.06.2020	
Норма бақылау	PhD докторы, ЭТжҒТ каф. сениор-лекторы Смайлов Н.К.	02.06.2020	

Ғылыми жетекшісі  А.А.Абдыкадыров
(қолы)

Тапсырманы орындауға алған білім алушы  Ж.Нүкетаев

Күні “02_” _____06_____ 2020 ж.

РЕФЕРАТ

Дипломдық жұмыс 41 бет мәтіннен, 13 суреттен, 1 кестеден, 1 қосымшадан, 14 пайдаланған әдебиеттен тұрады.

Дипломдық жұмыс "Smart home" жүйелерінің қауіпсіздігін талдауға арналған. Бұл жұмыста зиянды бағдарламаларға, бағдарламалық немесе апараттық жаңылыстарға, қателіктерге ұшыраған сенімді жүйелік құрылғыдан туындайтын қауіп-қатерлерден қорғану қарастырылған.

Қорғаныстықүшейту мақсатында жүйенің жағдайы жайлы ақпаратты жинастыратын және өзіне тәуелді қолжетімділік ережелерін модификациялайтын контексті қолжетімділікті басқаратын модель қолдану ұсынылады. Мұндай модель жүйенің жұмыс істеу уақытында оптималды қорғаныс деңгейін қамтамасыз ету үшін қолжетімділік ережелерін бейімдеуге мүмкіндік береді.

Жүргізілген тәжірибелер нәтижесі мұндай қолжетімділікті басқару әдісі бар жүйені құруға болатының дәлелдейді. Әр түрлі жоспарда жасалған мысалдар белгілі бір жағдайларда қолжетімділік ережелерінің сол уақыттағы өзгеше опрецияларға тыйым салуға байланысты өзгеру бағыттары мен мүмкіндітері көрсетілген.

МАЗМҰНЫ

АНЫҚТАМАЛАР, БЕЛГІЛЕУЛЕР ЖӘНЕ ҚЫСҚАРТУЛАР

АБЖ Автоматтандырылған басқару жүйесі

ҒБАЖ Ғимаратты басқарудың автоматтандырылған жүйесі

OSI Open Systems Interconnection (Ашық жүйелердің өзара әрекеттесуі)

PLC Power line communication (Электр желілері арқылы байланыс)

IEEE Institute of Electrical and Electronics Engineers (Электр және электроника инженерлері институты)

КІРІСПЕ

Қазіргі уақытта «ақылды орта» технологиясы қарқынды дамуда. Осы технологияның әлі күнге дейін жалпыға бірдей қабылданған анықтама жоқ, дегенмен, осындай ортаны сипаттайтын бірқатар ережелерді бөліп көрсетуге болады - бұл қауіпсіздікті немесе тиімді басқаруды қамтамасыз ету сияқты бірыңғай мақсатқа жету үшін динамикалық орталықтандырылмаған ортада әрекет ететін сенсорлар мен есептеу құрылғыларының пайдаланылуы. Мұндай орталардың келесі сипатты белгілері бар [1]:

– құрылғылар арасындағы тікелей өзара әрекеттесуі;
– құрылғыны қашықтан басқару;
– құрылғының күрделі функционалдығы;
– «интеллектуалды» құрылғылар;
– желілік өзара іс-қимыл стандарттарының көптүрлілігі.

Мұндай орталар бірінші кезекте әр түрлі автоматтандыру жүйелерінде қолданылады, бұл инфрақұрылымды құру үшін жақсы негіз береді. «Ақылды орталарды» пайдаланудың кең таралған мысалдарының бірі «Smart home» жүйесі болып табылады

«Smart home» жүйелері өмірдің ыңғайлылығы мен қауіпсіздігін қамтамасыз етуге, сонымен қатар ғимараттың энергия тиімділігін арттыруға арналған. Сонымен қатар, жүйенің өзі ақпараттық қауіпсіздікке аз көңіл бөледі. Ақауларды неғұрлым толық түсіну үшін жүйенің негізгі белгілерін және олармен байланысты қауіпсіздік ақауларын анықтау қажет.

«Smart home» жүйесі үшін негіз болып табылатын ғимаратты басқарудың классикалық автоматтандырылған жүйелерінде автоматтандырудың үш деңгейі бөлінеді.

– Персоналдың жүйемен өзара іс - қимылы жүзеге асырылатын диспетчерлендіру және әкімшілендіру деңгейі және статистикалық ақпарат жинау;

– Ғимараттың әр түрлі инженерлік жүйелеріндегі процестерді автоматтандыру іске асырылатын автоматты басқару деңгейі. Контроллерлер мен коммутациялық жабдықты қамтиды;

– Датчиктерді, атқарушы құрылғыларды және құрамдас бөліктер арасындағы тікелей физикалық қосылыстарды қамтитын құрылғылар деңгейі;

«Smart home» жүйесінде автоматтандырылған басқару деңгейін кеңейту және автономды шешім қабылдау мүмкіндігі есебінен диспетчерлендіру деңгейінің рөлін төмендету жүргізіледі. Автоматтандырудың жоғары деңгейі қауіпсіздіктің жаңа проблемаларына алып келеді. Ағымдағы қауіпсіздік зерттеулері бірінші кезекте құпиялылыққа, яғни жүйеде жиналатын және өңделетін ақпараттың құпиялылығына байланысты мәселелерді шешуге бағытталған. «Ақылды орта» үшін жалпы контексте негізделген қолжетімділікті бақылау модельдерін қолдану ұсынылады. Сонымен бірге қатынас субъектілері

жүйенің пайдаланушылары, ал объектілер біртұтас жүйені құрайтын құрылғылар болып табылады. Зерттеудің перспективалық бағыттарының бірі динамикалық орта компоненттерінің арасындағы өзара іс-қимыл кезінде қауіпсіздікті қамтамасыз ету үшін қолжетімділікті бақылауды қолдану болып табылады.

Мақсаты

«Smart home» жүйелеріндегі желілік өзара әрекеттесу кезінде қолжетімділікті басқарудың контекстік моделін қолдана отырып, компрометирленген құрылғылардан қорғауды қамтамасыз ету.

Міндеттер

1. «Smart home» жүйелеріндегі архитектураны, қауіпсіздік механизмдерін, желілік хаттамаларды талдау, қауіп моделін жасау.
2. «Smart home» жүйелеріне қолжетімділікті басқару контексттік модельдерінің қолданылуын талдау.
3. «Smart home» жүйелеріне арналған қолжетімділікті басқару контекстік моделін әзірлеу.
4. Әзірленген қолжетімділікті басқару моделін эксперименттік верификациялау үшін «smart home» бағдарламалық макетін жасау.

Нәтижелер

1. Қолданыстағы қауіпсіздік механизмдерімен қамтылмаған ағымдағы ішкі шабуылдау қауіптерін анықтау.
2. «Smart home» жүйелерінде қолжетімділікті басқару контекстік моделін қолдану мүмкіндігін және контекстік модельдің талап етілетін параметрлерін анықтау.
3. «Smart home» жүйелеріне әзірленген қолжетімділікті басқару контекстік моделі.
4. Әзірленген «Smart home» бағдарламалық макеті. Қауіпсіздікті бұзу сценарийлері негізінде эксперименталды верификация.

1 «Smart home» жүйелерінің қауіпсіздігін талдау

1.1 «Ақылды орта»

«Ақылды орта» - өз ресурстарын бөлісетін және бірге жұмыс істейтін құрылғылар қауымдастығы [2]. Ақылды ортаның табиғаты қарама-қарсы мақсаттарға ұмтыла алатын және қазіргі жағдай туралы әртүрлі тұжырымдамаға ие, бірақ сонымен бірге ортақ сенімді ақпараттық кеңістікте жұмыс істейтін әртүрлі құрылғылар мен қатысушылар арасындағы қақтығыстарға мүмкіндік береді. Ақпараттық қауіпсіздік қатерін азайту үшін ортақ ресурстарға қолжетімділікті басқарудің динамикалық тетігі қажет. Осылайша, операцияларды орындау контекст түрінде ортаның ағымдағы жағдайы туралы ақпаратты пайдаланатын қолжетімділікті басқару моделіне қажеттілік пайда болады.

«Ақылды ортаның» негізгі мақсаты қоршаған ортаға қатысты ақпаратты алу және талдау және пайдаланушыларға сыртқы ортамен өзара әрекеттесудің жаңа мүмкіндіктерін ұсыну болып табылады [1]. Бұдан басқа, пайдаланушылардың қажеттіліктеріне бейімделу механизмдері қолданылуы мүмкін. «Ақылды ортаның» келесі қасиеттерін анықтауға болады:

- құрылғылардың өзара әрекеттесуі;
- құрылғыны қашықтан басқару;
- құрылғылардың күрделі функционалы;
- «интеллектуалды» құрылғылар;
- желілік стандарттардың әртүрлілігі.

1.2 «Smart home»

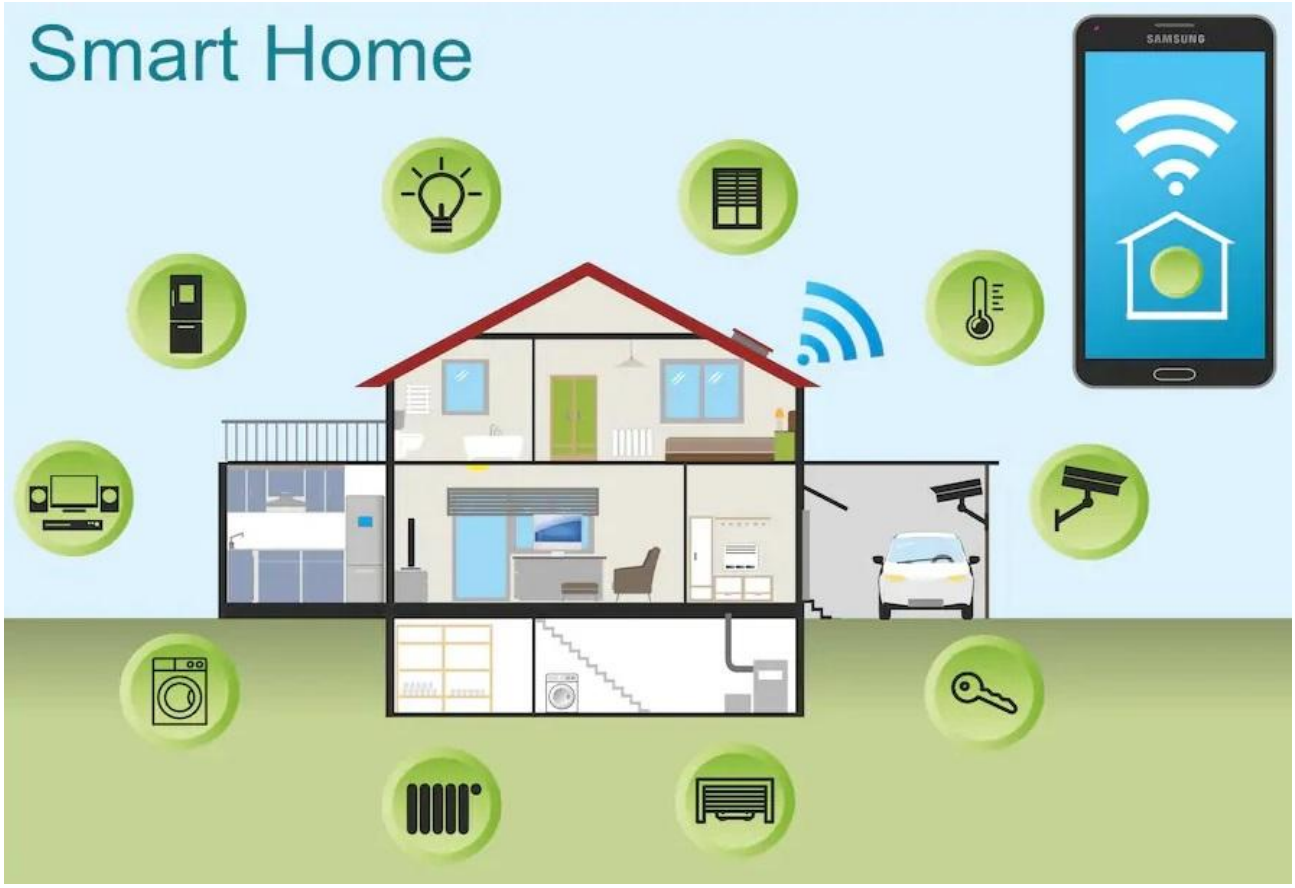
Ғимараттарды басқарудың автоматтандырылған жүйелері немесе технологиясы, «smart home» ғимараттарын пайдалану кезінде туындайтын түрлі міндеттерді шешу үшін кеңінен қолданылады.

«Smart home» технологиясы қауіпсіздікті қамтамасыз ету, ресурстарды үнемдеу және жалпы өмір сүру жағдайларын жақсарту мақсатында қазіргі заманғы автоматтандыру жүйелері мен әртүрлі перифериялық құрылғыларды қолдану болып табылады . Басты ерекшеліктердің бірі түрлі жағдайларға ден қою және тану бойынша жаңа мүмкіндіктер алу үшін түрлі автоматтандырылған кіші жүйелердің белсенді өзара іс-қимылы болып табылады. Физикалық тұрғыдан алғанда, мұндай жүйелер ҒБАЖ-ның дамуы болып табылады, олар өз кезегінде ғимараттар мен құрылыстарға АБЖ-ның бейімделуін білдіреді.

«Smart home» арналған электрониканың кез келген жиынтығы – пәтер, үй

коммуникациясы жүйелерінің қызметін автоматтандырылған және көбіне орталықтандырылған бақылауға, икемді, дәл басқаруға арналған жоғары технологиялық жабдық.

«Smart home» пәтерде немесе үйде әртүрлі инженерлік жүйелерді және басқа да жабдықтарды автоматты түрде басқаруға арналған бағдарламалық – техникалық кешеннен тұрады (1-сурет).



1 Сурет – «Smart home» жүйесі

Мұнда смартфоннан басқарылатын робот-шаңсорғыштардан бастап аспаптарға дейін тұрмыстық техника да, пәтерде немесе үйде не болып жатқанын бақылайтын жүйелер де бар. «Smart home» ғимаратта болып жатқан нақты жағдайларды түсінеді және алдын ала әзірленген алгоритмдер бойынша тиісті түрде оларға жауап береді. Бұл ретте адам бір командамен қалаған жағдайды көрсетеді, ал автоматика сыртқы және ішкі шарттарға сәйкес барлық инженерлік жүйелер мен электр құралдарының жұмыс режимін анықтайды және қадағалайды.

«Smart home» жүйесінің маңызды құраушылардың бірі – ақпаратты жинауға және оны басқару блогына беруге мүмкіндік беретін түрлі датчиктер. Тұрғын үй-жайларындағы датчиктер бірнеше түрге бөлінеді, олардың әрқайсысы белгілі бір функцияны орындайды және оларды кешенді пайдалану энергия ресурстарын үнемдеуге, қауіпсіздік пен мүлікті қорғаудың жоғары

деңгейінқомтамасыз етуге мүмкіндік береді.

1.3 «Smart home» жүйесі хаттамаларының қауіпсіздігін талдау

Ғимараттарды басқаруды автоматтандыру саласында қолданылатын көптеген хаттамалар бар. Қазіргі уақытта «Smart home» жүйесін құрайтын құрылғылардың желілік өзара әрекеттесуін ұйымдастыру үшін жалпы қабылданған стандарттар жоқ [3, 4]. Осы мақсатта жергілікті есептеу желілерін құру технологияларын қолдану олардың артық болуына байланысты перспективасы аз болып табылады. «Smart home» жүйесінде қолданылатын технологиялар келесі критерийлерді қанағаттандыруы тиіс:

- жоғары сенімділік және қауіпсіздік;
- қызмет түрлерінің бағасы төмен;;
- энергия экономды тұтыну;
- физикалық орналастырудың қарапайымдылығы.

Жүйені пайдаланудың көптеген сценарийлерінде деректерді берудің жоғары жылдамдықтарында қажеттіліктің жоқтығын жеке атап өтуге болады.

Сымды және сымсыз желілерді салыстыру кезінде шешуші фактор желілік құрылғыларды физикалық орналастырудың қарапайымдылығы болып табылады . Power Line Communication (PLC) деп аталатын бәсекеге қабілетті сымды желілік технологиялар тобы бар. Бұл технологиялар желіні орналастыратын үй-жайлар әдетте болатындығына негізделген электрлендірілген. Осылайша, электр желісінің сымдары арқылы байланысты қамтамасыз ету үшін X10, INSTEON, HomePlug, Lonworks сияқты бірқатар технологияларды қолдана отырып, сымды және сымсыз желілерді де, сымсыз байланыс үшін Bluetooth, Z-Wave және ZigBee құруға болады.

1.3.1 Z-Wave хаттамалар стегі

Z-Wave - Z-Wave Alliance әзірлеген және патенттелген хаттамалар стегі. Қазіргі уақытта «Smart home» құрылыс жүйелері саласында қолданудың ең перспективті хаттамаларының бірі. Z-Wave Alliance – бұл Z-Wave протоколын қолданатын немесе қолдайтын барлық компаниялардың альянсы. Z-Wave хаттамасы OSI жіктеудің барлық деңгейлерін қамтамасыз етеді, бұл гетерогенді желілерді құру кезінде әртүрлі өндірушілердің құрылғыларының үйлесімділігін қамтамасыз етуге мүмкіндік береді.

Z-Wave үшін келесі OSI деңгейлері анықталған:

- Физикалық деңгейі;

- Аралық деңгей. Бұл деңгейге тікелей көріну аймағында құрылғылардың тұтастығы мен адресациясы іске асырылады. Көп адресті және кен таратылатын таратылу мүмкін;
- Желі деңгейі. Z-Wave хаттамасының сипаттамалары тікелей қол жетімді емес құрылғылар арасында деректерді беру үшін пайдаланылатын пакеттік бағыттаудың алгоритмін анықтайды. Барлық тұрақты жұмыс істейтін желілік топтар басқа желі қатысушылары арасындағы пакеттерді бағыттауға қатысады. Пакеттік маршрут бастапқы түйін жебермес бұрын анықталады. Жіберушіге белгілі маршруттар бойынша қалаған түйінді табу мүмкін болмаса барлық желілік түйіндерге арнайы Explorer Frame пакетін жіберіп, бүкіл желі бойынша түйінді іздеу механизмі бар ;
- Көлік деңгейі. Бұл деңгейде Z-Wave жеткізілімді растайды және берілу кезінде пакет жоғалған жағдайда қайта жіберіледі. Ол үшін әрбір түйін қатысады. Бағыттау, хабарламаны алу фактісін растайды. Z-Wave-тегі желінің жүктемесін азайту үшін «үнсіз растау» механизмі қолданылады: пакет бағыты бойынша пакетті келесі В түйініне жеткізетін А түйіні, сәтті берілсе, эфирді тыңдау арқылы пакетті В түйінімен әрі қарай жіберу фактісін анықтай алад;
- Сеанс деңгейі. Сеанстық кілтті орнату үшін шифрлау қосылған кезде ғана қолданылады;
- Қолданбалы деңгей. Z-Wave спецификациясы бағдарлама деңгейінде алынған командаларды түсіндіру алгоритмін анықтайды. Бұл деңгей командалық класстар жиынтығымен сипатталады. Кейбір кластар үшін приборларды түсіндіруге арналған бірнеше нұсқа бар, олар құрылғы класына байланысты.

1.3.2 Z-Wave желісіне шабуылдар

Автоматтандыру жүйесінің өте қиын компоненттері құлыптар болып табылады, қазіргі уақытта AES-128 шифрлауын пайдаланады. Алайда, шифрлау стандарттары ескірген құрылғыларға қолданылмайды. Сонымен қатар, жұмыс барысында көрсетілгендей, бірқатар құрылғылар кілттерді алмасу хаттамаларын іске асыруда осалдықтарға ие болуы мүмкін, бұл оларға 00000000000000000000000000000000000000000000000000000000h әдепкі кілтті қолдану арқылы қолжетімділікті басқаруға мүмкіндік береді.

Z-Wave хаттамасына негізделген «smart home» жүйесін басқаруды жеңілдететін бірқатар шешімдер бар. Осындай сертификатталған шешімнің бірі - Z-Way. Жүйемен өзара әрекеттесудің негізгі құралы веб-интерфейс және ол қолданатын API болып табылады. Алайда, аутентификация және деректерді шифрлау тетіктері қамтамасыз етілмеген. Мұндай жағдайда шабуылдаушы жергілікті желіні бұзғаннан кейін «smart home» жүйесімен еркін әрекеттер жасай

алады.

1.3.3 ZigBee хаттамалар стегі

ZigBee - бұл автоматтандыру жүйелеріне арналған ашық сымсыз стандарт . Стандарт жоғарғы деңгейлі желілік хаттамалардың сипаттамасынан тұрады - қолданбалы қабат және желілік қабат [6]. Төменгі деңгейдегі қызметтер - ортаға және физикалық қабатқа қолжетімділікті басқару деңгейі IEEE 802.15.4 стандартымен реттеледі.

Қолданбалар деңгейі ZigBee құрылғысының нысанын, қолданбаларды қолдау деңгейін және қолданбаларды әзірлеу интерфейсінің деңгейін анықтайды.

Бағдарламалық жасақтама интерфейсі стандартты деректер түрлерін, қызметтерді табу дескрипторларын және пакеттік форматтарды анықтайтын сипаттаманы қамтиды. Мұның бәрі атрибуттарға негізделген қарапайым профильдерді жылдам жасауға мүмкіндік береді. Бағдарлама нысандары - ZigBee Endpoint құрылғыларын басқаратын бағдарламалық модульдер.

Қосымшаны қолдаудың ішкі қабаты ZigBee құрылғысының профильдері мен қосымшаларына мәлімет беруге жауап береді. Сонымен қатар, төменгі деңгей ZigBee желісіндегі құрылғылардың қосылуын бақылайды және олар туралы мәліметтерді сақтайды.

- Желілік деңгей желілік адрестерді басқару және бағыттау функцияларын орындайды. Оның міндеттеріне: желісін іске қосу;
- желілік мекенжай беру;
- желілік құрылғыларды қосу және жою;
- хабарларды бағыттау;
- қауіпсіздік саясатын қолдану;
- маршруттарды іздеу.

Физикалық деңгейлер IEEE 802.15.4 стандартпен анықталады:

- Ортаға қатынауды басқару деңгейі құрылғының тікелей көршілермен сенімді байланысы үшін жауап береді, коллизияларды шешуге көмектеседі;
- Физикалық деңгей физикалық тарату ортасында интерфейсті қамтамасыз етеді. Физикалық деңгей әртүрлі жиілік диапазондарында жұмыс істейтін екі деңгейден тұрады.

Қауіпсіздік провайдері шифрлауды пайдалану кезінде желілік деңгей мен бағдарлама деңгейіне арналған қауіпсіздік механизмдерін қамтамасыз етеді.

1.3.4 ZigBee желісіне шабуылдар

ZigBee желілері шифрланбаған режимдерде жұмыс істей алады. Стандартты қауіпсіздік деңгейі желілік кілттердің таратылу қауіпсіздігін қамтамасыз етпейді.

Қайталанатын шабуылдардың алдын алуға арналған монотонды ұлғайтқыш тетігі бар. Алайда, механизмді іске асыру желі жұмысындағы проблемаларды тудыруы мүмкін, бұл санауыштарды қолмен тастау қажеттілігіне әкеледі. Осы параметрді қосусыз қайталанатын шабуыл тривиальді болып табылады [7].

Кедергі трафигінен кілтті қайта алуға және алуға жасалған шабуылдар іс жүзінде ZigBee желілерін талдауға арналған KillerBee аясында жүзеге асырылады.

1.4 «Smart home» жүйелеріндегі қауіпсіздік қатері

«Smart home» жүйелері үшін көптеген компьютерлік желілерге ортақ бірқатар қауіп-қатерлер бар [8]. Оларды жүзеге асыру мүмкіндігіне әкелетін бірқатар әртүрлі шабуылдар мен осалдықтар қарастырылды [9].

1 кесте – «smart home» жүйелерінің қауіпсіздігіне қатер

№	Шабуыл түрі	Осалдық	Салдары
1	Орталық торапқа шабуылдар	«Smart home» желісін интернетке қосу. Желі периметрін қорғау тетіктерінің болмауы (тиімсіздігі)	Орталық сервердің, немесе бүкіл жүйенің дұрыс жұмыс істемеуі немесе істен шығуы. Құпиялылықты, ақпараттың тұтастығын және қолжетімділігін бұзу
2	Вирус және трояндық бағдарламалардың жүйенің жұмысына әсері	«Smart home» желісін интернетке қосу. Желі периметрін қорғау тетіктерінің болмауы (тиімсіздігі)	Жүйелікбағдарламалық қамтамасыз етудегі ақаулар. Құпиялылықты тұтастықты бұзу және ақпараттың қол жетімділігі
3	Сымды және сымсыз байланыс арналары бойынша берілетін ақпаратты ұстап қалу	Зиянкестердің сымды арналарға немесе желілік радио сигналдарды тұрақты ұстау аймағына кіру мүмкіндігі. Трафикі қорғау тетіктерінің болмауы (тиімсіздігі)	Қызмет – еңбектік құқық қатынастарының негізінде жүзеге асырылатын қызметтен басқа, тұлғалардың қажеттіліктерін қанағаттандыруға бағытталған кәсіпкерлік қызмет.

1 кестенің жалғасы

4	Парольдерді және қолжетімділікті шектеудің басқа да деректемелерін ұрлау арқылы орталық торапқа әкімші құқығымен кіру мүмкіндігі.	Аутентификация және сәйкестендіру тетіктерінің болмауы (тиімсіздігі)	Желі ішіндегі ақпараттың құпиялылығын, тұтастығын және қолжетімділігін бұзу
5	Рұқсат етілмеген пайдаланушылар желісіне кіру.	Аутентификация және сәйкестендіру тетіктерінің болмауы (тиімсіздігі)	Желі ішіндегі ақпараттың құпиялылығын, тұтастығын және қолжетімділігін бұзу
6	Пайдаланушының қателері.	Пайдаланушылардың қате әрекеттерінен жүйені қорғау тетіктерінің болмауы (тиімсіздігі)	Ақпараттың құпиялылығын, тұтастығын және қолжетімділігін бұзу. Жабдықты дұрыс пайдаланбау алдарынан жүйеде іркілістер болуы мүмкін
7	Жүйенің аппараттық ақаулығы	Жабдықтың төмен сенімділігі, персоналдың төмен біліктілігі	Ақпараттың құпиялылығын, тұтастығын және қолжетімділігін бұзу
8	Бағдарламалық қамтамасыз ету қателері	Лицензиясыз БҚ пайдалану, персоналдың біліктілігінің төмендігі	Ақпараттың құпиялылығын, тұтастығын және қолжетімділігін бұзу

Қарастырылған шабуылдардың негізінде қолжетімділікті басқарудың контекстік моделін пайдалану арқылы алдын алуға болатын қауіптерге қатысты қорытынды жасауға болады.

1.5 Қорытындылар

Жүйенің қауіпсіздігін қамтамасыз етудің алға қойылған мақсатына сүйене отырып, оны құрайтын құрылғылардың өзара іс-қимылы кезінде келесі қауіптер анықталды.

- Зиянкес код:
  - вирус жұққан құрылғыны қосу;
  - желідегі құрылғылардың зақымдануы.
- Құрылғының істен шығуы:
  - датчиктердің дұрыс емес деректері;
  - қате командалар.

– Конфигурация қатесі:
  – жүйенің дұрыс емес әрекеті;
  – жұмыс режиміндегі ақаулар.

Қолжетімділікті басқарудың әзірленетін контекстік моделі осы қатерлерден қорғауға бағытталатын болады.

2 «Smart home» жүйелерінің қауіпсіздігін күшейту үшін қолжетімділікті басқарудың контекстік моделін қолдану

2.1 Қолжетімділікті басқарудың формальді модельдері

2.1.1 Рөлдік модель

Негізгі рөлдік модельді сипаттаймыз [10]. *S* және *O* объектілері көптеген субъектілер ұғымын енгіземіз. Олардың мүшелерін келесідей белгіленеді S_i, *Oi:*

$$S_i \in Si\, o_i \in O. \quad (1)$$

Пәндерге берілген көптеген рөлдер туралы түсінік енгіземіз. Бұл жиынның мүшелері r_i болып табылады:

$$ri \in R. \quad (2)$$

Сондай-ақ, пайдаланушылар көптеген *P* операциялары үшін белгілі бір операцияларды орындай алады:

$$p_i \in P. \quad (3)$$

Қолжетімділікті басқарудың рөлдік моделі жұмыс істегенде келесі функциялар қолданылады:

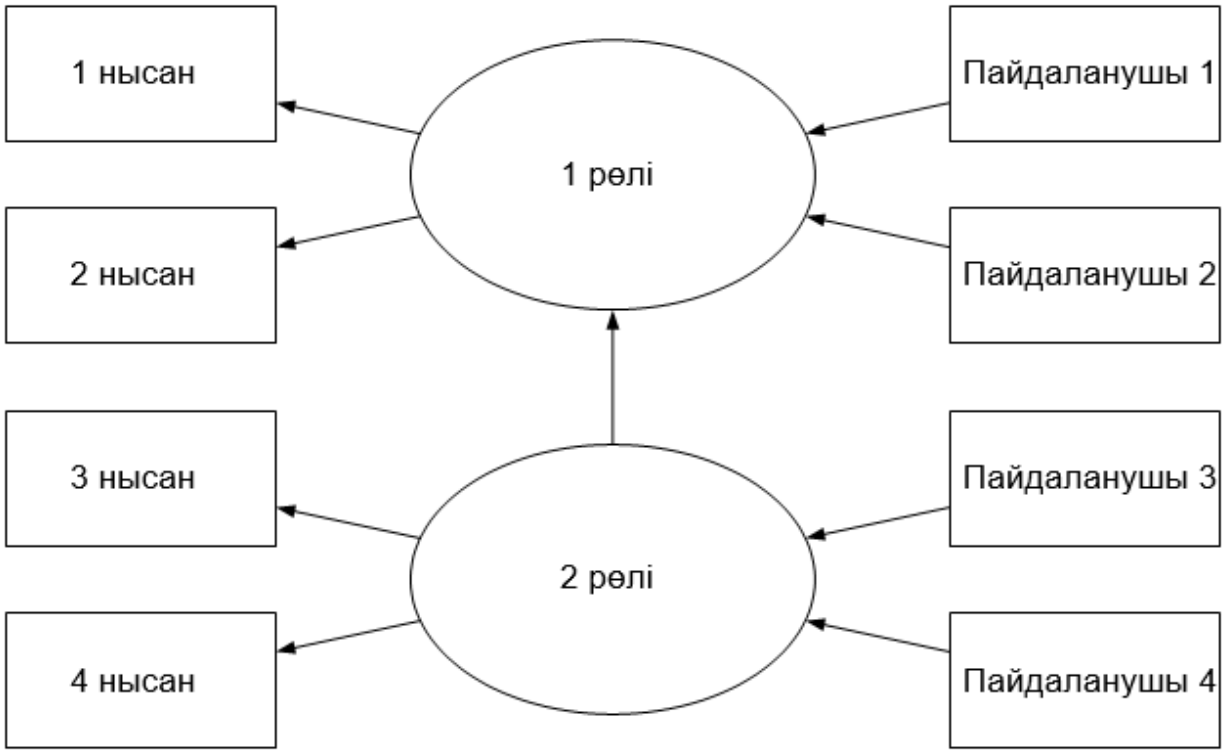
1. Пайдаланушы рөлдері тізімін алу функциясы:
   $Roles(s_i) = \{si$ пайдаланушыға тағайындалған рөлдер$\}$.
2. Қолжетімділікті бақылаудың рөлдер тізімін алу функциясы:
   $Ops\ (ri) = \{r_i$ рөлге байланысты операциялар$\}$.
3. Рөлге арналған объектіде жарамды операцияларды алу функциясы:
   $Perms\ (r_i, oj) = \{o_j$ бойынша операциялар, қолжетімді *ri* рөлдері$\}$.
4. Субъектінің объектіге операция жасау мүмкіндігін тексеру функциясы:

$$Execute\,(si, o_j, pk) = r_m \in Roles\,(s_i)\colon pk \in Ops\ (rm),\ p_k \in Perms\ (r_m, oj). \quad (4)$$

Бірінші үш функция осы қолжетімділікті басқару моделін пайдаланатын жүйенің ағымдағы конфигурациясы туралы ақпаратты алу үшін пайдаланылады. Соңғысы жүйеге кіру субъектілерінің жұмысы кезінде қолданылады. Дәл осы функция субъектінің сұрау салынған операцияны орындау мүмкіндігін анықтау және кіруді бақылау үшін қолданылады.

Рольдер иерархиясын қосу арқылы модельді қосымша кеңейту мүмкін (2-сурет). Мұндай механизм жаңа рөлдерді қосу рәсімін жеңілдетеді, оларды бұрыннан бар рөлдерге негіздеуге және олардың өкілеттігін кеңейтуге мүмкіндік

береді.



2 Сурет – қолжетімділікті басқарудың рөлдік моделіндегі рөлдердің иерархиясы

Келтірілген суретте рөлдер иерархиясы механизмімен ұсынылатын мүмкіндіктер үлгісі көрсетілген. Осылайша, 1 рөлінің негізінде 2 рөлі құрылды. Осының нәтижесінде 3 және 4 пайдаланушылар 3 және 4 объектілерге, сондай-ақ 1 тағайындалған рөлді пайдаланушылар рұқсаты бар объектілерге қол жеткізе алады.

2.1.2 Мандаттық модель

Қарауға екі мандаттық модель таңдалды - Белла-Лападулы және Биба моделі.

Белла-Лападулы моделі қорғалатын ақпаратқа қолжетімділікті шектеуге арналған және көптеген мемлекеттік мекемелерде қабылданған құжат айналымының ережелеріне негізделген [11].

Модельдің ресми сипаттамасы келесі анықтамалардан тұрады:

– *S* – көптеген қолжетімділік субъектілер, $S = \{s_1, s2, \ldots, s_k\}$;

– *O* – көптеген қолжетімді объектілері, көптеген субъектілерді қамтиды, $O = \{o1, o_{2,\ldots}, om, s_1, s2, \ldots, s_k\}$;

– R – көптеген қолжетімділік құқықтары; байланыстың екі түрі анықталған - оқу және жазу, яғни $R = \{read, write\}$;
– L – көптеген қауіпсіздік деңгейлері, $L = \{l_1, l2, \ldots, l_n\}$;
– $\Lambda = (L, \leq, \cdot, \otimes)$ – қауіпсіздік деңгейлерінің торы
– V – жүйенің көптеген күйлері, реттелген жұптардан тұратын (F, M), мұнда $F:S \cup O \rightarrow L$ – құпиялылық деңгейлерін субъектілермен және объектілермен салыстыратын функция, M – қолжетімділік құқығының матрицасы.

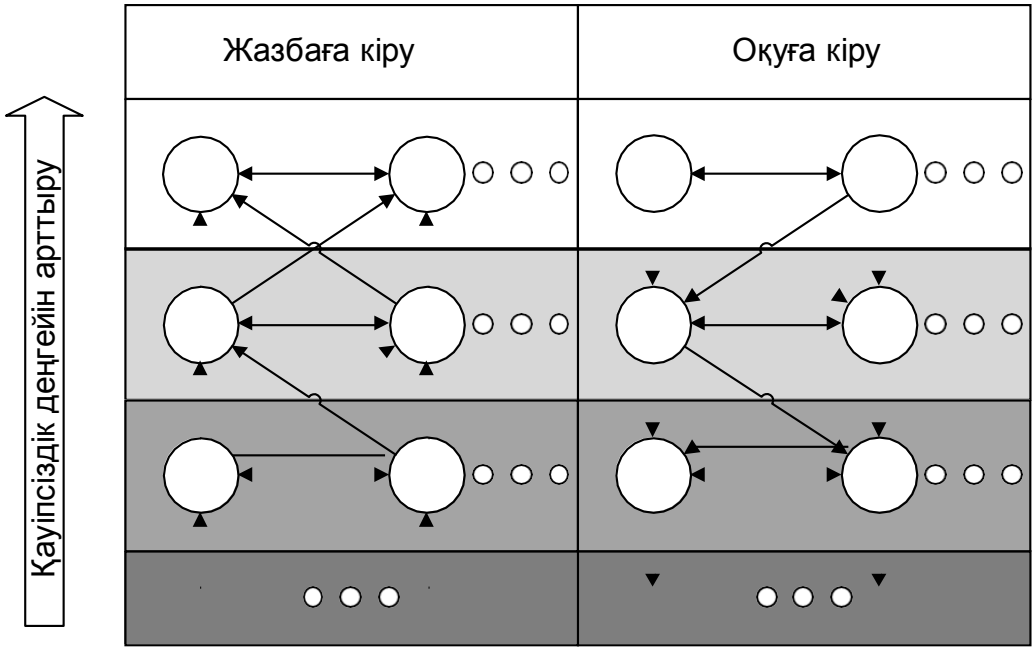
Қауіпсіздік деңгейлерінің торын қарастырайық – Λ. Ол көптеген қауіпсіздік деңгейлерін қамтиды L, реттің жартылай тұрақсыз қатынасының операторы $\leq$, ең аз жоғарғы және ең үлкен төменгі шектерді алу операторлары $\cdot$ және $\otimes$ тиісінше.

Операторлар $\cdot$ және $\otimes$ төмендегідей сипатталады:

– $l1 \cdot l_2 = l \leftrightarrow l_1, l2 \leq l \wedge l' \in L: (l' \leq l) \rightarrow (l \leq l_1 \vee l \leq l_2)$;

– $l1 \otimes l_2 = l \leftrightarrow l \leq l1, l_2 \wedge l' \in L: (l \leq l_1 \vee l' \leq l_2) \rightarrow (l' \leq l)$.

3 суретте қауіпсіздік деңгейлерінің торы бейнеленген және әр түрлі деңгейдегі субъектілер үшін рұқсат етілген қолжетімділікті басқару құқықтары көрсетілген.



3 Сурет – қауіпсіздік деңгейлерінің торы

Белла-Лападулы моделінің қауіпсіздігі келесі екі ережелерге негізделеді.

Қарапайым қауіпсіздік ережесі

ls қауіпсіздік деңгейі бар субъекті тек шарт орындалса ғана *lo* қауіпсіздік

деңгейі бар нысанға *read* рұқсаты беріледі:

$$l_o \leq ls \tag{5}$$

Қауіпсіздік ережесі

ls қауіпсіздік деңгейі бар субъекті тек шарт орындалса ғана *lo* қауіпсіздік деңгейі бар нысанға *write* рұқсаты беріледі:

$$ls \leq l_o \tag{6}$$

Осы екі шартты орындау кезінде жүйенің жай-күйі қауіпсіз деп есептеледі. Егер шарттар жүйенің барлық жағдайы үшін орындалса, онда жүйе қауіпсіз деп саналады.

Биба моделі алдыңғы үлгінің модификациясы болып табылады және ұқсас анықталады. Бұл ретте модель құпиялылық емес, деректердің тұтастығын қамтамасыз етуге бағытталған.

Негізгі анықтамалардың қысқаша сипаттамасы:

– S – көптеген қолжетімділік субъектілер, $S = \{s_1, s2, \ldots, s_k\}$;
– O – көптеген нысандар, $O = \{o1, o_{2,\ldots,} om, s_1, s2, \ldots, s_k\}$;
– R – көптеген қол жеткізу құқықтары, $R = \{read, write\}$;
– L – көптеген қауіпсіздік деңгейлері, $L = \{l1, l_2, \ldots, ln\}$;
– $\Lambda = (L, \leq, \cdot, X)$ – қауіпсіздік деңгейлерінің торы.

Бибі үлгісінде екі негізгі ереже бар.

Тұтастықтың қарапайым ережесі

ls қауіпсіздік деңгейі бар субъекті тек шарт орындалса ғана l_o қауіпсіздік деңгейі бар нысанға *read* рұқсаты беріледі:

$$lo \leq l_S \tag{7}$$

Тұтастық ережесі

ls қауіпсіздік деңгейі бар субъекті тек шарт орындалса ғана *lo* қауіпсіздік деңгейі бар нысанға *write* рұқсаты беріледі:

$$ls \leq l_o \tag{8}$$

Осы екі шартты орындау кезінде жүйенің жай-күйі қауіпсіз деп есептеледі.

2.2 Қолжетімділікті басқарудың контекстік модельдері

Қолжетімділікті басқарудың контекстік модельдері қорғалған жүйе туралы статистикалық ақпаратты қолданатын қолданыстағы модельдерден ерекшеленеді, себебі олар басқарылатын операция кезіндегі жүйенің жай-күйі туралы ақпаратты пайдалану әдістерін қамтиды. Бұл ақпарат контекст деп аталады.

2.2.1 Контекст ұғымы

Контекст - жұмыс уақытындағы жүйелік құрылғылардың кумулятивтік жағдайы. Құрылғы күйі үшінші тарап құрылғыларында оқуға болатын оның параметрлерінің жиынтығымен сипатталған. Осылайша, контекст жүйенің өлшенетін параметрлерін сипаттайтын гетерогенді элементтерден тұрады. Мұндай элементтердің мысалы ретінде қазіргі уақыт, құрылғының орналасуы, орындалған тапсырмалар болуы мүмкін.

Сондай-ақ, контекст жеке параметрлер туралы тарихи деректерді қамтуы мүмкін. Бұл жағдайда, сондай-ақ, параметрлердің уақыт бойынша бірлескен өзгерістерін қадағалау мүмкіндігі үшін байланыс ақпаратын сақтау қажет. Тарихи деректердің болуы операцияны орындау сәтіндегі жүйе жағдайы ретінде контекст анықтамасына қайшы келмейді, өйткені жүйе орналасқан ағымдағы жағдай бұрын болған және контекстің өзгеру тарихында көрініс тапқан белгілі бір оқиғалардың нәтижесі болып табылады.

2.2.2 Контексті жинау және талдау әдістері

Қолжетімділікті басқарудың контекстік модельдерін әзірлеу кезінде тұрған маңызды міндеттердің бірі контексті жинау және талдау болып табылады. Қолжетімділікті басқару мақсатында контексті қолдану мүмкіндігін алу үшін сенсорлардан алынатын өңделмеген деректерді дайындау қажет. Деректерді дайындаудың келесі кезеңдерін ерекшелеуге болады.

- Деректерді қалыпқа келтіру. Қолжетімділікті басқару жүйесімен өңдеу үшін жарамды әр түрлі құрылғылардан деректерді бірыңғай нысанға келтіру процесі.
- Деректерді сүзу. Талдауға қатысты деректерді алу процесі.
- Деректер корреляциясы. Бір-біріне тәуелді әр түрлі мәндерді өзара байланыстырудан тұратын мәліметтерді дайындаудың бастапқы кезеңі.

2.2.3 Қолжетімділікті басқару механизмдері

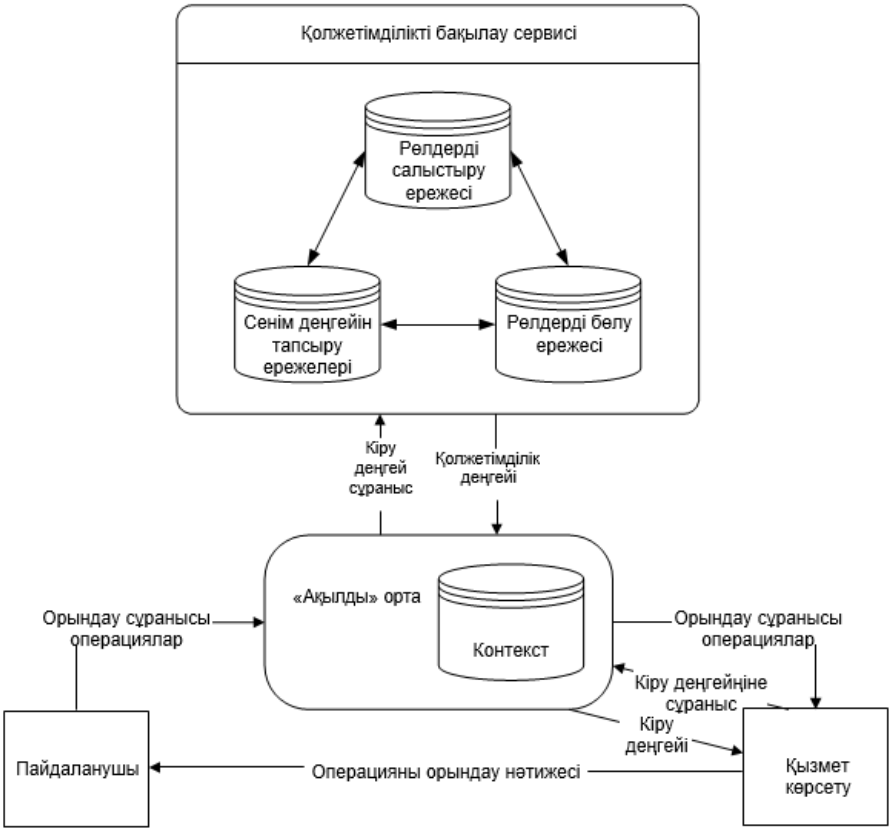
Контекстік модельдердегі қатынасты басқару контекстке негізделген жетілдірілген ережелерге негізделген. Ережелер белгілі контекст параметрлері негізінде берілген қолжетімділікті басқару құқығын көрсетуге мүмкіндік береді. Мәтінмәндік қолжетімділікті бақылау ережелерін сипаттау тілінің үлгісі жұмыста қолжетімділікті басқару саясатының тілі болып табылады

Қарастырылып отырған жұмыста контекстік модель рөлді кеңейтеді және рөлдерді динамикалық бөлу үшін контекст қолданады. Бұл үшін қолжетімділікті басқару саясатының үш жиынтығы анықталады:

1. TrustValue мәндер негізінде контекст элементтері бойынша пайдаланушының сенім деңгейін анықтайды;
2. Assign_role кейбір контекст элементтеріне сенім деңгейлерінің негізінде рөлдерді бөлуді орындайды;
3. Классикалық рөлдік модель ретінде Permissions рөлдерді артықшылықтар жиынтығымен салыстырады.

Қолжетімділікті басқару саясаты қорғалатын жүйеге қойылатын шарттар мен талаптарды негізге ала отырып, алдын ала жасалуы тиіс. Контекст мәні бойынша пайдаланушыға сенім деңгейін беру үшін ережелерді жасауға ерекше назар аудару қажет.

Қолжетімділікті қамтамасыз ету процесі 4 суретте көрсетілген схема түрінде ұсынуға болады.



4 Сурет – қолжетімділікті бақылаудың контекстік тетігінің жалпыланған архитектурасы.

4 суретте қолжетімділік процесіне қатысатын негізгі компоненттер көрсетілген. «Ақылды ортаны» құрайтын құрылғылардың бірі ұсынатын сервиске пайдаланушының қолжетімділігінің типтік сценарийі қарастырылады.

Пайдаланушы мен құрылғы арасындағы байланыс «ақылды ортаға» қолдау көрсететін арнайы құрылғылар арқылы бір желіге қосылу және контексттуралы ақпарат жинау арқылы жүзеге асырылады деп болжанады. Қоршаған ортаға пайдаланушының құқықтарын тексеру операцияларын орындау үшін жасалған қатынас брокері кіреді.

Сервисті пайдаланушы белгілі бір қатынау деңгейін талап ететін операцияны орындауға сұрау жібереді. Сұрау салуды орындау алдында брокер қолжетімділікті басқару сервисінен ағымдағы қолжетімділік құқықтары туралы ақпаратты оған ағымдағы контексті хабарлай отырып сұратады. Қолжетімділік басқару сервисі жүйенің қауіпсіздік саясатын сақтайды және келесі алгоритм бойынша қолжетімділік құқығын анықтайды:

1. Пайдаланушы контекстінің сандық қолтаңбасын тексеру орындалды. Егер қолтаңба дұрыс болса, келесі қадамға өту жүргізіледі. Қолтаңба дұрыс болмаса басқару қызметі қолжетімділіктен бас тартады.

2. Контекст элементтері бойынша пайдаланушының сенім деңгейі есептеледі. Дәл осы кезеңде контекст талдауы жүргізіледі, одан әрі контекст элементтерінің тікелей мәндері пайдаланылмайды.

3. Контекст элементтері бойынша сенім деңгейі негізінде пайдаланушыға рөлдерді беру мүмкіндігі тексеріледі. Пайдаланушы рөлдерінің тізімі анықталады.

4. Рөлдер тізімінің негізінде сұрау салынған қызметке кіру құқығын тексеру жүргізіледі. Операция нәтижесі брокерге қайтарылады.

Қолжетімділікті басқару құқығы болса, сұралған операция орындалады. Сервис пайдаланушының қолжетімділік деңгейі туралы ақпарат алады және операцияны орындау нәтижесін хабарлайды.

2.3 Қорытынды

Контексті қолдану қолжетімділікті басқарудың жаңа мүмкіндіктерін туғызады. Қарастырылған қолжетімділікті басқару моделінің сипаттамасына сүйене отырып, қолжетімділікті басқару контексттік модельдерінің келесі артықшылықтарын ажыратуға болады:

- қолжетімділікті басқару саясатының параметрлерін өзгерту;
- жүйені қоршаған ортаға бейімдеу.

Сонымен қатар, «smart home» жүйесінің басқа да автоматтандыру құралдары арасында оларды бөлетін «smart home» жүйесінің қасиеттеріне сәйкес келетіндіктен, модельдің мұндай қасиеттері толық көлемде «smart home» жүйелерінде іске қосылуы мүмкін.

3 Контексттік қолжетімділікті басқаудың моделіне негізделге «Smart home» қауіпсіздік жүйесін жобалау

Бұл тарауда жүргізілген зерттеулерге негізделген ұсынылған «smart home» қауіпсіздік жүйесі сипатталған.

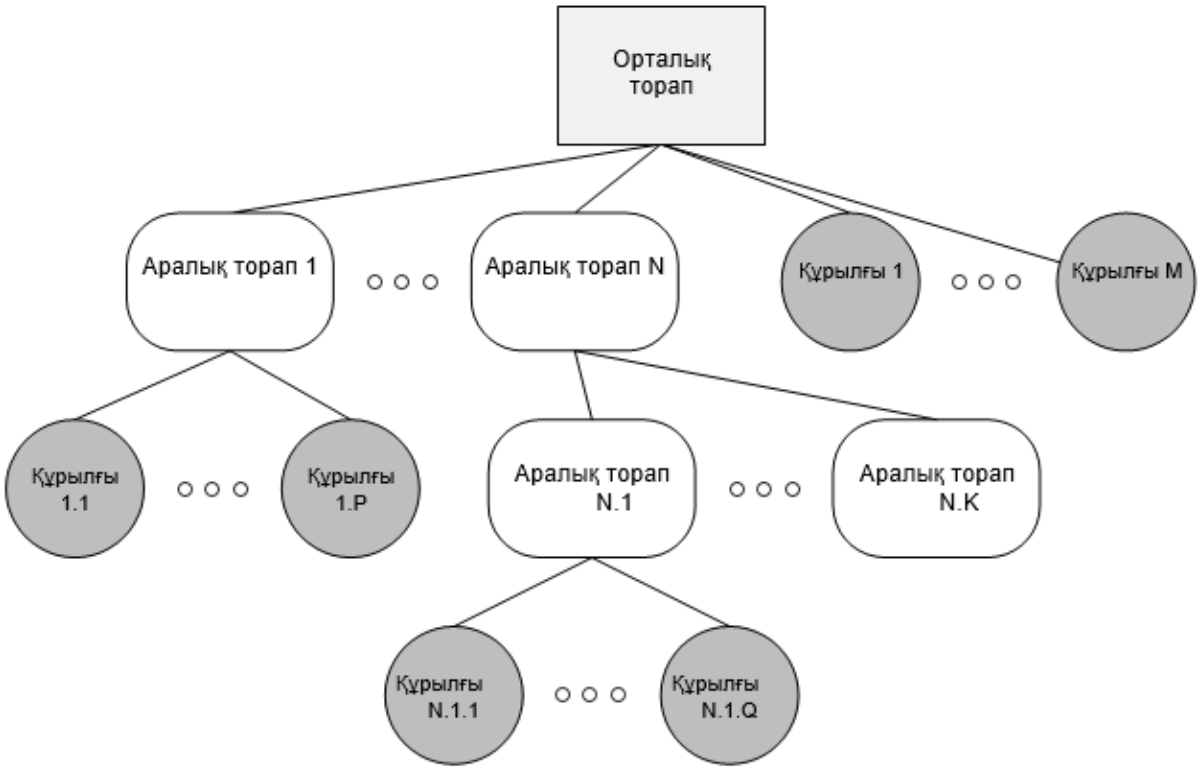
3.1 Контексттік қолжетімділікті басқарудың моделіне негізделген «smart home» жүйесінің архитектурасы

Қазіргі уақытта «smart home» жүйесін құруға кең таралған көзқарас мамандандырылған орталық тораптарды пайдалануды көздейді. Мұндай жүйелердің мысалы Philips және Samsung компаниялары ұсынатын шешімдер болып табылады [12] әр түрлі «ақылды құрылғылар» мен берілетін интерфейстерді пайдаланатын басқару бағдарламалары арасындағы көпір болып табылатын құрылғыда негізделген.

ZigBee сияқты технология негізіндегі желілер ұяшықты топологияны пайдалануға мүмкіндік бергеніне қарамастан, ZigBee қолдайтын "ағаш" топологиясын қолдану жиі ұсынылады. Бұл жағдайда желідегі тораптар үш топқа бөлінеді:

1. Орталық торап. Желідегі негізгі құрылғы болып табылады және құрылғылардың өзара әрекеттесуі мен қауіпсіздікті қамтамасыз ету бойынша негізгі функцияларын қамтамасыз етеді.
2. Аралық тораптар. «Smart home» автоматтандыру функцияларын орындаудан басқа, басқа тораптар арасында хабарламаларды ретрансляциялау жолымен желіні кеңейтуге мүмкіндік береді.
3. Соңғы түйіндер. Осы типті тораптар «Smart home» автоматтандыру бойынша түрлі функцияларды орындайды.

Суретте желінің мысалы көрсетілген. Аралық тораптар тізбекті қосу арқылы желіні кең ауқымда кеңейтуге мүмкіндік береді.



5 Сурет – «Smart home» желісінің топологиясы»

Топологияның осы түріне сүйене отырып, «smart home» жүйесінде қолжетімділікті басқарудың орталықтандырылған шлюзін пайдалану ұсынылады. Мұндай тәсіл қолжетімділікті контекстік бақылауды енгізу процесін жеңілдетуге мүмкіндік береді және «smart home» нақты жүйелерінде пайдаланылатын тәсілдерге сәйкес келеді. 6 суретте қолжетімділікті басқару жүйесінің жұмыс процесі көрсетілген.

Процесс төрт кезеңге бөлінеді:

1. Желілік өзара әрекеттесуді талдау. Құрылғылар қатынауды бақылау шлюзі арқылы бір-бірімен өзара әрекеттеседі, нәтижесінде бұл тапсырма тривиальды болады.

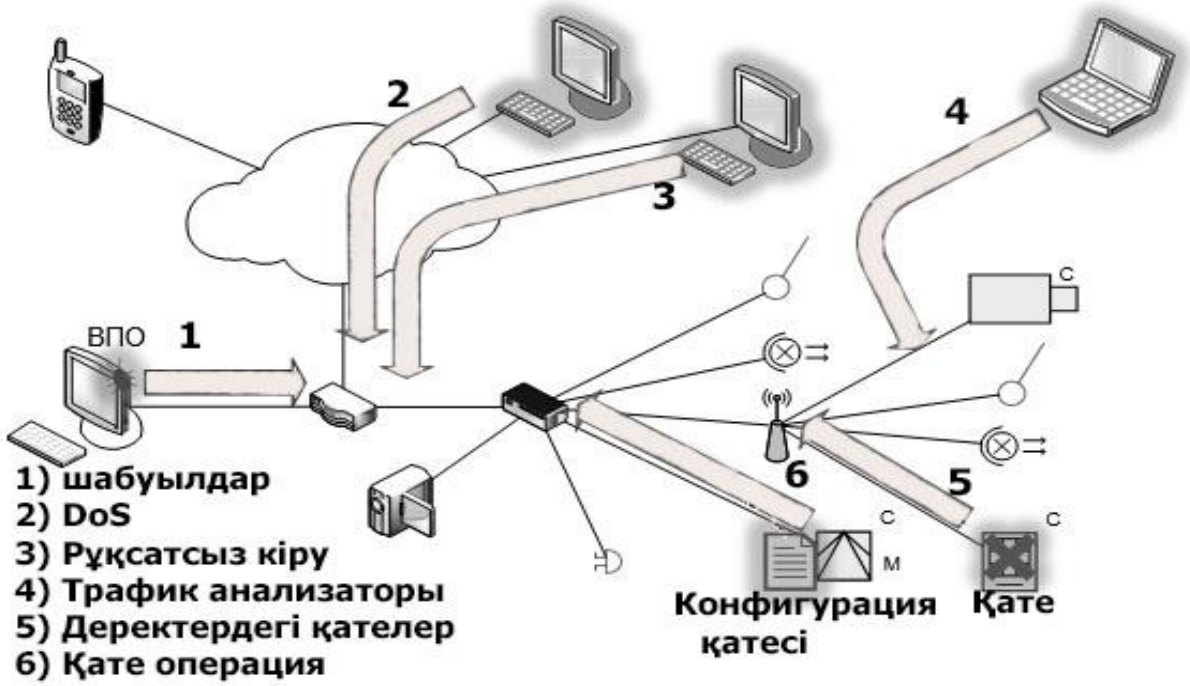
2. Қолжетімділікті басқару ережелерін қолдану. Бұл кезеңде құрылғылар арасындағы сұраулар қолжетімділікті басқару ережелеріне сәйкес сүзіледі.

3. Контексті жаңарту. Бұл бұрын алынған сұрауларға және құрылғыларды тікелей тексеруге негізделген. Параметр мәндерінің журналдары және орындалған операциялар контексттің бөлігі ретінде сақталады, өйткені олар жаңа күйге көшу процесін көрсетеді.

4. Қолжетімділікті басқару ережелерін жаңарту. Жаңартылған контекст және контекстік модель саясаты негізінде қолжетімділікті басқару ережелерін жаңарту және оларды іске қосу жүргізіледі.

6 Сурет – қолжетімділікті бақылау жүйесінің жұмыс процесі

Қолжетімділікті басқару шлюзінің архитектурасы 7 суретте көрсетілген. Шлюз компоненттері үш ішкі жүйеге біріктірілген – қолжетімділкті басқару, саясат пен контекст сақтау және желімен өзара әрекеттесу.



7 Сурет – қолжетімділікті басқару шлюзінің архитектурасы

Бұдан әрі жүйенің әртүрлі компоненттерін іске асыру бөлшектері сипатталады.

3.1.1. Контексті жинау және сақтау әдістері

Жүйенің негізгі құраушысы, контексті бақылау моделін іске асыратын, контексті сақтау мен жинау үшін жауап беретін кіші жүйе болып табылады. Кіші жүйе шешетін міндеттер 8 суретте көрсетілген. Қарастырылып отырған «smart home» жүйесінің архитектурасы шеңберінде осы операцияларды орындау бойынша бірқатар мүмкіндіктер бар.

8 Сурет – контексті жинау мен сақтаудың негізгі міндеттері

Әзірленген модель үшін бірнеше жолмен контекст жинау ұсынылады:

– құрылғылар арасындағы сұраныстарды талдау арқылы;
– құрылғы арқылы сауалнама жүргізу.

Бірінші әдісті іске асыру неғұрлым күрделі, сондай-ақ «smart home» желісіндегі құрылғыларға қосымша жүктеме тұрғысынан тиімдірек. Бұл қолжетімділікті басқару шлюзі қалыпты жұмыс кезінде құрылғылар арасындағы барлық сұраныстарды қабылдайтындығына және қолжетімділікті басқару ережелеріне сәйкес оларды сүзуге жауап беретіндігіне негізделген.

Осылайша, қолжетімділікті басқару шлюзі сұрау салудың орындалуыжәне орындау нәтижесін алуы тиіс бе екенін анықтай алады. Сұраныстарды талдау алгоритмі 8 суретте келтірілген.

9 Сурет – контексті жаңарту үшін сұраныстарды талдау алгоритмі

Екінші әдіс кез келген сұрауларды орындамай өзгертетін құрылғылардың параметрлерін алуға арналған. Мұндай құрылғылар параметрлері оның ішінде өлшенетін шамалар болып табылатын әр түрлі датчиктер болып табылады.

Бірінші әдіспен айырмашылығы, жүйенің жұмысы кезінде контекстті жаңарту үздіксіз жүреді, екінші әдіс құрылғыларды мерзімді түрде сұрауды қажет етеді.

3.1.2. Қолжетімділікті басқару әдісі

2 бөлімде қолжетімділікті басқарудың келесі модельдері қаралды:

- рөлі;
- Белла-Лападуланың мандатты моделі;
- Биба мандаттық моделі.

Қолжетімділікті басқарудың әзірленген моделі үшін Биба тұтастығының моделі таңдалды. Оның пайдасына таңдау келесі талаптардың негізінде жасалды :

- қолжетімділікті басқару моделі құрылғыларды әртүрлі қатынасу құқықтары бар топтарға бөлуге мүмкіндік беруі тиіс;
- жекелеген субъектілердің қолжетімділік құқықтарын өзгерту процесі автоматты режимде жүргізу үшін қарапайым болуы тиіс;
- бастапқы конфигурацияның мөлшері контекстік модель саясатын ығыстырмау болу үшін минималды болуы керек.

Алғашқы екі талап белгілі бір дәрежеде барлық қарастырылған модельдерге сәйкес келеді, алайда субъектілерді рөлдер бойынша қайта бөлу жалпы жағдайда қолжетімділік деңгейлерін салыстыруға қарағанда, көпуақытты қажет ететін міндет болып табылуы мүмкін.

Соңғы талап модельдерді таңдау кезінде шешуші болды. Классикалық мандаттық моделі жағдайында тек жүйемен қолдау көрсетілетін қолжетімділік деңгейлері және олардың арасындағы қатынастар туралы білу қажет. Рөлдік модель рөлдердің тағайындалуын, олардың өкілеттіктерін және кейбір жағдайларда жүйенің конфигурациясына маңызды талаптарды қоятынрөлдердің иерархиясын талап етеді.

Мандат үлгілерінен Биба тұтастығының моделі таңдалды. Компрометирленген құрылғылардан қорғауды қамтамасыз ету міндетін шешуге ұсынылатын тәсіл жүйенің ағымдағы жай-күйіндегі қауіпсіздікке әлеуетті әсер ететін операцияларды орындауға жол бермеу мақсатында жеке құрылғыларға шектеулер қойылды. Осыған сүйене отырып, осындай мүмкіндікті іске асыру үшін құрылғылардың бүтіндік деңгейлерін пайдалану мүмкіндігі туралы қорытынды жасау қажет.

Жүйеге кіруді бақылау қолжетімділікті басқару мандаттық үлгісі негізінде орындалады. Ұсынылған модель мандаттық модельді контекст моделіне динамикалық деңгей тағайындау механизмін қосу арқылы контекстік модельге кеңейтетін гибридті болып табылады.

3.1.3. Қолжетімділікті басқару саясатын орнату

Қолжетімділікті бақылау моделінің қолдану ыңғайлығына қолжетімділікті бақылау саясаттарын тапсырудың тәсілі әсер етеді. Ұсынылған саясат моделінде қағидалардың екі тобы түрінде ұсынылады:

– шарттарға сәйкес жүйе параметрлеріне шектеулер;

– субъектілердің объектілерге жол берілетін операциялары.

Субъектілердің объектілерге рұқсат етілген операцияларын сипаттайтын қағидалар мынадай түрге ие:

$$Execute\ (s, o, a),$$

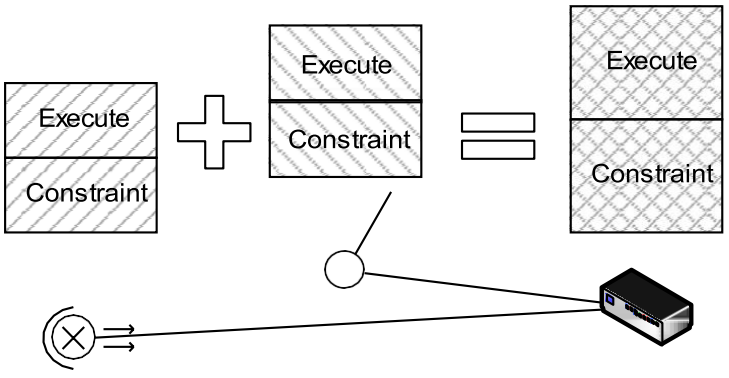
мұндағы *s* - объект, *o* - объект, *a* - операция. *A* операциясы *o* объектісінде орындалуға болатын операциялардың жиынтығына кіреді. Объектіге байланысты басқа ақпаратты алу үшін келесі функциялар анықталған:

Operstions (*o*) = {*o* нысанына рұқсат етілген операциялар};
Description (*o, a*) = {a операциясынан кейін o параметрлерін өзгерту};

Бірінші функция анықтамалық болып табылады және ережелердің дұрыстығын тексеру үшін қызмет етеді. Екінші функция контекстті талдау кезінде ықтимал операциялар кезінде пайда болатын қақтығыстарды анықтау үшін қолданылады.

Ұсынылған модельде қолжетімділікті басқару ережелері жүйеге қосылатын құрылғылармен анықталады деген болжам ұсынылады. Осылайша, қолжетімділікті бақылау жүйесінің конфигурациясын Орнату қажеттілігінен құтылуға болады, бұл «smart home» қауіпсіздігін қамтамасыз ету сияқты қолданбалар үшін маңызды. Бұл құрылғыға жету үшін алдын ала белгіленген кластарға бөлінеді. Осыдан кейін әр құрылғыға құрылғы кластарының тұрғысынан кіру ережелерінің тізімі беріледі.

«Smart home» жүйесіне жаңа құрылғы қосылған кезде қолжетімділікті басқару саясатын жаңарту процесі жүреді. 9 суретте көрсетілгендей, процесс жүйелік құрылғылар ережелерінің тізімдерін біріктіруден тұрады.



10 Сурет – қолжетімділікті бақылау ережелерін қалыптастыру

Параметрлік шектеулер келесі формалардың бірінде орнатылады:

Constraint (*context_condition, param, value_expression*);
Constraint (*context_condition, conditional_expression*).

Бірінші форма *context_condition* шарты орындалғанда *param* параметрін қабылдауға тиіс берілген мәнді көрсетуге мүмкіндік береді. Ереженің осы нысанында жүйенің құрылғыларымен анықталған негізде контексттің жаңа элементтерін анықтауға мүмкіндік береді.

Екінші форма контекст элементтеріне conditional_expression ерікті шектеулерді қою үшін қолданылады. Контекст элементтеріне шектеулер «smart home» жүйесінің қауіпсіз жағдайын сипаттаудың фрагменттері болып табылады .

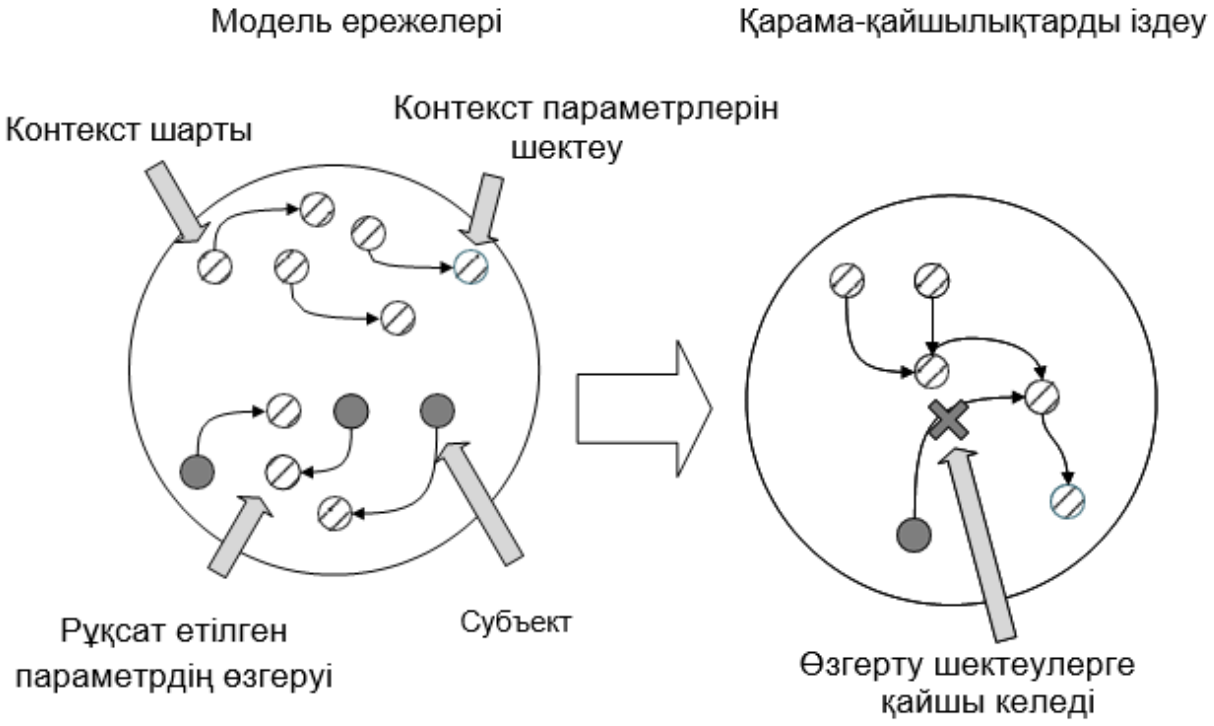
3.2. Жүйені басқару алгоритмдері

Қолжетімділікті басқарудың контекстік моделінің дұрыс жұмыс істеуі үшін тек жинау, сақтау ғана емес, контексті мерзімді жаңарту маңызды. Қауіпсіздік жүйесінің жұмысына көп жағдайда жиналған ақпаратты кейіннен өңдеу және қолжетімділікті бақылау ережелерін жасау алгоритмдері әсер етеді.

3.2.1. Контексті талдау алгоритмі

Бұл алгоритм «smart home» жүйесінде туындайтын қайшылықтарды іздеуге арналған. Кіріс контексті талдау алгоритмі қолжетімділікті басқару саясатын және өзекті контексті алады. Алгоритмнің блок-схемасы 1 қосымшада келтірілген. Бұл бөлімде оның сипаттамасы келтіріледі.

Қолжетімділікті басқарудың әзірленген үлгісінде контексті талдаудың негізгі міндеті «smart home» жүйесінде контекстке қойылған шектеулермен ықтимал операциялар арасындағы қайшылықтарды анықтау болып табылады. Сондықтан контексті талдау алгоритмі қолданыстағы шектеулерге қайшы келетін *Constraint* шектеулерінің тізімін және *Execute (s, o, a)* типті ережелерді анықтау үшін қызмет етеді. Бұл процесс схемалық түрде 10 суретте бейнеленген.



11 Сурет - контексті талдау процесі

Басты ерекшелігі *Constraint* (*condition, parameter, value_expression*) типті ереже контексті жаңа есептейтін параметрлермен толықтыруға мүмкіндік береді. Мұндай мүмкіндік жүйеге енгізілетін жаңа құрылғылардан ережелермен толықтырылуы мүмкін ережелердің күрделі тізбектерін жасауға мүмкіндік береді.

Осы ерекшелікті контексті талдау кезінде ескеру қажет. Алгоритмді сипаттау үшін іске қосылған *Constraint* ережесі ұғымы енгізіледі.

Алгоритм жұмысының басында *Constraint* ережелер тізімі жүргізіледі. Бастапқыда тізім жүйедегі барлық ережелерден тұрады. Іске қосылған *Constraint* (*condition, ...*) ережесі ағымдағы контексте орындалатын *condition* шарты өңдеуге жататын тізімдегі ереже деп аталады. Мұндай ереже тікелей іске қосу кезінде қолданылады. Одан кейінгі әрекеттер ереже түріне байланысты.

Егер бұл ереже *Constraint* (*condition, parameter, value_expression*) түріне ие болса, онда контекстке value_expression есептеу нәтижесінде алынған мәні бар жаңа parameter параметрі қосылады. Егер бұл параметр контексте бар болса, жаңа мән болуы мүмкін мәндер тізіміне қосылады. Сондай-ақ, жаңа мән контекст шектеулер тізіміне қосылады. Осы кезеңдегі қарама-қайшылықтар анықталмайды, өйткені олар тұтастық деңгейлерінің тағайындалуына әсер етпейді.

Егер *Constraint* (*condition, parameter, value_expression*) ереже қолданылса, онда шарт контекст шектеулер тізіміне қосылады.

Ереже іске қосылғаннан кейін ол өңдеуге жататын ережелер тізімінен шығарылады. Сипатталған процесс өңделетін ережелер тізімінде келесі итерацияда іске қосылған ережелер болмайынша қайталанады.

Контекстік шектеулердің құрастырылған тізімін әрі қарай өңдеу осы шектеулерді бұзатын Execute ережелерін анықтаудан тұрады. Ол үшін жүйеде қолданылатын әрбір Execute (*s, o, a*) ережесі үшін сипаттама (*o, a*) функциясының көмегімен өзгертілген параметрлер тексеріледі. Барлық ережелер , оларды орындау контекстке байланысты шарттарды бұзатын қайшылықтар тудыратын ережелер тізіміне қосылады.

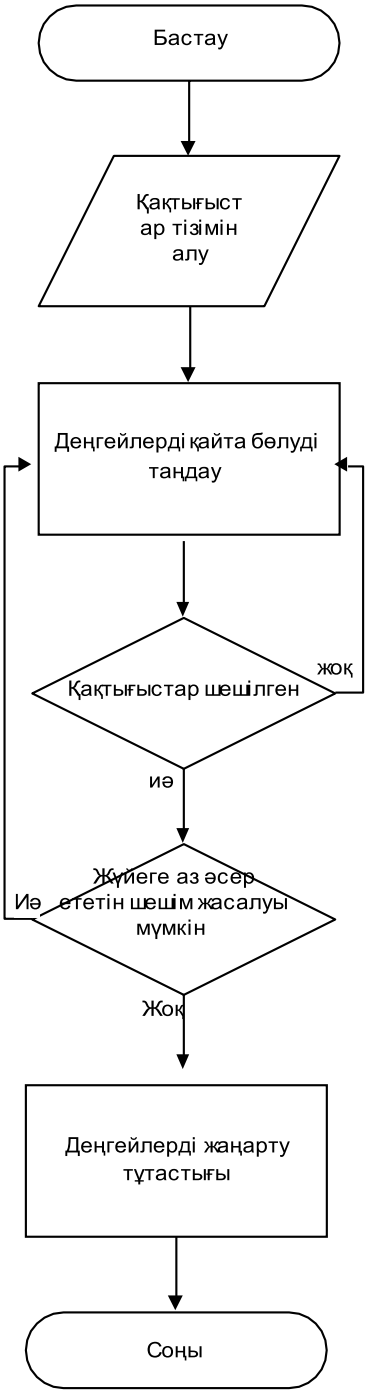
Алгоритмнің нәтижесі - контекст шектеулер мен оларға қайшы келетін қолжетімділік ережелерінің тізімі.

3.2.2. Тұтастық деңгейін белгілеу алгоритмі

Тұтастық деңгейін белгілеу алгоритмін орындау жай-күйді жаңарту кезінде қолжетімділікті басқарудың әзірленген контекстік моделі жұмысының қорытынды кезеңі болып табылады.

Кіріс алгоритм контекстік модель саясатын және контекст шектеулеріне қайшы келетін қолжетімділік ережелерінің тізімін алады. Осы тізімнің негізінде контексті қайшылықтарды жою үшін қолжетімділікке тыйым салатын көптеген құрылғылар анықталады.

Қолжетімділікті басқару ережелерін өзгерту тыйым салынған операциялар саны түрінде жүйеге ең аз ықпал етуге әкелетін, өзгерістің пайдасына таңдалады. Алгоритм 11 суретте келтірілген.



12 сурет – деңгейлерді қайта бөлу алгоритмі

4 Жүйені эксперименттік зерттеу

«Smart home» қауіпсіздігін қамтамасыз етудің әзірленген жүйесінің тиімділігін бағалау үшін оны модельдеу және модельді кейіннен тестілеу жүргізілді.

4.1 «Smart home» жүйесін модельдеу

Әр түрлі класстағы құрылғылардан тұратын «smart home» жүйесі модельденді. Іске асыру үшін Python тілі таңдалған.

Python тез прототиптеу есептерінде өзін жақсы көрсеткен жалпы тіл ретінде таңдалған [13]. Модельдеу үшін таңдалған кітапхана дискретті-событийной симуляциялар SimPy [14]. Кітапхана Python тілінің генераторларының интерфейсін пайдаланады және бірлескен бағдарламаларда агенттерді жүзеге асыру жолымен кооперативтік көп беріктік қолдана отырып, көп агентті жүйелерді симуляциялауға мүмкіндік береді.

«Smart home» жүйесінің сипаттамасы JSON-файлда сақталады, онда жүйенің құрамына кіретін құрылғылар, олардың параметрлері және *Description* (*o, a*) функциясының мәнін көрсете отырып, оларға рұқсат етілген Operations (*o*) операциялары көрсетіледі. Модельдеуші жүйенің құрамы 12 суретте көрсетілген .

13 Сурет – «Smart home» моделдейтін жүйесінің құрамы

Бағдарламалық жасақтамада желілік қабат ескерілмейді, тек қолжетімділікті басқару шлюзі модельдеуге жауап береді, ол контекстіөңдеуге және сақтауға және қатынасты басқаруға жауап береді. SimPy кітапханасының көмегімен сценарий көшіріледі, ол құрылғылар арасында бірнеше сұраныстарды жіберуден тұрады.

4.2 Сценарийлерді модельдеу

Негізгі қорғаныс мүмкіндіктерін көрсететін сценарийді қарастырайық.

Смартфонды пайдаланып есік құлпы ашылуы мүмкін. Тәртіп бұзушының мүмкіндіктерін шектеу үшін уақыт бойынша шарттарды сақтай отырып, қозғалыс пен жарықтандырудың болмауы кезінде есік құлпының бүтіндігінің деңгейін арттыруды ұйғаратын ереже жасалды. Бұл жағдайда смартфонды пайдаланып құлыпты тек адам ғана ашуы мүмкін.

Сценарийді модельдеу барысында контекстік үлгінің келесі ережелері қолданылады:

```
Constraint(жарық == true, адам_үй_ішінде, true) Constraint
(қозғалыс == true, адам_үй_ішінде, true) Constraint
(адам_үй_ішінде == false and (01:00 <= уақыт
<= 07:00), есік_жабық == true)
Execute(смартфон, есік, ашу) Execute
(смартфон, жарықтандыру, қосу)
Execute(есік, есік, ашу)
Description (есік, ашу) -> {есік _ жабық: false}
```

Осы ережелердің негізінде қабылданған шешім келесідей болады.

1. Жарық өшірілген және қозғалыс жоқ болғандықтан, контексте бөлмеде адамның жоқ екенін куәландыратын параметр сақталады.

2. Үй-жайда адамның уақыты мен болмауы бойынша есіктің жай-күйіне шектеу қойылады. Ағымдағы контексте есік жабық болуы тиіс.

3. Есіктің ашылу әрекеті контексті жарамсыз түрде өзгертетіндіктен, контексті бұзады. Нәтижесінде смартфоннан есік ашу мүмкіндігін тудыратын қақтығысты шешу қажет.

4. Қақтығыс смартфонның бүтіндік деңгейін төмендетумен немесе есік құлыптарының бүтіндік деңгейін арттырумен шешілуі мүмкін. Смартфон деңгейінің төмендеуі қақтығыс тудырмайтын басқа әрекеттерді орындауға тыйым салғандықтан, құлыптың бүтіндігін арттыру үшін шешім қабылданады.

Тағы бір сценарий «smart home» климатты бақылау жүйесіне әсер етеді. Үй-жайда адамдар болмаған кезде компьютердің суыту режимінде жылыту мен кондиционерді бір мезгілде қосу жағдайы басқару қатесі ретінде түсіндіріледі. Компьютер тұтастығының деңгейі одан әрі әсерді азайту мақсатында төмендейді . Келесі ережелер іске қосылған:

```
Constraint(жарық == true, адам_үй_ішінде, true)
Constraint(қозғалыс == true, адам_үй_ішінде, true)
Constraint(жылыту == true and адам_үй_ішінде == false,
кондиционер == false)
Execute(компьютер, жылыту, қосу)
Execute(компьютер, кондиционер, қосу) Description
(жылыту, қосу) -> {жылыту == true}
Description(кондиционер, қосу) -> {кондиционер == true}
```

Бұл жағдайда шешім келесідей қабылданады.

1. Бұл жағдайда жарықтандыру өшіріліп, ешқандай қозғалыс болмайды, сондықтан бөлмеде адамның болмауын көрсететін параметр сақталады.

2. Жылыту күйіне және бөлмеде адамның болмауына байланысты кондиционердің жағдайына шектеулер көрсетіледі.

3. Есіктің кондиционерін қосу әрекеті контексті бұзады. Бұл жағдайда шешім компьютердің тұтастығын төмендетудің пайдасына шешіледі.

4.3 Нәтижелері

Қауіпсіздікті қамтамасыз ету жүйесінің әзірленген бағдарламалық макеті «smart home» құрылғылар мен бағдарламалық іркілістерді компрометациялаудың модельденген сценарийлерінде оның жұмысқа қабілеттілігін көрсетеді.

Қауіпсіздікті қамтамасыз етудің енгізілетін механизмдерінің қолжетімділікті басқару жүйесінің өнімділігіне әсер етуі, модельдеуді пайдалану қиынға соғады. Алайда, қолжетімділікті бақылау шлюзінің ұсынылған архитектурасы өнімділік қажеттілігін ескере отырып әзірленген. Құрылғылар арасындағы сұрау салулар контексті талдаудың толық рәсімін тудырмайды, оларға тек қолжетімділікті бақылау ережелері ғана қолданылады. Қолжетімділікті басқару шлюзіндегі мәтінмәндік талдау бөлек орындалады және қолжетімділікті басқару ережелерін жаңарту кезінде сұраныстарды өңдеуге әсер етеді.

ҚОРЫТЫНДЫ

«Smart home» жүйесіндегі ішкі бұзушыдан туындайтын қауіп-қатерлер алдын алу күрделілігіне байланысты маңызды мәселе болып табылады. Қолжетімділікті басқарудың контекстік моделін пайдалану осы міндетті шешудің перспективалық тәсілі болып табылады. Контексті қолдану «smarthome » жүйелерінде толық көлемде іске қосылуы қолжетімділікті басқару бойынша жаңа мүмкіндіктер береді, себебі «smart home» жүйелерінің қасиеттеріне айтарлықтай дәрежеде сәйкес келеді.

Әзірленген «smart home» қауіпсіздік жүйесі жүйені баптау және пайдалану процесін жеңілдету үшін бірқатар механизмдерді ұсынады. Мысалы, контекстік модель саясаты қосылатын құрылғылар беретін ережелер негізінде жасалады. Бұл әрбір бірегей орнатылған «smart home» жүйесінің құрамындағы айырмашылық салдарынан пайда болатын конфигурациялау проблемасын шешуге мүмкіндік береді. . Сондай-ақ, қолжетімділікті басқару ережелерін қолдану үшін мандаттық модель таңдалды, бұл ең алдымен қарапайымдылығы мен конфигурацияланатын параметрлердің аздығына байланысты.

Қауіпсіздікті қамтамасыз ету «smart home» жүйесінің әзірленген бағдарламалық макеті оның жұмысқа қабілеттілігін көрсетті. Құрылғы мен бағдарламалық іркілістерді компрометациялаудың бірқатар сценарийлері кодталды, онда жүйе осындай қауіптерден қорғау қабілетін көрсетті.

Жүргізілген жұмыстар нәтижесінде әрі қарай жүргізілетін зерттеулердің бағыттары анықталды. Бағыттардың бірі - қолжетімділік деңгейлерін тағайындау туралы шешім қабылдау үшін жасанды интеллект әдістерін қолдану болып табылады. Бұл қолжетімділік басқарудың күрделі сценарийлерін іске асыруға мүмкіндік береді.

Зерттеу нәтижелерін практикалық тексеруге арналған аппараттық-бағдарламалық жасақтаманы әзірлеу тағы бір бағыт болып табылады, себебі осы жұмыс барысында жүйенің жұмысын бағалау мүмкін болмады.

ПАЙДАЛАНЫЛҒАН ӘДЕБИЕТТЕР ТІЗІМІ

1.Княгинин В. Н. «Умные» среды, «умные» системы, «умные» производства: Промышленный и технологический форсайт Российской Федерации на долгосрочную перспективу. – CSR North-West, 2013.

2.Smirnov A. et al. Context-based access control model for smart space // Cyber Conflict (CyCon), 2013 5th International Conference on. – IEEE, 2013. – С. 1-15.

3.Collotta M., Pau G. A Solution Based on Bluetooth Low Energy for Smart Home Energy Management //Energies. – 2015. – Т. 8. – №. 10. – С. 11916- 11938.

4.Cheng J., Kunz T. A survey on smart home networking //Carleton University, Systems and Computer Engineering, Technical Report, SCE-09-10. – 2009.

5.Fouladi B., Ghanoun S. Security Evaluation of the Z-Wave Wireless Protocol //Black hat USA. – 2013.

6.RTLS | Технологии | Сетевая инфраструктура системы РТЛС // RTSL URL: http://www.rtlsnet.ru/technology/view/3.

7.Dalrymple S. D. Comparison of ZigBee Replay Attacks Using a Universal Software Radio Peripheral and USB Radio. – AIR FORCE INSTITUTE OF TECHNOLOGY WRIGHT-PATTERSON AFB OH GRADUATE SCHOOL OF ENGINEERING AND MANAGEMENT, 2014. – №. AFIT-ENG-14-M-23.

8.Home Automation and Cybercrime // TrendMicro URL: http://apac.trendmicro.com/cloud-content/apac/pdfs/security-intelligence/white-papers/wp-home-automation-and-cybercrime.pdf.

9.Снегуров А. В., Ткаченко Е. А., Кравченко А. Д. Риски информационной безопасности систем, построенных по технологии" Умный дом" //Восточно-Европейский журнал передовых технологий. – 2011. – Т. 4. –№. 3 (52).

10.Ferraiolo D. F., Kuhn D. R. Role-based access controls //arXiv preprint arXiv:0903.2171. – 2009.

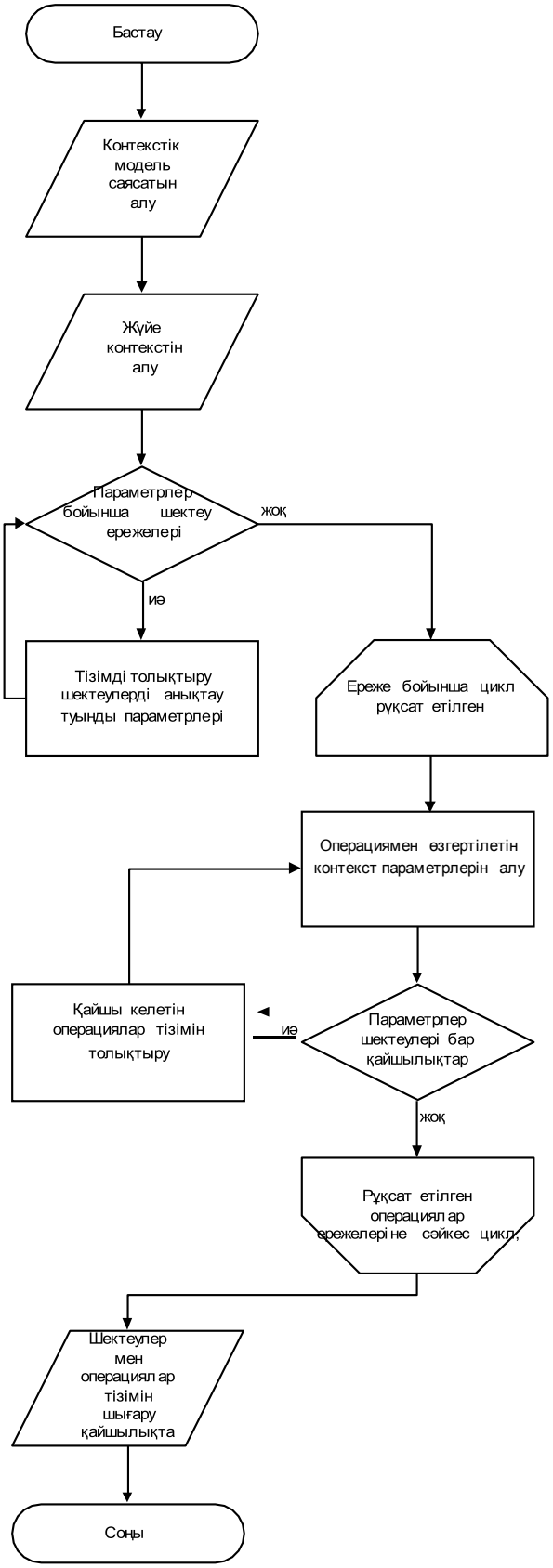
11.Зегжда Д. П., Ивашко А. М. Основы безопасности информационных систем. – М.: Горячая линия-Телеком, 2000.

12.Architecture — SmartThings Documentation 1.0 documentation // SmartThings Documentation URL: http://docs.smartthings.com/en/latest/architecture/index.html.

13.Quotes about Python | Python.org // Python.org URL: https://www.python.org/about/quotes/ .

14.Overview — SimPy 3.0.8 documentation // Read the Docs URL: https://simpy.readthedocs.org.

А ҚОСЫМШАСЫ
КОНТЕКСТІ ТАЛДАУ АЛГОРИТМІНІҢ БЛОК-СХЕМАСЫ



1 Сурет – контексті талдау алгоритмінің блок-схемасы