ҚАЗАҚСТАН РЕСПУБЛИКАСЫ ҒЫЛЫМ ЖӘНЕ ЖОҒАРЫ БІЛІМ МИНИСТРЛІГІ

«Л.Н. ГУМИЛЕВ АТЫНДАҒЫ ЕУРАЗИЯ ҰЛТТЫҚ УНИВЕРСИТЕТІ» КЕАҚ

Студенттер мен жас ғалымдардың
«ǴYLYM JÁNE BILIM - 2023»
XVIII Халықаралық ғылыми конференциясының
БАЯНДАМАЛАР ЖИНАҒЫ

СБОРНИК МАТЕРИАЛОВ
XVIII Международной научной конференции
студентов и молодых ученых
«ǴYLYM JÁNE BILIM - 2023»

PROCEEDINGS
of the XVIII International Scientific Conference
for students and young scholars
«ǴYLYM JÁNE BILIM - 2023»

2023
Астана

УДК 001+37
ББК 72+74
G99

«ǴYLYM JÁNE BILIM – 2023» студенттер мен жас ғалымдардың XVIII Халықаралық ғылыми конференциясы = XVIII Международная научная конференция студентов и молодых ученых «ǴYLYM JÁNE BILIM – 2023» = The XVIII International Scientific Conference for students and young scholars «ǴYLYM JÁNE BILIM – 2023». – Астана: – 6865 б. - қазақша, орысша, ағылшынша.

ISBN 978-601-337-871-8

Жинаққа студенттердің, магистранттардың, докоранттардың және жас ғалымдардың жаратылыстану-техникалық және гуманитарлық ғылымдардың өзекті мәселелері бойынша баяндамалары енгізілген.

The proceedings are the papers of students, undergraduates, doctoral students and young researchers on topical issues of natural and technical sciences and humanities.

В сборник вошли доклады студентов, магистрантов, докторантов и молодых ученых по актуальным вопросам естественно-технических и гуманитарных наук.

УДК 001+37
ББК 72+74

ISBN 978-601-337-871-8

УДК 004.056.5

«SMART HOUSE» ЖҮЙЕСІНДЕГІ АҚПАРАТТЫҚ ҚАУІПСІЗДІК

Дүйсенова Раушангүл Нұрболатқызы
Duisenova2809@mail.ru
Л.Н.Гумилев атындағы ЕҰУ, «Ақпараттық технологиялар»
факультетінің 4-курс студенті, Астана, Қазақстан
Ғылыми жетекшісі – «Ақпараттық қауіпсіздік» кафедрасының аға оқытушысы Г.И.Аймичева

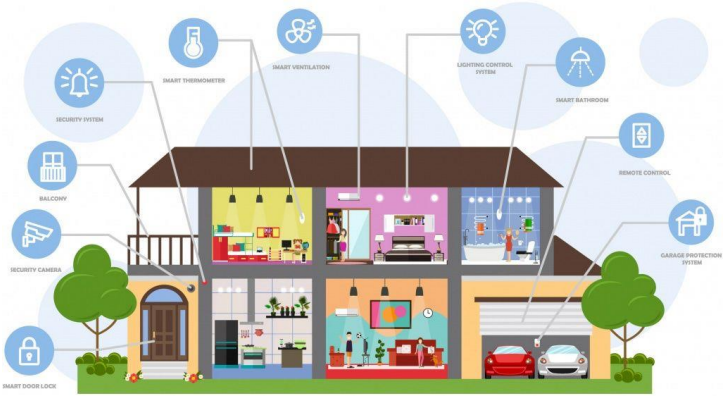
Аннотация

Заманауи технологиялардың үздіксіз дамуы тасымалданатын ақпараттың ұлғаюына әкелсе, екінші жағынан жүйеге жаңа қауіп-қатерлерге жол ашады. Мақалада «Smart house» жүйесінің негізгі функциялары қарастырылып, жүйеге туындайтын қауіпсіздік қатерлерінің мысалдары келтірілген. Жүйенің дүниежүзілік және Қазақстан бойынша статистикаларына зерттеу жасалды. Қауіпті алдын алу мақсатында бірнеше қорғау тәсілдері талданды.

Қазіргі уақытта адамзат үйлердегі жайлылықты арттыруға ұмтылуда: заманауи пәтерде әртүрлі тұрмыстық техника мен аудио-бейне кешенінен басқа, ауаны кондиционерлеу, жылыту, жарықтандыру және қауіпсіздік жүйелері бар. «Smart house» жүйелері соңғы онжылдықтарда өте танымал болды, өйткені олар жайлылық пен өмір сапасын арттырады. Жүйенің көпшілігі смартфондар мен микроконтроллерлер арқылы басқарылады. Смартфон қолданбасы сымсыз байланыс әдістерін пайдаланып үй функцияларын басқару және бақылау үшін пайдаланылады.

Кез-келген үйді автоматтаныру мақсатында пайдаланылатын «Smart house» жүйесі көпфункциялы (1-сурет). Мұндай жүйелер келесі тұрмыстық процестерді автоматты түрде басқара алады:

- жылыту, желдету;
- жарықтандыру;
- электр энергиясы;
- су;
- газ;
- бейнебақылау камерасы;
- қауіпсіздік және өрт қауіпсіздігі;
- аудио-бейне жабдықтарды пайдалану;
- мобильді қосымшаның көмегімен жүйенің жұмысын бақылау;
- перделерді, терезелерді ашу және жабу;
- өсімдіктерді суару, жануарларды азықтандыру.



1-сурет. «Smart house» жүйесінің функциялары [1]

Қазіргі уақытта барлық ел «Smart house» жүйенің әртүрлі түрін ұсынып жатыр. Мүмкіншіліктерін ескере отырып Vencon компаниясының мамандары дүниежүзі бойынша 2023 жылдың ең үздік 5 жүйесін анықтады [2] (1-кесте).

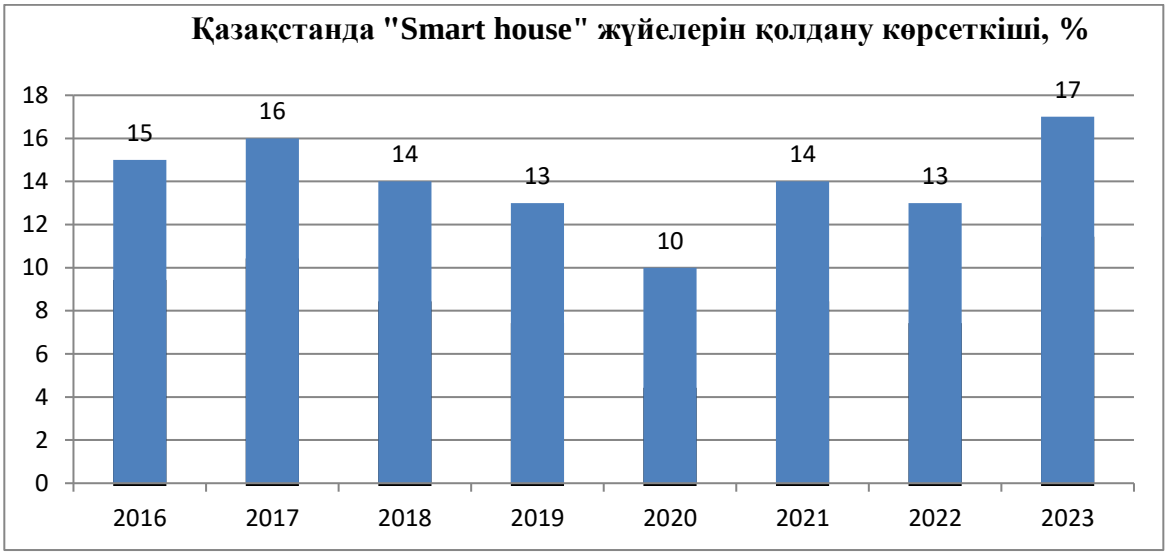
1-кесте. Vencon компаниясының анықтамасы бойынша 2023 жылғы ең жақсы 5 «Smart house» жүйесі

№	Жүйе	Өндіруші ел	Артықшылығы	Кемшілігі
1	Ajax	Украина	• Кең сигналды қамту аймағы (2000 м дейін); • аккумулятордан хабтың автономды жұмысы (16 сағатқа дейін); • Wi-Fi және GSM-байланыс; • кернеу төмендеген кезде автоматты түрде өшеді; • 100 құрылғыға дейін қосу; • қашықтан басқару пультінде (брелокта) дабыл түймесінің болуы; • жинақтың төмен құны (200 доллардан бастап).	• Орталық контроллердің (Hub) жұмысымен ғана жұмыс істеу, яғни сенсорлардың автономиясының болмауы; • жеке бейнебақылау камерасы жоқ; • тек телефон арқылы басқару, бұл компьютерге кез келген қосымша бағдарламаларды орнату қажеттілігін болдырмайды.
2	Broad Link	Қытай	• Әртүрлі құрылғыларды оңай қосуға және жоюға болады; • жылдам орнату, қосу, конфигурациялау; • сенсорлардың кең ауқымы бар; • жеке бақылау камерасы бар; әлемнің кез келген жерінен интернет арқылы Wi-Fi арқылы басқарылады; • жабдықтың бағасының қолайлылығы (200 доллардан).	• Қысқа сигнал диапазоны (50 м дейін); • хаб үшін резервтік қуаттың болмауы; • қашықтан басқару құралы тек сигналдарды қабылдау үшін жұмыс істейді.
3	Fibaro	АҚШ	• Бірден бірнеше телефонға хабарлама жіберу; • ағып кету сенсорының сиренамен жабдықталуы; • смарт розетка қосылған құрылғылардың қуат тұтыну деңгейін көрсетеді; • Google қызметі арқылы дауыспен басқару.	• Жабдықтың жоғары құны (600 доллардан); • тек кәсіби орнату және конфигурациялау; • Fibaro Home Center орталық контроллерін LAN кабелі арқылы Интернетке міндетті түрде қосу.
4	Orvibo	Қытай	• Құрылғылардың кең ауқымы және жүйені масштабтау мүмкіндігі (шамамен 100 сенсор) және басқа өндірушілер; • 10 нөмірге дейін қоңырау шалу; • өте қолжетімді баға (150 доллардан бастап).	• Сигналдың шағын қамту аймағы (30 м дейін); • негізгі конфигурациядағы қарапайым құрылғылар жиынтығы; • сымды интернет қосылымы.
5	Xiaomi	Қытай	• Құрылғылардың толық автономиясы; • Wi-Fi арқылы смартфон арқылы ыңғайлы басқару; • реттелетін сценарийлердің болуы;	• Сигналдың өте аз қамту аймағы (10 м дейін); • негізгі жинақтағы әртүрлі датчиктер өздерінің орналасуын қажет етуі;

			• ықшам және стильді дизайн; • негізгі жинақтың төмен құны (бар болғаны 90 доллар).	• хаб үшін резервтік қуаттың болмауы.

Бұл көрсеткіштер көптеген жүйелердің ортақ кемшілігі бар екенін көрсетті. Соның ішінде жүйеде хаб үшін резервтік қуаттың болмауы, орталық контроллердің жұмысымен ғана жұмыс істеу, яғни сенсорлардың автономиясының болмауы жүйелерді жиі кездесті.

Әлемде бірнеше жүздеген автоматтандыру жүйелері немесе «Smart house» өндірушілер бар. Бірақ «Smart house» Қазақстанда сататын және орнататын компаниялар казіргі уақытта тек ондаған. Соның ішінде Connected Home, MimiSmart, Teletask, Domintell компанияларының өнімдері Қазақстан бойынша Астана, Алматы, Атырау қалаларында қарқынды пайдаланып келеді (сурет-2).



Сурет-2. 2016-2023 жж аралығындағы J'son &Partners Consulting компаниясының зерттеуі бойынша Қазақстанда "Smart house" жүйелерін қолдану көрсеткіші [3]

1-кестеде көрстілгендей, технология жаңа мүмкіндіктер туғызады, бірақ ол жаңа қауіптер де әкелуі мүмкін. Мысалы, «Smart house» адам өмірінің қауіпсіздігін арттыруға, жүктемені азайтуға, коммуналдық шаруашылықтарды энергия үнемдеумен қамтамасыз етуге мүмкіндік береді. Сонымен қатар, IoT таралуы экономиканың көптеген салаларында тұрақсыздықты күшейтуі мүмкін: жаңа технологиялардың көпшілігі уақытша толқулар мен ойланбаған инвестицияларды тудырады. Сонымен қатар, хакерлер смарт үйлердің таралуын тиімді пайдалануға тырысқандықтан, киберқауіпсіздікке қатысты жаңа қиындықтар туындайды. Бұрынғыдан да көп кибершабуыл болады. Қоғамның смарт жүйелерді пайдалану қажеттілігі мен дайындығы арасында қайшылықтар дамыды, бірақ сонымен бірге мұндай жүйелерге кибершабуылдар салдарынан қауіпсіздік тәуекелдері артып келеді. Соның ішінде жүйеге туындайтын ең маңызды бірнеше қауіп анықталды (2-кесте).

2-кесте «Smart house» жүйесінде туындайтын қауіптер және қорғау әдістері [4]

№	Қауіп түрі	Жүйеге әсері	Қорғау тәсілі
1	Эксплойт	Осалдықты пайдалануға арналған код арқылы жүйеге қол жеткізеді. Әсер ететін активтерге байланысты маңызды қауіп арта бастайды.	Microsoft Windows жүйесінің заманауи шығарылымдары: Windows 7, 8 және 8.1-де пайдаланушыны эксплойттардың деструктивті әрекеттерінен қорғауға көмектесетін кіріктірілген механизмдер бар.

			DEP және ASLR механизмдері орындалмайтын жадты пайдалануға шектеулер қою және бағдарламаларды ерікті мекенжайларда жадқа орналастыру арқылы бағдарламалық жасақтама мен операциялық жүйелердегі белгілі бір осалдықты пайдалану мүмкіндігін айтарлықтай қиындатады. Windows 7+ жүйесінде DEP және ASLR мүмкіндігінше пайдаланылады.
2	Интернет заттарының веб-интерфейстері	Sql инъекциясы және сайттар арасындағы скриптингті туғызады.	Көптеген SQL бұзылулары жолдарда «қауіпті» тырнақшалар, апострофтар және басқа арнайы таңбалар болғандықтан орын алады. Ол үшін әрбір арнайы таңбаның алдында қосылған кері қиғаш сызықпен (\) $str жолын қайтаратын addslashes($str); функциясын пайдалану керек. Бұл тәсіл скрининг деп аталады.
3	IoT құрылғысының бұлттық қосылымы	Шабуыл жасаушылардың бұлт архитектурасын бұзу арқылы деректерді талдау мүмкіндігі бар. Егер шабуылдаушы бұлтты бұзатын болса, бір зиянды бағдарламаны бірнеше IoT құрылғыларына бір уақытта жүктеуге болады.	Екі тарапты қорғау үшін пайдаланушы мен қызметті тексеруді қамтамасыз ету үшін арнайы қауіпсіздік протоколдары пайдаланылады.Мысалы, AWS (Amazon) және Azure (Microsoft) қызметтері құрылғы мен бұлттық қызметтердің толық жиынтығы арасындағы өзара әрекеттесу үшін кіру порталын қамтамасыз етеді. Ұқсас портал бұлт пен кәсіпорын арасында қолданылады. Ол сәйкес әзірлеу пакеттерімен жүзеге асырылған аутентификация протоколдарын пайдаланады. Мысалы, AWS Device Gateway пайдаланады
4	IoT құрылғысының бағдарламалық құралын жаңарту	Бұлт қауіпсіздікке қауіп төндіретіндіктен, IoT құрылғыларына арналған бағдарламалық жасақтаманы жаңарту маңызды болып саналады.	Құрылғыны жаңартумен байланысты қауіпсіздік ресурстарының құрылғыда дұрыс қорғалғанын қамтамасыз ету маңызды. Түбірлік кілттер сияқты ресурстар өзгертуден қорғалуы керек. Мұны әртүрлі жолдармен жасауға болады, мысалы, қауіпсіздік құралдарын (TPM, SGX, HSM, т.б.) пайдалану немесе тіпті анықтамалық енгізуідегідей Құрылғыны жаңарту агентінде кодтау. Соңғы жағдайда агент кодының зиянды модификациясынан қорғау үшін құрылғыны жаңарту агентінің коды сандық қолтаңбамен және жүйе кодының тұтастығы қосылған болуы керек.
5	DDoS-шабуыл	DDoS шабуылы кезінде бірнеше жүйе бір нысанаға шабуыл	Жоғары ағындық қосылымның кіру интерфейсінде "ip бір бағыттағы кері жолды тексеру" пәрменін қосу керек. Бұл мүмкіндік DDoS қорғауындағы үлкен

		жасап, оны жүктеп, апатқа ұшыраиады. Көптеген байланыстар жасау арқылы, арнаны толтырып тастайды	қиындық болып табылатын жалған пакеттерді жібермес бұрын жояды. Сонымен қатар, резервтелген ауқымдардағы бастапқы мекенжайлары бар кіріс трафикті блоктауды ұмытпаңыз (яғни, 192.168.0.0). Бұл сүзгі көздері дұрыс емес пакеттерді жояды.Кіріс және шығыс сүзгілеу әдістері DDoS шабуылдарының алдын алу үшін де маңызды. Бұл қарапайым ACLs, егер барлық Интернет провайдерлері мен үлкен желілермен жүзеге асырылса, жалған пакеттерді жалпыға қолжетімді

Жоғарыда көрсетілген қауіптерді алдын алу мақсатында бірнеше әдістер талданды. Соның бірі жүйеге тым көп құрылғылар желіден қуат алса, иесі желіні шамадан тыс жүктемеу үшін құрылғылардың бірін өшіру қажет екендігі туралы хабарлама беру. Оны таратқыштар мен команда әзірлеген хаттаманың көмегімен қашықтан басқаруға болады. Ол сондай-ақ заңсыз кіруден қорғалған, оны тек иесі ғана қашықтықта қосып, өшіре алады. Оның қатысуымен оған қосылған құрылғылар тұтынатын электр энергиясын өлшеуге болады. Бұл әдісті С.Зимненко, Д.Невмержицкий және А.Силаевтан тұратын ITMO университетінің ақпараттық қауіпсіздік технологиялар департаментінің командасы ойлап тапты. Смарт розетка әдісін 1-кестеде көрстілгендей АҚШ-тың Fibaro жүйеінде қолданғанын көруге болады.

Сонымен қатар, екінші әдіс аутентификация [5] арқылы желіге кіру. Ол серверде https протоколы арқылы жүзеге асырылады, ол ашық арналар арқылы жіберілген кезде пайдаланушы деректерін қорғайды. Сондай-ақ сервер контроллерден деректерді сұрайды және оны пайдаланушыға береді, бұл контроллерден жүктеменің бір бөлігін алып тастауға мүмкіндік береді. Бұл әдіс Ajax, Orvibo жүйелерінде қолданылған.

Қорытынды.

Тұрғын үйдің жайлылығы мен қауіпсіздігін қамтамасыз ететін көп функционалды «Smart house» жүйелері жылдан жылға танымал болып келеді. Заманауи нарық үйді автоматтандыруға арналған техникалық құрылғылардың үлкен таңдауын ұсынады, сондықтан әртүрлі өндірушілердің «Smart house» жүйелерін салыстыру көптеген адамдар үшін пайдалы. Бұл мақалада IoT қауіпсіздік мәселелерінің талданды. IoT технологиясының құрамдас бөліктері анықталып, оны қолдану салалары қарастырылды.

Пайдаланылған әдебиеттер

1. https://wifi.kz/articles/umnyy-dom-na-kazakhskom-rynke/
2. https://vencon.ua/articles/reyting-sistem-umnyy-dom-po-proizvoditelyam
3. https://www.tadviser.ru/index.php/Статья:Интернет_вещей,_IoT,_M2M_%28рынок_Казахстана%29
4. Trabelsi Z. Iot based smart home security education using a hands-on approach //2021 IEEE Global Engineering Education Conference (EDUCON). – IEEE, 2021. – С. 294-301.
5. Советов Б. Я., Татарникова Т. М. Управление безопасностью системы умного дома //Информационные технологии в управлении. материалы конференции. Санкт-Петербург. – 2020. – С. 262.

УДК 004.85

РАСЧЕТ И ПРОГНОЗИРОВАНИЕ СТОИМОСТИ ЖИЛЬЯ НА ОСНОВЕ ТЕХНОЛОГИИ НЕЙРОСЕТЕЙ

Ерболов Аруан Каирбекович, Павлович Юрий Андреевич