https://doi.org/10.51885/3134-8025_JICS_2026_2_2
ХҒТАР 81.93.29

АҚЫЛДЫ ҮЙ ҚАУІПСІЗДІГІ: ИНТЕРНЕТ ЗАТТАРЫ ЖҮЙЕЛЕРІНДЕГІ ЕНУГЕ ТЕСТІЛЕУГЕ АРНАЛҒАН ҚҰРАЛДАР, ХАТТАМАЛАР ЖӘНЕ ЗЕРТХАНАЛЫҚ ТАПСЫРМАЛАР

БЕЗОПАСНОСТЬ УМНОГО ДОМА: ИНСТРУМЕНТЫ, ПРОТОКОЛЫ И ЛАБОРАТОРНЫЕ ЗАДАЧИ ДЛЯ ПРОНИКНОВЕНИЯ ИНТЕРНЕТА ВЕЩЕЙ

SMART HOME SECURITY: TOOLS, PROTOCOLS, AND LABORATORY TASKS FOR IOT PENETRATION

Т.А. Айдынов [1], **С.Т. Тлеубердин** [1*], **Ж.А. Боранбай** [1], **Ф.Б. Тебуева** [2], **А.К. Шайханова** [1], **Д.Ж. Сатыбалдина** [1]
[1]Л.Н. Гумилев атындағы Еуразия ұлттық университеті, Астана қ., Қазақстан
[2]Солтүстік Кавказ федералды университеті, Ставрополь, Ресей
*Жауапты автор: Тлеубердин Сакен, e-mail: sakentleuberdin@gmail.com

Түйінді сөздер:
ақылды үй, ZigBee, кедергі шабуылы, киберқауіпсіздік, заттар интернеті, бағдарламалық жасақтамамен анықталған радио, оқу стенді, зертханалық кешен.

ТҮЙІНДЕМЕ
Мақала Zigbee сымсыз арналарының кедергі шабуылдарын зерттеуге арналған Ақылды үй зертханалық стендін әзірлеуге арналған, олардың өзектілігі IoT құрылғыларының көбеюіне және олардың физикалық деңгейдегі әсерлерге осалдығына байланысты. Жұмыстың мақсаты – радиожиілік кедергілерін модельдеуді және олардың желінің жұмысына әсерін талдауды қамтамасыз ететін аппараттық-бағдарламалық кешен құру. Әдістер ретінде эксперименттік модельдеу, бағдарламалық-анықталатын радионы қолдана отырып, радиожиілік спектрін талдау және желілік параметрлерді бақылау қолданылды. Эксперименттер барысында кедергілерді іске асыру кезінде құрылғылардың қолжетімділігі 0-20 % дейін төмендейтіні, пакеттердің жоғалуы 90-100 %-ға дейін өсетіні және жүйенің қызмет көрсетудің істен шығу жағдайына көшетіні анықталды. Ғылыми жаңалық физикалық деңгейдегі шабуылдарды бақыланатын зерттеу үшін нақты әлемдегі ақылды үй құрылғылары мен мамандандырылған бағдарламалық жасақтаманы бірыңғай білім беру кешеніне біріктіруден тұрады. Жұмыстың практикалық маңыздылығы заттар интернетінің киберқауіпсіздігі саласындағы мамандарды даярлау кезінде стендті пайдалану мүмкіндігі.

Ключевые слова:
умный дом, ZigBee, атака глушения, кибербезопасность, интернет вещей, программно-определяемое радио,

АННОТАЦИЯ
Статья посвящена разработке учебного лабораторного стенда умного дома для исследования атак глушения беспроводных каналов ZigBee, актуальность которых обусловлена ростом числа устройств Интернета вещей и их уязвимостью к воздействиям на физическом уровне. Цель работы заключается в создании аппаратно-программного комплекса, обеспечивающего моделирова-

учебный стенд,
лабораторный комплекс.

ние радиочастотных помех и анализ их влияния на функционирование сети. В качестве методов использованы экспериментальное моделирование, анализ радиочастотного спектра с применением программно-определяемого радио и мониторинг сетевых параметров. В ходе экспериментов установлено, что при реализации помех происходит снижение доступности устройств до 0–20 %, рост потерь пакетов до 90–100 % и переход системы в состояние отказа обслуживания. Научная новизна состоит в интеграции реальных устройств умного дома и специализированного программного обеспечения в единый образовательный комплекс для контролируемого изучения атак физического уровня. Практическая значимость работы заключается в возможности использования стенда при подготовке специалистов в области кибербезопасности Интернета вещей.

keywords:
smart home, ZigBee, jamming attack, cybersecurity, Internet of things, software-defined radio, training stand, laboratory complex.

ABSTRACT
The article is devoted to the development of a smart home educational laboratory stand for investigating ZigBee wireless jamming attacks, the relevance of which is due to the growing number of Internet of Things devices and their vulnerability to impacts at the physical level. The purpose of the work is to create a hardware and software package that provides simulation of radio frequency interference and analysis of their impact on the functioning of the network. The methods used are experimental modeling, analysis of the radio frequency spectrum using software-defined radio and monitoring of network parameters. During the experiments, it was found that when interference occurs, device availability decreases to 0-20%, packet loss increases to 90-100%, and the system goes into a maintenance failure state. The scientific novelty consists in the integration of real smart home devices and specialized software into a single educational complex for the controlled study of physical layer attacks. The practical significance of the work lies in the possibility of using the stand in the training of specialists in the field of cybersecurity of the Internet of Things.

КІРІСПЕ

Ақылды үй технологиялары күнделікті өмірге белсенді түрде енгізіліп, жарықтандыруды, климатты, қауіпсіздік жүйелерін және тұрмыстық техниканы басқаруды автоматтандыруды қамтамасыз етеді. Сарапшылардың болжамы бойынша, 2030 жылға қарай әлемде қосылған IoT құрылғыларының саны 30 миллиардтан асады, олардың едәуір бөлігі тұрғын үй-жайларда пайдаланылатын болады (Zohourian et al., 2023). Қосылған құрылғылардың жылдам өсуі ақпараттық қауіпсіздік саласында жаңа қоңыраулар тудырады, өйткені әрбір құрылғы зиянкестер үшін ықтимал кіру нүктесін білдіреді (Vasilescu et al., 2023).

IEEE 802.15.4 стандартына негізделген ZigBee протоколы ақылды үй сымсыз желілерін ұйымдастырудың ең кең таралған шешімдерінің бірі болып табылады. Ол лицензиясыз 2,4 ГГц жиілік диапазонында жұмыс істейді және соңғы құрылғылардың төмен қуат тұтынуын қамтамасыз етеді, бұл оны батареямен жұмыс істейтін сенсорлар үшін тартымды етеді (IEEE, 2020). Сала сарапшыларының пікірінше, 2023 жылға қарай 500 миллионнан астам ZigBee чипсеті сатылды, ал 2025 жылға қарай болжамды сатылым 3,8 миллиард құрылғыны құрайды (Zigbee Alliance, 2021). Алайда, радиоарнаның ашықтығы әртүрлі шабуылдар үшін алғышарттар жасайды, олардың арасында кедергі шабуылы ерекше қауіп төндіреді, өйткені ол желінің криптографиялық кілттерін білуді қажет етпейді (Kumar et al., 2024).

Кедергі шабуылы мақсатты желінің жұмыс жиілігінде радиожиілік кедергілерін тудырады, бұл құрылғылар арасында деректер алмасудың мүмкін .стігіне әкеледі. Ақылды үй контекстінде бұл қауіпсіздік жүйелерінің істен шығуына, атқарушы құрылғыларды бақылауды жоғалтуға және тұрғын үйдің қалыпты жұмысының бұзылуына әкелуі мүмкін. Зерттеулер көрсеткендей, физикалық деңгейдегі шабуылдар сымсыз сенсорлық желілерге үлкен қауіп төндіреді, өйткені оларды жүзеге асыру криптографиялық қорғаныс механизмдерін бұзуды қажет етпейді (Pirayesh et al., 2021).

Киберқауіпсіздік саласындағы заманауи үрдістер мамандарды даярлауға тәжірибеге бағдарланған тәсілдің қажеттілігін көрсетеді. Материалды теориялық зерттеуге негізделген дәстүрлі оқыту әдістері нақты жабдықпен жұмыс істеудің қажетті практикалық дағдыларын қалыптастыруды қамтамасыз етпейді (García-Magariño et al., 2023). IoT Киберқауіпсіздік бойынша білікті мамандарды даярлау тек теориялық білімді ғана емес, сонымен қатар нақты жабдықпен жұмыс істеудің практикалық дағдыларын қажет етеді. Бұл жұмыстың мақсаты бақыланатын білім беру ортасында ZigBee протоколына дыбысты өшіру шабуылдарын зерттеу үшін оқу зертханалық стендін және арнайы бағдарламалық құралды құру болып табылады.

Сымсыз хаттамалардың қауіпсіздігін зерттеу үшін оқу стендтерін әзірлеудің өзектілігі әлемдік тәжірибемен расталады. Атап айтқанда, АҚШ Ұлттық Ғылым қоры интернет заттарының қауіпсіздігі негіздерін үйрету үшін арзан зертханалық кешендер құру жобаларын қаржыландырады (Fu & Zou, 2023). Осындай бастамалар Еуропа мен Азияның жетекші университеттерінде жүзеге асырылуда, бұл осы саладағы мамандарды практикалық даярлаудың маңыздылығын жаһандық мойындауды көрсетеді.

Әдебиеттерге шолу және қолданыстағы шешімдерді талдау

ZigBee протоколының қауіпсіздік мәселелерін халықаралық ғылыми қауымдастық белсенді түрде зерттеп жатыр. Zohourian және т.б. жұмысы OSI моделінің әртүрлі деңгейлеріндегі шабуылдарды талдауды қамтитын Zigbee құрылғыларының осалдығына жан-жақты шолу жасайды (Zohourian et al., 2023). Авторлар кедергі шабуылдарын желінің қол жетімділігі үшін ең маңызды қауіптердің бірі ретінде атап көрсетеді. Kumar, Yadav және Yadav IoT жүйелері контекстінде ZigBee желілерінің қауіпсіздігіне кеңейтілген талдау жүргізіп, радиожиілік шабуылдарынан қорғаудың жаңа әдістерін әзірлеу қажеттілігін атап өтті (Kumar et al., 2024).

Ren және т.б. зерттеуі Zigbee протоколын фаззинг әдісімен жүзеге асырудың қауіпсіздігін талдауға арналған (Ren et al., 2023). Авторлар бастапқы кодқа қол жеткізуді қажет етпестен құрылғылардың бағдарламалық жасақтамасында белгісіз осалдықтарды анықтау мүмкіндігін көрсетеді. Бұл тәсіл студенттердің осалдықтарды іздеу дағдыларын қалыптастыру үшін оқу процесіне біріктірілуі мүмкін.

Сымсыз протоколдардың қауіпсіздігін зерттеу үшін бағдарламалық жасақтамамен анықталған радионы (SDR) қолдану Виллануев пен авторлардың жұмысында қарастырылады (Villanueva-Miranda et al., 2021). Авторлар IOT технологияларына шабуылдарды жүзеге асыру үшін SDR платформаларын пайдаланудың жүйелі шолуын ұсынады, бұл тәсілдің білім беру мақсаттарындағы артықшылықтарын көрсетеді. Bouchendouka, Teguig және Sadoudi USRP платформасы мен GNU radio бағдарламалық жасақтамасын қолдана отырып, IEEE 802.11 протоколына шабуылдардың практикалық орындалуын сипаттайды (Bouchendouka et al., 2022).

IoT киберқауіпсіздігінің білім беру аспектілеріне арналған жұмыстар ерекше қызығушылық тудырады. García-Magariño және т.б. IoT құрылғыларының осалдығын зерттеуге арналған қашықтағы зертхана тұжырымдамасын ұсынады, бұл студенттерге интернет арқылы нақты аппараттық құралдармен тәжірибе жинақтауға мүмкіндік береді (García-Magariño et al., 2023). Fu және Zou өз еңбегінде криптографиялық сопроцессоры бар

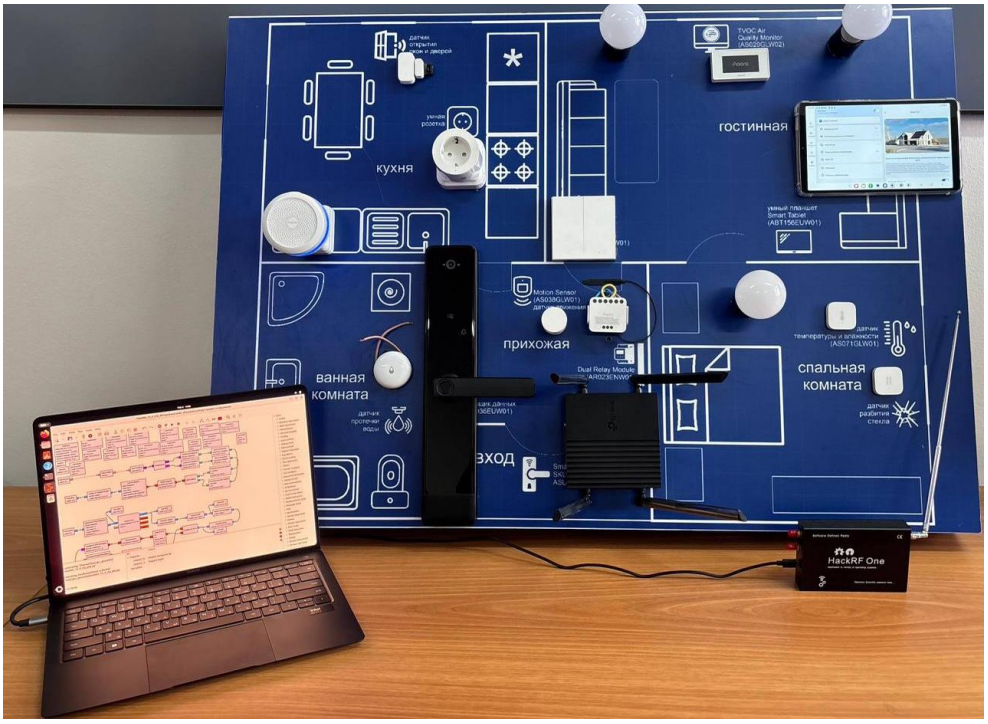
ESP32 микроконтроллеріне негізделген арзан IoT қауіпсіздік оқыту платформасын әзірлеуді сипаттайды (Fu & Zou, 2023).

Қазақстанда IoT киберқауіпсіздік саласындағы зерттеулер дамудың бастапқы кезеңінде тұр. Тлеубердин және Сейтқұлов жергілікті және жаһандық қауіптерді бөліп көрсете отырып, ақылды үй IoT құрылғыларына арналған киберқауіптердің жіктелуін енгізді (Тлеубердин & Сейткулов, 2022). Авторлар осы салада білім беру бағдарламаларын дамыту қажеттілігін атап көрсетеді. Қазақстанның 2023-2029 жылдарға арналған цифрлық трансформациясының тұжырымдамасы киберқауіпсіздікті дамудың басым бағыттарының бірі ретінде айқындайды, бұл білім беру процесіне мамандандырылған оқу стендтерін енгізу үшін қолайлы жағдайлар жасайды (Постановление Правительства Республики Казахстан № 269, 2023).

ЗЕРТТЕУ МАТЕРИАЛДАРЫ МЕН ӘДІСТЕРІ

Ақылды үйді оқыту стенді-Zigbee сымсыз желісі бар смарт үйдің типтік инфрақұрылымын модельдейтін аппараттық және бағдарламалық қамтамасыз ету кешені. Стенд үш функционалды блоктан тұрады: ақылды үйді басқару блогы, сымсыз құрылғылар блогы және радиожиілік спектрін талдау блогы. Стендті жобалау кезінде білім беру зертханалық кешендеріне қойылатын талаптар ескерілді: компоненттердің қол жетімділігі, масштабтау мүмкіндігі, эксперименттер жүргізу қауіпсіздігі және IoT жүйелерінің нақты жұмыс жағдайларына сәйкестігі.

Әзірленген оқу стендінің жалпы түрі және зертханалық кешен элементтерінің орналасуы 1-суретте көрсетілген. Суретте ақылды үй контроллері, сымсыз датчиктер, атқарушы құрылғылар, сондай-ақ радиожиілік спектрін талдауға арналған жабдықтар көрсетілген. Ұсынылған конфигурация зерттеу жүргізу кезінде қолданылатын эксперименттік қондырғының нақты құрылымын көрсетеді.



1-сурет. ZigBee арналарының кептелу шабуылдарын зерттеуге арналған оқу стендінің жалпы көрінісі

Ескерту – авторлар құрастырған

1-кесте. Оқу стендінің аппараттық құрамы

Компонент	Үлгі	Мақсаты
Ақылды үй контроллері	Aqara Hub	ZigBee құрылғыларын орталықтандырылған басқару
Қозғалыс датчигі	Aqara Motion Sensor	Қамту аймағында қозғалысты анықтау
Ашу датчигі	Aqara Door/Window Sensor	Есіктер мен терезелердің күйін бақылау
Ақылды розетка	Aqara Smart Plug	Аспаптардың электрмен қоректенуін басқару
Температура датчигі	Aqara Temperature Sensor	Микроклимат параметрлерін бақылау
SDR құрылғысы	HackRF One	Радио сигналдарды талдау және генерациялау
Ескерту – автор құрастырған		

Ақылды үйді басқару блогы Aqara Hub-та салынған. Бұл платформа интерфейс арқылы барлық ақылды үй құрылғыларын орталықтандырылған басқаруды қамтамасыз етеді және автоматтандыру сценарийлерін жасауға мүмкіндік береді. ZigBee құрылғыларын біріктіру үшін Aqara Hub қолданылады, бұл платформаны таңдау оның жаппай қолданылуына, қоғамдастықтың кең қолдауына және нарықтағы көптеген ZigBee құрылғыларымен үйлесімділігіне байланысты (Zigbee2MQTT Documentation, 2024).

Сымсыз құрылғылар блогы нақты ақылды үй инфрақұрылымын модельдеуге мүмкіндік беретін әртүрлі мақсаттағы сенсорлар мен атқарушы құрылғылар жиынтығын қамтиды. Барлық құрылғылар Zigbee протоколымен жұмыс істейді және батареяларды үнемдеу үшін ұйқы режимін қолдайды. Құрылғы түрлерінің әртүрлілігі студенттерге кедергі шабуылдарының әртүрлі жабдық санаттарына әсерін зерттеуге және радиожиілік кедергілері жағдайында құрылғылардың әр түрінің жұмыс ерекшеліктерін түсінуге мүмкіндік береді.

Сымсыз құрылғылар блогына сондай-ақ қауіпсіздік пен мониторингке арналған келесі сенсорлар енгізілген:

– Қозғалыс датчигі (Aqara Motion Sensor) – инфрақызыл (PIR) технология негізінде жұмыс істейді және қозғалысты анықтауға арналған. Бұл құрылғы радиожиілік кедергілері кезінде оқиға туралы хабарламалардың кешігуін немесе жоғалуын зерттеуге мүмкіндік береді.

– Есік/терезе ашылу датчигі (Aqara Door and Window Sensor) – магниттік байланыс принципі бойынша жұмыс істейді және объектінің ашылуын немесе жабылуын тіркейді. Ол желідегі пакеттердің жоғалуы немесе кешігуі кезінде оқиғалардың дұрыс тіркелуін талдау үшін қолданылады.

– Температура және ылғалдылық датчигі (Aqara Temperature and Humidity Sensor) – қоршаған ортаның параметрлерін өлшейді және периодтық түрде хабқа мәліметтер жібереді. Бұл құрылғы тұрақты телеметриялық трафикке радиожиілік кедергілерінің әсерін бағалауға мүмкіндік береді.

– Діріл/шыны сыну датчигі (Aqara Vibration Sensor) – механикалық әсерлерді анықтайды және қауіпсіздік сценарийлерінде қолданылады. Ол қысқа уақыттық импульстік хабарламалардың сенімділігін зерттеуге мүмкіндік береді.

– Ақылды шам (Aqara Smart Bulb) – атқарушы құрылғы ретінде сценарийлердің орындалуын көрсетеді және басқару командаларының жеткізілу уақытын өлшеу үшін пайдаланылады.

– Су ағуын анықтау датчигі (Aqara Water Leak Sensor) – су басу немесе ылғалдың шекті деңгейден жоғарылауын тіркеуге арналған. Бұл құрылғы сирек, бірақ критикалық оқиғаларды тіркейді, сондықтан радиожиілік кедергі жағдайында авариялық хабарламалардың жоғалу ықтималдығын бағалау үшін қолданылады.

– Сымсыз екі батырмалы қосқыш (Aqara Wireless Double Switch) – пайдаланушы әрекетін модельдеуге арналған құрылғы. Бұл құрылғы оқиғалық (event-driven) трафикті қалыптастырады және басқару командаларының орындалу сенімділігін зерттеуге мүмкіндік береді.

– Екі арналы құрғақ контактілі реле (Aqara Dual Relay Module, dry contact) – сыртқы атқарушы құрылғыларды басқаруға арналған. Ол нақты инженерлік жүйелермен (жарықтандыру, желдету, сорғылар) интеграцияны модельдеуге мүмкіндік береді және басқару сигналдарының радиожиілік кедергілер жағдайындағы тұрақтылығын зерттеу үшін пайдаланылады.

Құрылғылардың әртүрлі типтері (оқиғалық сенсорлар, периодтық сенсорлар және атқарушы құрылғылар) зертханалық стендте кедергі (jamming) шабуылдарының әртүрлі трафик модельдеріне әсерін салыстырмалы түрде талдауға мүмкіндік береді.

Радиожиілік спектрін талдау блогы бағдарламалық жасақтамамен анықталған радиодан (SDR) және арнайы бағдарламалық жасақтама орнатылған дербес компьютерден тұрады. HACKRF One SDR құрылғысы 1 МГц-тен 6 ГГц-ке дейінгі жиілік диапазонында радио сигналдарды қабылдауға және жіберуге мүмкіндік береді, бұл оны сымсыз протоколдарды зерттеудің әмбебап құралы етеді (Great Scott Gadgets, 2023). Hackrf One таңдауы оның қол жетімді құнына, ашық архитектурасына, GNU Radio қолдауына және зертханалық жағдайда эксперименттер жүргізу үшін жеткілікті таратқыш қуатына байланысты (Great Scott Gadgets, 2023; GNU Radio Project, 2024).

Оқу стендінің бағдарламалық жасақтамасы

Зертханалық жұмыстарды жүргізу үшін "ZigBee Security Lab" бағдарламалық жасақтамасы арнайы әзірленді, ол студенттерге ZigBee желісінің қауіпсіздігін зерттеудің барлық кезеңдерін дәйекті орындау үшін ыңғайлы интерфейсті ұсынады. Бағдарламалық жасақтама SDR құрылғысын басқару үшін GNU radio кітапханаларын қолдана отырып, Python тілінде жасалған және үш негізгі функционалды модульді жүзеге асырады.

GNU Radio-сигналдарды өңдеу бағдарламаларын құру үшін еркін таратылатын даму ортасы (GNU Radio Project, 2024). Бұл платформа модульдік архитектураның және дайын компоненттердің кең кітапханасының арқасында ғылыми зерттеулер мен білім беру жобаларында кеңінен қолданылады. GNU Radio-ны Python тілімен біріктіру радиожиілік сигналдарымен жұмыс істеу үшін икемді және кеңейтілетін қосымшалар жасауға мүмкіндік береді.

ZigBee белсенді арнаны анықтау модулі. ZigBee протоколы 11-ден 26-ға дейін нөмірленген 2,4 ГГц диапазонында 16 арнаны пайдаланады. Әр арнаның орталық жиілігі мына формула бойынша есептеледі: $f = 2405 + 5 \times (n - 11)$ МГц, мұндағы n - арна нөмірі. Анықтау модулі барлық 16 арнаны дәйекті сканерлейді және қабылданған сигнал деңгейін талдайды. Арнада белсенділік анықталған кезде бағдарлама ZigBee пакеттерінің кіріспесін декодтайды және желі идентификаторын (PAN ID) анықтайды. Сканерлеу нәтижелері спектрограмма және анықталған желілер кестесі ретінде көрсетіледі. Сканерлеу алгоритмі анықтаудың жоғары дәлдігін сақтай отырып, белсенді арналарды анықтау уақытын азайту үшін оңтайландырылған.

Желі жұмысының дұрыстығын диагностикалау модулі. Белсенді арнаны анықтағаннан кейін студент Zigbee желісінің трафигін пассивті бақылайтын диагностикалық модульді іске қоса алады. Модуль қабылданған пакеттердің статистикасын, әр құрылғыдан сигнал деңгейін, деректерді беру жиілігін көрсетеді. Бұл шабуыл жасамас бұрын желінің

қалыпты жұмыс істеуін қамтамасыз етуге және кейіннен шабуылдың құрылғылардың жұмысына әсерін бағалауға мүмкіндік береді. Модуль IEEE 802.15.4 пакеттерінің тақырыптарын декодтауды және пайдалы жүктемені декодтаусыз қызметтік ақпаратты алуды жүзеге асырады.

Кедергі шабуылын іске асыру модулі. Бұл модуль таңдалған ZigBee арнасында радиожиілік кедергілерін жасауға мүмкіндік береді. Студент шабуыл параметрлерін: мақсатты арнаны, кедергі жиілігінің диапазонын және қуат деңгейін реттей алады. Бағдарлама кең жолақты шу сигналын қалыптастырады және оны SDR құрылғысы арқылы жібереді. Шабуыл кезінде модуль желіні бақылауды жалғастырады және нақты уақыттағы байланыс сапасының көрсеткіштерінің өзгеруін көрсетеді. Кедергі сигналдарының бірнеше түрі жүзеге асырылады: үздіксіз шу, импульстік кедергі және адаптивті кедергі, бұл әртүрлі шабуыл сценарийлерін зерттеуге мүмкіндік береді.

2-кесте. Бағдарламалық жасақтаманың функционалдығы

Модуль	Функциялар	Параметрлер
Сканерлеу	Белсенді арналарды анықтау PAN ID анықтау	Арналар ауқымы 11-26
Диагностика	Трафикті бақылау, RSSI өлшеу, пакеттерді санау	Бақылау уақыты, жаңарту аралығы
Шабуыл	Кедергі жасау, сигнал түрін таңдау, қуатты реттеу	Арна, жолақ, деңгей, кедергі түрі
Ескерту – автор құрастырған		

Зерттеу жүргізу әдістемесі

Зерттеу әдістемесі эксперименттер жүргізудің бақыланатын шарттарын қолдана отырып, эксперименттік тәсілге негізделген. Нәтижелердің қайталануын қамтамасыз ету үшін дайындық кезеңін, өлшеу кезеңін және нәтижелерді талдау кезеңін қамтитын эксперименттер жүргізудің стандартталған хаттамасы әзірленді.

Дайындық кезеңінде жабдықты калибрлеу, стендтің барлық компоненттерінің жұмысын тексеру және бағдарламалық жасақтама параметрлерін реттеу жүзеге асырылады. SDR құрылғысын калибрлеу қабылдағыштың жергілікті шу деңгейін өлшеуді және таратқыштың пайда болуын анықтауды қамтиды. Бұл параметрлер өлшеу нәтижелерін қалыпқа келтіру үшін қолданылады.

Өлшеу кезеңі зертханалық жұмыстың сценарийіне сәйкес эксперименттерді дәйекті түрде орындауды қамтиды. Барлық өлшеулер сыртқы радиожиілік кедергілерінің әсерін азайту үшін экрандалған бөлмеде жүргізіледі. Өлшеу нәтижелері уақыт белгілері мен эксперимент параметрлері көрсетілген мәліметтер базасына автоматты түрде сақталады.

НӘТИЖЕЛЕР ЖӘНЕ ОЛАРДЫ ТАЛҚЫЛАУ

Зертханалық жұмысты студенттер жеке немесе жұпта орындайды. Жұмыстың ұзақтығы 8 академиялық сағатты құрайды, бұл шабуылдың барлық кезеңдерін егжей-тегжейлі зерттеуге және алынған нәтижелерді талдауға мүмкіндік береді. Жұмыс басталар алдында оқытушы радиожиілік жабдықтарымен жұмыс істеу кезінде қауіпсіздік техникасы бойынша нұсқама жүргізеді және радиожиілік спектрін пайдалану саласындағы заңнаманы сақтау қажеттігін еске салады.

Әзірленген зертханалық стенд негізінде ақылды үй жүйелері мен заттар интернеті хаттамаларының қауіпсіздігі бойынша тәжірибеге бағытталған зертханалық жұмыстарды жүргізу үшін әдістемелік нұсқаулар кешені құрылды. Кешен физикалық, арналық және желілік деңгейлерді зерттеуді, сондай-ақ сымсыз технологиялар мен қолданбалы басқару жүйелерінің осалдықтарын талдауды қамтиды. Зертханалық жұмыстардың құрылымы мен мазмұны 3-кестеде келтірілген.

3-кесте. Smart Home Security оқу стендіндегі зертханалық жұмыстар кешені

№	Зертханалық жұмыстың атауы	Жұмыстың мақсаты және қысқаша сипаттамасы
1	ZigBee протоколдарының стегін зерттеу және мақсатты радиожиілік арнасын анықтау	ZigBee протоколдарының стек архитектурасын, оның Заттар интернетінің (IoT) экожүйесіндегі рөлін және IEEE 802.15.4 стандартының төменгі деңгейлерімен өзара әрекеттесуін егжей-тегжейлі зерттеу. Практикалық бөлім радиожиілік спектрінде және жұмыс жиілігі арнасында Белсенді Zigbee желілерін пассивті анықтауға бағытталған. Бұл тапсырманы орындау үшін қосымша 2.4 ГГц диапазонын сканерлеуге конфигурацияланған мамандандырылған бағдарламалық жасақтама (SDR Hackrf One, CatSniffer) қолданылады. Жұмыс арнасын сәтті анықтау трафикті талдау бойынша барлық зертханалық жұмыстар үшін қажетті алдын ала қадам болып табылады
2	Zigbee трафигін пассивті ұстау және түсіру әдістемесі	Zigbee сымсыз трафигін пассивті ұстау үшін қажетті құралдар мен әдістерді меңгеріңіз. Студенттер №1 жұмыста анықталған жиілік арнасында бақылау режимінде жұмыс істеу үшін ZigBee-Sniffer конфигурациясын жасайды. Деректерді түсіру желілік оқиғаларды инициализациялау кезінде жүзеге асырылады. Нәтиже-деректер массиві. ZigBee (Beacon, Data, Command Frames) сипаттамаларына сәйкес желілік пакеттерді түсіруді және оларды сәйкестендіруді растау үшін желілік анализаторда ұсталған кадрларға негізгі талдау жасалады.
3	Шифрланған желілік кадрлардың құрылымдық және метадеректерді талдауы	ZigBee шифрланған кадрларынан алуға болатын ақпарат көлемін көрсетіңіз. Талдау шифрды ашу процесіне дейін қол жетімді желілік және арналық деңгейлерге бағытталған. Студенттер MAC тақырып өрістерін, желі тақырыбын талдайды. Талдаудың негізгі элементі – қайта ойнату шабуылдарының (Replay Attacks) алдын алу үшін қолданылатын кадр есептегішін (Frame Counter) бақылау. Метадеректерге талдау жасалады: трафиктің жиілігі, көлемі және бағыты, бұл желінің "белсенділік картасын" құруға және ықтимал маңызды түйіндерді анықтауға мүмкіндік береді (мысалы, үйлестіруші).
4	Арнаны өшіру шабуылын эксперименттік зерттеу (Jamming)	Jamming деп аталатын ZigBee протоколының төмен деңгейлерінде (PHY/MAC) қызмет көрсетуден бас тарту шабуылының (DoS) механизмі мен тиімділігін зерттеу. Зертханалық жұмыс бағытталған кедергіні жүзеге асыру принциптерін зерттеуді қамтиды. Бұл тапсырманы орындау үшін арнайы бағдарламалық жасақтама (SDR Hackrf One) қосымша қолданылады, оның көмегімен мақсатты арнада шудың үздіксіз берілуі жүзеге асырылады. Шабуылдың тиімділігі пакеттің жоғалу коэффициентін (Packet Error Rate) және заңды ZigBee желісіндегі байланыстың кешігуін бақылау арқылы сандық түрде өлшенеді. Нәтижелер төмен қуатты сымсыз желілердің осы әсер ету түріне жоғары осалдығын көрсетуі керек.
5	WEP протоколының қауіпсіздігін пароль арқылы талдау	WEP протоколы бар Wi-Fi желілерінің қауіпсіздік ерекшеліктерін зерделеу, мамандандырылған бағдарламалық жасақтаманы (Kali Linux ОЖ (Aircrack-Ng, Hashcat, VirtualBox, Wireshark) қолдана отырып, төрт рет қол алысу (4-way handshake) және парольдерді асыра пайдалану (dictionary/bruteforce) әдістерін меңгеру.

1-кестенің соңы

№	Зертханалық жұмыстың атауы	Жұмыстың мақсаты және қысқаша сипаттамасы
6	WPA-PSK протоколының қауіпсіздігін пароль арқылы талдау	WPA/WPA2-PSK бар Wi-Fi желілерінің қауіпсіздік ерекшеліктерін зерттеу, мамандандырылған бағдарламалық жасақтаманың көмегімен төрт рет қол алысу (4-way handshake) және парольдер арқылы шабуыл жасау (dictionary/bruteforce) әдістерін меңгеру.
7	WPA2-Enterprise протоколының қауіпсіздігін талдау	WPA2-Enterprise протоколы бар Wi-Fi желілерінің қауіпсіздік ерекшеліктерін зерттеу, TLS сертификатын құру әдістерін және төрт рет қол алысуды (4-way handshake) түсіру және арнайы бағдарламалық жасақтаманың көмегімен парольді асыра пайдалану (dictionary/bruteforce) шабуылын орындау үшін шабуыл жасауды меңгеру.
8	Ақылды құлыптау экожүйесінің қауіпсіздігін тексеру	Зерттеу узвисомтси ақылды құлып Физикалық деңгейде, желі деңгейінде және Қолданба деңгейінде. Электрондық басқаруды айналып өту үшін чипті физикалық клондау шабуылдарын, құрылғыны немесе желіні шамадан тыс жүктеу арқылы DDoS шабуылдарын, қолмен ұстауды, Evil Twin типті шабуылдарды (жалған кіру нүктесін құру) және аутентификация шабуылдарын жүзеге асырудың негізгі әдістері мен құралдарын зерттеңіз. Осалдықтарды анықтау мақсатында құлыпты басқару үшін қолданылатын мобильді қосымшаны зерттеу және бұзу

1-кезең. Стендті дайындау және бағдарламалық жасақтаманы іске қосу.

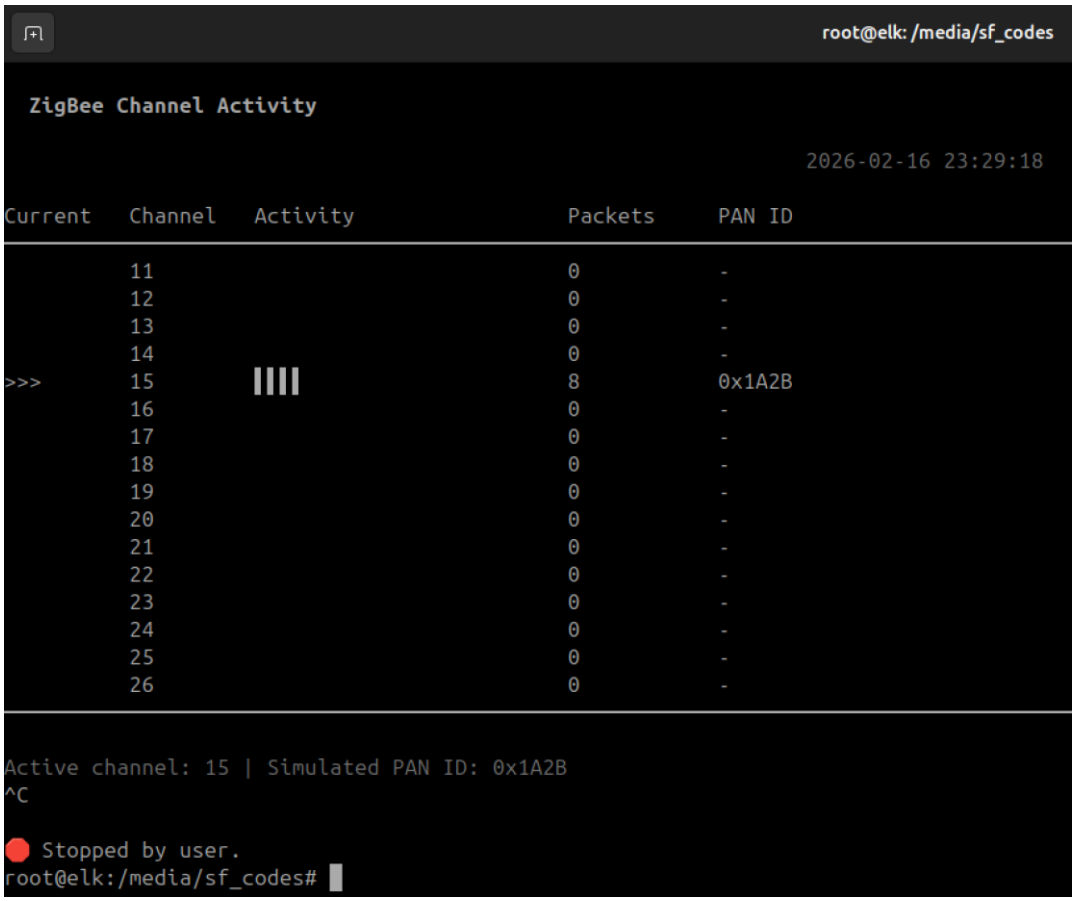
Студент Aqara Hub қуатын қосады және жүйенің жүктелуін күтеді, ол шамамен 2-3 минутты алады. Интерфейс арқылы студент барлық ZigBee құрылғыларының жүйеде көрсетілгенін және «қол жетімді» күйде екенін тексереді. Шабуылдаушының жұмыс станциясында студент SDR құрылғысын қосып, ZigBee Security Lab бағдарламасын іске қосады. Бағдарлама SDR құрылғысын инициализациялайды және оның жұмысының дұрыстығын тексереді. Студент есепте стендтің барлық компоненттерінің күйін және эксперимент жүргізуге дайындығын жазады.

2-сурет. Aqara Hub қосу

Ескерту – авторлар құрастырған

2-кезең. ZigBee желісінің белсенді арнасын анықтау.

ZigBee Security Lab бағдарламасында студент "сканерлеу" модуліне өтіп, белсенді арналарды анықтау процесін бастайды. Бағдарлама барлық 16 ZigBee арналарын дәйекті түрде талдайды және нақты уақыттағы спектрограмманы көрсетеді. Бір арнаны сканерлеу уақыты 500 миллисекундты құрайды, Толық сканерлеу циклі шамамен 8 секундты алады. Сканерлеу аяқталғаннан кейін студент есепте анықталған белсенді арнаның нөмірін, оның орталық жиілігін және Pan id желісінің идентификаторын тіркейді. Студент сонымен қатар электромагниттік жағдайды бағалау үшін көрші арналардағы сигнал деңгейін талдайды.

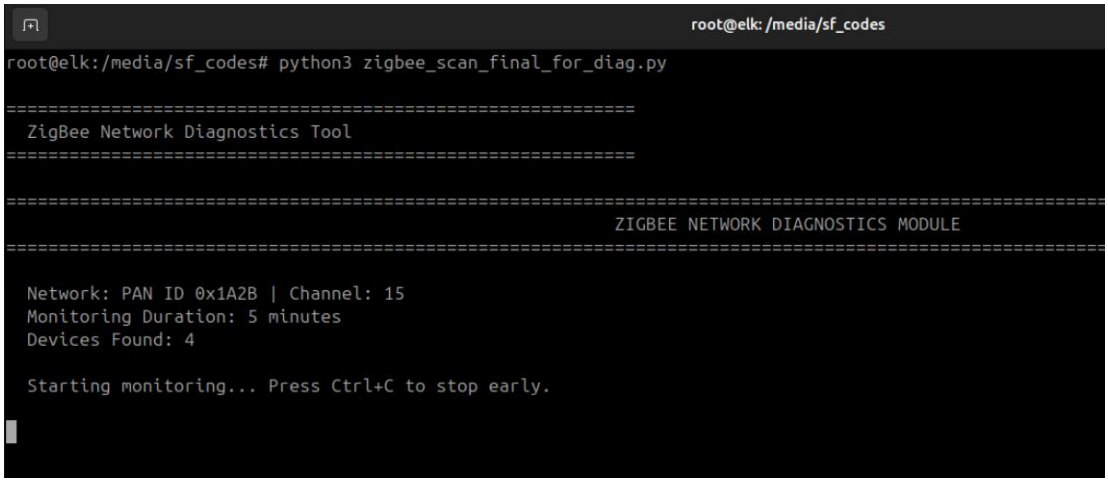


3-сурет. «Сканерлеу» модулі және процесті бастау

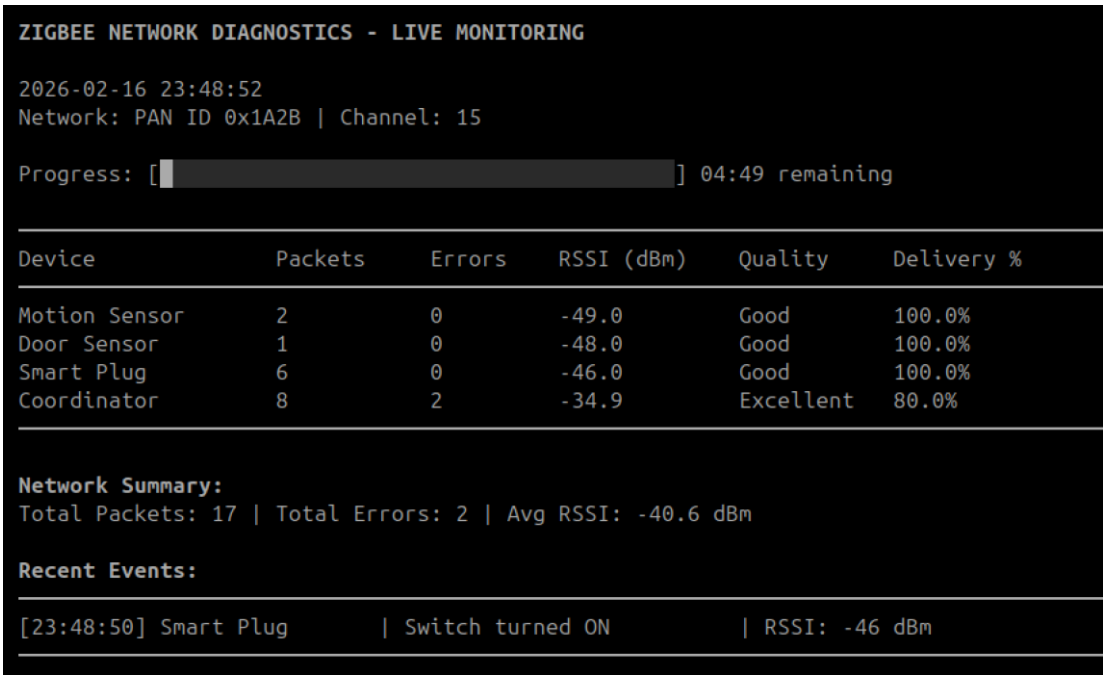
Ескерту – авторлар құрастырған

3-кезең. Желі жұмысының дұрыстығын диагностикалау.

Студент «Диагностика» модуліне ауысады және анықталған желіні бақылауды бастайды. 5 минут ішінде бағдарлама желінің жұмысы туралы статистиканы жинайды, жіберілген пакеттердің санын, әр құрылғыдан сигнал күшін және жіберу қателіктерінің болуын тіркейді. Студент сенсорлық белсенділікті бастайды: қозғалыс сенсорының алдынан өтіп, сенсоры бар есікті ашады және жабады, ақылды Розетканы қосады және өшіреді. Барлық оқиғалар басқару жүйесінің интерфейсінде көрсетіліп, Бақылау бағдарламасымен жазылуы керек. Студент есепке бастапқы көрсеткіштерді жазады: қабылданған пакеттер саны, RSSI сигналының орташа деңгейі, сәтті жеткізілген хабарламалардың пайызы. Дұрыс жұмыс істейтін желі үшін әдеттегі RSSI мәндері – 40-тан -70 дБм-ге дейін.



4-сурет. «Диагностика» модулін іске қосу процесі
Ескерту – авторлар құрастырған



5-сурет. «Диагностика» модулінің жұмыс процесі
Ескерту – авторлар құрастырған

4-кезең. Кептеліс шабуылын жүзеге асыру.

Студент «шабуыл» модуліне өтіп, кедергі параметрлерін реттейді: бұрын анықталған арнаны таңдайды, 5 МГц кедергі жолағын және ең төменгі қуат деңгейін орнатады. Оқытушы расталғаннан кейін студент кедергілерді тудырады. Бағдарлама шабуыл процесін және нақты уақыттағы желі параметрлерін өзгертуді көрсетеді. Студент RSSI деңгейінің өзгеруін және сәтті қабылданған пакеттер санын бақылайды.

Aqara Hub интерфейсінде студент құрылғылардың "қол жетімді емес"күйіне өтуін бақылайды. Ауысу уақыты есепте жазылады және әдетте жүйенің күту уақытының параметрлеріне байланысты 10-30 секундты құрайды. Студент сенсорларды белсендіру әрекеттерін қайталайды және оқиғалар жүйемен тіркелмейтініне көз жеткізеді. Шабуыл

механизмін тереңірек түсіну үшін студент кедергі қуатын дәйекті түрде арттырады және әр қадамда желі параметрлерінің өзгеруін жазады.

5-кезең. Өнімділікті қалпына келтіру және нәтижелерді талдау.

Студент кедергілердің пайда болуын тоқтатады және құрылғылармен байланыстың қалпына келуін бақылайды. Қалпына келтіру уақыты есепте жазылады және әдетте құрылғы түріне және желі параметрлеріне байланысты 5-60 секундты құрайды. Студент диагностикалық модульді қайта іске қосады және шабуылға дейін және одан кейінгі желі көрсеткіштерін салыстырады. Шабуылдың әртүрлі типтегі құрылғыларға әсері талданады: батареямен жұмыс істейтін сенсорлар, желі үйлестірушісі, маршрутизаторлар. Студент құрылғылардың әр түрі үшін өнімділікті қалпына келтіру ерекшеліктерін жазады.

4-кесте. Эксперименттің күтілетін нәтижелері

Параметрлер	Шабуылға дейін	Шабуыл кезеңінде	Шабуылдан кейін
RSSI деңгейі, дБм	-50...-70	-30...-40	-50...-70
Пакеттер саны / мин	20-50	0-5	15-45
Құрылғылардың қол жетімділігі	100%	0-20 %	80-100 %
Жауап беру уақыты, мс	100-500	Таймаут	200-1000
Тасымалдау қателері, %	0-5	90-100	5-15
Ескерту – автор құрастырған			

Жұмыс нәтижелері бойынша студент орындалған әрекеттердің сипаттамасын, әр кезеңдегі бағдарламаның скриншоттарын, өлшенген параметрлері бар кестені және Zigbee протоколының кедергі шабуылдарына осалдығы туралы қорытындыларды қамтитын есеп жасайды. Есепте сонымен қатар жүйенің осы шабуыл түріне төзімділігін арттыру бойынша ұсыныстар берілген.

Әзірленген оқу стенді ZigBee желілерінің OSI моделінің физикалық деңгейіндегі шабуылдарға осалдығын көрнекі түрде көрсетуге мүмкіндік береді. Студенттер бағдарламалық жасақтамамен анықталған радиода практикалық тәжірибе алады және сымсыз интернет заттарына радиожиілік шабуылдарының принциптерін түсінеді. Эксперименттік зерттеулер зертханалық сабақтарды ұйымдастыруға ұсынылған тәсілдің тиімділігін растады.

Арнайы әзірленген Zigbee Security Lab бағдарламалық құралы зерттеудің барлық кезеңдерін орындау үшін интуитивті интерфейсті қамтамасыз ете отырып, зертханалық жұмысты жүргізуді айтарлықтай жеңілдетеді. Бағдарламаның модульдік архитектурасы оның функционалдығын кеңейтуге және болашақта жаңа шабуыл сценарийлерін қосуға мүмкіндік береді. Оқу процесінде бағдарламаны қолдану тәжірибесі студенттердің бір зертханалық сабақта сымсыз желілер қауіпсіздігінің негізгі тұжырымдамаларын сәтті меңгергенін көрсетті.

Стендтің маңызды артықшылығы-эксперименттің жоғары шынайылығын қамтамасыз ететін нақты ақылды үй құрылғыларын пайдалану. Студенттер үйді автоматтандырудың нақты жүйелерінде қолданылатын сенсорлар мен хаттамалармен жұмыс істейді. Бұл студенттерде IoT жүйелерінің қауіпсіздігінің практикалық аспектілері туралы түсінік қалыптастырады және оларды кәсіби қызметтегі нақты мәселелерді шешуге дайындайды.

Әзірленген стендті қолданыстағы білім беру шешімдерімен салыстырмалы талдау оның бәсекеге қабілеттілігін көрсетеді. Таза бағдарламалық симмуляторлардан айырмашылығы, стенд нақты аппараттық құралдармен және радиожиілік сигналдарымен жұмыс істеуді қамтамасыз етеді. Коммерциялық зертханалық кешендермен

салыстырғанда, стенд білім беру мақсаттары үшін қажетті функционалдылықты сақтай отырып, айтарлықтай төмен бағамен сипатталады.

Әрі қарай даму бағыты ретінде Zigbee-ге шабуылдардың басқа түрлерін, соның ішінде ойнату шабуылдары мен желіге қосылу процедураларына шабуылдарды зерттеу үшін бағдарламалық жасақтаманың функционалдығын кеңейту жоспарлануда (Gavra et al., 2023; Ren et al., 2023; Caballero-Gil et al., 2024). Сондай-ақ адаптивті арналарды ауыстыру және кеңістіктік сүзу сияқты кедергі шабуылдарынан қорғау механизмдерін зерттеуге арналған модульдерді әзірлеу жоспарлануда (Fang et al., 2024; Pirayesh et al., 2021). Перспективалық бағыт кедергі шабуылдарын автоматты түрде анықтау үшін машиналық оқыту әдістерін біріктіру (Pirayesh et al., 2021).

ҚОРЫТЫНДЫ

Жұмыста интернет заттарының киберқауіпсіздігі бойынша мамандарды даярлау кезінде оқу процесінде қолдануға болатын ZigBee протоколына дыбысты өшіру шабуылдарын зерттеуге арналған Ақылды үй зертханалық стенді ұсынылған. Aqara Hub смарт үй контроллерін, әртүрлі мақсаттағы сымсыз сенсорлар жинағын және hackrf бағдарламалық құралымен анықталған радионы қамтитын стенд аппараттық құралының құрамы сипатталған.

Желінің белсенді арнасын анықтауды, оның жұмыс қабілеттілігін диагностикалауды және кедергі шабуылын жүзеге асыруды қамтамасыз ететін GNU radio платформасы негізінде ZigBee Security Lab мамандандырылған бағдарламалық жасақтамасы әзірленді. Бағдарламалық жасақтама модульдік архитектурамен, интуитивті интерфейспен және шабуылдардың қосымша түрлерін зерттеу үшін функционалдылықты кеңейту мүмкіндігімен сипатталады.

Бес негізгі кезеңді қамтитын зертханалық жұмыстың егжей-тегжейлі сценарийі келтірілген: стендті дайындау, белсенді арнаны анықтау, Желі жұмысын диагностикалау, кедергі шабуылын жүзеге асыру және нәтижелерді талдаумен өнімділікті қалпына келтіру. Эксперименттің күтілетін нәтижелері және зертханалық жұмыстың сәттілігін бағалау критерийлері ұсынылған.

Әзірленген стенд киберқауіпсіздік саласындағы білім беру зертханалық кешендеріне қойылатын заманауи талаптарға сәйкес келеді: ол нақты жабдықтармен жұмыс істеуді қамтамасыз етеді, шабуылдардың практикалық сценарийлерін модельдейді, қол жетімді құны мен масштабтау мүмкіндігімен сипатталады. Стенд Қазақстанның жоғары оқу орындарында ақпараттық қауіпсіздік мамандарын даярлаудың оқу бағдарламаларына біріктірілуі мүмкін.

Әрі қарайғы зерттеулердің бағыттары ретінде желіге қосылу процедурасына қайталанатын шабуылдар мен шабуылдарды зерттеу үшін модульдер әзірлеу, сондай-ақ кедергі шабуылдарын автоматты түрде анықтау үшін машиналық оқыту әдістерін біріктіру жоспарлануда. Студенттердің стенд жабдықтарына қашықтан қол жеткізуі үшін таратылған зертханалық инфрақұрылымды құру перспективалы болып табылады, бұл IoT киберқауіпсіздік саласындағы білім беру бағдарламаларын қамтуды кеңейтуге мүмкіндік береді.

МҮДДЕЛЕР ҚАЙШЫЛЫҒЫ: Автор(лар) мүдделер қайшылығы жоқ екенін мәлімдейді.

ҚАРЖЫЛАНДЫРУ: «Бұл мақала Қаланың тұрақты дамуы және азаматтардың өмір сүру сапасын жақсарту үшін Smart City цифрлық экожүйесінің интеллектуалды үлгілері мен әдістерін әзірлеу» атты BR24992852 тақырыбы бойынша Ғылым және жоғары білім министрлігінің ғылыми зерттеулерге арналған гранттық қаржыландыру жобасы аясында дайындалды».

ИНСТИТУЦИОНАЛДЫҚ ЭТИКА КОМИТЕТІНІҢ ҚОРЫТЫНДЫСЫ: Қолданылмайды.

ЕРІКТІ КЕЛІСІМ ТУРАЛЫ МӘЛІМДЕМЕ: Қолданылмайды.

ДЕРЕКТЕРДІҢ ҚОЛЖЕТІМДІЛІГІ ТУРАЛЫ МӘЛІМДЕМЕ: Жұмыс сандық модельдеу мен теориялық талдауға негізделгендіктен, жаңа эксперименттік деректер жиналмаған.

АЛҒЫС БІЛДІРУ: Авторлар әдістемелік қолдау мен пайдалы пікірлері үшін әріптестеріне, сондай-ақ мақаланың сапасын арттыруға септігін тигізген анонимді рецензенттерге алғыс білдіреді.

ЖАСАНДЫ ИНТЕЛЛЕКТ ТЕХНОЛОГИЯЛАРЫН ПАЙДАЛАНУ ТУРАЛЫ ХАБАРЛАМА: Қолданылмайды.

ӘДЕБИЕТТЕР ТІЗІМІ

Zohourian A., Dadkhah S., Neto E.C.P., Mahdikhani H., Danso P.K., Molyneaux H., Ghorbani A.A. (2023). IoT Zigbee device security: A comprehensive review. Internet of Things, 22, 100791. https://doi.org/10.1016/j.iot.2023.100791

Vasilescu N.G., Pocatilu P., Doinea M. (2023). IoT Security Challenges for Smart Homes. Smart Innovation, Systems and Technologies, 321, 35-48. https://doi.org/10.1007/978-981-19-6755-9_4

IEEE Standard 802.15.4-2020: Low-Rate Wireless Networks (2020). IEEE, 800 p.

Zigbee Alliance (2021). Analysts Confirm Half a Billion Zigbee Chipsets Sold. Igniting IoT Innovation. https://csa-iot.org/

Kumar M., Yadav V., Yadav S.P. (2024). Advance comprehensive analysis for Zigbee network-based IoT system security. Discover Computing, 27, 22. https://doi.org/10.1007/s10791-024-09456-3

Fang X., Zheng L., Fang X. et al. (2024). Pioneering advanced security solutions for reinforcement learning-based adaptive key rotation in Zigbee networks. Scientific Reports. 14, 13931. https://doi.org/10.1038/s41598-024-64895-8

García-Magariño I., Lacuesta R., Rajarajan M., Lloret J. (2023). Exploring IoT Vulnerabilities in a Comprehensive Remote Cybersecurity Laboratory. Sensors. 23, 9279. https://doi.org/10.3390/s23229279

Fu X., Zou C. (2023). Building a Low-Cost and State-of-the-Art IoT Security Hands-On Laboratory. NSF Award 1915780. https://www.nsf.gov/awardsearch/showAward?AWD_ID=1915780

Gavra V., Pop O.A., Dobra I.A. (2023). Comprehensive Analysis: Evaluating Security Characteristics of Xbee Devices against Zigbee Protocol. Sensors. 23, 8736. https://doi.org/10.3390/s23218736

Ren M., Ren X., Feng H., Ming J., Lei Y. (2023). Security analysis of ZigBee protocol implementation via device-agnostic fuzzing. Digital Threats: Research and Practice, 4, 1-24. https://doi.org/10.1145/3551894

Villanueva-Miranda I., Villalobos-Castaldi F.M., Gress N.H. (2021). A technical review of wireless security for the internet of things: Software defined radio perspective. Journal of King Saud University – Computer and Information Sciences, 33, 1050-1061. https://doi.org/10.1016/j.jksuci.2021.04.003

Bouchendouka H., Teguig D., Sadoudi S. (2022). SDR Implementation of WIFI Attacks Using GNURadio. Lecture Notes in Networks and Systems, 513, 305-315. https://doi.org/10.1007/978-3-031-12097-8_26

Benimam A., Sadoudi S., Belmeguenai A. (2023). Software defined radio implementation of a secure waveform for real-time data transmission using universal software radio peripheral. Security and Privacy, 6, e280. https://doi.org/10.1002/spy2.280

Тлеубердин, С., & Сейткулов, Е. (2022). Актуальные киберугрозы для IoT устройств умного дома. Вестник КазАТК, 122(3), 195–202. https://doi.org/10.52167/1609-1817-2022-122-3-195-

202 // Tleuberdin, S., & Seytkulov, E. (2022). Aktual'nyye kiberugrozy dlya IoT ustroystv umnogo doma [Current cyber threats for IoT smart home devices]. Vestnik KazATK, 122(3), 195–202. https://doi.org/10.52167/1609-1817-2022-122-3-195-202 (In Russ.)

Постановление Правительства Республики Казахстан от 28 марта 2023 года № 269. (2023). Концепция цифровой трансформации, развития отрасли информационно-коммуникационных технологий и кибербезопасности на 2023–2029 годы. https://adilet.zan.kz/rus/docs/P2300000269 // Postanovleniye Pravitel'stva Respubliki Kazakhstan ot 28 marta 2023 goda № 269. (2023). Kontseptsiya tsifrovoy transformatsii, razvitiya otrasli informatsionno-kommunikatsionnykh tekhnologiy i kiberbezopasnosti na 2023–2029 gody [Concept of digital transformation, development of the information and communication technology industry and cybersecurity for 2023–2029]. https://adilet.zan.kz/rus/docs/P2300000269 (In Russ.)

Zigbee2MQTT Documentation (2024). https://www.zigbee2mqtt.io/

Great Scott Gadgets. (2023). HackRF One Technical Documentation. https://greatscottgadgets.com/hackrf/

GNU Radio Project. (2024). GNU Radio Manual and C++ API Reference. https://www.gnuradio.org/

Caballero-Gil C., Alvarez R., Hernández-Goya C., Molina-Gil J. (2024). Research on smart-locks cybersecurity and vulnerabilities. Wireless Networks, 30, 5905-5917. https://doi.org/10.1007/s11276-023-03376-8

Pirayesh H., Kheirkhah Sangdeh P., Zeng H. (2021). Securing ZigBee communications against constant jamming attack using neural network. IEEE Internet of Things Journal, 8, 6. 4957-4968. https://doi.org/10.1109/JIOT.2020.3034219

Авторлар туралы мәліметтер
Информация об авторах
Information about authors

Айдынов Төлеген Айдынұлы – докторант, Л.Н. Гумилев атындағы Еуразия Ұлттық университеті, Астана, Қазақстан
Айдынов Төлеген Айдынұлы – докторант, Евразийский национальный университет им. Л.Н. Гумилева, Астана, Казахстан
Aidynov Tolegen – doctoral student, L. N. Gumilyov Eurasian National University, Astana, Kazakhstan,
e-mail: 951005351309@enu.kz,
ORCID: https://orcid.org/0009-0005-3327-9719,

Тлеубердин Сакен Токатович – докторант, Л.Н. Гумилев атындағы Еуразия Ұлттық университеті, Астана қ., Қазақстан
Тлеубердин Сакен Токатович – докторант, Евразийский национальный университет им. Л.Н. Гумилева, г. Астана, Казахстан
Tleuberdin Saken – doctoral student, L.N. Gumilyov Eurasian National University, Astana, Kazakhstan,
e-mail: sakentleuberdin@gmail.com,
ORCID: https://orcid.org/0000-0001-9170-9936

Боранбай Жандос Асылханұлы – докторант, Л.Н. Гумилев атындағы Еуразия Ұлттық университеті, Астана қ., Қазақстан
Боранбай Жандос Асылханұлы – докторант, Евразийский национальный университет им. Л.Н. Гумилева, г. Астана, Казахстан
Boranbay Zhandos – doctoral student, L.N. Gumilyov Eurasian National University, Astana, Kazakhstan,
e-mail: boranbai_zha_3@enu.kz,
ORCID: https://orcid.org/0009-0009-4096-3876

Тебуева Фариза Билялovна – физика-математика ғылымдарының докторы, профессор, Солтүстік Кавказ федералды университеті, Ставрополь, Ресей
Тебуева Фариза Билялovна – доктор физико-математических наук, профессор, Северо-Кавказский федеральный университет, Ставрополь, Россия
Tebueva Fariza – Doctor of Physico-Mathematical Sciences, Professor, North-Caucasus Federal University Stavropol, Russian Federation,
e-mail: ftebueva@nfcu.ru,
ORCID: https://orcid.org/0000-0002-7373-4692

Шайханова Айгуль Кайрулаевна – қауымдастырылған профессор, Л.Н.Гумилев атындағы Еуразия Ұлттық университеті, Астана, Қазақстан
Шайханова Айгуль Кайрулаевна – ассоциированный профессор, Евразийский национальный университет им. Л. Н. Гумилева, Астана, Казахстан
Shaikhanova Aigul – Associate Professor, L. N. Gumilyov Eurasian National University, Astana, Kazakhstan,
e-mail: shaikhanova_ak@enu.kz,
ORCID: https://orcid.org/0000-0001-6006-4813

Сатыбалдина Дина Жагипаровна – физика-математика ғылымдарының кандидаты, профессор, Ақпараттық қауіпсіздік және криптология ғылыми-зерттеу институты директоры, Л.Н. Гумилев атындағы Еуразия Ұлттық университеті, Астана қ., Қазақстан
Сатыбалдина Дина Жагипаровна – кандидат физико-математических наук, профессор, директор НИИ информационной безопасности и криптологии, Евразийский национальный университет им. Л.Н. Гумилева, г. Астана, Казахстан
Satybaldina Dina – Candidate of Physico-Mathematical Sciences, Professor, Head of the Research Institute of Information Security and Cryptology, L.N. Gumilyov Eurasian National University, Astana, Kazakhstan,
e-mail: satybaldina_dzh@enu.kz,
ORCID: https://orcid.org/0000-0003-0291-4685