ӘОЖ 004.056.5 **DOI 10.52167/1609-1817-2024-134-5-168-175**

Е. Майлыбаев[1], М. Руслан[2]
[1]Халықаралық көліктік-гуманитарлық университет, Алматы, Қазақстан
[2]Satbayev University, Алматы, Қазақстан
E-mail: ersind@mail.ru

IoT ЖҮЙЕЛЕРІНДЕГІ АҚПАРАТТЫ ҚОРҒАУДЫ ҰЙЫМДАСТЫРУ

Аңдатпа. Мақалада IoT жүйелерінде ақпаратты қорғауды ұйымдастыру мен технологияларын зерттеу мәселелері қарастырылған. Зерттеудің мақсаты – IoT жүйелерінің негіздері мен осалдықтарын анықтау, олардың жұмыс принциптерін талдау және ақпаратты қорғау технологияларын ұсыну. IoT жүйелерінің негіздері мен осалдықтары, сондай-ақ ақпаратты қорғаудың негізгі принциптері қарастырылады. Сонымен қатар IoT жүйелерінде ақпаратты қорғаудың нақты мысалдары, қолданыстағы шешімдердің талдауы және қауіпсіздікті қамтамасыз ету бойынша ұсыныстар берілді. Алынған нәтижелер бойынша IoT жүйелерінің қауіпсіздігін арттыруға бағытталған кешенді тәсіл ұсынылды.

Түйінді сөздер. Ақпарат, қауіпсіздік, IoT, осалдылықтар, желі.

Кіріспе.

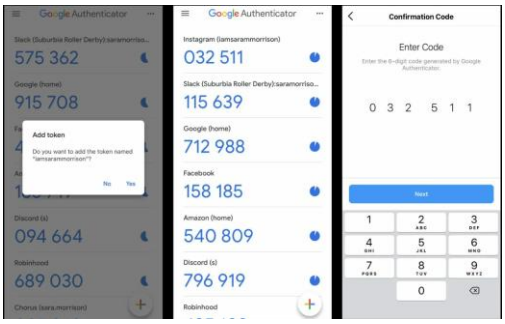
Интернет желісінің қауіпсіздігі қазіргі таңда өте өзекті мәселе болып отыр. Әсіресе, IoT құрылғыларының көптеп пайда болуы бұл мәселені одан сайын күрделендірді. Мақалада, қолданыстағы қауіпсіздік шешімдері қарастырылады және олардың тиімділігі талданады [1].

Материалдар мен тәсілдер.

Төменде ұсынылған шешімдер IoT жүйелерінің қауіпсіздігін қамтамасыз етуде қажетті рөл атқарылады. Жүйелік қауіпсіздікті арттыру үшін әртүрлі құралдар мен әдістерді қолдана отырып, қауіптерден толықтай қорғануға болады.

Екі факторлы аутентификация.

Google Authenticator – екі факторлы аутентификацияны (2FA) қолдану IoT жүйелеріндегі қауіпсіздікті едәуір арттырады. Google Authenticator жұмысын 1 суреттен көруге болады. Google Authenticator қолданушыға қосымша қауіпсіздік деңгейін қамтамасыз ету үшін арнайы генератор арқылы уақытқа байланысты бір реттік құпия кодтарды (TOTP) жібереді. Мысалы, қолданушы өз аккаунтына кірген кезде, ол әдеттегі құпия сөзін енгізеді және содан кейін Google Authenticator арқылы алынған бір реттік кодты енгізуі қажет. Бұл әдіс хакерлердің қолданушы аккаунтын бұзуын қиындатады.

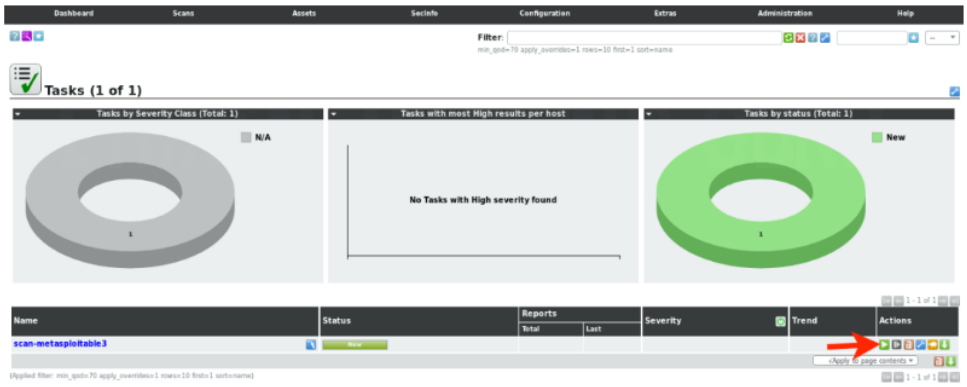


1 сурет – Google Authenticator екі сатылы аутентификация қолданбасы

Осалдықтарды бағалау.

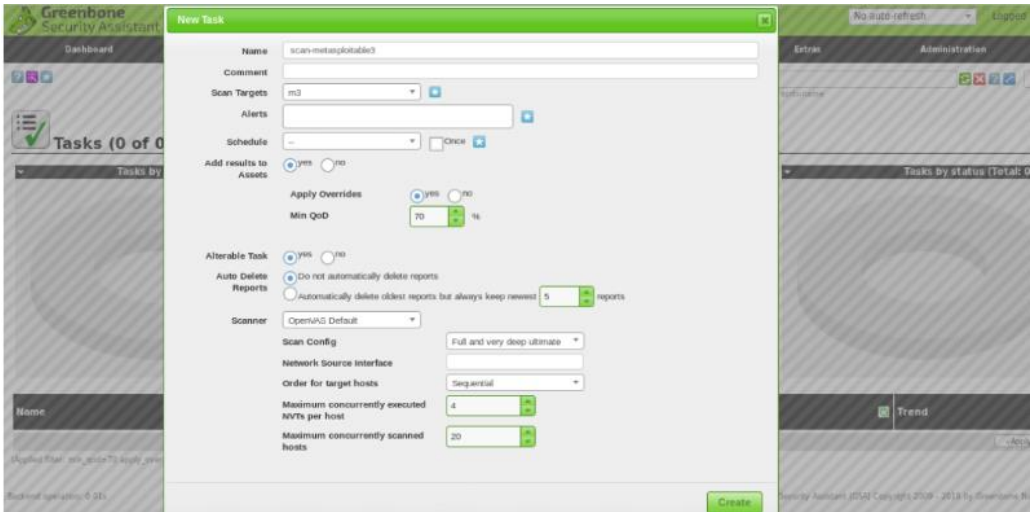
CVSS (Common Vulnerability Scoring System) – бұл жүйе, қауіпсіздік осалдықтарының ауырлығын бағалауға арналған ашық және стандартталған әдістеме. OpenVAS – бұл ашық бастапқы кодты осалдықтарды сканерлеу жүйесі, ол CVSS стандарттарын қолданады және желілік құрылғылар мен серверлердегі осалдықтарды анықтауға көмектеседі. OpenVAS жұмысын 2 суреттен көруге болады.

Qualys – бұл тағы бір осалдықтарды сканерлеу және басқару құралы, ол жүйелерді автоматты түрде сканерлеп, анықталған қауіптер туралы толық есеп береді.



2 сурет – OpenVas интерфейсі

Сканерлеу нәтижелерін қарап шыққаннан кейін табылған осалдықтарды талдау және түзету қажет. Нәтижелер әр осалдық үшін егжей-тегжейлі ақпаратты, сондай-ақ түзету бойынша ұсыныстарды қамтиды (3 сурет).



3 сурет – OpenVas қолдану процесі

Желілік қауіпсіздік.

SSH (Secure Shell) – бұл қашықтан серверлермен қауіпсіз байланыс орнатуға арналған протокол. SSH байланысы шифрланған, сондықтан деректерді ұрлауды немесе байланысқа араласуды қиындатады.

DMZ (Demilitarized Zone) – бұл желілік архитектурада ішкі желіні сыртқы қауіптерден қорғау үшін қолданылатын әдіс. DMZ ішкі желі мен сыртқы желі (интернет) арасында орналасады және оған тек қажетті сервистер ғана қойылады.

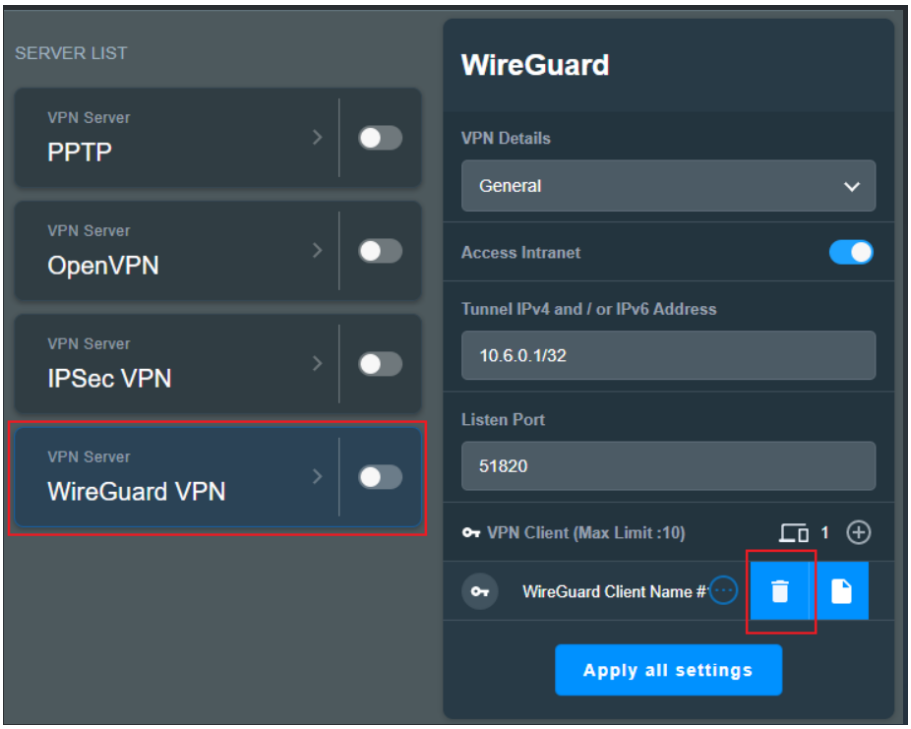
Брандмауэр – бұл желі трафигін бақылау және рұқсат етілген және рұқсат етілмеген трафикті ажырату үшін қолданылатын құрылғы немесе бағдарлама. Брандмауэр ішкі желіні сыртқы шабуылдардан қорғауда қажетті рөл атқарылады.

IDS және IPS.

IDS (Intrusion Detection System) – бұл жүйе желі трафигін бақылап, күдікті әрекеттерді анықтайды. IPS (Intrusion Prevention System) – бұл IDS жүйесінің жалғасы, ол тек анықтап қана қоймай, сонымен бірге шабуылдарды автоматты түрде тоқтатады. Мысалы, Snort – бұл ашық бастапқы коды бар IDS жүйесі, ал Suricata IDS және IPS функцияларын біріктіреді.

VPN.

VPN (Virtual Private Network) – бұл жалпыға ортақ желілер арқылы қауіпсіз байланыс орнатуға мүмкіндік беретін технология. VPN желісі арқылы жіберілетін барлық деректер шифрланады, бұл желілік трафиктің қауіпсіздігін қамтамасыз етеді. Мысалы, OpenVPN және WireGuard – бұл танымал VPN шешімдері. WireGuard VPN жұмысы 4 суретте көрсетілген.



4 сурет – WireGuard интерфейсі

Security Live CD.

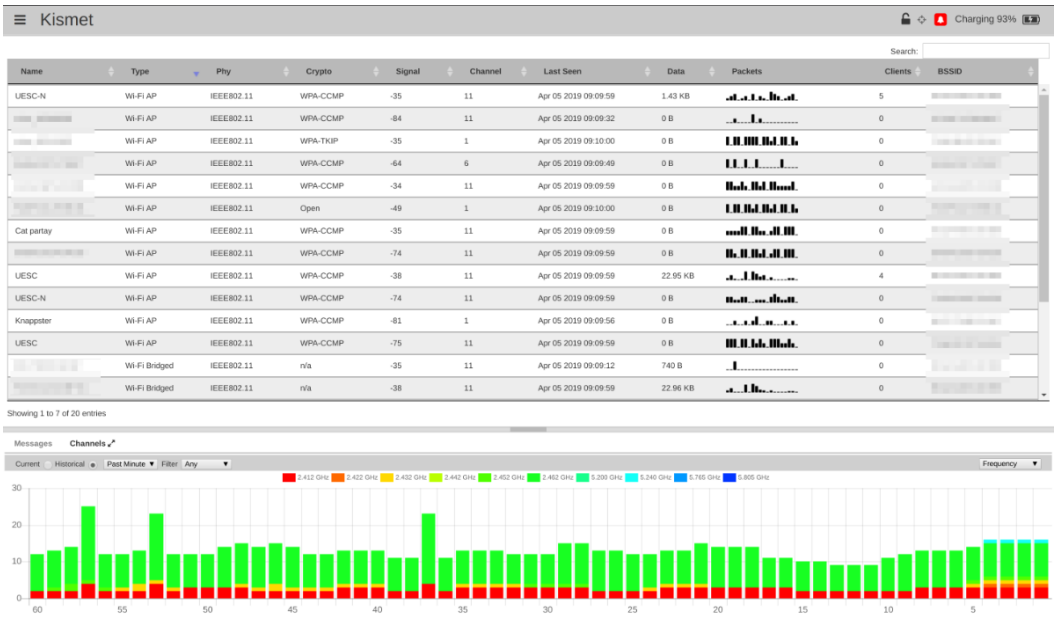
Security Live CD – бұл желілік қауіпсіздікті талдау және диагностика жасауға арналған арнайы құралдар жиынтығы бар жүктелетін диск. Мысалы, Kali Linux – бұл ақпараттық қауіпсіздік мамандарына арналған танымал Security Live CD болып табылады.

Қосымша құралдар ретінде келесі құрылғыларды қолдануға болады:

– Kismet – сымсыз желілерді қорғауға арналған құрал. Ол желідегі аномалияларды анықтап, қауіптер туралы ескертеді (5 сурет);

– Scapy – желілік трафикті талдауға және брандмауэр ережелерін тестілеуге арналған қуатты құрал;

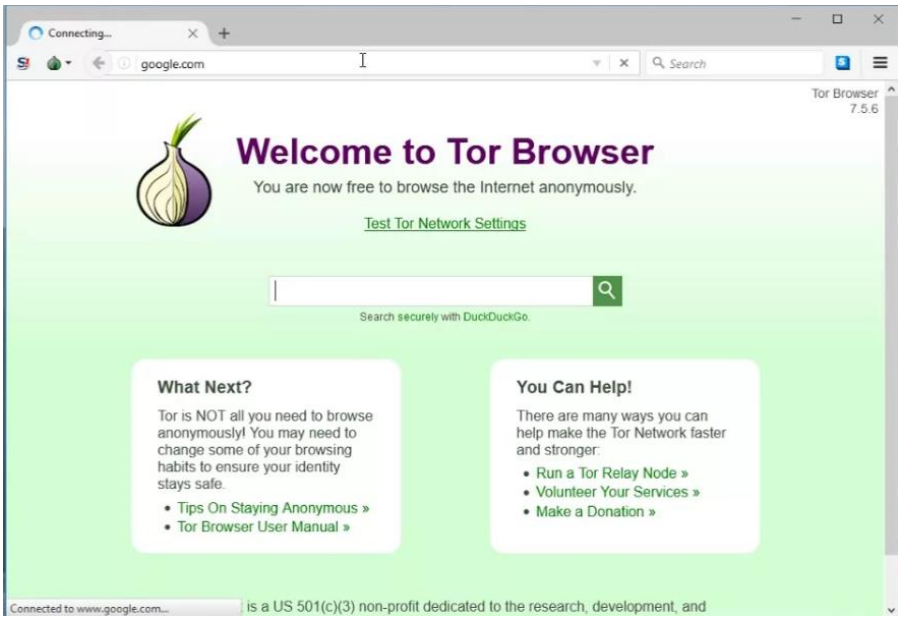
– AppLocker – қосымшаларды блоктауға және жүйеде рұқсат етілмеген бағдарламалардың жұмысын шектеуге мүмкіндік беретін құрал.



5 сурет – Kismet интерфейсі

Желінің анонимділігі.

Желінің анонимділігі – бұл интернеттегі қолданушының орналасқан жерін және жеке басын жасыру процесі. Бұл мақсатта анонимді прокси– серверлер, VPN қызметтері және Tor желісі қолданылады. Tor желісінің интерфейсі 6 суретте көрсетілген. Tor – анонимділікті қамтамасыз ету үшін қолданылатын желі, ол интернет трафигін көптеген серверлер арқылы бағыттайды [2].



6 сурет – Tor желісінің интерфейсі

Нәтижелер.

IoT жүйелерінде қауіпсіздікті қамтамасыз ету үшін құрылғылардың физикалық қауіпсіздігінен бастап деректердің құпиялылығын басқаруға дейінгі барлық деңгейлерді қамтитын әртүрлі технологиялар мен қорғаныс әдістерін кешенді пайдалану қажет.

Тұрақты жаңартулар, қолданушыларды оқыту және ең жақсы тәжірибелерді енгізу IoT жүйелерін қорғаудың тиімді стратегиясының негізгі элементтері болып табылады.

Нақты шешімдердің мысалдары:

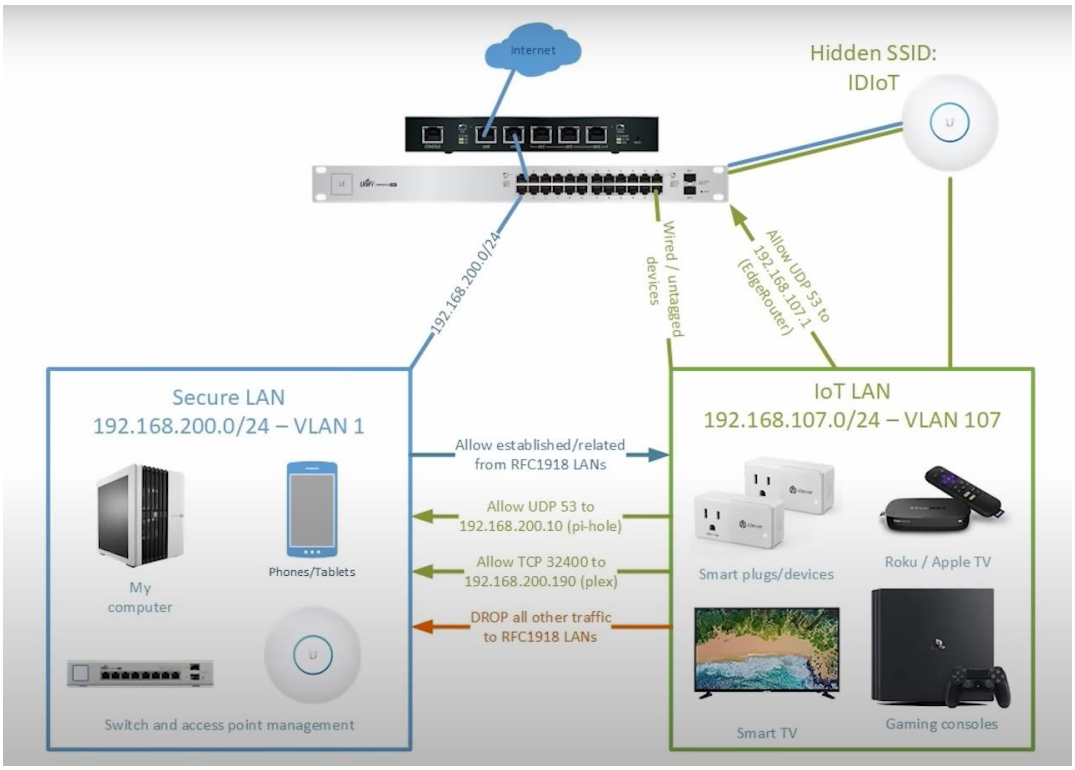
– Cisco IoT Threat Defence – аутентификация, шифрлау және желілік белсенділікті бақылауды қамтитын кешенді шешім;

– Microsoft Azure Sphere – қорғалған микроконтроллерді, операциялық жүйені және бұлтты қауіпсіздік қызметтерін қамтитын қорғалған IoT құрылғыларын әзірлеуге және орналастыруға арналған платформа;

– AWS IoT Device Defender – құрылғы қауіпсіздігі конфигурациясының аудиті, көрсеткіштерді бақылау және ауытқуларды анықтау функцияларын ұсынатын қызмет [3].

Интернет заттарының қауіпсіз конфигурациясы ретінде, IoT жеке компьютерде немесе негізгі желіге қосылған желілік жабдыққа қол жеткізе алмайтындай етіп, өздерінің IoT желісінде оқшауланған құрылғылардың мысалында талданады. (7 сурет).

Зерттеу барысында интернетке кіру мүмкіндігі және Edge маршрутизаторы бар жағдай қарастырылады, маршрутизатор Unify24 қосқышына қосылып, UAP AC pro–ға жалғанады. Қауіпсіз жергілікті желі VLAN1, дәл осы жерде желі қосқыштармен, кіру нүктелерін толық басқарады. Интернет заттарының жергілікті желісі VLAN107-ге, желідегі IoT құрылғылардың барлығы енеді. IoT құрылғыларды анықтау үшін жасырын SSID интернет заттарының идентификаторы пайдаланылғандықтан, қосылатын желіні табу үшін телефонда іздесеңіз аталған желіні көрмейсіз, сондықтан құрылғыларға қосылу үшін параметрлерді қолмен жазып енгізу керек.



7 сурет – Интернет заттарының қауіпсіз желісі

IoT желісі мен жергілікті желіні үйлестіру үшін, брандмауэр ережелерін тағайындау қажет:

– орнатылған және онымен байланысты трафикке кез келген жеке жергілікті желіден IoT аумағына кіруге рұқсат беру, сондықтан RFC1918 жеке жерүсті желісінің ауқымын қосу керек. Бұл ереже екі жақты байланыс үшін қолданылады;

– негізгі және қосымша DNS қажет болған жағдайда DNS іздеу жүйесін басқару. Зерттеу барысында негізгі порт 192.168.200.10 мекен жайында орналасты, сондықтан басқа желідегі порттарға қосылу үшін udp 53 портын ашуға тура келеді, желі міндетті түрде pie hole немесе DNS үшін емес, кез келген құрылғы үшін бапталады;

– барлық басқа трафикті өшіру. Барлық трафик өшіріледі, дегенмен udp 53–ке қосалқы DNS серверіне арналған Edge маршрутизаторына рұқсат беріледі, себебі, егер pi–hole сервер жауап бермесе немесе желіден тыс болса, екінші DNS сервер, құрылғыларға DHCP IP мекенжайын алуға мүмкіндік тудырады.

Талқылау.

IoT құрылғылары барған сайын кең таралып, онымен бірге қауіпсіздік тәуекелдері де артуда. Сол себепті IoT құрылғыларын қорғау үшін келесі нақты қадамдар жасалуы керек.

Алдымен, құрылғыларды сақтықпен таңдау қажеттілігі туындайды. Сенімді өндірушілерден сатып алынған құрылғылар қауіпсіздіктің жоғары сапасын қамтамасыз етіп, бағдарламалық жасақтаманы үнемі жаңартып отырады. Әрбір сатып алудан бұрын, құрылғының шифрлау, аутентификация және автоматты жаңарту сияқты қауіпсіздік мүмкіндіктерін қолдайтынына көз жеткізу қажет. Алдын ала орнатылған құпия сөздері бар құрылғылардан аулақ болу керек, сондықтан құрылғыны алғаннан кейін стандартты құпия сөз бірден сенімді етіп өзгертілуі қажет.

Желі қауіпсіздігін қамтамасыз ету келесі қажетті қадам болып табылады. IoT құрылғылары үшін бөлек желі жасалды, бұл оларды негізгі желіден оқшаулауға мүмкіндік береді. Аталған әдіс бұзылған жағдайда негізгі желіге ықтимал шабуылдардың алдын алуға көмектеседі. Wi-Fi желісі үшін күрделі және бірегей құпия сөз қолданылды, ал брандмауэр құрылғыларға рұқсатсыз кіруді блоктауға көмектесетін қажетті құрал болады.

Бағдарламалық жасақтаманы жаңарту үнемі жүзеге асырылды. Құрылғылар автоматты түрде жаңартуларды жүктеп-орнатуға конфигурацияланды. Автоматты жаңартуларды қолдамайтын құрылғылар үшін қол жетімді жаңартулар үнемі тексеріліп, қолмен орнатылады.

Күшті құпия сөздерді пайдалану басты назарда болуы қажет. Әртүрлі құрылғылар үшін әртүрлі құпия сөздер қолданылып, бір құрылғы үшін көптеген құпия сөздің қолданылуы қатаң сақталды.

Сақтық шаралары әрқашан басты назарда болу қажет. Фишингтік шабуылдардан сақ болу қажеттілігі түсіндірілді, тіркелгі деректерін алуға немесе зиянды сілтемелерді басуға тырысуы мүмкін электрондық пошталар мен мәтіндік хабарламалардан сақ болу ұсынылды. Белгісіз жіберушілерден келген күдікті тіркемелер немесе сілтемелер ешқашан ашылмауы қажет, ал құрылғылардың ерекше әрекеттері немесе жұмысындағы өзгерістер мұқият бақыланды.

Қосымша қауіпсіздік құралдарын пайдалану арқылы қорғау күшейтілді. Антивирустық бағдарламалық жасақтама құрылғыларды зиянды бағдарламалардан қорғауға арналған, VPN интернет трафикті шифрлауға және құпиялылықты қорғауға көмектесті. Қажетсіз мүмкіндіктер өшіріліп, ықтимал осалдықтар азайтылды [4].

Қорытынды.

IoT қауіпсіздігінің болашағы перспективті болып көрінеді, өйткені сала айтарлықтай өсуді күтуде және блокчейн сияқты жаңа технологиялар құпиялылық пен қауіпсіздікті жақсартудың әлеуетті мүмкіндіктерін ұсынуда. Бұл дамып келе жатқан қауіптерден сенімді қорғауды және құрылғылар мен интернет заттарын қорғауды дамыту үшін зерттеулерге, бірлескен күш–жігерге және қауіпсіздік туралы хабардар ету бағдарламаларына инвестицияларды қажет етеді . Осы қауіпсіздік мәселелерін шешу IoT-

ң барлық әлеуетін ашу, тұтынушылардың сенімін арттыру және болашақ жетістіктерге жағдай жасау үшін өте қажетті.

Қазіргі заманғы IoT құрылғылары қауіпке тойтарыс беруге қауқарсыз. Бұл IoT құрылғыларының шектеулі ресурстарына, сондай–ақ әзірленген стандарттардың болмауына және аппараттық, бағдарламалық жасақтамада қауіпсіздік шараларының нашар орындалуына байланысты.

Бұл мақалада IoT қауіпсіздігі мәселелеріне талдау жасалады. IoT технологиясының компоненттері анықталды және оны қолдану салалары қарастырылды. Қауіпсіздік мәселелерін шешудің және IoT технологиясын қорғаудың түпкі мақсаты–барлық ресурстарға басымдық беру, қажетті құпиялылық деңгейін сақтау және шабуылдарға төзімділіктің жоғары деңгейіне қол жеткізу және қолдау, осылайша жан–жақты қауіпсіздікті қамтамасыз ету.

ӘДЕБИЕТТЕР

[1] Верещагина Е.А., Проблемы безопасностей интернета вещей. - Москва, 2021. –с. 26.

[2] Аверкиев А.А., Кибербезопасность виды и методы, Научно-образовательный журнал для студентов и преподавателей «StudNet» №1/2022, Ростов на Дону,2022.- с. 567.

[3] Колисниченко Д.Н., Секреты безопасности и анонимности в интернете. - Санкт-Петербург, 2020. – с.33.

[4] Интернет вещей: обзор проблем безопасности [Электрондық ресурс]. – URL: https://business-online.su/blog/internet-veshchey-problemy-bezopasnosti

REFERENCES*

[1] Vereshhagina E.A., Problemy bezopasnostej interneta veshhej, Moskva, 2021. –s. 26.

[2] Averkiev A.A., Kiberbezopasnost' vidy i metody, Nauchno-obrazovatel'nyj zhurnal dlja studentov i prepodavatelej «StudNet» №1/2022, Rostov na Donu,2022.- s. 567.

[3] Kolisnichenko D.N., Sekrety bezopasnosti i anonimnosti v internete, Sankt-Peterburg, 2020. – s.33.

[4] Internet veshhej: obzor problem bezopasnosti [Jelektrondyқ resurs]. – URL: https://business-online.su/blog/internet-veshchey-problemy-bezopasnosti

Yersaiyn Mailybayev, PhD, International University of Transport and Humanities, Almaty, Kazakhstan, ersind@mail.ru

Ruslan Madi, student, Satbayev University, Almaty, Kazakhstan, ot2011@mail.ru

ORGANIZATION OF INFORMATION PROTECTION IN IoT SYSTEMS

Abstract. The article discusses the issues of studying the organization and technologies of information security in Its systems. The purpose of the study is to identify the basics and vulnerabilities of IoT systems, analyze the principles of their operation and propose information security technologies. The basics and vulnerabilities of IoT systems are considered, as well as the basic principles of information protection. Specific examples of information protection in IoT systems, an analysis of existing solutions and recommendations on security were also given. Based on the results obtained, a comprehensive approach is proposed aimed at improving the security of IoT system.

Keywords. Information, security, IoT, vulnerabilities, network.

Ерсайын Майлыбаев, PhD, Международный транспортно-гуманитарный университет, Алматы, Казахстан, ersind@mail.ru
Руслан Мади, студент, Satbayev University, Алматы, Казахстан, ot2011@mail.ru

ОРГАНИЗАЦИЯ ЗАЩИТЫ ИНФОРМАЦИИ В СИСТЕМАХ IoT

Аннотация. В статье рассматриваются вопросы изучения организации и технологий защиты информации в системах IoT. Цель исследования-выявить основы и уязвимости систем IoT, проанализировать принципы их работы и предложить технологии защиты информации. Рассматриваются основы и уязвимости систем IoT, а также основные принципы защиты информации. Также были даны конкретные примеры защиты информации в системах IoT, анализ существующих решений и рекомендации по обеспечению безопасности. По полученным результатам предложен комплексный подход, направленный на повышение безопасности систем IoT.

Ключевые слова. информация, безопасность, IoT, уязвимости, сеть.

****

Келіп түсті: 13 мамыр 2024 ж.; қабылданды: 16 қыркүйек 2024 ж.