

İradə Muradova

Neftqazəlmətdəqiqatlayihə İnstitutu
<https://orcid.org/0009-0009-3534-4835>
iradam992@gmail.com

Elektronika və IoT cihazların təhlükəsizliyi

Xülasə

Məqalədə elektronika və Əşyaların İnterneti (IoT) cihazlarının müasir informasiya-kommunikasiya texnologiyaları mühitində rolu və təhlükəsizlik problemləri araşdırılmışdır. Elektronikanın inkişafı nəticəsində yaranan IoT cihazlarının müxtəlif sahələrdə-ağıllı evlərdə, sənayedə, nəqliyyatda və səhiyyədə geniş tətbiqi onların təhlükəsizliyini aktual problemə çevirmişdir. Məqalədə internet və rəqəmsal texnologiyaların mərhələli inkişafı izah edilmiş, IoT konsepsiyasının formalaşması və tətbiq sahələri tədqiqatçıların fikirləri əsasında təhlil olunmuşdur. Eyni zamanda IoT, Fog və Cloud mühitlərini əhatə edən kiberhücum ssenariləri nəzərdən keçirilmiş, Mirai botnet, DDoS, Man-in-the-Middle və ransomware kimi hücumların sistemlərə təsiri izah edilmişdir. Araşdırma göstərir ki, IoT cihazlarının həm fiziki, həm də kibertəhlükəsizlik baxımından zəifliyi bütün şəbəkə ekosistemi üçün ciddi risklər yaradır. Bu səbəbdən elektronika və IoT cihazlarının təhlükəsizliyinin təmin edilməsi müasir texnoloji inkişafın əsas prioritetlərindən biri kimi qiymətləndirilir.

Açar sözlər: *elektronika, əşyaların interneti, IoT cihazları, informasiya təhlükəsizliyi, kibertəhlükəsizlik, fog computing, cloud computing.*

Security of Electronics and Iot Devices

Abstract

The article examines the role and security problems of electronics and Internet of Things (IoT) devices in the modern information and communication technology environment. The widespread application of IoT devices in various fields - smart homes, industry, transportation and healthcare - as a result of the development of electronics has made their security a pressing problem. The article explains the phased development of the Internet and digital technologies, analyzes the formation of the IoT concept and its application areas based on the ideas of researchers. At the same time, cyberattack scenarios covering IoT, Fog and Cloud environments are reviewed, and the impact of attacks such as Mirai botnet, DDoS, Man-in-the-Middle and ransomware on systems is explained. The study shows that the vulnerability of IoT devices in terms of both physical and cybersecurity poses serious risks to the entire network ecosystem. Therefore, ensuring the security of electronics and IoT devices is considered one of the main priorities of modern technological development.

Keywords: *electronics, internet of things, IoT devices, information security, cybersecurity, fog computing, cloud computing.*

Безопасность электроники и устройств интернета вещей

Резюме

В статье рассматривается роль и проблемы безопасности электроники и устройств Интернета вещей (IoT) в современной информационно-коммуникационной технологической среде. Широкое применение устройств IoT в различных областях — умные дома, промышленность, транспорт и здравоохранение — в результате развития электроники сделало их безопасность актуальной проблемой. В статье объясняется поэтапное развитие Интернета

и цифровых технологий, анализируется формирование концепции IoT и областей ее применения на основе идей исследователей. Одновременно рассматриваются сценарии кибератак, охватывающие среды IoT, туманных и облачных вычислений, и объясняется влияние таких атак, как ботнет Mirai, DDoS-атаки, атаки типа «человек посередине» и программы-вымогатели, на системы. Исследование показывает, что уязвимость устройств IoT как с точки зрения физической, так и кибербезопасности представляет серьезные риски для всей сетевой экосистемы. Таким образом, обеспечение безопасности электроники и устройств Интернета вещей считается одним из главных приоритетов современного технологического развития.

Ключевые слова: *электроника, интернет вещей, устройства интернета вещей, информационная безопасность, кибербезопасность, туманные вычисления, облачные вычисления.*

Giriş

Müasir dövrdə bir sıra elm sahələri vardır ki, onlar xüsusi aktualıq kəsb edir. Elektronika elektrik cərəyanının elektronların hərəkəti vasitəsilə idarə olunmasını, ötürülməsini və emalını öyrənən elm və texnika sahəsidir. Bu sahə əsasən yarımkeçirici materiallara və elektron elementlərə əsaslanır. Elektronikanın məqsədi elektrik siqnallarını gücləndirmək, dəyişdirmək, saxlamaq və müəyyən funksiyaları yerinə yetirən qurğular yaratmaqdır.

Elektronika gündəlik həyatda geniş tətbiq olunur. Kompüterlər, mobil telefonlar, televizorlar, radio qurğuları, tibbi cihazlar, avtomobil sistemləri və ağıllı texnologiyalar elektronikanın tətbiq sahələrinə daxildir. Elektronika müasir texnologiyanın əsasını təşkil edir və informasiya mübadiləsinin sürətlənməsində, avtomatlaşdırmada və texniki tərəqqidə mühüm rol oynayır.

Qısa olaraq, elektronika elektrik enerjisindən istifadə etməklə məlumatın və proseslərin idarə olunmasını təmin edən elmi və texniki sahədir.

IoT cihazlar (Əşyaların İnterneti cihazları)-internetə qoşula bilən, ətraf mühitdən məlumat toplayan, bu məlumatları ötürən və ya əməllərə uyğun fəaliyyət göstərən elektron qurğulardır. Bu cihazlar sensorlar, proqram təminatı və rabitə texnologiyalarından istifadə edərək bir-biri ilə və ya mərkəzi sistemlə əlaqə qurur.

Əsas hissə

IoT cihazlar real obyektləri rəqəmsal sistemlərlə birləşdirir. Onlar temperatur, rütubət, işıq, hərəkət, təzyiq, səs və digər göstəriciləri ölçə bilər. Toplanan məlumatlar internet vasitəsilə serverlərə və ya bulud sistemlərinə göndərilir və orada analiz olunur. Analizin nəticəsinə əsasən IoT cihazlar avtomatik qərar qəbul edə və ya istifadəçiyə məlumat verə bilər.

IoT cihazlar ağıllı ev sistemlərində, sənayedə, kənd təsərrüfatında, səhiyyədə, nəqliyyatda və təhlükəsizlik sahələrində geniş istifadə olunur. Məsələn, ağıllı termostatlara, ağıllı sayğaclar, sensorlu işıqlandırma sistemləri və geyilə bilən ağıllı qurğular IoT cihazlara aiddir. Qısa olaraq, IoT cihazlar fiziki dünyadakı obyektləri internet vasitəsilə ağıllı və avtomatik şəkildə idarə etməyə imkan verən elektron qurğulardır.

Tədqiqatçılar Əliquliyev, R.M., Mahmudov, R.Ş qeyd edir ki, “Əşyaların İnterneti” termini 2005-ci ildə Beynəlxalq Telekomunikasiya İttifaqının analitiklər qrupunun İnternetin vəziyyətinə həsr olunmuş hesabatında işlədildikdən sonra diqqəti cəlb etməyə başladı. Həmin hesabatda Əşyaların İnternetinin potensialından səmərəli istifadə etmək üçün zəruri olan standartlaşdırma, şəxsi həyatın toxunulmazlığı, sosial-etik məsələlərin həll edilməsinin zəruriliyi qeyd edilirdi” [3, s.30].

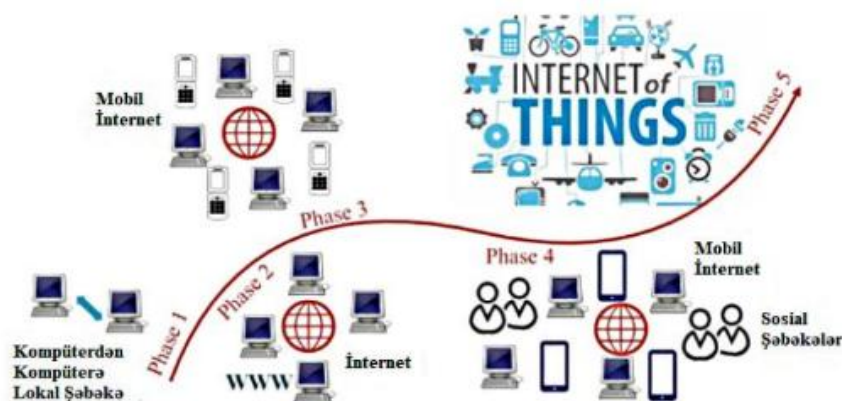
Tədqiqatçılar Balayev, R.Ə., Əlizadə, M.N., Musayev, İ.K. qeyd edirlər ki, “İlk hesablayıcı maşınlar, o cümlədən, EHM-lər, sonra isə ilk fərdi kompüterlər tək-tək, bir-biri ilə uyuşmayan nüsxələrdə hazırlandığından, Bəşəriyyəti narahat edən problemlərin həllində lazımi nəticə almaq mümkün olmadı və tezliklə ayrı-ayrı kompüterləri birləşdirib şəbəkə halına salmaq zərurəti bütün kəskinliyi ilə bu sahənin mütəxəssisləri qarşısında dayandı. Əvvəlcə ayrı-ayrı ölkələr miqyasında lokal şəbə-

kəlar və sonra qlobal şəbəkələr, sonra isə, beynəlxalq kompüter cəmiyyəti - qlobal informasiya şəbəkəsi internet yaradıldı” [2, s.20].

Tədqiqatçı A.Abdullayev qeyd edir ki, “IoT cihazları şəbəkəyə kabelsiz qoşularaq verilənləri ötürmə qabiliyyəti olan qeyri-standart hesablaşma cihazlarıdır. IoT cihazlarına termostatlar, lampalar, soyuducular, maşınlar və bu sahədə istifadə olunan digər əşyalar daxildir” [1, s. 23].

İnformasiya və kommunikasiya texnologiyalarının inkişafı insan həyatının bütün sahələrinə güclü təsir göstərmişdir. Kompüterlərin yaranması, internetin geniş yayılması və mobil texnologiyaların inkişafı nəticəsində məlumatların ötürülməsi və paylaşılması daha sürətli və əlçatan olmuşdur. Zamanla bu inkişaf təkcə insanların deyil, həm də müxtəlif cihazların bir-biri ilə əlaqə qurmasına şərait yaratmışdır. Bu proses texnologiyanın mərhələli şəkildə inkişaf etdiyini və yeni anlayışların, xüsusilə də Əşyaların İnterneti (Internet of Things – IoT) kimi konsepsiyaların ortaya çıxdığını göstərir.

İndi isə bu mərhələli inkişafı əks etdirən şəkildə baxaq.

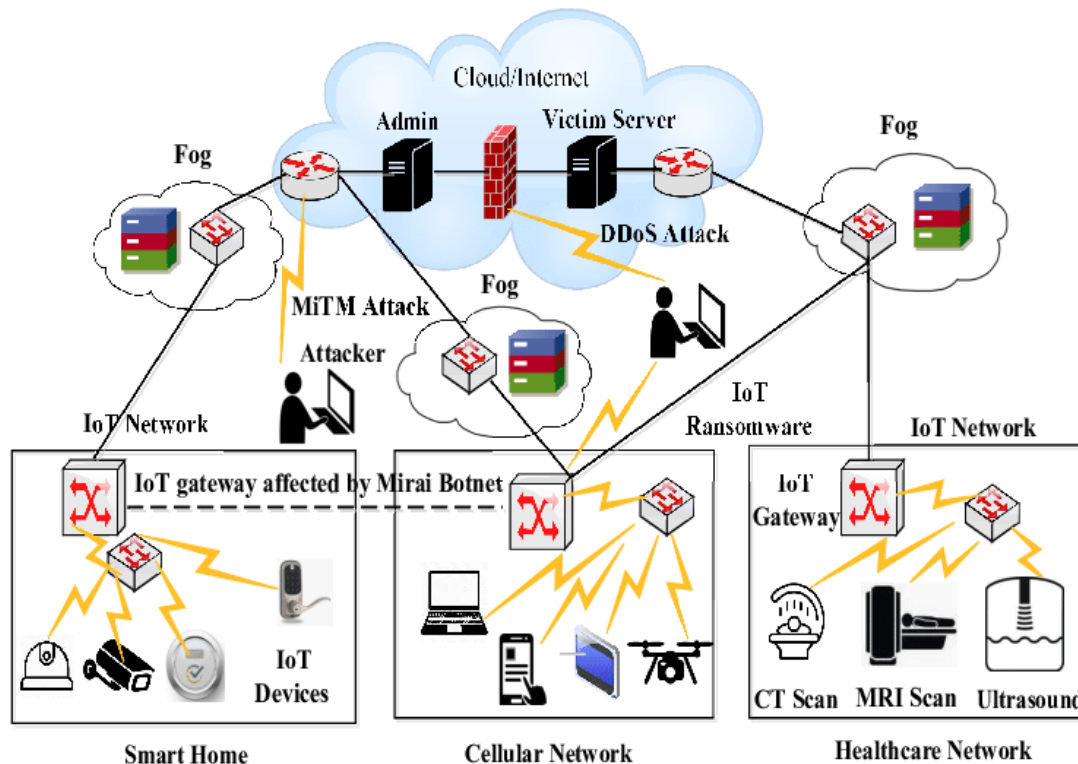


Şəkil 1. İnternet və rəqəmsal texnologiyaların inkişaf mərhələləri

Bu şəkil internetin və rəqəmsal texnologiyaların inkişaf mərhələlərini təsvir edir. Şəkildə proses ardıcıl “Phase 1”dən “Phase 5”ə qədər göstərilir.

İlk mərhələdə (Phase 1) kompüterlər əsasən lokal şəbəkələrdə bir-biri ilə əlaqə saxlayırdı. İnternet geniş yayılmamışdı və məlumat mübadiləsi məhdud idi. İkinci mərhələdə (Phase 2) WWW (World Wide Web) ortaya çıxdı və kompüterlər internet vasitəsilə qlobal şəkildə əlaqələndi. Üçüncü mərhələdə (Phase 3) mobil internet inkişaf etdi, noutbuklar və mobil cihazlar internetə qoşulmağa başladı. Dördüncü mərhələdə (Phase 4) sosial şəbəkələr ön plana çıxdı, insanlar müxtəlif cihazlar vasitəsilə bir-biri ilə daha aktiv ünsiyyət qurmağa başladılar. Beşinci mərhələdə (Phase 5) isə Əşyaların İnterneti (Internet of Things – IoT) anlayışı formalaşır: təkcə insanlar yox, gündəlik əşyalar, sensorlar və cihazlar da internetə qoşularaq bir-biri ilə məlumat mübadiləsi edir. Ümumilikdə, şəkil internetin sadə kompüter şəbəkələrindən başlayaraq, ağıllı cihazların bir-biri ilə əlaqədə olduğu müasir IoT mərhələsinə qədər keçdiyi inkişaf yolunu izah edir.

Tədqiqatçı Ş.Mansurova qeyd edir ki, “IoT konsepsiyasının tətbiq sahələri çox genişdir. Belə ki, neft və qaz sənayesi, ətraf mühitin monitorinqi, ağıllı evlər, nəqliyyatın intellektual idarəetməsi, elektron tibb və s. kimi müxtəlif sahələrdə geniş olaraq tətbiq edilə bilər. Nümunə olaraq qeyd etmək olar ki, sənaye və IoT konsepsiyasının integrasiyası nəticəsində istehsal proseslərinə cəlb olunan ağıllı cihazlar, insan xətasının minimuma endirilməsinə, real zamanda emal vasitəsilə qərar qəbulunun dəstəklənməsi sistemləri tərəfindən qiymətləndirmənin həyata keçirilməsinə nail olacaqdır. Bu isə istehsal zamanı keyfiyyətin yüksəldilməsinə, resursların optimal istismarını təmin etməklə maliyyə xərclərinin azaldılmasına, rəqabətə davamlı məhsulların istehsalına gətirib çıxaracaqdır” [6, s. 155].



Şəkil 2. Elektronika və IoT cihazların təhlükəsizliyi sxemi

Şəkil IoT, Fog və Cloud mühitlərini əhatə edən kiberhücum ssenarisini ardıcıl şəkildə təsvir edir. Sistem ən aşağı səviyyədə IoT cihazları ilə başlayır və yuxarı səviyyədə bulud serverlərinə qədər uzanır. Ən aşağı qat IoT şəbəkəsidir. Buraya ağıllı ev, mobil (cellular) şəbəkə və səhiyyə şəbəkəsi daxildir. Ağıllı ev mühitində təhlükəsizlik kameraları, ağıllı zənglər, sensorlar və digər məişət IoT cihazları mövcuddur. Bu cihazlar bir IoT gateway vasitəsilə şəbəkəyə qoşulur. Gateway zəif qorunmuş olduqda Mirai botnet tərəfindən yoluxdurulur və nəticədə evdəki bütün IoT cihazları hücum üçün istifadə edilə bilən botlara çevrilir.

Mobil və ya cellular şəbəkədə noutbuklar, serverlər, routerlər və dron kimi qurğular yerləşir. Bu qurğular IoT və Fog mühitləri arasında əlaqə yaradır. Yoluxmuş IoT gateway-lər və qurğular mobil şəbəkə üzərindən hücum trafiki ötürərək daha yüksək səviyyəli sistemlərə təsir göstərir.

Səhiyyə şəbəkəsində CT scan, MRI scan və Ultrasound kimi tibbi IoT cihazları fəaliyyət göstərir. Bu qurğular da IoT gateway vasitəsilə idarə olunur. Şəkildə bu mühitə qarşı ransomware hücumu göstərilir. Hücum nəticəsində tibbi qurğuların fəaliyyəti dayanır və məlumatlar şifrələnərək əlçatmaz olur. Bu isə səhiyyə xidmətləri üçün ciddi risk yaradır.

IoT şəbəkələri Fog computing səviyyəsinə qoşulur. Fog node-lar Cloud ilə IoT arasında aralıq rol oynayır və məlumatları lokal səviyyədə emal edir. Lakin bu qat da hücumlara açıqdır. Şəkildə Man-in-the-Middle hücumu göstərilir. Hücumçu IoT və Cloud arasında ötürülən məlumatları ələ keçirə, dəyişdirə və ya izləyə bilər.

Fog səviyyəsindən sonra sistem Cloud/Internet mühitinə keçir. Burada admin server, firewall və hədəf server yerləşir. Yoluxmuş IoT və Fog qurğularından gələn böyük həcmdə trafik Cloud səviyyəsində yerləşən victim server-ə yönəldilir. Bu proses DDoS hücumu kimi göstərilir və serverin normal fəaliyyətini dayandırır.

Şəkildə ildırım işarələri hücumların yayılma istiqamətini və zərərli trafik axını simvollaşdırır. Qara insan fiqurları isə hücumçuları ifadə edir. Hücumlar aşağı səviyyəli IoT cihazlarından başlayaraq Fog qatından keçib Cloud serverlərinə qədər ardıcıl şəkildə yayılır.

Nəticə olaraq şəkil göstərir ki, zəif qorunan IoT cihazları bütün şəbəkə ekosistemini təhlükə altına sala bilər. Bir IoT gateway-in yoluxması ağıllı evlərə, mobil şəbəkələrə, səhiyyə sistemlərinə və sonda Cloud serverlərinə qədər uzanan genişmiqyaslı kiberhücumlara səbəb olur.

Müasir dövrdə informasiya-kommunikasiya texnologiyalarının sürətli inkişafı cəmiyyətin sosial-iqtisadi strukturunda köklü dəyişikliklərə səbəb olmuşdur. Xüsusilə Əşyaların İnterneti (IoT) konsepsiyasının formalaşması istehsal, əmək münasibətləri və iqtisadi fəaliyyət modellərinə yeni yanaşmalar gətirmişdir. Bu texnoloji transformasiya hələ XX əsrin sonlarında gələcək barədə irəli sürülmüş bir sıra futurologiya nəzəriyyələrinin reallığa çevrilməyə başladığını göstərir. Məhz bu kontekstdə tədqiqatçılar Əliquliyev, R.M., Mahmudov, R.Ş qeyd edir ki, “Əşyaların İnternetinin meydana gəlməsi ilə Amerika futuroloqu E.Tofflerin vaxtilə söylədiyi “kütləvi standartlaşdırılmış istehsal informasiya texnologiyalarının tətbiq edildiyi intellektual fəaliyyətə əsaslanan yeni fərdiləşdirilmiş əmək sistemi ilə əvəz olunacaq, rəngarəng çeşidli, lakin kütləvi olmayan məhsulların istehsalı artacaq.” fikri özünü doğrultmağa başlayır. O qeyd edirdi ki, iqtisadiyyatda iri korporasiyaların hökmranlığının əvəzinə fərdi və qrup şəklində yaradıcı fəaliyyətin hər yerə yayılması və onun nəticələrinin İnternet vasitəsilə rəşional mübadiləsi baş verəcək” [3, s. 35].

Elektronika və IoT cihazların təhlükəsizliyi cihazların həm fiziki, həm də məlumat baxımından qorunmasını təmin edən geniş bir sahədir. Elektronika cihazlarının təhlükəsizliyi cihazların zədələnmədən, qısaqapanmadan, yanğın və elektromaqnit müdaxilələrindən qorunmasını əhatə edir. Bu tədbirlər cihazların düzgün işləməsini, uzunömürlülüynü və istifadəçilərin təhlükəsizliyini təmin edir. Məsələn, elektrik gərginliyinin normadan yüksək olması, qısaqapanmalar və ya cihazın mexaniki zədələnməsi ciddi problemlərə və hətta yanğın təhlükəsinə səbəb ola bilər. Buna görə cihazların hazırlanmasında material seçimi, qoruyucu lövhələr və təhlükəsizlik mexanizmləri mühüm rol oynayır.

IoT cihazlarının təhlükəsizliyi isə həm fiziki, həm də kibertəhlükələrə qarşı yönəlib. Bu cihazlar internetə qoşulduğu üçün məlumat sızması, haker hücumları və icazəsiz giriş kimi risklər daşıyır. Təhlükəsizlik tədbirləri bu riskləri minimuma endirmək üçün tətbiq olunur. Belə tədbirlər arasında məlumatların şifrələnməsi, güclü şifrələrin istifadəsi, cihazların proqram təminatının müntəzəm yenilənməsi və istifadəçi identifikasiyası sistemləri yer alır. Bundan əlavə, IoT cihazları tez-tez bulud sistemləri və digər cihazlarla əlaqə qurduğundan şəbəkə təhlükəsizliyi də xüsusi əhəmiyyət kəsb edir.

Əlavə olaraq, IoT cihazlarının təhlükəsizliyi yalnız cihazların özünü qorumaqla kifayətlənmir, eyni zamanda istifadəçi məlumatlarının məxfiliyini və təhlükəsizliyini təmin edir. Məsələn, ağıllı ev sistemləri və ya tibbi cihazlar vasitəsilə toplanan şəxsi məlumatlar yanlış əllərə keçərsə, ciddi risklər yarana bilər. Ona görə də, həm istehsalçılar, həm də istifadəçilər təhlükəsizlik qaydalarına riayət etməlidir.

Nəticə

Elektronika və IoT cihazların təhlükəsizliyi onların fiziki və rəqəmsal müdafiəsini, məlumatların qorunmasını və etibarlı işləməsini təmin edən kompleks tədbirlər sistemidir. Bu, cihazların funksionallığını qoruyur, kibertəhlükələrdən və zədələnmələrdən qoruyur, həmçinin istifadəçilərin təhlükəsizliyini təmin edir.

Aparılan təhlil göstərir ki, elektronika və Əşyaların İnterneti (IoT) texnologiyaları müasir informasiya cəmiyyətinin formalaşmasında mühüm rol oynayır və demək olar ki, bütün sahələrdə – sənaye, səhiyyə, nəqliyyat, kənd təsərrüfatı, təhlükəsizlik və gündəlik məişətdə geniş tətbiq olunur. Elektronikanın inkişafı və IoT cihazlarının şəbəkə üzərindən qarşılıqlı əlaqəsi texnoloji proseslərin avtomatlaşdırılmasını, real vaxt rejimində məlumatların toplanmasını və daha səmərəli qərarqəbul etməni mümkün etmişdir.

Lakin bu texnoloji üstünlüklərlə yanaşı, elektronika və IoT cihazlarının təhlükəsizliyi məsələsi xüsusi aktualıq kəsb edir. Tədqiqat nəticələri göstərir ki, IoT cihazlarının internetə qoşulması onları kibertəhlükələrə, icazəsiz girişlərə, məlumat sızmalarına və sistem manipulyasiyalarına açıq hala gətirir. Eyni zamanda, elektron qurğuların fiziki təhlükəsizliyi-elektrik riskləri, elektromaqnit təsirlər və mexaniki zədələnmələr-nəzərə alınmadıqda həm cihazların etibarlılığı, həm də istifadəçilərin təhlükəsizliyi üçün ciddi təhdidlər yarana bilər.

Bu baxımdan, elektronika və IoT təhlükəsizliyi yalnız texniki məsələ deyil, kompleks yanaşma tələb edən multidissiplinar bir sahə kimi çıxış edir. Təhlükəsizliyin təmin edilməsi üçün fiziki müdafiə

mexanizmləri ilə yanaşı, proqram təminatının mütəmadi yenilənməsi, məlumatların şifrələnməsi, identifikasiya və autentifikasiya mexanizmlərinin tətbiqi, eləcə də istifadəçi maarifləndirilməsi mühüm əhəmiyyət daşıyır. Xüsusilə şəxsi və həssas məlumatların emalı ilə bağlı IoT sistemlərində məxfilik və etik prinsiplərin qorunması prioritet istiqamət olmalıdır.

Nəticə etibarilə, elektronika və IoT cihazlarının təhlükəsizliyinin təmin edilməsi bu texnologiyaların davamlı inkişafı və cəmiyyət tərəfindən etibarlı şəkildə qəbul olunması üçün əsas şərtlərdən biridir. Gələcək tədqiqatlar IoT təhlükəsizliyinin standartlaşdırılması, milli və beynəlxalq normativ-hüquqi mexanizmlərin təkmilləşdirilməsi, eləcə də süni intellekt əsaslı təhlükəsizlik həllərinin tətbiqi istiqamətində aparılmalıdır. Bu yanaşma həm texnoloji risklərin azaldılmasına, həm də rəqəmsal transformasiyanın təhlükəsiz və səmərəli şəkildə həyata keçirilməsinə töhfə verəcəkdir.

Ədəbiyyat

Azərbaycan dilində

1. Abdullayev, A. IoT cihazlarının təhlükəsizliyi // İnformasiya təhlükəsizliyi jurnalı. – 2017. – № 1. – S. 23–26.
2. Balayev, R.Ə., Əlizadə, M.N., Musayev, İ.K. İntellektual sistemlər və texnologiyalar: dərs vəsaiti. – Bakı: MSV nəşr, 2016. – 256 s.
3. Əliquliyev, R.M., Mahmudov, R.Ş. Əşyaların İnterneti: mahiyyəti, imkanları və problemləri, İnformasiya cəmiyyəti problemləri, 2011, №2(4), s.29-40.
4. Həşimov, M. Əşyaların İnternetinin təhlükəsizlik məsələləri // “İnformasiya təhlükəsizliyinin aktual problemləri” III respublika elmi-praktiki seminarının materialları. – Bakı: AMEA İnformasiya Texnologiyaları İnstitutu, 2017. – 8 dekabr. – S. 108.
5. Qanbayev A., Əliyev R. IoT təhlükəsizliyi: əsaslar, analiz və praktik təcrübələr. – Bakı, 2025. – 234 s.
6. Mansurova Ş. IoT arxitekturasının səviyyələr üzrə təhlükəsizlik məsələləri // İnformasiya təhlükəsizliyinin aktual multidissiplinar elmi-praktiki problemləri: IV respublika konfransının materialları (14 dekabr 2018-ci il). – Bakı, 2018. – S. 155–157.

İngilis dilində

7. Fernandez, E. Security Patterns in Internet of Things Systems. Elsevier, 2021. ISBN 978-0-12-819605-3.
8. Park, J. Cyber Security in IoT Networks: Threats, Attacks, and Countermeasures. CRC Press, 2022. ISBN 978-1-032-15238-7.
9. Sharma, R., Kumar, P. IoT-Based Cyber Attacks and Defense Strategies. Wiley, 2023. ISBN 978-1-119-87342-2.
10. Sun, Y., Song, H., Jara, A. Internet of Things Security: Principles and Technologies. CRC Press, 2018. ISBN 978-1-4987-4692-4.
11. Wang, C., Lee, S. IoT-Based Smart Security and Privacy Protection Systems. Springer, 2021. ISBN 978-981-16-0401-3.
12. Weber, R. Internet of Things: Legal Aspects, Security, and Privacy. Springer, 2020. ISBN 978-3-030-61264-2.