Əşyaların İnternetinin bəzi təhlükəsizlik problemləri

Rasim Mahmudov

AMEA İnformasiya Texnologiyaları İnstitutu

rasimmahmudov@gmail.com

***Xülasə*— Tədqiqat işində Əşyaların İnterneti ilə bağlı mövcud təhlükələr araşdırılır. O cümlədən, informasiya təhlükəsizliyi, fərdi məlumatların qorunması məsələlərinə baxılır. Bu sahədəki problemlər şərh olunur və həlli yolları göstərilir.**

Açar sözlər— Əşyaların İnterneti; RFID; informasiya təhlükəsizliyi; fərdi məlumatlar

I. GİRİŞ

İnternetin növbəti inkişaf mərhələsində bu qlobal şəbəkənin imkanlarının hədsiz dərəcədə genişləndirilməsi və onun mahiyyətində əsaslı dəyişikliklərin baş verəcəyi gözlənilir. İnternetin növbəti inkişaf mərhələsində isə bizi əhatə edən bütün faydalı əşya və predmetlərin (məişət avadanlıqlarının, elektrik cihazlarının, gündəlik istehlak mallarının, nəqliyyat vasitələrinin, istehsal qurğularının, əmək alətlərinin, informasiya daşıyıcılarının, tibbi ləvazimatların, mühafizə və nəzarət sistemlərinin, bitki və heyvanat aləminin) bu qlobal şəbəkəyə qoşulması, Əşyaların İnternetinin (*Internet of things – IoT)* yaradılması gözlənilir.

Əşyaların İnternetində təkcə insanlarla əşyalar arasında deyil, həmçinin əşyaların öz aralarında da qarşılıqlı əlaqələrin qurulması nəzərdə tutulur. Əşyaların İnterneti hamı üçün əlyetərli olan adi İnternet qovşaqlarından və qeyri-məhdud sayda xüsusi şəbəkədən (Əşyaların İntranetindən) ibarət olacaq [1].

Əşyaların İnterneti – kompyuter, İnternet və mobil telefon rabitəsindən sonra informasiya texnologiyaları sənayesinin növbəti inqilabi inkişaf mərhələsi kimi xarakterizə olunur. Bu konsepsiyasının reallaşacağı təqdirdə isə yaxın gələcəkdə bizi əhatə edən bütün faydalı əşyalar İP ünvanına malik olacaq.

Proqnozlara görə, bir neçə ildən sonra Əşyaların İnterneti hər yerdə və hərtərəfli şəkildə insanların həyat tərzinə daxil olaraq, onu əhəmiyyətli dərəcədə dəyişəcək. Əşyaların İnternetinin istifadəçilərinin sayı 2 milyard nəfərə, bu şəbəkənin hesabına əldə edilən illik gəlirin həcmi isə 800 milyard dollara çatacaq [2]. *Gartner* analitik şirkəti iddia edir ki, 2020-ci ilə qədər Əşyaların İnternetinə 26 milyard obyekt və qurğu qoşulacaq [3].

Əşyaların İnternetinin reallaşdırılması ilə cəmiyyətdəki bir sıra mühüm problemlərin həlli gözlənilir. O cümlədən, tibbi xidmətlərin keyfiyyətinin yüksəldilməsi, ictimai təhlükəsizliyin daha etibarlı şəkildə təmin edilməsi, idarəetmə proseslərinin təkmilləşdirilməsi məsələləri öz həllini tapacaq. Bütövlükdə, Əşyaların İnterneti texnologiyalarının uğurla reallaşdırılması insanların həyat şəraitinin yaxşılaşdırılmasına, yeni və daha əlverişli iş yerlərinin açılmasına, biznes üçün yeni imkanların yaranmasına, istehsalda məhsuldarlığın və rəqabətədavamlılığın artmasına gətirib çıxaracağı gözlənilir.

Əşyaların İnterneti konsepsiyasının hərtərəfli tətbiqi nəticəsində insanların, cəmiyyətin sosial-psixoloji durumunun da ciddi şəkildə dəyişəcəyi gözlənilir. Belə ki, gündəlik məişət həyatında Əşyaların İnterneti qovşaqlarından ibarət olan intellektual əşyalarla təmasda olan insanların yeni dəyərlər sisteminin formalaşması gözlənilir. Bu intellektual mühitə uyğunlaşmaq, burada uğur qazana bilmək üçün insanlardan yeni spesifik bilik və vərdişlər tələb olunacaq.

Lakin Əşyaların İnterneti vəd etdiyi bir sıra üstünlüklərlə yanaşı, ciddi problemlər də yarada bilər. Həmin problemləri həll etmədən bu konsepsiyanı uğurla tətbiq etmək, onun üstünlüklərindən faydalanmaq mümkün deyil. İnternetin tənzimlənməsi ilə bağlı mövcud olan problemlərin əksəriyyəti Əşyaların İnterneti üçün də xarakterikdir. İnformasiya təhlükəsizliyni, fərdi məlumatların qorunması kimi məsələlər həll edilmədən bu şəbəkənin uğurlu fəaliyyəti mümkün deyil.

II. İNFORMASİYA TƏHLÜKƏSİZLİYİNİN TƏMİN EDİLMƏSİ PROBLEMLƏRİ

Aparılan müxtəlif tədqiqatlar göstərir ki, Əşyaların İnterneti şəbəkələrində və qurğularında informasiya təhlükəsizliyi təmin olunmayıb, bu sahədə ciddi boşluqlar mövcuddur.

Məsələn, terrorçular göndərilən siqnallarla nəqliyyat vasitələrinin doğru qrafikini pozaraq, onların bir-biri ilə toqquşmasına səbəb ola bilərlər. Həmçinin sistemdəki təsadüfi qüsurlar və ya qəsdən yaradılan problemlər kredit kartındakı hesabı dəyişdirə, avtomobilin hərəkətini məhdudlaşdıra, vətəndaşın öz evinə daxil olmasına əngəl törədə, əmtəə haqqındakı zəruri məlumatların itməsinə səbəb ola bilər.

ABŞ-ın Mərkəzi Kəşfiyyat İdarəsinin 2008-ci il üçün hesabatında Əşyaların İnterneti yaxın gələcəyin (2025-ci ilə qədər olan dövr üçün) potensial təhlükəli texnologiyalarından biri kimi göstərilir. Əşyaların İnternetinin yaratdığı təhlükələr sırasında terrorizm, şəxsi həyatın və müxtəlif konfidensial informasiyanın qorunması qeyd edilir. Hesabatda o da vurğulanır ki, 2035-ci ildən sonra Əşyaların İnternetindən təhlükəsiz istifadə edilə bilər. Yəni bu qurum ümid edir ki, həmin vaxta kimi Əşyaların İnterneti konsepsiyasındakı təhlükə yaradan boşluqlar aradan qaldırılacaq [1].

Amsterdam Universitetinin tədqiqatçıları Əşyaların İnternetinin əsas texnoloji platformalarından biri olan *RFID* çiplərinin virusa yoluxmuş variantını yaradaraq sübut ediblər ki, bu qurğular olduqca kiçik yaddaş həcminə malik olsalar da, bədniyyətli müdaxilələrə qarşı davamlı deyillər. Yəni virusa yoluxmuş *RFID*-çip yanlış informasiya verə bilər, yaxud

ümumiyyətlə, öz fəaliyyətini dayandırar. Belə bir şəraitdə onun qurulduğu sistemlərdə hansı katastrofik halların baş verməsini təsəvvür etmək çətin deyil [4].

Böyük Britaniyanın *BBC* telekanalı da Əşyaların İnternetinin təhlükəsizlik səviyyəsini yoxlamaq üçün bir eksperiment aparmışdır: Şirkət informasiya təhlükəsizliyi üzrə 7 mütəxəssisi bir "ağıllı" evə dəvət edir. Mütəxəssislər bir neçə saat ərzində evdəki qurğuların hamısını sıradan çıxarmağa müvəffəq olurlar [1].

Hewlett-Packard (HP) şirkətinin 2014-cü ildə apardığı tədqiqatın nəticələrinə görə, İnternetə qoşulan əşyaların 70%-nin qurğularında onların sahibləri üçün təhlükələr yarada biləcək ciddi boşluqlar mövcuddur [5].

Yoxlanılan hər bir qurğuda orta hesabla 25 müxtəlif boşluq aşkarlanmışdır. O cümlədən şifrələnməmiş şəbəkə servisləri, təhlükəsizliyi təmin edilməyən interfeys, konfidensial informasiyanın əlyetərli olması, proqram təminatının mühafizəsinin, autentifikasiyanın yetərli olmaması müəyyən edilmişdir.

Belə bir şəraitdə kibercinayətkarlar bu qurğuların iş prinsipini, çatışmazlıqlarını öyrənirlər və onları "sındırmağın" yollarını tapırlar.

Amerikalı tədqiqatçılar K.Rezendes və D.Stivenson bu problemin ciddiliyini göstərmək üçün qeyd edirlər ki, hazırda bu ölkədə kritik infrastrukturun (elektrik şəbəkəsi, neft-qaz kəmərləri, körpülər, tunellər və s.) 85%-i özəl sektorda cəmləşib. Bu sektorda informasiya təhlükəsizliyi fraqmentləşdirilib və eyni səviyyədə deyil. Yəni bu sahədə vahid siyasət həyata keçirilmir. Həmin bazarlar isə hazırda xərclərin xeyli azaldılmasını və məhsuldarlığın əhəmiyyətli dərəcədə artırılmasını vəd edən Əşyaların İnternetini aktiv şəkildə tətbiq etməkdə çox maraqlıdır. Belə bir şəraitdə kritik infrastrukturun fəaliyyəti böyük risklərlə bağlıdır [6].

Qeyd etmək lazımdır ki, Əşyaların İnterneti texnologiyaları hələ tam formalaşmayıb. Amma bu texnologiyanın arxitekturu *Bluetooth*-a çox yaxındır. Ona görə də hər iki texnologiyanın problemləri də oxşardır. İnsanların sıx olduğu yerlərdə hərəkət edərkən kənar qurğuların istifadəçinin *Bluetooth*-u ilə əlaqə saxlamaq cəhdlərinə nəzarət etmək praktiki olaraq mümkün deyil. Ona görə də istifadəçilərə tövsiyə olunur ki, belə yerlərdə *Bluetooth*-u söndürsünlər. Amma heç kim zəmanət vermir ki, istifadəçi evdə olarkən hansısa bədniyyətli xüsusi antenlərin köməyi ilə kənardan *Bluetooth*-a, sensoru, yaxud verilənləri toplayan qurğuya daxil ola bilməsin [7].

Əşyaların İnternetinin əsas təhlükəsizlik problemlərindən biri aktiv və passiv qurğuların – baza stansiyalarının və kliyent avadanlıqlarının bir-birindən fərqlənməsi ilə bağlıdır. Məlumdur ki, bədniyyətlilər həmişə passiv və az intellektual olan qurğulara "girişirlər" (məsələn, zəif şifrələmə alqorimini "sındırmaq" üçün). Çox böyük ehtimalla, Əşyaların İnterneti üçün elektron komponentlər istehsal edənlər uyğunluq üçün çatışmazlıqları məlum olan köhnə protokollardan istifadə edirlər ki, bu da "sındırmanı" asanlaşdırır.

Əşyaların İnterneti şəbəkələrinə edilən hücumlardan qorunmanın əsas metodu kənar qurğuların müdaxiləsindən qorunmağa imkan verən asimmetrik kriptoqrafiyaya əsaslanan şifrələmədir.

Əşyaların İnternetinin elektrik xətləri üzərində qurulan kommunikasiyaya əsaslanan naqil hissəsi də təhlükəsiz deyil. Belə ki, elektrik şəbəkələri ilə ötürülən verilənləri izləmək asandır. Çünki qollara ayrılan elektrik şəbəkəsi yaxşı antendir. Ona görə də şəbəkə üzrə ötürülən verilənləri mənzil və ya ofisdən kənarda ələ keçirmək mümkündür [6].

Qeyd etmək lazımdır ki, Əşyaların İnternetinin əsas məqsədlərindən biri müxtəlif avtomatlaşdırılmış qurğular arasında qarşılıqlı əlaqə infrastrukturunu yaratmaqdır. Bu cür əlaqə "maşın-maşın" (*M2M*) adlanır və qərarların qəbulu zamanı insanın iştirakını istisna edir. Bu halda kompüter, planşet və ya smartfon müxtəlif qurğuları idarə etmək üçün pult rolunda çıxış edir. Qurğular insandan başlanğıc əmrini aldıqdan sonra müstəqil şəkildə fəaliyyət göstərirlər. TCP/IP protokolları ilə işləmək üçün bütün bu qurğularda quraşdırılan prosessorlar evin, təşkilat ofisinin, yaxud ticarət mərkəzinin daxilində əmrlərin vahid informasiya mübadiləsi sistemində ötürülməsini təmin edirlər [7].

Hazırda idarəetmə komandalarının mübadiləsi üçün *XML* standartından istifadə təklif olunur. Lakin bu standartın köməyi ilə idarə olunan sistemlər üçün xüsusi tip hücum – "XML obyektləri üçün inyeksiya" mövcuddur. Belə ki, bədniyyətli informasiya axınına öz əlavə *XML*-obyektlərini daxil edir və icraçı qurğular müəyyən ardıcıllıqla istədiyi komandaları yerinə yetirməyə vadar edir. Ona görə də *M2M* üçün işlənən protokollarda bu cür nisbətən yeni texnoloji hücumlardan qorunmaq nəzərdə tutulmalıdır [1].

Mütəxəssislər hesab edirlər ki, təhlükəsizlik məsələlərinin həll edilməsi üçün müvafiq proqram təminatının lisenziyalaşdırılması, intellektual mülkiyyət obyektlərindən istifadə və onların qorunması üçün xüsusi qaydalar hazırlanıb tətbiq olunmalıdır [8].

Mənzillərin, fərdi evlərin, avtomobillərin, digər infrastruktur və qurğuların İnternetə qoşulması üçün, ilk növbədə, informasiya təhlükəsizliyi təmin edilməlidir. Bütün qurğu və obyektlərin İnternetə qoşulması üçün autentifikasiya, şifrələmə məsələləri yüksək səviyyədə təmin olunmalıdır.

"Ağıllı" qurğuların istehsalçıları da yaratdıqları boşluqları aradan qaldırmağa səy göstərməlidirlər. Bütün bu cür qurğular üçün ümumi təhlükəsizlik standartlarının işlənib hazırlanması vacibdir.

FƏRDİ MƏLUMATLARIN QORUNMASI PROBLEMLƏRİ

Əşyaların İnterneti texnologiyalarının geniş yayılması və tətbiqi ilə bağlı yaranan ən ciddi problemlərdən biri də fərdi məlumatların, istehlakçı hüquqlarının qorunması ilə bağlıdır. İstehlakçılar bu texnologiyaların tətbiqinin onların şəxsi həyatının toxunulmazlığını zərbə altına qoymasından ehtiyatlanır. Müvafiq texnologiyaların geniş tətbiq edildiyi ölkələrdə müxtəlif ictimai təşkilatların fəalları *RFID* texnologiyalarının kommersiya məqsədilə sınaqdan keçirilməsi hallarına qarşı çıxırlar. Bu, onu göstərir ki, Əşyaların İnterneti texnologiyalarının tətbiqi yalnız vətəndaşların informasiya, şəxsi həyatın toxunulmazlığı ilə

bağlı hüquqlarının qorunmasına təminat veriləcəyi halda uğur qazana bilər [6, 9].

ABŞ-da və Avropada istehlakçı hüquqlarının müdafiəçiləri *RFID* çiplərinin pərakəndə ticarət mallarında istifadə edilməsindən narahatdırlar. Onlar qorxurlar ki, həmin texnologiyaların köməyi ilə şirkətlər istehlakçıların bütün maraq dairələrini öyrənə biləcəklər – kimin hansı növ kolbasanı xoşlamasından başlamış, hansı rəngdə və dəbdə olan paltara üstünlük verməsinə qədər. Bu sahədə çalışan mütəxəssislərin bir çoxu hesab edir ki, *RFID* texnologiyalarından xidmət keyfiyyətinin yüksəldilməsi ilə əlaqədar istifadənin üstünlükləri şəxsi həyat sirri ilə bağlı istənilən narahatçılığı üstələyir. Yəni bu texnologiyaların üstünlükləri çatışmazlıqlarından daha mühümdür [1].

RFID-çipdən informasiyanı bir neçə metrlik məsafədən oxumağın mümkünlüyü də vətəndaş hüquq və azadlıqlarının müdafiəçilərini narahat edir. Onlar hesab edirlər ki, mağazalarda *RFID*-oxuculara malik olan bədniyyətli insanlar istehlakçıların malları üzərində olan bu cür nişanlardan əldə etdiyi informasiyanı onun özünə qarşı istifadə edə bilər (məsələn, mağazanın verilənlər bazasına daxil olaraq, istehlakçının kredit kartının nömrəsini öyrənə bilər).

ABŞ-ın *Wal-Mart* korporasiyasının nəhəng ticarət şəbəkəsi vasitəsi ilə satdığı malların *RFID* çipləri ilə təchiz olunması haqqında qərarı da istehsalçılar tərəfindən kəskin narazılıqlarla qarşılanmışdı. Məsələ o yerə gəlib çatmışdır ki, hüquq müdafiəçiləri bu cür halların qarşısını ala biləcək qanun layihəsi hazırladılar. Bu məsələ ilə əlaqədar *CASPLAN* hüquq-müdafiə təşkilatı xüsusi fəallıq nümayiş etdirdi. Həmin qanun layihəsində *RFID*-çiplər vasitəsi ilə əldə edilən informasiyanın məhdudlaşdırılması ilə bağlı sərt tədbirlər nəzərdə tutulur [4].

Gillette (ABŞ) şirkətinin *RFID*-çiplərdən istifadə etmək təşəbbüsü də istehlakçıların narazılığına səbəb olmuşdu. Şirkət məhsullarının dünyanın müxtəlif ölkələrindən olan alıcıları öz etirazlarını bildirmişdilər. Bu *Gillette*-in Kembricdəki mağazasında satışa çıxarılan *RFID*-çipli malların boykot edilməsi ilə nəticələnmişdi. Bu cür etirazları nəzərə alan şirkət rəhbərliyi sınaq satışlarını dayandıraraq, bu təşəbbüsdən əl çəkməli oldu [1].

İnformasiya təhlükəsizliyi sahəsində fəaliyyət göstərən *ISACA* analitik şirkəti 2013-cü ildə 110 ölkədən olan ekspert və istifadəçi arasında Əşyaların İnternetinin təhlükələrini müəyyən etmək üçün geniş sorğu keçirmişdir. Rəyi soruşulanların 90%-i fərdi məlumatların qanunsuz olaraq əldə keçirilməsi təhlükəsini qeyd etmişdir [10].

ABŞ Federal Ticarət Komissiyasının Əşyaların İnterneti ilə bağlı 2013-cü ildə dərc edilən hesabatında təhlükəsizlik məsələlərinə, o cümlədən şəxsi həyatın və fərdi məlumatların qorunması məsələlərinə xüsusi diqqət yönəldilir [11].

Hesabatda həmin məsələlərlə bağlı Əşyaların İnterneti avadanlıqlarının və qurğularının istehsalçılarına 3 hissədən ibarət müvafiq tövsiyələr verilir:

1. Verilənlərin təhlükəsizliyi (şirkətlər informasiya sahiblərinin təhlükəsizliyini təmin edən mexanizm yaratmalıdırlar);
2. Verilənlərin minimallaşdırılması (şirkətlər qəbul olunmuş normadan artıq məlumat toplamalı deyillər);
3. Azad seçimin təmin edilməsi (insanlar özləri qərar verməlidirlər ki, hansı fərdi məlumatlarını başqaları ilə bölüşməyə hazırdırlar).

Komissiya hələlik Əşyaların İnterneti sahəsində xüsusi qanunvericiliyin yaradılmasına ehtiyac görmür. Hesab edir ki, özünütənzimləmə mexanizmi təşkilatlarda konfidensiallıq və təhlükəsizlik siyasətinin həyata keçirilməsi üçün yetərlidir. Bununla belə, ABŞ Konqresinə tövsiyə olunur ki, şirkətlər üçün müştərilərinə təhlükəsizlik qaydalarının pozulması halları ilə bağlı məlumat vermək vəzifəsini müəyyən edən güclü, çevik, texnoloji baxımdan neytral qanunvericilik formalaşdırsın.

NƏTİCƏ

Əşyaların İnternetinin hər şeyi əhatə etmək imkanı onun geniş tətbiqinin nəticələri ilə bağlı müəyyən narahatlıqlara əsas verir. Bu sistemin istehsal, xidmət proseslərinə, sosial-mədəni və məişət sferalarına tətbiqi böyük risklərlə bağlıdır. Ona görə də bu cür proseslərin tətbiqinə tam hazır olmaq, bütün nüansları qiymətləndirmək lazımdır.

Əşyaların İnterneti konsepsiyasının uğurla həyata keçirilməsi və inkişaf etdirilməsi üçün bir sıra mühüm məsələlər həll edilməlidir. Yalnız mövcud və gözlənilən problemlərin dərindən dərk edilməsi və buna uyğun texnoloji və hüquqi qərarların qəbul edilməsi nəticəsində Əşyaların İnterneti konsepsiyasını uğurla reallaşdırmaq olar.

ƏDƏBİYYAT

[1] R. M. Əliquliyev, R. Ş. Mahmudov, "Əşyaların İnterneti". Ekspress-informasiya, "İnformasiya Texnologiyaları", 2012, 48 s.

[2] S.C.Mukhopadhyay, "Internet of Things: Challenges and Opportunities", Springer Science & Business Media, 2014, 269 p.

[3] Gartner, "Forecast: The Internet of Things, Worldwide," 2013, https://www.gartner.com

[4] R. M. Əliquliyev, R. Ş. Mahmudov, "Əşyaların İnterneti: mahiyyəti, imkanları və problemləri", "İnformasiya cəmiyyəti problemləri", 2011, № 2, s. 29-40.

[5] Hewlett-Packard, Internet of Things Research Study, 2014 report, http://www8.hp.com

[6] A. Bahga, V. Madisetti, "Internet of Things: A Hands-On Approach", VPT, 2014, 446 p.

[7] J. Holler, V. Tsiatsis, C. Mulligan et all., "From Machine-to-Machine to the Internet of Things: Introduction to a New Age of Intelligence". Academic Press, 2014, 352 p.

[8] Y. N. İmamverdiyev, T. V. Kang, "Əşyaların İnternetin üçün yüngülçəkili kriptoqrafiya", "İnformasiya təhlükəsizliyi problemləri üzrə I respublika elmi-praktiki konfransı", 17-18 may, 2013, s.137-140.

[9] Р. М. Алигулиев, Р. Ш. Махмудов, "Интернет Вещей", Информационное общество, Москва, № 3, с.42-48, 2013.

[10] ISACA, Internet of Things: Risk and Value Considerations, 2013, http://www.isaca.org

[11] Federal Trade Commission, "Internet of Things - Privacy and Security in a Connected World". https://www.ftc.gov