



## 1-SHO‘BA AXBOROT XAVFSIZLIGI

### BUYUMLAR INTERNETINI ASOSIY TASHKIL ETUVCHILARI VA UNDA QO‘LLANILADIGAN PROTOKOLLAR TAHLILI

<sup>1</sup>Olimov Iskandar Salimboyevich, <sup>2</sup>Karimov Abduqodir Abdusalomovich,  
<sup>3</sup>Bo‘riyev Yusuf Absamat o'g'li

<sup>1,2,3</sup>Toshkent axborot texnologiyalari universiteti

[iskandar.olimov@gmail.com](mailto:iskandar.olimov@gmail.com)

**Annotatsiya:** Ushbu maqolada buyumlar Interneti, uni asosiy tashkil etuvchilari, unga qo‘yiladigan xavfsizlik talablar, unda qo‘llaniladigan protokollari tasnifi keltirilgan.

**Kalit so‘zlar:** Simsiz sensor tarmoq (Wireless sensor network, WSN), Radio chastotasini aniqlash (Radio Frequency Identification, RFID), Autentifikasiya.

Hozirgi kunda axborot texnologiyalari jadal suratlar bilan rivojlanib bormoqda. Bunday texnologiyalardan biri bu buyumlar Interneti hisoblanadi. Buyumlar Interneti inson va foydalanuvchilarning ko‘p maqsadlarini amalga oshiruvchi hamda apparat yoki qurilmalar o‘rtasidagi o‘zaro aloqani ta‘minlovchi rivojlanayotgan texnologiyalar jamlanmasi hisoblanadi.

Buyumlar Interneti ko‘plab Simsiz sensor tarmoq (Wireless sensor network, WSN), Bluetooth, Radio chastotasini aniqlash (Radio Frequency Identification, RFID) va boshqa turli tarmoq texnologiyalari jamlanmasidan iborat bo‘lib ular o‘rtasida o‘zaro aloqani internet texnologiyalaridan foydalangan holda amalga oshiriladi [2,5]. Natijada foydalanuvchilar uchun buyumlar Interneti kerakli bo‘lgan xizmatlarini istalgan vaqtda taqdim eta oladi [1].

Buyumlar Interneti o‘z navbatida identifikasiya, xizmatlar, hisoblash, semantik, aloqa, sezish kabi asosiy elementlardan iborat.

**Identifikasiya.** Bu foydalanuvchi shaxsni tasdiqlash uchun o‘z idintifikatorini tizimga taqdim qilish jarayoni. Odatda identifikator tanlashda standart nomlardan foydalanish lozim, va shu bilan birga foydalanuvchi haqidagi qo‘shimcha ma‘lumotlarni oshkor etmasligi kerak (masalan, ish joyi, IP va MAC addresslar).

Buyumlar Internetini boshqa texnologiyalardan ko‘p sonli ulanish imkoniyati mavjud ekanligi, ya‘ni ko‘plab qurilmalar bir-biriga mos keladigan Elektron mahsulot kodlari (Electronic Product Codes, EPC) va universal IPv6 manzillari orqali ulanishlari



amalga oshirish xususiyatlari bilan ajratib turadi.

TCP/IP ga asoslangan IPv6 IP address miqdori ko‘p bo‘lganligi uchun juda ko‘plab qurilmalarga IP berish imkoni mavjud. IPv6 nafaqat noaniqlikni yo‘q qiladi, bundan tashqari, Internet orqali qurilmalarga masofadan turib kirish imkoniyatini beradi [1].

Buyumlar Interneti uchun identifikasiyalashning 2 xil usuli mavjud bo‘lib, UCode (Ubiquitous Codes) va Elektron mahsulot kodlar (EPC). Ushbu usullar barcha qurilmalar uchun tarmoq ichida noyob identifikatorni (ID) ta‘minlash uchun xizmat qiladi. 6LoWPAN hozirda ko‘p manzilli va kam quvvatli simsiz tizimlar uchun tafsiya qilinmoqda [4].

**Hizmatlar.** Buyumlar Internetining asosiy qism elementlaridan biri Hizmatlar hisoblanib, u quydagicha turkumlanadi: *Axborot yig‘ish xizmatlari* (Information Aggregation Services, IAS), Hamma joyda xizmat (Ubiquitous Services, US), Identifikasiya bilan bog‘liq xizmatlar (Identity related Services, IRS), va Hamkorlikda xabardor xizmatlar (Collaborative Aware Services, CAS).

**Hisoblash.** U ikki qismdan iborat, apparat va dasturiy. Apparat qismiga aqlli qurilmalar, Android, TinyOS, Riot OS, Contiki va LiteOS kabilar misol bo‘la oladi. Dasturiy qismiga esa Android, TinyOS, Riot OS, Contiki va LiteOS kabilar misoldir. Undan tashqari, Cloud computing buyumlar Internetining asosiy qismlaridan bir hisoblanib, u nafaqat ma‘lumotlarni uzoq muddatli saqlash, balki ma‘lumotlarni yagona kirish joyida saqlash va qayta ishlash imkonini beradi [3].

**Simantik.** Bu qismning asosiy vazifasi axborotlarni analiz qilish hisoblanadi. Tanib olish undan tashqari axborotlarni ajratib olish vazifalarini ham bajaradi. Bu kabi vazifani bajaruvchilariga misol sifatida EXI (Efficient XML Interchange), RDF (Resource Description Framework), va OWL (Web Ontology Language) kabilarni keltirish mumkin.

**Sezish.** Buyumlar Interneti butun qurilmalarni boshqarish, ular o‘rtasida o‘zaro aloqa xosil qilishni amalga oshiradi [5]. Kelib chiqishi va funksional imkoniyatlari turlicha bo‘lgan qurilmalar o‘rtasida o‘zaro aloqani ta‘minlashda Elektr va elektron muhandislar instituti (Institute of Electrical and Electronics Engineers (IEEE)), Internet muhandisligi ishchi guruhi (Internet Engineering Task Force (IETF)), Yevropa telekommunikasiya standartlari instituti (European Telecommunications Standards Institute, ETSI), Butunjahon Internet tarmog‘idagi konsorsium (World Wide Web Consortium (W3C)), Elektron mahsulot kodlar (EPC), Xalqaro Biznes Mashinalari (International Business Machines (IBM)), va Ob‘ektlarni boshqarish guruhi (Object Management Group, OMP) kabi tashkilotlar tomonidan ishlab chiqilgan WiFi, WiFi Direct, Z-Wave, IEEE 802.15.4, Bluetooth, RFID, Yaqin maydon aloqasi (Near Field Communication, NFC), WSN, va Ultra keng tarmoqli (Ultra-Wide Bandwidth, UWB)



protokollar va texnologiyalardan foydalaniladi [1,6].

Buyumlar Internetining asosiy elementlari quyidagi irarxiyada keltirilgan:

- Identifikasiya;
  - Address;
    - EPC, uCode.
  - Nomi;
    - IPv4, IPv6.
  - Semantik.
    - RDF, OWL, EXI.
- Hizmetlar;
  - Axborot yig‘ish xizmatlari (Information Aggregation Services, IAS),  
Hamma joyda xizmat (Ubiquitous Services, US).
- Hisoblash;
  - Apparat;
    - Aqlli qurilmalar, Arduino, Phidgets, Intel Gailileo, aqlli telefon.
  - Dasturiy ;
    - OS(Contiki, TinoOS, LiteOS, RiotOS, va Android);
    - Cloud (Nimbits, Hadoop, va boshqalar).
- Aloqa;
  - RFID, Bluetooth, IEEE 802.15.4, Z-Wave, WiFi, LTE-A.
- Sezish.
  - Smart Sensors, Sensing Devices, Actuators, RFID teg.

**Buyumlar Internetiga qo‘yiladigan xavfsizlik talablari va unda qo‘llaniladigan protokollar.** Buyumlar Internetida tarmoq orqali bajariladigan vazifalar aniq belgilangan standartlar orqali amalga oshiriladi. Shu bilan birga, xavfsizlik talablari qo‘yilishiga qarab vaqt o‘tishi bilan tarmoq qurilmalarining imkoniyatlari takkomillashtirilib boriladi.

O‘z navbatida buyumlar Interneti quydagi xavfsizlik talablarini ta‘minlashi kerak. Ular maxfiylik, butunlik, foydalanuvchanlik, ruxsatlarni boshqarish, xavfsiz aloqa, autentifikasiya, ma‘murlashdir [6].

**Maxfiylik.** Bu ruxsat etilmagan o‘qishdan himoyalaniş ya‘ni axborotdan huquqqa ega bo‘lgan foydalanuvchilargina foydalanishi va aksinchi huquqqa ega bo‘lmaganlardan axborotni himoyalaniş tushuniladi. Buyumlar Internetida axborotni konfidensiyalligini ta‘minlashda simmetrik shifrlash algoritmlari va kriptobardoshliligi yuqori bo‘lgan shifrlash algoritmlaridan foydalangan holda ta‘minlash mumkin [1,4].

Buyumlar Internetida foydalanuvchilarni salmog‘i, qurilmalar ko‘pligi va barcha xizmatlar asosan Internet tarmog‘i orqali bajarilganligi sababli, axborotning



maxfiylikni ta'minlash buyumlar Internetining asosiy xavfsizlik talablaridan biri hisoblanadi.

**Butunlik.** Bu ruxsat etilmagan o'zgartirishdan himoyalash, ya'ni faqat axborotdan foydalana olish huquqiga ega bo'lgan foydalanuvchilardagina o'zgartirish imkoni mavjud va aksinchi bunday huquqqa ega bo'lmaganlardan axborotni o'zgartirishdan himoyalash tushuniladi. Buyumlar Internetida axborotni butunligini ta'minlashda xavfsizlik protokollari, hesh algoritmlaridan foydalaniladi [3].

**Xavfsiz aloqa.** Buyumlar Internetiga qo'yilgan xavfsizlik talablaridan biri tarmoq qurilmalari o'rtasida xavfsiz ma'lumot, aloqa almashish hisoblanadi.

**Ruxsatlarni boshqarish.** Ruxsatlarni boshqarish foydalanuvchilarni haqiqiylikni tekshirish, resurslardan foydalanish imkoniyatlarini boshqarishdir. Tizimdagi barcha foydalanuvchilarning harakatlari va ularning foydalanish imkoniyatlari huquqlar orqali belgilanadi. Kirish - bu sub'yekt (shaxs, jarayon yoki dastur) va ob'yekt (ya'ni tizim resursi, fayl, printer va boshqalar) o'rtasidagi ma'lumotlar oqimidir. Tizim tomonidan ruxsat etilgan foydalanuvchilarga foydalanishi mumkin bo'lgan ma'lumotlar oqimi taqdim etiladi. Aksincha hollarda ruxsat etilmagan foydalanuvchilarga axborotdan foydalanish rad etiladi.

**Autentifikasiya.** Autentifikasiya foydalanuvchining haqiqiylikni aniqlash jarayoni. O'zining haqiqiylikni tasdiqlash uchun sub'yekt tizimga turli axborotni taqdim etadi. Bunday axborot turi “Autentifikasiya faktori” deb yuritiladi. Autentifikasiyalashning quydagi uchta faktori farqlanadi:

– Biror narsani bilish asosida. Misol sifatida parol, shaxsiy identifikasiya kodi PIN (Personal Identification Number) hamda “so'rov javob” xilidagi protokollarda namoyish etiluvchi maxfiy va ochiq kalitlarni ko'rsatish mumkin;

– Biror narsaga egaligi asosida. Odatda bular magnit kartalar, smart-kartalar, sertifikatlar va touch memory qurilmalari orqali amalga oshiriladi;

– Qandaydir daxlsiz xarakteristikalar asosida. Ushbu faktor o'z tarkibiga foydalanuvchining biometrik xarakteristikalariga (ovozlar, ko'zining rangdor pardasi va to'r pardasi, barmoq izlari va h.z.) asoslangan usullarni oladi.

**Ma'murlash(auditing).** Sub'yektlarni tizimdagi harakatlarini nazorat qilish jarayoni.

Buyumlar Internetida qurilmalar o'rtasida identifikasiya va autentifikasiya qilish, kuzatib borish va xavfsiz ma'lumot almashishni amalga oshirishda protokollardan foydalaniladi.

Qo'llaniladigan standartlar va protokollarni umumiy holatiga ko'ra quydagicha sinflarga ajratish mumkin. Ular ilovalar(Applications), xizmatni aniqlash(service discovery), infratuzulma (infrastructure) va boshqa protokollardan iborat. Buyumlar Internetini qo'llab-quvvatlovchi bir qator protokollar tasnifi



1-jadvalda keltirilgan.

1-jadval

Buyumlar Internetini qo‘llab-quvvatlovchi protokollar

<b>Infratuzilma protokollar</b>		
<b>Sathlar</b>	<b>Protokollar</b>	<b>Tashkilot nomi</b>
Routing protokol	RPL	IETF
tarmoq sathi	6LowPAN	IETF
kanal sathi	IEEE 802.15.4	IEEE
Fizik sath	EPC global, LTE-A, Z-Wave	EPCglobal, Nokia, ZenSys & Z-Wave Alliance

### **Xulosa**

Buyumlar Interneti ko‘plab qurilmalardan iborat murakkab tizim hisoblanganligi bois ushbu maqolada buyumlar Internetining asosiy tashkil etuvchilari, unda qo‘llaniladigan protokollar tahlil keltirilgan.

### **Foydalanilgan adabiyotlar ro‘yxati:**

1. Olimov I.S., Boriyev Y.A., Sadikov M.A., Khamidov SH.J. (2020, November). Internet of things architecture and security challenges. In 2020 International Conference on Information Science and Communications Technologies (ICISCT) (pp. 1-4). IEEE.

2. Deebak B. D., Al-Turjman F. A hybrid secure routing and monitoring mechanism in IoT-based wireless sensor networks //Ad Hoc Networks. – 2020. – T. 97. – C. 102022.

3. Thomas D., Shankaran R. A secure barrier coverage scheduling framework for WSN-based IoT applications //Proceedings of the 23rd International ACM Conference on Modeling, Analysis and Simulation of Wireless and Mobile Systems. – 2020. – C. 215-224.

4. Alshambri H. et al. Cybersecurity attacks on wireless sensor networks in smart cities: an exposition //INTERNATIONAL JOURNAL OF SCIENTIFIC & TECHNOLOGY RESEARCH. – 2020. – T. 8. – №. 1.

5. Galeano-Brajones J. et al. Detection and mitigation of dos and ddos attacks in iot-based stateful sdn: An experimental approach //Sensors. – 2020. – T. 20. – №. 3. – C. 816.

6. Tayyab M., Belaton B., Anbar M. ICMPv6-based DoS and DDoS attacks detection using machine learning techniques, open challenges, and blockchain applicability: a review //IEEE Access. – 2020. – T. 8. – C. 170529-170547.