**<https://center2m.ru/informatsionnaya-bezopasnost-veschey>**

**https://www.kaspersky.ru/resource-center/preemptive-safety/best-practices-for-iot-security**

**IoT ulgamynyň howpsuzlygyny üpjün etmek**

**IoT (Internet of Things)** — internet arkaly biri-biri bilen baglanyşykly işleýän enjamlaryň ulgamy bolup, olara sensorlar, akylly kameralar, saglyk enjamlary, senagat awtomatika ulgamlary, öý enjamlary we beýleki sanly tehnologiýalar girýär. IoT ulgamlarynyň giňden ýaýramagy bilen, olaryň howpsuzlygyny üpjün etmek has möhüm mesele bolup durýar. Kiberhüjümlerden goragly bolmak üçin IoT enjamlary fiziki we programma taýdan goralmaly.

**1. IoT ulgamynyň howpsuzlygyny üpjün etmegiň usullary**

IoT enjamlarynyň howpsuzlygyny üpjün etmek üçin dürli gorag çäreleri ýerine ýetirilmelidir:

**2.1. Güýçli autentifikasiýa we ygtyýarnama (Authentication & Authorization)**

* **Öňden kesgitlenen (default) parollary üýtgetmek:** Enjamlaryň köpüsi öňünden kesgitlenen gowşak parollar bilen gelýär. Olary güýçli, çylşyrymly parollar bilen çalyşmaly.
* **Iki derejeli tassyklama (2FA) ulanmak:** Ulanyjy ulgama girende goşmaça tassyklama (meselem, SMS kody) ulanmaly.
* **Sertifikatlar we tokenler arkaly ygtyýarnama bermek:** IoT enjamlaryna rugsatsyz girmegiň öňüni almak üçin şahsyýet tassyklama ulgamlaryny ulanmak.

**2.2. Şifrleme (Encryption) ulanmak**

* **AES-256 ýa-da RSA ýaly güýçli şifrleme algoritmlerini ulanmak:** Maglumatlary şifrlemek bilen, olary rugsatsyz ele salnyp bilmez ýaly goramak.
* **End-to-End Encryption (E2EE) ulanmak:** IoT enjamlary bilen merkezi serweriň arasynda maglumatlaryň howpsuz geçirilmegini üpjün etmek.

**2.3. Firmware we programma üpjünçiligini yzygiderli täzeläp durmak**

* **Firmware-iň howpsuzlyk täzelenmelerini awtomatiki almak:** IoT enjamlary kiberhowplara garşy täzelenen programma üpjünçiligini yzygiderli almagy üçin awtomatiki täzelenme funksiýasyny açyk saklamaly.
* **IoT enjamlarynyň zyýanly programmalardan arassa bolmagyny üpjün etmek:** IoT ulgamlarynda diňe ygtybarly we sertifikatlaşdyrylan programma üpjünçiligini ulanmak.

**2.4. Şebeke howpsuzlygyny üpjün etmek**

* **VPN ulanmak:** IoT enjamlarynyň internete goragly birikmegini üpjün etmek üçin Wirtual Hususy Tor (VPN) ulanmak.
* **Şebeke gorag diwarlaryny (Firewall) ulanmak:** IoT enjamlarynyň rugsatsyz tor baglanyşyklaryndan goralmagyny üpjün etmek.
* **Wi-Fi tor howpsuzlygyny güýçlendirmek:** WPA3 ýaly güýçli şifrleme protokollaryny ulanmak we IoT enjamlaryny aýratyn torlara (VLAN) bölmek.

**2.5. Fiziki howpsuzlygy üpjün etmek**

* **IoT enjamlarynyň fiziki taýdan berkidilmegi:** IoT enjamlaryny rugsatsyz adamlaryň elýeterli bolmadyk ýerlerde saklamak.
* **Portlary we interfeýsleri petiklemek:** IoT enjamlarynyň USB, UART we JTAG portlaryny rugsatsyz ulanyjylardan goramak.
* **Sensor we hereket duýujylary (motion sensors) ulanmak:** Eger IoT enjamyna rugsatsyz elýeterlilik ýüze çyksa, duýduryş bermek.

**2.6. Hüjümleri ýüze çykarmak we öňüni almak**

* **IDS/IPS ulgamlaryny ulanmak:** Tor gorag ulgamlary (Intrusion Detection Systems / Intrusion Prevention Systems) arkaly nädogry traffikleri ýüze çykarmak.
* **IoT enjamlary üçin howpsuzlyk auditi geçirmek:** IoT ulgamlaryny yzygiderli howpsuzlyk barlagyndan geçirmek.
* **Maglumat akymlaryny yzygiderli gözegçilikde saklamak:** IoT enjamlarynyň maglumat alyş-çalyşlaryny seljerip, nädogry hereketleri anyklamak.

**4. Netije**

IoT ulgamlarynyň howpsuzlygyny üpjün etmek üçin toplumlaýyn çemeleşme gerek. Aşakdaky çäreler IoT howpsuzlygyny ýokarlandyrmaga kömek eder:

✅ Güýçli autentifikasiýa we ygtyýarnama (2FA, sertifikatlar)  
✅ Maglumatlary şifrlemek (AES-256, RSA)  
✅ Firmware we programma üpjünçiligini yzygiderli täzeläp durmak  
✅ Şebeke howpsuzlygyny güýçlendirmek (Firewall, VPN, IDS/IPS)  
✅ Fiziki goragy üpjün etmek (portlary petiklemek, enjamy berkidilen ýerde saklamak)  
✅ Hüjümleri anyklamak we öňüni almak üçin tor auditi geçirmek

Bu çäreler ýerine ýetirilse, IoT enjamlarynyň howpsuzlygy ýokarlanyp, kiberhowplara garşy güýçli gorag dörediler.

**IoT Enjamlarynyň Howpsuzlygyny Üpjün Etmek Üçin Esasy Gorag Çäreleri**

IoT ulgamynyň howpsuzlygy köp taraply çäreleri talap edýär. Aşakdaky usullar enjamlaryň, maglumatlaryň we torlaryň goragyny üpjün etmäge kömek eder:

**1. Enjamlaryň Fiziki we Programma Üpjünçiligi 🔒**

**✔ Fiziki Gorag**

* **Tampering (düzmek) sensorlary** – Enjamyň gabygy açylsa, howpsyzlyk ulgamy habar berer.
* **TPM (Trusted Platform Module)** – Kriptografiýa açarlaryny goramak üçin fiziki mikroçip.
* **Fabrik Öňünden Gurlan Parollar** – Hemişe paroly üýtgetmeli we güýçli parollar ulanylmaly.

**✔ Programma Üpjünçilik**

* **Firmware Täzelenmeleri** – Yzygiderli täzelemeler (OTA – Over-The-Air updates).
* **Minimal Işleýiş Ulgamy** – Gereksiz funksiýalary öçürmek (Linux-da "unnecessary services").
* **Kod Yglan Edilmegi** – Firmware-da arkaplan (backdoor) ýoklugyny barlamak.

**2. Tor Howpsuzlygy 🌐**

**✔ Şifrlemek (Encryption)**

* **TLS/SSL** – HTTPS, MQTT over TLS (port 8883).
* **VPN (Virtual Private Network)** – IoT enjamlary aýratyn torlara birikdirilmeli.
* **MAC Adresleriň Filterlenmegi** – Diňe ygtyýarly enjamlara rugsat bermek.

**✔ Tor Segmentasiýasy (Network Segmentation)**

* **VLAN (Virtual LAN)** – IoT enjamlary aýratyn tor bölüminde saklanmaly.
* **Firewall Düzgüleri** – IoT enjamlary diňe gerekli portlar arkaly aragatnaşyk etmeli.

**✔ IDS/IPS (Hüjümleri Anyklamak we Öňüni Almak)**

* **Snort/Suricata** – IoT trafigini analiz etmek.
* **Zeek (Bro)** – Şübheli hereketleri anyklamak.

**3. Giriş Kontroli we Awtorizasiýa 🔑**

**✔ Güýçli Parol Ulanyşy**

* **Fabrik Parollaryny Üýtgetmek** (admin/admin ýaly adaty parollar ýok edilmeli).
* **2FA (Iki Faktorly Awtentifikasiýa)** – Biometriýa ýa-da TOTP (Google Authenticator).

**✔ API Howpsuzlygy**

* **Token we JWT (JSON Web Token)** – Rugsatsyz girişiň öňüni almak.
* **OAuth 2.0** – Üçünji tarap programmalar üçin çäklendirme.

**4. Maglumat Howpsuzlygy we Gizlinlik 🛡️**

**✔ Maglumatlaryň Şifrlenmegi**

* **AES-256** – Sensor maglumatlary üçin güýçli şifrleme.
* **End-to-End Encryption (E2EE)** – Bulut bilen enjam arasyndaky aragatnaşyk.

**✔ Gizlinlik Sazlamalary**

* **GDPR we IoT** – Ulanyjylaryň maglumatlaryny goramak.
* **Anonymization** – Sensor maglumatlarynda şahsy maglumatlary aýyrmak.

**5. Hüjümlere Karşı Gözegçilik we Jogap 🚨**

**✔ Loglamak we Monitoriň Etmek**

* **SIEM (Security Information and Event Management)** – Splunk, ELK Stack.
* **Anomaly Detection (Aňsatlyklary Anyklamak)** – Maşyn öwrenişi (ML) ulanyp.

**✔ DDoS Goragy**

* **Rate Limiting** – Bir enjamyň iberýän sorawlaryny çäklendirmek.
* **Cloudflare IoT Protection** – Bulut esasy DDoS goragy.

**✔ Inzidentlere Jogap Bermek**

* **IRP (Incident Response Plan)** – Hüjüm bolsa näme etmeli?
* **Automated Blocking** – Şübheli IP adresleri awtomatik bloklanmaly.

**6. Standartlar we Kanunlar 📜**

* **ISO/IEC 27001** – Maglumat howpsuzlygy standartlary.
* **NIST IoT Security Guidelines** – ABŞ-nyň IoT üçin usullary.
* **GDPR, CCPA** – Ulanyjylaryň maglumatlaryny goramak.

**Netije**

IoT enjamlaryny goramak üçin **fiziki, programma, tor we maglumat goragy** bir wagtda amala aşyrylmaly. Esasy ädimler:  
✅ **Enjamlary Täzelemek we Fiziki Goramak**.  
✅ **Tor Segmentasiýasy we Şifrlemek**.  
✅ **Güýçli Parollar we 2FA Ulanyşy**.  
✅ **Hüjümleri Monitoriň Etmek we DDoS Goragy**.

Eger aýratyn bir IoT senaryo üçin howpsuzlyk meýilnamasy gerek bolsa, aýratyn sorag berip bilersiňiz! 🔐

## Безопасность

Потенциальные угрозы безопасности, возникающие в среде IoT, также можно рассматривать с точки зрения эталонной модели. На каждом уровне модели присутствуют угрозы безопасности, как специфичные только для этого уровня, так и общие для всей модели. Так, на всех уровнях модели присутствует угроза несанкционированного доступа к приложению или устройству. В случае исполнительных устройств несанкционированный доступ может привести к несанкционированным действиям самой вещи. На уровне приложения – это угрозы утечки информации, нарушения целостности данных и неприкосновенности частной жизни. На уровне сети – угрозы утечки данных об использовании сигнализации и нарушения их целостности. На уровне устройства – угрозы несанкционированного вскрытия, несанкционированного контроля/управления, утечки данных, хранящихся в устройстве, повреждения их целостности.

Для нейтрализации описанных угроз безопасности применяются алгоритмы авторизации и идентификации, производится шифрование передаваемых и хранимых данных, проводится аудит систем и применяется антивирусное программное обеспечение. Но не все устройства и приложения обладают высокой производительностью, поэтому применение криптостойких алгоритмов не всегда является возможным.

Важным моментом, по мнению автора, с точки зрения потенциальных угроз также является аспект социальных последствий применения IoT. Во-первых, при взаимодействии типа устройство–устройство роль человека уже в настоящее время ограничена. А во-вторых, в будущем, по мнению автора, угроза частной жизни будет исходить не от всезнающего "Большого Брата", отслеживающего и регистрирующего каждый шаг, а от сотен маленьких устройств, постоянно вмешивающихся в нашу частную жизнь.

## Заключение

Концепция IoT несет в себе огромный потенциал возможностей. Но наряду с этим возникает и целый спектр угроз безопасности, в том числе имеющих и социальные последствия. По мнению автора, конечной задачей развития IoT является создание проекций для каждой физической вещи в виртуальном пространстве. Чем больше вещей может контролировать IoT, тем больше возможностей он сможет предоставить. Если этот процесс оставить без должного контроля, то, в конечном счете, у любого реального объекта будет виртуальная копия, представляющая свойства физического объекта, но, возможно, обладающая иными способностями в виртуальном мире. Это приведет к появлению централизованной системы, способной к производству и управлению большим количеством данных. Поэтому возникает вопрос о том, кто будет управлять этой системой и к какому виду отношений между виртуальными объектами это может привести.