**IoT ulgamynyň howpsuzlygyny üpjün etmek**

**IoT ulgamlarynyň** giňden ýaýramagy bilen, olaryň howpsuzlygyny üpjün etmek has möhüm mesele bolup durýar. IoT enjamlaryny kiberhüjümlerden goramak üçin **fiziki, programma, tor we maglumat goragy** bir wagtda amala aşyrylmaly.

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

**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 ulanyjylary tassyklama ulgamlaryny ulanmak.

**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.

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

* **Firmware-iň howpsuzlyk täzelenmelerini awtomatiki almak:** IoT enjamlary kiberhowplara garşy täzelenen programma üpjünçiligini yzygiderli almaly.
* **IoT enjamlarynyň zyýanly programmalardan arassa bolmagyny üpjün etmek:** IoT ulgamlarynda diňe ygtybarly we sertifikatlaşdyrylan programma üpjünçiligini ulanmaly.

**4. Tor howpsuzlygyny üpjün etmek**

* **VPN ulanmak:** IoT enjamlarynyň internete goragly birikmegini üpjün etmek üçin Wirtual Hususy Tor (VPN) ulanmak.
* **Tory goramak (Firewall):** IoT enjamlarynyň rugsatsyz tor birikmelerinden goraglylygyny üpjün etmek.
* **TLS/SSL** – HTTPS, MQTT over TLS (port 8883).
* **MAC Adresleriň Filterlenmegi** – Diňe ygtyýarly enjamlara rugsat bermek.
* **Wi-Fi tor howpsuzlygyny güýçlendirmek:** WPA3 ýaly güýçli şifrleme protokollaryny ulanmak we IoT enjamlaryny aýratyn torlara (VLAN) bölmek.

**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.

**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.
* **SIEM (Security Information and Event Management)** – Splunk, ELK Stack.
* **Adaty däl hererkerleri ýüze çykarmak (Anomaly Detection)** –ML (Machine learning) ulanmak arkaly ýüze çykarmak.
* **Awtomatik bloklama (Automated Blocking)** – Şübheli IP adresleri awtomatik bloklanmaly (IP black list)

**7. DDoS Goragy**

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

**8. Iot-enjamlarynyň howpsuzlygy barada okuwlary geçmek.**

* **Ulanyjylar:** Iot-enjamlarynyň howpsuzlygyny üpjün etmek boýunça öňdebaryjy usullary öwretmek we öwrenmek, jemgyýetçilik howpsuzlyk çärelerini güýçlendirmek we howpsuzlyk bilen baglanyşykly bilimleri ýokarlandyrmakda möhüm rol oýnap biler. Bu, ulanyjylara howpsuz parollary ulanmagyň, programmalaryň yzygiderli täzelänmeginiň we howpsuz bolmadyk IoT-enjamlaryny ulanmakdan gaçmagyň möhümdigi barada maglumat bermekdir.
* **Işgärler:** belli bir işgärler ýa-da işgärler toparlary üçin howpsuzlyk boýunça ýörite taýýarlyk düzmek, olar üçin dürli hüjümleriň garşysyna täsirli garşy durmak üçin zerur bilimler we başarnyklary üpjün etmek möhümdir.
* **Öndürijiler:** IoT öndürilmegine jogapkär bolan işgärleriň umumy bilim derejesini ýokarlandyrmak, maglumat howpsuzlygy ýagdaýynda howplary azaltýar. Bilimi ýokarlandyrmak üçin, diňe täze protokollary däl, eýsem infrastruktura we her bir enjam üçin hüjüm usullaryny öwrenmek boýunça yzygiderli iş alyp barmak zerurdyr. Maglumat howpsuzlygy boýunça yzygiderli konferensiýalarda gatnaşmak, bu meseleleri üstünlikli çözmäge kömek edýär.

**9. IoT ulanmakda umumy howpsuzlygy gowulandyrmak üçin oňa gatnaşyjy taraplar bilen hyzmatdaşlyk.**

* IoT-enjamlaryny öndürijileriň, tor üpjün edijileriň we howpsuzlyk ekspertleriň arasynda hyzmatdaşlygy gurmak, howpsuzlyk meselelerini bilelikde çözmäge kömek edip biler. Bu, howplar barada maglumat alyş-beriş, howpsuzlyk auditi geçirmegi we howpsuzlyk boýunça öňdebaryjy tejribeleri paýlaşmagy öz içine alýar. IoT önümlerini we hyzmatlaryny howpsuzlyk boýunça synagdan geçirmäge mümkinçilik berýän ylmy barlag guramalary bilen aragatnaşyk, öndürilen önümiň bazardaky abraýyny gowulandyrar. Bu mümkinçilikler, IoT ekosystemasynda üýtgeýän howpsuzlyk meselelerini çözmek üçin yzygiderli innowasiýalary we hyzmatdaşlygy talap edýär.

**IoT (Internet of Things)** ulgamynyň howpsuzlygyny üpjün etmek, bu tehnologiýanyň giňden ulanylyşyny göz öňünde tutup, möhüm bir mesele bolup durýar. IoT enjamlary, internet arkaly bir-biri bilen aragatnaşyk saklap, dürli maglumatlary alyş-beriş edýärler. Olary goramak we howpsuzlygyny üpjün etmek, ulanyjylaryň şahsy maglumatlarynyň, maliýe maglumatlarynyň, we hatda fiziki ýerleriň goragyny üpjün etmek üçin möhümdir. Şeýlelik bilen, IoT ulgamlarynyň howpsuzlygynyň üpjün edilmegi, şahsyýetleriň we jemgyýetleriň goragyny we howpsuzlygyny üpjün edýän möhüm faktor bolup galýar.

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

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

**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**

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! 🔐

**Potensial howplar we howpsuzlyk meseleleri IoT (Internet of Things) gurşawynda, şeýle hem standard model boýunça seredilip bilner. Her bir derejesinde, modelde diňe şol derejä degişli bolan we ähli model üçin umumy bolan howplar bar. Şeýlelikde, modeliň ähli derejelerinde, programma ýa-da enjamda ygtyýarsyz girmäge degişli howpa gabat gelinýär. Işläp düzýän enjamlar üçin, ygtyýarsyz girmek enjamyň özüne ygtyýarsyz hereketleriň amala aşyrylmagyna sebäp bolup biler. Programma derejesinde – maglumatlaryň sızmagy, maglumatlaryň dolandyryşyny we gizlinlik hukuklarynyň bozulmagy ýaly howplar bar. Tor derejesinde – maglumatlaryň sızmagy we signalizasiýanyň dolandyryşyny bozmaga degişli howplar mövcuddyr. Enjam derejesinde – ygtyýarsyz açylyş, ygtyýarsyz kontrol we dolandyryş, enjamda saklanýan maglumatlaryň sızmagy, olaryň dolandyryşyny bozmaga degişli howplar bar.**

**Düşünilen howplary ýok etmek üçin, awtorizasiýa we identifikasiýa algoritmleri ulanylýar, geçirilýän we saklanýan maglumatlar şifrelenýär, ulgamlaryň auditi geçirilýär we antiwirus programmalary ulanýandyklary bellenilýär. Emma ähli enjamlar we programmalar ýokary öndürijilige eýe däl, şonuň üçin kriptoýatyrylan algoritmleriň ulanylmagy her zaman mümkin bolmaýar.**

## 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.

Иными словами, DDoS-атака – атака, направленная на замедление работы или выведение из строя серверов, сетевой инфраструктуры, а также бомбардировка трафика приложений из нескольких ресурсов. В результате DDoS-атак сайты и приложения становятся заторможенными либо вообще перестают работать. В настоящее время более 30% случаев простоя приложений и серверов вызваны DDoS-атаками [1]. В глобальном масштабе ежедневно регистрируется две тысячи DDoS-атак. Средняя атака DDoS обходится крупной компании в 250 долл. в час [2].

Угроза для кибербезопасности, связанная с распространением ботсетей IoT, была предсказана в 2016 году, но специалисты по безопасности в Интернете не уделили достаточно внимания этой проблеме. В то время эта угроза представлялась довольно ограниченной. Однако вскоре появился набор инструментов, позволяющих ботнетам пользоваться уязвимостью в незащищенных устройствах IoT. Атака Mirai в октябре 2016 года стала ключевым поворотным моментом в развитии IoT.

И, наконец, вы никогда не должны идти на компромисс по обеспечению качества [10].

• Отключайте функции, которые не будут использоваться.

• Отслеживайте журнал работы. Например, что делал регулятор тепла, пока вас не было дома.

• Используйте специально разработанные для умного дома антивирусные программы, которые защитят ваши устройства от атак ботнетов. 13

• Если вы используете управление через голосовые команды, то пробуйте иногда менять фразы для их активации.

• Отключите протокол UPnP (Universal Plug & Play). UPnP находит схожие устройства и подключается к ним. Однако такой протокол вредоносное ПО также может взламывать ввиду наличия уязвимостей. То есть если предмет умного дома соединен с другим предметами, то они также будут заражены.

Global IoT (Internet of Things) enjamlarynyň sany 2025-nji ýylda 15 milliarddan gowrak bolup, 2030-njy ýyla çenli bu sanyň 30 milliarddan gowrak boljakdygy çaklanylýar. Bu enjamlar öý hojalyklary, senagat, saglygy goraýyş we beýleki pudaklarda giňden ulanylýar. Şeýle-de bolsa, takyk sanlar pudaga we geografiki sebite görä üýtgäp biler.

6. **Обучение пользователей и разработчиков**. Содействие обучению и обучению передовым методам обеспечения безопасности IoT может сыграть важную роль в повышении осведомленности и укреплении общих мер безопасности. Это включает в себя информирование пользователей о важности использования надежных паролей, регулярном обновлении программного обеспечения и отказе от использования небезопасных устройств IoT. Международный научный журнал «ВЕСТНИК НАУКИ» № 7 (64) Т.4..............................ИЮЛЬ 2023 г.

Кроме того, крайне важно назначить специальную подготовку по безопасности для отдельных сотрудников или категорий сотрудников, вооружив их необходимыми знаниями и навыками для эффективного противодействия различным типам атак, с которыми они могут столкнуться в своих областях. Так как говоря о IoT системах мы не задумываемся что это могут быть все устройства, имеющие доступ в сеть от серверов до автомобилей, стоит помнить, что для безопасности каждого устройства нужно иметь свой подход. Повышая общий уровень осведомленности персонала ответственного за создания IoT уменьшает риски ИБ. Для повышения осведомленности требуется постоянное следование за прогрессом и изучения не только новых протоколов, но и методов атак как на инфраструктуру, так и на каждое отдельное устройство. Участие в постоянных конференция по информационной безопасности достаточно хорошо справляется с этим [17, 18]. 7. Сотрудничество с заинтересованными сторонами в улучшении общей безопасности использования IoT. Установление партнерских отношений и сотрудничества между производителями устройств IoT, сетевыми поставщиками и экспертами по безопасности может помочь коллективно решать проблемы безопасности. Это может включать в себя обмен информацией об угрозах, проведение аудитов безопасности и распространение передового опыта в области безопасности. Связи с исследовательскими компаниями, которые смогут протестировать устройство или целый программный комплекс на соответствие передовой безопасности хорошо улучшат репутацию на рынке как производителя безопасного продукта. Эти возможности подчеркивают необходимость постоянных инноваций и сотрудничества для решения постоянно меняющихся проблем безопасности в экосистеме IoT