https://www.sentinelone.com/cybersecurity-101/data-and-ai/iot-security-risks/

https://www.youtube.com/watch?v=PrIwGos7vHM&ab\_channel=SamsungInnovationCampus

IoT (Internet of Things) enjamlaryna edilýän atakalar, uly zyyanlara we howpsuzlyk meselelerine sebäp bolup biler. Aşakda IoT enjamlaryna edilip bilinýän atakalaryň sowly amala aşyrylyp, ýitirilýän we döredilen zyyanlar barada maglumat berilýär:

### 1. ****DDoS (Distributed Denial of Service) Atakasy****

* **Zyyanlar**:
  + **Hyzmatlaryň elýeterliliginiň ýitirilmegi**: DDoS atakasy, IoT enjamlarynyň aragatnaşygy arkaly bir web hyzmatyny ýa-da ulgamy çykarmak üçin giňden ulanylýar. Bu atakalar web serwerlerine ýa-da bulut hyzmatlaryna elýeterliligi çäklendirip, şol hyzmatlary ýa-da ulgamly serwisleri dowamly işlemeýän hala getirip biler.
  + **Maliýe ýitgileri**: Web sahypalarynyň ýa-da hyzmatlarynyň elýeterliliginiň bozulmagy müşderileriň we işiň ygtybarlygyny we mahabatyny ýitirmäge sebäp bolup biler. Bu bolsa maliýe ýitgilerine we ygtybarlylygyň bozulmagyna getirýär.

### 2. ****Brute Force Atakasy****

* **Zyyanlar**:
  + **Şahsy maglumatlaryň çalşygy**: IoT enjamlarynyň parollaryny tapmak üçin ulanylan brute force atakasy, enjamyň hasaplarynyň gowşaklyklaryny peýdalanyp, şahsy maglumatlary ýa-da kontentleri çalyp almak üçin mümkinçilik döredýär.
  + **Enjamyň basyp alynmagy**: Şahsy parollaryň ýa-da login maglumatlarynyň tapylmagy, enjamy basyp almak ýa-da ulanmak üçin hakerlere ýol açýar. Bu ýagdaýda enjamdan şübheli maksatlar üçin peýdalanmak mümkin.

### 3. ****Man-in-the-Middle (MITM) Atakasy****

* **Zyyanlar**:
  + **Maglumatlaryň aldanmagy**: MITM atakasy, aragatnaşykda bolan maglumatlary okap ýa-da üýtgedip, bu maglumatlaryň aldanmagyny döredýär. Hakerler şahsy maglumatlary, şifrlenmedik aragatnaşyk arkaly üýtgedip ýa-da öňünden alyp bilýärler.
  + **Şahsyýetiň ýoluna çykmagy**: Aragatnaşykda şahsy maglumatlaryň (şifrler, kart maglumatlary) çalyşylmagy, hakerleriň bu maglumatlary giňden peýdalanyp, başga biri hökmünde hereket etmegine sebäp bolup biler.

### 4. ****Firmware Atakalary****

* **Zyyanlar**:
  + **Enjamyň işini bozmak**: IoT enjamlarynyň firmware'ine edilýän atakalar, enjamyň işini basyp almak ýa-da bozmak üçin ulanylyp biler. Bu, enjamyň doly işini ýerine ýetirip bilmezlige getirer.
  + **Enjamyň gurnama mümkinçiliginiň ýok edilmegi**: Firmware'ine edilýän hüjümler, enjamy özgerdýän kodlary goýup, ulgamyň işine täsir eder. Bu ýagdaýda, enjamyň doly gurnama ýa-da täzelenme işleriniň ýerine ýetirilmegi mümkin däl bolup biler.

### 5. ****Sosial Injenerçilik (Social Engineering)****

* **Zyyanlar**:
  + **Şahsy maglumatlaryň açylmagy**: Sosial inženerlik, ulanyjynyň ynamyny gazanmak arkaly, onuň şahsy maglumatlaryny (parollar, maglumatlar) almak üçin ulanylyp bilner. Bu, enjamyň ýa-da ulgamyň hasaplaryna girmäge mümkinçilik döredýär.
  + **Zäherli linkleriň ýa-da kodlaryň täsir etmegi**: Hakerler ulanyjyny şübheli linkleri basmaga mejbur edip, bu link arkaly enjamda zäherli programma üpjünçiligini ýerleşdirip bilerler.

### 6. ****Cross-Site Scripting (XSS) Atakasy****

* **Zyyanlar**:
  + **Web interfeýsiniň bozulmagy**: XSS atakasy, web interfeýsine zäherli kod ýerleşdirip, enjamyň web sahypasyna täsir edip biler. Bu, ulanyjylaryň we maglumatlaryň howpsuzlygyny ýok eder.
  + **Şahsy maglumatlaryň çalyşylmagy**: XSS atakasy arkaly, şahsy maglumatlar (login maglumatlary, şifrler) çalynyp, şübheli maksada ýüklenip bilner.

### 7. ****SQL Injection Atakasy****

* **Zyyanlar**:
  + **Maglumat bazasynyň bozulmagy**: SQL injection atakasy, enjamyň maglumat bazasyna girmäge mümkinçilik berýär we bu maglumat bazasyny üýtgedip, adatça goýberilmedik maglumatlary alyp biler.
  + **Enjamdan we maglumatlardan peýdalanmak**: Hakerler, SQL injection arkaly, enjamdaky maglumatlary, şahsy maglumatlary ýa-da biznes maglumatlaryny almaga mümkinçilige eýe bolup bilerler.

### 8. ****Botnetler****

* **Zyyanlar**:
  + **Hyzmatyň elýeterliliginin bozulmagy**: Botnetler, IoT enjamlarynyň köpüsi bir arada bolanda, ulgamyň we hyzmatyň çäklendirilmegine ýa-da basyp alynmagyna sebäp bolup biler.
  + **Zäherli maksatlar üçin ulanylyp bilner**: IoT enjamlary botnetlere goşulyp, şübheli maksatlar üçin, mysal üçin, DDoS hüjümlerini amala aşyrmak üçin ulanylyp biler.

### 9. ****Zero-Day Atakalary****

* **Zyyanlar**:
  + **Enjamyň gowşaklygyny peýdalanmak**: Zero-day atakasy, enjamda ýa-da ulgamda öňünden ýüze çykmadyk gowşaklykdan peýdalanmagy mümkin edýär. Bu, enjamda howpsuzlyk gowşaklyklaryny tapyp, bu gowşaklygy ulanyp enjamyň basyp almagyna sebäp bolup biler.
  + **Täzelenmeleriň we aragatnaşyklaryň täsir etmegi**: Zero-day atakasy, täzelenme ýa-da enjamdaky gowşaklyklar zerarly, hakerlere enjamyň içindäki maglumatlary ýitirmäge ýa-da täsir etmäge mümkinçilik döredýär.

### 10. ****Physical Attacks (Fiziki Atakalar)****

* **Zyyanlar**:
  + **Enjamyň fiziki taýdan bozulyşy**: Fiziki atakalar, enjamyň fiziki taýdan kesilmegine ýa-da işiniň bozulmagyna sebäp bolup biler. Bu, enjamyň işini çäklendirip, ulgamdan çykmagyna sebäp bolup biler.
  + **Maglumatlaryň aşkar edilmegi**: Fiziki atakalar arkaly, enjamlar arkaly toplanan maglumatlar fiziki ýagdaýda olýalyp, olaryň gizlinligi we howpsuzlygy bozulýar.

Bu atakalar sowly amala aşyrylýan ýagdaýlarda, IoT enjamlary we olaryň sistemy üçin uly zyyanlar döredip biler. Hakerler, bu atakalar arkaly enjamlar ýa-da ulgamlara, olaryň işini basyp almak, şahsy maglumatlary almak we hasaplary basyp almak ýaly howplary döredýärler. Howpsuzlyk çärelere we täzelenmelere yzygiderli üns bermek, bu görnüşli atakalary peseltmekde we olaryň yzyna galmagyna garşy durmakda möhüm rol oýnaýar.

IoT (Internet of Things) enjamlaryna edilýän atakalar, uly zyyanlara we howpsuzlyk meselelerine sebäp bolup biler. Aşakda IoT enjamlaryna edilip bilinýän atakalaryň sowly amala aşyrylyp, ýitirilýän we döredilen zyyanlar barada maglumat berilýär:

### 1. ****DDoS (Distributed Denial of Service) Atakasy****

* **Zyyanlar**:
  + **Hyzmatlaryň elýeterliliginiň ýitirilmegi**: DDoS atakasy, IoT enjamlarynyň aragatnaşygy arkaly bir web hyzmatyny ýa-da ulgamy çykarmak üçin giňden ulanylýar. Bu atakalar web serwerlerine ýa-da bulut hyzmatlaryna elýeterliligi çäklendirip, şol hyzmatlary ýa-da ulgamly serwisleri dowamly işlemeýän hala getirip biler.
  + **Maliýe ýitgileri**: Web sahypalarynyň ýa-da hyzmatlarynyň elýeterliliginiň bozulmagy müşderileriň we işiň ygtybarlygyny we mahabatyny ýitirmäge sebäp bolup biler. Bu bolsa maliýe ýitgilerine we ygtybarlylygyň bozulmagyna getirýär.

### 2. ****Brute Force Atakasy****

* **Zyyanlar**:
  + **Şahsy maglumatlaryň çalşygy**: IoT enjamlarynyň parollaryny tapmak üçin ulanylan brute force atakasy, enjamyň hasaplarynyň gowşaklyklaryny peýdalanyp, şahsy maglumatlary ýa-da kontentleri çalyp almak üçin mümkinçilik döredýär.
  + **Enjamyň basyp alynmagy**: Şahsy parollaryň ýa-da login maglumatlarynyň tapylmagy, enjamy basyp almak ýa-da ulanmak üçin hakerlere ýol açýar. Bu ýagdaýda enjamdan şübheli maksatlar üçin peýdalanmak mümkin.

### 3. ****Man-in-the-Middle (MITM) Atakasy****

* **Zyyanlar**:
  + **Maglumatlaryň aldanmagy**: MITM atakasy, aragatnaşykda bolan maglumatlary okap ýa-da üýtgedip, bu maglumatlaryň aldanmagyny döredýär. Hakerler şahsy maglumatlary, şifrlenmedik aragatnaşyk arkaly üýtgedip ýa-da öňünden alyp bilýärler.
  + **Şahsyýetiň ýoluna çykmagy**: Aragatnaşykda şahsy maglumatlaryň (şifrler, kart maglumatlary) çalyşylmagy, hakerleriň bu maglumatlary giňden peýdalanyp, başga biri hökmünde hereket etmegine sebäp bolup biler.

### 4. ****Firmware Atakalary****

* **Zyyanlar**:
  + **Enjamyň işini bozmak**: IoT enjamlarynyň firmware'ine edilýän atakalar, enjamyň işini basyp almak ýa-da bozmak üçin ulanylyp biler. Bu, enjamyň doly işini ýerine ýetirip bilmezlige getirer.
  + **Enjamyň gurnama mümkinçiliginiň ýok edilmegi**: Firmware'ine edilýän hüjümler, enjamy özgerdýän kodlary goýup, ulgamyň işine täsir eder. Bu ýagdaýda, enjamyň doly gurnama ýa-da täzelenme işleriniň ýerine ýetirilmegi mümkin däl bolup biler.

### 5. ****Sosial Injenerçilik (Social Engineering)****

* **Zyyanlar**:
  + **Şahsy maglumatlaryň açylmagy**: Sosial inženerlik, ulanyjynyň ynamyny gazanmak arkaly, onuň şahsy maglumatlaryny (parollar, maglumatlar) almak üçin ulanylyp bilner. Bu, enjamyň ýa-da ulgamyň hasaplaryna girmäge mümkinçilik döredýär.
  + **Zäherli linkleriň ýa-da kodlaryň täsir etmegi**: Hakerler ulanyjyny şübheli linkleri basmaga mejbur edip, bu link arkaly enjamda zäherli programma üpjünçiligini ýerleşdirip bilerler.

### 6. ****Cross-Site Scripting (XSS) Atakasy****

* **Zyyanlar**:
  + **Web interfeýsiniň bozulmagy**: XSS atakasy, web interfeýsine zäherli kod ýerleşdirip, enjamyň web sahypasyna täsir edip biler. Bu, ulanyjylaryň we maglumatlaryň howpsuzlygyny ýok eder.
  + **Şahsy maglumatlaryň çalyşylmagy**: XSS atakasy arkaly, şahsy maglumatlar (login maglumatlary, şifrler) çalynyp, şübheli maksada ýüklenip bilner.

### 7. ****SQL Injection Atakasy****

* **Zyyanlar**:
  + **Maglumat bazasynyň bozulmagy**: SQL injection atakasy, enjamyň maglumat bazasyna girmäge mümkinçilik berýär we bu maglumat bazasyny üýtgedip, adatça goýberilmedik maglumatlary alyp biler.
  + **Enjamdan we maglumatlardan peýdalanmak**: Hakerler, SQL injection arkaly, enjamdaky maglumatlary, şahsy maglumatlary ýa-da biznes maglumatlaryny almaga mümkinçilige eýe bolup bilerler.

### 8. ****Botnetler****

* **Zyyanlar**:
  + **Hyzmatyň elýeterliliginin bozulmagy**: Botnetler, IoT enjamlarynyň köpüsi bir arada bolanda, ulgamyň we hyzmatyň çäklendirilmegine ýa-da basyp alynmagyna sebäp bolup biler.
  + **Zäherli maksatlar üçin ulanylyp bilner**: IoT enjamlary botnetlere goşulyp, şübheli maksatlar üçin, mysal üçin, DDoS hüjümlerini amala aşyrmak üçin ulanylyp biler.

### 9. ****Zero-Day Atakalary****

* **Zyyanlar**:
  + **Enjamyň gowşaklygyny peýdalanmak**: Zero-day atakasy, enjamda ýa-da ulgamda öňünden ýüze çykmadyk gowşaklykdan peýdalanmagy mümkin edýär. Bu, enjamda howpsuzlyk gowşaklyklaryny tapyp, bu gowşaklygy ulanyp enjamyň basyp almagyna sebäp bolup biler.
  + **Täzelenmeleriň we aragatnaşyklaryň täsir etmegi**: Zero-day atakasy, täzelenme ýa-da enjamdaky gowşaklyklar zerarly, hakerlere enjamyň içindäki maglumatlary ýitirmäge ýa-da täsir etmäge mümkinçilik döredýär.

### 10. ****Physical Attacks (Fiziki Atakalar)****

* **Zyyanlar**:
  + **Enjamyň fiziki taýdan bozulyşy**: Fiziki atakalar, enjamyň fiziki taýdan kesilmegine ýa-da işiniň bozulmagyna sebäp bolup biler. Bu, enjamyň işini çäklendirip, ulgamdan çykmagyna sebäp bolup biler.
  + **Maglumatlaryň aşkar edilmegi**: Fiziki atakalar arkaly, enjamlar arkaly toplanan maglumatlar fiziki ýagdaýda olýalyp, olaryň gizlinligi we howpsuzlygy bozulýar.

Bu atakalar sowly amala aşyrylýan ýagdaýlarda, IoT enjamlary we olaryň sistemy üçin uly zyyanlar döredip biler. Hakerler, bu atakalar arkaly enjamlar ýa-da ulgamlara, olaryň işini basyp almak, şahsy maglumatlary almak we hasaplary basyp almak ýaly howplary döredýärler. Howpsuzlyk çärelere we täzelenmelere yzygiderli üns bermek, bu görnüşli atakalary peseltmekde we olaryň yzyna galmagyna garşy durmakda möhüm rol oýnaýar.

Häzirki wagtda IoT enjamlaryna edilýän atakalar we olaryň amala aşyran zyyanlary baradaky hakykatdaky köp sanly wakalar we kynçylyklar bar. IoT ulgamynyň dünýäde giňden ulanylmagy, bu enjamlaryň howpsuzlyk gowşaklyklaryny we potensial zorluklary açyp görkezdi. Aşakda IoT enjamlaryna edilen uly atakalar we olaryň döredýän zyyanlary barada birnäçe hakykatlyk wakany we meseleleri ýatlap bileris:

### 1. ****Mirai Botnet Hüjümi (2016)****

* **Hüjüm**: Mirai botneti, 2016-njy ýylda IoT enjamlary arkaly amala aşyrylan iň uly DDoS hüjümlerinden biri bolup, enjamlar (kamera, routerler, TV'ler we beýleki IoT enjamlar) botnetleriň bir bölegine öwrüldi. Bu botnet, «Internet of Things» enjamlaryny ulanmak arkaly, internete bagly web serwislerine we serverlere uly basyş edip, olaryň işini basyp aldy.
* **Zyyanlar**:
  + **Hyzmatlaryň çäklendirilmegi**: Mirai botneti, Dyn (bir internet provayderi) we beýleki kompaniýalara garşy DDoS hüjümlerini amala aşyrdy. Bu hüjümler, onlarça şübheli ulgam we servisi basyp aldy.
  + **Maliýe Ýitgileri**: Şeýle hüjümler birnäçe kompaniýalaryň we hyzmatlaryň ýitirişine sebäp boldy. Ekranda ýüze çykýan hyzmatlaryň wagtynda işlemek üçin ähli hyzmatlaryň bozulmagy, ulanyjylara we kompaniýalara uly maliýe ýitgilerini getirýär.

### 2. ****Stuxnet (2010)****

* **Hüjüm**: Stuxnet, IoT we senagat ulgamyna garşy edilýän ilkinji giňden tanalan hüjümlerden biridir. Bu zäherli programma, Iran döwletiniň yklym energiýasy pudagyndaky natriýum merkezi we beýleki senagat enjamlaryny nygtap, olaryň işini hasaplap, fizik taýdan zoýun çykarmak üçin amala aşyryldy.
* **Zyyanlar**:
  + **Fiziki Zyyan**: Stuxnet, senagat ulgamlaryny çalt ýitirmäge we giňişleýin fiziki zyyanlara sebäp boldy. Bu hüjüm, öňki döwürde fiziki ulgamlara edilýän iň uly we tehnologik taýdan ösüşi ulanyp edilýän ataklaryň biri boldy.
  + **Maliýe Ýitgileri**: Senagat ulgamyndaky wagtyň geçmegi, tebigy gaz we gazada işlere bolan ykdysady ýitirişleri döretdi.

### 3. ****Target DDoS Atakasy (2013)****

* **Hüjüm**: 2013-nji ýylda ABŞ-nyň Target kompaniýasyna DDoS atakasy edilip, web serwisiniň ýa-da IoT enjamlarynyň ulanylyp, müşderi maglumatlarynyň giňişleýin açylmagyna sebäp boldy.
* **Zyyanlar**:
  + **Şahsy Maglumatlaryň Çalynmagy**: Bu atakalar müşderileriň şahsy maglumatlaryny, kredit kartalaryny we beýleki möhüm maglumatlary çalyşmaga sebäp boldy.
  + **Reputasiýa We Maliýe Ýitgileri**: Target kompaniýasy bu hüjüme garşy dürli jogapkärçilikleri almak we uly maliýe ýitgileri ýüze çykdy. Şeýle hüjümler kompaniýalaryň itibarını çalt ýitirmäge sebäp bolýar.

### 4. ****WannaCry Ransomware (2017)****

* **Hüjüm**: WannaCry, IoT we beýleki ulgamlara gurallary arkaly edilýän ransomware hüjümleriniň biri bolup, botnet ulgamlaryndan peýdalanylyp, dünýä boýunça ähli ulgamlara girmäge mümkinçilik berýärdi.
* **Zyyanlar**:
  + **Maglumatlaryň ýitirilmegi**: WannaCry hüjümi bilen, köp sanly kompýuterlere we ulgamlara gurallary şifrlemek we ondan maglumatlary almagy maksat edinmek üçin ulanyldy.
  + **Işleriň basylmagy**: Hüjüme sezewar bolan kompaniýalar we guramalar, öz ulgamyny we maglumatlaryny açmak üçin bölek-bölek tölegler we dolandyryşlarynda güýçli kynçylyklar görýärdi.

### 5. ****Hackerler tarapyndan IoT Enjamlarynyň Basyp Alnmagy****

* **Hüjümler**: 2017-nji ýylda, hakerler IoT enjamlary arkaly Wi-Fi-routerlere, kameralara, öýdeki awtomatlaşdyrylan ulgamlara we beýleki IoT enjamlaryna girmäge başladylar. Bu atakalar, şahsy maglumatlary almak we enjamdan şübheli maksatlar üçin peýdalanmak üçin amala aşyryldy.
* **Zyyanlar**:
  + **Şahsy Maglumatlaryň Çalynmagy**: Enjamlar fiziki ýa-da aragatnaşyk arkaly şübheli peýdalanyldy, bu bolsa ulanyjylaryň maglumatlarynyň ýitirilmegine sebäp boldy.
  + **Aşkar Edilen Ulgamlar**: Enjamlar, howpsuzlyk gowşaklyklary we parol sowadyşlary arkaly ulanyldy, olardan ýüzlerçe adam, IoT enjamlarynyň işine täsir edip, hasaplaryna girmäge mümkinçilik tapdy.

### Netije

IoT enjamlary we ulgamlary üçin atakalar dünýäde dürli uly zyyanlary döretdi. Bu zyyanlar diňe sanly dünýäde däl, eýsem fiziki we maliýe taýdan-da uly täsirler galdyrdy. Netijede, IoT enjamlary üçin howpsuzlyk çärelere degişli esaslykly ulaglar we tejribeler (şifrlenme, parol üpjünçiligi, täzelenmeler) gurnalan. Bu hüjümler, ýönekeý adamlaryň we kompaniýalaryň IoT ulgamlaryna bolan ynamynyň azalmagyna sebäp boldy. Howpsuzlyk derejesi ýokarlandyrylmadyk ýagdaýda, täze atakalar has giňişleýin zyyan döredip biler.

## Типы рисков Интернета вещей

Разнообразие устройств, приложений и сетей Интернета вещей порождает множество потенциальных рисков, в том числе:

* **Конфиденциальность данных:**  устройства Интернета вещей часто собирают и передают огромные объемы конфиденциальных данных, что делает их привлекательными целями для киберпреступников, стремящихся использовать личную или конфиденциальную информацию.
* **Перехват устройств:**  злоумышленники могут взломать устройства IoT, получить контроль над их функциями и использовать их для запуска дальнейших атак или срыва операций.
* **Атаки типа «отказ в обслуживании» (DoS):**  крупномасштабные ботнеты, состоящие из взломанных устройств Интернета вещей, могут быть использованы для подавления и отключения критически важной инфраструктуры и онлайн-сервисов.
* **Атаки «человек посередине» (MitM):**  злоумышленники могут перехватывать сообщения между устройствами Интернета вещей и их предполагаемыми получателями, что позволяет осуществлять прослушивание и манипулирование данными.
* **Уязвимости прошивки:**  недостатки в программном обеспечении, управляющем устройствами IoT, могут стать для злоумышленников возможностью использовать уязвимости и получить несанкционированный доступ.
* **Атаки на цепочку поставок:**  Взлом цепочки поставок устройств Интернета вещей может привести к внедрению вредоносного кода или компонентов, что сделает устройства уязвимыми для атак.
* **Риски физической безопасности:**  Физическая доступность устройств Интернета вещей может сделать их уязвимыми для взлома, кражи или несанкционированного доступа к конфиденциальным данным.

Интернет вещей (IoT) — это термин, используемый для описания сети взаимосвязанных электронных устройств с «умной» технологией. В то время как смартфоны теперь стали обычным явлением, другие умные устройства все еще находятся в зачаточном состоянии, но их использование постоянно растет, и в настоящее время [к Интернету подключено около 6,4 млрд «вещей»](http://www.gartner.com/newsroom/id/3165317) , что на 30% больше, чем в 2015 году. Ожидается, что в 2020 году это число вырастет до [ошеломляющих 20,8 млрд.](https://www.symantec.com/content/dam/symantec/docs/infographics/istr-iot-en.pdf)

К таким интеллектуальным устройствам относятся автомобили, бытовая техника, системы зданий, такие как освещение и отопление, телевизоры, медицинские приборы, производственное оборудование и многие другие типы систем, используемых как в потребительских, так и в промышленных условиях.

Умные устройства призваны сделать нашу жизнь проще и удобнее. Например, системы домашней автоматизации позволяют домовладельцам включать термостат по пути домой с работы зимой или немедленно получать оповещения о предполагаемом вторжении в дом, пока их нет дома.

Однако все это дополнительное оборудование и программное обеспечение, подключенное к Интернету и потенциально доступное любому человеку (при наличии соответствующих учетных данных или через уязвимость программного обеспечения), представляет огромную угрозу безопасности предприятий и частных лиц, которые его используют.

## Риски безопасности устройств Интернета вещей

Любое используемое вами оборудование и программное обеспечение, подключенное к Интернету, может быть потенциально доступно киберпреступникам. С появлением каждого нового устройства растет число потенциальных точек доступа для хакеров.

Уже было несколько примеров взлома или уязвимости смарт-устройств, в том числе:

* Многие [интеллектуальные медицинские устройства,](http://www.24x7mag.com/2014/08/beware-nine-medical-device-vulnerabilities/) включая инсулиновые помпы и внутренние дефибрилляторы, используют устаревшее программное обеспечение и незашифрованные данные, что создает серьезные уязвимости с точки зрения конфиденциальности и физического благополучия пациентов.
* Миллионы [смарт-телевизоров](https://www.symantec.com/connect/blogs/how-my-tv-got-infected-ransomware-and-what-you-can-learn-it) подвержены риску мошенничества с кликами, бот-сетей, кражи данных и программ-вымогателей.
* [1,4 миллиона автомобилей Fiat Chrysler были отозваны](http://money.cnn.com/2015/07/24/technology/chrysler-hack-recall/) после того, как исследователи обнаружили, что с их помощью можно получить доступ к автомобилям и управлять ими удаленно через Интернет, в том числе выключить двигатель и съехать с дороги.
* Обнаружено, что [75% дверных замков с технологией Bluetooth Smart имеют уязвимости, позволяющие легко их взломать.](https://www.cnet.com/news/have-a-smart-lock-yeah-it-can-probably-be-hacked/)
* Недавно была осуществлена [​​крупнейшая в истории DDoS-атака с использованием более 150 000 взломанных смарт-устройств по всему миру, включая камеры, принтеры и холодильники.](http://thehackernews.com/2016/09/ddos-attack-iot.html)

Эксперты по безопасности предупреждают, что многие смарт-устройства уязвимы для атак, поскольку они не проходят достаточного тестирования безопасности, часто используют устаревшее программное обеспечение, и на них невозможно установить брандмауэр или другое защитное программное обеспечение, как это можно сделать на обычном компьютере.

Поскольку компьютерное программное обеспечение становится все более надежным и устойчивым к вредоносным атакам, хакеры обращаются к новому поколению интеллектуальных устройств как к более простому варианту, часто добиваясь большого успеха.

## Почему умные устройства так уязвимы?

Есть несколько причин, по которым Интернет вещей представляет такую ​​угрозу нашей цифровой безопасности. [Исследование, проведенное HP,](https://www.scribd.com/document/263392568/IOT-Research-Study-by-HP) рассмотрело некоторые из самых популярных устройств IoT, чтобы оценить их общий уровень безопасности, и обнаружило несколько проблемных моментов:

### 1. Отсутствие защиты личных данных

Большинство потребительских смарт-устройств (90% из тех, которые были оценены в исследовании) хранят персональные [конфиденциальные данные пользователя](https://spin.ai/blog/sensitive-data-protection/)  либо на самом устройстве, либо в облаке, либо через мобильное приложение, которое интегрируется с устройством. Эти данные часто не защищены должным образом и часто передаются в незашифрованном виде по сетям.

### 2. Небезопасное программное обеспечение

Поскольку интеллектуальные технологии развиваются так быстро, производители вынуждены как можно быстрее выводить свою продукцию на рынок. Это означает, что важные части жизненного цикла программного обеспечения, такие как безопасность и тестирование, часто выполняются в спешке.

Хотя обновления для таких устройств, как правило, выпускаются регулярно, 60% опрошенных загружали эти обновления автоматически без шифрования. Это означает, что существует вероятность перехвата и изменения загрузки хакерами.

Во многих случаях уязвимости не могут быть устранены немедленно, поскольку компания не хочет беспокоить своих пользователей, заставляя их обновлять прошивку.

### 3. Недостаточная процедура аутентификации

Небезопасные пароли и [управление облачной идентификацией](https://spin.ai/blog/sensitive-data-protection/) являются распространенной уязвимостью во всех видах цифровых систем. Хотя большинство компьютерных программ теперь заставляют пользователей создавать надежный пароль, это не относится ко всем смарт-устройствам.

Кроме того, пользователи часто используют пароли для нескольких аккаунтов. Если безопасность подключенного устройства недостаточна и хакеры получают доступ к паролю, они могут использовать этот пароль для доступа к другим, более конфиденциальным аккаунтам, принадлежащим пользователю.

80% протестированных устройств не требовали достаточно длинных и сложных паролей.

### 4. Отсутствие шифрования данных

Было обнаружено, что 70% устройств отправляют данные по сети в незашифрованном виде. [Шифрование данных необходимо](https://spin.ai/blog/what-is-the-reason-for-encrypting-data-in-a-backup/) для предотвращения их перехвата неавторизованными лицами, особенно при передаче через Интернет между облаком и устройством или мобильным приложением.

### 5. Плохо закодированный пользовательский интерфейс

Более половины протестированных устройств имели плохо закодированные веб-интерфейсы, что приводило к уязвимостям безопасности из-за таких проблем, как плохая обработка сеансов, слабые учетные данные по умолчанию и постоянный межсайтовый скриптинг.

Эти уязвимости безопасности позволяют хакерам легко получить доступ к веб-интерфейсу с помощью таких уловок, как использование функции сброса пароля, и таким образом получить доступ к данным и управлению самим устройством.

## Как сделать Интернет вещей более безопасным?

Безопасность Интернета вещей начинает восприниматься все серьезнее, и [даже ФБР](https://www.ic3.gov/media/2015/150910.aspx) выпустило предупреждения о рисках безопасности, которые могут возникнуть при использовании таких устройств.

Несколько советов безопасности и альянсов также были созданы различными технологическими организациями с целью разработки передовых методов и предоставления образования по надлежащей защите интеллектуальных устройств. К ним относятся [Совет безопасности Интернета вещей](http://www.smartcardalliance.org/activities-councils-internet-of-things-security/) и [Фонд безопасности Интернета вещей.](https://iotsecurityfoundation.org/)

В то время как производители должны брать на себя большую ответственность за создание защищенных устройств и выпуск исправлений безопасности сразу после обнаружения уязвимостей, частные лица и компании, использующие устройства Интернета вещей, также должны убедиться, что они приняли собственные меры безопасности.

Одним из возможных решений являются интегрированные в облако панели управления безопасностью, которые отслеживают подключенные интеллектуальные устройства и информируют пользователя о рисках и компрометациях безопасности с помощью [интеллектуальных](https://spin.ai/blog/cloud-insider-threats-control-for-google-workspace/)[инструментов](https://spin.ai/blog/data-loss-prevention-tools-advantages/) обнаружения угроз   и предотвращения потери данных.

Также важно, чтобы облачные сервисы, используемые устройствами для хранения пользовательских данных, были безопасными, чтобы предотвратить серьезные [утечки данных](https://spin.ai/blog/how-to-implement-data-leak-prevention-in-google-workspace/) .

Чтобы обеспечить достаточный уровень цифровой безопасности в корпоративной среде, ИТ-отделы должны полностью интегрировать интеллектуальные устройства в [общие процессы мониторинга](https://spin.ai/blog/spin-ai-releases-google-workspace-security-policies/) и тестирования безопасности.

Перед покупкой компаниям также следует [учитывать риски безопасности,](https://spin.ai/blog/cybersecurity-awareness-importance-and-purpose/) связанные с интеллектуальными устройствами, и сопоставлять эти риски с преимуществами, которые они предоставляют компании.

Под давлением конечных пользователей производители, скорее всего, будут уделять больше внимания безопасности, начиная с первоначального производства и заканчивая обновлениями и исправлениями программного обеспечения.

Aşakda IoT (Internet of Things) enjamlaryna edilýän iň möhüm 10 atak, olaryň getiren zyyanlary we nämäniň ýaly ataklaryň haýsy ýagdaýlarda ýerine ýetirildigi barada maglumatlar berilýär:

### 1. ****Mirai Botnet Atakasy (2016)****

* **Näme edilendir?**: Mirai botneti, IoT enjamlarynyň (kamera, routerler, printerler we ş.m.) gurnalmagy arkaly, hakerler bu enjamlary botnetlere öwürdüler we soňra bu botnetlerden DDoS (Distributed Denial of Service) hüjümleri üçin peýdalandylar.
* **Zyyanlar**:
  + **Web hyzmatlarynyň we serwisleriň bozulmagy**: Mirai, Dyn, Twitter, Reddit, GitHub ýaly birnäçe uly web serwislerine DDoS hüjümleri düzen we olaryň çäklendirilmegine sebäp boldy.
  + **Maliýe ýitgileri**: Serwisleriň işlemeýän wagty, milyardlarça dollar maliýe ýitgi döredildi.
* **Ýerine ýetirilýän ýer**: ABŞ, Ýaponiýa, we beýleki ýurtlarda dürli internet hyzmatlaryna garşy hüjümler.

### 2. ****Stuxnet (2010)****

* **Näme edilendir?**: Stuxnet, IoT we senagat ulgamyny nygtap, atom reaktoryndaky enjamlar üçin ýörite döredilen zäherli programma (worm) bolup, Senagat we nebitgaz pudaklaryny nygtap, enjamda fiziki zeperler ýetirdi.
* **Zyyanlar**:
  + **Fiziki zeperler**: Stuxnet, Iranyň Natanzdaky urany aýyrmak üçin ulanylýan merkeziyini we beýleki enjamları nygtap, olaryň işini bozdy.
  + **Senagat ulgamynyň howpsuzlyk gowşaklygy**: Stuxnet, täze enjamlaryň we tehnologiyalaryň gowşaklygyny açyp, şunuň ýaly ataklaryň käbiriniň fiziki ulgamlara degişli bolandygyny görkezdi.
* **Ýerine ýetirilýän ýer**: Iran (Natanz), dünýäde beýleki senagat we tehnologik ulgamlara täsir etdi.

### 3. ****DDoS Atakasy (Dyn, 2016)****

* **Näme edilendir?**: Dyn kompaniýasyna edilýän DDoS hüjümi, IoT enjamlary (kamera, router, printerler) arkaly, bu enjamlary botnetlere öwürüp, neteň web serwislerine we internete serwerlerine saldırmak üçin ulanyldy.
* **Zyyanlar**:
  + **Web hyzmatlarynyň elýeterliligi ýitirilýär**: Dyn hyzmatynyň bozulmagy, bir gämi hyzmatyny (GitHub, Twitter, Reddit) çäklendirip, malyýedäki ýitgiler bolup geçdi.
  + **Reputasiýa we maliýe ýitgi**: Ulgam bozulmasy sebäpli internet ulgamynyň hasaplamasyna zäherli täsirler ýetdi.
* **Ýerine ýetirilýän ýer**: ABŞ, beýleki dünýä ýurtlary.

### 4. ****WannaCry Ransomware (2017)****

* **Näme edilendir?**: WannaCry, şifrlenmedik we öňki Windows ulgamyny ulanýan IoT enjamlar üçin ýagny şifrlenmedik we gowşak ulgamlara görnüşde girýär we global derejesinde şifrlemäge sebäp boldy.
* **Zyyanlar**:
  + **Maglumatlaryň ýitirilmegi**: Ransomware, şifrlenen maglumatlary almaýar, bu enjamda maglumatlary ýitirýär.
  + **Maliýe ýitgileri**: Kompaniýalar, guramalar üçin resminamalary, ähli maglumatlary we maliýe hyzmatlary çalyşylýar.
* **Ýerine ýetirilýän ýer**: Dünýäniň dürli ýerlerinde, hususan-da, Britaniýa, Fransiýa, Russiýa, Hindistan ýaly ýurtlarda.

### 5. ****Brute Force Atakasy****

* **Näme edilendir?**: Brute force atakasy, IoT enjamynyň şifrini ýa-da login maglumatlaryny tapmak üçin ähli mümkin bolan kombinasiýalary synap görýär. Bu atakalar, enjamyň gowşak şifrlendirilmiş parollaryny tapmak üçin amala aşyrylýar.
* **Zyyanlar**:
  + **Enjamyň basyp alynmagy**: Parollar tapylandan soň, enjam ulanyjynyň hasaplaryna girip, maglumatlary alyp bilýär.
  + **Şahsy maglumatlaryň ýitirilmegi**: Şahsy maglumatlar, kamera, router, öý awtomatlaşdyrylyşy ýaly enjamlar ulanylar.
* **Ýerine ýetirilýän ýer**: Dünýäniň ähli ýerlerinde, esasanam ulanyjylaryň gowşak parollary ulanýan ýerlerde.

### 6. ****Man-in-the-Middle (MITM) Atakasy****

* **Näme edilendir?**: MITM hüjümi, iki enjam arasynda aragatnaşygyň gözegçilik edilmegini aňladýar. Hakerler, şifrlenmedik maglumatlary okap ýa-da üýtgedip bilýärler.
* **Zyyanlar**:
  + **Maglumatlaryň aşkar edilmegi**: Şahsy we gizlin maglumatlar üýtgedilip ýa-da okalyp bilner.
  + **Enjamyň we maglumatlaryň howpsuzlygynyň bozulmagy**.
* **Ýerine ýetirilýän ýer**: Dünýäniň dürli ýerlerinde, esasanam şifrlenmedik Wi-Fi jaýlarynda.

### 7. ****SQL Injection****

* **Näme edilendir?**: SQL injection atakasy, IoT enjamlarynyň arka plandaky maglumat bazasyna SQL kodlary ýazylyp, ulanyjylaryň maglumatlaryna ýa-da ulgam resminamalaryna girmäge mümkinçilik berýär.
* **Zyyanlar**:
  + **Maglumatlaryň çalynmagy**: Hakerler, maglumat bazasyna girip, şahsy maglumatlary ýa-da iş maglumatlaryny alyp bilýärler.
  + **Ulgamyň işiniň bozulmagy**: Ulgamda SQL soraglaryny üýtgedip, tizligi ýa-da hyzmaty bozulýar.
* **Ýerine ýetirilýän ýer**: Ulgamlar we IoT enjamlary web aragatnaşyk protokollary arkaly.

### 8. ****Zero-Day Atakasy****

* **Näme edilendir?**: Zero-day atakasy, öňünden kesgitlenmedik gowşaklykdan peýdalanyp, enjamyň howpsuzlygyny bozup, ýalňyş programmalary girizip, enjamy basyp alýar.
* **Zyyanlar**:
  + **Enjamyň işini bozmak**: Enjamlar, onuň ykjam işlerini bozmak ýa-da özbaşdak hereket etmek üçin ulanylyp bilner.
  + **Enjamyň fiziki zeperleri**.
* **Ýerine ýetirilýän ýer**: Dünyada her bir täze gowşaklyk ýüze çykan ýerlerde.

### 9. ****Cross-Site Scripting (XSS)****

* **Näme edilendir?**: XSS atakasy, web interfeýsine zäherli kod ýerleşdirip, ulanyjylara seredilen sahypa ýa-da çemeleşmeler arkaly hakerleriň enjamy basyp almagy üçin işleýär.
* **Zyyanlar**:
  + **Şahsy maglumatlaryň alnanlygy**: Şahsy maglumatlar, loginler we şifrler çalyşylýar.
* **Ýerine ýetirilýän ýer**: IoT enjamlarynyň web interfeýsi ulanylan ýerlerde.

### 10. ****Botnet Atakasy****

* **Näme edilendir?**: Botnetler, IoT enjamlarynyň köpüsini bir arada gurup, zäherli maksatlar üçin ulanylan botneteri düzýär.
* **Zyyanlar**:
  + **Enjamlaryň we ulgamlaryň işiniň bozulmagy**: DDoS hüjümleri we enjamlaryň basyp alynmagy.
* **Ýerine ýetirilýän ýer**: Dünyada IoT enjamlarynyň köpçülikleýin ulanylandygy ýerlerde.

Bu atakalar we zyyanlar, IoT enjamlarynyň gowşaklyklarını we howpsuzlyk gowşaklyklaryny görkezýär. Howpsuzlyk çärelerine, şifrlenmäge, täzelenmelere we parol howpsuzlygyna üns bermek, IoT ulgamlarynyň howpsuzlygyny güýçlendirmäge kömek eder.