2025/03/11 15:46:06

[https://www.tadviser.ru/images/5/58/Labelpub2.jpg](https://www.tadviser.ru/index.php/%D0%A1%D1%82%D0%B0%D1%82%D1%8C%D0%B8)

**Информационная безопасность интернета вещей  
(Internet of Things)**

Данная статья посвящена аспектам информационной безопасности интернета вещей, в том числе, инцидентам, связанным с этой технологией.

|  |
| --- |
| Содержание  [[Свернуть](javascript:toggleToc())]   * + [Стандартизация в области безопасности](https://www.tadviser.ru/index.php/%D0%A1%D1%82%D0%B0%D1%82%D1%8C%D1%8F:%D0%98%D0%BD%D1%84%D0%BE%D1%80%D0%BC%D0%B0%D1%86%D0%B8%D0%BE%D0%BD%D0%BD%D0%B0%D1%8F_%D0%B1%D0%B5%D0%B7%D0%BE%D0%BF%D0%B0%D1%81%D0%BD%D0%BE%D1%81%D1%82%D1%8C_%D0%B8%D0%BD%D1%82%D0%B5%D1%80%D0%BD%D0%B5%D1%82%D0%B0_%D0%B2%D0%B5%D1%89%D0%B5%D0%B9_(Internet_of_Things)#.D0.A1.D1.82.D0.B0.D0.BD.D0.B4.D0.B0.D1.80.D1.82.D0.B8.D0.B7.D0.B0.D1.86.D0.B8.D1.8F_.D0.B2_.D0.BE.D0.B1.D0.BB.D0.B0.D1.81.D1.82.D0.B8_.D0.B1.D0.B5.D0.B7.D0.BE.D0.BF.D0.B0.D1.81.D0.BD.D0.BE.D1.81.D1.82.D0.B8)     - [**2025: ФСТЭК представила стандарт разработки систем с иммунитетом к киберугрозам**](https://www.tadviser.ru/index.php/%D0%A1%D1%82%D0%B0%D1%82%D1%8C%D1%8F:%D0%98%D0%BD%D1%84%D0%BE%D1%80%D0%BC%D0%B0%D1%86%D0%B8%D0%BE%D0%BD%D0%BD%D0%B0%D1%8F_%D0%B1%D0%B5%D0%B7%D0%BE%D0%BF%D0%B0%D1%81%D0%BD%D0%BE%D1%81%D1%82%D1%8C_%D0%B8%D0%BD%D1%82%D0%B5%D1%80%D0%BD%D0%B5%D1%82%D0%B0_%D0%B2%D0%B5%D1%89%D0%B5%D0%B9_(Internet_of_Things)#.2A2025:_.D0.A4.D0.A1.D0.A2.D0.AD.D0.9A_.D0.BF.D1.80.D0.B5.D0.B4.D1.81.D1.82.D0.B0.D0.B2.D0.B8.D0.BB.D0.B0_.D1.81.D1.82.D0.B0.D0.BD.D0.B4.D0.B0.D1.80.D1.82_.D1.80.D0.B0.D0.B7.D1.80.D0.B0.D0.B1.D0.BE.D1.82.D0.BA.D0.B8_.D1.81.D0.B8.D1.81.D1.82.D0.B5.D0.BC_.D1.81_.D0.B8.D0.BC.D0.BC.D1.83.D0.BD.D0.B8.D1.82.D0.B5.D1.82.D0.BE.D0.BC_.D0.BA_.D0.BA.D0.B8.D0.B1.D0.B5.D1.80.D1.83.D0.B3.D1.80.D0.BE.D0.B7.D0.B0.D0.BC)     - [2019: Российские эксперты стали соредакторами международного стандарта интернета вещей в области безопасности](https://www.tadviser.ru/index.php/%D0%A1%D1%82%D0%B0%D1%82%D1%8C%D1%8F:%D0%98%D0%BD%D1%84%D0%BE%D1%80%D0%BC%D0%B0%D1%86%D0%B8%D0%BE%D0%BD%D0%BD%D0%B0%D1%8F_%D0%B1%D0%B5%D0%B7%D0%BE%D0%BF%D0%B0%D1%81%D0%BD%D0%BE%D1%81%D1%82%D1%8C_%D0%B8%D0%BD%D1%82%D0%B5%D1%80%D0%BD%D0%B5%D1%82%D0%B0_%D0%B2%D0%B5%D1%89%D0%B5%D0%B9_(Internet_of_Things)#2019:_.D0.A0.D0.BE.D1.81.D1.81.D0.B8.D0.B9.D1.81.D0.BA.D0.B8.D0.B5_.D1.8D.D0.BA.D1.81.D0.BF.D0.B5.D1.80.D1.82.D1.8B_.D1.81.D1.82.D0.B0.D0.BB.D0.B8_.D1.81.D0.BE.D1.80.D0.B5.D0.B4.D0.B0.D0.BA.D1.82.D0.BE.D1.80.D0.B0.D0.BC.D0.B8_.D0.BC.D0.B5.D0.B6.D0.B4.D1.83.D0.BD.D0.B0.D1.80.D0.BE.D0.B4.D0.BD.D0.BE.D0.B3.D0.BE_.D1.81.D1.82.D0.B0.D0.BD.D0.B4.D0.B0.D1.80.D1.82.D0.B0_.D0.B8.D0.BD.D1.82.D0.B5.D1.80.D0.BD.D0.B5.D1.82.D0.B0_.D0.B2.D0.B5.D1.89.D0.B5.D0.B9_.D0.B2_.D0.BE.D0.B1.D0.BB.D0.B0.D1.81.D1.82.D0.B8_.D0.B1.D0.B5.D0.B7.D0.BE.D0.BF.D0.B0.D1.81.D0.BD.D0.BE.D1.81.D1.82.D0.B8)   + [Законодательство](https://www.tadviser.ru/index.php/%D0%A1%D1%82%D0%B0%D1%82%D1%8C%D1%8F:%D0%98%D0%BD%D1%84%D0%BE%D1%80%D0%BC%D0%B0%D1%86%D0%B8%D0%BE%D0%BD%D0%BD%D0%B0%D1%8F_%D0%B1%D0%B5%D0%B7%D0%BE%D0%BF%D0%B0%D1%81%D0%BD%D0%BE%D1%81%D1%82%D1%8C_%D0%B8%D0%BD%D1%82%D0%B5%D1%80%D0%BD%D0%B5%D1%82%D0%B0_%D0%B2%D0%B5%D1%89%D0%B5%D0%B9_(Internet_of_Things)#.D0.97.D0.B0.D0.BA.D0.BE.D0.BD.D0.BE.D0.B4.D0.B0.D1.82.D0.B5.D0.BB.D1.8C.D1.81.D1.82.D0.B2.D0.BE)     - [2020: Великобритания готовит закон по защите IoT-устройств](https://www.tadviser.ru/index.php/%D0%A1%D1%82%D0%B0%D1%82%D1%8C%D1%8F:%D0%98%D0%BD%D1%84%D0%BE%D1%80%D0%BC%D0%B0%D1%86%D0%B8%D0%BE%D0%BD%D0%BD%D0%B0%D1%8F_%D0%B1%D0%B5%D0%B7%D0%BE%D0%BF%D0%B0%D1%81%D0%BD%D0%BE%D1%81%D1%82%D1%8C_%D0%B8%D0%BD%D1%82%D0%B5%D1%80%D0%BD%D0%B5%D1%82%D0%B0_%D0%B2%D0%B5%D1%89%D0%B5%D0%B9_(Internet_of_Things)#2020:_.D0.92.D0.B5.D0.BB.D0.B8.D0.BA.D0.BE.D0.B1.D1.80.D0.B8.D1.82.D0.B0.D0.BD.D0.B8.D1.8F_.D0.B3.D0.BE.D1.82.D0.BE.D0.B2.D0.B8.D1.82_.D0.B7.D0.B0.D0.BA.D0.BE.D0.BD_.D0.BF.D0.BE_.D0.B7.D0.B0.D1.89.D0.B8.D1.82.D0.B5_IoT-.D1.83.D1.81.D1.82.D1.80.D0.BE.D0.B9.D1.81.D1.82.D0.B2)   + [Теоретические аспекты ИБ интернета вещей](https://www.tadviser.ru/index.php/%D0%A1%D1%82%D0%B0%D1%82%D1%8C%D1%8F:%D0%98%D0%BD%D1%84%D0%BE%D1%80%D0%BC%D0%B0%D1%86%D0%B8%D0%BE%D0%BD%D0%BD%D0%B0%D1%8F_%D0%B1%D0%B5%D0%B7%D0%BE%D0%BF%D0%B0%D1%81%D0%BD%D0%BE%D1%81%D1%82%D1%8C_%D0%B8%D0%BD%D1%82%D0%B5%D1%80%D0%BD%D0%B5%D1%82%D0%B0_%D0%B2%D0%B5%D1%89%D0%B5%D0%B9_(Internet_of_Things)#.D0.A2.D0.B5.D0.BE.D1.80.D0.B5.D1.82.D0.B8.D1.87.D0.B5.D1.81.D0.BA.D0.B8.D0.B5_.D0.B0.D1.81.D0.BF.D0.B5.D0.BA.D1.82.D1.8B_.D0.98.D0.91_.D0.B8.D0.BD.D1.82.D0.B5.D1.80.D0.BD.D0.B5.D1.82.D0.B0_.D0.B2.D0.B5.D1.89.D0.B5.D0.B9)     - [Безопасной экосистемы IoT не существует](https://www.tadviser.ru/index.php/%D0%A1%D1%82%D0%B0%D1%82%D1%8C%D1%8F:%D0%98%D0%BD%D1%84%D0%BE%D1%80%D0%BC%D0%B0%D1%86%D0%B8%D0%BE%D0%BD%D0%BD%D0%B0%D1%8F_%D0%B1%D0%B5%D0%B7%D0%BE%D0%BF%D0%B0%D1%81%D0%BD%D0%BE%D1%81%D1%82%D1%8C_%D0%B8%D0%BD%D1%82%D0%B5%D1%80%D0%BD%D0%B5%D1%82%D0%B0_%D0%B2%D0%B5%D1%89%D0%B5%D0%B9_(Internet_of_Things)#.D0.91.D0.B5.D0.B7.D0.BE.D0.BF.D0.B0.D1.81.D0.BD.D0.BE.D0.B9_.D1.8D.D0.BA.D0.BE.D1.81.D0.B8.D1.81.D1.82.D0.B5.D0.BC.D1.8B_IoT_.D0.BD.D0.B5_.D1.81.D1.83.D1.89.D0.B5.D1.81.D1.82.D0.B2.D1.83.D0.B5.D1.82)     - [Слабые места IoT](https://www.tadviser.ru/index.php/%D0%A1%D1%82%D0%B0%D1%82%D1%8C%D1%8F:%D0%98%D0%BD%D1%84%D0%BE%D1%80%D0%BC%D0%B0%D1%86%D0%B8%D0%BE%D0%BD%D0%BD%D0%B0%D1%8F_%D0%B1%D0%B5%D0%B7%D0%BE%D0%BF%D0%B0%D1%81%D0%BD%D0%BE%D1%81%D1%82%D1%8C_%D0%B8%D0%BD%D1%82%D0%B5%D1%80%D0%BD%D0%B5%D1%82%D0%B0_%D0%B2%D0%B5%D1%89%D0%B5%D0%B9_(Internet_of_Things)#.D0.A1.D0.BB.D0.B0.D0.B1.D1.8B.D0.B5_.D0.BC.D0.B5.D1.81.D1.82.D0.B0_IoT)     - [Насколько безопасны «умные дома будущего»](https://www.tadviser.ru/index.php/%D0%A1%D1%82%D0%B0%D1%82%D1%8C%D1%8F:%D0%98%D0%BD%D1%84%D0%BE%D1%80%D0%BC%D0%B0%D1%86%D0%B8%D0%BE%D0%BD%D0%BD%D0%B0%D1%8F_%D0%B1%D0%B5%D0%B7%D0%BE%D0%BF%D0%B0%D1%81%D0%BD%D0%BE%D1%81%D1%82%D1%8C_%D0%B8%D0%BD%D1%82%D0%B5%D1%80%D0%BD%D0%B5%D1%82%D0%B0_%D0%B2%D0%B5%D1%89%D0%B5%D0%B9_(Internet_of_Things)#.D0.9D.D0.B0.D1.81.D0.BA.D0.BE.D0.BB.D1.8C.D0.BA.D0.BE_.D0.B1.D0.B5.D0.B7.D0.BE.D0.BF.D0.B0.D1.81.D0.BD.D1.8B_.C2.AB.D1.83.D0.BC.D0.BD.D1.8B.D0.B5_.D0.B4.D0.BE.D0.BC.D0.B0_.D0.B1.D1.83.D0.B4.D1.83.D1.89.D0.B5.D0.B3.D0.BE.C2.BB)     - [Сертификация устройств IoT для защиты от хакеров](https://www.tadviser.ru/index.php/%D0%A1%D1%82%D0%B0%D1%82%D1%8C%D1%8F:%D0%98%D0%BD%D1%84%D0%BE%D1%80%D0%BC%D0%B0%D1%86%D0%B8%D0%BE%D0%BD%D0%BD%D0%B0%D1%8F_%D0%B1%D0%B5%D0%B7%D0%BE%D0%BF%D0%B0%D1%81%D0%BD%D0%BE%D1%81%D1%82%D1%8C_%D0%B8%D0%BD%D1%82%D0%B5%D1%80%D0%BD%D0%B5%D1%82%D0%B0_%D0%B2%D0%B5%D1%89%D0%B5%D0%B9_(Internet_of_Things)#.D0.A1.D0.B5.D1.80.D1.82.D0.B8.D1.84.D0.B8.D0.BA.D0.B0.D1.86.D0.B8.D1.8F_.D1.83.D1.81.D1.82.D1.80.D0.BE.D0.B9.D1.81.D1.82.D0.B2_IoT_.D0.B4.D0.BB.D1.8F_.D0.B7.D0.B0.D1.89.D0.B8.D1.82.D1.8B_.D0.BE.D1.82_.D1.85.D0.B0.D0.BA.D0.B5.D1.80.D0.BE.D0.B2)     - [Как обеспечить безопасность устройств IoT с приходом 5G и Индустрии 4.0](https://www.tadviser.ru/index.php/%D0%A1%D1%82%D0%B0%D1%82%D1%8C%D1%8F:%D0%98%D0%BD%D1%84%D0%BE%D1%80%D0%BC%D0%B0%D1%86%D0%B8%D0%BE%D0%BD%D0%BD%D0%B0%D1%8F_%D0%B1%D0%B5%D0%B7%D0%BE%D0%BF%D0%B0%D1%81%D0%BD%D0%BE%D1%81%D1%82%D1%8C_%D0%B8%D0%BD%D1%82%D0%B5%D1%80%D0%BD%D0%B5%D1%82%D0%B0_%D0%B2%D0%B5%D1%89%D0%B5%D0%B9_(Internet_of_Things)#.D0.9A.D0.B0.D0.BA_.D0.BE.D0.B1.D0.B5.D1.81.D0.BF.D0.B5.D1.87.D0.B8.D1.82.D1.8C_.D0.B1.D0.B5.D0.B7.D0.BE.D0.BF.D0.B0.D1.81.D0.BD.D0.BE.D1.81.D1.82.D1.8C_.D1.83.D1.81.D1.82.D1.80.D0.BE.D0.B9.D1.81.D1.82.D0.B2_IoT_.D1.81_.D0.BF.D1.80.D0.B8.D1.85.D0.BE.D0.B4.D0.BE.D0.BC_5G_.D0.B8_.D0.98.D0.BD.D0.B4.D1.83.D1.81.D1.82.D1.80.D0.B8.D0.B8_4.0)   + [Оценка рынка](https://www.tadviser.ru/index.php/%D0%A1%D1%82%D0%B0%D1%82%D1%8C%D1%8F:%D0%98%D0%BD%D1%84%D0%BE%D1%80%D0%BC%D0%B0%D1%86%D0%B8%D0%BE%D0%BD%D0%BD%D0%B0%D1%8F_%D0%B1%D0%B5%D0%B7%D0%BE%D0%BF%D0%B0%D1%81%D0%BD%D0%BE%D1%81%D1%82%D1%8C_%D0%B8%D0%BD%D1%82%D0%B5%D1%80%D0%BD%D0%B5%D1%82%D0%B0_%D0%B2%D0%B5%D1%89%D0%B5%D0%B9_(Internet_of_Things)#.D0.9E.D1.86.D0.B5.D0.BD.D0.BA.D0.B0_.D1.80.D1.8B.D0.BD.D0.BA.D0.B0)     - [2017: Расходы на безопасность IoT в $1,2 млрд](https://www.tadviser.ru/index.php/%D0%A1%D1%82%D0%B0%D1%82%D1%8C%D1%8F:%D0%98%D0%BD%D1%84%D0%BE%D1%80%D0%BC%D0%B0%D1%86%D0%B8%D0%BE%D0%BD%D0%BD%D0%B0%D1%8F_%D0%B1%D0%B5%D0%B7%D0%BE%D0%BF%D0%B0%D1%81%D0%BD%D0%BE%D1%81%D1%82%D1%8C_%D0%B8%D0%BD%D1%82%D0%B5%D1%80%D0%BD%D0%B5%D1%82%D0%B0_%D0%B2%D0%B5%D1%89%D0%B5%D0%B9_(Internet_of_Things)#2017:_.D0.A0.D0.B0.D1.81.D1.85.D0.BE.D0.B4.D1.8B_.D0.BD.D0.B0_.D0.B1.D0.B5.D0.B7.D0.BE.D0.BF.D0.B0.D1.81.D0.BD.D0.BE.D1.81.D1.82.D1.8C_IoT_.D0.B2_.241.2C2_.D0.BC.D0.BB.D1.80.D0.B4)   + [История инцидентов](https://www.tadviser.ru/index.php/%D0%A1%D1%82%D0%B0%D1%82%D1%8C%D1%8F:%D0%98%D0%BD%D1%84%D0%BE%D1%80%D0%BC%D0%B0%D1%86%D0%B8%D0%BE%D0%BD%D0%BD%D0%B0%D1%8F_%D0%B1%D0%B5%D0%B7%D0%BE%D0%BF%D0%B0%D1%81%D0%BD%D0%BE%D1%81%D1%82%D1%8C_%D0%B8%D0%BD%D1%82%D0%B5%D1%80%D0%BD%D0%B5%D1%82%D0%B0_%D0%B2%D0%B5%D1%89%D0%B5%D0%B9_(Internet_of_Things)#.D0.98.D1.81.D1.82.D0.BE.D1.80.D0.B8.D1.8F_.D0.B8.D0.BD.D1.86.D0.B8.D0.B4.D0.B5.D0.BD.D1.82.D0.BE.D0.B2)     - [Вымогатели-шифровальщики вещей](https://www.tadviser.ru/index.php/%D0%A1%D1%82%D0%B0%D1%82%D1%8C%D1%8F:%D0%98%D0%BD%D1%84%D0%BE%D1%80%D0%BC%D0%B0%D1%86%D0%B8%D0%BE%D0%BD%D0%BD%D0%B0%D1%8F_%D0%B1%D0%B5%D0%B7%D0%BE%D0%BF%D0%B0%D1%81%D0%BD%D0%BE%D1%81%D1%82%D1%8C_%D0%B8%D0%BD%D1%82%D0%B5%D1%80%D0%BD%D0%B5%D1%82%D0%B0_%D0%B2%D0%B5%D1%89%D0%B5%D0%B9_(Internet_of_Things)#.D0.92.D1.8B.D0.BC.D0.BE.D0.B3.D0.B0.D1.82.D0.B5.D0.BB.D0.B8-.D1.88.D0.B8.D1.84.D1.80.D0.BE.D0.B2.D0.B0.D0.BB.D1.8C.D1.89.D0.B8.D0.BA.D0.B8_.D0.B2.D0.B5.D1.89.D0.B5.D0.B9)     - [2024: Умные устройства вашего дома под прицелом хакеров. Как от них защититься - инструкция](https://www.tadviser.ru/index.php/%D0%A1%D1%82%D0%B0%D1%82%D1%8C%D1%8F:%D0%98%D0%BD%D1%84%D0%BE%D1%80%D0%BC%D0%B0%D1%86%D0%B8%D0%BE%D0%BD%D0%BD%D0%B0%D1%8F_%D0%B1%D0%B5%D0%B7%D0%BE%D0%BF%D0%B0%D1%81%D0%BD%D0%BE%D1%81%D1%82%D1%8C_%D0%B8%D0%BD%D1%82%D0%B5%D1%80%D0%BD%D0%B5%D1%82%D0%B0_%D0%B2%D0%B5%D1%89%D0%B5%D0%B9_(Internet_of_Things)#2024:_.D0.A3.D0.BC.D0.BD.D1.8B.D0.B5_.D1.83.D1.81.D1.82.D1.80.D0.BE.D0.B9.D1.81.D1.82.D0.B2.D0.B0_.D0.B2.D0.B0.D1.88.D0.B5.D0.B3.D0.BE_.D0.B4.D0.BE.D0.BC.D0.B0_.D0.BF.D0.BE.D0.B4_.D0.BF.D1.80.D0.B8.D1.86.D0.B5.D0.BB.D0.BE.D0.BC_.D1.85.D0.B0.D0.BA.D0.B5.D1.80.D0.BE.D0.B2._.D0.9A.D0.B0.D0.BA_.D0.BE.D1.82_.D0.BD.D0.B8.D1.85_.D0.B7.D0.B0.D1.89.D0.B8.D1.82.D0.B8.D1.82.D1.8C.D1.81.D1.8F_-_.D0.B8.D0.BD.D1.81.D1.82.D1.80.D1.83.D0.BA.D1.86.D0.B8.D1.8F)     - [2022](https://www.tadviser.ru/index.php/%D0%A1%D1%82%D0%B0%D1%82%D1%8C%D1%8F:%D0%98%D0%BD%D1%84%D0%BE%D1%80%D0%BC%D0%B0%D1%86%D0%B8%D0%BE%D0%BD%D0%BD%D0%B0%D1%8F_%D0%B1%D0%B5%D0%B7%D0%BE%D0%BF%D0%B0%D1%81%D0%BD%D0%BE%D1%81%D1%82%D1%8C_%D0%B8%D0%BD%D1%82%D0%B5%D1%80%D0%BD%D0%B5%D1%82%D0%B0_%D0%B2%D0%B5%D1%89%D0%B5%D0%B9_(Internet_of_Things)#2022)       * [Неисправленная DNS-уязвимость подвергает опасности миллионы IoT-устройств](https://www.tadviser.ru/index.php/%D0%A1%D1%82%D0%B0%D1%82%D1%8C%D1%8F:%D0%98%D0%BD%D1%84%D0%BE%D1%80%D0%BC%D0%B0%D1%86%D0%B8%D0%BE%D0%BD%D0%BD%D0%B0%D1%8F_%D0%B1%D0%B5%D0%B7%D0%BE%D0%BF%D0%B0%D1%81%D0%BD%D0%BE%D1%81%D1%82%D1%8C_%D0%B8%D0%BD%D1%82%D0%B5%D1%80%D0%BD%D0%B5%D1%82%D0%B0_%D0%B2%D0%B5%D1%89%D0%B5%D0%B9_(Internet_of_Things)#.D0.9D.D0.B5.D0.B8.D1.81.D0.BF.D1.80.D0.B0.D0.B2.D0.BB.D0.B5.D0.BD.D0.BD.D0.B0.D1.8F_DNS-.D1.83.D1.8F.D0.B7.D0.B2.D0.B8.D0.BC.D0.BE.D1.81.D1.82.D1.8C_.D0.BF.D0.BE.D0.B4.D0.B2.D0.B5.D1.80.D0.B3.D0.B0.D0.B5.D1.82_.D0.BE.D0.BF.D0.B0.D1.81.D0.BD.D0.BE.D1.81.D1.82.D0.B8_.D0.BC.D0.B8.D0.BB.D0.BB.D0.B8.D0.BE.D0.BD.D1.8B_IoT-.D1.83.D1.81.D1.82.D1.80.D0.BE.D0.B9.D1.81.D1.82.D0.B2)       * [IoT-ботнет Enemybot на базе Mirai набирает обороты](https://www.tadviser.ru/index.php/%D0%A1%D1%82%D0%B0%D1%82%D1%8C%D1%8F:%D0%98%D0%BD%D1%84%D0%BE%D1%80%D0%BC%D0%B0%D1%86%D0%B8%D0%BE%D0%BD%D0%BD%D0%B0%D1%8F_%D0%B1%D0%B5%D0%B7%D0%BE%D0%BF%D0%B0%D1%81%D0%BD%D0%BE%D1%81%D1%82%D1%8C_%D0%B8%D0%BD%D1%82%D0%B5%D1%80%D0%BD%D0%B5%D1%82%D0%B0_%D0%B2%D0%B5%D1%89%D0%B5%D0%B9_(Internet_of_Things)#IoT-.D0.B1.D0.BE.D1.82.D0.BD.D0.B5.D1.82_Enemybot_.D0.BD.D0.B0_.D0.B1.D0.B0.D0.B7.D0.B5_Mirai_.D0.BD.D0.B0.D0.B1.D0.B8.D1.80.D0.B0.D0.B5.D1.82_.D0.BE.D0.B1.D0.BE.D1.80.D0.BE.D1.82.D1.8B)     - [2020](https://www.tadviser.ru/index.php/%D0%A1%D1%82%D0%B0%D1%82%D1%8C%D1%8F:%D0%98%D0%BD%D1%84%D0%BE%D1%80%D0%BC%D0%B0%D1%86%D0%B8%D0%BE%D0%BD%D0%BD%D0%B0%D1%8F_%D0%B1%D0%B5%D0%B7%D0%BE%D0%BF%D0%B0%D1%81%D0%BD%D0%BE%D1%81%D1%82%D1%8C_%D0%B8%D0%BD%D1%82%D0%B5%D1%80%D0%BD%D0%B5%D1%82%D0%B0_%D0%B2%D0%B5%D1%89%D0%B5%D0%B9_(Internet_of_Things)#2020)       * [Исследование Check Point показало, как сети могут быть взломаны с помощью лампочки](https://www.tadviser.ru/index.php/%D0%A1%D1%82%D0%B0%D1%82%D1%8C%D1%8F:%D0%98%D0%BD%D1%84%D0%BE%D1%80%D0%BC%D0%B0%D1%86%D0%B8%D0%BE%D0%BD%D0%BD%D0%B0%D1%8F_%D0%B1%D0%B5%D0%B7%D0%BE%D0%BF%D0%B0%D1%81%D0%BD%D0%BE%D1%81%D1%82%D1%8C_%D0%B8%D0%BD%D1%82%D0%B5%D1%80%D0%BD%D0%B5%D1%82%D0%B0_%D0%B2%D0%B5%D1%89%D0%B5%D0%B9_(Internet_of_Things)#.D0.98.D1.81.D1.81.D0.BB.D0.B5.D0.B4.D0.BE.D0.B2.D0.B0.D0.BD.D0.B8.D0.B5_Check_Point_.D0.BF.D0.BE.D0.BA.D0.B0.D0.B7.D0.B0.D0.BB.D0.BE.2C_.D0.BA.D0.B0.D0.BA_.D1.81.D0.B5.D1.82.D0.B8_.D0.BC.D0.BE.D0.B3.D1.83.D1.82_.D0.B1.D1.8B.D1.82.D1.8C_.D0.B2.D0.B7.D0.BB.D0.BE.D0.BC.D0.B0.D0.BD.D1.8B_.D1.81_.D0.BF.D0.BE.D0.BC.D0.BE.D1.89.D1.8C.D1.8E_.D0.BB.D0.B0.D0.BC.D0.BF.D0.BE.D1.87.D0.BA.D0.B8)       * [Данные 515 тыс. серверов, домашних маршрутизаторов и IoT-устройств оказались в открытом доступе](https://www.tadviser.ru/index.php/%D0%A1%D1%82%D0%B0%D1%82%D1%8C%D1%8F:%D0%98%D0%BD%D1%84%D0%BE%D1%80%D0%BC%D0%B0%D1%86%D0%B8%D0%BE%D0%BD%D0%BD%D0%B0%D1%8F_%D0%B1%D0%B5%D0%B7%D0%BE%D0%BF%D0%B0%D1%81%D0%BD%D0%BE%D1%81%D1%82%D1%8C_%D0%B8%D0%BD%D1%82%D0%B5%D1%80%D0%BD%D0%B5%D1%82%D0%B0_%D0%B2%D0%B5%D1%89%D0%B5%D0%B9_(Internet_of_Things)#.D0.94.D0.B0.D0.BD.D0.BD.D1.8B.D0.B5_515_.D1.82.D1.8B.D1.81._.D1.81.D0.B5.D1.80.D0.B2.D0.B5.D1.80.D0.BE.D0.B2.2C_.D0.B4.D0.BE.D0.BC.D0.B0.D1.88.D0.BD.D0.B8.D1.85_.D0.BC.D0.B0.D1.80.D1.88.D1.80.D1.83.D1.82.D0.B8.D0.B7.D0.B0.D1.82.D0.BE.D1.80.D0.BE.D0.B2_.D0.B8_IoT-.D1.83.D1.81.D1.82.D1.80.D0.BE.D0.B9.D1.81.D1.82.D0.B2_.D0.BE.D0.BA.D0.B0.D0.B7.D0.B0.D0.BB.D0.B8.D1.81.D1.8C_.D0.B2_.D0.BE.D1.82.D0.BA.D1.80.D1.8B.D1.82.D0.BE.D0.BC_.D0.B4.D0.BE.D1.81.D1.82.D1.83.D0.BF.D0.B5)       * [Сексуальное вымогательство через умные камеры](https://www.tadviser.ru/index.php/%D0%A1%D1%82%D0%B0%D1%82%D1%8C%D1%8F:%D0%98%D0%BD%D1%84%D0%BE%D1%80%D0%BC%D0%B0%D1%86%D0%B8%D0%BE%D0%BD%D0%BD%D0%B0%D1%8F_%D0%B1%D0%B5%D0%B7%D0%BE%D0%BF%D0%B0%D1%81%D0%BD%D0%BE%D1%81%D1%82%D1%8C_%D0%B8%D0%BD%D1%82%D0%B5%D1%80%D0%BD%D0%B5%D1%82%D0%B0_%D0%B2%D0%B5%D1%89%D0%B5%D0%B9_(Internet_of_Things)#.D0.A1.D0.B5.D0.BA.D1.81.D1.83.D0.B0.D0.BB.D1.8C.D0.BD.D0.BE.D0.B5_.D0.B2.D1.8B.D0.BC.D0.BE.D0.B3.D0.B0.D1.82.D0.B5.D0.BB.D1.8C.D1.81.D1.82.D0.B2.D0.BE_.D1.87.D0.B5.D1.80.D0.B5.D0.B7_.D1.83.D0.BC.D0.BD.D1.8B.D0.B5_.D0.BA.D0.B0.D0.BC.D0.B5.D1.80.D1.8B)     - [2019](https://www.tadviser.ru/index.php/%D0%A1%D1%82%D0%B0%D1%82%D1%8C%D1%8F:%D0%98%D0%BD%D1%84%D0%BE%D1%80%D0%BC%D0%B0%D1%86%D0%B8%D0%BE%D0%BD%D0%BD%D0%B0%D1%8F_%D0%B1%D0%B5%D0%B7%D0%BE%D0%BF%D0%B0%D1%81%D0%BD%D0%BE%D1%81%D1%82%D1%8C_%D0%B8%D0%BD%D1%82%D0%B5%D1%80%D0%BD%D0%B5%D1%82%D0%B0_%D0%B2%D0%B5%D1%89%D0%B5%D0%B9_(Internet_of_Things)#2019)       * [75% атак на устройства интернета вещей приходится на США](https://www.tadviser.ru/index.php/%D0%A1%D1%82%D0%B0%D1%82%D1%8C%D1%8F:%D0%98%D0%BD%D1%84%D0%BE%D1%80%D0%BC%D0%B0%D1%86%D0%B8%D0%BE%D0%BD%D0%BD%D0%B0%D1%8F_%D0%B1%D0%B5%D0%B7%D0%BE%D0%BF%D0%B0%D1%81%D0%BD%D0%BE%D1%81%D1%82%D1%8C_%D0%B8%D0%BD%D1%82%D0%B5%D1%80%D0%BD%D0%B5%D1%82%D0%B0_%D0%B2%D0%B5%D1%89%D0%B5%D0%B9_(Internet_of_Things)#75.25_.D0.B0.D1.82.D0.B0.D0.BA_.D0.BD.D0.B0_.D1.83.D1.81.D1.82.D1.80.D0.BE.D0.B9.D1.81.D1.82.D0.B2.D0.B0_.D0.B8.D0.BD.D1.82.D0.B5.D1.80.D0.BD.D0.B5.D1.82.D0.B0_.D0.B2.D0.B5.D1.89.D0.B5.D0.B9_.D0.BF.D1.80.D0.B8.D1.85.D0.BE.D0.B4.D0.B8.D1.82.D1.81.D1.8F_.D0.BD.D0.B0_.D0.A1.D0.A8.D0.90)       * [ФБР: для каждого IoT-устройства необходима отдельная сеть](https://www.tadviser.ru/index.php/%D0%A1%D1%82%D0%B0%D1%82%D1%8C%D1%8F:%D0%98%D0%BD%D1%84%D0%BE%D1%80%D0%BC%D0%B0%D1%86%D0%B8%D0%BE%D0%BD%D0%BD%D0%B0%D1%8F_%D0%B1%D0%B5%D0%B7%D0%BE%D0%BF%D0%B0%D1%81%D0%BD%D0%BE%D1%81%D1%82%D1%8C_%D0%B8%D0%BD%D1%82%D0%B5%D1%80%D0%BD%D0%B5%D1%82%D0%B0_%D0%B2%D0%B5%D1%89%D0%B5%D0%B9_(Internet_of_Things)#.D0.A4.D0.91.D0.A0:_.D0.B4.D0.BB.D1.8F_.D0.BA.D0.B0.D0.B6.D0.B4.D0.BE.D0.B3.D0.BE_IoT-.D1.83.D1.81.D1.82.D1.80.D0.BE.D0.B9.D1.81.D1.82.D0.B2.D0.B0_.D0.BD.D0.B5.D0.BE.D0.B1.D1.85.D0.BE.D0.B4.D0.B8.D0.BC.D0.B0_.D0.BE.D1.82.D0.B4.D0.B5.D0.BB.D1.8C.D0.BD.D0.B0.D1.8F_.D1.81.D0.B5.D1.82.D1.8C)       * [Зафиксировано 105 млн атак на IoT-устройства за первое полугодие](https://www.tadviser.ru/index.php/%D0%A1%D1%82%D0%B0%D1%82%D1%8C%D1%8F:%D0%98%D0%BD%D1%84%D0%BE%D1%80%D0%BC%D0%B0%D1%86%D0%B8%D0%BE%D0%BD%D0%BD%D0%B0%D1%8F_%D0%B1%D0%B5%D0%B7%D0%BE%D0%BF%D0%B0%D1%81%D0%BD%D0%BE%D1%81%D1%82%D1%8C_%D0%B8%D0%BD%D1%82%D0%B5%D1%80%D0%BD%D0%B5%D1%82%D0%B0_%D0%B2%D0%B5%D1%89%D0%B5%D0%B9_(Internet_of_Things)#.D0.97.D0.B0.D1.84.D0.B8.D0.BA.D1.81.D0.B8.D1.80.D0.BE.D0.B2.D0.B0.D0.BD.D0.BE_105_.D0.BC.D0.BB.D0.BD_.D0.B0.D1.82.D0.B0.D0.BA_.D0.BD.D0.B0_IoT-.D1.83.D1.81.D1.82.D1.80.D0.BE.D0.B9.D1.81.D1.82.D0.B2.D0.B0_.D0.B7.D0.B0_.D0.BF.D0.B5.D1.80.D0.B2.D0.BE.D0.B5_.D0.BF.D0.BE.D0.BB.D1.83.D0.B3.D0.BE.D0.B4.D0.B8.D0.B5)       * [В Trend Micro выяснили, как киберкриминальные группировки используют устройства IoT](https://www.tadviser.ru/index.php/%D0%A1%D1%82%D0%B0%D1%82%D1%8C%D1%8F:%D0%98%D0%BD%D1%84%D0%BE%D1%80%D0%BC%D0%B0%D1%86%D0%B8%D0%BE%D0%BD%D0%BD%D0%B0%D1%8F_%D0%B1%D0%B5%D0%B7%D0%BE%D0%BF%D0%B0%D1%81%D0%BD%D0%BE%D1%81%D1%82%D1%8C_%D0%B8%D0%BD%D1%82%D0%B5%D1%80%D0%BD%D0%B5%D1%82%D0%B0_%D0%B2%D0%B5%D1%89%D0%B5%D0%B9_(Internet_of_Things)#.D0.92_Trend_Micro_.D0.B2.D1.8B.D1.8F.D1.81.D0.BD.D0.B8.D0.BB.D0.B8.2C_.D0.BA.D0.B0.D0.BA_.D0.BA.D0.B8.D0.B1.D0.B5.D1.80.D0.BA.D1.80.D0.B8.D0.BC.D0.B8.D0.BD.D0.B0.D0.BB.D1.8C.D0.BD.D1.8B.D0.B5_.D0.B3.D1.80.D1.83.D0.BF.D0.BF.D0.B8.D1.80.D0.BE.D0.B2.D0.BA.D0.B8_.D0.B8.D1.81.D0.BF.D0.BE.D0.BB.D1.8C.D0.B7.D1.83.D1.8E.D1.82_.D1.83.D1.81.D1.82.D1.80.D0.BE.D0.B9.D1.81.D1.82.D0.B2.D0.B0_IoT)     - [2018: Nokia Threat Intelligence Report](https://www.tadviser.ru/index.php/%D0%A1%D1%82%D0%B0%D1%82%D1%8C%D1%8F:%D0%98%D0%BD%D1%84%D0%BE%D1%80%D0%BC%D0%B0%D1%86%D0%B8%D0%BE%D0%BD%D0%BD%D0%B0%D1%8F_%D0%B1%D0%B5%D0%B7%D0%BE%D0%BF%D0%B0%D1%81%D0%BD%D0%BE%D1%81%D1%82%D1%8C_%D0%B8%D0%BD%D1%82%D0%B5%D1%80%D0%BD%D0%B5%D1%82%D0%B0_%D0%B2%D0%B5%D1%89%D0%B5%D0%B9_(Internet_of_Things)#2018:_Nokia_Threat_Intelligence_Report)     - [2017](https://www.tadviser.ru/index.php/%D0%A1%D1%82%D0%B0%D1%82%D1%8C%D1%8F:%D0%98%D0%BD%D1%84%D0%BE%D1%80%D0%BC%D0%B0%D1%86%D0%B8%D0%BE%D0%BD%D0%BD%D0%B0%D1%8F_%D0%B1%D0%B5%D0%B7%D0%BE%D0%BF%D0%B0%D1%81%D0%BD%D0%BE%D1%81%D1%82%D1%8C_%D0%B8%D0%BD%D1%82%D0%B5%D1%80%D0%BD%D0%B5%D1%82%D0%B0_%D0%B2%D0%B5%D1%89%D0%B5%D0%B9_(Internet_of_Things)#2017)       * [Gemalto: У потребителей нет уверенности в безопасности устройств IoT](https://www.tadviser.ru/index.php/%D0%A1%D1%82%D0%B0%D1%82%D1%8C%D1%8F:%D0%98%D0%BD%D1%84%D0%BE%D1%80%D0%BC%D0%B0%D1%86%D0%B8%D0%BE%D0%BD%D0%BD%D0%B0%D1%8F_%D0%B1%D0%B5%D0%B7%D0%BE%D0%BF%D0%B0%D1%81%D0%BD%D0%BE%D1%81%D1%82%D1%8C_%D0%B8%D0%BD%D1%82%D0%B5%D1%80%D0%BD%D0%B5%D1%82%D0%B0_%D0%B2%D0%B5%D1%89%D0%B5%D0%B9_(Internet_of_Things)#Gemalto:_.D0.A3_.D0.BF.D0.BE.D1.82.D1.80.D0.B5.D0.B1.D0.B8.D1.82.D0.B5.D0.BB.D0.B5.D0.B9_.D0.BD.D0.B5.D1.82_.D1.83.D0.B2.D0.B5.D1.80.D0.B5.D0.BD.D0.BD.D0.BE.D1.81.D1.82.D0.B8_.D0.B2_.D0.B1.D0.B5.D0.B7.D0.BE.D0.BF.D0.B0.D1.81.D0.BD.D0.BE.D1.81.D1.82.D0.B8_.D1.83.D1.81.D1.82.D1.80.D0.BE.D0.B9.D1.81.D1.82.D0.B2_IoT)       * [Уязвимость HomeHack позволяет взять под контроль IoT-устройства LG SmartThinQ](https://www.tadviser.ru/index.php/%D0%A1%D1%82%D0%B0%D1%82%D1%8C%D1%8F:%D0%98%D0%BD%D1%84%D0%BE%D1%80%D0%BC%D0%B0%D1%86%D0%B8%D0%BE%D0%BD%D0%BD%D0%B0%D1%8F_%D0%B1%D0%B5%D0%B7%D0%BE%D0%BF%D0%B0%D1%81%D0%BD%D0%BE%D1%81%D1%82%D1%8C_%D0%B8%D0%BD%D1%82%D0%B5%D1%80%D0%BD%D0%B5%D1%82%D0%B0_%D0%B2%D0%B5%D1%89%D0%B5%D0%B9_(Internet_of_Things)#.D0.A3.D1.8F.D0.B7.D0.B2.D0.B8.D0.BC.D0.BE.D1.81.D1.82.D1.8C_HomeHack_.D0.BF.D0.BE.D0.B7.D0.B2.D0.BE.D0.BB.D1.8F.D0.B5.D1.82_.D0.B2.D0.B7.D1.8F.D1.82.D1.8C_.D0.BF.D0.BE.D0.B4_.D0.BA.D0.BE.D0.BD.D1.82.D1.80.D0.BE.D0.BB.D1.8C_IoT-.D1.83.D1.81.D1.82.D1.80.D0.BE.D0.B9.D1.81.D1.82.D0.B2.D0.B0_LG_SmartThinQ)       * [Хакеры атаковали сеть ИВ-устройств университета](https://www.tadviser.ru/index.php/%D0%A1%D1%82%D0%B0%D1%82%D1%8C%D1%8F:%D0%98%D0%BD%D1%84%D0%BE%D1%80%D0%BC%D0%B0%D1%86%D0%B8%D0%BE%D0%BD%D0%BD%D0%B0%D1%8F_%D0%B1%D0%B5%D0%B7%D0%BE%D0%BF%D0%B0%D1%81%D0%BD%D0%BE%D1%81%D1%82%D1%8C_%D0%B8%D0%BD%D1%82%D0%B5%D1%80%D0%BD%D0%B5%D1%82%D0%B0_%D0%B2%D0%B5%D1%89%D0%B5%D0%B9_(Internet_of_Things)#.D0.A5.D0.B0.D0.BA.D0.B5.D1.80.D1.8B_.D0.B0.D1.82.D0.B0.D0.BA.D0.BE.D0.B2.D0.B0.D0.BB.D0.B8_.D1.81.D0.B5.D1.82.D1.8C_.D0.98.D0.92-.D1.83.D1.81.D1.82.D1.80.D0.BE.D0.B9.D1.81.D1.82.D0.B2_.D1.83.D0.BD.D0.B8.D0.B2.D0.B5.D1.80.D1.81.D0.B8.D1.82.D0.B5.D1.82.D0.B0)     - [2016: Хакеры впервые взломали унитаз](https://www.tadviser.ru/index.php/%D0%A1%D1%82%D0%B0%D1%82%D1%8C%D1%8F:%D0%98%D0%BD%D1%84%D0%BE%D1%80%D0%BC%D0%B0%D1%86%D0%B8%D0%BE%D0%BD%D0%BD%D0%B0%D1%8F_%D0%B1%D0%B5%D0%B7%D0%BE%D0%BF%D0%B0%D1%81%D0%BD%D0%BE%D1%81%D1%82%D1%8C_%D0%B8%D0%BD%D1%82%D0%B5%D1%80%D0%BD%D0%B5%D1%82%D0%B0_%D0%B2%D0%B5%D1%89%D0%B5%D0%B9_(Internet_of_Things)#2016:_.D0.A5.D0.B0.D0.BA.D0.B5.D1.80.D1.8B_.D0.B2.D0.BF.D0.B5.D1.80.D0.B2.D1.8B.D0.B5_.D0.B2.D0.B7.D0.BB.D0.BE.D0.BC.D0.B0.D0.BB.D0.B8_.D1.83.D0.BD.D0.B8.D1.82.D0.B0.D0.B7)   + [Проекты в России](https://www.tadviser.ru/index.php/%D0%A1%D1%82%D0%B0%D1%82%D1%8C%D1%8F:%D0%98%D0%BD%D1%84%D0%BE%D1%80%D0%BC%D0%B0%D1%86%D0%B8%D0%BE%D0%BD%D0%BD%D0%B0%D1%8F_%D0%B1%D0%B5%D0%B7%D0%BE%D0%BF%D0%B0%D1%81%D0%BD%D0%BE%D1%81%D1%82%D1%8C_%D0%B8%D0%BD%D1%82%D0%B5%D1%80%D0%BD%D0%B5%D1%82%D0%B0_%D0%B2%D0%B5%D1%89%D0%B5%D0%B9_(Internet_of_Things)#.D0.9F.D1.80.D0.BE.D0.B5.D0.BA.D1.82.D1.8B_.D0.B2_.D0.A0.D0.BE.D1.81.D1.81.D0.B8.D0.B8)     - [2024: В России представили ИТ-решение, которое выявляет дыры в системах интернета вещей на этапе разработки](https://www.tadviser.ru/index.php/%D0%A1%D1%82%D0%B0%D1%82%D1%8C%D1%8F:%D0%98%D0%BD%D1%84%D0%BE%D1%80%D0%BC%D0%B0%D1%86%D0%B8%D0%BE%D0%BD%D0%BD%D0%B0%D1%8F_%D0%B1%D0%B5%D0%B7%D0%BE%D0%BF%D0%B0%D1%81%D0%BD%D0%BE%D1%81%D1%82%D1%8C_%D0%B8%D0%BD%D1%82%D0%B5%D1%80%D0%BD%D0%B5%D1%82%D0%B0_%D0%B2%D0%B5%D1%89%D0%B5%D0%B9_(Internet_of_Things)#2024:_.D0.92_.D0.A0.D0.BE.D1.81.D1.81.D0.B8.D0.B8_.D0.BF.D1.80.D0.B5.D0.B4.D1.81.D1.82.D0.B0.D0.B2.D0.B8.D0.BB.D0.B8_.D0.98.D0.A2-.D1.80.D0.B5.D1.88.D0.B5.D0.BD.D0.B8.D0.B5.2C_.D0.BA.D0.BE.D1.82.D0.BE.D1.80.D0.BE.D0.B5_.D0.B2.D1.8B.D1.8F.D0.B2.D0.BB.D1.8F.D0.B5.D1.82_.D0.B4.D1.8B.D1.80.D1.8B_.D0.B2_.D1.81.D0.B8.D1.81.D1.82.D0.B5.D0.BC.D0.B0.D1.85_.D0.B8.D0.BD.D1.82.D0.B5.D1.80.D0.BD.D0.B5.D1.82.D0.B0_.D0.B2.D0.B5.D1.89.D0.B5.D0.B9_.D0.BD.D0.B0_.D1.8D.D1.82.D0.B0.D0.BF.D0.B5_.D1.80.D0.B0.D0.B7.D1.80.D0.B0.D0.B1.D0.BE.D1.82.D0.BA.D0.B8)     - [2023: ФСТЭК получит 400 млн рублей на защиту промышленного интернета вещей в России](https://www.tadviser.ru/index.php/%D0%A1%D1%82%D0%B0%D1%82%D1%8C%D1%8F:%D0%98%D0%BD%D1%84%D0%BE%D1%80%D0%BC%D0%B0%D1%86%D0%B8%D0%BE%D0%BD%D0%BD%D0%B0%D1%8F_%D0%B1%D0%B5%D0%B7%D0%BE%D0%BF%D0%B0%D1%81%D0%BD%D0%BE%D1%81%D1%82%D1%8C_%D0%B8%D0%BD%D1%82%D0%B5%D1%80%D0%BD%D0%B5%D1%82%D0%B0_%D0%B2%D0%B5%D1%89%D0%B5%D0%B9_(Internet_of_Things)#2023:_.D0.A4.D0.A1.D0.A2.D0.AD.D0.9A_.D0.BF.D0.BE.D0.BB.D1.83.D1.87.D0.B8.D1.82_400_.D0.BC.D0.BB.D0.BD_.D1.80.D1.83.D0.B1.D0.BB.D0.B5.D0.B9_.D0.BD.D0.B0_.D0.B7.D0.B0.D1.89.D0.B8.D1.82.D1.83_.D0.BF.D1.80.D0.BE.D0.BC.D1.8B.D1.88.D0.BB.D0.B5.D0.BD.D0.BD.D0.BE.D0.B3.D0.BE_.D0.B8.D0.BD.D1.82.D0.B5.D1.80.D0.BD.D0.B5.D1.82.D0.B0_.D0.B2.D0.B5.D1.89.D0.B5.D0.B9_.D0.B2_.D0.A0.D0.BE.D1.81.D1.81.D0.B8.D0.B8)   + [Смотрите также](https://www.tadviser.ru/index.php/%D0%A1%D1%82%D0%B0%D1%82%D1%8C%D1%8F:%D0%98%D0%BD%D1%84%D0%BE%D1%80%D0%BC%D0%B0%D1%86%D0%B8%D0%BE%D0%BD%D0%BD%D0%B0%D1%8F_%D0%B1%D0%B5%D0%B7%D0%BE%D0%BF%D0%B0%D1%81%D0%BD%D0%BE%D1%81%D1%82%D1%8C_%D0%B8%D0%BD%D1%82%D0%B5%D1%80%D0%BD%D0%B5%D1%82%D0%B0_%D0%B2%D0%B5%D1%89%D0%B5%D0%B9_(Internet_of_Things)#.D0.A1.D0.BC.D0.BE.D1.82.D1.80.D0.B8.D1.82.D0.B5_.D1.82.D0.B0.D0.BA.D0.B6.D0.B5) |

Стандартизация в области безопасности

2025: ФСТЭК представила стандарт разработки систем с иммунитетом к киберугрозам

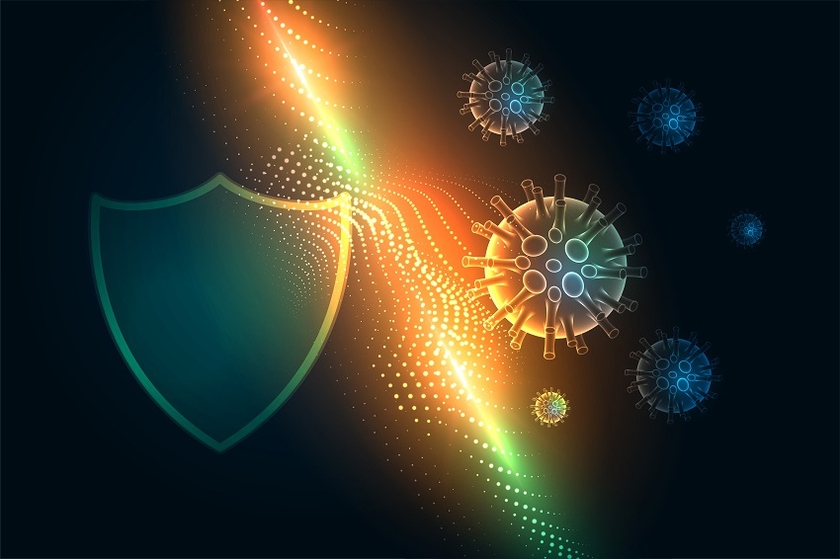
В конце февраля 2025 г. [ФСТЭК](https://www.tadviser.ru/index.php/%D0%A4%D0%A1%D0%A2%D0%AD%D0%9A) вынесла на рассмотрение в технический комитет №362 [Росстандарта](https://www.tadviser.ru/index.php/%D0%A0%D0%BE%D1%81%D1%81%D1%82%D0%B0%D0%BD%D0%B4%D0%B0%D1%80%D1%82%D0%B0) проект[[1]](https://www.tadviser.ru/index.php/%D0%A1%D1%82%D0%B0%D1%82%D1%8C%D1%8F:%D0%98%D0%BD%D1%84%D0%BE%D1%80%D0%BC%D0%B0%D1%86%D0%B8%D0%BE%D0%BD%D0%BD%D0%B0%D1%8F_%D0%B1%D0%B5%D0%B7%D0%BE%D0%BF%D0%B0%D1%81%D0%BD%D0%BE%D1%81%D1%82%D1%8C_%D0%B8%D0%BD%D1%82%D0%B5%D1%80%D0%BD%D0%B5%D1%82%D0%B0_%D0%B2%D0%B5%D1%89%D0%B5%D0%B9_(Internet_of_Things)#cite_note-0) ГОСТа под названием «Защита информации. Системы с конструктивной информационной безопасностью. Методология разработки». Он в случае принятия должен определить такое понятие как системы с конструктивной информационной безопасностью (СКИБ), которые некоторое время назад компания «[Лаборатория Касперского](https://www.tadviser.ru/index.php/%D0%9A%D0%BE%D0%BC%D0%BF%D0%B0%D0%BD%D0%B8%D1%8F:%D0%9B%D0%B0%D0%B1%D0%BE%D1%80%D0%B0%D1%82%D0%BE%D1%80%D0%B8%D1%8F_%D0%9A%D0%B0%D1%81%D0%BF%D0%B5%D1%80%D1%81%D0%BA%D0%BE%D0%B3%D0%BE)» продвигала как кибериммунные.

Стандарт разработан ФСТЭК России, ФАУ «ГНИИИ ПТЗИ ФСТЭК России», «Лабораторией Касперского» и [ИСП РАН](https://www.tadviser.ru/index.php/%D0%9A%D0%BE%D0%BC%D0%BF%D0%B0%D0%BD%D0%B8%D1%8F:%D0%98%D0%A1%D0%9F_%D0%A0%D0%90%D0%9D). Обсуждение проекта стандарта продлится до 11 марта.

В стандарте подход к проектированию СКИБ определяется так: «подход, при использовании которого системе в процессе её создания с момента замысла придаются характеристики (свойства), обеспечивающие соответствие целям безопасности, включая проверку такого соответствия».

Также определены важные термины доверенной системы («система, для которой доказано (обосновано) соответствие целям безопасности при условии выполнения предположений безопасности») и доверенной среды («среда функционирования системы, в которой обеспечено выполнение предположений безопасности и политики безопасности системы»).

|  |  |  |
| --- | --- | --- |
| « | Использование принципа кибериммунности, конструктивной безопасности или, в англоязычной версии - security by design, при разработке информационных систем, в том числе промышленных решений, не является новым, – напомнил читателям TAdviser канд. экон. наук. [Сергей Гатауллин](https://www.tadviser.ru/index.php/%D0%9F%D0%B5%D1%80%D1%81%D0%BE%D0%BD%D0%B0:%D0%93%D0%B0%D1%82%D0%B0%D1%83%D0%BB%D0%BB%D0%B8%D0%BD_%D0%A1%D0%B5%D1%80%D0%B3%D0%B5%D0%B9_%D0%A2%D0%B8%D0%BC%D1%83%D1%80%D0%BE%D0%B2%D0%B8%D1%87), ведущий научный сотрудник лаборатории социального моделирования [ЦЭМИ](https://www.tadviser.ru/index.php/%D0%9A%D0%BE%D0%BC%D0%BF%D0%B0%D0%BD%D0%B8%D1%8F:%D0%A6%D0%B5%D0%BD%D1%82%D1%80%D0%B0%D0%BB%D1%8C%D0%BD%D1%8B%D0%B9_%D1%8D%D0%BA%D0%BE%D0%BD%D0%BE%D0%BC%D0%B8%D0%BA%D0%BE-%D0%BC%D0%B0%D1%82%D0%B5%D0%BC%D0%B0%D1%82%D0%B8%D1%87%D0%B5%D1%81%D0%BA%D0%B8%D0%B9_%D0%B8%D0%BD%D1%81%D1%82%D0%B8%D1%82%D1%83%D1%82_(%D0%A6%D0%AD%D0%9C%D0%98_%D0%A0%D0%90%D0%9D)) РАН. – Эта методология развивается на протяжении нескольких десятилетий наряду с другими подходами и принципами доверенной разработки. Поэтому говорить о принципиальном усложнении создания новых ИТ-продуктов при следовании методологии разработки систем с конструктивной информационной безопасностью не совсем уместно. Период разработки и публичного обсуждения российского ГОСТа СКИБ позволял заинтересованным участникам рынка подготовиться к ожидаемым изменениям. | » |

𝓲

Системы с конструктивной безопасностью можно также назвать кибериммунными или, в английском варианте, security by design

Действительно, принцип «безопасность по умолчанию», который и положен в основу СКИБ, известен давно, однако следуют ему далеко не все производители решений для интернета вещей ([IoT](https://www.tadviser.ru/index.php/IoT)) и промышленных систем IoT ([IIoT](https://www.tadviser.ru/index.php/IIoT)). Именно поэтому и потребовался стандарт, ссылка на который в техническом задании и позволила бы заказчикам не допускать к внедрению «небезопасные» решения.

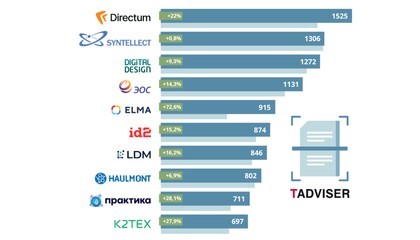
|  |  |  |
| --- | --- | --- |
| « | Разработка новых продуктов не должна значительно усложниться, поскольку методология СКИБ ориентирована на критически важные инфраструктурные системы, включая промышленную автоматизацию, энергетику, транспорт, телекоммуникации и IoT, – заявил для TAdviser Сергей Гаркуша, старший консультант отдела безопасности и защиты приложений [Infosecurity](https://www.tadviser.ru/index.php/%D0%9A%D0%BE%D0%BC%D0%BF%D0%B0%D0%BD%D0%B8%D1%8F:%D0%98%D0%BD%D1%84%D0%BE%D1%81%D0%B5%D0%BA%D1%8C%D1%8E%D1%80%D0%B8%D1%82%D0%B8_(Infosecurity)). – В этих областях релизный цикл традиционно длительный, что позволяет интегрировать новые требования без критического влияния на сроки. Кроме того, внедрение принципов безопасности на ранних этапах жизненного цикла способствует систематизации процесса защиты информации. Это не только не увеличивает сложность разработки, но и делает ее более управляемой и предсказуемой. Для IoT и IIoT важно не только следовать стандартам проектирования, но и применять технологии контроля взаимодействий компонентов, обеспечивая соответствие утвержденной политике безопасности. | » |

Предлагаемый проект стандарта опирается на этапы жизненного цикла разработки промышленных программных решений, которые определены в международном стандарте [ГОСТ Р ИСО/МЭК 12207-2010](https://www.tadviser.ru/index.php/%D0%A1%D1%82%D0%B0%D1%82%D1%8C%D1%8F:%D0%91%D0%B5%D0%B7%D0%BE%D0%BF%D0%B0%D1%81%D0%BD%D0%BE%D1%81%D1%82%D1%8C_%D0%BA%D1%80%D0%B8%D1%82%D0%B8%D1%87%D0%B5%D1%81%D0%BA%D0%BE%D0%B9_%D0%B8%D0%BD%D1%84%D0%BE%D1%80%D0%BC%D0%B0%D1%86%D0%B8%D0%BE%D0%BD%D0%BD%D0%BE%D0%B9_%D0%B8%D0%BD%D1%84%D1%80%D0%B0%D1%81%D1%82%D1%80%D1%83%D0%BA%D1%82%D1%83%D1%80%D1%8B_%D0%A0%D0%A4). В проекте стандарта для каждого этапа указаны работы, которые должны выполнять разработчики и эксплуатанты для обеспечения безопасности изделий.

|  |  |  |
| --- | --- | --- |
| « | По моему мнению, обсуждаемый проект стандарта упрощает разработку систем с конструктивной информационной безопасностью, – считает Валерий Ледовской, директор по развитию [ARinteg](https://www.tadviser.ru/index.php/ARinteg). – Разработчикам СКИБ предлагаются готовые подходы к созданию архитектуры продуктов, которые уже с возникновения задумки включают в себя механизмы защиты. Предлагаются типовые шаблоны проектирования разработок, обладающих свойствами конструктивной безопасности, т.е. не придётся каждый раз изобретать велосипед, можно действовать по аналогии. Заказчикам тоже будет проще проводить приёмку СКИБ, т.к. предъявляются стандартизованные требования. | » |

Действительно, важной частью проекта стандарта является приложение А, где перечислены типовые шаблоны проектирования программного обеспечения, обладающего свойствами конструктивной информационной безопасности. Их применение описано в главе №9 стандарта.

|  |  |  |
| --- | --- | --- |
| « | Предлагаемые инициативы по созданию единой методологии разработки и шаблонам проектирования в будущем положительно скажутся на качестве и безопасности создаваемых решений, особенно это важно для бизнес-критичных информационных систем и средств защиты информации, – отметил для читателей TAdviser важность обсуждаемого документа Александр Черных, директор Центра разработки [Angara Security](https://www.tadviser.ru/index.php/%D0%9A%D0%BE%D0%BC%D0%BF%D0%B0%D0%BD%D0%B8%D1%8F:Angara_Security_(%D0%90%D0%BD%D0%B3%D0%B0%D1%80%D0%B0_%D0%A2%D0%B5%D1%85%D0%BD%D0%BE%D0%BB%D0%BE%D0%B4%D0%B6%D0%B8%D0%B7_%D0%93%D1%80%D1%83%D0%BF,_%D0%90%D0%A2_%D0%93%D1%80%D1%83%D0%BF)_%D1%80%D0%B0%D0%BD%D0%B5%D0%B5_Angara_Technologies_Group). – Однако увеличение доли нефункциональных требований может повлиять на время выхода продукта на рынок, а вместе с необходимостью соблюдения процедур безопасной разработки программного обеспечения — на стоимость продукции и сроки предоставления функциональных ценностей конечному потребителю. | » |

Перечисление уже готовых шаблонов – важная часть, которая фактически предлагает разработчикам уже готовый набор компонент по созданию СКИБ-решений – они необходимы для создания доверенных программно-аппаратных комплексов (ПАК). Стандарт позволить разрабатывать их быстрее по предлагаемым шаблонам.[Российский рынок СЭД: актуальные тенденции, новые технологии, крупнейшие поставщики. Обзор TAdviser 11.7 т[](https://www.tadviser.ru/index.php/%D0%9D%D0%BE%D0%B2%D0%BE%D1%81%D1%82%D0%B8:%D0%A0%D0%BE%D1%81%D1%81%D0%B8%D0%B9%D1%81%D0%BA%D0%B8%D0%B9_%D1%80%D1%8B%D0%BD%D0%BE%D0%BA_%D0%A1%D0%AD%D0%94%3A_%D0%B0%D0%BA%D1%82%D1%83%D0%B0%D0%BB%D1%8C%D0%BD%D1%8B%D0%B5_%D1%82%D0%B5%D0%BD%D0%B4%D0%B5%D0%BD%D1%86%D0%B8%D0%B8%2C_%D0%BD%D0%BE%D0%B2%D1%8B%D0%B5_%D1%82%D0%B5%D1%85%D0%BD%D0%BE%D0%BB%D0%BE%D0%B3%D0%B8%D0%B8%2C_%D0%BA%D1%80%D1%83%D0%BF%D0%BD%D0%B5%D0%B9%D1%88%D0%B8%D0%B5_%D0%BF%D0%BE%D1%81%D1%82%D0%B0%D0%B2%D1%89%D0%B8%D0%BA%D0%B8._%D0%9E%D0%B1%D0%B7%D0%BE%D1%80_TAdviser)](https://www.tadviser.ru/index.php/%D0%9D%D0%BE%D0%B2%D0%BE%D1%81%D1%82%D0%B8:%D0%A0%D0%BE%D1%81%D1%81%D0%B8%D0%B9%D1%81%D0%BA%D0%B8%D0%B9_%D1%80%D1%8B%D0%BD%D0%BE%D0%BA_%D0%A1%D0%AD%D0%94%3A_%D0%B0%D0%BA%D1%82%D1%83%D0%B0%D0%BB%D1%8C%D0%BD%D1%8B%D0%B5_%D1%82%D0%B5%D0%BD%D0%B4%D0%B5%D0%BD%D1%86%D0%B8%D0%B8%2C_%D0%BD%D0%BE%D0%B2%D1%8B%D0%B5_%D1%82%D0%B5%D1%85%D0%BD%D0%BE%D0%BB%D0%BE%D0%B3%D0%B8%D0%B8%2C_%D0%BA%D1%80%D1%83%D0%BF%D0%BD%D0%B5%D0%B9%D1%88%D0%B8%D0%B5_%D0%BF%D0%BE%D1%81%D1%82%D0%B0%D0%B2%D1%89%D0%B8%D0%BA%D0%B8._%D0%9E%D0%B1%D0%B7%D0%BE%D1%80_TAdviser)

Следует отметить, что уже есть предварительный стандарт [ПНСТ 905-2023](https://www.tadviser.ru/index.php/%D0%A1%D1%82%D0%B0%D1%82%D1%8C%D1%8F:%D0%91%D0%B5%D0%B7%D0%BE%D0%BF%D0%B0%D1%81%D0%BD%D0%BE%D1%81%D1%82%D1%8C_%D0%BA%D1%80%D0%B8%D1%82%D0%B8%D1%87%D0%B5%D1%81%D0%BA%D0%BE%D0%B9_%D0%B8%D0%BD%D1%84%D0%BE%D1%80%D0%BC%D0%B0%D1%86%D0%B8%D0%BE%D0%BD%D0%BD%D0%BE%D0%B9_%D0%B8%D0%BD%D1%84%D1%80%D0%B0%D1%81%D1%82%D1%80%D1%83%D0%BA%D1%82%D1%83%D1%80%D1%8B_%D0%A0%D0%A4), который был принят в 2023 году и будет действовать до апреля 2027 года. Он был утвержден техническим комитетом №167 Росстандарта, который контролируется «[Росатомом](https://www.tadviser.ru/index.php/%D0%A0%D0%BE%D1%81%D0%B0%D1%82%D0%BE%D0%BC)». В разработке проекта по СКИБ также принимали участие разработчики этой госкорпорации.

|  |  |  |
| --- | --- | --- |
| « | Цель данного ГОСТ не усложнить разработку, а описать методику разработки отдельных видов ПАК (и ПО), следуя которой можно обеспечить их безопасность на конструктивном уровне, – прокомментировали TAdviser в пресс-службе «[Росатом автоматизированные системы управления](https://www.tadviser.ru/index.php/%D0%9A%D0%BE%D0%BC%D0%BF%D0%B0%D0%BD%D0%B8%D1%8F:%D0%A0%D0%BE%D1%81%D0%B0%D1%82%D0%BE%D0%BC_%D0%90%D0%B2%D1%82%D0%BE%D0%BC%D0%B0%D1%82%D0%B8%D0%B7%D0%B8%D1%80%D0%BE%D0%B2%D0%B0%D0%BD%D0%BD%D1%8B%D0%B5_%D0%A1%D0%B8%D1%81%D1%82%D0%B5%D0%BC%D1%8B_%D0%A3%D0%BF%D1%80%D0%B0%D0%B2%D0%BB%D0%B5%D0%BD%D0%B8%D1%8F_(%D0%A0%D0%90%D0%A1%D0%A3))» проект стандарта по СКИБ. – В методике уделяется особое внимание начальному этапу проектирования ПАК, на котором необходимо учесть требования по информационной безопасности. Далее, на протяжении всего жизненного цикла, они уточняются и реализуются вместе с функциональными требованиями. Такой подход позволяет не только уменьшить количество потенциальных уязвимостей, но и сократить ресурсы на последующее «встраивание» функций безопасности в уже готовое изделие. Данный ГОСТ позволит расширить номенклатуру безопасных ПАК, например, для технологии интернета вещей. | » |

Именно создание доверенных ПАК, для которых определены понятия доверенной системы и среды исполнения, и должны помочь в формировании планов российских компаний по переходу на отечественные решения в рамках постановления правительства РФ №1912. Оно требует от российских предприятий перехода на доверенные ПАКи к 2030 года. За счет этого постановления на российском рынке возникла высокая потребность в быстрой разработке доверенных ПАК, и новый стандарт должен помочь в этой работе.

|  |  |  |
| --- | --- | --- |
| « | Утверждение стандарта – это важный сигнал рынку, – заявил для TAdviser канд.экон.наук. Александр Батищев, доцент, руководитель по работе с вузами Международной школы математики и программирования «[Алгоритмика](https://www.tadviser.ru/index.php/%D0%9A%D0%BE%D0%BC%D0%BF%D0%B0%D0%BD%D0%B8%D1%8F:%D0%90%D0%BB%D0%B3%D0%BE%D1%80%D0%B8%D1%82%D0%BC%D0%B8%D0%BA%D0%B0)». – Если ИТ-компания не будет ориентироваться на этот стандарт, то потеряет доверие потребителей и бизнес-партнёров, не сможет участвовать в тендерах по государственным и муниципальным контрактам. Консолидация на рынке заказной разработки ПО в ближайшее время неизбежна, т.к. помимо внедрения стандарта на российском рынке по-прежнему наблюдается нехватка кадров (по разным оценкам от 500 тыс. до 1 млн. человек), рост преступлений с использованием информационно-телекоммуникационных технологий в прошлом году до 40% от общего числа зарегистрированных в России преступлений, и как следствие ужесточение требований по информационной и кибербезопасности со стороны бизнеса и государства. | » |

2019: Российские эксперты стали соредакторами международного стандарта интернета вещей в области безопасности

11 июня 2019 года стало известно, что представляющий [РФ](https://www.tadviser.ru/index.php/%D0%A0%D0%A4) Технический комитет 194 «[Технический комитет кибер-физические системы (ТК 194)](https://www.tadviser.ru/index.php/%D0%9A%D0%BE%D0%BC%D0%BF%D0%B0%D0%BD%D0%B8%D1%8F:%D0%A2%D0%B5%D1%85%D0%BD%D0%B8%D1%87%D0%B5%D1%81%D0%BA%D0%B8%D0%B9_%D0%BA%D0%BE%D0%BC%D0%B8%D1%82%D0%B5%D1%82_%D0%BA%D0%B8%D0%B1%D0%B5%D1%80-%D1%84%D0%B8%D0%B7%D0%B8%D1%87%D0%B5%D1%81%D0%BA%D0%B8%D0%B5_%D1%81%D0%B8%D1%81%D1%82%D0%B5%D0%BC%D1%8B_(%D0%A2%D0%9A_194))» [Росстандарта](https://www.tadviser.ru/index.php/%D0%A0%D0%BE%D1%81%D1%81%D1%82%D0%B0%D0%BD%D0%B4%D0%B0%D1%80%D1%82), созданный на базе [РВК](https://www.tadviser.ru/index.php/%D0%A0%D0%92%D0%9A), получил статус соредактора международного стандарта [ISO](https://www.tadviser.ru/index.php/ISO)/IEC технологии [интернета вещей](https://www.tadviser.ru/index.php/IoT). Подробнее [здесь](https://www.tadviser.ru/index.php/%D0%A1%D1%82%D0%B0%D1%82%D1%8C%D1%8F:ISO/IEC_30149_Internet_of_Things_(IoT)_%E2%80%94_Trustworthiness_frameworks).

Законодательство

2020: Великобритания готовит закон по защите IoT-устройств

28 января 2020 года стало известно, что [Правительство Великобритании](https://www.tadviser.ru/index.php/%D0%9F%D1%80%D0%B0%D0%B2%D0%B8%D1%82%D0%B5%D0%BB%D1%8C%D1%81%D1%82%D0%B2%D0%BE_%D0%92%D0%B5%D0%BB%D0%B8%D0%BA%D0%BE%D0%B1%D1%80%D0%B8%D1%82%D0%B0%D0%BD%D0%B8%D0%B8) обнародовало законопроект, направленный на защиту [IoT](https://www.tadviser.ru/index.php/IoT)-устройств.

Законопроект содержит три основных требования для производителей «умных» устройств. В частности, все [пароли](https://www.tadviser.ru/index.php/%D0%A1%D1%82%D0%B0%D1%82%D1%8C%D1%8F:%D0%9F%D0%B0%D1%80%D0%BE%D0%BB%D0%B8) пользовательских IoT-устройств должны быть уникальными и без возможности сбросить их до «универсальных» заводских настроек; производители должны предоставить общедоступную точку контакта, чтобы каждый мог сообщить об уязвимости и рассчитывать на «своевременное принятие мер»; производители обязаны четко указать минимальный период времени, в течение которого устройства будут получать обновления безопасности в местах продаж.

|  |  |  |
| --- | --- | --- |
| « | Наш законопроект обязывает фирмы, производящие и продающие подключенные к [интернету](https://www.tadviser.ru/index.php/%D0%98%D0%BD%D1%82%D0%B5%D1%80%D0%BD%D0%B5%D1%82) устройства, учитывать и пресекать действия [хакеров](https://www.tadviser.ru/index.php/%D0%A1%D1%82%D0%B0%D1%82%D1%8C%D1%8F:%D0%A5%D0%B0%D0%BA%D0%B5%D1%80%D1%8B), угрожающих конфиденциальности и безопасности людей. Это будет означать, что надежные стандарты безопасности будут внедряться на этапе проектирования, а не применяться в качестве запасного плана,  **сообщил министр по цифровым и широкополосным технологиям**[**Великобритании**](https://www.tadviser.ru/index.php/%D0%92%D0%B5%D0%BB%D0%B8%D0%BA%D0%BE%D0%B1%D1%80%D0%B8%D1%82%D0%B0%D0%BD%D0%B8%D0%B8)**Мэтт Уормен (Matt Warman)** | » |

Норма была разработана Министерством по делам культуры, [СМИ](https://www.tadviser.ru/index.php/%D0%A1%D0%9C%D0%98) и [спорта](https://www.tadviser.ru/index.php/%D0%A1%D0%BF%D0%BE%D1%80%D1%82) Великобритании после продолжительного периода консультаций, которые начались в мае 2019 года.

Как сообщили в правительстве Великобритании, законопроект планируется принять «как можно скорее»[[2]](https://www.tadviser.ru/index.php/%D0%A1%D1%82%D0%B0%D1%82%D1%8C%D1%8F:%D0%98%D0%BD%D1%84%D0%BE%D1%80%D0%BC%D0%B0%D1%86%D0%B8%D0%BE%D0%BD%D0%BD%D0%B0%D1%8F_%D0%B1%D0%B5%D0%B7%D0%BE%D0%BF%D0%B0%D1%81%D0%BD%D0%BE%D1%81%D1%82%D1%8C_%D0%B8%D0%BD%D1%82%D0%B5%D1%80%D0%BD%D0%B5%D1%82%D0%B0_%D0%B2%D0%B5%D1%89%D0%B5%D0%B9_(Internet_of_Things)#cite_note-1).

Теоретические аспекты ИБ интернета вещей

Безопасной экосистемы IoT не существует

Эксперты настойчиво заявляют о том, что поставщики услуг и устройств рынка [IoT](https://www.tadviser.ru/index.php/IoT) нарушают принцип сквозной [информационной безопасности](https://www.tadviser.ru/index.php/%D0%98%D0%BD%D1%84%D0%BE%D1%80%D0%BC%D0%B0%D1%86%D0%B8%D0%BE%D0%BD%D0%BD%D0%B0%D1%8F_%D0%B1%D0%B5%D0%B7%D0%BE%D0%BF%D0%B0%D1%81%D0%BD%D0%BE%D1%81%D1%82%D1%8C) (ИБ), который рекомендован для всех ИКТ-продуктов и услуг. Согласно этому принципу, ИБ должна закладываться на начальной стадии проектирования продукта или услуги и поддерживаться вплоть до завершения их жизненного цикла.

Но что же мы имеем на практике? Вот, например, некоторые данные исследований корпорации [HP](https://www.tadviser.ru/index.php/HP) (лето 2014 года), целью которых было не выявить какие-то конкретные небезопасные интернет-устройства и уличить их изготовителей, но обозначить проблему ИБ-рисков в мире IoT в целом.

Исследователи [HPE](https://www.tadviser.ru/index.php/HPE) обращают внимание на проблемы как на стороне владельцев устройств, так и на проблемы, над которыми должны подумать разработчики. Так, в самом начале эксплуатации пользователю обязательно нужно заменить фабричный [пароль](https://www.tadviser.ru/index.php/%D0%9F%D0%B0%D1%80%D0%BE%D0%BB%D1%8C), установленный по умолчанию, на свой личный, поскольку фабричные пароли одинаковы на всех устройствах и не отличаются стойкостью. К сожалению, делают это далеко не все. Поскольку не все приборы имеют встроенные средства ИБ-защиты, владельцам также следует позаботиться об установке внешней защиты, предназначенной для домашнего использования, с тем чтобы интернет-устройства не стали открытыми шлюзами в домашнюю сеть или прямыми инструментами причинения ущерба.

В ходе проведенного HP исследования обнаружено, что примерно в 70% проанализированных устройств не шифруется беспроводной трафик. Веб-интрефейс 60% устройств эксперты HP посчитали небезопасным из-за небезопасной организации доступа и высоких рисков межсайтового скриптинга. В большинстве устройств предусмотрены пароли недостаточной стойкости. Примерно 90% устройств собирают ту или иную персональную информацию о владельце без его ведома.

Всего же специалисты HP насчитали около 25 различных уязвимостей в каждом из исследованных устройств (телевизоров, дверных замков, бытовых весов, домашних охранных систем, электророзеток...) и их мобильных и облачных компонентах.

Вывод экспертов HP неутешителен: безопасной экосистемы IoT на сегодняшний день не существует. Особую опасность вещи [Интернета](https://www.tadviser.ru/index.php/%D0%98%D0%BD%D1%82%D0%B5%D1%80%D0%BD%D0%B5%D1%82) таят в себе в контексте распространения [целевых атак](https://www.tadviser.ru/index.php/%D0%A6%D0%B5%D0%BB%D0%B5%D0%B2%D1%8B%D1%85_%D0%B0%D1%82%D0%B0%D0%BA) (APT). Стоит только злоумышленникам проявить интерес к кому-либо из нас, и наши верные помощники из мира IoT превращаются в предателей, нараспашку открывающих доступ в мир своих владельцев.

Слабые места IoT

* Переход на [IPv6](https://www.tadviser.ru/index.php/%D0%A1%D1%82%D0%B0%D1%82%D1%8C%D1%8F:IPv6).
* Питание датчиков.
* Стандартизация архитектуры и протоколов, сертификация устройств.
* [Информационная безопасность](https://www.tadviser.ru/index.php/%D0%98%D0%BD%D1%84%D0%BE%D1%80%D0%BC%D0%B0%D1%86%D0%B8%D0%BE%D0%BD%D0%BD%D0%B0%D1%8F_%D0%B1%D0%B5%D0%B7%D0%BE%D0%BF%D0%B0%D1%81%D0%BD%D0%BE%D1%81%D1%82%D1%8C).
* стандартные учётные записи от производителя, слабая [аутентификация](https://www.tadviser.ru/index.php/%D0%90%D1%83%D1%82%D0%B5%D0%BD%D1%82%D0%B8%D1%84%D0%B8%D0%BA%D0%B0%D1%86%D0%B8%D1%8F)
* отсутствие поддержки со стороны производителе для устранения уязвимостей
* трудно или невозможно обновить [ПО](https://www.tadviser.ru/index.php/%D0%A1%D1%82%D0%B0%D1%82%D1%8C%D1%8F:%D0%9F%D1%80%D0%BE%D0%B3%D1%80%D0%B0%D0%BC%D0%BC%D0%BD%D0%BE%D0%B5_%D0%BE%D0%B1%D0%B5%D1%81%D0%BF%D0%B5%D1%87%D0%B5%D0%BD%D0%B8%D0%B5) и [ОС](https://www.tadviser.ru/index.php/%D0%9E%D0%A1)
* использование текстовых протоколов и ненужных открытых портов
* используя слабость одного гаджета, хакеру легко попасть во всю сеть
* использование незащищённых мобильных технологий
* использование незащищённой облачной инфраструктуры
* использование небезопасного ПО

Насколько безопасны «умные дома будущего»

Ниже [Panda](https://www.tadviser.ru/index.php/Panda) собрала несколько идей о способах, благодаря которым хакеры могли бы получить беспрецедентный доступ к Вашей повседневной жизни через комплексные устройства, которые расположены у Вас дома[[3]](https://www.tadviser.ru/index.php/%D0%A1%D1%82%D0%B0%D1%82%D1%8C%D1%8F:%D0%98%D0%BD%D1%84%D0%BE%D1%80%D0%BC%D0%B0%D1%86%D0%B8%D0%BE%D0%BD%D0%BD%D0%B0%D1%8F_%D0%B1%D0%B5%D0%B7%D0%BE%D0%BF%D0%B0%D1%81%D0%BD%D0%BE%D1%81%D1%82%D1%8C_%D0%B8%D0%BD%D1%82%D0%B5%D1%80%D0%BD%D0%B5%D1%82%D0%B0_%D0%B2%D0%B5%D1%89%D0%B5%D0%B9_(Internet_of_Things)#cite_note-2).

**Выкуп за вход домой?**

Т.к. [Интернет вещей](https://www.tadviser.ru/index.php/%D0%98%D0%BD%D1%82%D0%B5%D1%80%D0%BD%D0%B5%D1%82_%D0%B2%D0%B5%D1%89%D0%B5%D0%B9_Internet_of_Things_(IoT)) продолжает интегрировать, казалось бы, бессмысленные и несвязанные объекты, то полноценная домашняя [операционная система](https://www.tadviser.ru/index.php/%D0%9E%D0%A1) выглядит вполне вероятной. Хотя это превратит Ваш дом в оптимизированное жизненное пространство, полностью предназначенное для обеспечения Вашего комфорта, тем не менее, она может также нести Вам серьезные риски стать жертвой кибер-атаки в Вашем собственном доме.

**Центральное звено любой системы безопасности**[**умного дома**](https://www.tadviser.ru/index.php/%D0%A1%D1%82%D0%B0%D1%82%D1%8C%D1%8F:%D0%A3%D0%BC%D0%BD%D1%8B%D0%B9_%D0%B4%D0%BE%D0%BC_(Smart_home))**будущего – это его замок.**

Кстати, недавнее исследование показало, что умные замки пугающе легко можно взломать, в результате чего они не могут гарантировать выполнение своей основной функции, для которой, собственно говоря, они и существуют.

Существующие системы достаточно просты для кибер-хакеров и не являются препятствием для того, чтобы проникнуть в Ваш дом.

И мы решили подумать дальше: а что если хакеры в будущем смогут использовать это технологическое достижение против Вас? Если умный замок можно взломать, чтобы его открыть, возможно, хакеры найдут способ, как полностью его закрыть, чтобы Вы не могли его открыть.

В этом случае в будущем можно будет достаточно тихо проникать в чужой дом: хакер сможет контролировать все события удаленно. Более того, он сможет запрашивать у своих жертв какой-нибудь разумный выкуп за то, чтобы они могли попасть в свои собственные дома.

Кстати, это может быть идеей для сценария какого-нибудь страшного фильма (Совсем один дома), но это ужасная мысль. Если все Ваши устройства безопасности взаимосвязаны, то кибер-преступники потенциально могли бы получить доступ также к Вашей домашней сигнализации и даже ключам от Вашего автомобиля.

**Задымленный экран – тревога о пожаре**

Одна функция безопасности, которая уже встроена в некоторые доступные на рынке детекторы дыма, - это возможность, позволяющая [умному дому](https://www.tadviser.ru/index.php/%D0%A1%D1%82%D0%B0%D1%82%D1%8C%D1%8F:%D0%A3%D0%BC%D0%BD%D1%8B%D0%B9_%D0%B4%D0%BE%D0%BC_(Smart_home)) получать информацию (и использовать ее в дальнейшей работе) от других смарт-устройств, что позволяет системе реагировать соответствующим образом в случае опасности. Данная функция внедрена для безопасности пользователя, позволяя домашней системе, которая обнаружила пожар, например, разблокировать все двери в доме, чтобы помочь выбраться из него как можно быстрее.

Это отличный пример того, как производители [IoT](https://www.tadviser.ru/index.php/IoT)-решений работают над прозрачной интеграцией и взаимодействием смарт-устройств внутри умного дома. Однако есть одна оговорка: если эта технология будет использоваться [кибер-преступниками](https://www.tadviser.ru/index.php/%D0%9A%D0%B8%D0%B1%D0%B5%D1%80-%D0%BF%D1%80%D0%B5%D1%81%D1%82%D1%83%D0%BF%D0%BD%D0%B8%D0%BA%D0%B0%D0%BC%D0%B8), то существует вероятность создания нежелательной цепной реакции, которая в конечном итоге может, наоборот, снизить уровень безопасности умного дома.

Еще один способ, когда хакер мог бы потенциально издалека навредить, - это создание ложной тревоги о пожаре, которая отправляется в пожарные службы. Хаотическая сцена может выглядеть в виде задымленного экрана, что также в итоге может сделать Вас легкой добычей для других потенциально вредоносных кибер-атак.

**Пылесос смерти**

Наверное, это одна из наших «уайлдеровских» идей, но если вспомним про фурор, который произвел на всех самовзрывающийся [смартфон](https://www.tadviser.ru/index.php/%D0%A1%D0%BC%D0%B0%D1%80%D1%82%D1%84%D0%BE%D0%BD), то не будем удивляться и тому, что IoT-устройства все чаще ставят нас в такое положение, которое предоставляет хакерам доступ к потенциально взрывоопасным устройствам!

**Можно ли использовать IoT-устройства для кибер-атаки? Легко.**

Злоумышленники, как правило, работают на массы: например, распределенные атаки на отказ в обслуживании ([DDOS](https://www.tadviser.ru/index.php/DDOS)), когда тысячи электронных писем или запросов отправляются на какой-то сервер, чтобы замедлить его работу или вообще вывести его из строя.

В этом случае в будущем мы можем столкнуться с ситуациями, когда [хакеры](https://www.tadviser.ru/index.php/%D0%A1%D1%82%D0%B0%D1%82%D1%8C%D1%8F:%D0%A5%D0%B0%D0%BA%D0%B5%D1%80%D1%8B) попытаются «завалить» как можно больше машин в надежде на то, что какая-то их часть будет работать неправильно, что приведет к тяжелым последствиям. Вообще-то, пугающая перспектива. Возможно, как раз по этой причине правительственные органы говорят о потенциальных опасностях [Интернета вещей](https://www.tadviser.ru/index.php/%D0%98%D0%BD%D1%82%D0%B5%D1%80%D0%BD%D0%B5%D1%82_%D0%B2%D0%B5%D1%89%D0%B5%D0%B9_Internet_of_Things_(IoT)), связанных с кибер-атаками.

**Остерегайтесь холодильника**

Помните эпизод в «Симпсонах», когда Мардж нападает на домашнюю операционную систему с искусственным интеллектом, озвученную Пирсом Броснаном, которая готовит еду, но тайно планирует «избавится» от остальных членов семьи? Да, конечно, это забавная пародия, но смущает то, что нам потребуется всего несколько технологических достижений, чтобы эти события уже перестали быть смешными, а оказались ужасной действительностью.

Хорошо, допустим, что Ваш холодильник пока не ведет с Вами интеллектуальных бесед, и уж тем более, не прорабатывает какие-то убийственные схемы в отношении Вашей семьи. Однако еще два года назад ЦРУ отметили угрозу со стороны смарт-холодильников в умных домах. К чему бы это?

ЦРУ всполошилось от того, что холодильник использовался как часть бот-сети для выполнения DDOS-атаки. И все это происходило совершенно незаметно для хозяина этого холодильника, который даже и понятия не имел о том, что его смарт-устройство может выполнять какие-то дьявольские действия, кроме как охлаждать и сохранять еду.

**Что дальше?**

Т.к. смарт-устройства становятся все умнее, отслеживая Ваши покупательские предпочтения и осуществляя заказы на дом, мог бы хакер получить доступ к Вашим банковским данным или вмешаться в Ваши покупки? Мы все знаем, что [искусственный интеллект](https://www.tadviser.ru/index.php/%D0%98%D1%81%D0%BA%D1%83%D1%81%D1%81%D1%82%D0%B2%D0%B5%D0%BD%D0%BD%D1%8B%D0%B9_%D0%B8%D0%BD%D1%82%D0%B5%D0%BB%D0%BB%D0%B5%D0%BA%D1%82) и холодильники лучше оставить как жуткое видение в мультиках, а не ужас в реальной жизни!

Сертификация устройств IoT для защиты от хакеров

11 октября 2016 года стало известно о планах [Еврокомиссии](https://www.tadviser.ru/index.php/%D0%A1%D1%82%D0%B0%D1%82%D1%8C%D1%8F:%D0%95%D0%B2%D1%80%D0%BE%D0%BF%D0%B5%D0%B9%D1%81%D0%BA%D0%B8%D0%B9_%D1%81%D0%BE%D1%8E%D0%B7_(%D0%95%D0%B2%D1%80%D0%BE%D1%81%D0%BE%D1%8E%D0%B7,_%D0%95%D0%A1)) - ввести обязательную сертификацию или другую аналогичную процедуру всех приборов, подключаемых к [интернету вещей](https://www.tadviser.ru/index.php/%D0%A1%D1%82%D0%B0%D1%82%D1%8C%D1%8F:%D0%98%D0%BD%D1%82%D0%B5%D1%80%D0%BD%D0%B5%D1%82_%D0%B2%D0%B5%D1%89%D0%B5%D0%B9:_%D1%83%D1%81%D0%BF%D0%B5%D1%82%D1%8C_%D0%BD%D0%B5%D0%BB%D1%8C%D0%B7%D1%8F_%D0%BE%D1%81%D1%82%D0%B0%D1%82%D1%8C%D1%81%D1%8F). Предполагается принять меры на государственном уровне, что должно помешать хакерам использовать [интернет вещей](https://www.tadviser.ru/index.php/%D0%A1%D1%82%D0%B0%D1%82%D1%8C%D1%8F:%D0%98%D0%BD%D1%82%D0%B5%D1%80%D0%BD%D0%B5%D1%82_%D0%B2%D0%B5%D1%89%D0%B5%D0%B9,_IoT_(%D1%80%D1%8B%D0%BD%D0%BE%D0%BA_%D0%A0%D0%BE%D1%81%D1%81%D0%B8%D0%B8)) для создания [ботнетов](https://www.tadviser.ru/index.php/%D0%91%D0%BE%D1%82%D0%BD%D0%B5%D1%82).

Как вариант, не исключается установка на устройства сети специальных унифицированных чипов, которые обезопасят их от атак хакеров. Эти меры, по мнению чиновников [Еврокомиссии](https://www.tadviser.ru/index.php/%D0%A1%D1%82%D0%B0%D1%82%D1%8C%D1%8F:%D0%95%D0%B2%D1%80%D0%BE%D0%BF%D0%B5%D0%B9%D1%81%D0%BA%D0%B8%D0%B9_%D1%81%D0%BE%D1%8E%D0%B7_(%D0%95%D0%B2%D1%80%D0%BE%D1%81%D0%BE%D1%8E%D0%B7,_%D0%95%D0%A1)), должны повысить уровень доверия к [интернету вещей](https://www.tadviser.ru/index.php/%D0%A1%D1%82%D0%B0%D1%82%D1%8C%D1%8F:%D0%98%D0%BD%D1%82%D0%B5%D1%80%D0%BD%D0%B5%D1%82_%D0%B2%D0%B5%D1%89%D0%B5%D0%B9:_%D1%83%D1%81%D0%BF%D0%B5%D1%82%D1%8C_%D0%BD%D0%B5%D0%BB%D1%8C%D0%B7%D1%8F_%D0%BE%D1%81%D1%82%D0%B0%D1%82%D1%8C%D1%81%D1%8F) в обществе и помешать хакерам создавать [ботнеты](https://www.tadviser.ru/index.php/%D0%91%D0%BE%D1%82%D0%BD%D0%B5%D1%82) из подключаемой техники[[4]](https://www.tadviser.ru/index.php/%D0%A1%D1%82%D0%B0%D1%82%D1%8C%D1%8F:%D0%98%D0%BD%D1%84%D0%BE%D1%80%D0%BC%D0%B0%D1%86%D0%B8%D0%BE%D0%BD%D0%BD%D0%B0%D1%8F_%D0%B1%D0%B5%D0%B7%D0%BE%D0%BF%D0%B0%D1%81%D0%BD%D0%BE%D1%81%D1%82%D1%8C_%D0%B8%D0%BD%D1%82%D0%B5%D1%80%D0%BD%D0%B5%D1%82%D0%B0_%D0%B2%D0%B5%D1%89%D0%B5%D0%B9_(Internet_of_Things)#cite_note-a516688-3).



После DDoS-атаки на ресурс Krebs, индустрия в шоке от ее размера, глубины и сложности, (2016)

|  |  |  |
| --- | --- | --- |
| « | Меры по защите [интернета вещей](https://www.tadviser.ru/index.php/%D0%A1%D1%82%D0%B0%D1%82%D1%8C%D1%8F:%D0%98%D0%BD%D1%82%D0%B5%D1%80%D0%BD%D0%B5%D1%82_%D0%B2%D0%B5%D1%89%D0%B5%D0%B9:_%D1%83%D1%81%D0%BF%D0%B5%D1%82%D1%8C_%D0%BD%D0%B5%D0%BB%D1%8C%D0%B7%D1%8F_%D0%BE%D1%81%D1%82%D0%B0%D1%82%D1%8C%D1%81%D1%8F) от хакеров следует принимать именно на государственном уровне, поскольку в контроле нуждаются не только сами приборы, но и сети, к которым они подключены, а также облачные хранилища. Схема сертификации [интернета вещей](https://www.tadviser.ru/index.php/%D0%A1%D1%82%D0%B0%D1%82%D1%8C%D1%8F:%D0%98%D0%BD%D1%82%D0%B5%D1%80%D0%BD%D0%B5%D1%82_%D0%B2%D0%B5%D1%89%D0%B5%D0%B9,_IoT,_M2M_(%D0%BC%D0%B8%D1%80%D0%BE%D0%B2%D0%BE%D0%B9_%D1%80%D1%8B%D0%BD%D0%BE%D0%BA)) сравнима с европейской системой маркировки энергопотребляющих товаров, принятой в 1992 году. Маркировка обязательна для автомобилей, бытовой техники и электрических ламп. Но производители техники считают систему подобной маркировки неэффективной для защиты от хакеров. Вместо этого они предпочли бы установить в приборы стандартный чип, который будет отвечать за безопасность подключения к [интернету](https://www.tadviser.ru/index.php/%D0%98%D0%BD%D1%82%D0%B5%D1%80%D0%BD%D0%B5%D1%82).  **Тибо Клейнер (Thibault Kleiner), заместитель европейского комиссара по цифровой экономике и обществу** | » |

В группу приборов, подключаемых к [интернету](https://www.tadviser.ru/index.php/%D0%98%D0%BD%D1%82%D0%B5%D1%80%D0%BD%D0%B5%D1%82), входят видеокамеры, телевизоры, принтеры, холодильники и другая техника. Большая часть этих устройств неудовлетворительно защищена от хакерских атак. Сами по себе эти устройства могут не представлять интереса для преступников. Однако хакеры взламывают их, чтобы использовать в качестве роботов для создания [ботнетов](https://www.tadviser.ru/index.php/%D0%91%D0%BE%D1%82%D0%BD%D0%B5%D1%82), посредством которых можно атаковать более серьезные системы. Большинство владельцев взломанных устройств даже не подозревают, как используется их техника.

В качестве примера приведена масштабная [DDoS-атака](https://www.tadviser.ru/index.php/%D0%A1%D1%82%D0%B0%D1%82%D1%8C%D1%8F:DDoS-%D0%B0%D1%82%D0%B0%D0%BA%D0%B0) на [интернет](https://www.tadviser.ru/index.php/%D0%98%D0%BD%D1%82%D0%B5%D1%80%D0%BD%D0%B5%D1%82)-ресурс Krebs On Security, в сентябре 2016 года.

|  |  |  |
| --- | --- | --- |
| « | Интенсивность запросов от ботсети во время атаки достигла 700 Гб/с. В составе [ботсети](https://www.tadviser.ru/index.php/%D0%91%D0%BE%D1%82%D0%BD%D0%B5%D1%82) более 1 млн камер, видорегистраторов и других подключенных к [интернету вещей](https://www.tadviser.ru/index.php/%D0%A1%D1%82%D0%B0%D1%82%D1%8C%D1%8F:%D0%98%D0%BD%D1%82%D0%B5%D1%80%D0%BD%D0%B5%D1%82_%D0%B2%D0%B5%D1%89%D0%B5%D0%B9,_IoT,_M2M_(%D0%BC%D0%B8%D1%80%D0%BE%D0%B2%D0%BE%D0%B9_%D1%80%D1%8B%D0%BD%D0%BE%D0%BA)) устройств. Это не первый резонансный случай, когда подобные устройства становятся частью [ботнета](https://www.tadviser.ru/index.php/%D0%91%D0%BE%D1%82%D0%BD%D0%B5%D1%82), однако впервые сеть состояла почти полностью из таких приборов.  **Брайан Кребс (Brian Krebs), владелец ресурса** | » |

По данным [Gartner](https://www.tadviser.ru/index.php/%D0%9A%D0%BE%D0%BC%D0%BF%D0%B0%D0%BD%D0%B8%D1%8F:Gartner), к [интернету вещей](https://www.tadviser.ru/index.php/%D0%A1%D1%82%D0%B0%D1%82%D1%8C%D1%8F:%D0%98%D0%BD%D1%82%D0%B5%D1%80%D0%BD%D0%B5%D1%82_%D0%B2%D0%B5%D1%89%D0%B5%D0%B9:_%D1%83%D1%81%D0%BF%D0%B5%D1%82%D1%8C_%D0%BD%D0%B5%D0%BB%D1%8C%D0%B7%D1%8F_%D0%BE%D1%81%D1%82%D0%B0%D1%82%D1%8C%D1%81%D1%8F) подключено около 6 млрд приборов, а к 2020 году их число достигнет 20 млрд, что создаст хакерам более широкие возможности для проведения масштабных атак посредством [ботнетов](https://www.tadviser.ru/index.php/%D0%91%D0%BE%D1%82%D0%BD%D0%B5%D1%82).

Как обеспечить безопасность устройств IoT с приходом 5G и Индустрии 4.0

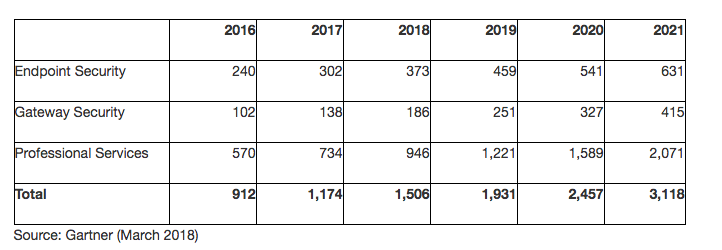
[Интернет](https://www.tadviser.ru/index.php/%D0%98%D0%BD%D1%82%D0%B5%D1%80%D0%BD%D0%B5%D1%82) вещей ([IoT](https://www.tadviser.ru/index.php/IoT)) активно распространяется по миру и находится на пороге всплеска развития. Этому способствуют несколько факторов: сети [5G](https://www.tadviser.ru/index.php/5G), [Индустрия 4.0](https://www.tadviser.ru/index.php/%D0%98%D0%BD%D0%B4%D1%83%D1%81%D1%82%D1%80%D0%B8%D1%8F_4.0) или Четвертая промышленная революция, растущие возможности микро[процессорных](https://www.tadviser.ru/index.php/%D0%9F%D1%80%D0%BE%D1%86%D0%B5%D1%81%D1%81%D0%BE%D1%80) вычислений. [Умный дом](https://www.tadviser.ru/index.php/%D0%A3%D0%BC%D0%BD%D1%8B%D0%B9_%D0%B4%D0%BE%D0%BC), бизнес и промышленный сегмент IoT-устройств имеют схожие проблемы внедрения – отсутствие единых стандартов, в том числе стандартов документации, качественных описаний протоколов и соединений и соответствующая дороговизна анализа уровня фактической защищенности, отсутствие стандартов функций защиты и, как правило, нехватка ресурсов микрочипов на качественное внедрение этих функций ([шифрование](https://www.tadviser.ru/index.php/%D0%A8%D0%B8%D1%84%D1%80%D0%BE%D0%B2%D0%B0%D0%BD%D0%B8%D0%B5), [аутентификация](https://www.tadviser.ru/index.php/%D0%90%D1%83%D1%82%D0%B5%D0%BD%D1%82%D0%B8%D1%84%D0%B8%D0%BA%D0%B0%D1%86%D0%B8%D1%8F) и т.д.). О том, какие риски внедрения IoT-устройств следует учитывать и как обезопасить такие решения, [читайте в материале](http://www.tadviser.ru/a/529925), подготовленном экспертом в сфере ИБ [Анной Михайловой](https://www.tadviser.ru/index.php/%D0%9F%D0%B5%D1%80%D1%81%D0%BE%D0%BD%D0%B0:%D0%9C%D0%B8%D1%85%D0%B0%D0%B9%D0%BB%D0%BE%D0%B2%D0%B0_%D0%90%D0%BD%D0%BD%D0%B0_%D0%AE%D1%80%D1%8C%D0%B5%D0%B2%D0%BD%D0%B0).

Оценка рынка

2017: Расходы на безопасность IoT в $1,2 млрд

21 марта 2018 года аналитическая компания [Gartner](https://www.tadviser.ru/index.php/%D0%9A%D0%BE%D0%BC%D0%BF%D0%B0%D0%BD%D0%B8%D1%8F:Gartner) обнародовала результаты исследования мирового рынка [информационной безопасности](https://www.tadviser.ru/index.php/%D0%98%D0%BD%D1%84%D0%BE%D1%80%D0%BC%D0%B0%D1%86%D0%B8%D0%BE%D0%BD%D0%BD%D0%B0%D1%8F_%D0%B1%D0%B5%D0%B7%D0%BE%D0%BF%D0%B0%D1%81%D0%BD%D0%BE%D1%81%D1%82%D1%8C) в сфере [Интернета вещей](https://www.tadviser.ru/index.php/%D0%98%D0%BD%D1%82%D0%B5%D1%80%D0%BD%D0%B5%D1%82_%D0%B2%D0%B5%D1%89%D0%B5%D0%B9_Internet_of_Things_(IoT)). Расходы компаний на обеспечение киберзащиты IoT-систем в 2017 году достигли $1,17 млрд, увеличившись на 29% относительно предыдущего года, когда затраты измерялись $912 млн.

Большая часть рассматриваемого рынка пришлось на профессиональные услуги, которые в 2017 году оказаны на сумму $734 млн против $570 млн годом ранее. В сегментах безопасности межсетевых устройств и пользовательского оборудования зафиксированы инвестиции в размере 138 и 302 млн [долларов](https://www.tadviser.ru/index.php/%D0%A1%D1%82%D0%B0%D1%82%D1%8C%D1%8F:%D0%94%D0%BE%D0%BB%D0%BB%D0%B0%D1%80_%D0%A1%D0%A8%D0%90) соответственно. В 2016-м эти показатели измерялись 240 и 102 млн долларов.



Расходы на безопасность Интернета вещей, данные Gartner

В исследовании отмечается, что [кибератаки](https://www.tadviser.ru/index.php/%D0%9A%D0%B8%D0%B1%D0%B5%D1%80%D0%B0%D1%82%D0%B0%D0%BA%D0%B8) на Интернет вещей стали реальностью. С ними в период с 2015 по 2018 годы столкнулись около 20% организаций, опрошенных Gartner.

По словам аналитика Gartner Руггеро Конту (Ruggero Contu), развертывая Интернет вещей, компании чаще всего не уделяют внимания источникам закупки оборудования и [программного обеспечения](https://www.tadviser.ru/index.php/%D0%A1%D1%82%D0%B0%D1%82%D1%8C%D1%8F:%D0%9F%D1%80%D0%BE%D0%B3%D1%80%D0%B0%D0%BC%D0%BC%D0%BD%D0%BE%D0%B5_%D0%BE%D0%B1%D0%B5%D1%81%D0%BF%D0%B5%D1%87%D0%B5%D0%BD%D0%B8%D0%B5), а также их особенностям.

Прогнозируется, что еще до 2020 года безопасность Интернета вещей не будет приоритетной для бизнеса. Кроме того, внедрение наилучших ИБ-практик и инструментов при планировании IoT будет игнорироваться. Из-за этих двух сдерживающих факторов рынок ИБ-решений для Интернета вещей лишится 80% потенциальной выручки.

Главным драйвером роста рассматриваемого рынка специалисты называют спрос на инструменты и сервисы, улучшающие обнаружение угроз и управление активами, оценку безопасности оборудования и [софта](https://www.tadviser.ru/index.php/%D0%A1%D1%82%D0%B0%D1%82%D1%8C%D1%8F:%D0%9F%D1%80%D0%BE%D0%B3%D1%80%D0%B0%D0%BC%D0%BC%D0%BD%D0%BE%D0%B5_%D0%BE%D0%B1%D0%B5%D1%81%D0%BF%D0%B5%D1%87%D0%B5%D0%BD%D0%B8%D0%B5), а также тестирование на защиту IoT-систем от несанкционированного доступа. Благодаря этим факторам расходы на информационную безопасность Интернета вещей вырастут до $3,1 млрд в 2021 году, прогнозируют в Gartner.[[5]](https://www.tadviser.ru/index.php/%D0%A1%D1%82%D0%B0%D1%82%D1%8C%D1%8F:%D0%98%D0%BD%D1%84%D0%BE%D1%80%D0%BC%D0%B0%D1%86%D0%B8%D0%BE%D0%BD%D0%BD%D0%B0%D1%8F_%D0%B1%D0%B5%D0%B7%D0%BE%D0%BF%D0%B0%D1%81%D0%BD%D0%BE%D1%81%D1%82%D1%8C_%D0%B8%D0%BD%D1%82%D0%B5%D1%80%D0%BD%D0%B5%D1%82%D0%B0_%D0%B2%D0%B5%D1%89%D0%B5%D0%B9_(Internet_of_Things)#cite_note-4)

История инцидентов

Вымогатели-шифровальщики вещей

*Основная статья*: [Ransomware of Things (RoT)](https://www.tadviser.ru/index.php/%D0%A1%D1%82%D0%B0%D1%82%D1%8C%D1%8F:Ransomware_of_Things_(RoT))

2024: Умные устройства вашего дома под прицелом хакеров. Как от них защититься - инструкция

Почти половину из [паролей](https://www.tadviser.ru/index.php/%D0%A1%D1%82%D0%B0%D1%82%D1%8C%D1%8F:%D0%9F%D0%B0%D1%80%D0%BE%D0%BB%D0%B8) к [IoT](https://www.tadviser.ru/index.php/IoT)-устройствам хакеры могут подобрать менее чем за одну минуту – такие данные приводят специалисты [Kaspersky Lab](https://www.tadviser.ru/index.php/%D0%9A%D0%BE%D0%BC%D0%BF%D0%B0%D0%BD%D0%B8%D1%8F:%D0%9B%D0%B0%D0%B1%D0%BE%D1%80%D0%B0%D1%82%D0%BE%D1%80%D0%B8%D1%8F_%D0%9A%D0%B0%D1%81%D0%BF%D0%B5%D1%80%D1%81%D0%BA%D0%BE%D0%B3%D0%BE_(Kaspersky)).[[6]](https://www.tadviser.ru/index.php/%D0%A1%D1%82%D0%B0%D1%82%D1%8C%D1%8F:%D0%98%D0%BD%D1%84%D0%BE%D1%80%D0%BC%D0%B0%D1%86%D0%B8%D0%BE%D0%BD%D0%BD%D0%B0%D1%8F_%D0%B1%D0%B5%D0%B7%D0%BE%D0%BF%D0%B0%D1%81%D0%BD%D0%BE%D1%81%D1%82%D1%8C_%D0%B8%D0%BD%D1%82%D0%B5%D1%80%D0%BD%D0%B5%D1%82%D0%B0_%D0%B2%D0%B5%D1%89%D0%B5%D0%B9_(Internet_of_Things)#cite_note-5) Какие методы взлома используются чаще всего и есть ли способы защитить умные устройства? Подробнее читайте в [статье](https://www.tadviser.ru/index.php/%D0%9D%D0%BE%D0%B2%D0%BE%D1%81%D1%82%D0%B8:%D0%A3%D0%BC%D0%BD%D1%8B%D0%B5_%D1%83%D1%81%D1%82%D1%80%D0%BE%D0%B9%D1%81%D1%82%D0%B2%D0%B0_%D0%B2%D0%B0%D1%88%D0%B5%D0%B3%D0%BE_%D0%B4%D0%BE%D0%BC%D0%B0_%D0%BF%D0%BE%D0%B4_%D0%BF%D1%80%D0%B8%D1%86%D0%B5%D0%BB%D0%BE%D0%BC_%D1%85%D0%B0%D0%BA%D0%B5%D1%80%D0%BE%D0%B2._%D0%9A%D0%B0%D0%BA_%D0%BE%D1%82_%D0%BD%D0%B8%D1%85_%D0%B7%D0%B0%D1%89%D0%B8%D1%82%D0%B8%D1%82%D1%8C%D1%81%D1%8F_-_%D0%B8%D0%BD%D1%81%D1%82%D1%80%D1%83%D0%BA%D1%86%D0%B8%D1%8F).

2022

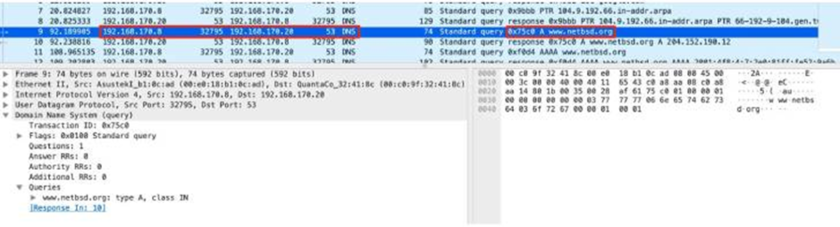
**Неисправленная DNS-уязвимость подвергает опасности миллионы IoT-устройств**

3 мая 2022 года стало известно о том, что неисправленная [DNS](https://www.tadviser.ru/index.php/%D0%A1%D1%82%D0%B0%D1%82%D1%8C%D1%8F:DNS)-уязвимость подвергает опасности миллионы [IoT](https://www.tadviser.ru/index.php/IoT)-устройств.

Уязвимость затрагивает реализацию системы [доменных](https://www.tadviser.ru/index.php/%D0%A1%D1%82%D0%B0%D1%82%D1%8C%D1%8F:%D0%94%D0%BE%D0%BC%D0%B5%D0%BD%D1%8B) имен (DNS) в двух популярных библиотеках на [языке C](https://www.tadviser.ru/index.php/%D0%9F%D1%80%D0%BE%D0%B4%D1%83%D0%BA%D1%82:C_%D0%AF%D0%B7%D1%8B%D0%BA_%D0%BF%D1%80%D0%BE%D0%B3%D1%80%D0%B0%D0%BC%D0%BC%D0%B8%D1%80%D0%BE%D0%B2%D0%B0%D0%BD%D0%B8%D1%8F).

О проблеме впервые сообщили в сентябре 2021 года. Уязвимость затрагивает создание системы доменных имен (DNS) в библиотеках uClibc и uClibc-ng на языке C, используемых для разработки встраиваемых [Linux](https://www.tadviser.ru/index.php/Linux)-систем. uClibc хорошо известна благодаря крупным компаниям, библиотеку используют [Linksys](https://www.tadviser.ru/index.php/%D0%9A%D0%BE%D0%BC%D0%BF%D0%B0%D0%BD%D0%B8%D1%8F:Linksys), [Netgear](https://www.tadviser.ru/index.php/%D0%9A%D0%BE%D0%BC%D0%BF%D0%B0%D0%BD%D0%B8%D1%8F:Netgear) и [Axis](https://www.tadviser.ru/index.php/Axis), а также дистрибутивы Linux.

|  |  |  |
| --- | --- | --- |
| « | Уязвимость вызвана предсказуемостью идентификаторов транзакций внутри DNS-запросов, генерируемых библиотекой., – сказали **Джаннис Царайас и Андреа Паланка из Nozomi Networks.** — Изъян может позволить злоумышленникам использовать DNS-[спуфинг](https://www.tadviser.ru/index.php/%D0%A1%D1%82%D0%B0%D1%82%D1%8C%D1%8F:%D0%A1%D0%BF%D1%83%D1%84%D0%B8%D0%BD%D0%B3_(spoofing)_-_%D0%BA%D0%B8%D0%B1%D0%B5%D1%80%D0%B0%D1%82%D0%B0%D0%BA%D0%B0) против выбранного устройства. | » |



Отравление кэша DNS или DNS-спуфинг – техника повреждения кэша DNS-резолверов с целью перенаправления пользователя на вредоносные веб-сайты.

Использование ошибки позволяет проводить [атаки](https://www.tadviser.ru/index.php/%D0%9A%D0%B8%D0%B1%D0%B5%D1%80%D0%B0%D1%82%D0%B0%D0%BA%D0%B8) типа " человек посередине " (MITM) и повреждать кэш DNS, эффективно перенаправляя [интернет](https://www.tadviser.ru/index.php/%D0%98%D0%BD%D1%82%D0%B5%D1%80%D0%BD%D0%B5%D1%82)-трафик на подконтрольный злоумышленнику сервер.

[Nozomi Networks](https://www.tadviser.ru/index.php/%D0%9A%D0%BE%D0%BC%D0%BF%D0%B0%D0%BD%D0%B8%D1%8F:Nozomi_Networks) предупредила о возможности использования уязвимости против [операционных систем](https://www.tadviser.ru/index.php/%D0%9E%D0%A1), настроенных на использование фиксированного или предсказуемого порта источника.

|  |  |  |
| --- | --- | --- |
| « | Использовав уязвимость, [хакер](https://www.tadviser.ru/index.php/%D0%A1%D1%82%D0%B0%D1%82%D1%8C%D1%8F:%D0%A5%D0%B0%D0%BA%D0%B5%D1%80%D1%8B) может управлять передаваемой пользователями [информацией](https://www.tadviser.ru/index.php/%D0%A1%D1%82%D0%B0%D1%82%D1%8C%D1%8F:%D0%98%D0%BD%D1%84%D0%BE%D1%80%D0%BC%D0%B0%D1%86%D0%B8%D1%8F) и выполнять другие атаки на зараженные устройства, – заявили специалисты[[7]](https://www.tadviser.ru/index.php/%D0%A1%D1%82%D0%B0%D1%82%D1%8C%D1%8F:%D0%98%D0%BD%D1%84%D0%BE%D1%80%D0%BC%D0%B0%D1%86%D0%B8%D0%BE%D0%BD%D0%BD%D0%B0%D1%8F_%D0%B1%D0%B5%D0%B7%D0%BE%D0%BF%D0%B0%D1%81%D0%BD%D0%BE%D1%81%D1%82%D1%8C_%D0%B8%D0%BD%D1%82%D0%B5%D1%80%D0%BD%D0%B5%D1%82%D0%B0_%D0%B2%D0%B5%D1%89%D0%B5%D0%B9_(Internet_of_Things)#cite_note-6). | » |

**IoT-ботнет Enemybot на базе Mirai набирает обороты**

14 апреля 2022 года стало известно, что специалисты [ИБ](https://www.tadviser.ru/index.php/%D0%98%D0%91)-компании [Fortinet](https://www.tadviser.ru/index.php/%D0%9A%D0%BE%D0%BC%D0%BF%D0%B0%D0%BD%D0%B8%D1%8F:Fortinet) обнаружили [ботнет](https://www.tadviser.ru/index.php/%D0%A1%D1%82%D0%B0%D1%82%D1%8C%D1%8F:%D0%91%D0%BE%D1%82%D0%BD%D0%B5%D1%82_(Botnet)) на базе [исходного кода](https://www.tadviser.ru/index.php/%D0%A1%D1%82%D0%B0%D1%82%D1%8C%D1%8F:%D0%98%D1%81%D1%85%D0%BE%D0%B4%D0%BD%D1%8B%D0%B9_%D0%BA%D0%BE%D0%B4) Mirai, получивший название Enemybot. [Ботсеть](https://www.tadviser.ru/index.php/%D0%A1%D1%82%D0%B0%D1%82%D1%8C%D1%8F:%D0%91%D0%BE%D1%82%D0%BD%D0%B5%D1%82_(Botnet)) набирает обороты, заражая модемы, [маршрутизаторы](https://www.tadviser.ru/index.php/%D0%9C%D0%B0%D1%80%D1%88%D1%80%D1%83%D1%82%D0%B8%D0%B7%D0%B0%D1%82%D0%BE%D1%80%D1%8B_(%D1%80%D0%BE%D1%83%D1%82%D0%B5%D1%80%D1%8B)) и [IoT](https://www.tadviser.ru/index.php/IoT)-устройства через известные [уязвимости](https://www.tadviser.ru/index.php/%D0%A1%D1%82%D0%B0%D1%82%D1%8C%D1%8F:%D0%A3%D1%8F%D0%B7%D0%B2%D0%B8%D0%BC%D0%BE%D1%81%D1%82%D0%B8_%D0%B2_%D0%9F%D0%9E_%D0%B8_%D0%BE%D0%B1%D0%BE%D1%80%D1%83%D0%B4%D0%BE%D0%B2%D0%B0%D0%BD%D0%B8%D0%B8). Подробнее [здесь](https://www.tadviser.ru/index.php/%D0%A1%D1%82%D0%B0%D1%82%D1%8C%D1%8F:%D0%91%D0%BE%D1%82%D0%BD%D0%B5%D1%82_(Botnet)#.2AIoT-.D0.B1.D0.BE.D1.82.D0.BD.D0.B5.D1.82_Enemybot_.D0.BD.D0.B0_.D0.B1.D0.B0.D0.B7.D0.B5_Mirai_.D0.BD.D0.B0.D0.B1.D0.B8.D1.80.D0.B0.D0.B5.D1.82_.D0.BE.D0.B1.D0.BE.D1.80.D0.BE.D1.82.D1.8B).

2020

**Исследование Check Point показало, как сети могут быть взломаны с помощью лампочки**

6 февраля 2020 года компания [Check Point Software Technologies](https://www.tadviser.ru/index.php/%D0%9A%D0%BE%D0%BC%D0%BF%D0%B0%D0%BD%D0%B8%D1%8F:Check_Point_Software_Technologies) сообщила об уязвимостях, которые могли бы позволить [хакеру](https://www.tadviser.ru/index.php/%D0%A5%D0%B0%D0%BA%D0%B5%D1%80) доставить вымогателей или другие [вредоносные](https://www.tadviser.ru/index.php/%D0%A1%D1%82%D0%B0%D1%82%D1%8C%D1%8F:%D0%92%D1%80%D0%B5%D0%B4%D0%BE%D0%BD%D0%BE%D1%81%D0%BD%D0%B0%D1%8F_%D0%BF%D1%80%D0%BE%D0%B3%D1%80%D0%B0%D0%BC%D0%BC%D0%B0_(%D0%B7%D0%BB%D0%BE%D0%B2%D1%80%D0%B5%D0%B4)) программы в офисные и домашние сети, захватив умные лампочки и их контроллер. Подробнее [здесь](https://www.tadviser.ru/index.php/%D0%9F%D1%80%D0%BE%D0%B4%D1%83%D0%BA%D1%82:Philips_Hue).

**Данные 515 тыс. серверов, домашних маршрутизаторов и IoT-устройств оказались в открытом доступе**

Киберпреступник выложил в открытый доступ списки учетных [данных](https://www.tadviser.ru/index.php/%D0%A1%D1%82%D0%B0%D1%82%D1%8C%D1%8F:%D0%94%D0%B0%D0%BD%D0%BD%D1%8B%D0%B5) [Telnet](https://www.tadviser.ru/index.php/%D0%A1%D1%82%D0%B0%D1%82%D1%8C%D1%8F:Telnet) для более 515 тыс. [серверов](https://www.tadviser.ru/index.php/%D0%A1%D0%B5%D1%80%D0%B2%D0%B5%D1%80), домашних [маршрутизаторов](https://www.tadviser.ru/index.php/%D0%9C%D0%B0%D1%80%D1%88%D1%80%D1%83%D1%82%D0%B8%D0%B7%D0%B0%D1%82%D0%BE%D1%80) и [IoT](https://www.tadviser.ru/index.php/IoT)-устройств. Об этом стало известно 20 января 2020 года. Подробнее [здесь](https://www.tadviser.ru/index.php/%D0%A1%D1%82%D0%B0%D1%82%D1%8C%D1%8F:Telnet).

**Сексуальное вымогательство через умные камеры**

В середине января 2020 года исследователи забили тревогу из-за волны нового вида мошенничества — сексуального вымогательства на фоне паники по поводу безопасности умных камер.

Опасения по поводу подключенных к [интернету](https://www.tadviser.ru/index.php/%D0%98%D0%BD%D1%82%D0%B5%D1%80%D0%BD%D0%B5%D1%82) камер в сочетании с простой рассылкой по электронной почте позволяют обмануть ничего не подозревающую жертву. По сети прокатилась волна новой версии старой аферы - преступники пытаются убедить жертву в том, что у них есть компрометирующая информация, которую они выпустят в свет, если им не заплатить выкуп. Теперь мошенники утверждают, что получили записи сексуального характера с умных камер безопасности, и угрожают загрузить их в общедоступную сеть или разослать друзьям жертвы.



Исследователи забили тревогу из-за волны нового вида мошенничества — сексуального вымогательства на фоне паники по поводу безопасности умных камер

Исследователи из компании Mimecast зафиксировали огромный всплеск нового вида мошенничества: всего за два дня с 2 по 3 января было перехвачено более 1600 мошеннических писем. Злоумышленники пишут, что у них есть несколько компрометирующих фотографий или видеороликов и дают ссылку на веб-сайт, где отображаются обычные кадры с камер наблюдения в общей зоне, например, в баре или ресторане — месте, которое любой человек мог посетить на прошлой неделе. Эти кадры должны убедить жертву, что его или ее компрометирующие действия записали с помощью камер безопасности или [смартфона](https://www.tadviser.ru/index.php/%D0%A1%D0%BC%D0%B0%D1%80%D1%82%D1%84%D0%BE%D0%BD).

|  |  |  |
| --- | --- | --- |
| « | Представьте все, что вы сделали за последний год, и представьте, что мы видели, как вы делаете, — писали злоумышленники. — Видео с вами уже загружены на несколько порно-сайтов и у вас есть только одна неделя, прежде чем они станут доступны для просмотра. | » |

На самом деле такое видео не существует, а мошенники просто закидывают удочку, надеясь, что жертва клюнет на приманку. Это очень дешевый и невероятно эффективный способ мошенничества. В 2018 году общее количество жалоб на вымогательство по электронной почте выросло на 242%, и специалисты предупреждают пользователей не реагировать на угрозы и немедленно обращаться в полицию.[[8]](https://www.tadviser.ru/index.php/%D0%A1%D1%82%D0%B0%D1%82%D1%8C%D1%8F:%D0%98%D0%BD%D1%84%D0%BE%D1%80%D0%BC%D0%B0%D1%86%D0%B8%D0%BE%D0%BD%D0%BD%D0%B0%D1%8F_%D0%B1%D0%B5%D0%B7%D0%BE%D0%BF%D0%B0%D1%81%D0%BD%D0%BE%D1%81%D1%82%D1%8C_%D0%B8%D0%BD%D1%82%D0%B5%D1%80%D0%BD%D0%B5%D1%82%D0%B0_%D0%B2%D0%B5%D1%89%D0%B5%D0%B9_(Internet_of_Things)#cite_note-7)

2019

**75% атак на устройства интернета вещей приходится на США**

В 2020 году [атаки](https://www.tadviser.ru/index.php/%D0%9A%D0%B8%D0%B1%D0%B5%D1%80%D0%B0%D1%82%D0%B0%D0%BA%D0%B8) на объекты [интернета](https://www.tadviser.ru/index.php/%D0%98%D0%BD%D1%82%D0%B5%D1%80%D0%BD%D0%B5%D1%82) вещей ([IoT](https://www.tadviser.ru/index.php/IoT)) значительно возрастут. Об этом стало известно 17 декабря 2019 года. Такие прогнозы дает [Национальный координационный центр по компьютерным инцидентам (НКЦКИ)](https://www.tadviser.ru/index.php/%D0%9A%D0%BE%D0%BC%D0%BF%D0%B0%D0%BD%D0%B8%D1%8F:%D0%9D%D0%B0%D1%86%D0%B8%D0%BE%D0%BD%D0%B0%D0%BB%D1%8C%D0%BD%D1%8B%D0%B9_%D0%BA%D0%BE%D0%BE%D1%80%D0%B4%D0%B8%D0%BD%D0%B0%D1%86%D0%B8%D0%BE%D0%BD%D0%BD%D1%8B%D0%B9_%D1%86%D0%B5%D0%BD%D1%82%D1%80_%D0%BF%D0%BE_%D0%BA%D0%BE%D0%BC%D0%BF%D1%8C%D1%8E%D1%82%D0%B5%D1%80%D0%BD%D1%8B%D0%BC_%D0%B8%D0%BD%D1%86%D0%B8%D0%B4%D0%B5%D0%BD%D1%82%D0%B0%D0%BC_(%D0%9D%D0%9A%D0%A6%D0%9A%D0%98)). В 2020 г. традиционно наибольшей опасности подвергнутся объекты [кредитно](https://www.tadviser.ru/index.php/%D0%A1%D1%82%D0%B0%D1%82%D1%8C%D1%8F:%D0%9A%D1%80%D0%B5%D0%B4%D0%B8%D1%82%D0%BE%D0%B2%D0%B0%D0%BD%D0%B8%D0%B5_%D0%B2_%D0%A0%D0%BE%D1%81%D1%81%D0%B8%D0%B8)-[финансовой](https://www.tadviser.ru/index.php/%D0%A4%D0%B8%D0%BD%D0%B0%D0%BD%D1%81%D1%8B) сферы, поскольку злоумышленники будут следовать желанию заработать.

Об этом сообщил заместитель директора Национального координационного центра по [компьютерным](https://www.tadviser.ru/index.php/%D0%A1%D1%82%D0%B0%D1%82%D1%8C%D1%8F:%D0%9A%D0%BE%D0%BC%D0%BF%D1%8C%D1%8E%D1%82%D0%B5%D1%80) инцидентам Николай Мурашов.

Такой прогноз замглавы НКЦКИ объяснил тем, что на декабрь 2019 года в мире насчитывается уже около 5 млрд устройств IoT, а в ближайшие несколько лет эта цифра вырастет в 10 раз. Вместе с тем, говорит он, производители оборудования спешат выпустить свою продукцию на рынок, мало задумываясь о безопасности. Именно это, предупредил Николай Мурашов, создает наибольшие угрозы в области [кибербезопасности](https://www.tadviser.ru/index.php/%D0%9A%D0%B8%D0%B1%D0%B5%D1%80%D0%B1%D0%B5%D0%B7%D0%BE%D0%BF%D0%B0%D1%81%D0%BD%D0%BE%D1%81%D1%82%D0%B8) в 2020 г.

Как рассказал Николай Мурашов, с 2015 г. сохраняется тенденция использования [DDoS](https://www.tadviser.ru/index.php/DDoS)-атак с использованием бот-сетей [интернета](https://www.tadviser.ru/index.php/%D0%98%D0%BD%D1%82%D0%B5%D1%80%D0%BD%D0%B5%D1%82) вещей. К таким устройствам относятся, например, домашние [роутеры](https://www.tadviser.ru/index.php/%D0%A0%D0%BE%D1%83%D1%82%D0%B5%D1%80), веб-камеры, устройства [умного дома](https://www.tadviser.ru/index.php/%D0%A3%D0%BC%D0%BD%D1%8B%D0%B9_%D0%B4%D0%BE%D0%BC), средства контроля самочувствия и др. Такие устройства часто взламываются, захватываются в бот-сети и используются для атак на другие объекты, в том числе на объекты [КИИ](https://www.tadviser.ru/index.php/%D0%A1%D1%82%D0%B0%D1%82%D1%8C%D1%8F:%D0%9A%D1%80%D0%B8%D1%82%D0%B8%D1%87%D0%B5%D1%81%D0%BA%D0%B0%D1%8F_%D0%B8%D0%BD%D1%84%D0%BE%D1%80%D0%BC%D0%B0%D1%86%D0%B8%D0%BE%D0%BD%D0%BD%D0%B0%D1%8F_%D0%B8%D0%BD%D1%84%D1%80%D0%B0%D1%81%D1%82%D1%80%D1%83%D0%BA%D1%82%D1%83%D1%80%D0%B0_%D0%A0%D0%BE%D1%81%D1%81%D0%B8%D0%B8), приводит пример он. Николай Мурашов предупреждает, что совокупность таких атак с использованием бот-сетей может быть настолько велика, что может привести к нарушению работы интернет-сети в целом регионе.

По [данным](https://www.tadviser.ru/index.php/%D0%A1%D1%82%D0%B0%D1%82%D1%8C%D1%8F:%D0%94%D0%B0%D0%BD%D0%BD%D1%8B%D0%B5) [McAfee](https://www.tadviser.ru/index.php/%D0%9A%D0%BE%D0%BC%D0%BF%D0%B0%D0%BD%D0%B8%D1%8F:McAfee) за I квартал 2019 г., на [США](https://www.tadviser.ru/index.php/%D0%A1%D0%A8%D0%90) приходится 75% атак на устройства интернета вещей, на [Китай](https://www.tadviser.ru/index.php/%D0%9A%D0%B8%D1%82%D0%B0%D0%B9) и [Германию](https://www.tadviser.ru/index.php/%D0%93%D0%B5%D1%80%D0%BC%D0%B0%D0%BD%D0%B8%D1%8E) - по 4%, а на [Бразилию](https://www.tadviser.ru/index.php/%D0%91%D1%80%D0%B0%D0%B7%D0%B8%D0%BB%D0%B8%D1%8F) и [Италию](https://www.tadviser.ru/index.php/%D0%98%D1%82%D0%B0%D0%BB%D0%B8%D1%8F) - по 3%. Как гласит исследование [Lumen Technologies (ранее CenturyLink)](https://www.tadviser.ru/index.php/%D0%9A%D0%BE%D0%BC%D0%BF%D0%B0%D0%BD%D0%B8%D1%8F:Lumen_Technologies_(%D1%80%D0%B0%D0%BD%D0%B5%D0%B5_CenturyLink)) (США), центрами управления бот-сетями чаще всего управляют группы, находящиеся в США, [Китае](https://www.tadviser.ru/index.php/%D0%9A%D0%B8%D1%82%D0%B0%D0%B9), России, [Нидерландах](https://www.tadviser.ru/index.php/%D0%9D%D0%B8%D0%B4%D0%B5%D1%80%D0%BB%D0%B0%D0%BD%D0%B4%D1%8B) и [Мексике](https://www.tadviser.ru/index.php/%D0%9C%D0%B5%D0%BA%D1%81%D0%B8%D0%BA%D0%B0)[[9]](https://www.tadviser.ru/index.php/%D0%A1%D1%82%D0%B0%D1%82%D1%8C%D1%8F:%D0%98%D0%BD%D1%84%D0%BE%D1%80%D0%BC%D0%B0%D1%86%D0%B8%D0%BE%D0%BD%D0%BD%D0%B0%D1%8F_%D0%B1%D0%B5%D0%B7%D0%BE%D0%BF%D0%B0%D1%81%D0%BD%D0%BE%D1%81%D1%82%D1%8C_%D0%B8%D0%BD%D1%82%D0%B5%D1%80%D0%BD%D0%B5%D1%82%D0%B0_%D0%B2%D0%B5%D1%89%D0%B5%D0%B9_(Internet_of_Things)#cite_note-8).

**ФБР: для каждого IoT-устройства необходима отдельная сеть**

В начале декабря 2019 года [ФБР](https://www.tadviser.ru/index.php/%D0%9A%D0%BE%D0%BC%D0%BF%D0%B0%D0%BD%D0%B8%D1%8F:%D0%A4%D0%91%D0%A0_(FBI)) порекомендовало пользователям [интернета](https://www.tadviser.ru/index.php/%D0%98%D0%BD%D1%82%D0%B5%D1%80%D0%BD%D0%B5%D1%82) вещей изолировать основные подключенные [IoT](https://www.tadviser.ru/index.php/%D0%98%D0%BD%D1%82%D0%B5%D1%80%D0%BD%D0%B5%D1%82_%D0%B2%D0%B5%D1%89%D0%B5%D0%B9_Internet_of_Things_(IoT))-устройства, такие как ноутбуки или [смартфоны](https://www.tadviser.ru/index.php/%D0%A1%D0%BC%D0%B0%D1%80%D1%82%D1%84%D0%BE%D0%BD), от остальных с помощью отдельной сети [Wi-Fi](https://www.tadviser.ru/index.php/%D0%A1%D1%82%D0%B0%D1%82%D1%8C%D1%8F:Wi-Fi) или [локальной сети](https://www.tadviser.ru/index.php/%D0%A1%D1%82%D0%B0%D1%82%D1%8C%D1%8F:LAN_(Local_Area_Network)_-_%D0%BB%D0%BE%D0%BA%D0%B0%D0%BB%D1%8C%D0%BD%D0%B0%D1%8F_%D0%B2%D1%8B%D1%87%D0%B8%D1%81%D0%BB%D0%B8%D1%82%D0%B5%D0%BB%D1%8C%D0%BD%D0%B0%D1%8F_%D1%81%D0%B5%D1%82%D1%8C).

|  |  |  |
| --- | --- | --- |
| « | Ваш холодильник и ноутбук не должны быть в одной сети, - говорится в сообщении ФБР. | » |

Специалисты по киберезопасности из бюро рекомендуют использовать два [интернет-шлюза](https://www.tadviser.ru/index.php/%D0%A1%D1%82%D0%B0%D1%82%D1%8C%D1%8F:%D0%98%D0%BD%D1%82%D0%B5%D1%80%D0%BD%D0%B5%D1%82-%D1%88%D0%BB%D1%8E%D0%B7): один для устройств, которые хранят конфиденциальные данные, а другой для цифровых помощников, таких как устройства домашней безопасности, [умные часы](https://www.tadviser.ru/index.php/%D0%A1%D1%82%D0%B0%D1%82%D1%8C%D1%8F:%D0%A3%D0%BC%D0%BD%D1%8B%D0%B5_%D1%87%D0%B0%D1%81%D1%8B_(%D1%81%D0%BC%D0%B0%D1%80%D1%82-%D1%87%D0%B0%D1%81%D1%8B)), игровые системы, [фитнес-трекеры](https://www.tadviser.ru/index.php/%D0%A1%D1%82%D0%B0%D1%82%D1%8C%D1%8F:%D0%A4%D0%B8%D1%82%D0%BD%D0%B5%D1%81-%D1%82%D1%80%D0%B5%D0%BA%D0%B5%D1%80%D1%8B), термостаты, умные лампочки и т. д. Также рекомендуется изменить все заводские пароли по умолчанию.



По мнению ФБР IoT-устройства должны подключаться к изолированным источникам

Согласно данным ФБР, потенциальные уязвимости в устройствах IoT позволяют хакерам получить доступ к сети [маршрутизатора](https://www.tadviser.ru/index.php/%D0%9C%D0%B0%D1%80%D1%88%D1%80%D1%83%D1%82%D0%B8%D0%B7%D0%B0%D1%82%D0%BE%D1%80%D1%8B_(%D1%80%D0%BE%D1%83%D1%82%D0%B5%D1%80%D1%8B)), обеспечив тем самым доступ к другим подключенным устройствам в домашней сети. Создание отдельных сетевых систем позволит предотвратить вторжение злоумышленников на основные устройства.

Кроме того, специалисты рекомендуют использовать микросегментацию. Данная функция, доступная во встроенном программном обеспечении большинства маршрутизаторов WiFi: она позволяет администраторам маршрутизаторов создавать виртуальные сети (VLAN), которые ведут себя как разные сети, даже если работают на одном маршрутизаторе.

В целом ФБР предложило следующие принципы цифровой обороны:

* Измените заводские настройки устройства с пароля по умолчанию.
* Пароли должны быть максимально длинными и уникальными для всех устройств IoT.
* Многие подключенные устройства работают в связке с мобильными приложениями. Эти приложения могут работать в фоновом режиме и использовать разрешения по умолчанию, о которых вы даже не подозревали. Узнайте, какую личную информацию собирают эти приложения и скорректируйте разрешения.
* Убедитесь, что все ваши устройства регулярно обновляются.[[10]](https://www.tadviser.ru/index.php/%D0%A1%D1%82%D0%B0%D1%82%D1%8C%D1%8F:%D0%98%D0%BD%D1%84%D0%BE%D1%80%D0%BC%D0%B0%D1%86%D0%B8%D0%BE%D0%BD%D0%BD%D0%B0%D1%8F_%D0%B1%D0%B5%D0%B7%D0%BE%D0%BF%D0%B0%D1%81%D0%BD%D0%BE%D1%81%D1%82%D1%8C_%D0%B8%D0%BD%D1%82%D0%B5%D1%80%D0%BD%D0%B5%D1%82%D0%B0_%D0%B2%D0%B5%D1%89%D0%B5%D0%B9_(Internet_of_Things)#cite_note-9)

**Зафиксировано 105 млн атак на IoT-устройства за первое полугодие**

16 октября 2019 года стало известно, что в первой половине 2019 года специалисты из «[Лаборатории Касперского](https://www.tadviser.ru/index.php/%D0%9B%D0%B0%D0%B1%D0%BE%D1%80%D0%B0%D1%82%D0%BE%D1%80%D0%B8%D0%B8_%D0%9A%D0%B0%D1%81%D0%BF%D0%B5%D1%80%D1%81%D0%BA%D0%BE%D0%B3%D0%BE)» с помощью ханипотов (ресурс, представляющий собой приманку для злоумышленников) зафиксировали 105 млн [атак](https://www.tadviser.ru/index.php/%D0%9A%D0%B8%D0%B1%D0%B5%D1%80%D0%B0%D1%82%D0%B0%D0%BA%D0%B8) на [IoT](https://www.tadviser.ru/index.php/IoT)-устройства, исходящих с 276 тыс. уникальных [IP](https://www.tadviser.ru/index.php/%D0%A1%D1%82%D0%B0%D1%82%D1%8C%D1%8F:IP)-адресов. Данный показатель в семь раз больше, чем в первой половине 2018 года, когда было обнаружено около 12 млн атак с 69 тыс. IP-адресов. Пользуясь слабой защитой IoT-продуктов, [киберпреступники](https://www.tadviser.ru/index.php/%D0%A1%D1%82%D0%B0%D1%82%D1%8C%D1%8F:%D0%A5%D0%B0%D0%BA%D0%B5%D1%80%D1%8B) прикладывают больше усилий для создания и [монетизации](https://www.tadviser.ru/index.php/%D0%A1%D1%82%D0%B0%D1%82%D1%8C%D1%8F:%D0%9C%D0%BE%D0%BD%D0%B5%D1%82%D0%B8%D0%B7%D0%B0%D1%86%D0%B8%D1%8F_%D0%B4%D0%B0%D0%BD%D0%BD%D1%8B%D1%85) IoT-[ботнетов](https://www.tadviser.ru/index.php/%D0%91%D0%BE%D1%82%D0%BD%D0%B5%D1%82).

Количество кибератак на IoT-устройства стремительно увеличивается, поскольку все чаще пользователей и организаций приобретают «умные» устройства, такие как [маршрутизаторы](https://www.tadviser.ru/index.php/%D0%9C%D0%B0%D1%80%D1%88%D1%80%D1%83%D1%82%D0%B8%D0%B7%D0%B0%D1%82%D0%BE%D1%80) или камеры видеорегистрации, но при этом не все заботятся об их защите. Киберпреступники, в свою очередь, видят все больше [финансовых](https://www.tadviser.ru/index.php/%D0%A4%D0%B8%D0%BD%D0%B0%D0%BD%D1%81%D1%8B) возможностей в использовании таких устройств. Они используют сети зараженных «умных» устройств для проведения [DDoS](https://www.tadviser.ru/index.php/DDoS)-атак или в качестве прокси-[сервера](https://www.tadviser.ru/index.php/%D0%A1%D0%B5%D1%80%D0%B2%D0%B5%D1%80) для других типов [вредоносных](https://www.tadviser.ru/index.php/%D0%97%D0%BB%D0%BE%D0%B2%D1%80%D0%B5%D0%B4) действий.

Согласно собранным [данным](https://www.tadviser.ru/index.php/%D0%A1%D1%82%D0%B0%D1%82%D1%8C%D1%8F:%D0%94%D0%B0%D0%BD%D0%BD%D1%8B%D0%B5), атаки на IoT-устройства не отличаются сложностью, однако достаточно скрытны, чтобы пользователи не заметили их. Семейство вредоносных программ Mirai применялось в 39% от всех атак, в рамках которых использовались эксплойты, позволяющие ботнетам компрометировать устройства, эксплуатируя старые уязвимости, и контролировать их. На втором месте оказалось семейство вредоносов Nyadrop (38,57%) с применением техники бруфорса. Nyadrop также часто служил в качестве загрузчика Mirai. Третьим наиболее распространенным ботнетом стал Gafgyt (2,12% от всех атак).

Исследователи также определили страны, которые чаще других оказывались источниками заражения в первой половине 2019 года. 30% от всех атак происходили в [Китае](https://www.tadviser.ru/index.php/%D0%9A%D0%B8%D1%82%D0%B0%D0%B5), в [Бразилии](https://www.tadviser.ru/index.php/%D0%91%D1%80%D0%B0%D0%B7%D0%B8%D0%BB%D0%B8%D1%8F) — 19%, за ней следует [Египет](https://www.tadviser.ru/index.php/%D0%95%D0%B3%D0%B8%D0%BF%D0%B5%D1%82) с показателем в 12%. В первой половине 2018 года ситуация была иной — Бразилия лидировала с показателем в 28%, [Китай](https://www.tadviser.ru/index.php/%D0%9A%D0%B8%D1%82%D0%B0%D0%B9) занимал второе место (14%), [Япония](https://www.tadviser.ru/index.php/%D0%AF%D0%BF%D0%BE%D0%BD%D0%B8%D1%8F) третье (11%).

Страны-источники Telnet-атак на ханипоты «Лаборатории Касперского»

IoT является плодотворной областью для злоумышленников, которые используют даже самые примитивные методы, такие как угадывание комбинаций [паролей](https://www.tadviser.ru/index.php/%D0%A1%D1%82%D0%B0%D1%82%D1%8C%D1%8F:%D0%9F%D0%B0%D1%80%D0%BE%D0%BB%D0%B8) и логинов для [авторизации](https://www.tadviser.ru/index.php/%D0%90%D0%B2%D1%82%D0%BE%D1%80%D0%B8%D0%B7%D0%B0%D1%86%D0%B8%D0%B8) в системе. Пользователи очень часто пользуются распространенными комбинациями, как, например, «support/support», за которыми следуют «admin/admin», «default/default»[[11]](https://www.tadviser.ru/index.php/%D0%A1%D1%82%D0%B0%D1%82%D1%8C%D1%8F:%D0%98%D0%BD%D1%84%D0%BE%D1%80%D0%BC%D0%B0%D1%86%D0%B8%D0%BE%D0%BD%D0%BD%D0%B0%D1%8F_%D0%B1%D0%B5%D0%B7%D0%BE%D0%BF%D0%B0%D1%81%D0%BD%D0%BE%D1%81%D1%82%D1%8C_%D0%B8%D0%BD%D1%82%D0%B5%D1%80%D0%BD%D0%B5%D1%82%D0%B0_%D0%B2%D0%B5%D1%89%D0%B5%D0%B9_(Internet_of_Things)#cite_note-10).

Среди государств, с территории которых исходили атаки на ханипоты «Лаборатории Касперского», на первом месте оказался Китай, на втором — Бразилия; далее с разрывом в 0,1% шли Египет и [Россия](https://www.tadviser.ru/index.php/%D0%A0%D0%BE%D1%81%D1%81%D0%B8%D1%8F). Наблюдаемые тенденции в целом сохранялись на протяжении 2018 и 2019 годов с небольшими изменениями в рейтинге стран по количеству атак[[12]](https://www.tadviser.ru/index.php/%D0%A1%D1%82%D0%B0%D1%82%D1%8C%D1%8F:%D0%98%D0%BD%D1%84%D0%BE%D1%80%D0%BC%D0%B0%D1%86%D0%B8%D0%BE%D0%BD%D0%BD%D0%B0%D1%8F_%D0%B1%D0%B5%D0%B7%D0%BE%D0%BF%D0%B0%D1%81%D0%BD%D0%BE%D1%81%D1%82%D1%8C_%D0%B8%D0%BD%D1%82%D0%B5%D1%80%D0%BD%D0%B5%D1%82%D0%B0_%D0%B2%D0%B5%D1%89%D0%B5%D0%B9_(Internet_of_Things)#cite_note-11).



**В Trend Micro выяснили, как киберкриминальные группировки используют устройства IoT**

10 сентября 2019 года компания [Trend Micro](https://www.tadviser.ru/index.php/%D0%9A%D0%BE%D0%BC%D0%BF%D0%B0%D0%BD%D0%B8%D1%8F:Trend_Micro) опубликовала исследование «Uncovering IoT Threats in the Cybercrime Underground», в котором описывается, как [киберкриминальные](https://www.tadviser.ru/index.php/%D0%A1%D1%82%D0%B0%D1%82%D1%8C%D1%8F:%D0%9A%D0%B8%D0%B1%D0%B5%D1%80%D0%BF%D1%80%D0%B5%D1%81%D1%82%D1%83%D0%BF%D0%BD%D0%BE%D1%81%D1%82%D1%8C_%D0%B2_%D0%BC%D0%B8%D1%80%D0%B5) группировки используют устройства [IoT](https://www.tadviser.ru/index.php/IoT) в своих целях и какие угрозы это создаёт.

Аналитики Trend Micro исследовали [даркнет](https://www.tadviser.ru/index.php/%D0%A1%D1%82%D0%B0%D1%82%D1%8C%D1%8F:%D0%94%D0%B0%D1%80%D0%BA%D0%BD%D0%B5%D1%82_(%D1%82%D0%B5%D0%BD%D0%B5%D0%B2%D0%BE%D0%B9_%D0%B8%D0%BD%D1%82%D0%B5%D1%80%D0%BD%D0%B5%D1%82)), выясняя, какие уязвимости IoT наиболее популярны среди киберпреступников, а также на каких языках говорят участники киберподполья. В ходе исследования выяснилось, что [русский](https://www.tadviser.ru/index.php/%D0%A0%D0%BE%D1%81%D1%81%D0%B8%D1%8F) язык вошёл в пятёрку наиболее популярных в Даркнете. Кроме русского в топ-5 языков даркнета присутствуют [английский](https://www.tadviser.ru/index.php/%D0%92%D0%B5%D0%BB%D0%B8%D0%BA%D0%BE%D0%B1%D1%80%D0%B8%D1%82%D0%B0%D0%BD%D0%B8%D1%8F), [португальский](https://www.tadviser.ru/index.php/%D0%9F%D0%BE%D1%80%D1%82%D1%83%D0%B3%D0%B0%D0%BB%D0%B8%D1%8F), [испанский](https://www.tadviser.ru/index.php/%D0%98%D1%81%D0%BF%D0%B0%D0%BD%D0%B8%D1%8F) и арабский. В отчёте представлен анализ пяти киберпреступных сообществ, классифицированных в соответствии с языками, которые они используют для общения. Язык оказался более важным объединяющим фактором, чем географическое положение.



[Интернет вещей](https://www.tadviser.ru/index.php/%D0%A1%D1%82%D0%B0%D1%82%D1%8C%D1%8F:%D0%98%D0%BD%D1%82%D0%B5%D1%80%D0%BD%D0%B5%D1%82_%D0%B2%D0%B5%D1%89%D0%B5%D0%B9) стал важной частью современного общества. Рост количества устройств IoT делает их желанной целью для киберпреступников, формируя новый ландшафт угроз. Производители зачастую потворствуют киберпреступникам, выпуская изделия без каких-либо функций обеспечения [безопасности](https://www.tadviser.ru/index.php/%D0%98%D0%91). В результате такие устройства пополняют ряды очередного [ботнета](https://www.tadviser.ru/index.php/%D0%91%D0%BE%D1%82%D0%BD%D0%B5%D1%82) и работают на благо киберкриминала.

Главная движущая сила, управляющая действиями киберпреступного сообщества — это деньги. В связи с этим [хакеры](https://www.tadviser.ru/index.php/%D0%A5%D0%B0%D0%BA%D0%B5%D1%80) рассматривают уязвимости IoT не сами по себе, а в контексте возможной [монетизации](https://www.tadviser.ru/index.php/%D0%A1%D1%82%D0%B0%D1%82%D1%8C%D1%8F:%D0%9C%D0%BE%D0%BD%D0%B5%D1%82%D0%B8%D0%B7%D0%B0%D1%86%D0%B8%D1%8F_%D0%B4%D0%B0%D0%BD%D0%BD%D1%8B%D1%85). Именно поэтому в исследовании основное внимание уделяется не уязвимостям и [атакам](https://www.tadviser.ru/index.php/%D0%9A%D0%B8%D0%B1%D0%B5%D1%80%D0%B0%D1%82%D0%B0%D0%BA%D0%B0), а бизнес-моделям, которые используют преступные сообщества.

Русскоязычный киберкриминальный рынок, по данным Trend Micro — самый сложный и самый процветающий из всех, приведённых в исследовании. Здесь продаются свежие уязвимости для [маршрутизаторов](https://www.tadviser.ru/index.php/%D0%9C%D0%B0%D1%80%D1%88%D1%80%D1%83%D1%82%D0%B8%D0%B7%D0%B0%D1%82%D0%BE%D1%80%D1%8B_(%D1%80%D0%BE%D1%83%D1%82%D0%B5%D1%80%D1%8B)), модифицированные прошивки для счётчиков электроэнергии. Здесь обсуждают взлом бензоколонок, продают и покупают ботнеты на базе устройств IoT.

Среди основных направлений монетизации взломанных устройств IoT в исследовании выделяют их использование для организации [DDoS-атак](https://www.tadviser.ru/index.php/DDoS) и в качестве узлов выхода [VPN](https://www.tadviser.ru/index.php/VPN). В обоих случаях преступники продают свои услуги другим участникам сообщества.

Большой интерес среди русскоговорящего андерграунда вызывают [криптомайнеры](https://www.tadviser.ru/index.php/%D0%A1%D1%82%D0%B0%D1%82%D1%8C%D1%8F:%D0%9A%D1%80%D0%B8%D0%BF%D1%82%D0%BE%D0%BC%D0%B0%D0%B9%D0%BD%D0%B5%D1%80) для устройств на базе [Android](https://www.tadviser.ru/index.php/%D0%9F%D1%80%D0%BE%D0%B4%D1%83%D0%BA%D1%82:Android), причём речь не о [смартфонах](https://www.tadviser.ru/index.php/%D0%A1%D0%BC%D0%B0%D1%80%D1%82%D1%84%D0%BE%D0%BD), ограниченная ёмкость батарей которых не позволяет использовать их для извлечения прибыли, а о смарт-[телевизорах](https://www.tadviser.ru/index.php/%D0%A1%D1%82%D0%B0%D1%82%D1%8C%D1%8F:%D0%A2%D0%B5%D0%BB%D0%B5%D0%B2%D0%B8%D0%B7%D0%BE%D1%80%D1%8B_(%D0%BC%D0%B8%D1%80%D0%BE%D0%B2%D0%BE%D0%B9_%D1%80%D1%8B%D0%BD%D0%BE%D0%BA)), [приставках](https://www.tadviser.ru/index.php/%D0%A1%D1%82%D0%B0%D1%82%D1%8C%D1%8F:%D0%9F%D1%80%D0%B8%D1%81%D1%82%D0%B0%D0%B2%D0%BA%D0%B8_Smart_TV_(%D1%80%D1%8B%D0%BD%D0%BE%D0%BA_%D0%A0%D0%BE%D1%81%D1%81%D0%B8%D0%B8)) и других устройствах.

Российские хакеры активно ищут возможности модификации и продажи специализированных прошивок для интеллектуальных счётчиков газа, воды и электричества, поскольку российское правительство санкционировало замену всех [коммунальных](https://www.tadviser.ru/index.php/%D0%96%D0%9A%D0%A5) счетчиков на умные, подключенные к [интернету](https://www.tadviser.ru/index.php/%D0%98%D0%BD%D1%82%D0%B5%D1%80%D0%BD%D0%B5%D1%82). Судя по сообщениям на форумах, пока имеется лишь один план монетизации — физически продавать модифицированные счетчики как средство экономии на ежемесячных коммунальных счетах за электроэнергию, воду и [газ](https://www.tadviser.ru/index.php/%D0%93%D0%B0%D0%B7%D0%BE%D0%B2%D0%B0%D1%8F_%D0%BF%D1%80%D0%BE%D0%BC%D1%8B%D1%88%D0%BB%D0%B5%D0%BD%D0%BD%D0%BE%D1%81%D1%82%D1%8C). Возможно, в будущем взлом интеллектуальных счетчиков станет новым способом криминального заработка, но на сентябрь 2019 года взлом этих устройств больше похож на [хактивизм](https://www.tadviser.ru/index.php/%D0%A1%D1%82%D0%B0%D1%82%D1%8C%D1%8F:%D0%A5%D0%B0%D0%BA%D1%82%D0%B8%D0%B2%D0%B8%D0%B7%D0%BC), чем на профессиональные атаки, отметили в Trend Micro.

В качестве итога специалисты Trend Micro делятся прогнозом связанных с IoT угроз на ближайшие 12-18 месяцев (2019-2020 гг.):

1. Уменьшение количества взломанных маршрутизаторов, поскольку большая часть атак связана с изменением настроек [DNS](https://www.tadviser.ru/index.php/%D0%A1%D1%82%D0%B0%D1%82%D1%8C%D1%8F:DNS), которые легко предотвратить. Если интернет-[провайдеры](https://www.tadviser.ru/index.php/%D0%A1%D1%82%D0%B0%D1%82%D1%8C%D1%8F:%D0%9F%D1%80%D0%BE%D0%B2%D0%B0%D0%B9%D0%B4%D0%B5%D1%80) и производители [роутеров](https://www.tadviser.ru/index.php/%D0%A0%D0%BE%D1%83%D1%82%D0%B5%D1%80) начнут защищать эти настройки, возможно появление новых векторов атак.
2. Рост числа атак на [промышленные устройства интернета вещей (IIoT)](https://www.tadviser.ru/index.php/IIoT), причём в качестве вектора монетизации будет использоваться вымогательство.
3. Появление новых инструментальных средств для проведения атак на IoT/[IIoT](https://www.tadviser.ru/index.php/IIoT) и рост популярности двух основных коммерческих наборов [вредоносных программ](https://www.tadviser.ru/index.php/%D0%92%D1%80%D0%B5%D0%B4%D0%BE%D0%BD%D0%BE%D1%81%D0%BD%D1%8B%D1%85_%D0%BF%D1%80%D0%BE%D0%B3%D1%80%D0%B0%D0%BC%D0%BC) для IoT.
4. Появление более сложных угроз, таких как низкоуровневые [руткиты](https://www.tadviser.ru/index.php/%D0%A1%D1%82%D0%B0%D1%82%D1%8C%D1%8F:%D0%A0%D1%83%D1%82%D0%BA%D0%B8%D1%82) или заражение микропрограммного обеспечения.
5. Новые оригинальные способы монетизации заражения смарт-устройств.
6. Развитие экосистемы автоматизированных атак.

2018: Nokia Threat Intelligence Report

В ноябре 2018 года компания [Nokia](https://www.tadviser.ru/index.php/%D0%9A%D0%BE%D0%BC%D0%BF%D0%B0%D0%BD%D0%B8%D1%8F:Nokia) опубликовала отчет, согласно которому доля [IoT](https://www.tadviser.ru/index.php/%D0%A1%D1%82%D0%B0%D1%82%D1%8C%D1%8F:%D0%98%D0%BD%D1%82%D0%B5%D1%80%D0%BD%D0%B5%D1%82_%D0%B2%D0%B5%D1%89%D0%B5%D0%B9)-ботнетов среди всех вредоносных программ в сетях провайдеров услуг связи в 2018 году выросла до 78%. Это более чем в два раза превышает показатели 2016 года, когда о ботнетах стали говорить, как о значимой угрозе. Прогнозируется, что в 2019 году ситуация только ухудшится. Подробнее [здесь](https://www.tadviser.ru/index.php/%D0%A1%D1%82%D0%B0%D1%82%D1%8C%D1%8F:%D0%91%D0%BE%D1%82%D0%BD%D0%B5%D1%82_(Botnet)).

2017

**Gemalto: У потребителей нет уверенности в безопасности устройств IoT**

Компания [Gemalto](https://www.tadviser.ru/index.php/%D0%9A%D0%BE%D0%BC%D0%BF%D0%B0%D0%BD%D0%B8%D1%8F:Gemalto) обнародовала в октябре 2017 года данные: оказывается, 90% потребителей не доверяют безопасности устройств [Интернета вещей](https://www.tadviser.ru/index.php/%D0%98%D0%BD%D1%82%D0%B5%D1%80%D0%BD%D0%B5%D1%82_%D0%B2%D0%B5%D1%89%D0%B5%D0%B9_Internet_of_Things_(IoT)) (Internet of Things или [IoT](https://www.tadviser.ru/index.php/IoT)). Вот почему более двух третей потребителей и почти 80% организаций поддержали правительства, принимающие меры по обеспечению безопасности IoT.

Основные опасения потребителей (согласно двум третям респондентов) касаются хакеров, которые могут установить контроль над их устройством. Фактически, это вызывает большее беспокойство, чем утечка данных (60%) и доступ хакеров к личной информации (54%). Несмотря на то, что устройствами IoT владеет более половины (54%) потребителей (в среднем, по два устройства на человека), только 14% считают себя хорошо осведомленными о безопасности этих устройств. Такая статистика показывает, что как потребителям, так и предприятиям, необходимо дополнительное образование в данной сфере.

Что касается уровня инвестиций в безопасность, то опрос показал, что производители устройств IoT и поставщики услуг тратят всего 11% своего общего IoT-бюджета на обеспечение безопасности устройств Интернета вещей. Исследование показало, что эти компании действительно признают важность защиты устройств и данных, которые они генерируют или передают, а 50% компаний обеспечивают безопасность на основе проектного подхода. Две трети (67%) организаций сообщают о применении [шифрования](https://www.tadviser.ru/index.php/%D0%A8%D0%B8%D1%84%D1%80%D0%BE%D0%B2%D0%B0%D0%BD%D0%B8%D0%B5) в качестве основного метода защиты активов IoT с 62%-ным шифрованием данных сразу по достижении IoT-устройства, а 59% − при выходе из устройства. Девяносто два процента компаний наблюдали увеличение продаж или использования продукта после внедрения мер по обеспечению безопасности IoT.

**Поддержка правил безопасности IoT набирает обороты**

Согласно опросу, компании поддерживают положения, дающие понять, кто несет ответственность за обеспечение безопасности устройств и данных IoT на каждом этапе их применения (61%) и каковы последствия несоблюдения безопасности (55%). Фактически, почти каждая организация (96%) и каждый потребитель (90%) испытывают необходимость в правилах по обеспечению безопасности Интернета вещей, принятых на уровне правительства.

**Отсутствие всесторонних возможностей, способствующих налаживанию партнерства**

К счастью, компании постепенно осознают, что им нужна поддержка в понимании технологии IoT и обращаются к партнерам за помощью, отдавая наибольшее предпочтение провайдерам облачных услуг (52%) и поставщикам услуг IoT (50%). В качестве главной причины для такого обращения они чаще всего называют отсутствие опыта и навыков (47%), а затем − помощь и ускорение развертывания Интернета вещей (46%).

Несмотря на то, что такие партнерские отношения могут принести пользу бизнесу при внедрении Интернета вещей, организации признают, что они не имеют полного контроля над данными, собираемыми продуктами или сервисами Интернета вещей, когда эти данные переходят от партнера к партнеру, что потенциально оставляет их незащищенными.

**Уязвимость HomeHack позволяет взять под контроль IoT-устройства LG SmartThinQ**

Компания [Check Point Software Technologies](https://www.tadviser.ru/index.php/%D0%9A%D0%BE%D0%BC%D0%BF%D0%B0%D0%BD%D0%B8%D1%8F:Check_Point_Software_Technologies) Ltd., поставщик решений по [кибербезопасности](https://www.tadviser.ru/index.php/%D0%98%D0%91) во всем мире, 26 октября 2017 года объявила об обнаружении HomeHack — уязвимости, из-за которой миллионы домашних смарт-устройств SmartThinkQ могли оказаться под угрозой взлома и удаленного управления. HomeHack позволила исследователям Check Point создать поддельную учетную запись LG, а затем использовать ее, чтобы завладеть учетной записью и умными устройствами пользователя LG.

**Контроль над смарт-устройствами**

Уязвимости в [мобильном](https://www.tadviser.ru/index.php/%D0%9C%D0%BE%D0%B1%D0%B8%D0%BB%D1%8C%D0%BD%D1%8B%D0%B5_%D0%BF%D1%80%D0%B8%D0%BB%D0%BE%D0%B6%D0%B5%D0%BD%D0%B8%D1%8F) и [облачном](https://www.tadviser.ru/index.php/%D0%9E%D0%B1%D0%BB%D0%B0%D0%BA%D0%BE) приложениях [LG](https://www.tadviser.ru/index.php/%D0%9A%D0%BE%D0%BC%D0%BF%D0%B0%D0%BD%D0%B8%D1%8F:LG) SmartThinkQ позволили исследователям Check Point удаленно войти в облачное приложение SmartThinQ, и, завладев учетной записью LG, получить контроль над пылесосом и встроенной в него видеокамерой. Получив контроль над учетной записью конкретного пользователя LG, злоумышленник может контролировать любое устройство LG или устройство, связанное с этой учетной записью, включая пылесосы, холодильники, плиты, посудомоечные и стиральные машины, фены и кондиционеры, рассказали в компании.

**Слежка за пользователем**

Уязвимость HomeHack дает хакерам возможность следить за домашней жизнью пользователей с помощью видеокамеры [робота](https://www.tadviser.ru/index.php/%D0%A1%D1%82%D0%B0%D1%82%D1%8C%D1%8F:%D0%A0%D0%BE%D0%B1%D0%BE%D1%82%D1%8B_(%D1%80%D0%BE%D0%B1%D0%BE%D1%82%D0%BE%D1%82%D0%B5%D1%85%D0%BD%D0%B8%D0%BA%D0%B0))-пылесоса Hom-Bot, которая в режиме реального времени отправляет видео в приложение LG SmartThinQ в рамках функции HomeGuard Security. В зависимости от моделей устройств LG злоумышленники могут также включать и отключать посудомоечные или стиральные машины.

*Видео, демонстрирующее, как может быть проведена атака посредством уязвимости HomeHack*

**Уязвимость устранена**

Check Point обнаружила уязвимость 31 июля 2017 года и сообщила об этом LG, соблюдая политику конфиденциальности информации. LG устранила уязвимости в приложении SmartThinQ в конце сентября.

**Как защититься**

Для защиты от возможного взлома мобильных приложений и устройств LG SmartThinQ Check Point рекомендует пользователям выполнить следующие действия:

* Обновить приложение LG SmartThinQ до последней версии (V1.9.23). Это можно сделать через [Google Play Store](https://www.tadviser.ru/index.php/%D0%9F%D1%80%D0%BE%D0%B4%D1%83%D0%BA%D1%82:Google_Play_Store), [Apple App Store](https://www.tadviser.ru/index.php/Apple_App_Store) или через настройки приложения LG SmartThinQ.
* Обновить сами устройства Smart Home до последней версии. Необходимо нажать на «интеллектуальный домашний продукт» под панелью инструментов SmartThinQ (если доступно обновление, пользователь получит всплывающее оповещение).

**Об устройствах SmartThinQ**

Умные устройства и решения по безопасности SmartThinQ от LG позволяют пользователям проверять и поддерживать состояние своего дома со [смартфона](https://www.tadviser.ru/index.php/%D0%A1%D1%82%D0%B0%D1%82%D1%8C%D1%8F:%D0%A1%D0%BC%D0%B0%D1%80%D1%82%D1%84%D0%BE%D0%BD%D1%8B_(%D1%80%D1%8B%D0%BD%D0%BE%D0%BA_%D0%A0%D0%BE%D1%81%D1%81%D0%B8%D0%B8)). По данным LG, только в первом полугодии 2016 года объем продаж роботизированного пылесоса Hom-Bot превысил 400 тыс. ед. В 2016 году 80 млн смарт-устройств были распроданы по всему миру — на 64% больше, чем в 2015 году.

**Хакеры атаковали сеть ИВ-устройств университета**

Компании и организации по всему миру все чаще сталкиваются с [кибератаками](https://www.tadviser.ru/index.php/%D0%9A%D0%B8%D0%B1%D0%B5%D1%80%D0%B0%D1%82%D0%B0%D0%BA%D0%B0%D0%BC%D0%B8), способными остановить или серьезно замедлить их бизнес-операции, говорится в отчете от компании [Verizon](https://www.tadviser.ru/index.php/%D0%9A%D0%BE%D0%BC%D0%BF%D0%B0%D0%BD%D0%B8%D1%8F:Verizon) (весна 2017 года). В частности, эксперты по безопасности приводят пример неназванного американского университета, который столкнулся с крупной [хакерской](https://www.tadviser.ru/index.php/%D0%A5%D0%B0%D0%BA%D0%B5%D1%80) атакой через сеть из более чем пяти тысяч устройств [интернета](https://www.tadviser.ru/index.php/%D0%98%D0%BD%D1%82%D0%B5%D1%80%D0%BD%D0%B5%D1%82) вещей (ИВ) на территории кампуса[[13]](https://www.tadviser.ru/index.php/%D0%A1%D1%82%D0%B0%D1%82%D1%8C%D1%8F:%D0%98%D0%BD%D1%84%D0%BE%D1%80%D0%BC%D0%B0%D1%86%D0%B8%D0%BE%D0%BD%D0%BD%D0%B0%D1%8F_%D0%B1%D0%B5%D0%B7%D0%BE%D0%BF%D0%B0%D1%81%D0%BD%D0%BE%D1%81%D1%82%D1%8C_%D0%B8%D0%BD%D1%82%D0%B5%D1%80%D0%BD%D0%B5%D1%82%D0%B0_%D0%B2%D0%B5%D1%89%D0%B5%D0%B9_(Internet_of_Things)#cite_note-12).

Данный тип атаки эксперты называют «ботнет заграждением». Изначально представители ИТ-служб университета зарегистрировали множество жалоб на медленное или совсем недоступное подключение к [интернету](https://www.tadviser.ru/index.php/%D0%98%D0%BD%D1%82%D0%B5%D1%80%D0%BD%D0%B5%D1%82) в кампусе. После проверки выяснилось, что [DNS](https://www.tadviser.ru/index.php/%D0%A1%D1%82%D0%B0%D1%82%D1%8C%D1%8F:DNS)-[серверы](https://www.tadviser.ru/index.php/%D0%A1%D0%B5%D1%80%D0%B2%D0%B5%D1%80) сети университета производили огромное количество запросов, а также создали множество поддоменов с именами, связанными с морепродуктами. После более подробного расследования было выявлено более пяти тысяч отдельных устройств, отправлявших сотни DNS-запросов каждые пятнадцать минут.

«Среди этих устройств, почти все относились к сегменту сети, составляющей нашу инфраструктуру интернета вещей. Ситуация была крайне сложная, так как на сегодняшний день специалисты по борьбе с кибератаками неплохо подготовлены для исправления проблем со сторонним доступам к компьютерам или серверам, но не имеют ни малейшего понятия о том, что делать в случае атаки на устройства интернета вещей, кроме, разве что, полной замены каждой машины с напитками и каждого фонарного столба», — говорится в отчете Verizon.

Исследование показало, что [ботнет](https://www.tadviser.ru/index.php/%D0%91%D0%BE%D1%82%D0%BD%D0%B5%D1%82), захвативший сеть устройств интернета вещей в университете, распространялся от одного девайса к другому, подбирая доступ к устройствам со слабыми или совсем отсутствующими [паролями](https://www.tadviser.ru/index.php/%D0%9F%D0%B0%D1%80%D0%BE%D0%BB%D1%8F%D0%BC%D0%B8) с помощью техники полного перебора. Чтобы вернуть управление над скомпрометированными устройствами, специалисты университета использовали специальный алгоритм, позволяющий перехватывать пароли взломанных устройств с последующей оперативной их заменой до того, как [вредоносное ПО](https://www.tadviser.ru/index.php/%D0%92%D1%80%D0%B5%D0%B4%D0%BE%D0%BD%D0%BE%D1%81%D0%BD%D0%BE%D0%B5_%D0%9F%D0%9E) успеет провести обновление.

2016: Хакеры впервые взломали унитаз

Футуристические высокотехнологичные унитазы весьма уязвимы к кибернападениям. Это удалось доказать группе взломщиков, работающих в подразделении компании [Panasonic](https://www.tadviser.ru/index.php/%D0%9A%D0%BE%D0%BC%D0%BF%D0%B0%D0%BD%D0%B8%D1%8F:Panasonic), которое занимается вопросами безопасности, написала в феврале 2016 года Mirror[[14]](https://www.tadviser.ru/index.php/%D0%A1%D1%82%D0%B0%D1%82%D1%8C%D1%8F:%D0%98%D0%BD%D1%84%D0%BE%D1%80%D0%BC%D0%B0%D1%86%D0%B8%D0%BE%D0%BD%D0%BD%D0%B0%D1%8F_%D0%B1%D0%B5%D0%B7%D0%BE%D0%BF%D0%B0%D1%81%D0%BD%D0%BE%D1%81%D1%82%D1%8C_%D0%B8%D0%BD%D1%82%D0%B5%D1%80%D0%BD%D0%B5%D1%82%D0%B0_%D0%B2%D0%B5%D1%89%D0%B5%D0%B9_(Internet_of_Things)#cite_note-13).

Глава подразделения, Хикохиро Лин, рассказал, что "умный" унитаз, который управляется через беспроводное соединение [Bluetooth](https://www.tadviser.ru/index.php/%D0%A1%D1%82%D0%B0%D1%82%D1%8C%D1%8F:Bluetooth) при помощи [смартфона](https://www.tadviser.ru/index.php/%D0%A1%D0%BC%D0%B0%D1%80%D1%82%D1%84%D0%BE%D0%BD), очень легко поддается взлому. В результате хакеры получают доступ ко всем возможностям устройства - например, они могут в любой момент включить спуск воды и испугать посетителя туалета.

По словам исследователей, причиной легкого взлома стал стандартный пароль, который устанавливается производителем и практически никогда не меняется самими пользователями.

"Всякий раз, когда кто-то использует туалет, мы можем контролировать все", - заявил Хикохиро Лин. Стоит отметить, что, по мнению многих специалистов, разработчики устройств для "[интернета](https://www.tadviser.ru/index.php/%D0%98%D0%BD%D1%82%D0%B5%D1%80%D0%BD%D0%B5%D1%82) вещей" слишком мало внимания уделяют вопросам безопасности. В результате хакеры, используя уязвимости в программном обеспечении, могут похищать личные данные владельцев устройств.

Проекты в России

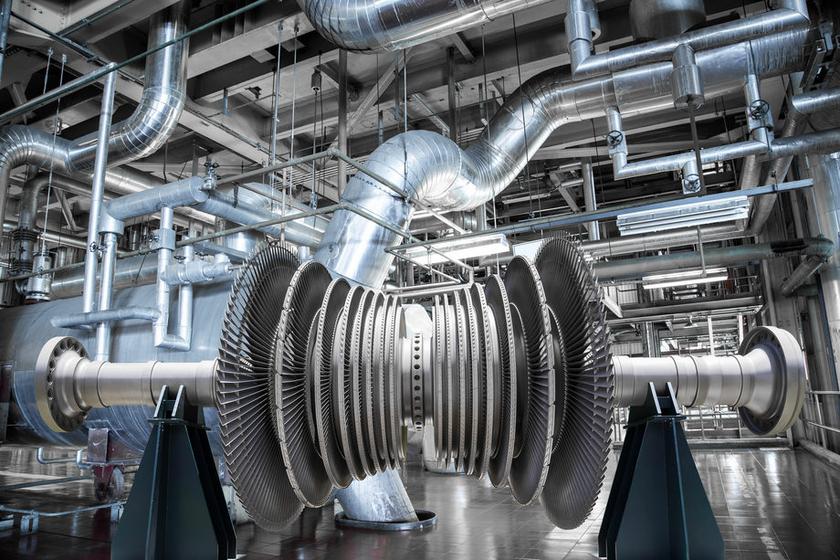
2024: В России представили ИТ-решение, которое выявляет дыры в системах интернета вещей на этапе разработки

В сентябре 2024 года в [России](https://www.tadviser.ru/index.php/%D0%A0%D0%BE%D1%81%D1%81%D0%B8%D1%8F) представили новое ИТ-решение, которое позволяет выявлять уязвимости в системах [интернета вещей](https://www.tadviser.ru/index.php/IoT) еще на этапе разработки. Это инновационное решение разработано учеными [Санкт-Петербургского федерального исследовательского центра РАН (СПб ФИЦ РАН)](https://www.tadviser.ru/index.php/%D0%9A%D0%BE%D0%BC%D0%BF%D0%B0%D0%BD%D0%B8%D1%8F:%D0%A1%D0%B0%D0%BD%D0%BA%D1%82-%D0%9F%D0%B5%D1%82%D0%B5%D1%80%D0%B1%D1%83%D1%80%D0%B3%D1%81%D0%BA%D0%B8%D0%B9_%D1%84%D0%B5%D0%B4%D0%B5%D1%80%D0%B0%D0%BB%D1%8C%D0%BD%D1%8B%D0%B9_%D0%B8%D1%81%D1%81%D0%BB%D0%B5%D0%B4%D0%BE%D0%B2%D0%B0%D1%82%D0%B5%D0%BB%D1%8C%D1%81%D0%BA%D0%B8%D0%B9_%D1%86%D0%B5%D0%BD%D1%82%D1%80_%D0%A0%D0%90%D0%9D_(%D0%A1%D0%9F%D0%B1_%D0%A4%D0%98%D0%A6_%D0%A0%D0%90%D0%9D)) и призвано обеспечить высокий уровень защиты критически важных цифровых систем. Подробнее [здесь](https://www.tadviser.ru/index.php/%D0%9F%D1%80%D0%BE%D0%B4%D1%83%D0%BA%D1%82:%D0%A4%D0%98%D0%A6_%D0%A0%D0%90%D0%9D:_%D0%A1%D0%B5%D1%80%D0%B2%D0%B8%D1%81_%D0%B7%D0%B0%D1%89%D0%B8%D1%82%D1%8B_%D0%B8%D0%BD%D1%82%D0%B5%D1%80%D0%BD%D0%B5%D1%82%D0%B0_%D0%B2%D0%B5%D1%89%D0%B5%D0%B9).

2023: ФСТЭК получит 400 млн рублей на защиту промышленного интернета вещей в России

В конце марта 2023 года стало известно о выделении Федеральной службе по техническому и экспортному контролю ([ФСТЭК](https://www.tadviser.ru/index.php/%D0%9A%D0%BE%D0%BC%D0%BF%D0%B0%D0%BD%D0%B8%D1%8F:%D0%A4%D0%B5%D0%B4%D0%B5%D1%80%D0%B0%D0%BB%D1%8C%D0%BD%D0%B0%D1%8F_%D1%81%D0%BB%D1%83%D0%B6%D0%B1%D0%B0_%D0%BF%D0%BE_%D1%82%D0%B5%D1%85%D0%BD%D0%B8%D1%87%D0%B5%D1%81%D0%BA%D0%BE%D0%BC%D1%83_%D0%B8_%D1%8D%D0%BA%D1%81%D0%BF%D0%BE%D1%80%D1%82%D0%BD%D0%BE%D0%BC%D1%83_%D0%BA%D0%BE%D0%BD%D1%82%D1%80%D0%BE%D0%BB%D1%8E_(%D0%A4%D0%A1%D0%A2%D0%AD%D0%9A_%D0%A0%D0%BE%D1%81%D1%81%D0%B8%D0%B8))) около 400 млн [рублей](https://www.tadviser.ru/index.php/%D0%A1%D1%82%D0%B0%D1%82%D1%8C%D1%8F:%D0%A0%D0%BE%D1%81%D1%81%D0%B8%D0%B9%D1%81%D0%BA%D0%B8%D0%B9_%D1%80%D1%83%D0%B1%D0%BB%D1%8C) создание отечественного ресурса об уязвимостях автоматизированных систем управления технологическими процессами ([АСУ ТП](https://www.tadviser.ru/index.php/%D0%90%D0%A1%D0%A3_%D0%A2%D0%9F)) и [промышленного интернета вещей](https://www.tadviser.ru/index.php/IIoT).

Как пишет [CNews](https://www.tadviser.ru/index.php/CNews) со ссылкой на федеральный проект «[Информационная безопасность](https://www.tadviser.ru/index.php/%D0%98%D0%BD%D1%84%D0%BE%D1%80%D0%BC%D0%B0%D1%86%D0%B8%D0%BE%D0%BD%D0%BD%D0%B0%D1%8F_%D0%B1%D0%B5%D0%B7%D0%BE%D0%BF%D0%B0%D1%81%D0%BD%D0%BE%D1%81%D1%82%D1%8C)», госинициатива предполагает создание исследовательского стенда и банка данных угроз. Предполагается, что новый ресурс работать с критически важными, потенциально опасными и опасными производственными объектами. Целью его создания является информирование об уязвимостях пользователей указанных объектов.



Власти потратят 400 млн руб. на безопасность промышленного интернета вещей

Проект будет реализовываться в несколько этапов. Сначала должен быть проведен анализ перспективных [информационных технологий](https://www.tadviser.ru/index.php/%D0%98%D0%BD%D1%84%D0%BE%D1%80%D0%BC%D0%B0%D1%86%D0%B8%D0%BE%D0%BD%D0%BD%D1%8B%D0%B5_%D1%82%D0%B5%D1%85%D0%BD%D0%BE%D0%BB%D0%BE%D0%B3%D0%B8%D0%B8), планируемых к применению в автоматизированных системах управления производственными и технологическими процессами (АСУ ТП). Далее должен быть создан исследовательский стенд для проведения оценки защищенности перспективных технологий, планируемых к применению в АСУ ТП, и проведена оценка защищенности перспективных технологий, планируемых к применению в АСУ ТП.

Затем должны быть разработаны рекомендации по повышению защищенности информационных технологий, планируемых к применению в АСУ ТП. Должен быть создан раздел банка данных угроз безопасности информации, содержащий сведения о типовых рисках (потенциальных, негативных последствиях) АСУ ТП, об угрозах безопасности АСУ ТП и техниках их реализации, об уязвимостях [программного обеспечения](https://www.tadviser.ru/index.php/%D0%A1%D1%82%D0%B0%D1%82%D1%8C%D1%8F:%D0%9F%D1%80%D0%BE%D0%B3%D1%80%D0%B0%D0%BC%D0%BC%D0%BD%D0%BE%D0%B5_%D0%BE%D0%B1%D0%B5%D1%81%D0%BF%D0%B5%D1%87%D0%B5%D0%BD%D0%B8%D0%B5) АСУ ТП, о мерах [защиты информации](https://www.tadviser.ru/index.php/%D0%97%D0%B0%D1%89%D0%B8%D1%82%D1%8B_%D0%B8%D0%BD%D1%84%D0%BE%D1%80%D0%BC%D0%B0%D1%86%D0%B8%D0%B8) АСУ ТП.

Следующие этапы:

* проведение опытной эксплуатации раздела банка данных угроз безопасности информации;
* принятие его в эксплуатацию;
* создание базы знаний, необходимой специалистам для проведения контроля за обеспечением уровня защищенности АСУ ТП.[[15]](https://www.tadviser.ru/index.php/%D0%A1%D1%82%D0%B0%D1%82%D1%8C%D1%8F:%D0%98%D0%BD%D1%84%D0%BE%D1%80%D0%BC%D0%B0%D1%86%D0%B8%D0%BE%D0%BD%D0%BD%D0%B0%D1%8F_%D0%B1%D0%B5%D0%B7%D0%BE%D0%BF%D0%B0%D1%81%D0%BD%D0%BE%D1%81%D1%82%D1%8C_%D0%B8%D0%BD%D1%82%D0%B5%D1%80%D0%BD%D0%B5%D1%82%D0%B0_%D0%B2%D0%B5%D1%89%D0%B5%D0%B9_(Internet_of_Things)#cite_note-14)