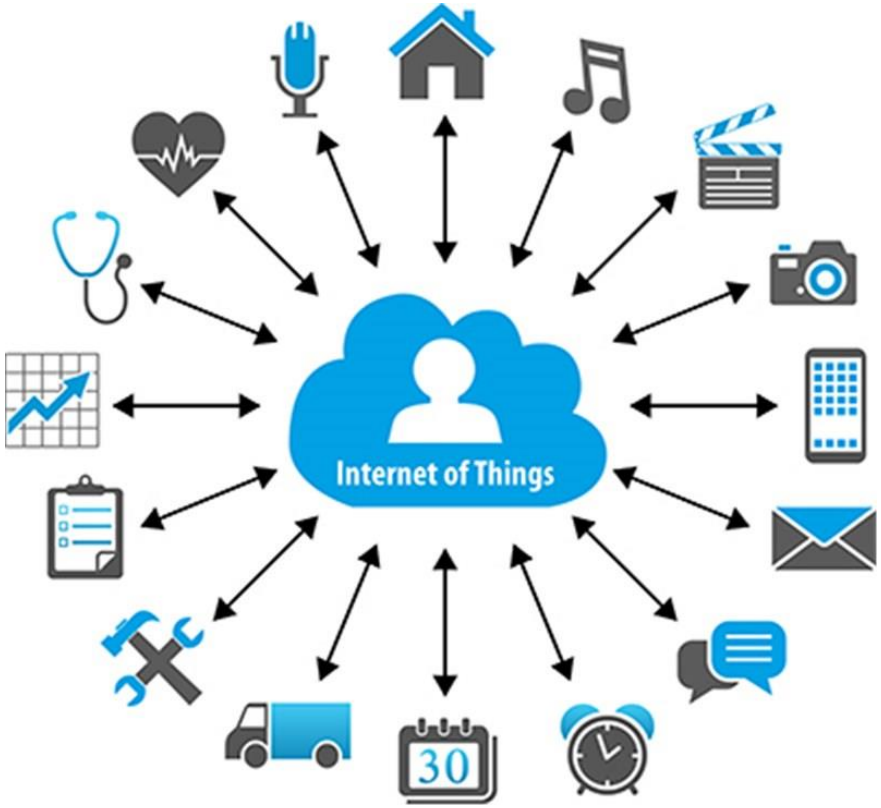
ОМСКИЙ НИИ ПРИБОРОСТРОЕНИЯ
ОНИИП
ДАЛЬНЯЯ РАДИОСВЯЗЬ.
АППАРАТУРА И КОМПЛЕКСЫ

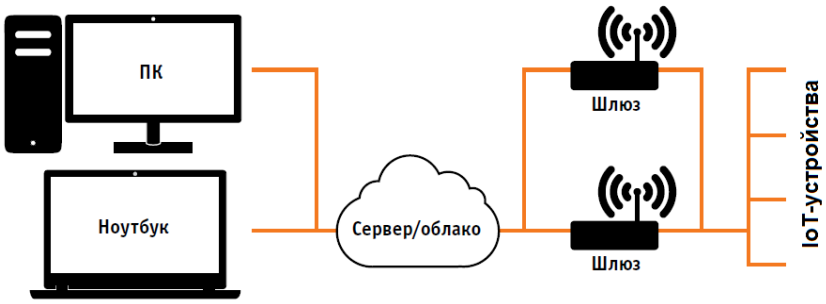
Новый стандарт интернета вещей

НИЛ Кибербезопасности
Шилер А. В., Степанова Е. А.

Докладчик:
Научный сотрудник АО «ОНИИП»
Степанова Елизавета

Применение IoT-устройств





Типовая схема работы IoT

Целевая классификация атак на IoT

{DDoS}

2016 Mirai

2017Hajime

2017Reaper

Брутфорс атаки с перебором паролей

Имена пользователей	Пароли
root	admin
admin	root
test	1234
access	ubnt
DUP root	123456
DUP admin	password
ubnt	12345
oracle	test
postgres	qwerty
pi	raspberry

Low-power Wide-area Network (LPWAN)

- энергоэффективная сеть дальнего радиуса действия

1) LoRaWAN Long Range Wide Area Networks: Semtech, IBM

- собственная модуляция
- открытый сетевой протокол LoRaWAN
- топологии: ячеистая, звезда, точка-точка
- нелицензируемые частоты : 868/915, 433 МГц
- низкое энергопотребление

- невысокая скорость передачи данных 0,3 – 50 кбит/с
- проприетарный чип Semtech

1) LoRaWAN

Безопасность:

- Используются 2 ключа AES-128:
  NwkSKey – ключ идентификации в сети;
  AppSKey – ключ для установления сессии;

- Аутентификация:
  с использованием персональных настроек;
  активация через сервер;

- легко заблокировать каналы базовой станции путем отправки произвольных пакетных данных в большом количестве;

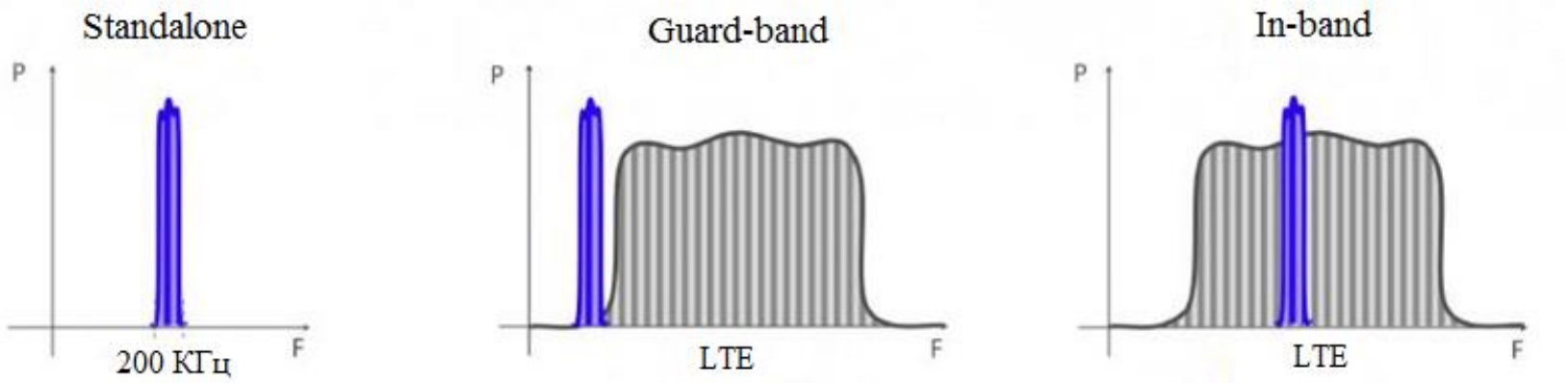
- для каждого устройства необходим свой уникальный ключ.

2) Мобильные сети **NB-IoT**

Narrow band IoT standart: 3GPP

- скорость 20-250 кбит/с
- готовая инфраструктура
- частоты лицензируемые: UL 890-915 DL 935-960 МГц
- невысокая дальность в городе

Варианты реализации NB-IoT



Проект российского стандарта NB-Fi

ТК -194 «Кибер-физические системы»

- Сверхузкополосные сигналы (UNB)
- Топология «звезда»
- Базовые станции типа SDR
- Безлицензионный диапазон 868 МГц
- Радиус действия:
  до 10 км в городе
  до 30 км в сельской местности
- DBPSK
- Полоса 100 Гц, 5000 каналов

Безопасность в NB-Fi

+ Скорость пакетов Downlink = Uplink, быстрое обновление прошивки
+ Шифрование XTEA-256
+ Надежная доставка пакетов Handshake Simple
+ HTTPS/SSL с RSA

- Нет четкой рекомендации по шифрованию
- Защита серверов возлагается на заказчика
- Вопрос доверия к оператору при хранении ключей в облаке открыт

Предлагаемая архитектура безопасности IoT

Защита устройств:
- криптографическая подпись программного кода;
- защита узлов сети.

Защита каналов связи:
- шифрование;
- проверка подлинности устройств.

Аналитика безопасности:
- использование данных телеметрии.

Контроль работы устройств:
- настройка обновлений;
- проверка на наличие уязвимостей.

Стандартизация и сертификация

Выводы

Для эффективной защиты IoT необходимы:

- Разработка и отладка механизмов реагирования на инциденты киберугроз IoT
- Мониторинг IoT сетей и механизмы регулярного обновления прошивки
- Четкие требования к шифрованию
- Вопросы взаимодействия оператора и абонента, хранение ключей шифрования
- Комплексный подход к безопасности