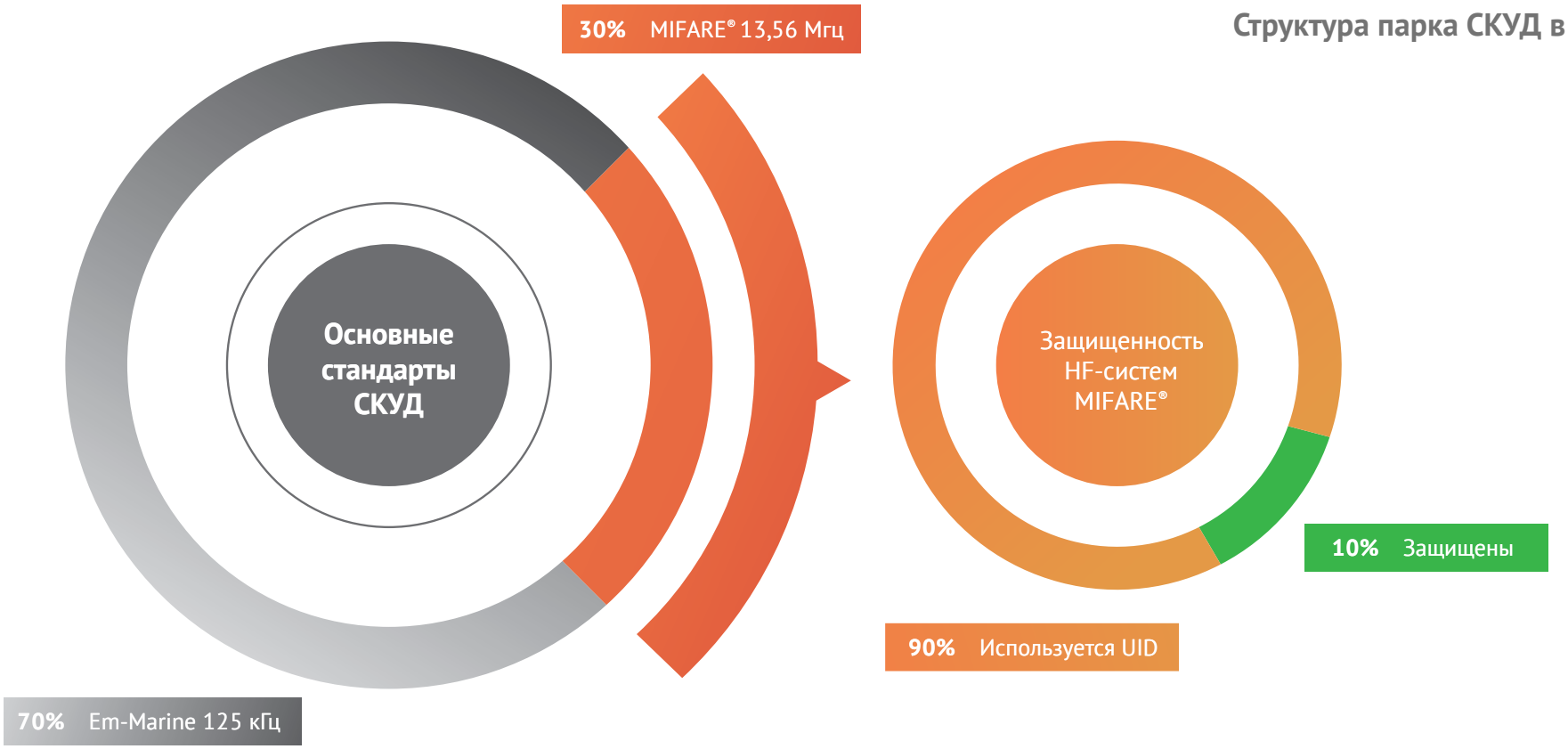
ESMART®

Применение российской криптографии и технологий M2M, IoT для решения проблем безопасности СКУД на объектах КИИ

www.esmart.ru

Безопасен ли современный СКУД?

Для идентификации в 90% случаев используется электронный номер карты



Можно легко сделать копию карты, присвоить ей такой же электронный номер и пройти на объект!

eSMART®

В 90% случаев **5 минут** достаточно, чтобы скопировать пропуск

Стоимость услуги по клонированию карты не более 500 рублей, на любом строительном рынке

В год покупается несколько миллионов новых карт для СКУД

Причины низкой безопасности СКУД

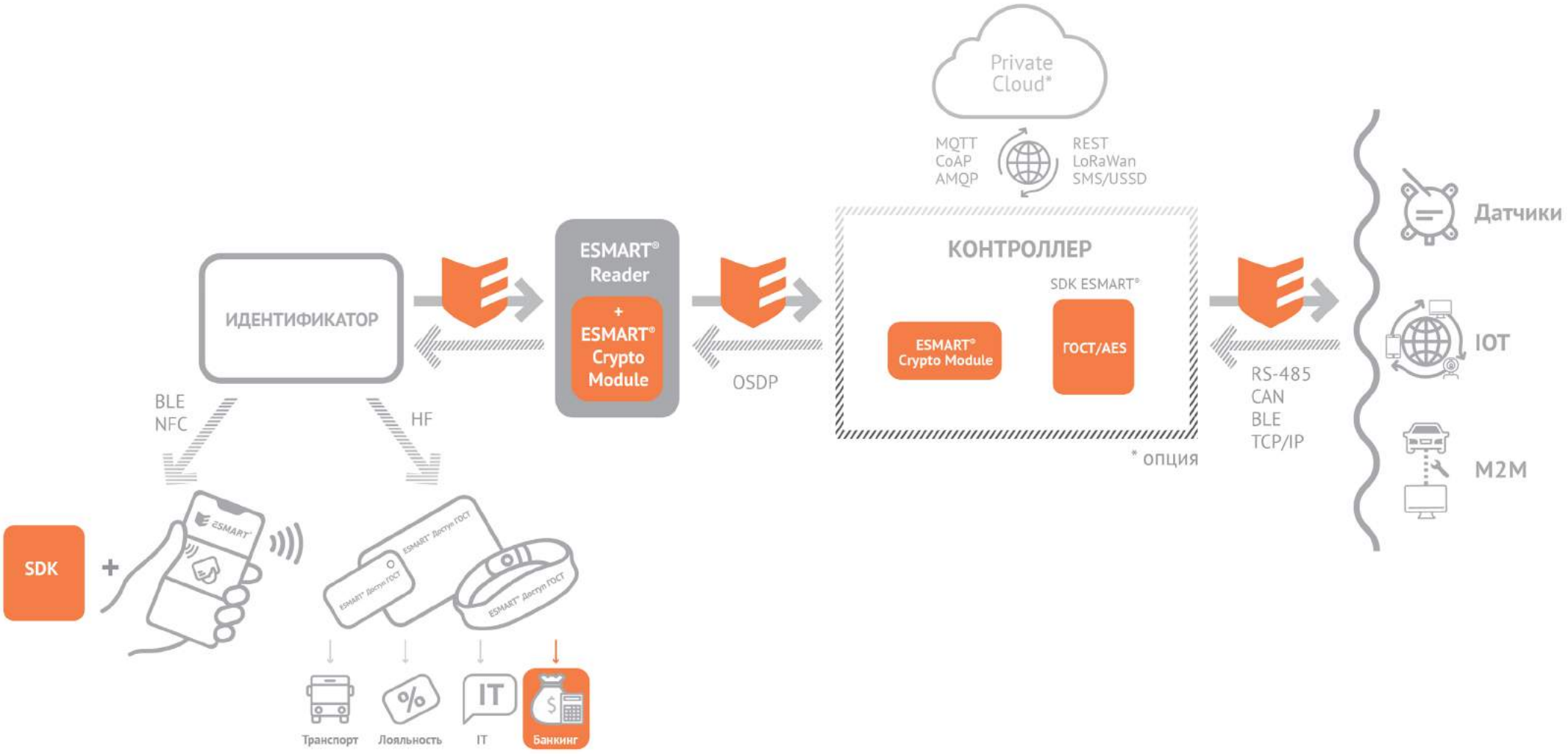
- В СКУД системы устанавливались **5-10 лет назад** и до сих пор эксплуатируются
- Рынок без регулирования насыщается все **более дешёвым оборудованием**
- **Низкий уровень знаний** специалистов рынка СКУД о технологиях смарт-карт

Основная угроза – неправомерное проникновение на объект!

ESMART®

Как обеспечить антитеррористическую защищенность и безопасный доступ?

Состав платформы ESMART® Доступ 2.0



Ключевые приемущества технологии ESMART® Доступ ГОСТ

Безопасность и защита от копирования

- Шифрование AES, ГОСТ-28147-89, ГОСТ 34.12-2015
- Диверсификация ключей шифрования
- Взаимная аутентификация
- Конфиденциальность и целостность данных
- Защита от replay атак

Мобильная идентификация

- Поддержка iOS и Android
- Работа по BLE и NFC
- Защищенный обмен
- Проверка подлинности

Защищенный протокол для передачи данных от считывателя к контроллеру

- OSDP v2
- SCP (Secure Channel Protocol)

Физический доступ Логический доступ

ESMART®

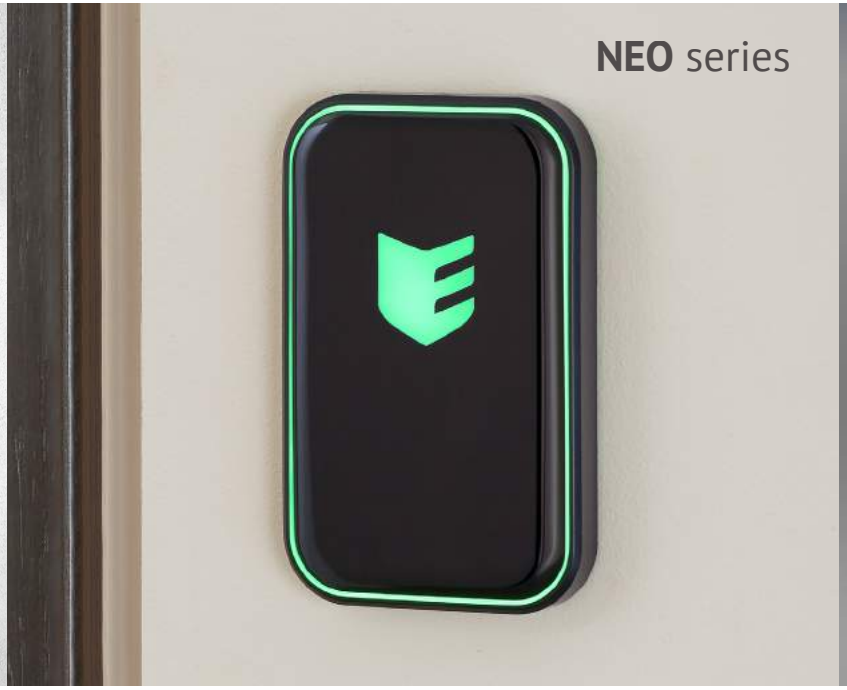
Сертификация

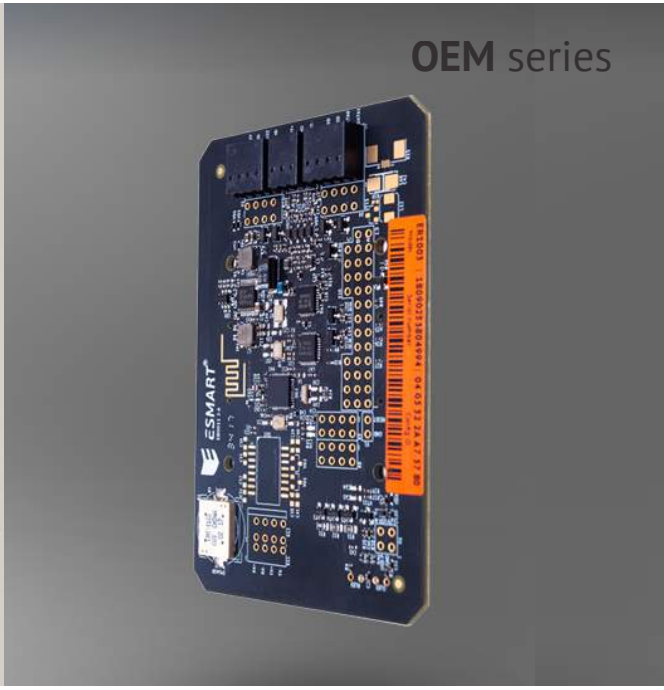
Технология **ESMART® Доступ ГОСТ** построена на СКЗИ, сертифицированном в ФСБ по классу КС3 - Сертификат №СФ/124-3189

Соответствует требованиям

- ГОСТ 28147-89
- ГОСТ Р 34.11-94
- ГОСТ Р 34.10-2001
- ГОСТ Р 34.11-2012
- ГОСТ Р 34.10-2012

Настенные считыватели ESMART® Reader





Инновации ESMART® Reader ГОСТ

- **Шифрование по российскому стандарту ГОСТ** на базе отечественного криптопроцессора MIK51SC72DV6, производство – Микрон
- **Интеграция** технологии СКУД ESMART® Доступ с технологией информационной безопасности ESMART® CryptoModule
- **Возможность встраивания технологии безопасности ESMART® CryptoModule** (шифрование ГОСТ, AES) в любые контроллеры: СКУД, IoT, работа с датчиками

Пассивные IoT-устройства:
RFID-идентификаторы ESMART® Доступ ГОСТ

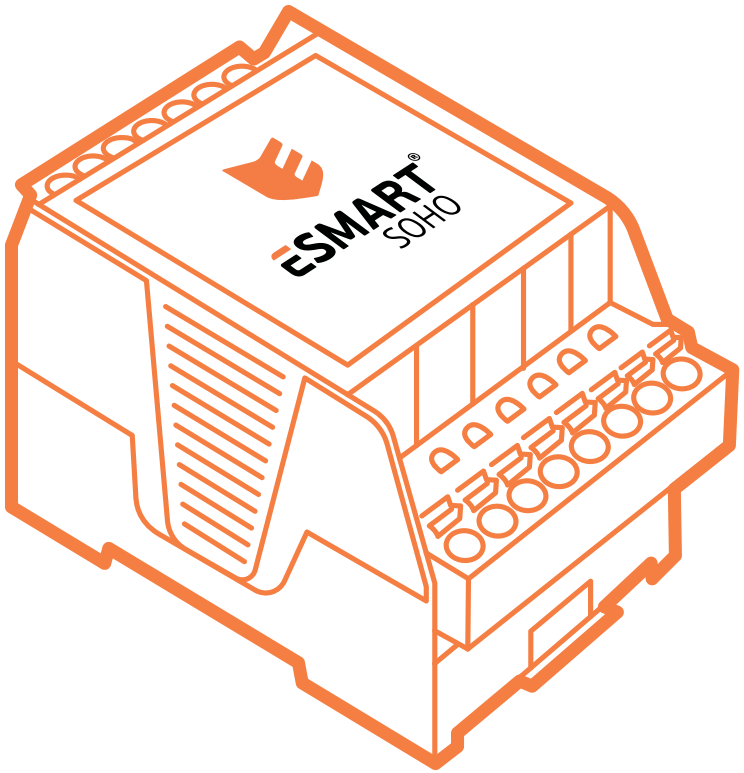
1. Безопасность.
Защита от копирования по воздуху, клонирования и взлома:
• использование ГОСТ шифрования при обмене данными между считывателем и идентификатором
• диверсификация ключа шифрования
• MAC подпись идентификатора
• защита от replay атак

2. Аппаратное ГОСТ шифрование на базе отечественной микросхемы MIK51SC72DV6
Производитель – Микрон

3. Конвергенция доступов
• двухфакторная аутентификация
• электронная подпись
• Доступ СКУД

ESMART®

Ваш контроллер IoT с технологией ESMART® CryptoModule



- По данным ФГУП «НИИР», сейчас на рынке 80% IoT использует для передачи сети близкого радиуса действия.
- Наша идея - реализовать возможность сбора данные с таких устройств на контроллере и передача далее в уже защищенном виде
- Контроллер и все устройства IoT, СКУД оснащаются модулями ESMART® Crypto Module с аппаратным шифрованием ГОСТ 28147-89 или ГОСТ 34.12-2015
- Используется отечественная микросхема MIK51SC72DV6, производство – Микрон
- Обеспечивается взаимодействие с M2M системами, пассивными или активными датчиками: ModBus, CAN, BLE, TCP/IP
- Поддержка протоколов IoT: MQTT, CoAP, AMQO, REST
- Шифрованием и подпись данных на прикладном уровне по ГОСТ-алгоритмам
- Упаковка структурированной информации в TLV, CBOR

Решение соответствует ГОСТ Р 51241-2008 и реализует меры защиты из приказа ФСТЭК России №17

Защита IoT с технологией ESMART® CryptoModule

- Шифрование применяется на прикладном уровне, поэтому нет требований использовать шифрование в транспорте, менять симки, заботиться о безопасном хранении ключей в SIM.

- Транспорт может быть любой в том числе открытые каналы: GSM Data, SMS, USSD, WiFi, ZigBee, LoRaWAN. Зачастую каналы можно комбинировать, использовать несколько транспортных протоколов одновременно для ускорения.

- Все это позволяет не требовать от своих устройств IoT какой-либо безопасности, если они находятся в контролируемой зоне.

- Прикладной уровень шифрования позволяет за счет упаковки структурированной информации в TLV, CBOR подстраиваться под особенности протокола и размер MTU, что особенно критично для LPWA, NB-IoT. При этом обеспечивается аутентификация и конфиденциальность каждой посылки.

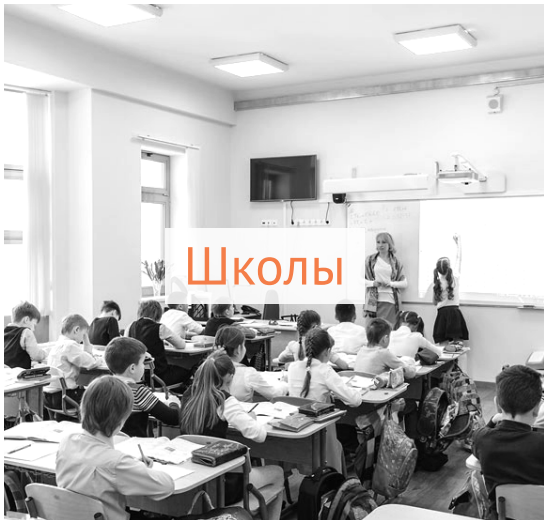
- Возможность использование сигнальной GSM сети (SMS/USSD) позволяет обеспечить почти 10-кратную экономию потребления электричества IoT- устройствами.

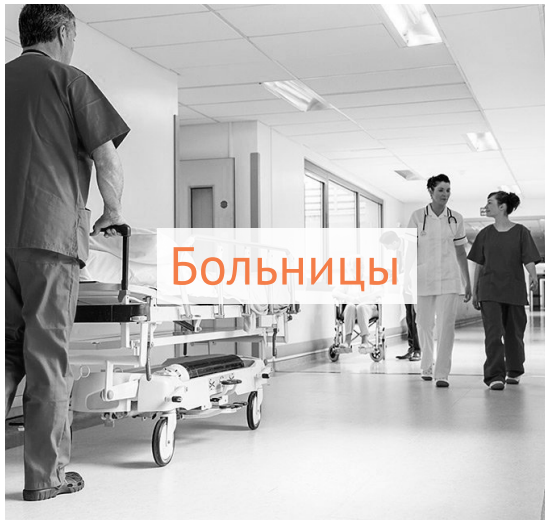
Платформа ESMART® Доступ не только для безопасного СКУД, но и защиты любых систем IoT, M2M:

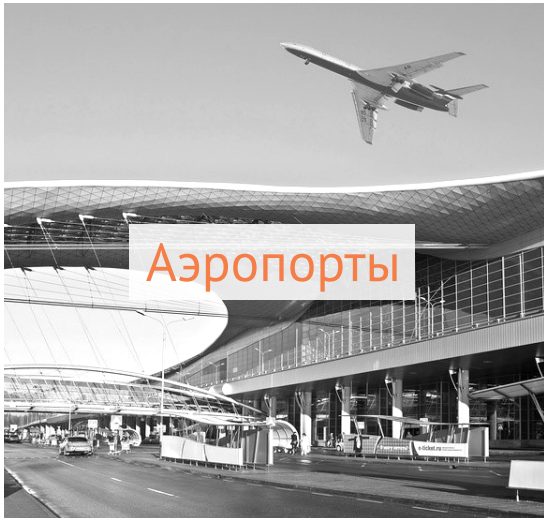
- **Умный Город**
- **Умное предприятие (Smart Plant)**
- **Умный дом, вкл. АСКУЭ в ЖКХ**
- **Умные решения для различных территориально распределенных объектов:** трубопроводы, железные дороги, автодороги, электросети

и многое другое ....

Сферы применения







О Группе компаний ISBC

17 5000

17 ЛЕТ УСПЕШНОГО РОСТА

УСПЕШНО РЕАЛИЗОВАНО БОЛЕЕ 5 000 ПРОЕКТОВ В ОБЛАСТИ RFID И ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ

250

В НАШЕЙ КОМАНДЕ 250 СОТРУДНИКОВ

50 000 000

БОЛЕЕ 50 000 000 РОССИЯН ПОЛЬЗУЮТСЯ НАШЕЙ ПРОДУКЦИЕЙ

10000

НАМ ДОВЕРЯЮТ БОЛЕЕ 10 000 КОРПОРАТИВНЫХ КЛИЕНТОВ

Спасибо за внимание!