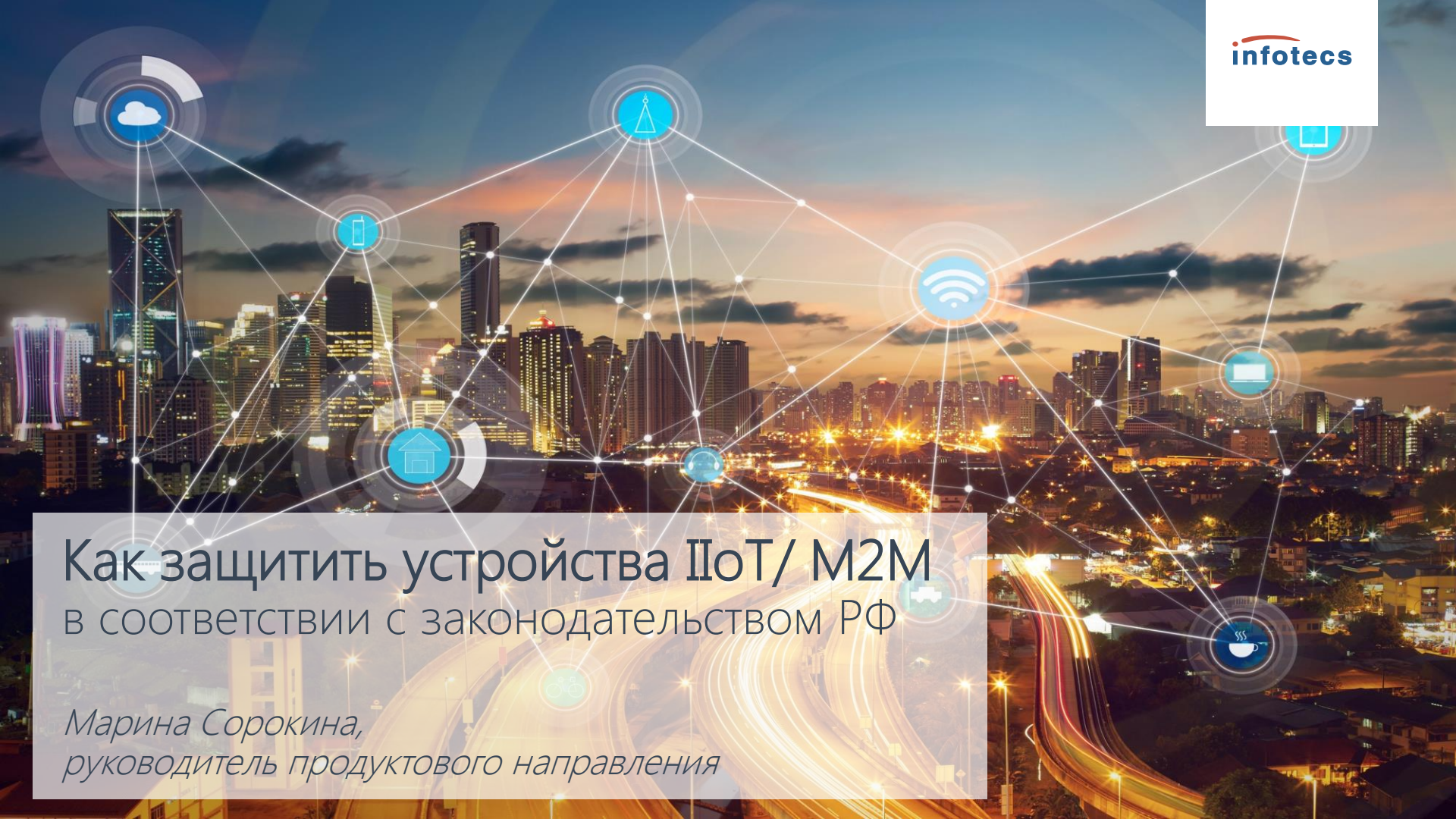


Как защитить устройства IIoT/ M2M
в соответствии с законодательством РФ

Марина Сорокина,
руководитель продуктового направления

Рынок IIoT/M2M сегодня

Мировой рынок IIoT

$ 646 млрд.

Российский рынок IIoT

93 млрд. руб.

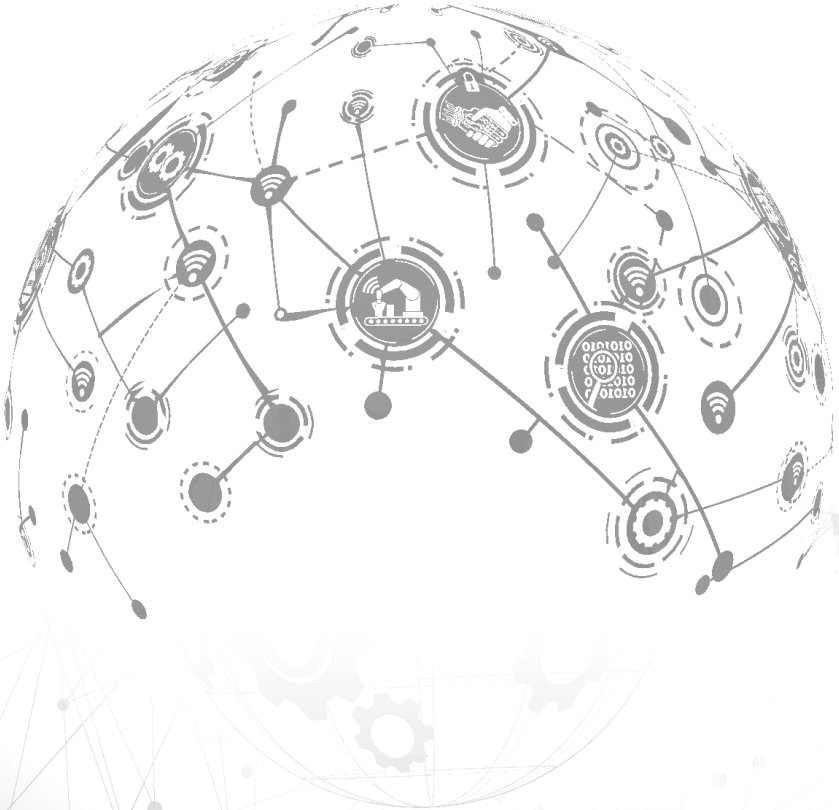
Количество соединений в мире

407 млн.

Подключенные устройства

15,9 млн.

Рынок IIoT/M2M к 2023 году



Годовой рост мирового рынка

14,36%

Годовой рост РФ рынка

18 - 20%

Мировой рынок

$ 700 млрд.

Российский рынок

270 млрд. руб

Информационная безопасность IIoT/M2M-систем

60% протоколов IIoT/ M2M не имеют встроенных механизмов защиты

80 % протоколов IIoT/ M2M беспроводные

26 % компаний внедрило криптографическую защиту в свои устройства

MIRAI - самая масштабная DDoS-атака в мире (2016 г) была проедена с использованием IIoT устройств

60% IIoT устройств используется для DDoS-атак

$13,2 млн теряют компании в энергетической и коммунальной отраслях ежегодно из-за атак на IIoT-устройства

Основные атаки на IIoT/M2M

Навязывание устаревших данных (REPLAY ATTACK)

Подмена команд (COMMAND INJECTION)

Подача команды аварийного останова

Подмена IIoT/M2M устройств

«Перепрошивка» IIoT/M2M устройств

DDOS-атака для отказа в обслуживании

Архитектура и особенности

- Отсутствие периметра
- Малые вычислительные ресурсы устройств
- Работа от «батарейки»
- Чувствительность к оверхеду
- Территориально-распределенное размещение
- Множество не стандартизированных протоколов
- Возможность физического доступа

Рекомендованные механизмы защиты

Средства защиты информации для IIoT/M2M

Встраиваемые средства

"Security by design"

Наложенные средства

Устройства

IIoT-шлюз

Облако

Сторонние приложения

Мировая практика по защите устройств IIoT/ M2M

Для устройств, которые технически позволяют*

IIoT/ M2M
Устройства

- TLS, DTLS
- Защищенные протоколы (LoRA, OPC UA)
- Библиотеки для аутентификации, доверенной загрузки, белые списки

- Криптографические библиотеки
- TPM, HSM, Secure Element
- Чипы с криптографией

Можно ли защитить устройства IIoT/ M2M в соответствии с требованиями РФ сегодня?

Организационные моменты

	Встраиваемые средства	Security by design
IIoT/M2M устройства являются СКЗИ КС1-КС3	+/-	+
Разработчик IIoT/M2M устройств должен иметь лицензию ФСБ Россия	+ (создание системы с СКЗИ)	+ (разработка)
Все участники цепочки поставки должны иметь лицензию ФСБ Россия	+ (распространение)	+ (распространение)
Обслуживать устройства должны назначенные лица	+	+

Можно ли защитить устройства IIoT/ M2M в соответствии с требованиями РФ сегодня?

Технические аспекты

- Большой оверхед криптографических протоколов
- Не учтены требования доступности
- Нет сертификатов на устройства
- Необходимость частой смены ключевой информации
- Высокие ресурсные требования, в том числе и по потребляемой мощности
- Долгое восстановление после спящего режима и при выключения

Можно ли защитить устройства IIoT/ M2M в соответствии с требованиями РФ сегодня?

Бизнесу проще не использовать средства защиты в IIoT/M2M- системах, чем выполнять требования

Высокая стоимость устройств

Длительный процесс разработки новых устройств

Высокая стоимость внедрения

Высокая стоимость эксплуатации

Industrial Key Infrastructure

Инфраструктура индустриальных ключей INDUSTRIAL KEY INFRASTRUCTURE (IKI) – набор средств, служб и компонентов, в совокупности используемых для поддержки криптозадач IIoT/M2M-систем

Методологические и организационные принципы IKI

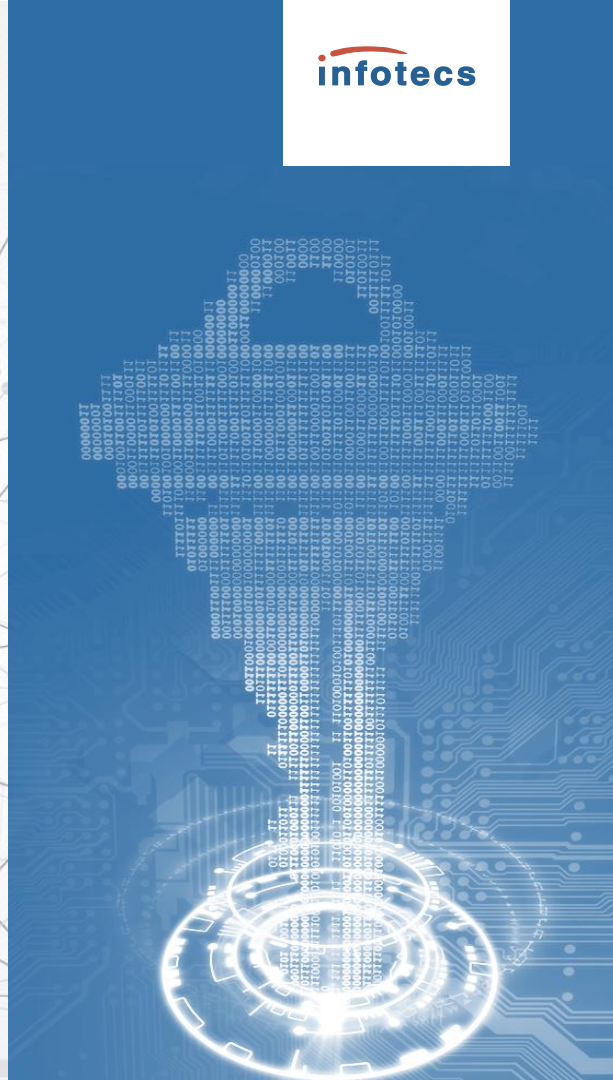
- Требования к разработке, производству, реализации и эксплуатации для IIoT/M2M-устройств с криптографией
  - Упрощение схемы распространения устройств (исключение учета при внедрений определенных технических решений)
  - Механизмы дистанционного ввода в эксплуатацию
  - Пересмотренные требования к обслуживанию и размещению
- Декларация вместо сертификации

Технические принципы IKI

- Специальные криптографические протоколы:
  - Малый объем накладных расходов
  - Обеспечение целостности и опциональная конфиденциальность
  - Отсутствие сессионности
  - Работа с IIoT-протоколами с принципами работы «подписочная модель» и multicast
- Механизмы обеспечения доступности
- Переход на легкоресурсную криптографию

Криптографические принципы IKI

- Специальные требования к ключевой информации:
  - Длинный срок действия ключей
  - Сертификаты для устройств
  - Короткие сертификаты
  - Механизмы работы со списком отозванных сертификатов
  - «Облачный» ДСЧ
- Требования к индустриальному УЦ
  - Выпуск сертификатов для устройств
  - Автоматический выпуск сертификатов на основании серийных номеров
- Правила взаимодействия с PKI



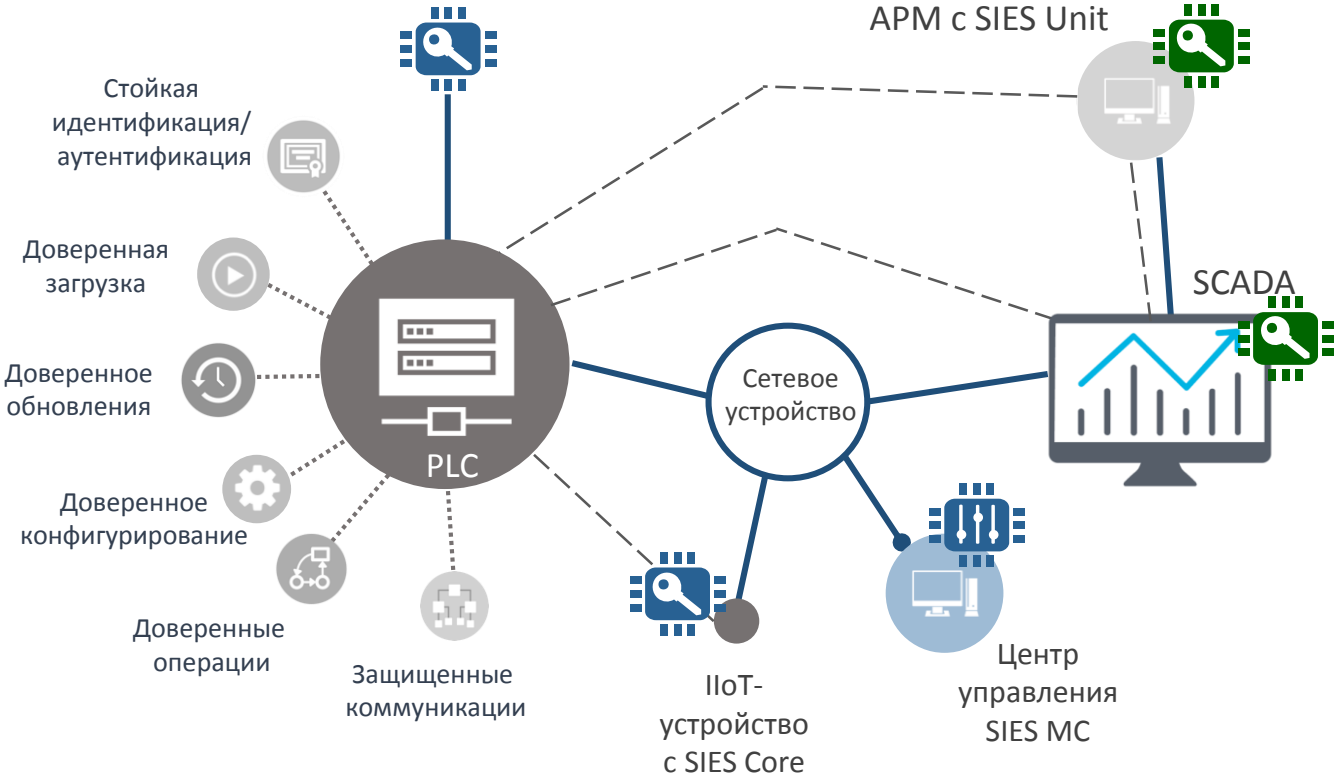
Предпринятые шаги в рамках IKI

CRISP 1.0 – бессесионный протокол защищенной передачи данных для индустриальных систем, M2M и IoT/IIoT коммуникаций; разработан в рамках РГ «Криптографические механизмы для M2M и индустриальных сетей» ТК26

Требования к разработке, производству, реализации и эксплуатации для IIoT/M2M-устройств с криптографией – заложены в план работ РГ «Криптографические механизмы для M2M и индустриальных сетей» ТК26

Разработка решения ViPNet SIES – комплекс встраиваемых продуктов для защиты IIoT/M2M-устройства. Позволит уже сейчас с одной стороны осознать разработчикам IIoT/M2M-устройств трудности, а с другой реализовывать решения согласно требованиям РФ

VIPNet SIES - встраиваемое решение для защиты IIoT/M2M устройств



- ViPNet SIES Core
- ViPNet SIES Unit
- ViPNet SIES MC

ViPNet SIES - это интегрируемые в IIoT/M2M устройства, предоставляющие криптографический сервис, на основе которого эти устройства строят свои сценарии безопасности.

IoBT - Интернет больших вещей

- Дополнительная стоимость ПАК
- Низкая энергоэффективность
- Достаточно большие размеры

- Сертификация как законченного СКЗИ класса КС1 и КС3
- Не нужно сертифицировать как СКЗИ каждое IIoT/M2M-устройство
- Централизованное удаленное управление ключами
- Реализован протокол CRISP
- Отсутствие существенного влияния на срок вывода IIoT/M2M- устройств на рынок

Вместо вывода

Для того, чтобы ИБ из препятствий к распространению IIoT/M2M-систем превратилась в драйвер, нужны совместные активные действия разработчиков устройств, владельцев инфраструктуры, криптографического сообщества и регуляторов рынка.


infotecs
Спасибо за внимание!