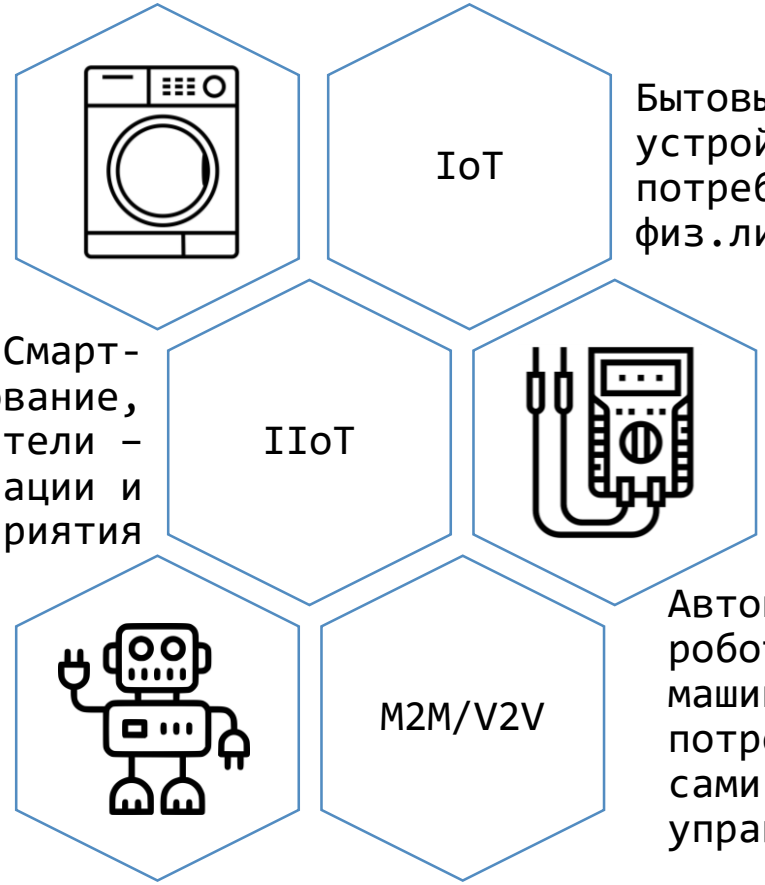
X симпозиум
«Современные тенденции в криптографии» CTCrypt 2021

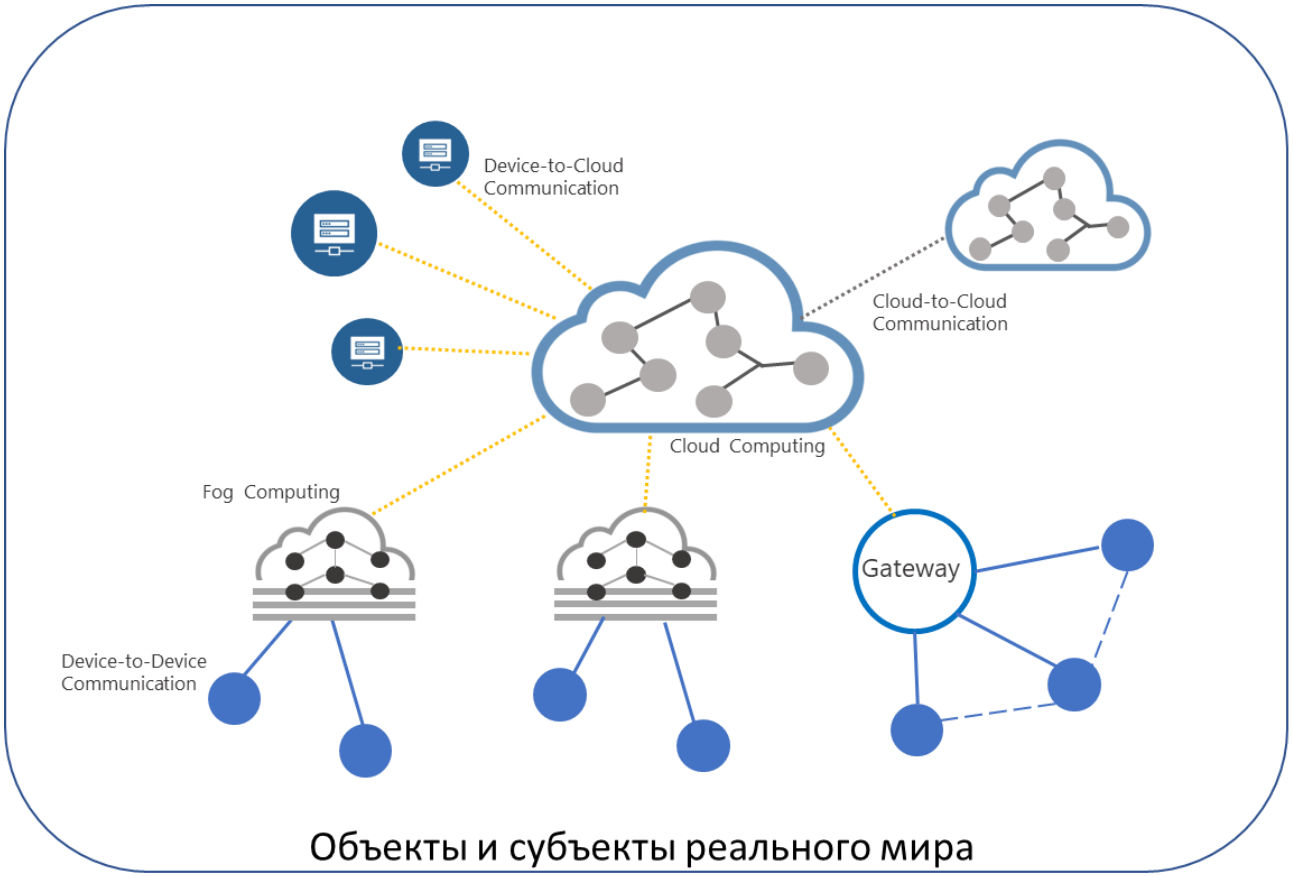
Криптография в Интернете-вещей
Учимся говорить на одном языке

Дмитрий Гусев
Зам.генерального директора АО «ИнфоТеКС», к.т.н.

Что мы понимаем под Интернетом-вещей



Архитектурные особенности Интернета-вещей



Интернет-вещей через свои конечные устройства взаимодействует с объектами и субъектами реального мира

Риски:

- Материальные
- Экономические
- Политические
- Жизнь и здоровье
- Социальные

Общие особенности устройств Интернета-вещей

- Большой диапазон объемов информационного обмена (от десятков байт в сутки до мегабайт в секунды) и допустимых задержек (от десятков наносекунд до минут)
- Оптимизированные вычислительные ресурсы
- Специализированное ПО (firmware), часто без ОС
- Автономное питание
- Многообразие протоколов и каналов связи (как обычных, так и специализированных), в т.ч. нестандартизованных
- Исполнения для работы в сложных условиях
- Малообслуживаемые или необслуживаемые условия работы
- Емкость отдельной логической сети может достигать миллионов устройств
- Жизненный цикл устройств (разработка-внедрение-эксплуатация-вывод из эксплуатации) может быть от года до десятков лет
- Разнообразие отраслевых стандартов и условий оценки соответствия

Особенности устройств Интернета-вещей и безопасность

РУТОКЕН

- Неопределенность периметра безопасности
- Жесткие требования по стоимости для массовых устройств, которые не дают добавить защитные механизмы
- Слабые возможности для реализации криптографии у многих аппаратных платформ
- Сложности защиты прошивок дешевых микроконтроллеров применяемых устройствах IoT, неумение разработчиков пользоваться даже штатными возможностями
- В IoT много устройств с серьезными требованиями к энергопотреблению:
  - спящие режимы: sleep, deep sleep
  - быстрое пробуждение, особенно из режима глубокого сна
  - адаптированные механизмы инициализации криптографических возможностей
- Достаточно закрытое комьюнити компаний умеющих разрабатывать прошивки для защищенных микроконтроллеров

От чего, как и что защищаем

Основные виды угроз

- Несанкционированный доступ к данным
- Перехват управления
  - Навязывание команд
  - Выведения из строя/остановка устройств
- Подмена устройств
  - Передача некорректных данных
  - Дестабилизация работы сети устройств
- Перепрошивка устройств
  - Организация ботнетов
  - Воздействие на объект управления

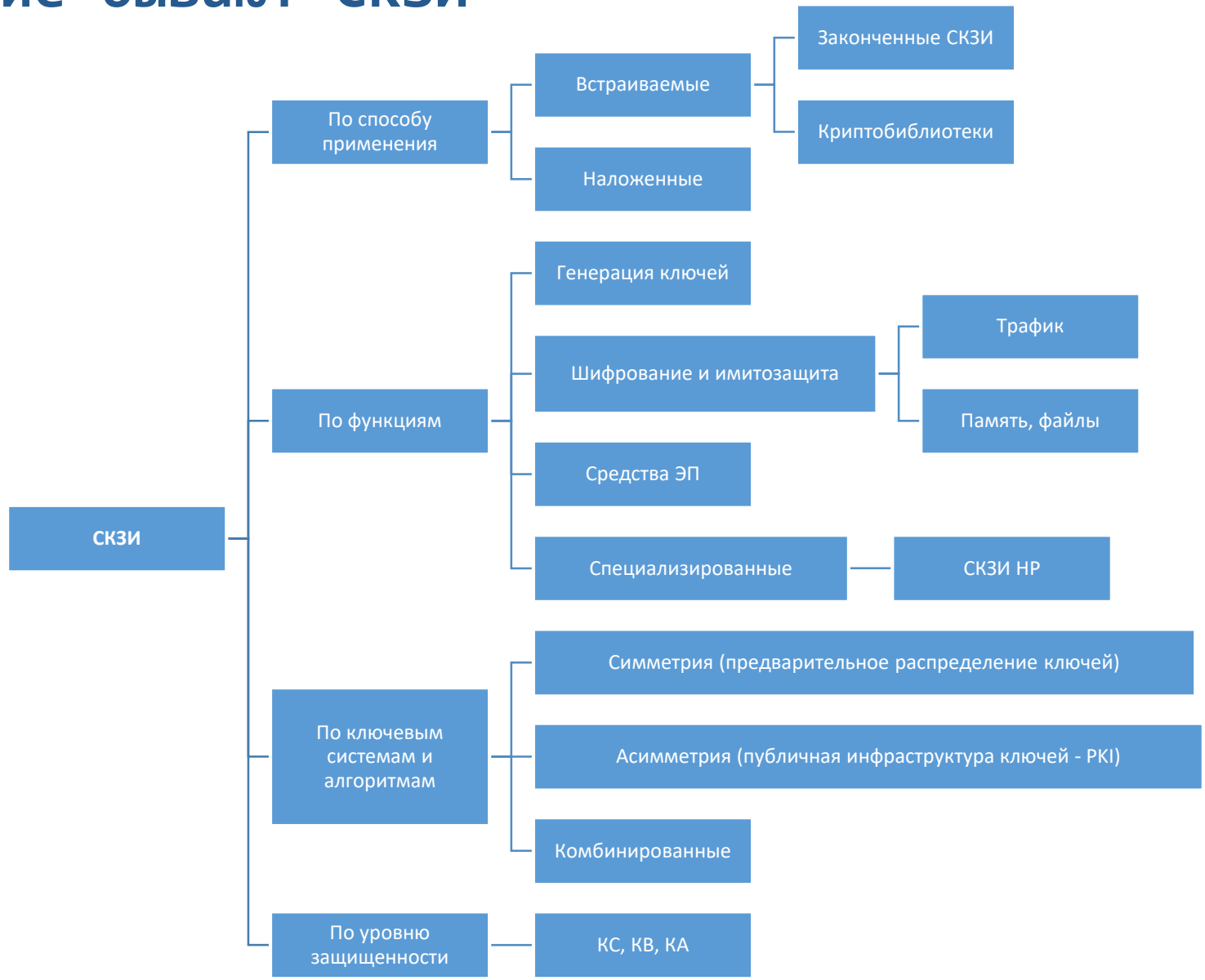
Возможности криптографии

- Целостность
- Конфиденциальность
- Аутентичность

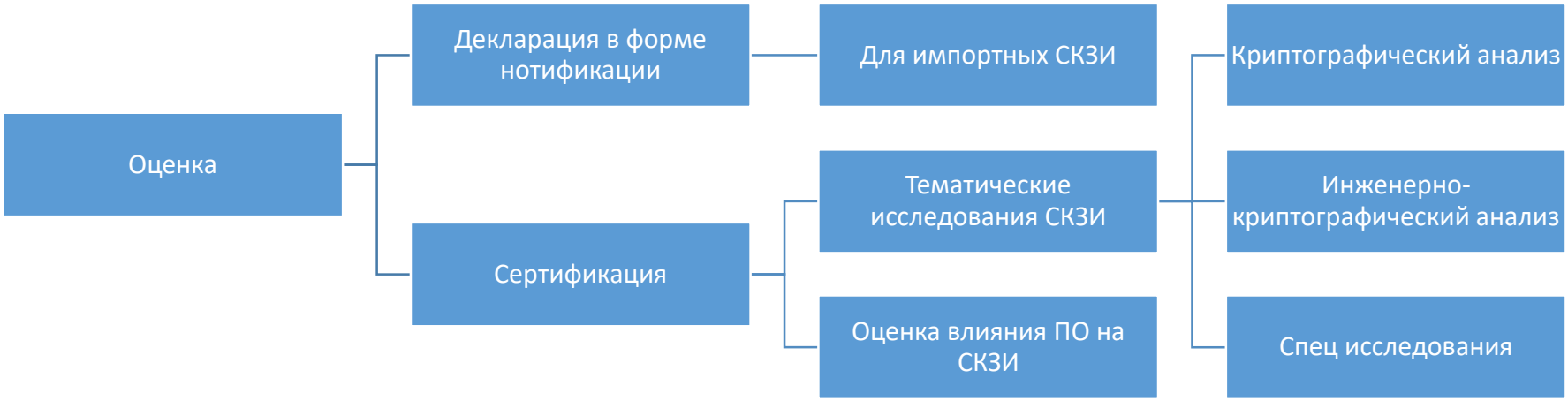
Объекты защиты

- Данные
- Команды управления и телеметрия
- Каналы связи (протоколы разных уровней OSI)
- Прошивки/ПО управления

Какие бывают СКЗИ



Оценка соответствия СКЗИ и ПО с СКЗИ



Типичные вопросы и заблуждения

- У нас свой протокол обмена/своя ОС/свой модем, хакеры их не взломают…
- У нас все данные открытые, зачем их защищать?
- Дайте нам библиотеку для шифрования, мы сами все встроим
- У нас уже используется шифрование на встроенном AES, достаточно будет заменить его ГОСТом?
- Мы собираемся делать свое устройство на отечественном чипе с аппаратным ГОСТом, зачем нам ваше СКЗИ?
- Зачем нам сертификация, если мы собираемся использовать сертифицированные криптобиблиотеки?
- Почему нельзя сразу зашить в устройство все ключи и не мучиться с системами управления ключами?
- Если все российские СКЗИ сертифицированы, то они же должны быть совместимы?

Криптографы работают (рекомендации ТК26)

- Р 1323565.1.034–2020 «Информационная технология. Криптографическая защита информации. Протокол безопасности сетевого уровня» (IPLir)
- Р 1323565.1.032-2020 «Информационная технология. Криптографическая защита информации. Использование российских криптографических механизмов для реализации обмена данными по протоколу DLMS» (СПОДЭС)
- Р 1323565.1.029–2019 «Информационная технология. Криптографическая защита информации. Протокол защищенного обмена для индустриальных систем» (CRISP 1.0)
- Р 1323565.1.028–2019 «Информационная технология. Криптографическая защита информации. Криптографические механизмы защищенного взаимодействия контрольных и измерительных устройств»
- Р 1323565.1.018-2018 «Информационная технология. Криптографическая защита информации. Криптографические механизмы аутентификации в контрольных устройствах для автотранспорта»

Вопросы для круглого стола

1. Нужны ли рынку Интернета вещей специализированные криптоалгоритмы/криптопротоколы и СКЗИ или достаточно уже существующих продуктов и решений для обычных ИТ/ИБ?

2. Требуется ли специальное регулирование вопросов разработки и эксплуатации СКЗИ для Интернета-вещей?

3. Встраивание криптографии VS. практики разработки безопасного ПО?

4. Возможно ли и в какой перспективе такое же прозрачное применение криптографии российскими разработчиками устройств и систем Интернета вещей, как с этим обстоит у их иностранных коллег?*

* На зарубежном рынке существует не только огромное число различных микроконтроллеров/процессоров с аппаратной криптой на борту, но и множество поддерживающих их ОС, систем разработки и управления. Все это делает задачу использования криптографии для зарубежных разработчиками простой и прозрачной для разработчика устройств Интернета-вещей

Спасибо за внимание!

Подписывайтесь на наши соцсети

@infotecs.ru

@vpninfotecs

@InfoTeCS_Moscow