

СКЗИ: лицензирование, сертификация, оценка влияния

О докладчике



Петренко Сергей

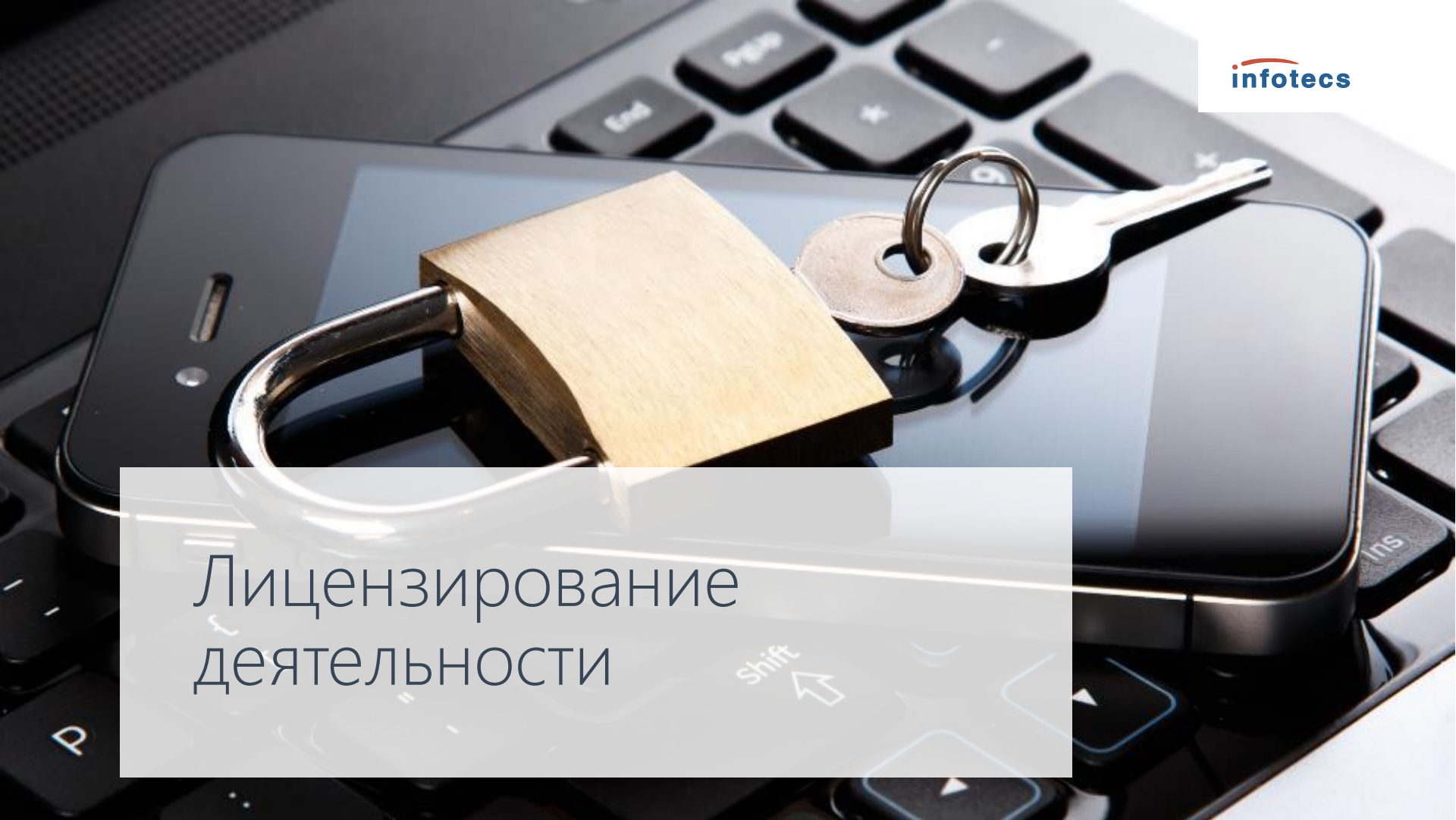
- Руководитель продуктового направления криптографических библиотек ОАО «ИнфоТеКС»
- Эксперт ПК 3 «Криптографические алгоритмы и механизмы в национальной платёжной системе Российской Федерации» Технического комитета «Криптографическая защита информации» (ТК 26)
- Руководитель рабочей группы «Криптографические механизмы для M2M и индустриальных систем» ПК 4 ТК 26

©2017, ОАО «ИнфоТеКС».

Структура доклада



©2017, ОАО «ИнфоТеКС».



Лицензирование деятельности

ФЗ "О лицензировании отдельных видов деятельности"



Постановление Правительства РФ от 16.04.2012 **N 313** (ред. от 18.05.2017) «Об утверждении Положения о лицензировании деятельности по разработке, производству …»

©2017, ОАО «ИнфоТеКС».

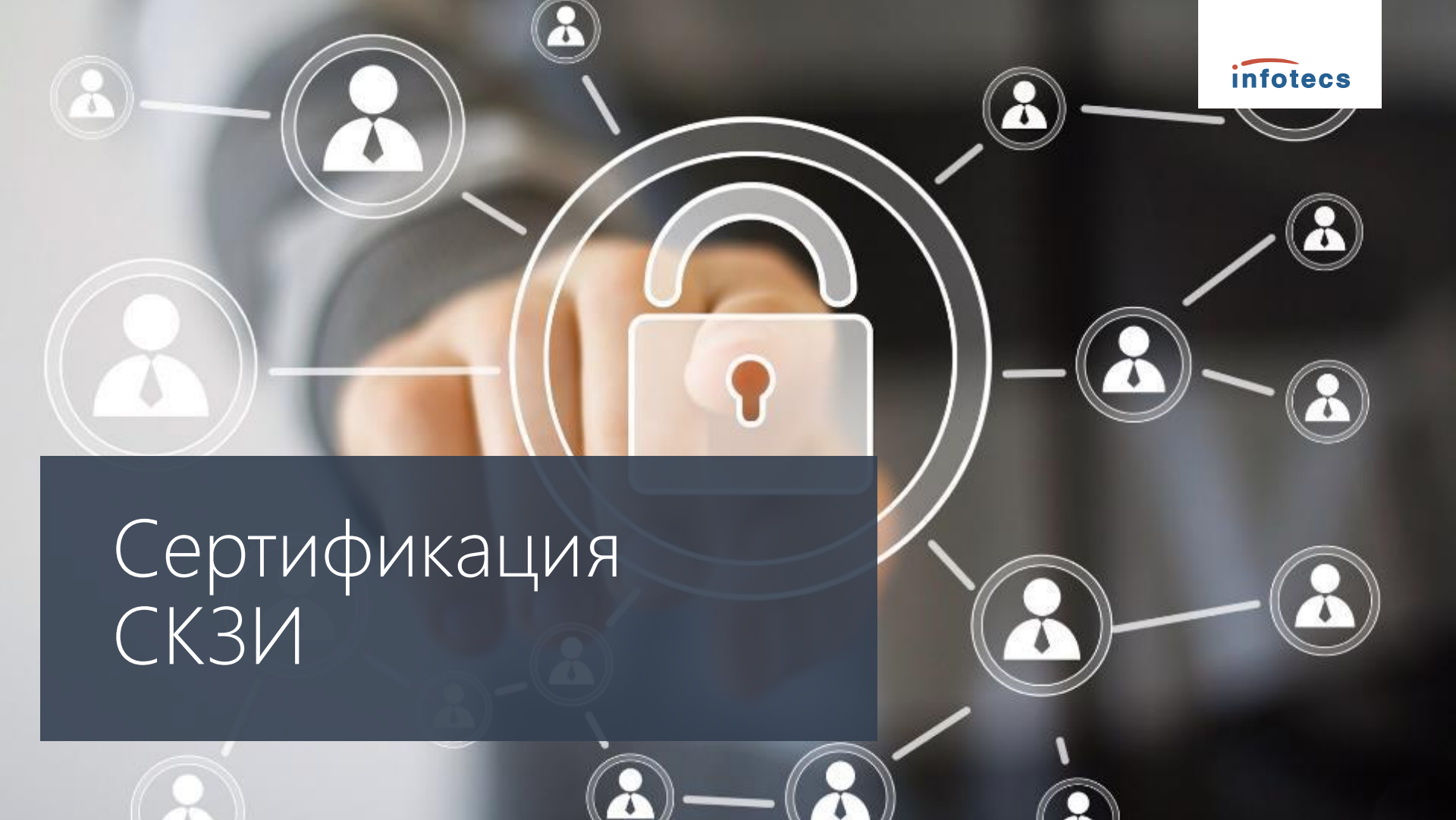
Требования к соискателю

- Специалисты в штате
- Помещения
- Оборудование и ПО



Все можно получить «под ключ»

©2017, ОАО «ИнфоТеКС».



Сертификация СКЗИ

ТЗ (на НИР или ОКР)



Варианты

- По заказу потребителя
- По инициативе разработчика

Согласовывается с регулятором

©2017, ОАО «ИнфоТеКС».

Требования к СКЗИ

Существуют

- «Открытые» на сайте tc26.ru
- «Закрытые» в РСО у лицензиатов



©2017, ОАО «ИнфоТеКС».

Криптографические функции



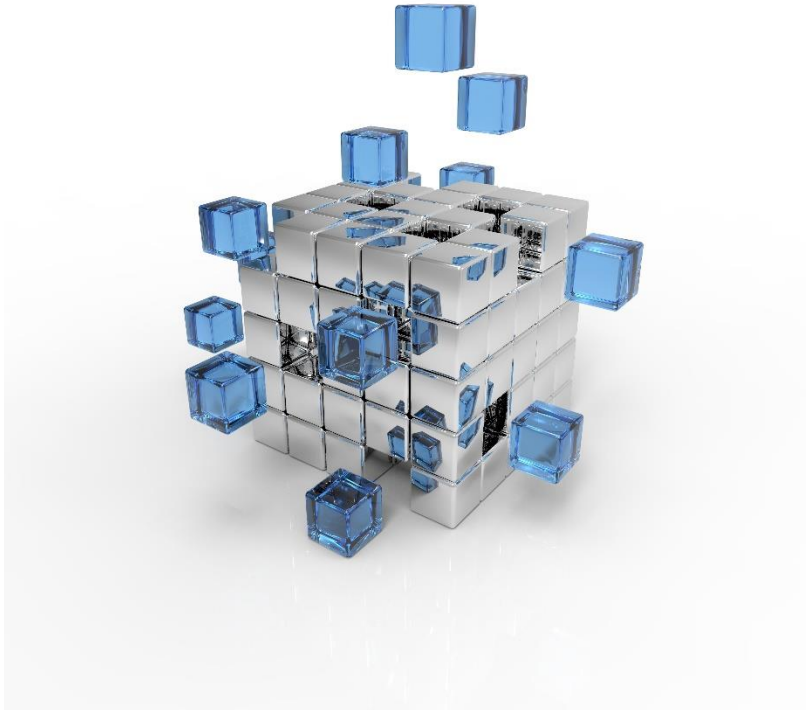
- выработка ПСЧ
- зашифрование/расшифрование
- имитозащита (контроль целостности)
- создание электронной подписи
- проверка электронной подписи
- создание ключа ЭП и ключа проверки ЭП
- изготовление ключевых документов
- передача КИ по каналам связи
- аутентификация

©2017, ОАО «ИнфоТеКС».

Криптографические механизмы

Это

- Алгоритмы (ГОСТы)
- Протоколы (IPSec, TLS)
- Схемы (выработка общего ключа)

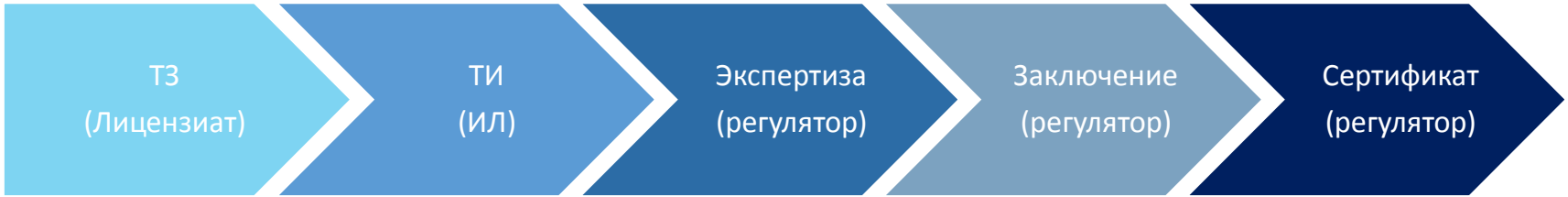


©2017, ОАО «ИнфоТеКС».

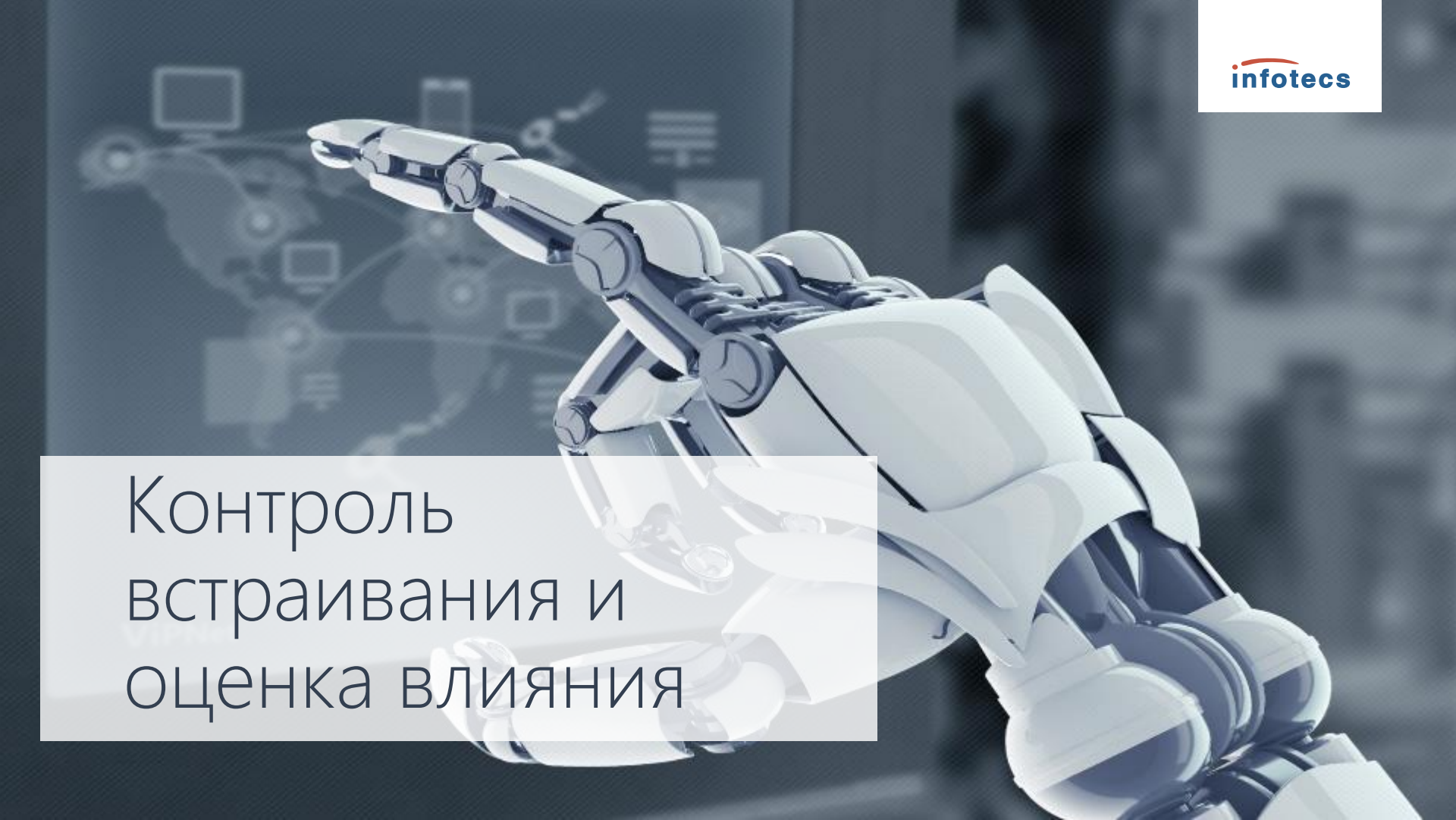
Порядок сертификации

Начинается всё с согласованного ТЗ и заканчивается сертификатом

При этом на каждом из этапов продукт может зависать «бесконечно» долго



©2017, ОАО «ИнфоТеКС».



Контроль встраивания и оценка влияния

Контроль встраивания



- Нормативные документы – отсутствуют
- Юридически сейчас такого понятия не существуют, как и понятия «корректность встраивания»

©2017, ОАО «ИнфоТеКС».

Оценка влияния

Положение ПКЗ-2005

- П.35 Оценка влияния аппаратных, … и программных средств сети (системы) конфиденциальной связи, совместно с которыми предполагается штатное функционирование СКЗИ, на выполнение … требований осуществляется разработчиком СКЗИ совместно со специализированной организацией



©2017, ОАО «ИнфоТеКС».

Оценка влияния



Необходимо проводить, если:

- Выполняется П.3 ПКЗ-2005 (описывает, когда необходимо руководствоваться Положением):
  - Если инф-я подлежит защите в соответствии с законодательством РФ;
  - При организации КЗИ в ФОИВ;
  - И т.д.

- Среда функционирования отличается от прописанной в ПП

©2017, ОАО «ИнфоТеКС».



Сценарии

Сценарии с партнерами



- Есть набор сущностей
- В зависимости от него выбирается техническое решение и бизнес-модель:
  - доработка прикладного ПО партнера
  - доработка библиотек/СКЗИ
  - создание совместно решения и его сертификация при необходимости
  - лицензионный договор

©2017, ОАО «ИнфоТеКС».



Спасибо за внимание!

Сергей Петренко
Sergey.Petrenko@infotecs.ru
+7 (495) 737-61-92 (5240)