Практики безопасной разработки программного обеспечения как важная составляющая соответствия требованиям безопасности информации

Смирнов Николай
директор по продуктам

infotecs®

конференция РусКрипто

Опыт внедрения SDL
или
насколько глубока кроличья нора

конференция РусКрипто

infotecs®

Продукты компании Инфотекс

конференция РусКрипто

infotecs

Целевые ИС это
ГИС, ИСПДН и КИИ

Продукты производства
Инфотекс сертифицируются
по требованиям
ФСТЭК России и ФСБ России

Zoom Shape 1

Продукты компании Инфотекс

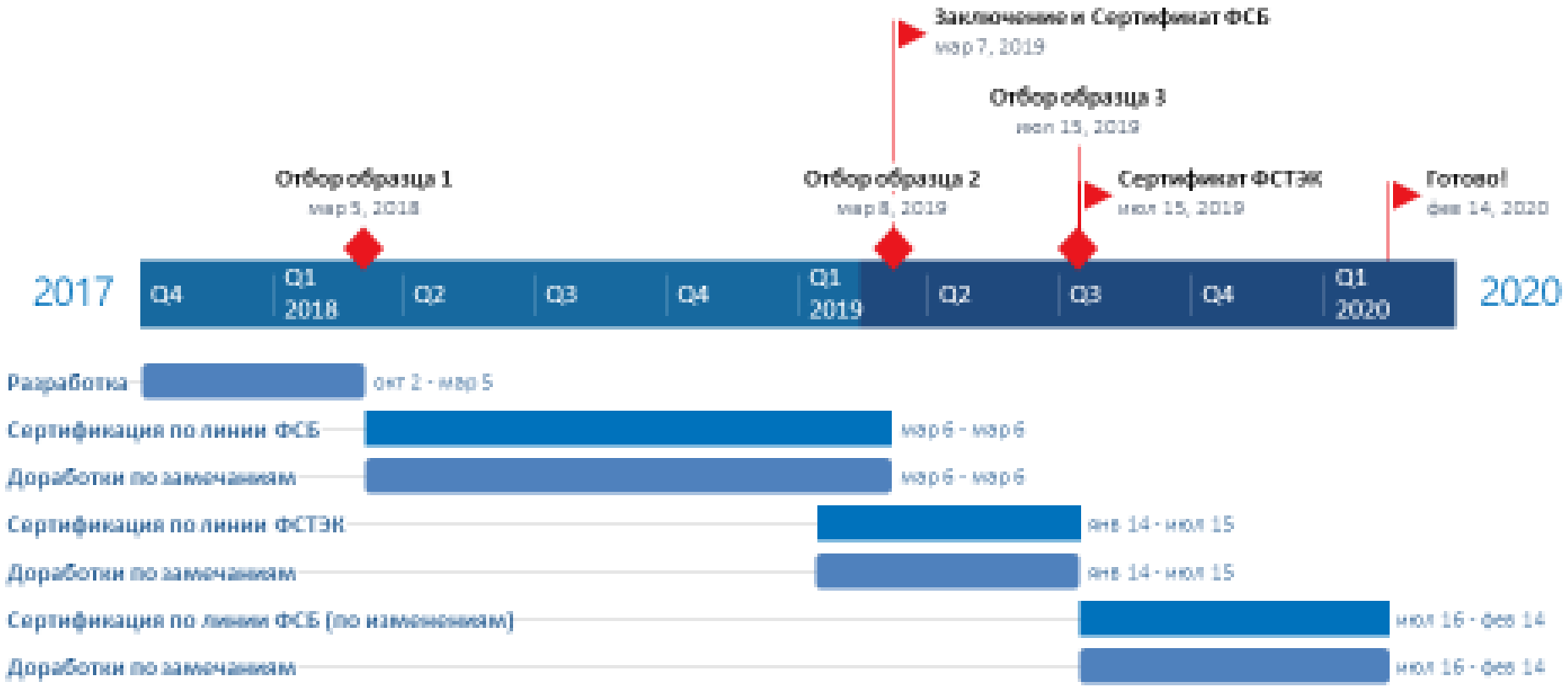
конференция РусКрипто

infotecs

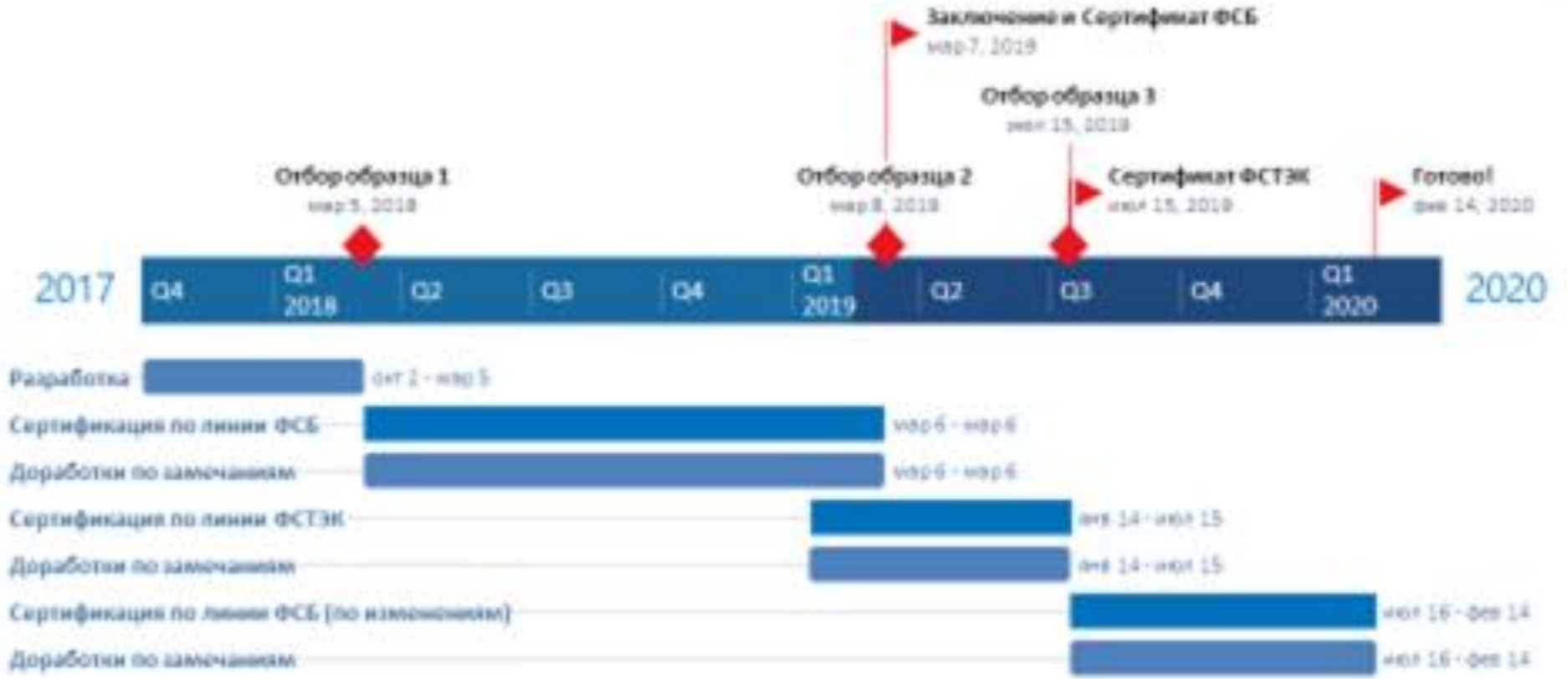
Целевые ИС это
ГИС, ИСПДН и КИИ

Продукты производства
Инфотекс сертифицируются
по требованиям
ФСТЭК России и ФСБ России

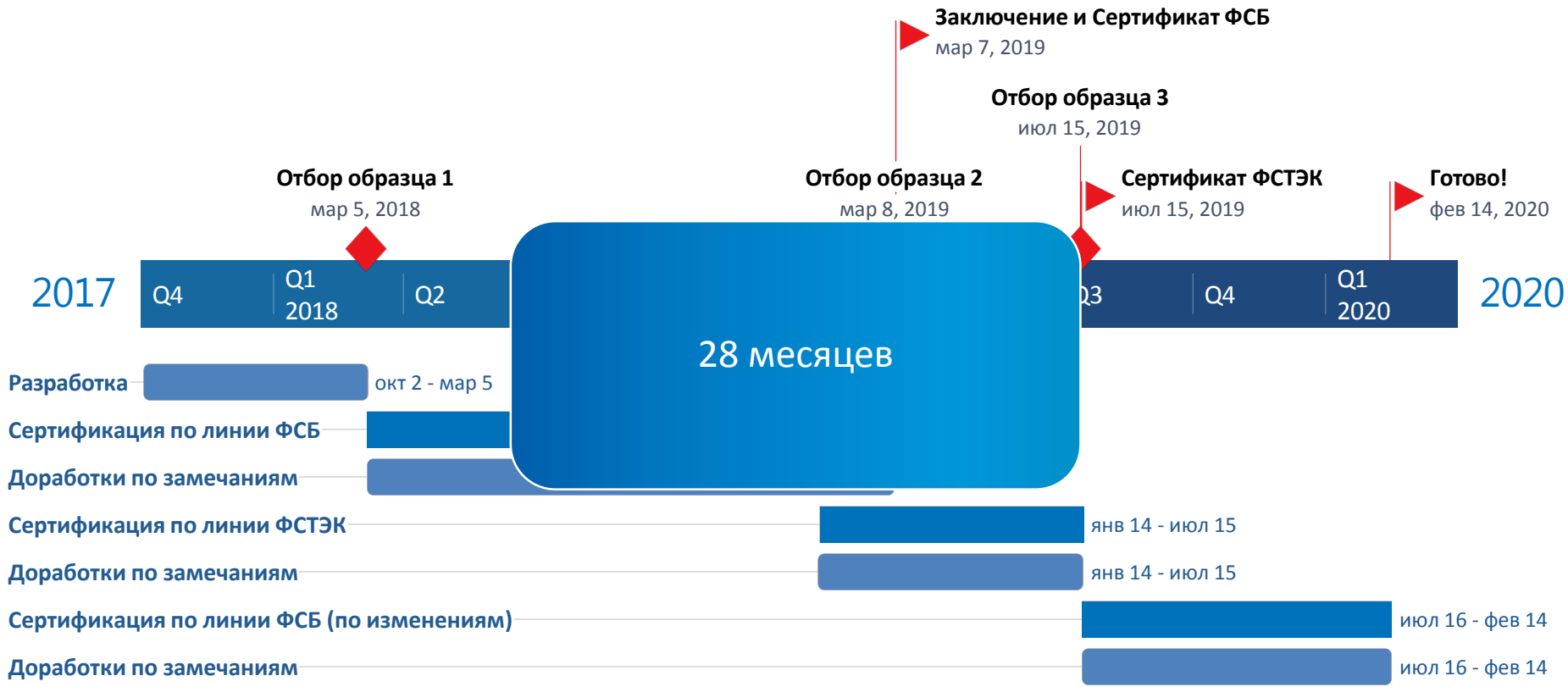
Типовой график сертификации



Типовой график сертификации



Типовой график сертификации



Продукты производства
Инфотекс сертифицируются
по требованиям
ФСТЭК России и ФСБ России

Продукты компании Инфотекс

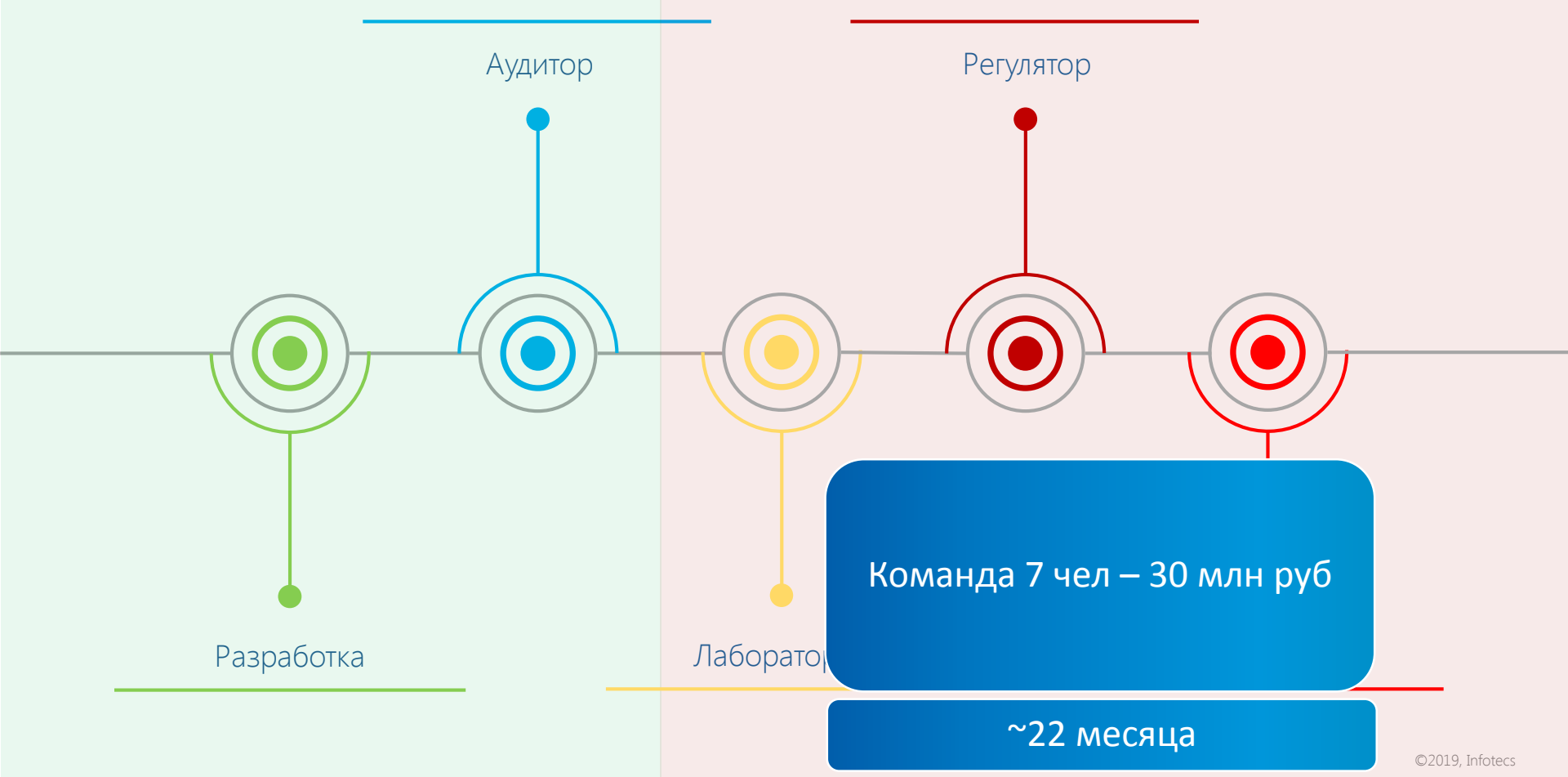
конференция РусКрипто

infotecs

Целевые ИС это
ГИС, ИСПДН и КИИ

Продукты производства
Инфотекс сертифицируются
по требованиям
ФСТЭК России и ФСБ России

Обнаружение уязвимости



Задача

конференция РусКрипто

infotecs

2014

50+ Продуктов

Каждый Продукт имеет свою стадию цикла

Убрать вероятность выявления неприятностей после стадии аудита

Приоритезация продуктов

Иерархия критериев успешности

Иерархия мер и практик

Задача

конференция РусКрипто

infotecs

2014

50+ Продуктов

Каждый Продукт имеет свою стадию цикла

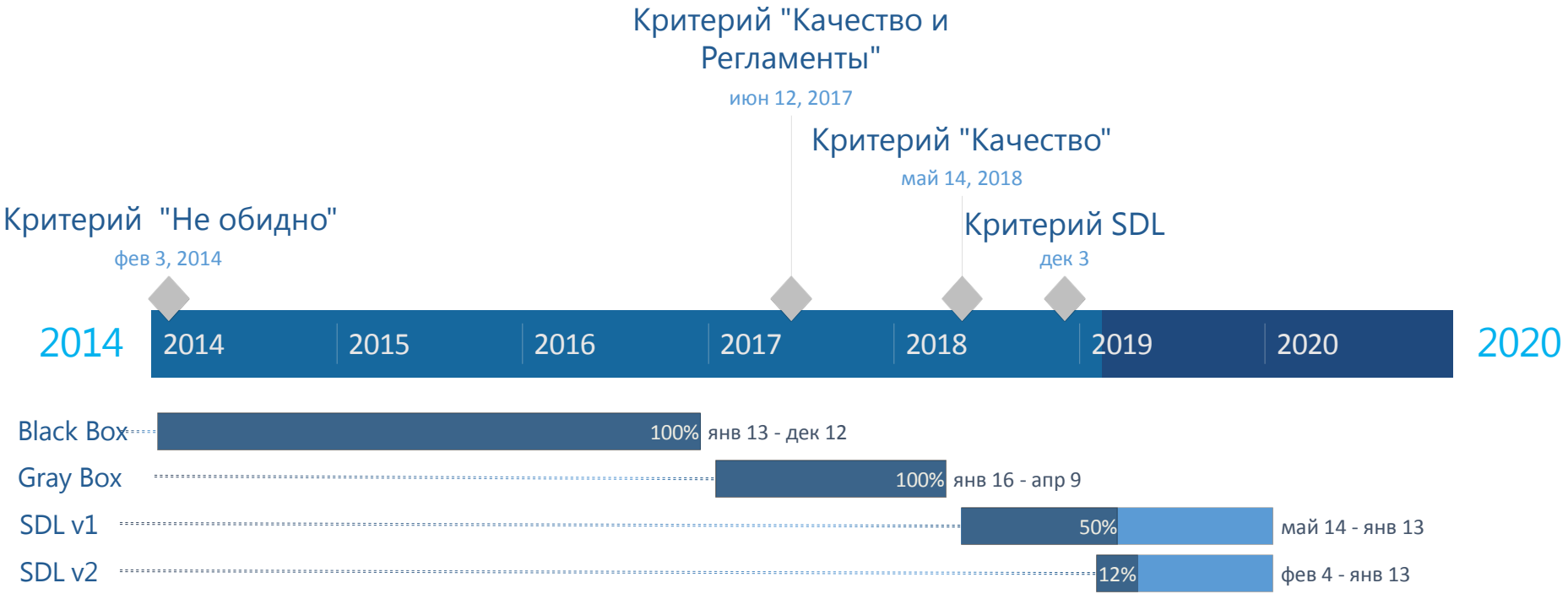
Убрать вероятность выявления неприятностей после стадии аудита

Приоритезация продуктов

Иерархия критериев успешности

Иерархия мер и практик

Динамика

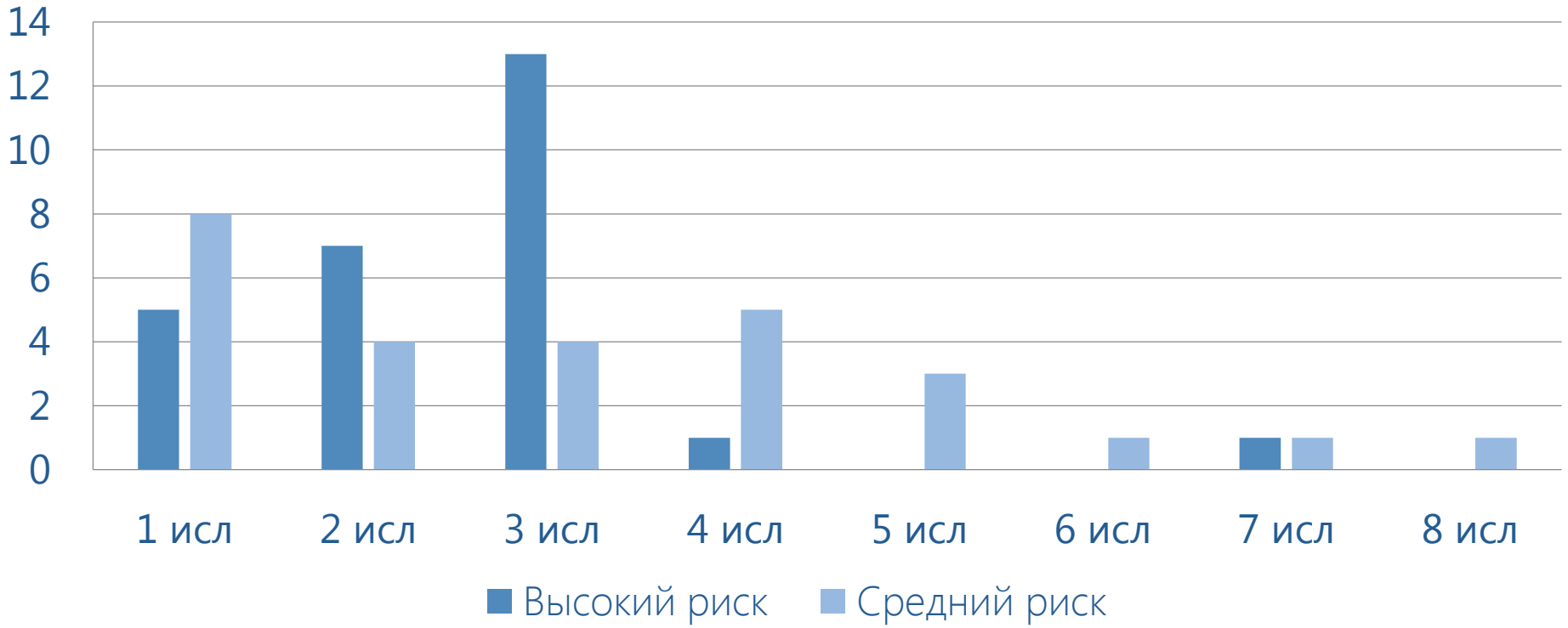


Статистика

конференция РусКрипто

infotecs

Продукты 1-го приоритета



Статус

Не было ни одного аудита без выявления неприятностей

Сокращение собственных ошибок компенсируется выявлением уязвимостей в общих библиотеках

Частота внеплановых выпусков релизов не изменилась

Объемы инвестиций растут год от года. Статус: дефицит инвестиций

Удовлетворенность

Ожидания

Реальность

Причины

Культура

Условия имплементации внешних библиотек

Огромный объем накопленных внутренних и внешних зависимостей кода

Длительные сроки «фиксации» версий

Причины

- Культура
- Условия имплементации внешних библиотек
- Огромный объем накопленных внутренних и внешних зависимостей кода
- Длительные сроки «фиксации» версий

Культура

Культура

Культура

Причины

Культура

Условия имплементации внешних библиотек

Zoom Shape 1

Огромный объем накопленных внутренних и внешних зависимостей кода

Длительные сроки «фиксации» версий

Причины

infotecs

- Культура
- Условия имплементации внешних библиотек
- Огромный объем накопленных внутренних и внешних зависимостей кода
- Длительные сроки «фиксации» версий

Условия имплементации внешних библиотек

Условия имплементации внешних библиотек

Причины

Условия имплементации внешних библиотек

Должны быть последние версии

- свой собственный ЖЦ
- уязвимости

Варианты решений

- Аудит сторонних библиотек
- Согласование ЖЦ
- Переход на 1 уровень абстракций интерфейсов выше

Причины

Условия имплементации внешних библиотек

Условия имплементации внешних библиотек

Причины

Культура

Условия имплементации внешних библиотек

Огромный объем накопленных внутренних и внешних зависимостей кода

Zoom Shape 1

Длительные сроки «фиксации» версий

Причины

- Культура
- Условия имплементации внешних библиотек
- Огромный объем накопленных внутренних и внешних зависимостей кода
- Длительные сроки «фиксации» версий

Огромный объем накопленных внутренних и внешних зависимостей кода

Огромный объем накопленных внутренних и внешних зависимостей кода

Причины

Огромный объем накопленных внутренних и внешних зависимостей кода

Переход на «атомарные» версии продуктов

- Client
- Personal FW

Оптимизация

- Архитектурная
- Продуктовая

Причины

Огромный объем накопленных внутренних и внешних зависимостей кода

Огромный объем накопленных внутренних и внешних зависимостей кода

Причины

Культура

Условия имплементации внешних библиотек

Огромный объем накопленных внутренних и внешних зависимостей кода

Длительные сроки «фиксации» версий

Zoom Shape 1

Причины

- Культура
- Условия имплементации внешних библиотек
- Огромный объем накопленных внутренних и внешних зависимостей кода
- Длительные сроки «фиксации» версий

Длительные сроки «фиксации» версий

Длительные сроки «фиксации» версий

Причины

Длительные сроки «фиксации» версий

Новый порядок сертификации ФСТЭК России

Оптимизация работ с сертификационными исследованиями вцелом

Длительные сроки «фиксации» версий

Причины

Культура

Условия имплементации внешних библиотек

Огромный объем накопленных внутренних и внешних зависимостей кода

Длительные сроки «фиксации» версий

Еще причины и следствия

конференция РусКрипто

infotecs

Движущиеся цели и нечеткие границы

- Растет степень понимания задачи
- Меняются ожидания
- Меняются требования

Цели и сроки

- Надежность – остался год
- Быстрое управление изменениями – осталось 3 года
- Экономическая целесообразность - новый срок

Выводы

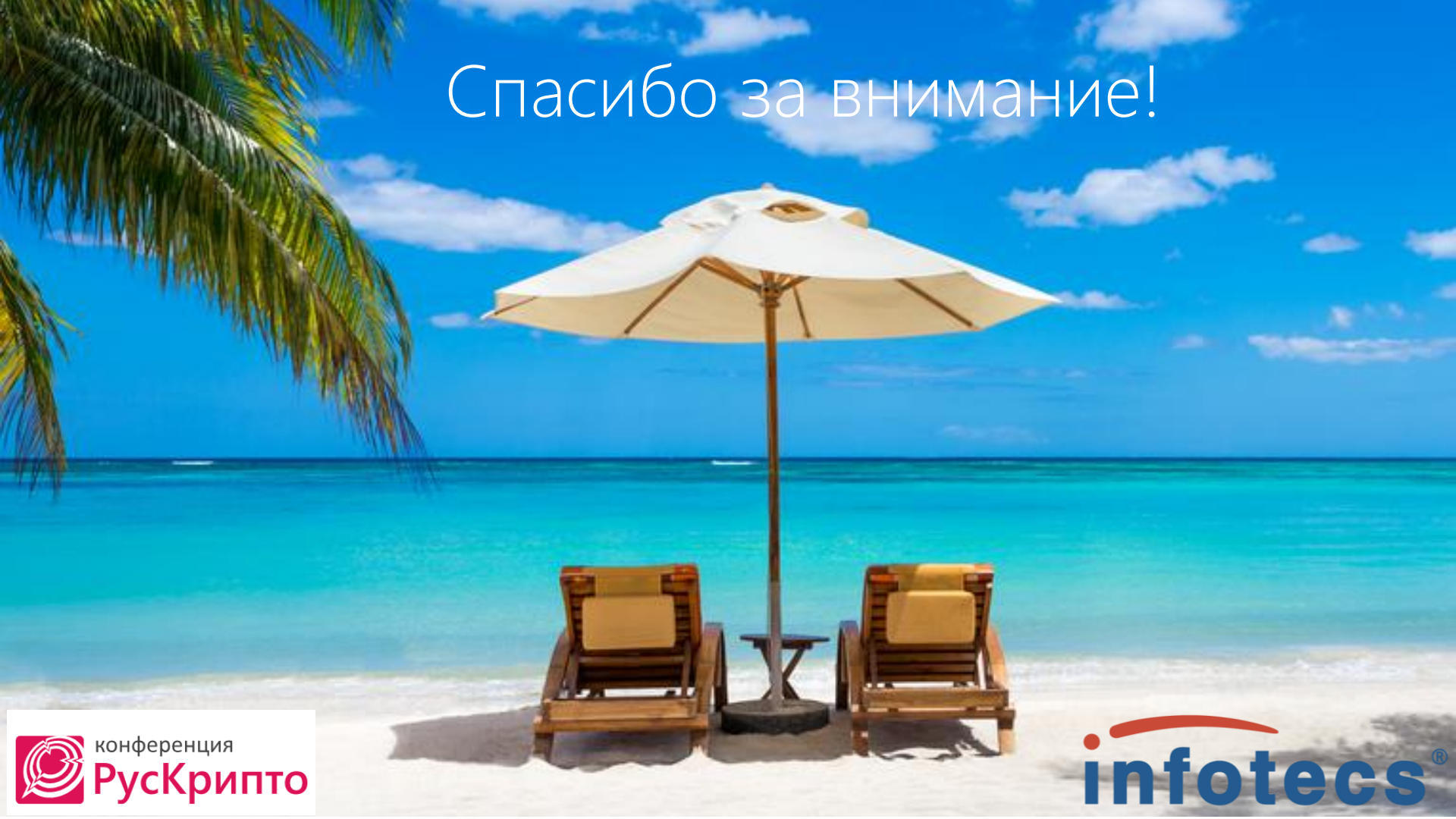
конференция РусКрипто

infotecs

Процесс оказался сложным, долгим, дорогим

Мы все-таки вышли на пляж*

Спасибо за внимание!



конференция РусКрипто

infotecs®