

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

Смирнов Николай
директор по продуктам

infotecs®

конференция
РусКрипто



INFORMATION SECURITY

Опыт внедрения SDL
или
насколько глубока кроличья нора

ПРОДУКТЫ КОМПАНИИ ИНФОТЕКС



конференция
РусКрипто



Целевые ИС это
ГИС, ИСПДН и КИИ

Завод

VPNet Coordinator HW
VPNet Coordinator IG
VPNet SIES
VPNet TLS Gateway

VPNet IDS HS
VPNet TLS Gateway
VPNet PKI Client
VPNet TIAS

Офис

VPNet StateWatcher
VPNet Coordinator HW
VPNet Client
VPNet IDS HS
VPNet IDS
VPNet PKI Client
VPNet Connect
VPNet TIAS
VPNet Administrator
VPNet Policy Manager

Банк

VPNet HSM
VPNet PKI Client
VPNet TLS Gateway
VPNet IDS HS
VPNet IDS
VPNet Coordinator HW
VPNet TIAS

ЦОД / РЦОД

VPNet Coordinator HW/VA
VPNet IDS

Портал

VPNet TLS Gateway
VPNet HSM
VPNet Registration Point
VPNet Publication Service

Госуслуги

VPNet Connect
VPNet Client
VPNet Coordinator HW
VPNet PKI Client
VPNet EDI

Поликлиника

VPNet PKI Client
VPNet TLS Gateway
VPNet IDS HS
VPNet IDS
VPNet Coordinator HW
VPNet Client

УЦ

VPNet Certification Authority
VPNet Coordinator HW
VPNet TLS Gateway
VPNet TSP OCSP
VPNet Registration Point
VPNet CA WEB
VPNet CA Informing

Железная дорога

VPNet Coordinator IG
VPNet Client
VPNet SIES
VPNet TIAS

Парк

VPNet Connect
VPNet Client

Продукты производства
Инфотекс сертифицируются
по требованиям
Zoom Shape 1
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

ТИПОВОЙ ГРАФИК СЕРТИФИКАЦИИ



Разработка: окт 2 - мар 5

Сертификация по линии ФСЕ: мар 6 - мар 6

Доработки по замечаниям: мар 6 - мар 6

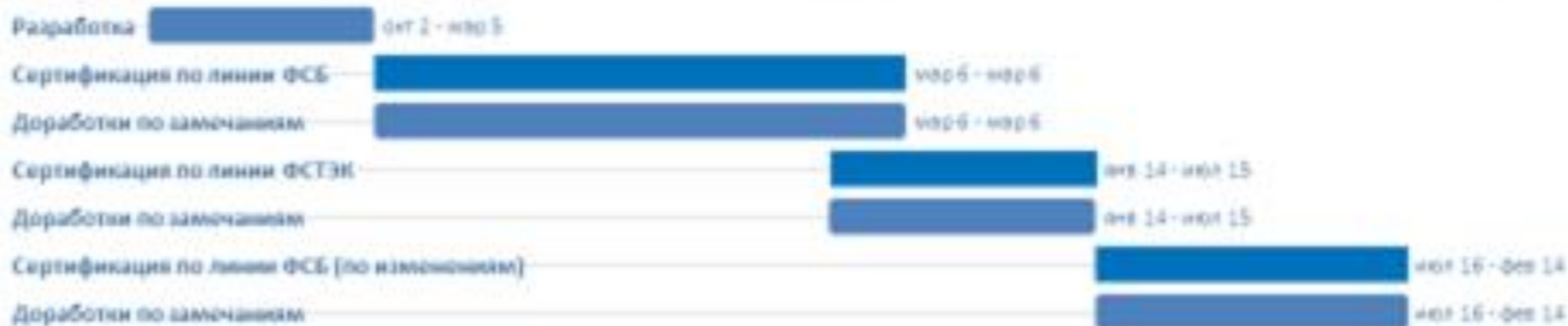
Сертификация по линии ФСТЭК: июл 14 - июл 15

Доработки по замечаниям: июл 14 - июл 15

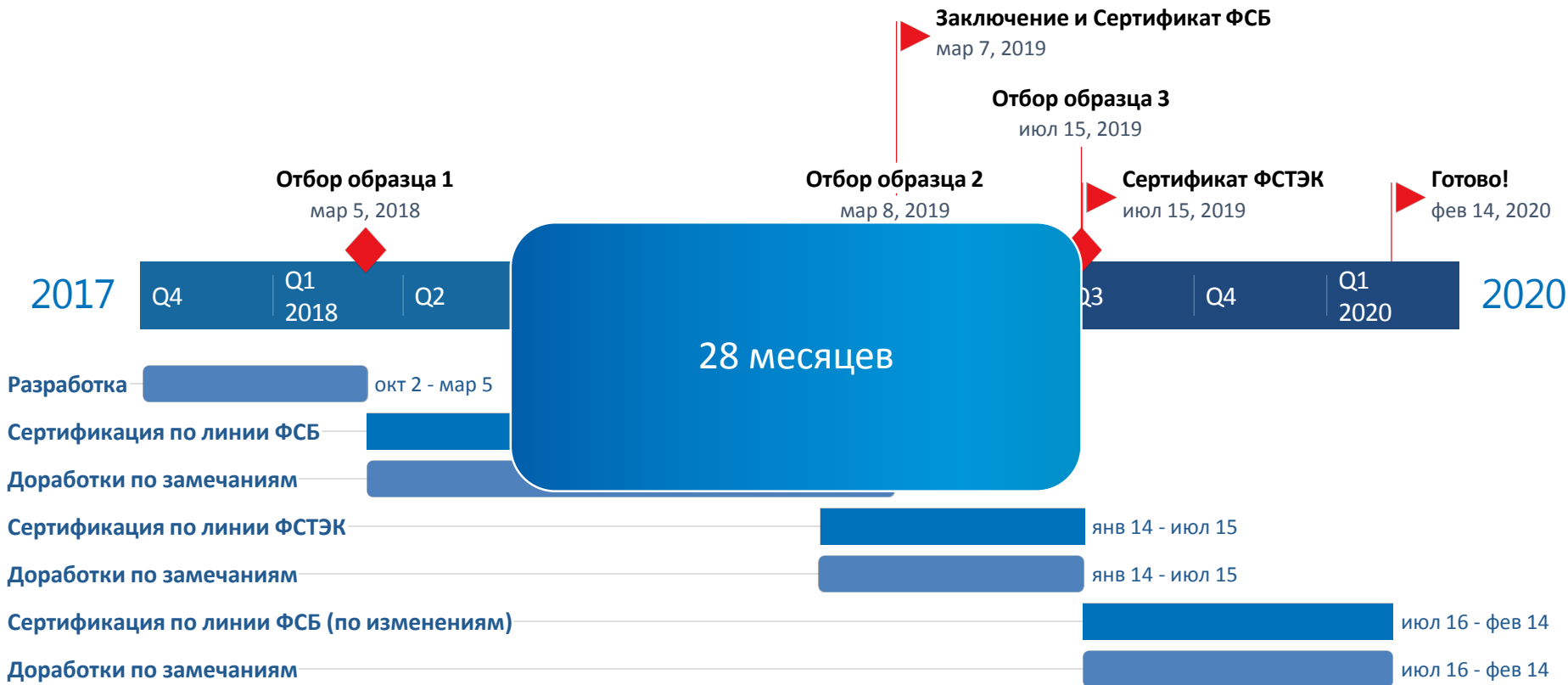
Сертификация по линии ФСЕ (по замечаниям): июл 16 - фев 14


Доработки по замечаниям: июл 16 - фев 14

ТИПОВОЙ ГРАФИК СЕРТИФИКАЦИИ



ТИПОВОЙ ГРАФИК СЕРТИФИКАЦИИ





Продукты производства
Инфотекс сертифицируются
по требованиям
ФСТЭК России и ФСБ России

ПРОДУКТЫ КОМПАНИИ ИНФОТЕКС



конференция
РусКрипто



Целевые ИС это
ГИС, ИСПДн и КИИ

Завод
VPNnet Coordinator HW
VPNnet Coordinator IG
VPNnet SIES
VPNnet TLS Gateway

VPNnet IDS HS
VPNnet TLS Gateway
VPNnet PKI Client
VPNnet TIAS

Офис

VPNnet StateWatcher
VPNnet Coordinator HW
VPNnet Client
VPNnet IDS HS
VPNnet IDS
VPNnet PKI Client
VPNnet Connect
VPNnet TIAS
VPNnet Administrator
VPNnet Policy Manager

Банк

VPNnet HSM
VPNnet PKI Client
VPNnet TLS Gateway
VPNnet IDS HS
VPNnet IDS
VPNnet Coordinator HW
VPNnet TIAS

ЦОД / РЦОД

VPNnet Coordinator HW/VA
VPNnet IDS

Портал

VPNnet TLS Gateway
VPNnet HSM
VPNnet Registration Point
VPNnet Publication Service

Госуслуги

VPNnet Connect
VPNnet Client
VPNnet Coordinator HW
VPNnet PKI Client
VPNnet EDI

Поликлиника

VPNnet PKI Client
VPNnet TLS Gateway
VPNnet IDS HS
VPNnet IDS
VPNnet Coordinator HW
VPNnet Client

УЦ

VPNnet Certification Authority
VPNnet Coordinator HW
VPNnet TLS Gateway
VPNnet TSP OCSP
VPNnet Registration Point
VPNnet CA WEB
VPNnet CA Informing

Железная дорога

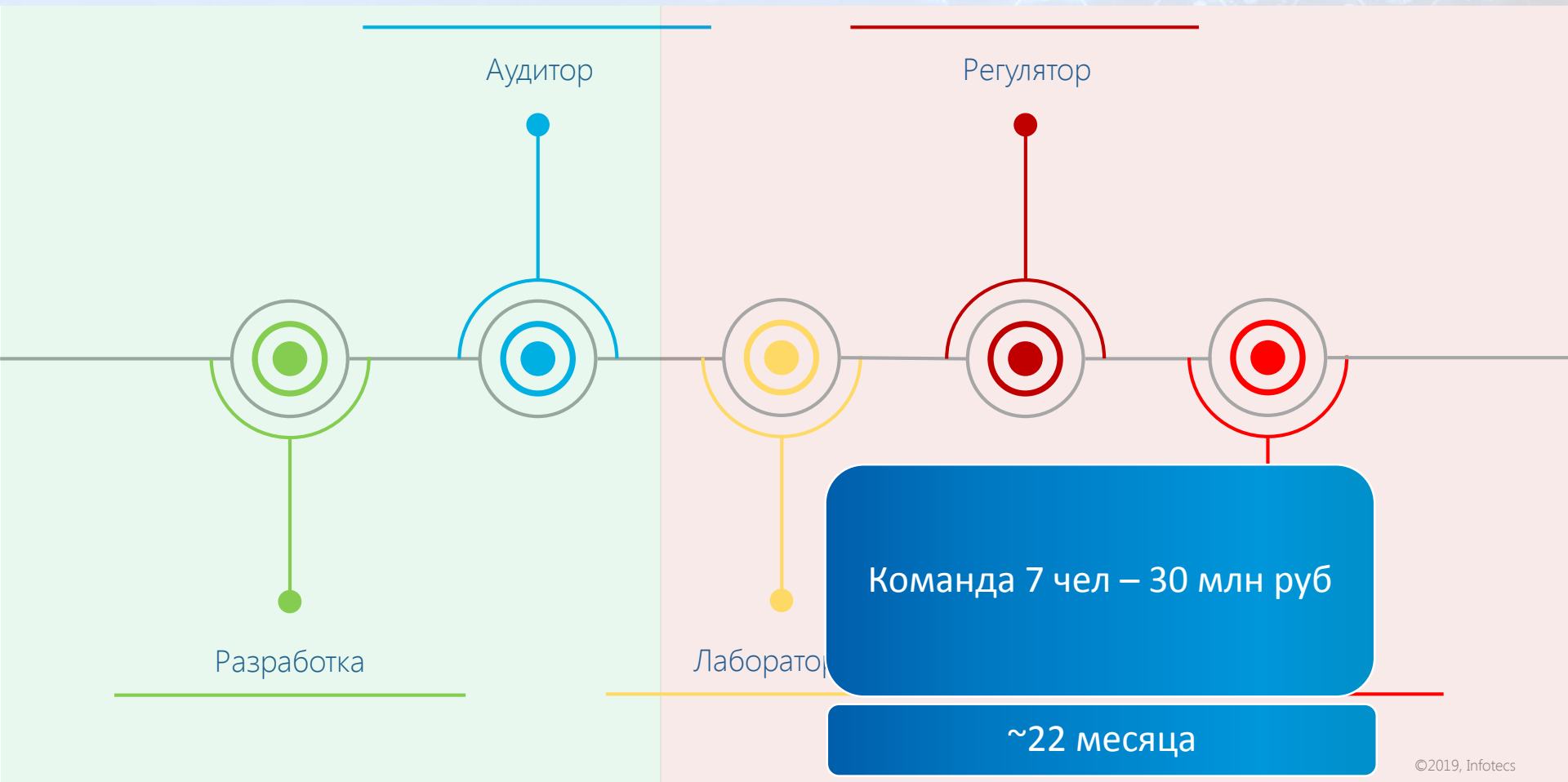
VPNnet Coordinator IG
VPNnet Client
VPNnet SIES
VPNnet TIAS

Парк

VPNnet Connect
VPNnet Client

Продукты производства
Инфотекс сертифицируются
по требованиям
ФСТЭК России и ФСБ России

ОБНАРУЖЕНИЕ УЯЗВИМОСТИ



ЗАДАЧА

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



Критерий "Качество и Регламенты"

июн 12, 2017

Критерий "Качество"

май 14, 2018

Критерий SDL

дек 3

Критерий "Не обидно"

фев 3, 2014

2014

2014

2015

2016

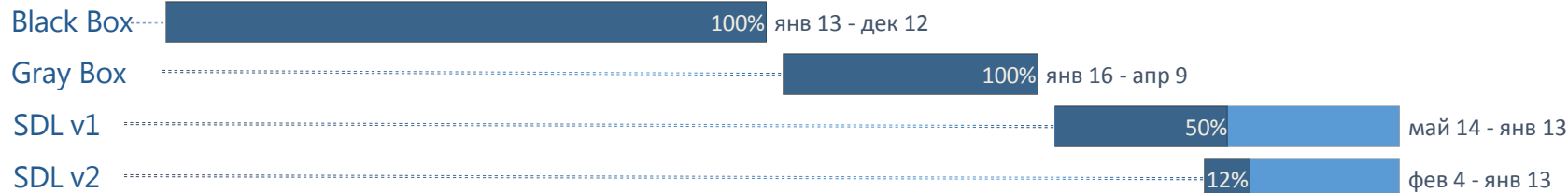
2017

2018

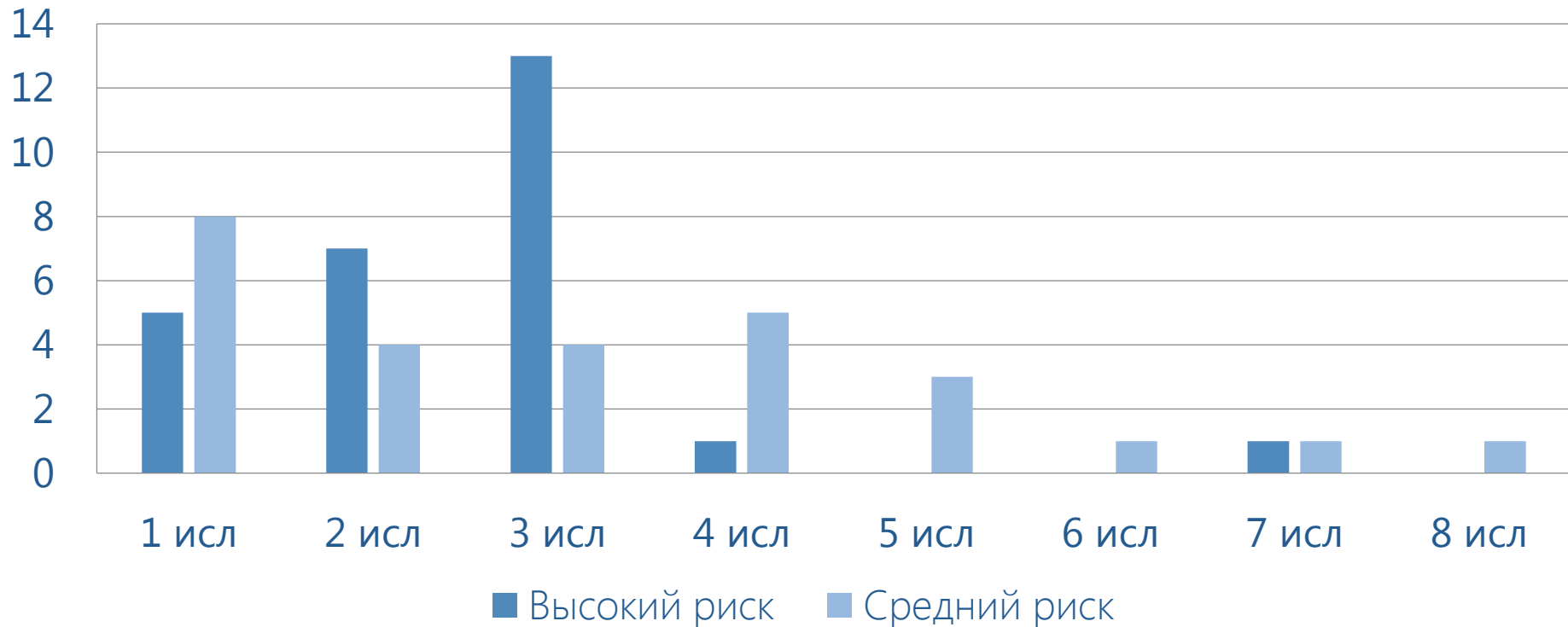
2019

2020

2020



ПРОДУКТЫ 1-ГО ПРИОРИТЕТА





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



Ожидания



Реальность

Культура

Условия имплементации
внешних библиотек

Огромный объем
накопленных внутренних
и внешних зависимостей
кода

Длительные сроки
«фиксации» версий



Культура

Условия имплементации
внешних библиотек

Огромный объем
накопленных внутренних
и внешних зависимостей
кода

Длительные сроки
«фиксации» версий

Культура

Культура

Культура

Культура

Условия имплементации
Zoom Shape 1
внешних библиотек

Огромный объем
накопленных внутренних
и внешних зависимостей
кода

Длительные сроки
«фиксации» версий

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

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



Условия имплементации внешних библиотек

Условия имплементации внешних библиотек

Культура

Условия имплементации
внешних библиотек

Огромный объем
накопленных внутренних
и внешних зависимостей
кода

Zoom Shape 1

Длительные сроки
«фиксации» версий



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



Огромный объем
накопленных внутренних
и внешних зависимостей
кода

Переход на «атомарные»
версии продуктов

- Client
- Personal FW

Оптимизация

- Архитектурная
- Продуктовая



Огромный объем
накопленных внутренних
и внешних зависимостей
кода

Огромный объем
накопленных внутренних
и внешних зависимостей
кода

Культура

Условия имплементации
внешних библиотек

Огромный объем
накопленных внутренних
и внешних зависимостей
кода

Длительные сроки
Zoom Shape 1
«фиксации» версий

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

Длительные сроки
«фиксации» версий

Новый порядок
сертификации ФСТЭК
России

Оптимизация работ с
сертификационными
исследованиями в целом

Длительные сроки
«фиксации» версий

Культура

Условия имплементации
внешних библиотек

Огромный объем
накопленных внутренних
и внешних зависимостей
кода

Длительные сроки
«фиксации» версий



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

Процесс оказался сложным, долгим,
дорогим

Мы все-таки вышли на пляж*



Спасибо за внимание!