

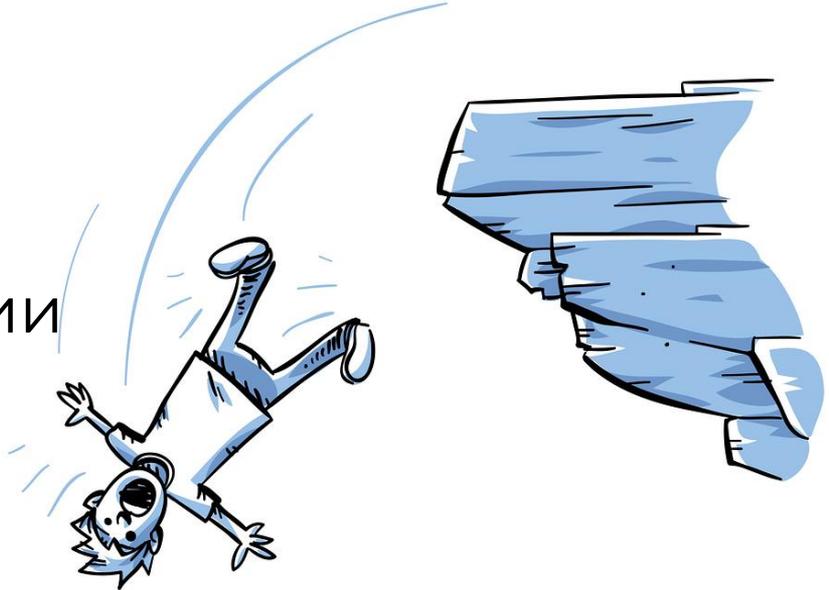
Практические аспекты информационной безопасности на предприятии в контексте цифровой трансформации



Эдуард Мураховский
директор департамента проектного
управления ГК «ФАРМИМЭКС»

Базовые навыки по ИБ

1. Определять ценность / ущерб от утраты информации
2. Доносить эту ценность до:
 - ответственных за ИБ
 - других сотрудников
3. Понимать ограничения по бюджету ИБ
4. Выбирать адекватные технические средства
5. Учитывать негативные сценарии и иметь «План Б»



Четко сформулированные задачи ИБ!



Откуда готовилось нападение

ХАКЕРЫ «ДЛЯ ИНТЕРЕСА»

- Взломы ради известности
- Ограничены ресурсы
- Только известные эксплойты

ХАКЕРЫ «ДЛЯ УЩЕРБА»

- Вандализм
- Ограниченные ресурсы

ПРЕСТУПНОСТЬ

- Взлом ради прибыли
- Существенные ресурсы
- Синдикаты
- Специально разработанные программы для кражи данных

СПЕЦСЛУЖБЫ

- Атаки на критические инфраструктуры, промышленный шпионаж
- Практически неограниченные ресурсы
- Сложное ВПО и программы для взлома
- Постоянные угрозы

Рост затрат ресурсов и сложности атак

Тренды информационной опасности

- Облака
- Аутсорсинг
- Дипфейк
- Усложнение вирусов-шифровальщиков
- Рост квалификации киберпреступников



Безопасность: от наложенной к интегрированной



Интегрированная безопасность

РАЗВИТИЕ ТЕХНОЛОГИЙ

- Информационные системы «теряют» границы
- Все взаимодействует со всеми
- Рост и развитие интегрированных возможностей
- Автономные системы и «умные» устройства
- Смещение в сторону аппаратных возможностей

УГРОЗЫ

- Уязвимости прошивок и АО
- Утечки через встроенное ПО и СФ блоки
- НДВ в АО и встроенном ПО
- Манипулирование параметрами работы

ВОЗМОЖНОСТИ

- Доверенная загрузка
- Изолированная среда для критических функций
- Безопасная среда для СКЗИ
- Защищенное хранение данных
- Контроль работы на аппаратном уровне
- Мониторинг и управление

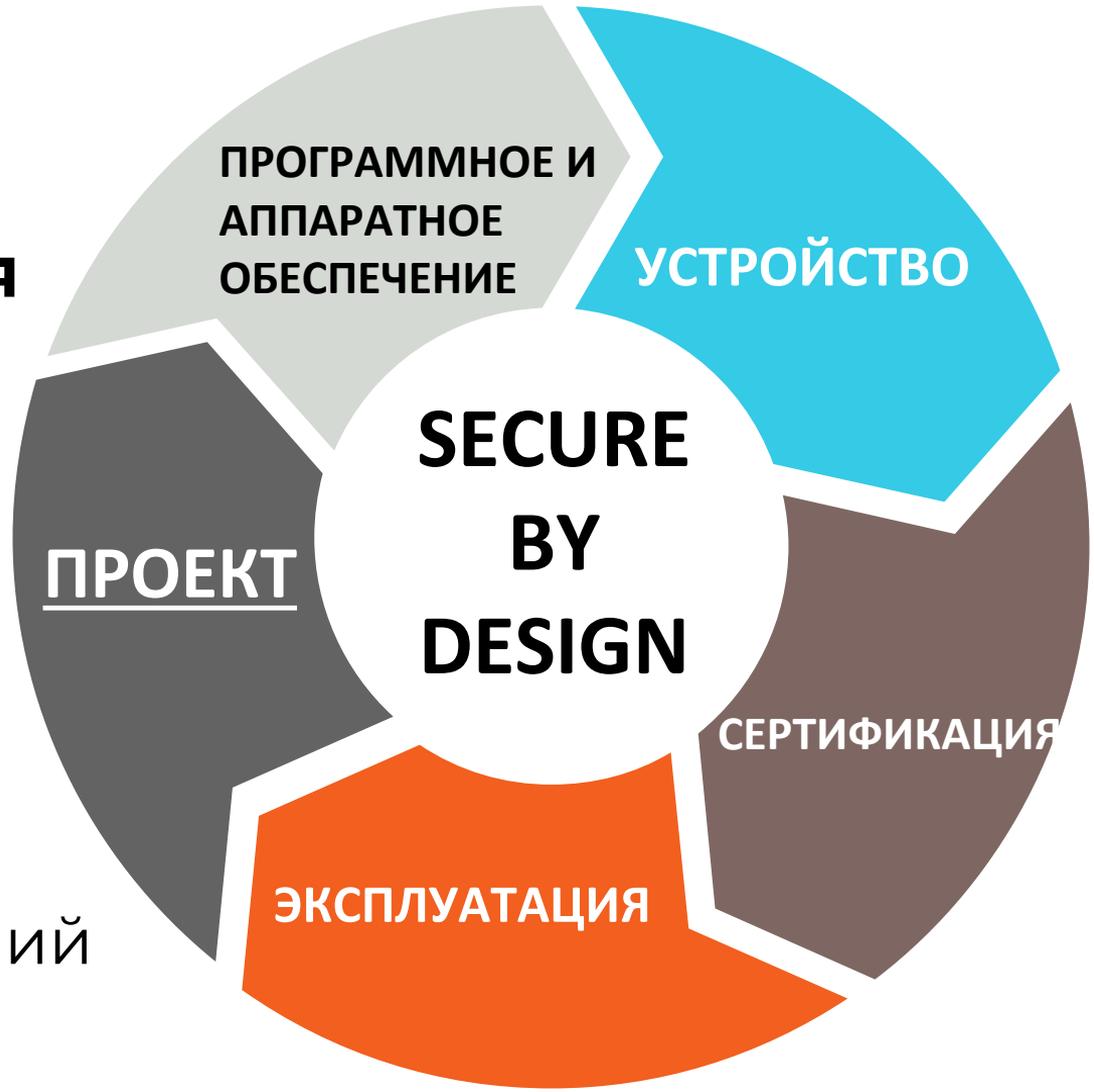
Жизненный цикл с учетом импортозамещения

1. Доверенное

2. Безопасное

3. Российское:

- возможность глубокой верификации
- отсутствие ограничений на использование



Мировые практики

ШАГ 04

МЕТОДИКИ И СООТВЕТСТВИЕ

ТРЕБОВАНИЯ

ШАГ 03

GP TEE PP
GP BOOTREQ
GP SA

OMTP-TR0
OMTP-TR1

ARM TBSA
ARM TBBR

ФСТЭК

ШАГ 02

МОДЕЛИ УГРОЗ

ФСТЭК

ARM TBSA

TCG-PCCLIENT

OMTP-THREATS

GP TEE PP

СЦЕНАРИИ

ШАГ 01

OMTP TR0
OMTP-THREATS

ARM TBSA

GP TEE PP

Человеческий фактор

- Товарищ прапорщик,
остановите поезд!
- Может → хочет → делает
- Предупрежден –
значит вооружен
- Push & Pull
- Повторенье – мать ученья



Благодарю за внимание!

Эдуард Мураховский
директор департамента проектного
управления ГК «ФАРМИМЭКС»

6440 м

ABC

