Построение ИБ с нуля, это полная реконструкция ИТ

Алексей Кан

CISSP, CISA, CCNP R&S, SSCP

Директор департамента ИТ безопасности

АО «Евразийский Банк»

2013 год…

- Правление банка принимает решение по смене команды ИБ.
- Первичный анализ текущего состояния, привел нас в шок и породил два ключевых вопроса:

к ИБ: Как вас еще не взломали?

к ИТ: Сейчас на дворе конец 90-х?

2013 год… Что было не так?!

1. Не контролируемый внешний периметр
2. Отсутствие процессов управления обновлениями и уязвимостями
3. Не контролируемый процесс управления доступом к ИС
4. Полное отсутствие внутренних процессов ITIL
5. Внешний периметр контролируется при помощи Cisco 6500 с > 4000 ACL
6. Использование static-IP и L2-сетей во всех офисах
7. Отсутствие резервирования критичного оборудования

Что требовалось от ИТ

Для построения СУИБ необходимо наличие ключевых процессов ИТ:

- **Change Management**, для планирования и контроля изменений
- **Incident Management**, для реагирования и устранения инцидентов
- **Configuration Management**, для управления активами
- **Availability Management**, для обеспечения доступности ИС

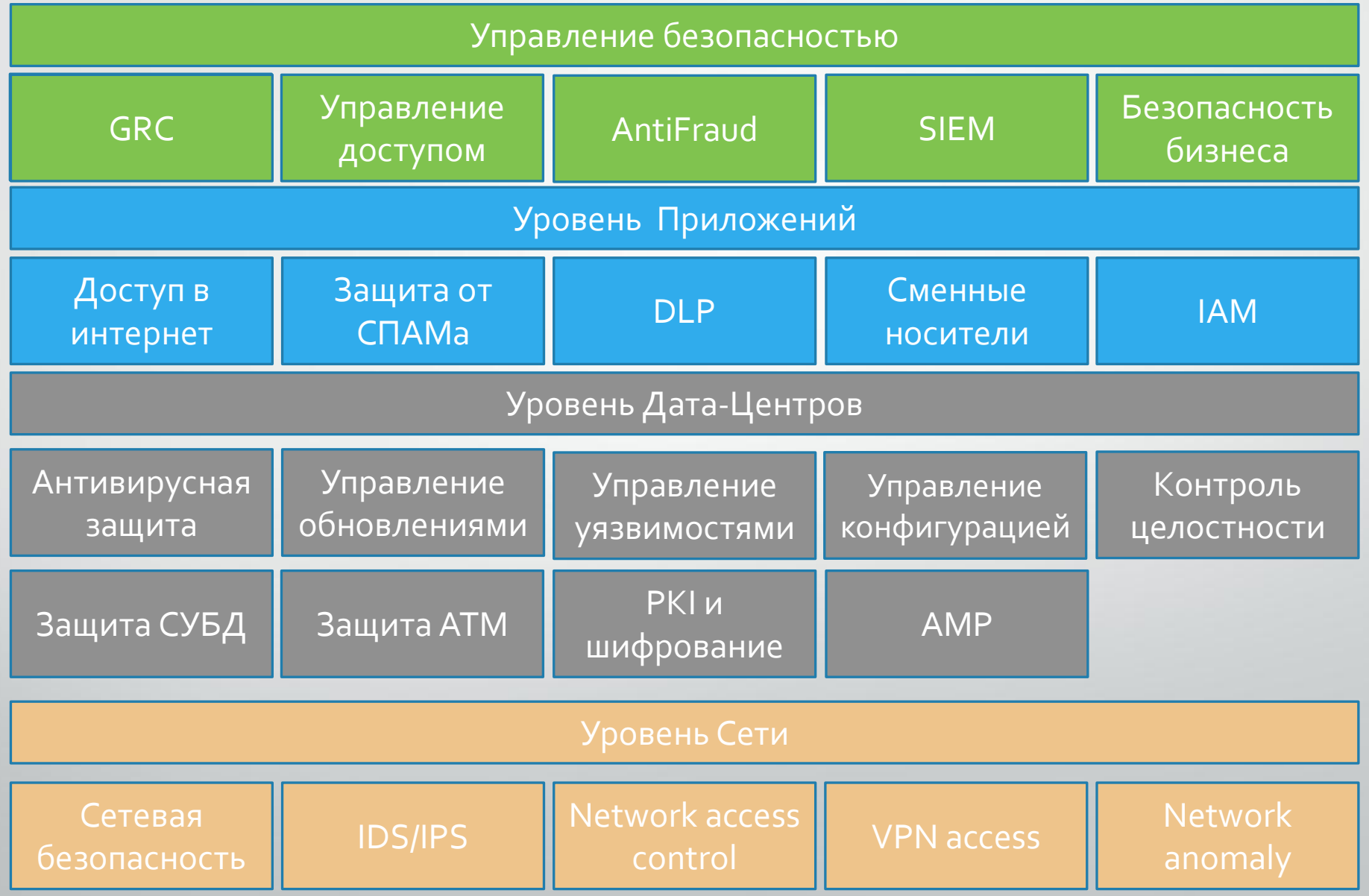
Ключевые проблемы взаимодействия с ИТ

- Полное отсутствие доверия к ИБ
- Наличие «звездных» начальников
- Наличие «псевдо» профессионалов
- ИБ ломает у ИТ привычный стиль работы
- Команда не видевшая лучших практик
- ИТ – черный ящик для всего банка

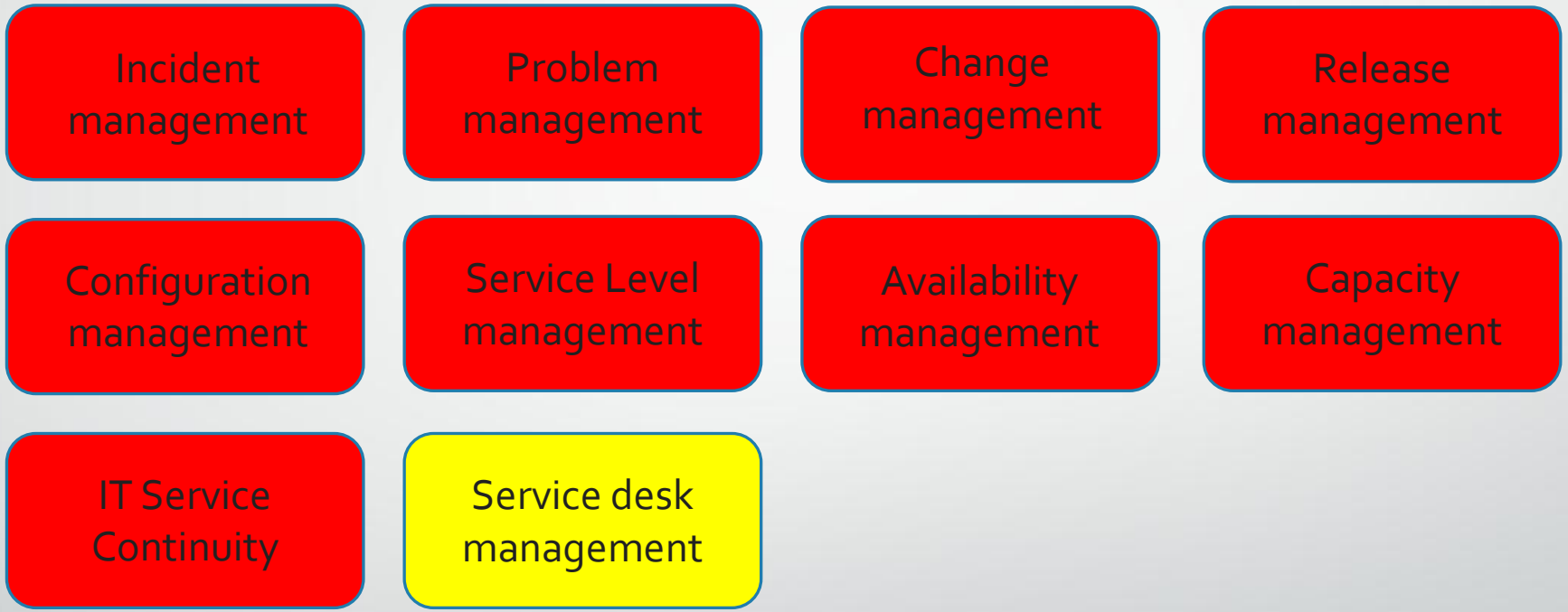
Как мы решали проблемы с ИТ

- Постепенное разъяснение сути проблемы и способов его решения
- Внедрение «идеи» в ИТ, и ожидание когда «идея» перерастет в «решение от ИТ»
- Наработка профессионального авторитета, как на уровне руководителей ИТ, так и на уровне персонала
- Разработка ITIL процессов под контролем ИБ
- Жесткое навязывание требований ИБ

2016 год. К чему пришли в ИБ



2016 год. К чему пришли с ИТ



Подведение итогов

- Построение СУИБ не возможно без ИТ
- ИТ должно полностью понимать цели и задачи СУИБ
- ИТ должно осознавать, что ИБ это не прихоть группы людей, а современная реальность
- Зрелые процессы ITIL это решение 50% проблем при внедрении СУИБ

На этом все!

Вопросы?

Алексей Кан

aleksey.kan@eubank.kz

+7 701 527 4962