Архитектура информационной безопасности

Алексей Лукацкий

Бизнес-консультант по безопасности

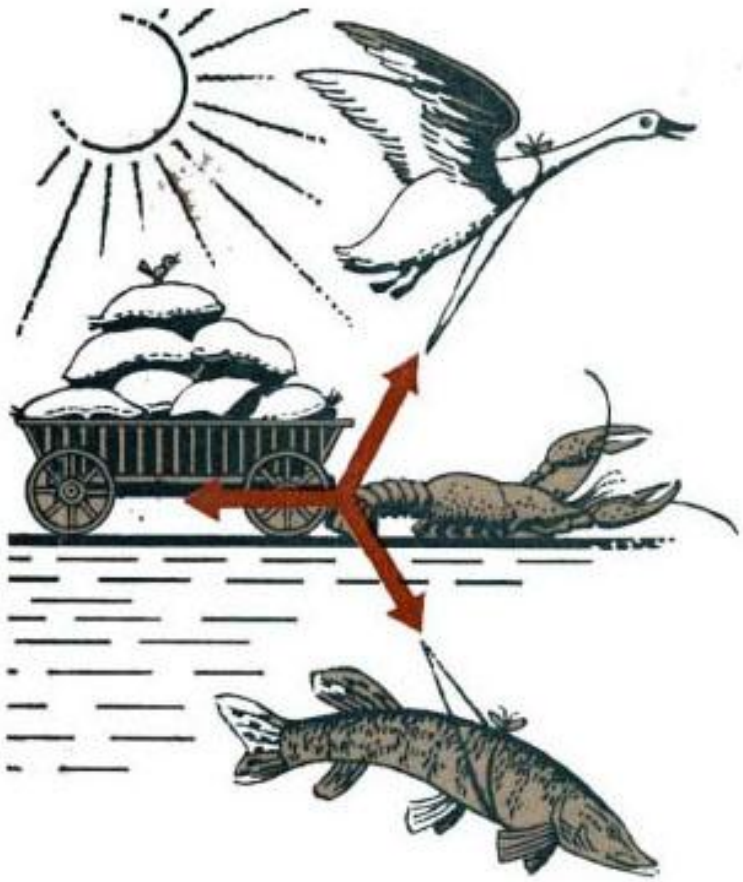
О чем пойдет речь?

- Зачем нужна архитектура ИБ?
- Что такое архитектура ИБ?
- Место архитектуры ИБ в программе ИБ
- Особенности разработки архитектуры ИБ

Зачем нужна архитектура ИБ?

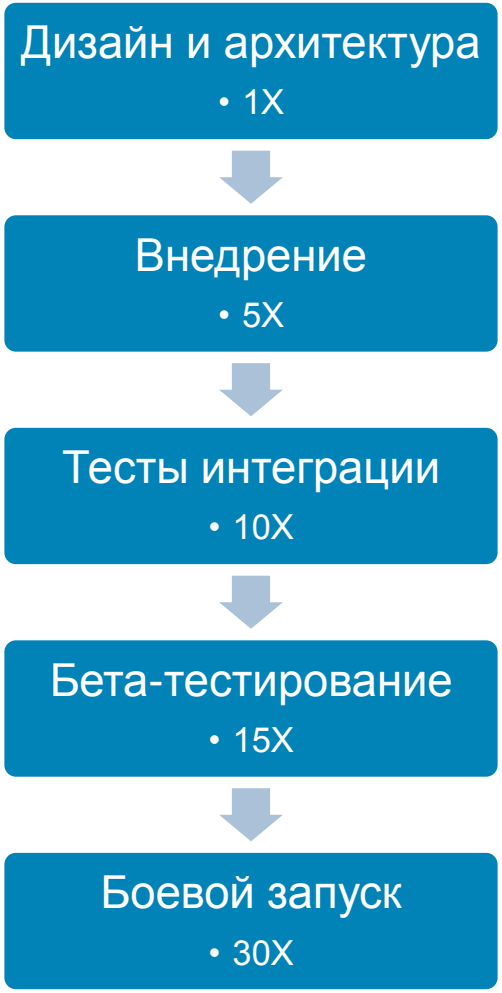
Технологические проблемы

- Отсутствие стандартизации и унификации
  - Лебедь, рак и щука
- Повтор и избыточность
  - Не путать с резервированием
- Рост ресурсо-затрат
- Упущения неочевидных вещей
- Отсутствие планов развития
- Отсутствие интеграции с ИТ и бизнесом

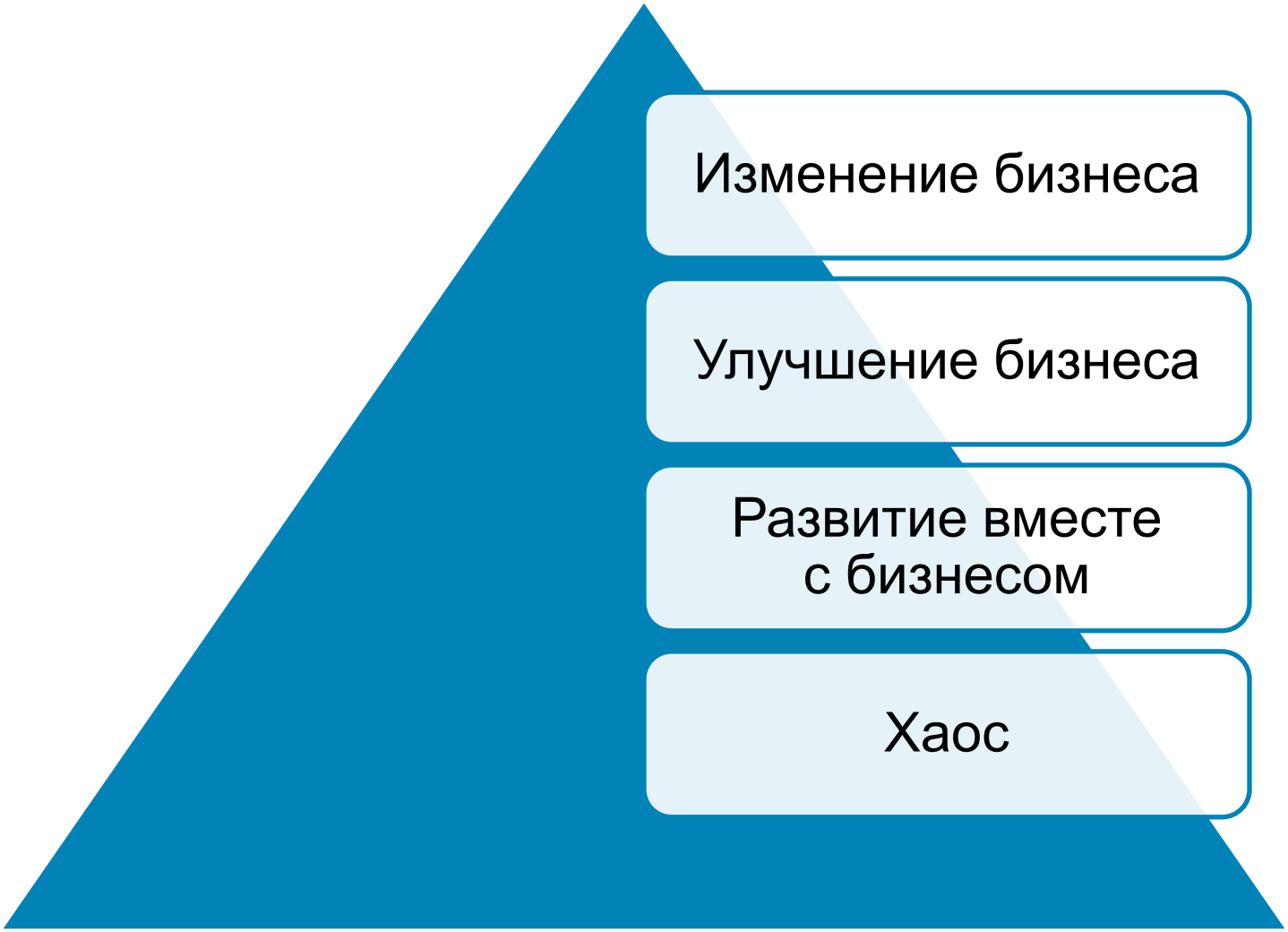


Бизнес-проблемы

- Финансирование по остаточному принципу
- Неудовлетворенность пользователей
- Потенциальные наезды со стороны регуляторов
- Неэффективность ИБ в виду забывчивости в отношении некоторых направлений бизнеса
- Несогласованность отделов



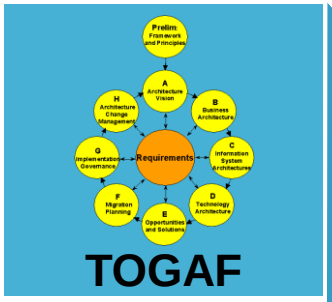
Отсутствие привязки к бизнесу



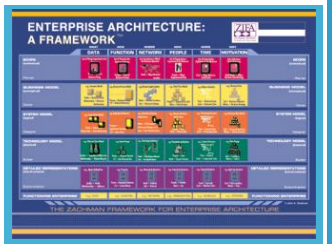
Как связать безопасность и бизнес?

1. Оценка текущей ситуации с ИБ
   - Как есть
2. Анализ потребностей бизнеса своей компании
   - Стратегические цели и тактические задачи
   - Бизнес-среда
3. Планирование будущей архитектуры ИБ
   - Как надо
4. Анализ разрыва
5. Способы сокращения разрыва
   - Стратегия ИБ

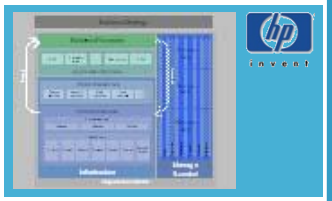
Разные архитектуры

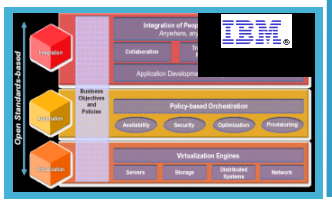


TOGAF

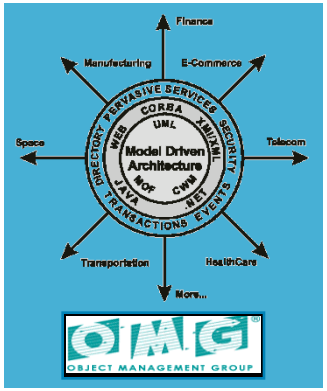


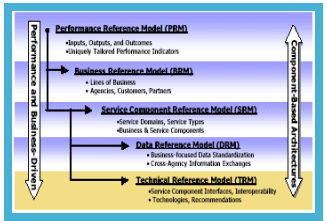
Zachman Framework



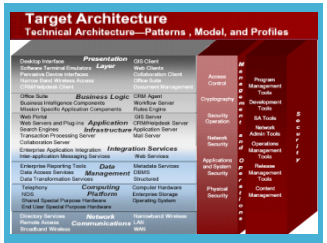


ИТ-архитектура – каркас для деятельности ИТ-подразделения





Federal Enterprise Architecture



Homeland Security

Архитектура ИБ

Архитектура ИБ

- Архитектура ИБ существует всегда

  Мы не всегда знаем об этом, мы не всегда грамотно ее используем…

- Архитектура описывает желаемую структуру инфраструктуры безопасности организации и других связанных с ИБ компонентов и интерфейсов

  Включает процессы, людей, техологии и разные типы информации

Архитектура ИБ обеспечивает

- Путь оценки новых технологий, продуктов и сервисов
- План для развития приложений и инфраструктуры
- Каркас для принятия решений в области ИБ, а также для планирования, дизайна и внедрения
- Метод для снижения издержек
- Макровзгляд на системы и компоненты ИБ
- Метод для создания и документирования консенсуса
- Направление движения для ИТ с точки зрения ИБ

Архитектура ИБ обеспечивает (продолжение)

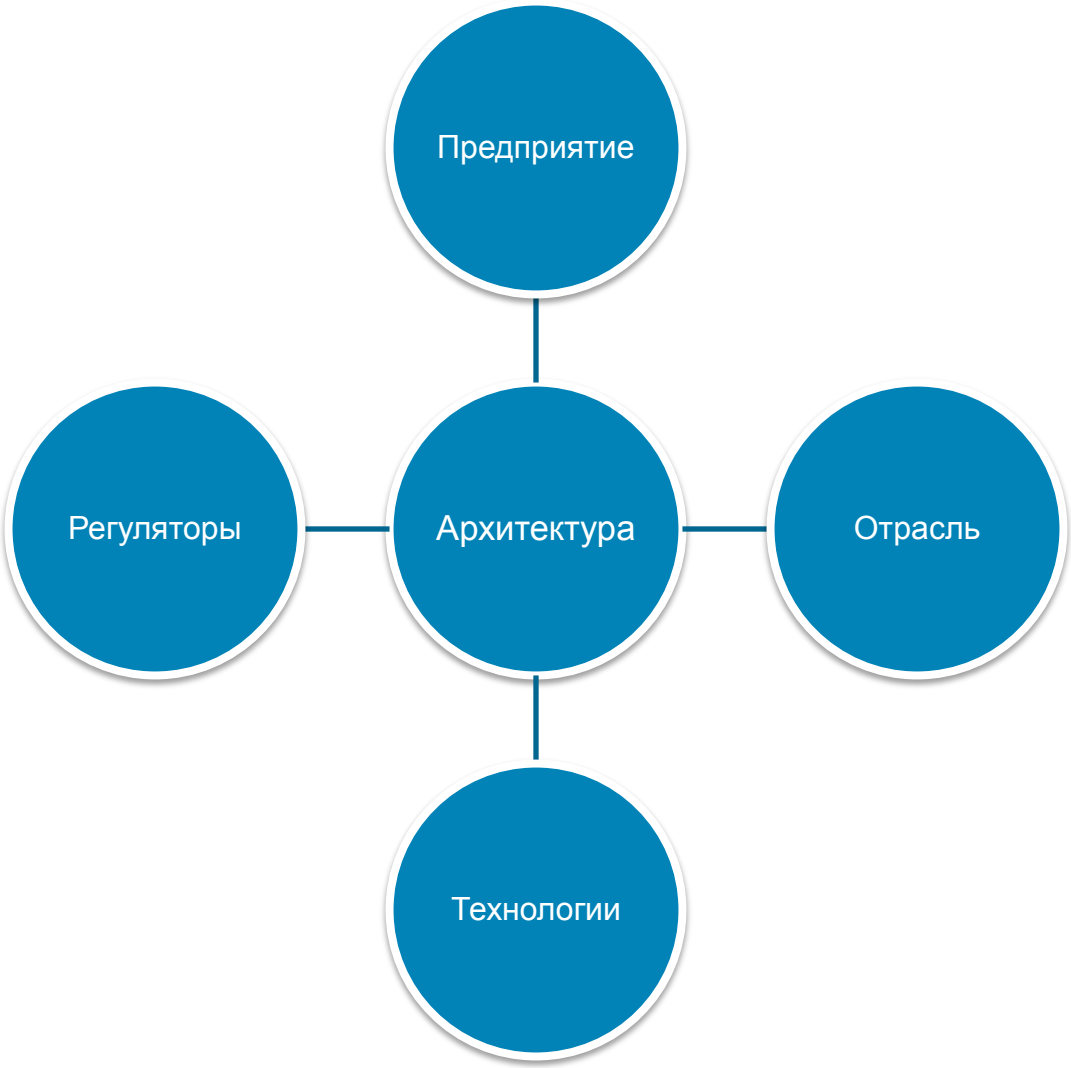
- Путь снижения проектных и технологических рисков
- Руководство к созданию стандартов и инфраструктуры для новых, ранее непредвиденных приложений
- Путь к совместимости и непротиворечивости разных систем

Содержание архитектуры ИБ

Содержание архитектуры ИБ

- Бизнес
- Информация
- Инфраструктура
- Информационные системы
- Риски и угрозы
- Информационная безопасность
- ИБ-служба

Факторы влияния на архитектуру



3 горизонтальных уровня архитектуры

- Технологический уровень обычно проработан лучше всех
  - По сравнению с 2-мя другими уровнями

3 вертикальных уровня архитектуры

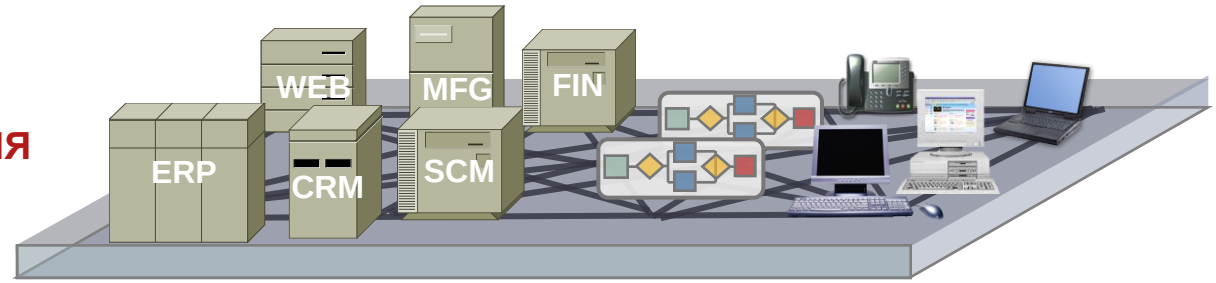
БИЗНЕС, ЛЮДИ

- M&A
- ПЕРСОНАЛ
- СОВЕТ ДИРЕКТОРОВ
- ЛОЯЛЬНОСТЬ КЛИЕНТОВ

ИНФОРМАЦИЯ

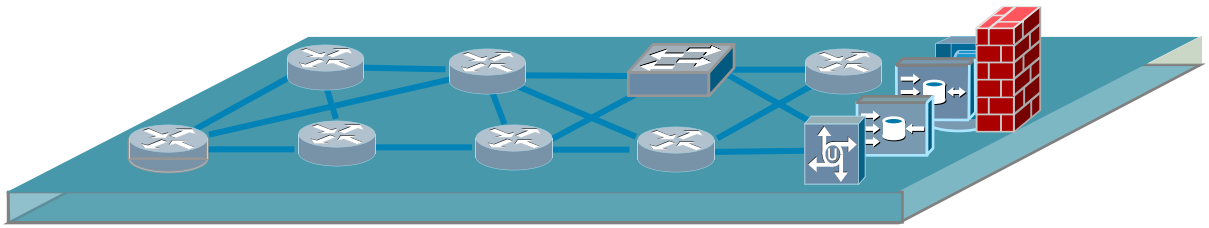
- РЕЧЕВАЯ ИНФОРМАЦИЯ
- ВИДЕОКОНФЕРЕНЦИИ
- НОСИТЕЛИ
- ФАЙЛЫ и ПОЧТА

ПРИЛОЖЕНИЯ



- ERP
- XML
- ДОКУМЕНТООБОРОТ
- БИЗНЕС-ПРОЦЕСС

СЕТЬ



- МЕЖСЕТЕВЫЕ ЭКРАНЫ
- СИСТЕМЫ ПРЕДОТВРАЩЕНИЯ
- VPN
- АНТИВИРУСЫ

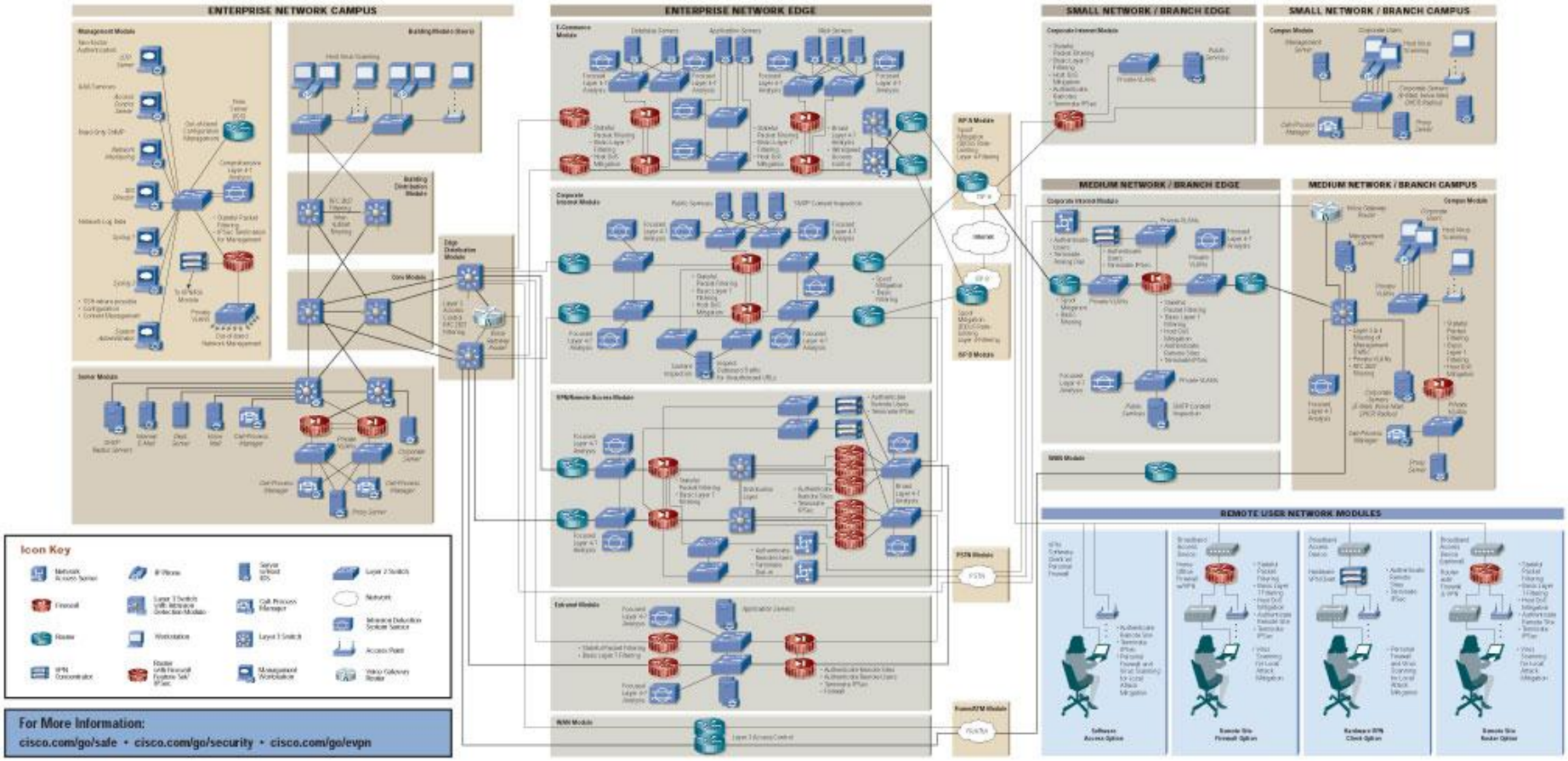
Разное представление информации

- Речевая информация
- Информация, обрабатываемая техническими средствами
- Информация в виде информативных электрических сигналов
- Информация в виде физических полей
- Носители на бумажной, магнитной, оптической и иной основе
- Информационные массивы
- Базы данных

7 элементов стратегического уровня

- Уровни доверия
  - Ограничения бизнеса, риски, взаимодействия с другими…
- Концептуальные дизайны и модели
  - Например, «ЛВС – DMZ – Интернет»
- Система взглядов на политики безопасности
  - Иерархия, примерный состав и т.п.
- Система взглядов на классификацию информации
- Процессная модель
- Модель стратегических ролей и ответственности
  - Владельцы, управленцы, «эксплуататоры»…
- Миссия ИБ

Концепция защищенного дизайна

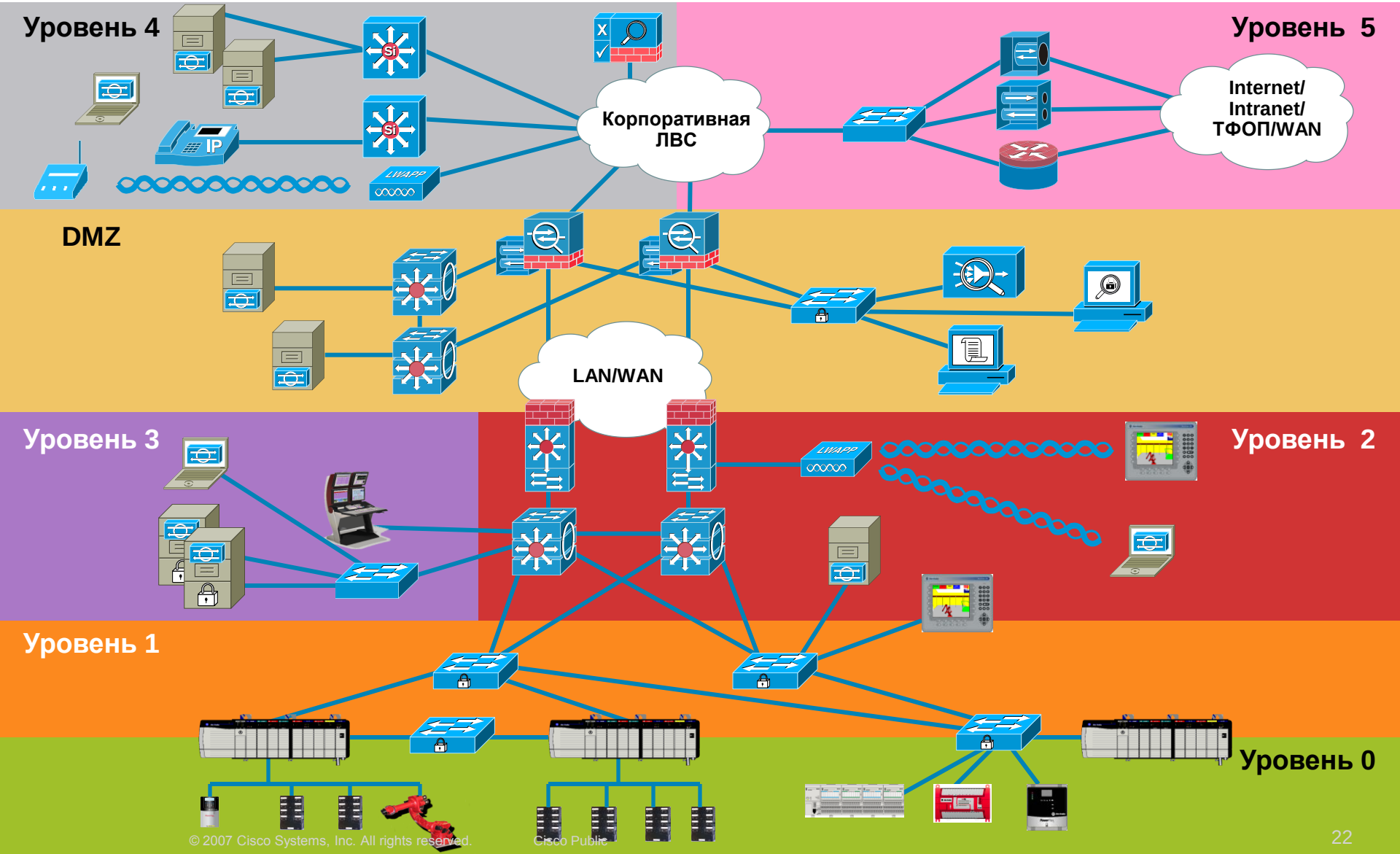


Загрузить брошюру «Cisco SAFE» можно на сайте my.cisco.ru

7 элементов логического уровня

- Сервисы безопасности
  - Какие сервисы помогают достичь уровней доверия
- Модель доменов доверия
  - Группирование ресурсов на основе общих критериев
- Принципы дизайна защищенной инфраструктуры
  - Разделение полномочий, ролевое управление и т.п.
- Модели дизайна
  - Декомпозиция моделей верхнего уровня
- Модель информационных потоков
- Организационные модели
- Шаблоны требований

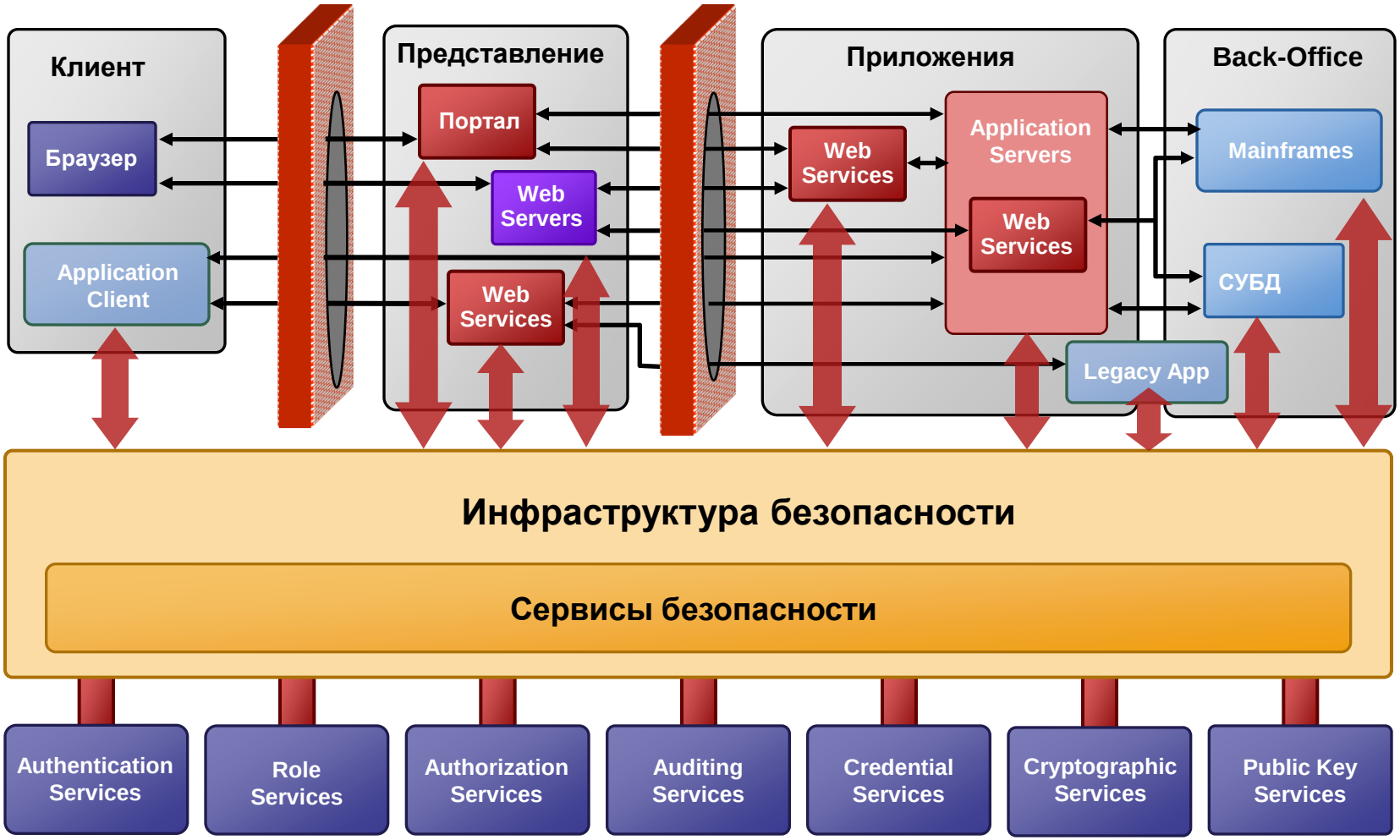
Домены доверия АСУ ТП



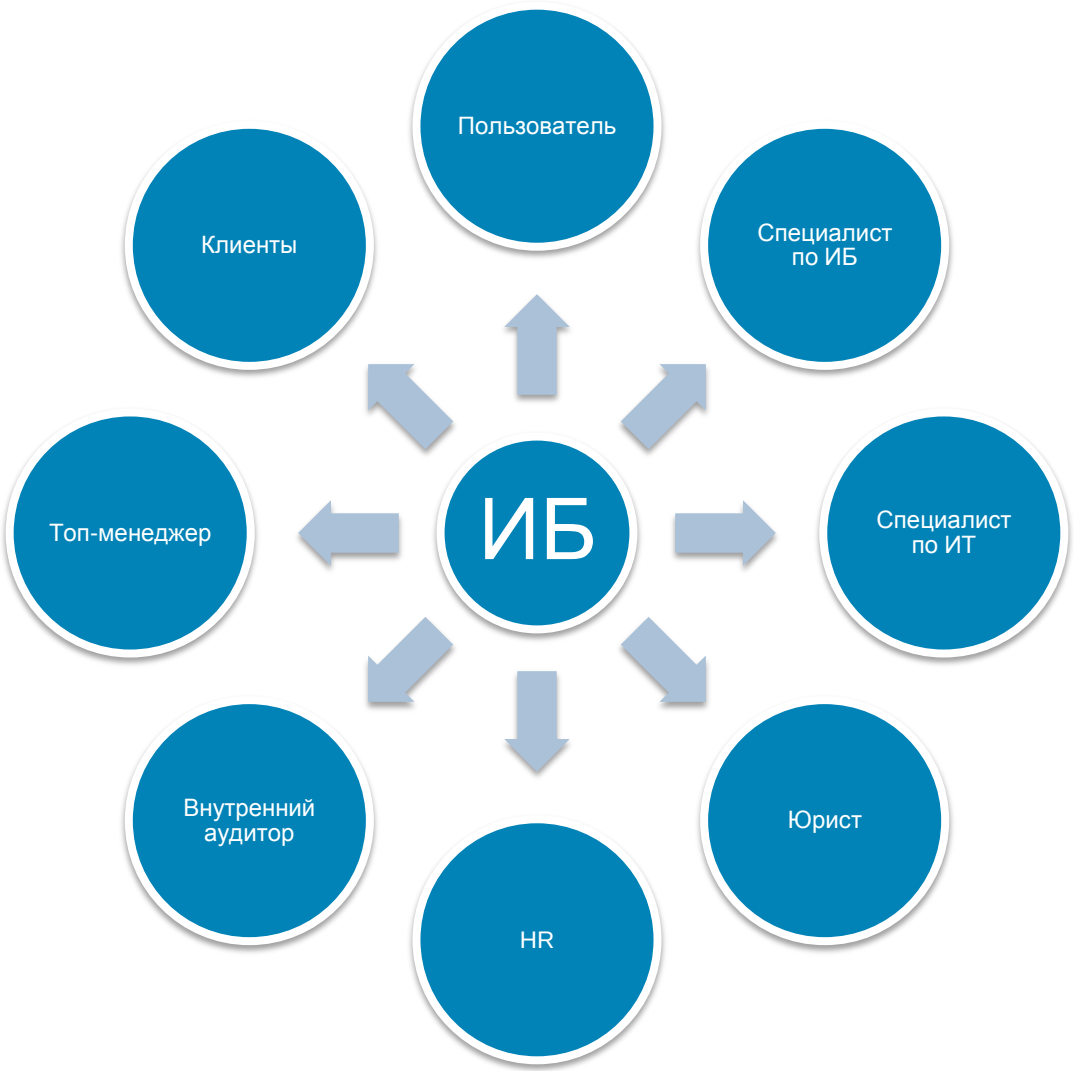
7 элементов технологического уровня

- Архитектура безопасности приложений
  - Включая ERP, CRM, SCM, SCADA
- Архитектура сетевой/инфраструктурной безопасности
  - Не забывать про интегрированные функции
- Архитектура сервисов безопасности
- Классификатор защищаемой информации
- Архитектура управления безопасности
- Принципы стандартизации и унификации ИБ
- Организационная архитектура
  - Должностные обязанности, повышение осведомленности…

Сервис-ориентированная архитектура



8 точек зрения на архитектуру

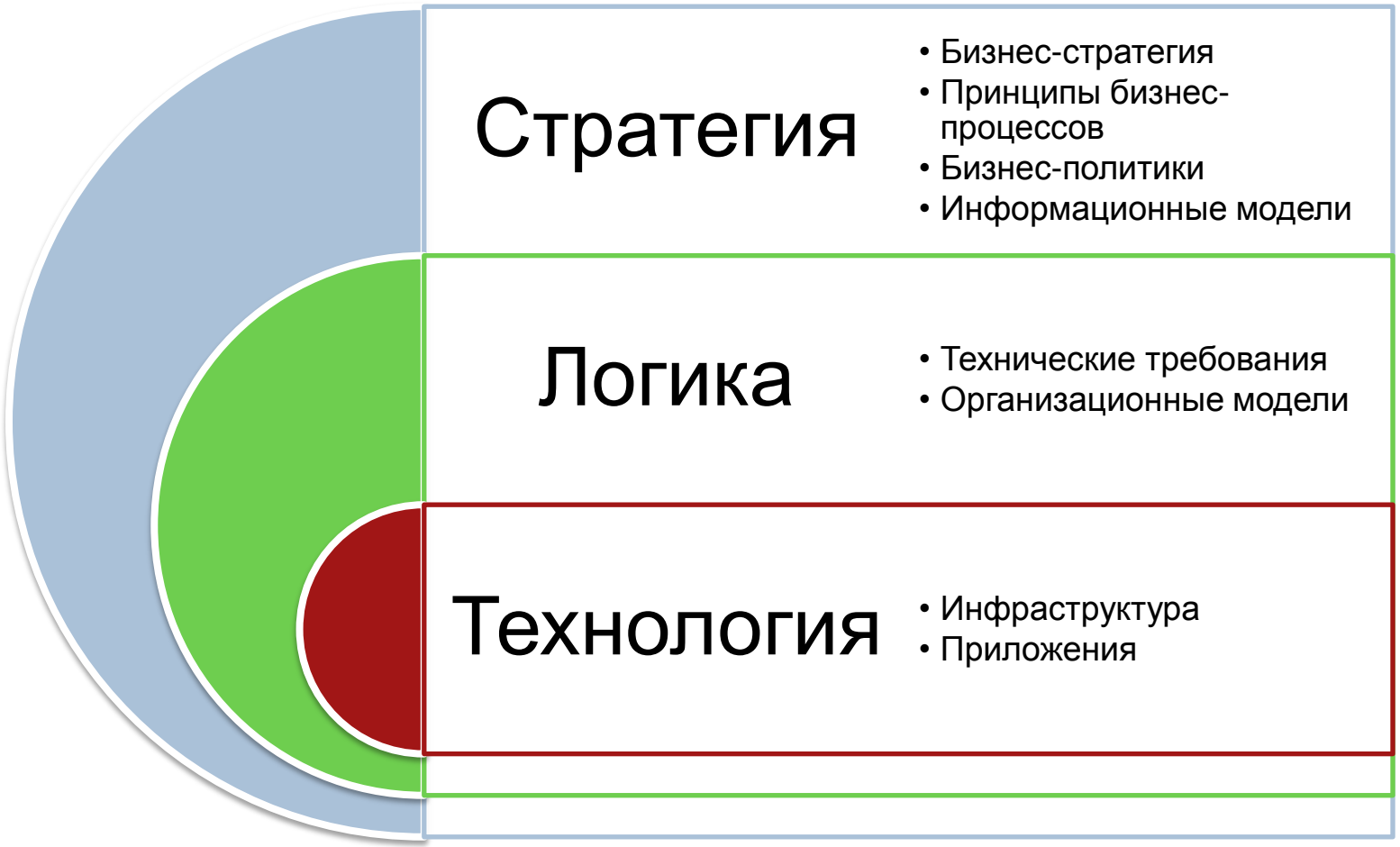


Особенности разработки архитектуры ИБ

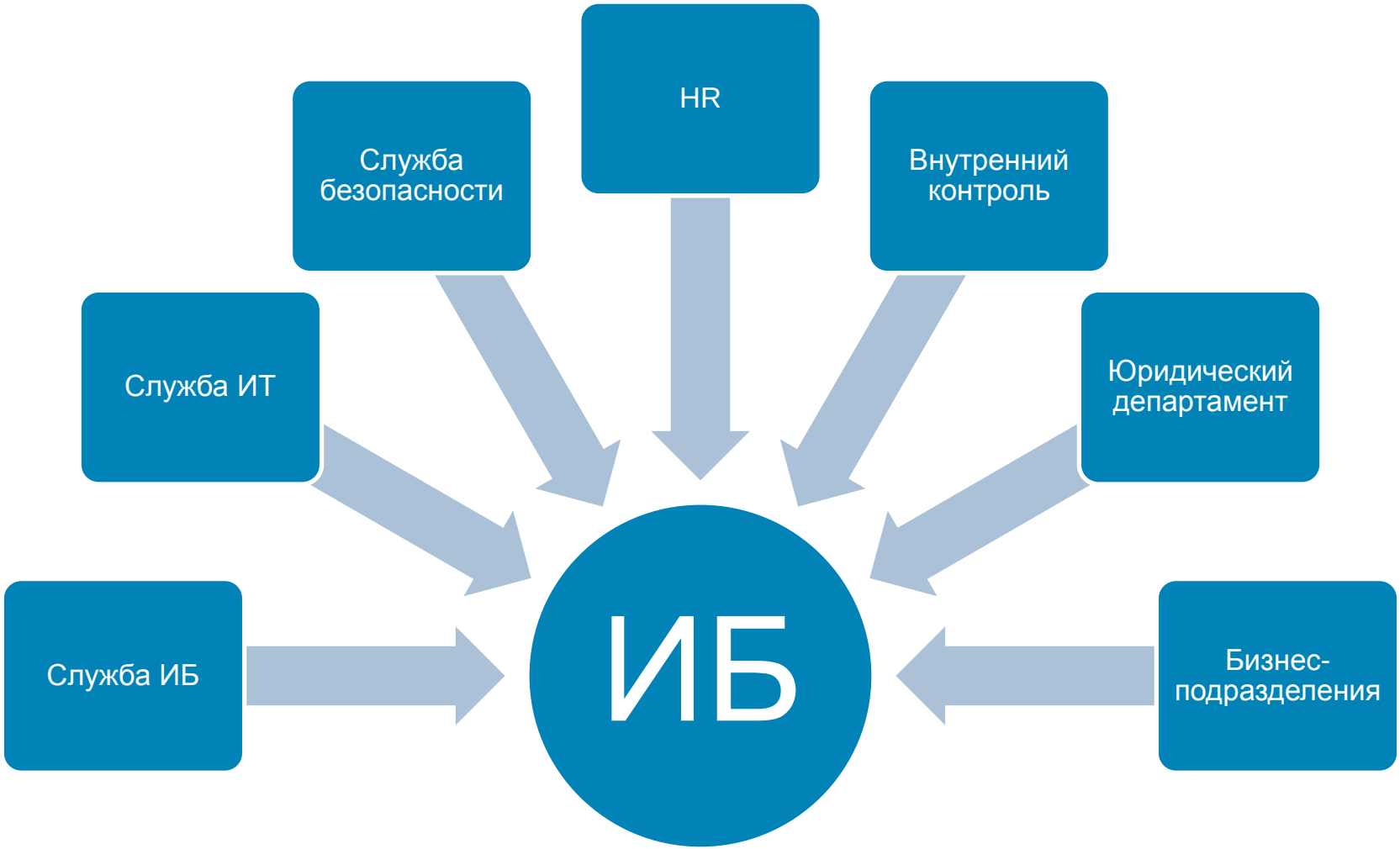
Этапы разработки архитектуры ИБ

1. Определение бизнес-кейса
2. Создание команды
3. Сбор информации для архитектуры ИБ
4. Бизнес-требования и драйверы к архитектуре
5. Gap-анализ
6. Разработка финальной архитектуры
7. Разработка стратегии миграции
8. Определение процесса пересмотра архитектуры

Изоляции нет!



Участие в разработке архитектуры ИБ



Разработка архитектуры ИБ

- Чем сложнее архитектура, тем больше вероятность ошибки
- Лучше делать упор на методах снижения риска, чем на технологиях и продуктах

  Обучение, физическая безопасность, реинжиниринг процессов, PR и т.д.
- Архитектура может охватывать как один проект или подразделение так и всю компанию

  Но… ни проект, ни подразделение не могут быть полностью изолированы

Не только технологии

- Достичь нужного состояния ИБ можно путем использования разных мер:
  - Практика управления
  - Политики
  - Стандарты
  - Процедуры
  - Документация
  - Практика аудита
  - Тестирование безопасности

Не только технологии (продолжение)

- Достичь нужного состояния ИБ можно путем использования разных мер:
  - Физическая безопасность
  - Безопасность персонала
  - Управление инцидентами
  - Юридические меры
  - Повышение осведомленности
  - Организационная структура

Российская специфика

Российская специфика

- Рынок продуктов ИБ не развит

  Все решается классической связкой «МСЭ + AV + VPN + IPS + сканер безопасности»

- Приоритет отдается техническим мерам
- Масштаб страны
- Низкий уровень проникновения best practices
- Большое количество регуляторов в области ИБ и несогласованность их действий
- Концентрация усилий на консалтинге и внедрении средств защиты в ущерб security operations

Концепция или архитектура

Концепция

- Сотни страниц
- Что и как надо делать
- Безопасники для безопасников
- Монолитный документ
- Отсутствие бизнес-привязки
- Отказ от учета мнения стейкхолдеров

Архитектура

- 30-50 страниц
- Зачем это надо делать
- Документ для всех стейкхолдеров
- Главный документ и подмножество политик и т.п.
- Бизнес превыше всего

Заключение

Преимущества архитектуры ИБ

- Понимание «куда бежать» и «что делать»
- Отсутствие излишней избыточности и повторов
- Отсутствие противоречивости
- Эффективная трата времени на управление ИБ
- Интеграция с ИТ и бизнесом
- Охват всех аспектов деятельности предприятия

Вопросы?

Дополнительные вопросы Вы можете задать по электронной почте security-request@cisco.com
или по телефону: +7 495 961-1410