KPMG

Функционирование и эффективность ИТ. Новые вызовы

Бишкек, 25 февраля 2016

СОДЕРЖАНИЕ

KPMG

Новая операционная модель ИТ

Технологический прорыв как мотивация к изменениям

Прорыв и неудовлетворенные ожидания

Технологии

Непрерывное продвижение технологий вперед

- Привлекательные и доступные решения

Планируй → Строй → Веди

Типичная ИТ организация

- Поддерживают сложные, дорогостоящие и недостаточно эффективные решения
- Морально устаревшие процессы, навыки, культура

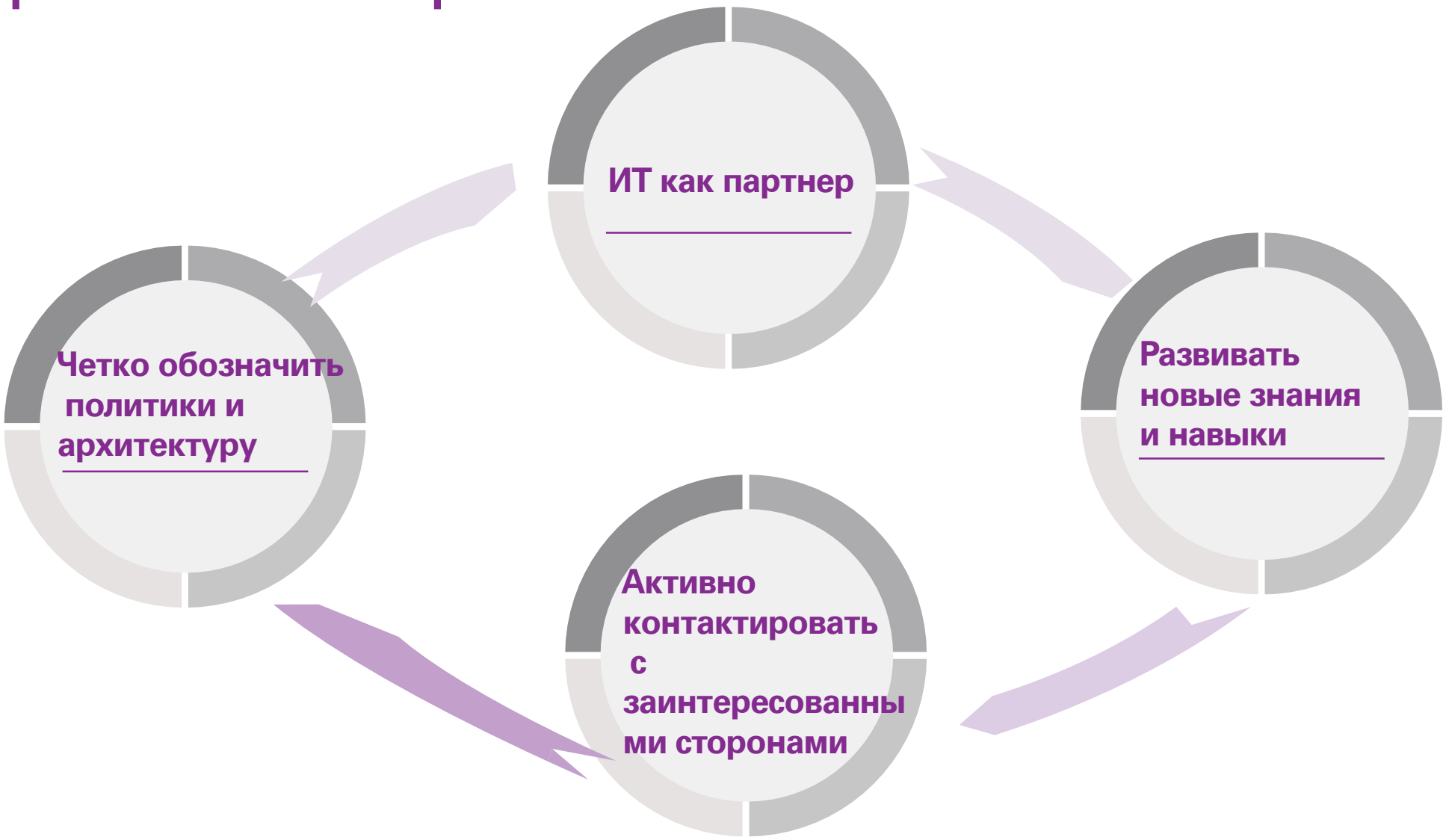
Обычный пользователь

- ИТ-грамотность
- Нетерпение

Неудовлетворенные ожидания

- Инновации
- Оперативность
- Эффективность
- Бизнес-ориентированность

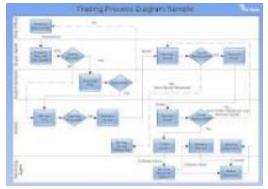
ИТ организации должны улучшать взаимодействие с заинтересованными сторонами



Новая операционная модель ИТ

Посредничество, Интеграция, Руководство

Основные компоненты операционной модели



•Структура ИТ

Функции и процессы

Взаимодействие между функциями

•Организационная структура

•Структура управления включая RACI

Должностные инструкции

•Управление людьми и вспомогательные процессы

•Навыки и способности планирования и развитие

•Развитие организации

•Технологическая инфраструктура

•Ландшафт приложений

•Поддерживающие инструменты

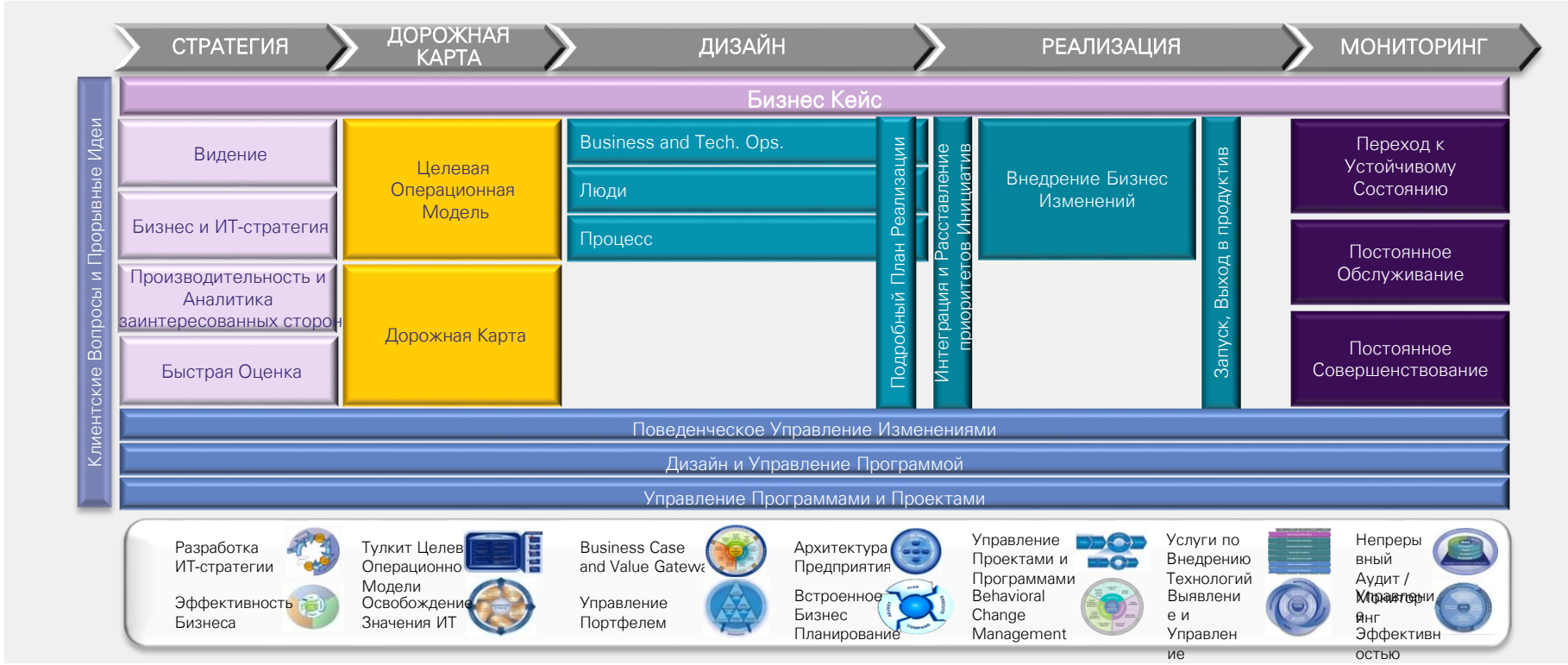
Определение KPI

•Модель сорсинга

•Стратегия местоположения

•Предпочтительные поставщики

Подход к построению целевой операционной модели ИТ. Основные этапы.



Цифровая трансформация

Технологии для новой операционной модели ИТ

Цифровая волна – Центральный взгляд

1

Коммерческое внедрение

Выбор, внедрение и интеграция полномасштабных технологических продуктов и платформ, представляющих ROI (SAP, Oracle, Workday, Service Now, Appian и др.) играют основную роль.

2

Ранняя мобилизация

За последние пять лет, наши клиенты начали закладывать основы, необходимые для мобильности своих компаний, включая BYOD (Bring your own devices), MDM (Master data management), федеративная безопасность, удаленный доступ, виртуализация, корпоративный склад приложений.

3

Ориентация на клиента

Век Клиента возвестил о необходимости большего числа технологий для клиентов.

4

Переход на цифровые технологии

Новые системы записи, корпоративная инфраструктура и выстраивание бизнеса с нуждами клиентов, переработанные через аналитику создали новый уровень для использования цифровых технологий.

5

Рационализация

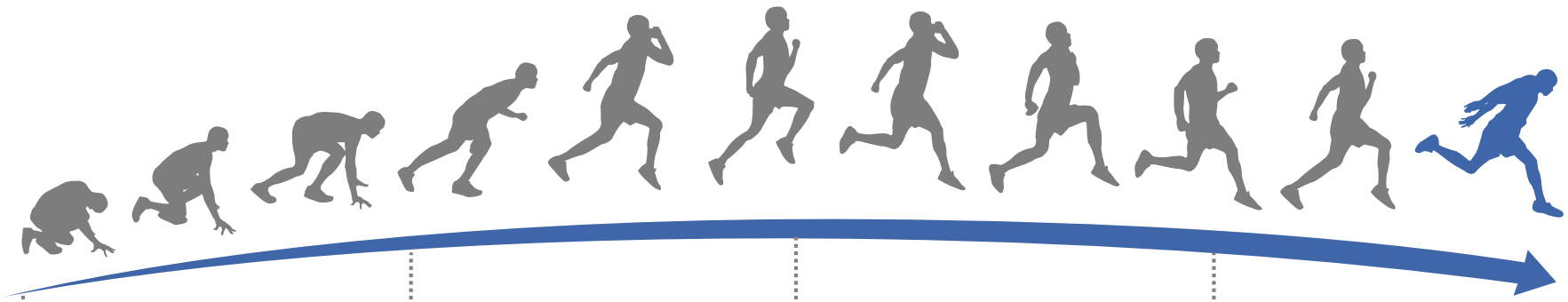
Рыночное и технологическое давление заставляют информационные технологии изменять организации, управление и архитектуру технологий для того, чтобы предоставить возможность использования новых технологий.

6

Трансформация

Цифровая трансформация, инновации и ускорение требует единую бизнес стратегию, новые операционные модели и бизнес процессы, ориентированные на людей.

Уровень развития цифровых технологий в банках



30%

Контент

Ранняя фаза присутствия в Интернете с использованием статической информации на веб-сайте. Присутствует ограниченое взаимодействие с клиентами.

50%

Взаимодействие

Повышенное внимание к созданию постоянных отношений с клиентом, через популярные социальные медиа ресурсы

20%

Коммерция

Монетизация отношений и цифровых инвестиций путём прямых продаж через цифровые каналы, например, по средствам электронной коммерции, онлайн-платежей и т.д.

0%

Сотрудничество

Тесное сотрудничество клиентов с банками, участие клиентов в формировании продуктов и услуг, оптимизация бизнес-процессов и т.д.

ZhongAng – китайская электронная страховая компания, подбирающая продукты автострахования в зависимости от активностей пользователя в магазине Alibaba, игровых сайтах, социальных сетях.

Avant – одна из наиболее прибыльных компаний Чикаго, постоянно пополняющая базу клиентов за счет персонифицированных предложений по кредитованию на определенные цели. Поиск и взаимодействие с клиентами осуществляются автоматически.

Atom – великобританский банк, представленный исключительно мобильными приложениями.

Lufax – китайская электронная платформа для оценки рисков инвесторами, основываясь на анализе больших данных из социальных сетей, открытых публикаций, финансовых отчетов и собственных баз. Моделирование рисков происходит практически мгновенно.

FinTech в 2015 – это:

25% - инновационные платежные системы

22% - альтернативные виды кредитования

14% - технологические решения в области управления активами

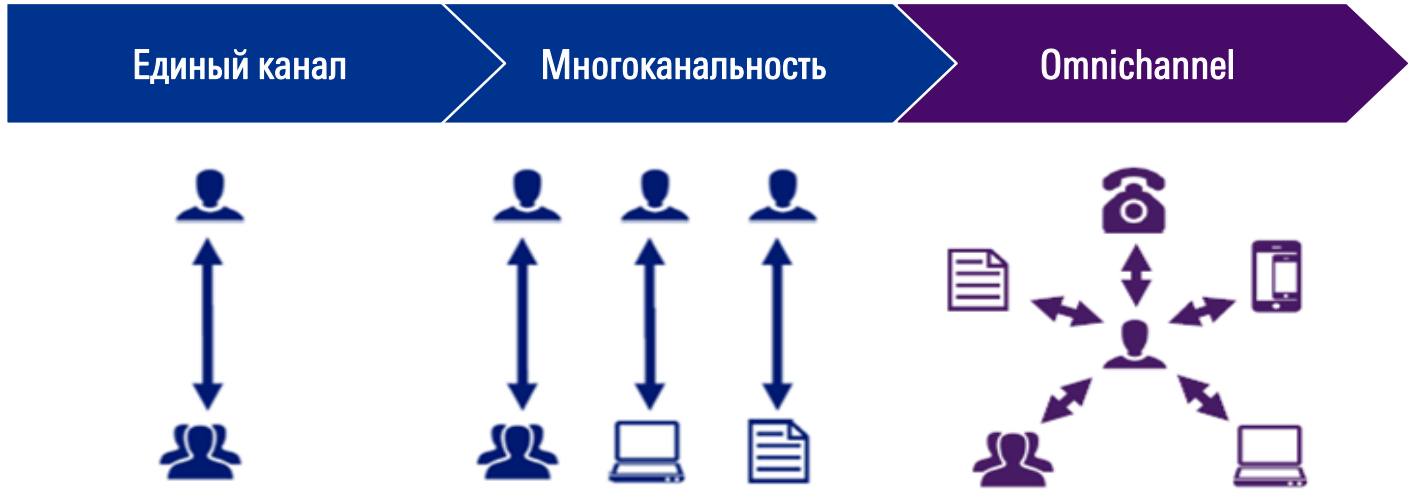
7% - решения для страховых компаний

Источник:The 100 Leading Fintech Innovators Report, KPMG & H2 Ventures

Примеры цифровых решений

Что такое omni-channel?

Дать клиентам сервис, который они хотят, через каналы доступа, которые они хотят



	Единый канал	Многоканальность	Omnichannel
Клиент	▪ Единая точка входа для клиента	▪ Клиент может взаимодействовать через разные каналы, но пользовательский опыт при этом не сохраняется	▪ Клиенту предлагается согласованный пользовательский опыт по всем каналам
Канал	▪ Предлагается только один канал	▪ Все каналы работают независимо друг от друга	▪ Все каналы интегрированы, поддерживается единый взгляд на опыт клиента

Пример

- Одновременное использование двух каналов, например, call-center и вебсайт
- Переключение между каналами
- Возможность начать процесс в одном канале и продолжить в другом

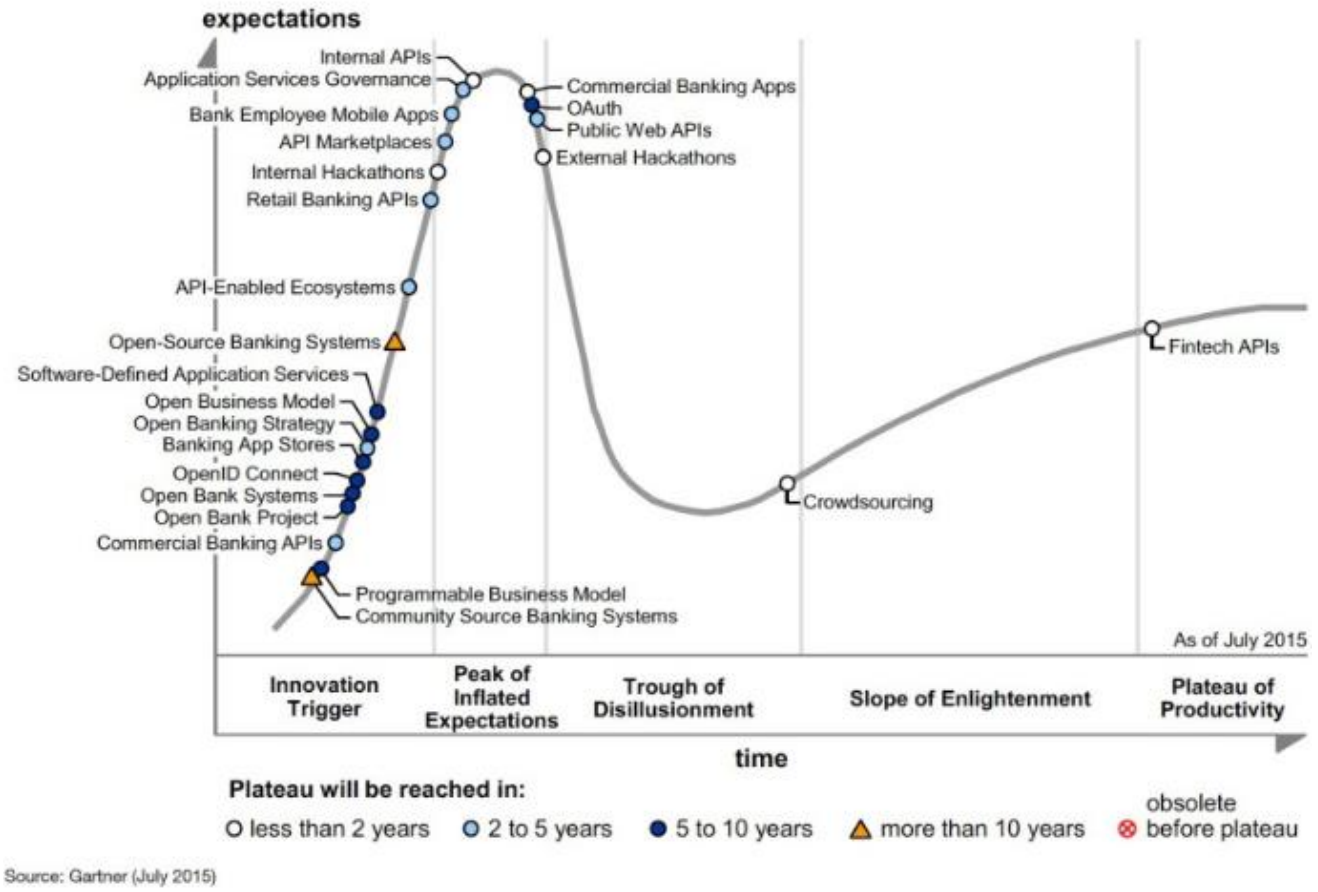
Основные характеристики модели omni-channel

Основные характеристики	Описание
1 Единый опыт клиента во всех цифровых и традиционных каналах	▪ Возможность начать процесс в одном канале и закончить в другом. Клиентский опыт предоставляемый через все каналы синхронизирован.
2 Единый взгляд на клиента и понимание его потребностей	▪ Интеграция корпоративных данных должна позволять в реальном времени предоставлять информацию к текущей информации о клиенте и клиентском опыте. ▪ Динамическая модель сегментации клиентов для постоянной оптимизации персональных предложений.
3 Организационные изменения	▪ Корпоративная культура и организационная модель открыты к постоянному изменению целевой организационной модели, основная цель изменений изменяющиеся требования клиента и возможности новых технологий
4 Открытость к инновациям	▪ Открытость к инновациям и краудсорсингу для того, чтобы совместно развивать цифровые возможности. Открытие инновационных центров инвестиции в технологические стар тапы.
5 Консьюмеризация корпоративных приложений	▪ Интерфейс должен быть интуитивно понятным не только для клиентов, но и для пользователей корпоративных приложений.
6 Ценообразование должно быть консистентным для всех каналов продаж - цифровых и традиционных	▪ Ценообразование должно быть консистентным для всех каналов и продуктов. ▪ Не повышать цены за использование более дорогих каналов, а наоборот бонусировать за использование предпочтительных для банка каналов.

Цикл Зрелости технологий для Open Banking

- Согласно Gartner, к 2016 году 75% банков из топ50 откроют свои API и 25% этих банков будут иметь магазины приложений для клиентов.

Figure 1. Hype Cycle for Open Banking APIs, Apps and App Stores, 2015



Source: Gartner (July 2015)

Hype Cycle for Open Banking APIs, Apps and App Stores, 2015

- Gartner, Hype Cycle for Open Banking APIs, Apps and App Stores, 2015

Что такое Open API?

Open

- Трансграничная интеграция услуг.
- Доступ к сторонним платформам и системам с целью получения полной и сбалансированной услуги.
- Переход на новый уровень взаимодействия: внутренние силы компании+ доступ сторонним разработчикам для создания новых приложений.
- Сокращение дистанции между компанией и партнерами.

Partner

- Partner API используются для интеграции между системами группы компаний или партнеров. Способствует повышению качества получаемых услуг в рамках группы компаний.

Private

- Private API используются только внутри компании для интеграции внутренних систем.

К основным преимуществам относятся:

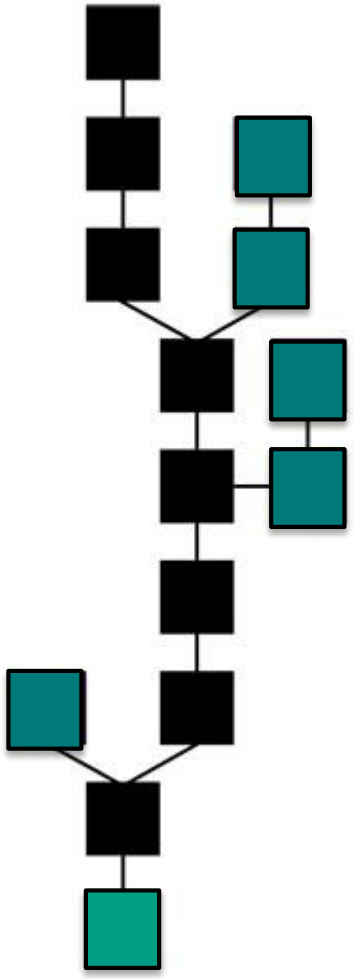
Уменьшение затрат на интеграцию систем

Уменьшение затрат на инфраструктуру

Основные характеристики концепции «open API»

Основные характеристики	Описание
1 Открытость	▪ Эффективных способов для банка включиться в экосистему и получить свежие идеи для развития бизнеса.
2 Возможность доступа к большому массиву данных	▪ Банки обладают огромными массивами данных о своих клиентах, а с увеличением числа цифровых каналов коммуникаций, возможностей применения этих данных для бизнеса становится все больше.
3 Сотрудничество	▪ Банки разрабатывают схожие по функционалу API с большими затратами. Сотрудничество с внешними разработчиками позволит уменьшить затраты на разработку приложений, расширит перечень предлагаемых услуг. В BIAN организована рабочая группа по Open API для создания единого стандарта в этом направлении. ▪ Сотрудничество с FinTech компаниями.
4 Продуктивное взаимодействие с клиентами	▪ Открытая архитектура для взаимодействия с внешними приложениями через открытые API, расширение функций CRM для работы с клиентами в реальном времени.

Что такое blockchain?



- Технология цепочки блоков, или публичного реестра, представляет собой выстроенную по определенным правилам цепочку из блоков транзакций, специальных структур для записи транзакций.
- Каждый из блоков содержит информацию о предыдущем блоке, а все блоки можно выстроить в цепочку и перепроверить всю историю всех транзакций.
- Имеет уникальные методы защиты, которые практически исключают возможность подмены отдельных записей. Децентрализованная система и у нее нет единого регулятора.
- Bitcoin основана на технологии blockchain.

Основные характеристики технологии blockchain

Основные характеристики	Описание
1 **Прозрачноть данных. Уникальные методы защиты от умышленных изменений.**	▪ Технология не позволяет целенаправленно умышленно изменить отдельные записи в блоке, так как такой блок не будет признан достоверным. Каждая транзакция криптографически привязана к предыдущей транзакции.
2 **Децентрализованная система. Нет регулятора.**	▪ Децентрализованная система и у нее нет единого регулятора. ▪ Использование технологии, чтобы не зависить от международной системы передачи финансовых сообщений SWIFT (Сбербанк).
3 **Хранение всей истории всех транзакций**	▪ Каждый из блоков содержит информацию о предыдущем блоке, а все блоки можно выстроить в цепочку и перепроверить всю историю всех транзакций.

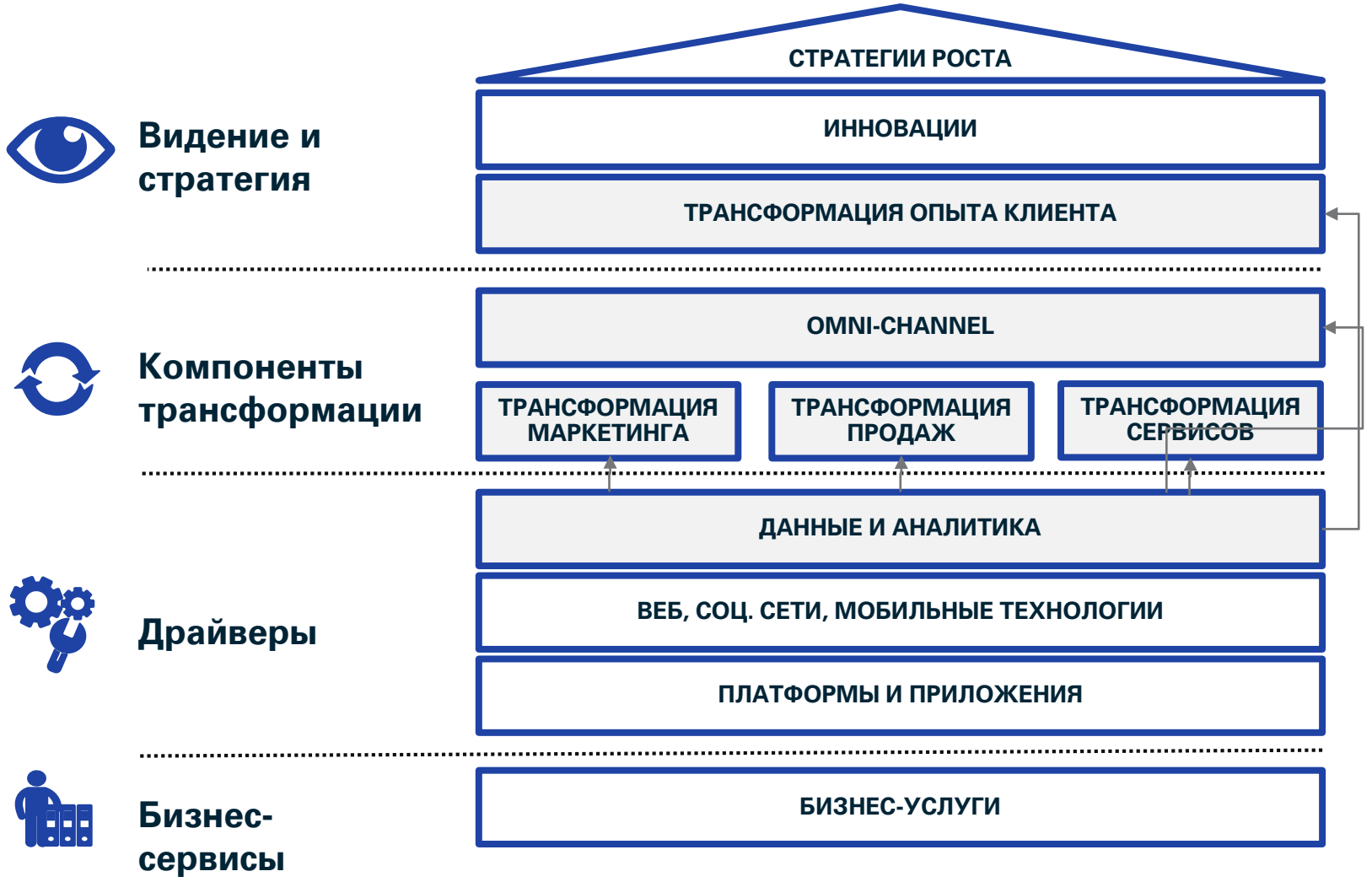
Примеры применения технологии

- Различные базы данных, кадастры, реестры, всю информацию можно перенести в blockchain. И данные будут достоверны, если они прошли через валидацию blockchain.
- Встает вопрос о необходимости в архивах, репозитариях, дополнительных системах.
- Потенциально могут быть упрощены процедуры бэкофиса банков и других учреждений, работающих с большим массивом данных, где актуален вопрос достоверности данных. Повышение безопасности транзакций.
- С помощью технологии участники надеются экономить время и деньги на выпуске ценных бумаг, денежных переводах.
- При помощи blockchain могут быть сняты часть политических рисков банков (SWIFT).
- Сокращение зависимости от бумажных носителей.

Управление жизненным циклом клиента

Цифровая трансформация организации

Концепция «В центре – КЛИЕНТ»



Под опытом клиента мы понимаем совокупность всего опыта общения с банком: знакомство, изучение продуктов и условий, привлечение, взаимодействие с сотрудниками, приобретение услуг, пользование услугами. То есть, в фокусе нашего внимания находится клиент и все отношения с ним.

Не внедрение технологий, а трансформация организации

Уровень дигитализации

Уровень дигитализации, масштабы и темпы предполагаемых изменений

Фазы изменений

Цифровые преобразования – марафон, а не спринт.

Для того, чтобы уменьшить риски, связанные с «цифровой» трансформацией, организациям следует рассмотреть фазы изменений, необходимые для достижения уровня амбиций в рамках организационной готовности и способности к изменениям.

Стратегия

Видение	Стратегия	Лидерство

Организационная структура и управление

Организационная структура	Модель управления и отчетность	Культура и управление изменениями	Привлечение ресурсов

Опыт клиентов

Стратегия	Многоканальная система	Потребности потребителей

Операции

Обеспечение ресурсами	Инновационные продукты и услуги	Автоматизация и сквозная обработка

Данные и аналитика

Данные (Single Customer View and MDM)	Взаимодействие	Сегментация и анализ	Интеграция

Технологии

Технология и архитектурный план	Платформа и инфраструктура	Технологии рабочего места

Ключевые аспекты трансформации

РОСТ

Цифровая корпорация

- Управление знаниями и совместной работой (внутренние социальные сети)
- Обеспечение кадровыми ресурсами
- Производительность / улучшение процесса
- Управление контентом, дизайн, внедрение и интеграция
- Повышение квалификации персонала

Взаимодействие с клиентом

- Концепция, ориентированная на клиента
- Привлечение и удержание клиентов
- Более глубокое понимание клиентов (отчетности и аналитика)
  - Многоканальная стратегия (Omni-channel)
  - CRM, CMS - автоматизация
  - Оптимизация использования клиентского опыта

ВНУТРЕНИЕ

ВНЕШНИЕ

Вспомогательные технологии

- Средства совместной работы
- CRM
- Бизнес-аналитика
- Автоматизация маркетинга
- Финансовые системы
- Мобильные и платежные платформы
- Электронная коммерция

Меркантильность и управление

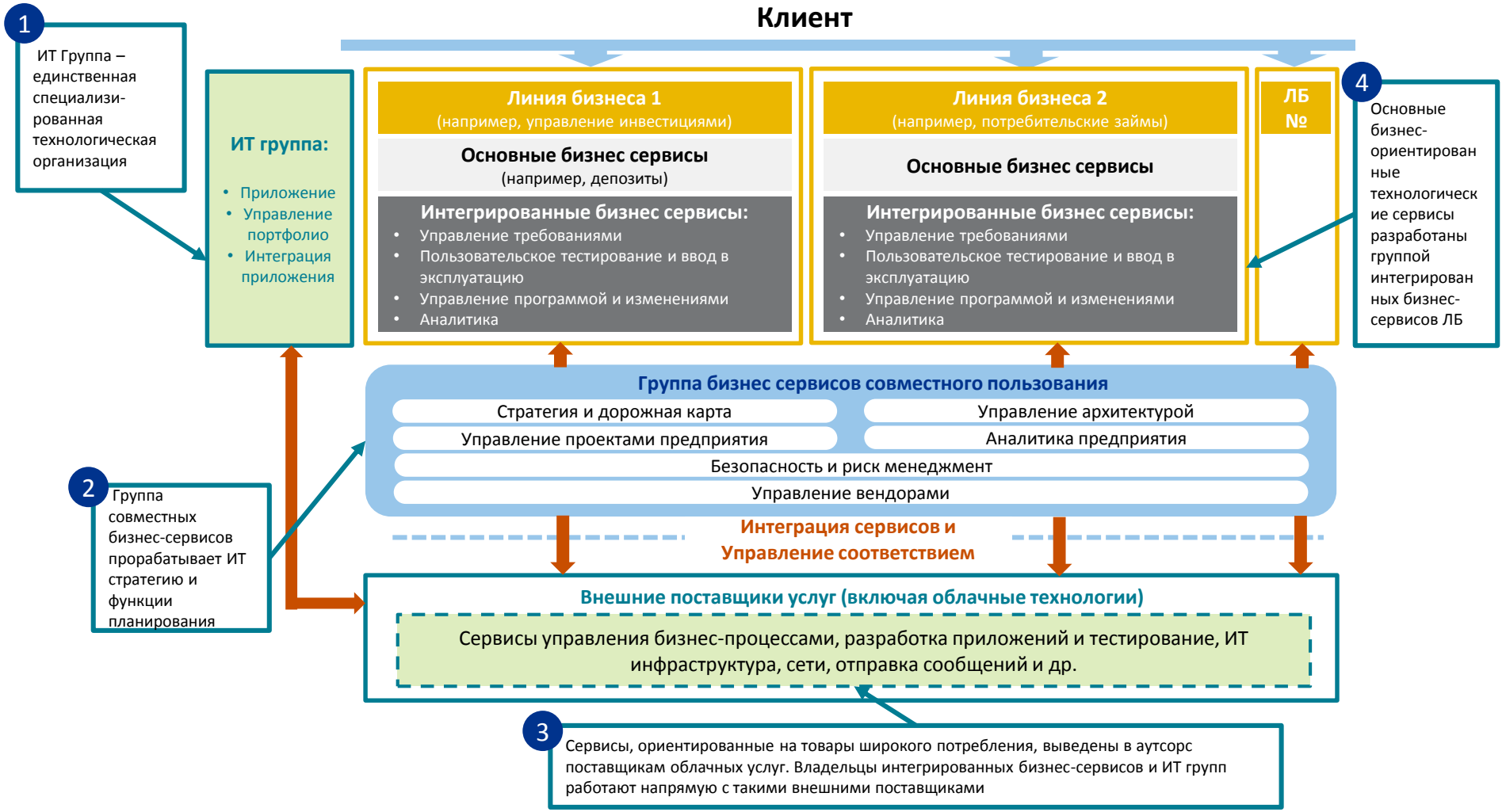
- Целостная модель управления
- Защита ценностей (бренд, репутация)
- Совершенствование процессов
- Управление рисками
- Развитие бизнеса и моделирование стоимости
- Технико-экономическое обоснование
- Управления информацией в режиме реального времени

Мобильные устройства

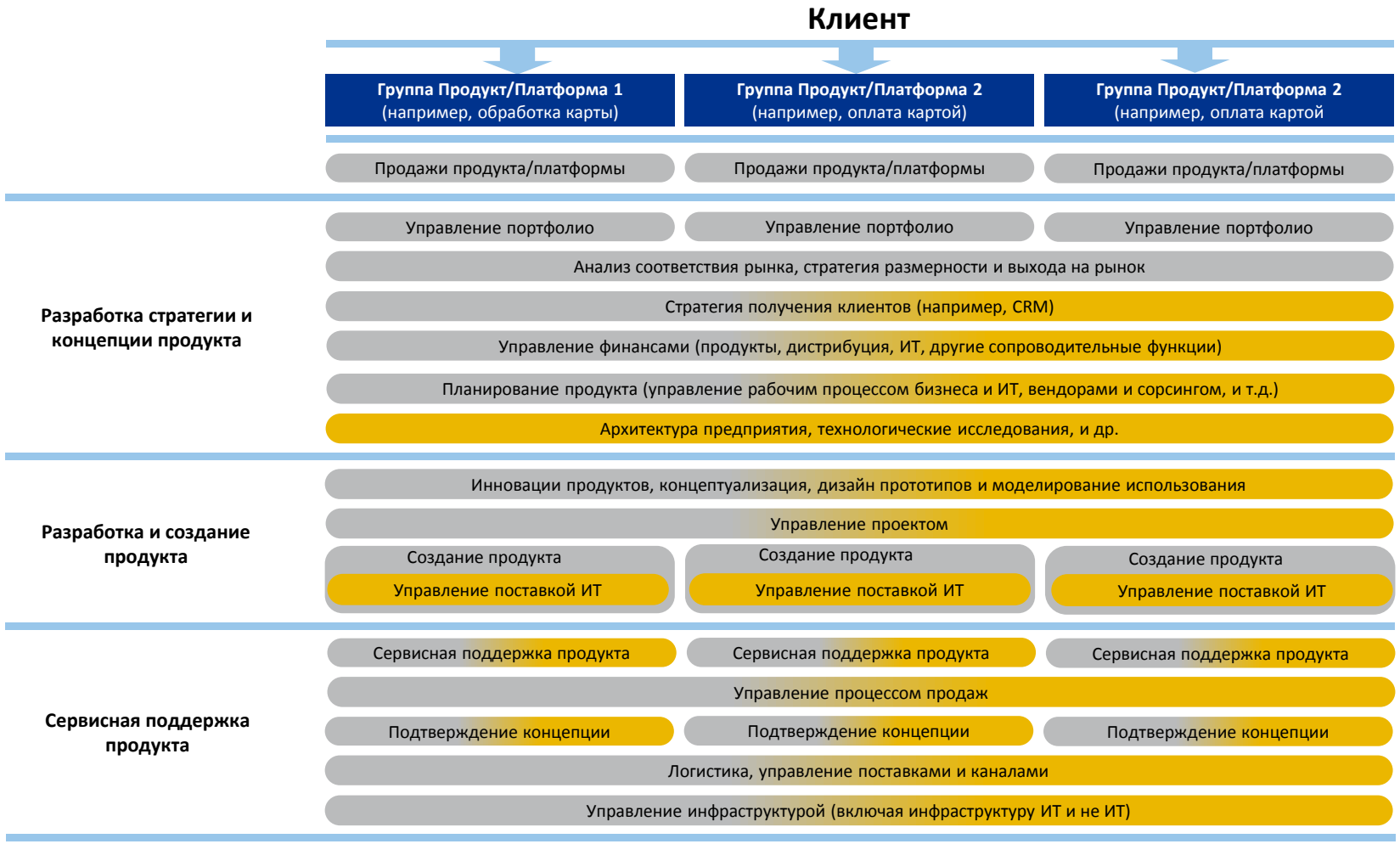
- Стратегия развития в области мобильных устройств
- Опыт клиентов как стимул развития
- Прочные разработки, тестирование и эксплуатация
- Безопасность, приватность и соответствие
- Обеспечение торговым персоналом
- Преобладание мобильных технологий

ЭФФЕКТИВНОСТЬ

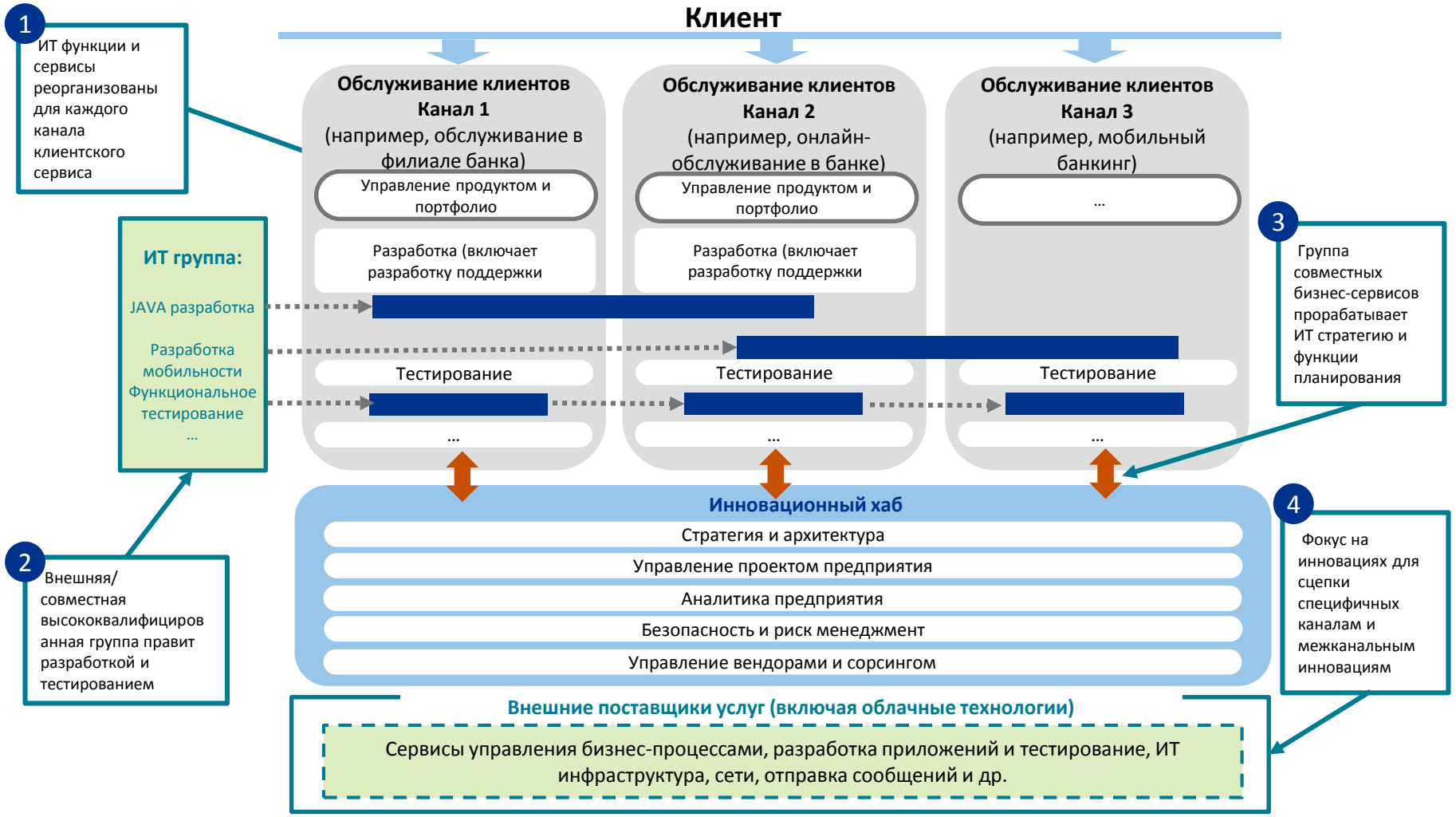
Структура модели интегрированных бизнес-сервисов



Структура продукт/платформ-ориентированной модели



Структура клиент/канал-ориентированной модели



KPMG

Применение цифровых технологий

«Повседневный банк»

Повседневный банк =

1: Сквозная интеграция каналов обслуживания

2: Единое непрерывное общение с клиентом

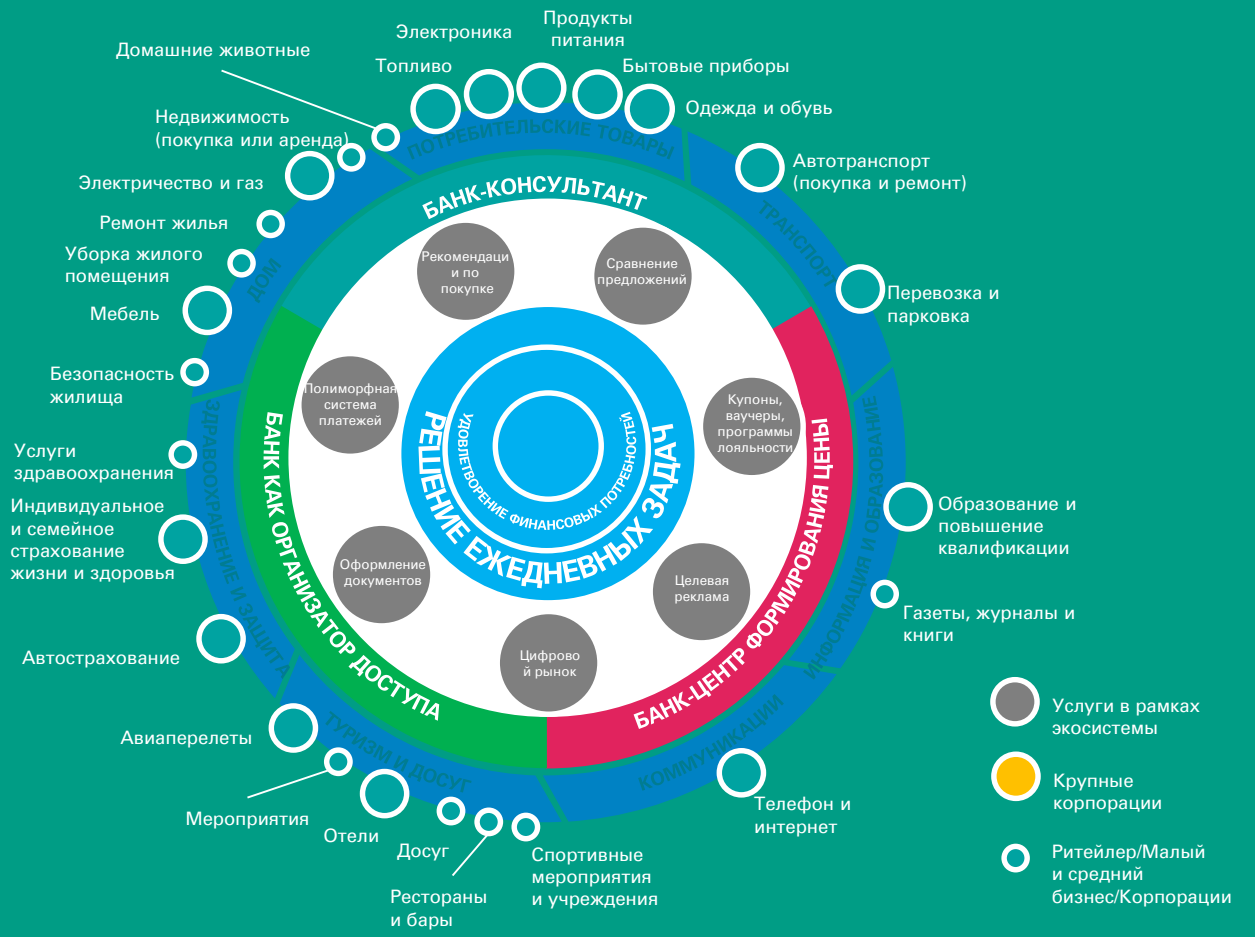
3: Динамическое предложение персонифицированных продуктов

4: Предложение комплексных (интегрированных с партнерскими) продуктов

5: Мониторинг поведения клиента в реальном времени

6: Аналитика во всём

7: Рост при низких затратах



Пример архитектуры повседневного банка

BBVA (1/2)

Описание компании

- Испанский банк, штаб квартира в Мадриде
- Работает в Европе, Латинской Америке, США, Китае и Турции

Размер

- Активы 409 млн евро[5]
- 109,305 сотрудников[5]
- 7,512 отделений (3,230 в Испании)[5]

Omnichannel стратегия

- BBVA поставил клиентов в центре своей цифровой трансформации.
- На текущий момент банк инвестировал $362 млн для внедрения omnichannel стратегии strategy to replace legacy system and offer customers real-time experience across all channels
- 'Omnichannel Banking' была приоритетная инициативой BBVA в 2013 году; которая включала идентификацию клиента в каналах, работу с цифровым контентом, и кросс-канальные инициативы.
- В 2014 банк купил мобильный банк Simple. На момент покупки Simple обслуживал 1 000 000 клиентов при штате 90 человек.
- To respond to the changing needs of the customer while leapfrogging the competition ,BBVA purchased Simple earlier this year to leverage their strong online and mobile banking features.
- BBVA подписал соглашение, чтобы адаптировать Google Apps для бизнес задач. Облачные инструменты используются сотрудниками для взаимодействия, это повысило эффективность взаимодействия и обмена информацией в реальном времени.
- В 2012 году 110,000 сотрудников в 26 странах мигрировали с Microsoft на Google Apps.
- BBVA публикует журнал 'Innovation Edge'. Был открыт инновационный центр; основной фокус на Big Data и банк для клиента.
- BBVA венчурный фонд: Фонд инвестирует в start-up компании, которые разрабатывают инновационные цифровые платформы и бизнес-модели в индустриях, схожих с бизнесом BBVA.

Основные метрики

- 1.2 млн подписчиков на on facebook; 19.1тыс подписчиков на twitter
- В 2015 году совокупный доход увеличился на 10.9%
- 19.2% кредитов выдано через цифровые каналы

Использование каналов

Web

- Недавно сделали инвестиции в новый web- сайт с дружелюбным интерфейсом на всех основных рынках[5]
- Публикация новостей в реальном времени в корпоративном блоге в социальных сетях
- С 2009 BBVA использует аналитику для анализа обратной связи

Mobile

- BBVA Compass лучшее решение для мобильного банкинга в стране
- Используют геймификацию для управления мобильными транзакциями
- 1й приз за функциональность мобильного банка *American Banker* 1

Social Media

- Обсуждение проекта по социальной ответственности занимает более 50 страниц на twitter
- Расходы на социальные сети учитываются в корпоративном бюджете банка

Tradi-tional

- Новый дизайн и инновационные решения в отделениях
- Банкомат – не только средство снятия денег

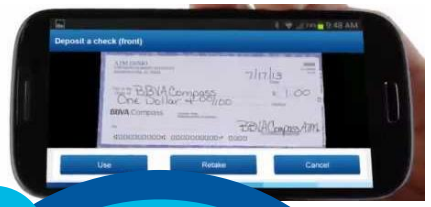
BBVA (2/2)

BBVA

1 В то время, когда Карлос просматривал Facebook, он заметил очень привлекательное предложение по депозиту

2 Он зашел на сайт BBVA, чтобы посмотреть детали и заполнить заявку. Он нашел ближайшее отделение.

3 Когда он зашел в отделение, открытие счета заняло 5 минут. Его менеджер также посоветовал открыть кредитную карту.



4 Дома Карлос загрузил приложение с сайта для своего телефона. Он сфотографировал счет на оплату коммунальных услуг и отправил его на оплату.

5 Позже Карлос играл в игру, которая была на сайте банка на своем tablet

Он смотрел видео, отвечал на интересные вопросы и делал оплату онлайн и он выиграл приз

6 По пути на концерт Карлос отправил сестре деньги, введя текст PopMoney

Примеры использования технологии blockchain

По мнению управляющего директора R3 Чарли Купера, банки смогут внедрить Blockchain на практике в течение ближайших двух лет.

«Реализация кредита – это трудоемкий процесс, регулирование которого может занять недели», — заметил Даниэль Пинто, глава инвестиционного банка JP Morgan. «Имеет смысл исследовать потенциал blockchain для улучшения этого процесса».

- **Создан консорциум R3 мировых банков по разработкам в области технологии Blockchain:**

J.P. Morgan, Goldman Sachs,
Banco Santander,
Bank of America,
Barclays,
BBVA,
BMO Financial Group,
BNP Paribas, BNY Mellon,
CIBC,
Commonwealth Bank of Australia,
Citi,
Commerzbank,
Credit Suisse,
Danske Bank,
Deutsche Bank,
HSBC,
ING Bank,
Intesa Sanpaolo,
Macquarie Bank,
Mitsubishi UFJ Financial Group,
Mizuho Financial Group,
Morgan Stanley,
National Australia Bank,
Natixis,
Nomura,
Nordea,
Northern Trust,
OP Financial Group,
Scotiabank,
State Street,
Sumitomo Mitsui Banking Corporation,
Royal Bank of Canada,
Royal Bank of Scotland,
SEB,
Societe Generale,
Toronto-Dominion Bank,
UBS,
UniCredit,
U.S. Bancorp,
Wells Fargo and Westpac Banking Corporation.

- Сбербанк рассматривает вариант вступления в международный консорциум R3, для внедрения сервисов, работающих на основе blockchain. должно снизить зависимость кредитной организации от системы SWIFT, а также повысить защиту ее транзакций

- Европейский Центробанк изучает возможности, которые предлагает технология blockchain.

Модели sourcing

Объединенные центры обслуживания (ОЦО) и услуги провайдеров облачных услуг

Стандартизация, оптимизация, комплайенс – ключевые козыри сегодняшних моделей сорсинга

Источник: Исследование HfS «Состояние аутсорсинга 2014», проведенное при поддержке КПМГ

Модель выделения ОЦО. Целью может быть не только сокращение затрат

…при этом затраты на построение ОЦО окупаются, как правило, в течение трех лет.

Экономические выгоды	**Повышение производительност и труда**	■ Перевод нескольких процессов в ОЦО позволяет значительно оптимизировать численность за счет одновременной унификации и стандартизации большего числа сквозных поддерживающих процессов ■ При объединении нескольких функций в едином ОЦО достигается существенный синергетический эффект, обеспечивающий интеграцию целей и задач всех функций, большую прозрачность в оценке эффективности и повышение скорости внедрения изменений в процессах и процедурах в рамках всей Компании
	Снижение операционных затрат	■ Создание ОЦО в регионах, где на это требуются наименьшие затраты (ценовой арбитраж) и эффект масштаба от централизации большего количества процессов ведёт к более значительному снижению операционных затрат на поддерживающие функции ■ Объединение нескольких функций в едином ОЦО позволяет сократить затраты на организацию работы самого ОЦО (подбор и обучение персонала, инфраструктура, снабжение) и воспользоваться преимуществами единой модели управления
Качественные выгоды	**Повышение качества внутреннего обслуживания**	■ Централизация процессов в ОЦО приводит к унификации и повышению качества обслуживания внутренних клиентов за счет более широкого распространения сервисного подхода и создания единого стандарта интерфейса взаимодействия с клиентами ОЦО ■ Уменьшение финансовых и бизнес-рисков благодаря введению и централизации контролей за процессами
	Повышение эффективности контролей	■ Повышение эффективности контролей организации за счет централизации персонала и информации в рамках одного подразделения, имеющего прозрачную структуру и процессы управления на базе SLA ■ Стандартизация процессов для всех бизнес-единиц/ дочерних обществ. Устранение дублирования функций между смежными подразделениями
	Фокус на ключевых компетенциях бизнеса	■ Перевод поддерживающих стандартных процессов в ОЦО позволяет руководству организации сфокусироваться на развитии и совершенствовании ключевых бизнес-процессов, создающих добавленную стоимость

Какие функции, связанные с ИТ, передаются в ОЦО?

Разработка ИТ- стратегии	Локальные ИТ- решения	ИТ-поддержка	ИТ-развитие	Прочие функции
ИТ-стратегия	Создание локальных ИТ-решений	**Служба ИТ-поддержки**	**Разработка программного обеспечения**	**Внутренние контроли**
ИТ-политика и стандарты	**Разработка политик / стандартов по нетиповым процессам**	**Центр обработки/ хранения данных**	**Тестирование программного обеспечения**	**Внутренний аудит**
Формулирование/ одобрение требований к контрольной среде	**Доработка глобальных ИТ-решений под потребности отдельных бизнес единиц**	**Восстановление данных**	**Управление программным обеспечением**	
		Администрирование сети		
		Колл-центр		

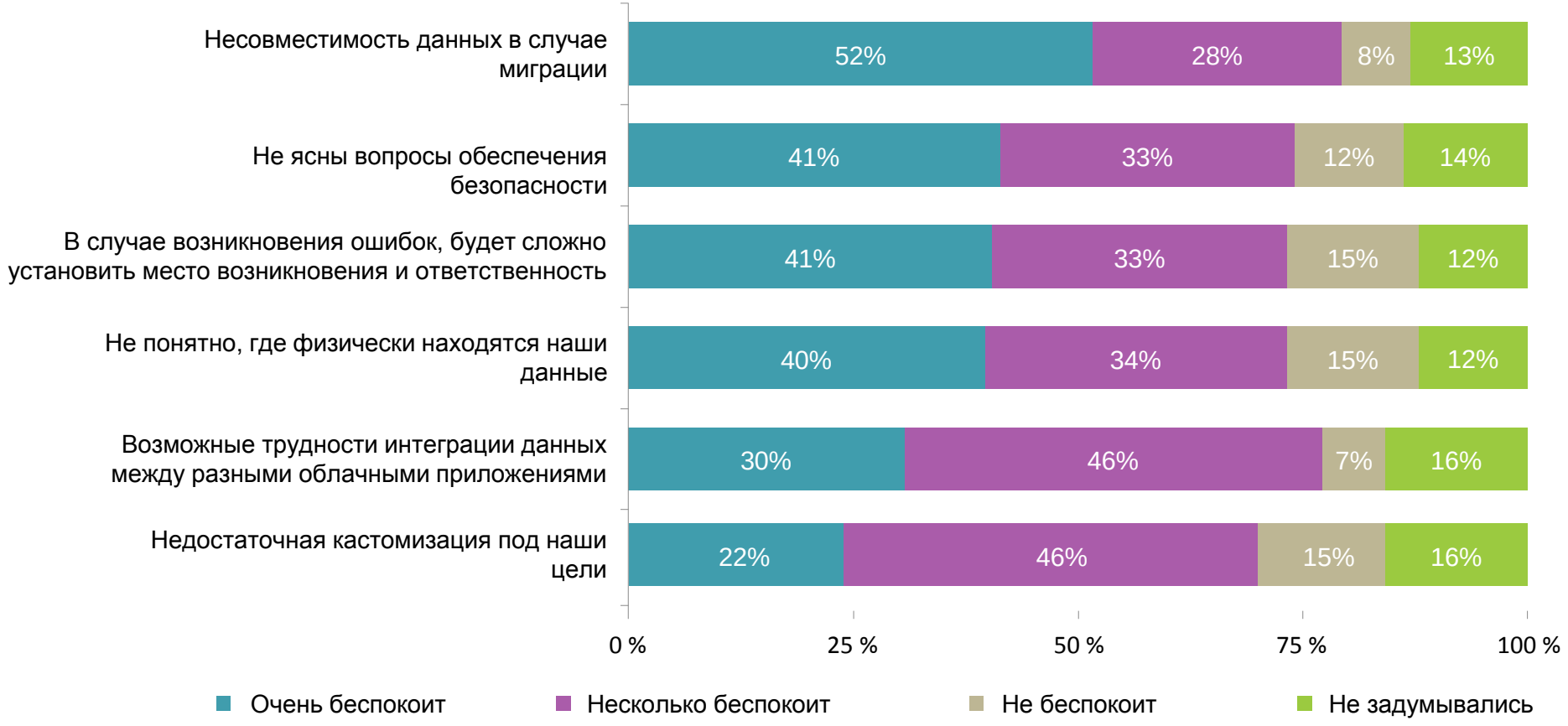
Функции передаваемые в ОЦО

Функции передаваемые в ОЦО частично

Функции не передаваемые в ОЦО

Облачные решения. Почему нет?

Что беспокоит компании при оценке возможности перехода в облака?



Источник: Исследование HfS «Состояние аутсорсинга 2014», проведенное при поддержке КПМГ

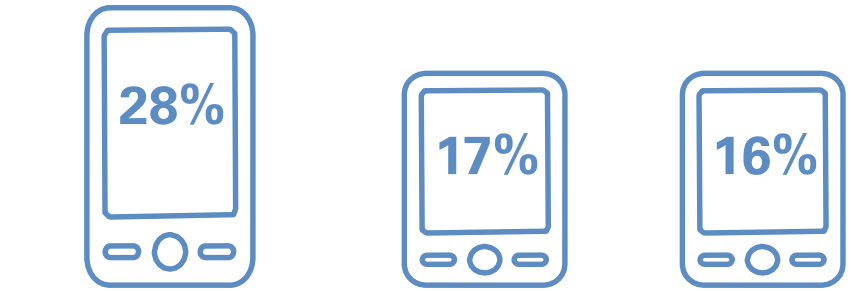
Безопасность – ключевой барьер перехода в облака

Провайдеры облачных технологий (SaaS, IaaS, PaaS) активнее других аутсорсеров предлагают рынку инновационные решения, сервисы и инструменты, предоставляя ряд возможностей по сокращению издержек. Облачные технологии также играют значимую роль при создании центров разделяемых сервисов. Популярность «облаков» растет, но, тем не менее, результаты опроса КПМГ в мире показывают, что процесс перехода к таким технологиям протекает достаточно медленно.

В числе основных препятствий, названных респондентами, – риски, связанные с безопасностью и защитой персональных данных, проблемы интеграции с существующими процессами и решениями, риски нарушения требований регуляторов. Боязнь подобных рисков понятна, но ими вполне возможно управлять.

Затраты компаний на облачные технологии растут не очень быстрыми темпами

Основные барьеры, препятствующие инвестициям в облачные технологии



Местонахождение данных – риски безопасности и защиты персональных данных

Проблемы интеграции с существующей операционной моделью ИТ

Опасения несоответствия **регуляторным требованиям**

Источник: Глобальное исследование КПМГ (KPMG IT Outsourcing Service Provider Performance & Satisfaction Study 2014/15).

KPMG

Новые подходы к оценке ИТ

ТОП-10 областей для аудита в технологичных компаниях

2015 vs 2013

		2015	2013
⇔	1	Кибербезопасность	Инф. безопасность, защита ПД
↑	2	Защита интеллектуальной собственности	Общее управление ИТ (IT Governance)
↑	3	Развитие бизнес-моделей	Внедрение и разработка ключевых систем
↑	4	Международные операции	Социальные медиа
⇔	5	Управление отношениями с поставщиками	Управление отношениями с поставщиками
↑	6	Контракты с правительством	Внедрение и обновление систем: переход в облако
↓	7	Внедрение и обновление систем: переход в облако	Новые технологии и обновление инфраструктуры
↑	8	Слияния, поглощения, расформирования	Использование техник анализа данных и непрерывного аудита
↑	9	Выручка от основной деятельности	Соответствие требованиям PCI DSS
↓	10	Использование техник анализа данных и непрерывного аудита	Непрерывность бизнеса (BCP, DRP)

+ снижение затрат на фоне роста регуляторного давления (особенно в свете IFRS 9 и Базель II/III)

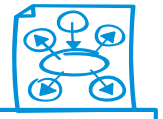
Источники: KPMG, ISACA, Protiviti.

Кибербезопасность

Кибербезопасность

Этапы аудита кибербезопасности кардинально не отличаются от типичных аудитов функции информационной безопасности. Разница – в глубине анализа рисков и операционной модели.

СТРАТЕГИЧЕСКИЙ ОБЗОР



Выстраивание глубокого понимания **ключевых предпосылок**:

- **Структура управления**, риск-аппетит, роли и обязанности
- **Навыки и компетенции** функции информационной/кибер-безопасности
- **Риски,** присущие организации (и ее клиентам)
- **Позиции на рынке** (для целей бенчмарка)
- **Стратегические цели** и предоставляемые сервисы
- **Целевая операционная модель**

1

ФУНКЦИОНАЛЬНЫЙ ОБЗОР

Интервью, анализ документации, тестирование контролей:

- Определение эффективности текущей **операционной модели, модели корпоративного управления, управления проектами** кибербезопасности
- **Изучение опыта заранее определенных бизнес-подразделений** с целью выстраивания понимания того, как функция кибербезопасности влияет на оказание услуг и соблюдаются ли установленные принципы и контроли
- **Оценка возможностей сервисов и решений**

2

НЕДОСТАЮЩИЕ ВОЗМОЖНОСТИ

Гэп-анализ между текущим состоянием и целевой операционной моделью в части:

- Митигирования рисков, связанных с **человеческим фактором, операционными и технологическими инцидентами**
- Постоянной оценки и повышения уровня **внутренней осведомленности** сотрудников о **сервисах и принципах** функции кибербезопасности
- **Операционной модели и структуры** (методология «12 шагов к кибербезопасности»)
- **Бенчмарк уровня кибербезопасности** относительно конкурентов (в том числе с точки зрения клиентов конкурентов)
- **Идентификация остаточных рисков,** которые могут негативно сказаться на клиентах организации и ее бренде

3

ОТЧЕТ С НАБЛЮДЕНИЯМИ

Набор **наблюдений и рекомендаций** для развития текущей модели управления кибербезопасностью и закрытия существующих недостатков:

- Рекомендации по **подходам** к улучшению возможностей в части **технологий, процессов и людей**
- **Оценка потенциальных рисков кибербезопасности,** присущих организации и рекомендуемые митигирующие действия
- **Инсайты** в существующие **передовые практики**

4

Методология KPMG «12 шагов к кибербезопасности»

Традиционно в основе методологии оценки и повышения эффективности функции кибербезопасности лежит риск-ориентированный подход.

- Идентификация **гэпов** и планирование **исправительных** мероприятий
- Оценка эффективности стратегий в области развития **персонала, процессов** и **технологий**
- Анализ возможностей **персонала, процессов и технологических** решений с точки зрения предлагаемых услуг и продуктов

- Определение **возможностей** по улучшению уровня кибербезопасности
- Анализ рисков и среды внутреннего контроля с точки зрения процессов, связанных с оказанием услуг и ведением технологичных проектов
- Оценка эффективности **функции кибербезопасности**

- Определение **бизнес-драйверов** для повышения уровня кибербезопасности
- Оценка соответствия стратегии кибербезопасности общим **целям бизнеса**

- Понимание **целей** менеджмента, функции кибербезопасности, организационной структуры, клиентов
- Понимание **стратегии** кибербезопасности
- Идентификация ключевых **заинтересованных сторон** в кибербезопасности предприятия
- Идентификация гэпов в механизмах **корпоративного управления**

Подход снизу вверх

Внедрение

Люди | Процессы | Технологии

Осведомленность и обучение

Архитектура предприятия

Планирование и контроль

Управление проектами, программами и портфелями проектов

Управление отношениями с поставщиками и интеграторами

Управление рисками ⟷ Соответствие регуляторным требованиям

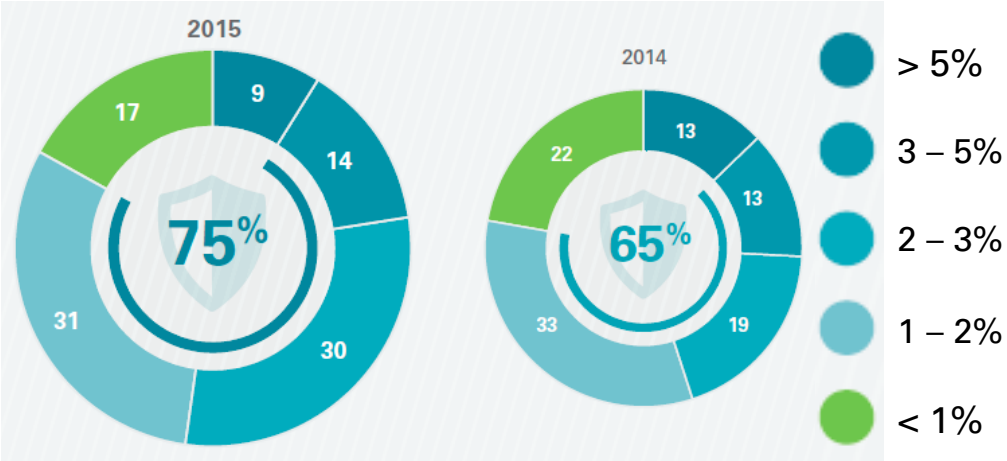
Понимание

Цели и стратегия бизнеса | Активы | Знания | Требования регуляторов

Начало начал

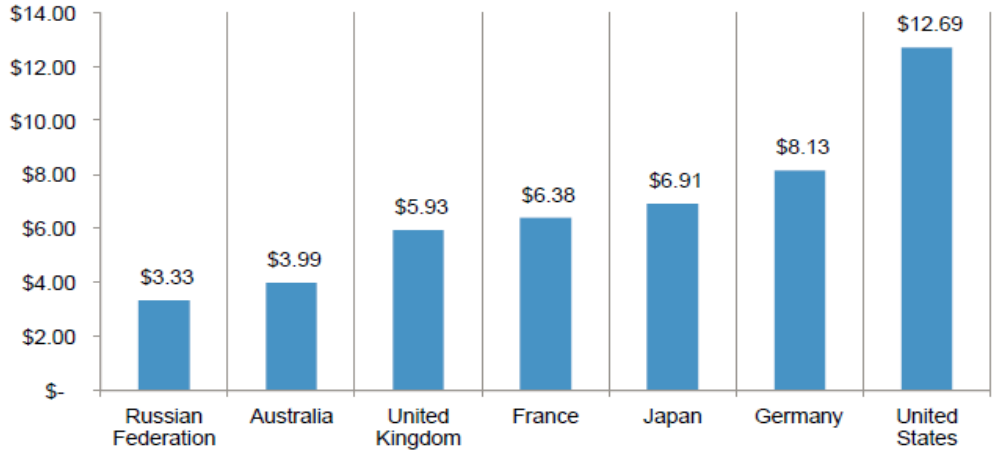
Владельцы | Ответственность | Политики | Бюджет и спонсор проекта

Траты на проекты в области кибербезопасности в % от выручки



Источник: данные KPMG за 2015.

Потери от кибератак в млн долл. США



Источник: данные Ponemon Institute за 2015.

KPMG

Области аудита кибербезопасности

Управление и руководство

Роли (топ-)менеджмента, владение и управление верхнеуровневыми рисками.

Человеческий фактор

Культура (знания, умения, навыки) в области информационной безопасности.

Управление ИТ-рисками

Подходы к управлению рисками владения информацией, в том числе интеллектуальной собственностью.

Непрерывность бизнеса

Уровень подготовленности к сбоям, возможности по предотвращению сбоев и минимизации последствий таковых.

Процессы и технологии

Уровень эффективности среды внутреннего контроля.

Соответствие регуляторным требованиям

Подходы к поддержанию и повышению уровня соответствия требованиям различных регуляторов, национальных и международных стандартов.

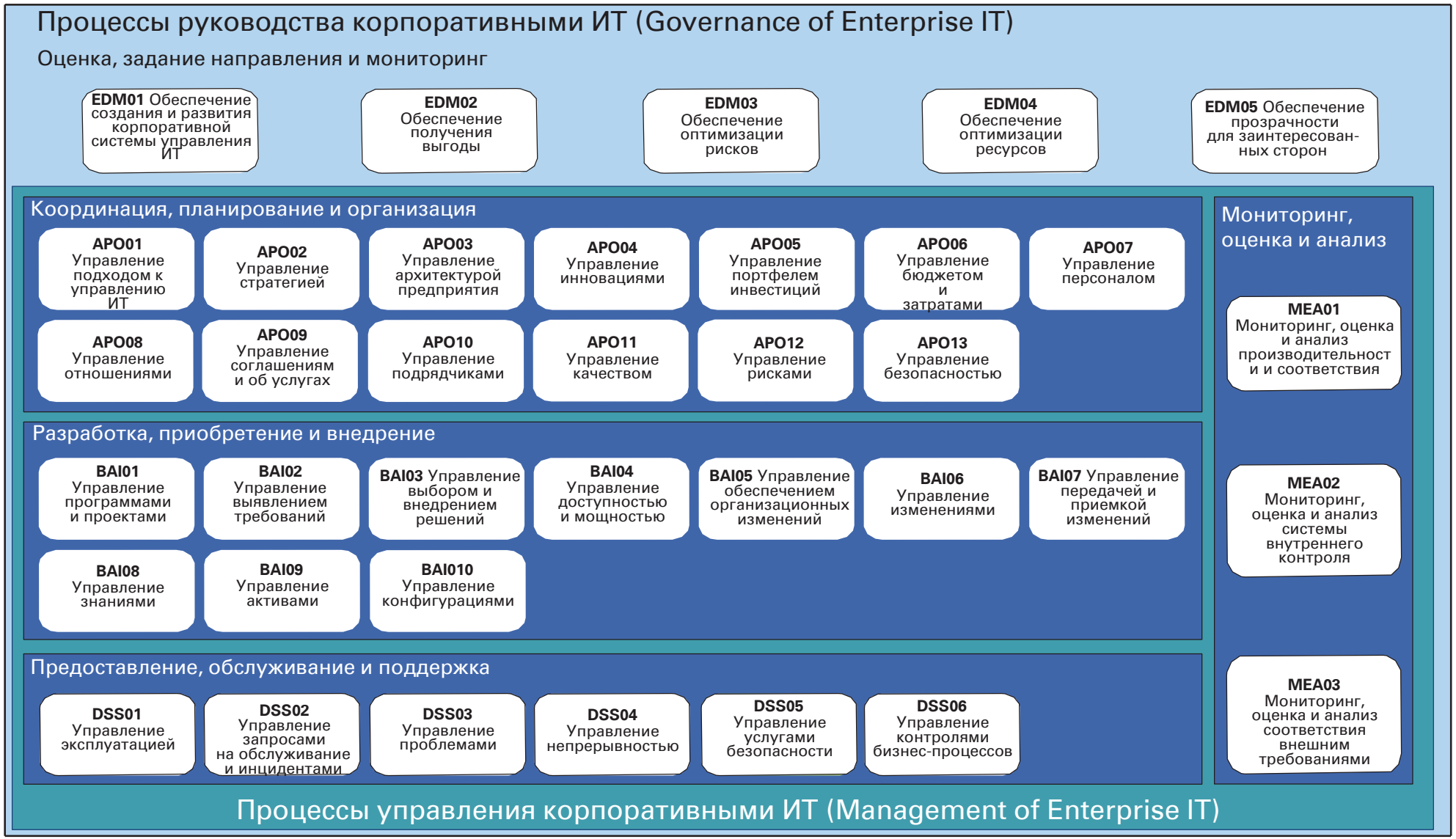
KPMG

COBIT 5

Комплексная оценка эффективности процессов корпоративного руководства и управления ИТ

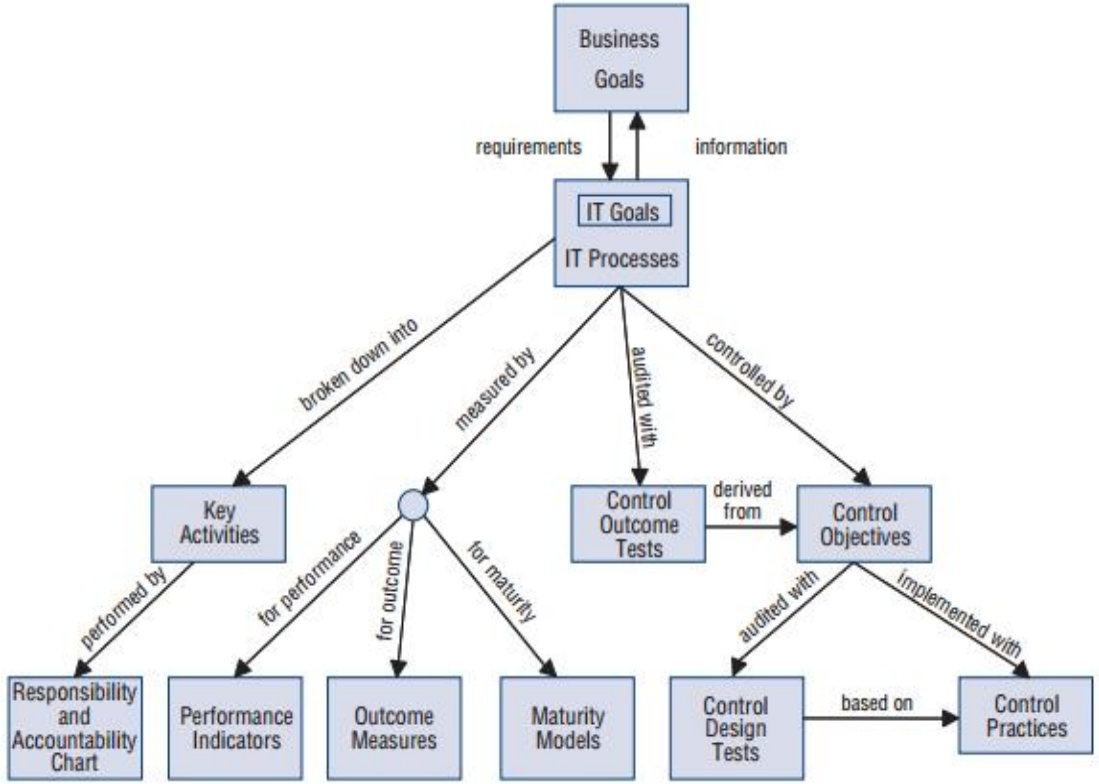
Повышение эффективности ИТ и COBIT 5

Модель COBIT 5 была пересмотрена с целью наиболее полного охвата всех основных аспектов и процессов, связанных с руководством и управлением корпоративных информационных технологий.



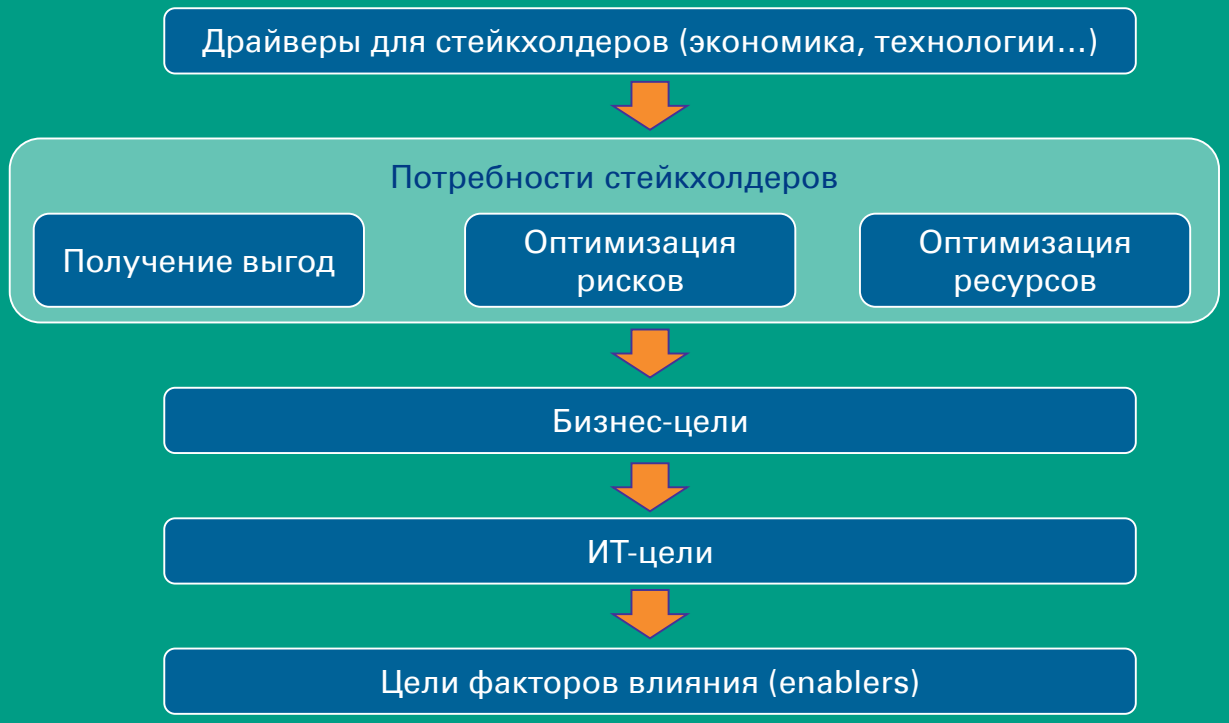
Фокусы аудита по COBIT 4.1

- Подходы к управлению ИТ-процессами. Процессы, роли и ответственность
- Цели контроля и средства их достижения



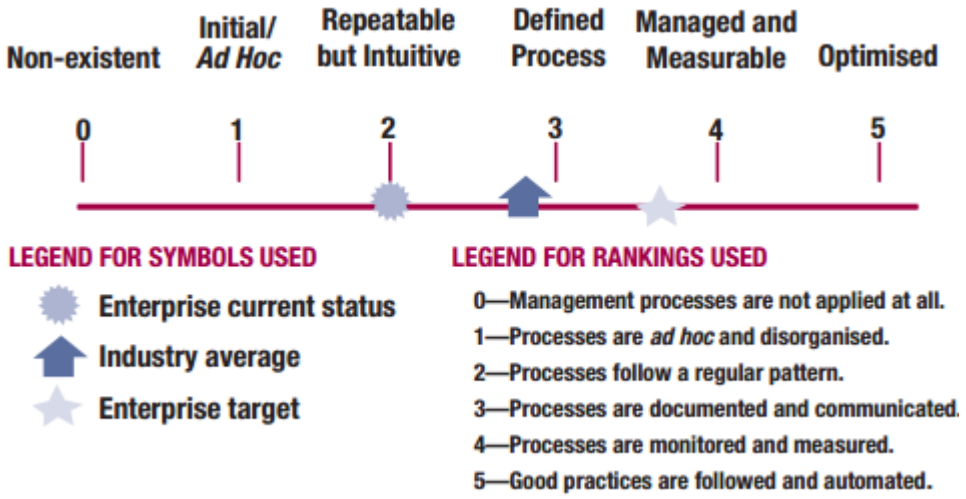
и аудита по COBIT 5

- Подходы к корпоративному руководству и управлению информационными технологиями. Процессы, роли и ответственность
- Ценности для стейкхолдеров и цели бизнеса
- Возможности, драйверы (мотивы), факторы влияния



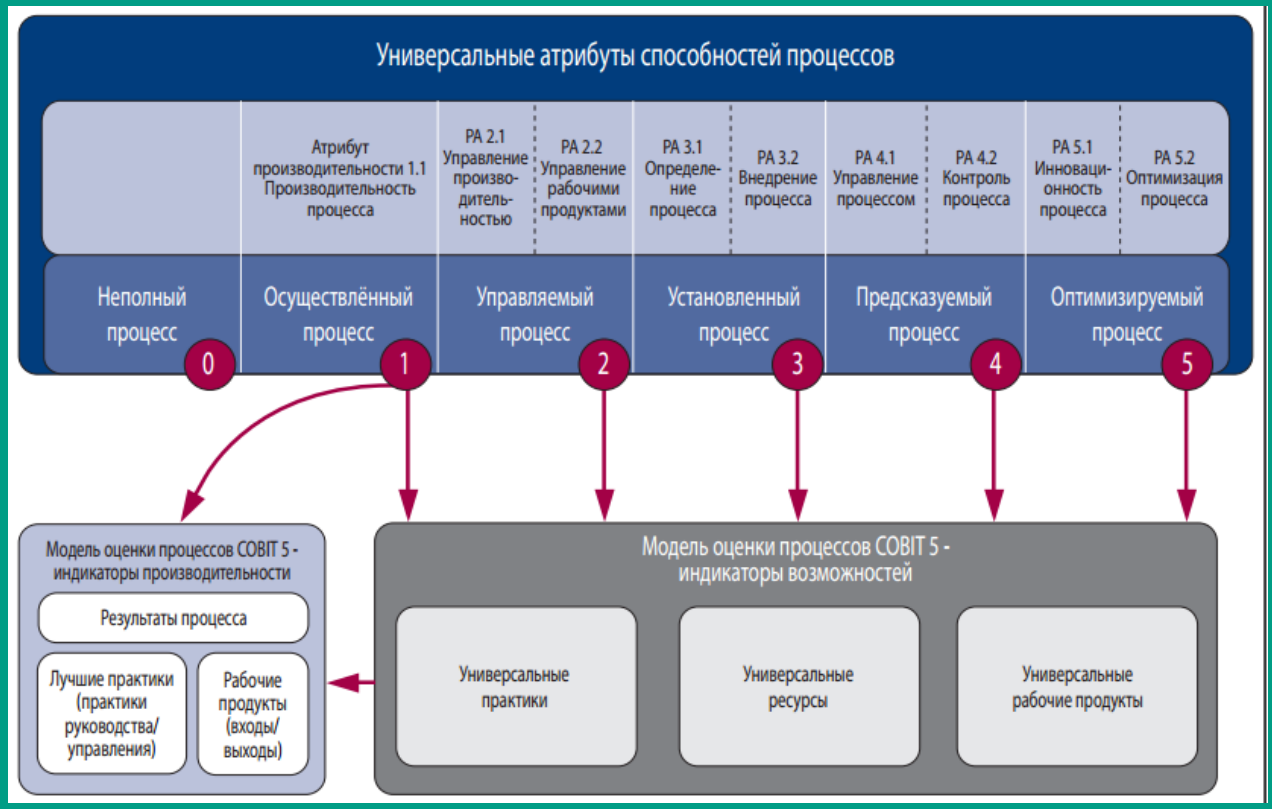
Метрики аудита по COBIT 4.1 и аудита по COBIT 5

- Контролируемость и повторяемость процессов



- Полнота, управляемость, эффективность процессов

-> Соответствие методики оценки стандарту ISO 15504



Источник: ISACA.

Услуги поставщиков и облачных провайдеров

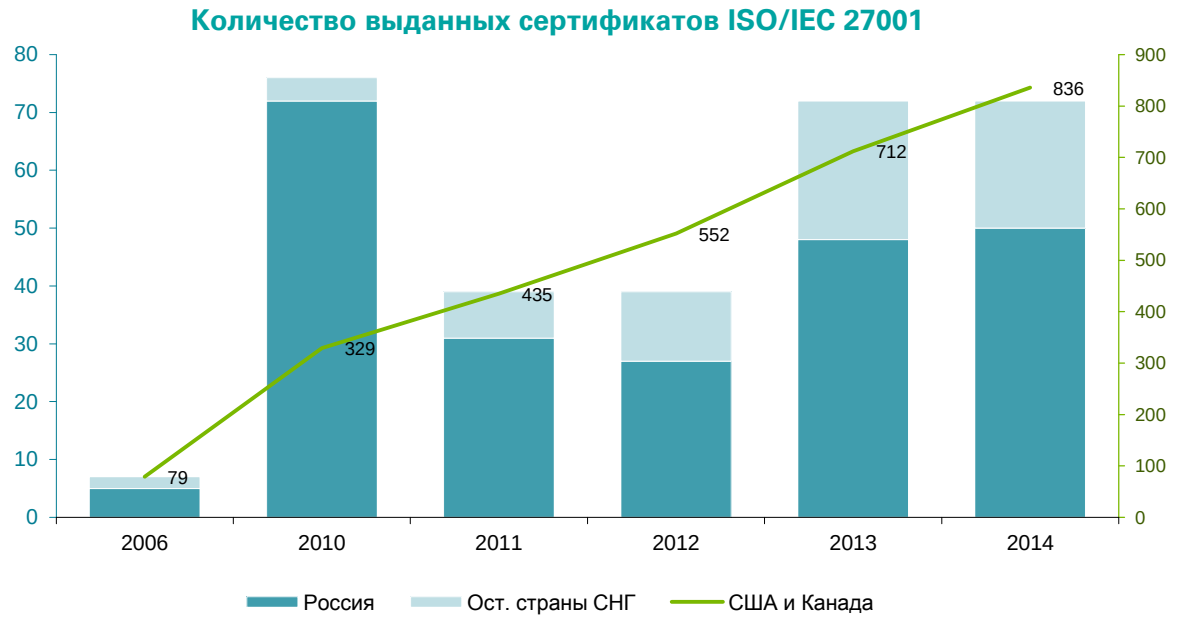
Стандарты ISO и SOC

Основная сертификация по информационной безопасности не может набрать популярность в СНГ

ISO/IEC 27001 – «Информационные технологии. Методы обеспечения безопасности. Системы управления информационной безопасностью. Требования»

ISO/IEC 27002 – «Информационные технологии. Методы обеспечения безопасности. Практические правила управления информационной безопасностью»

ISO/IEC 27005 – «Информационные технологии. Методы обеспечения безопасности. Управление рисками информационной безопасности»



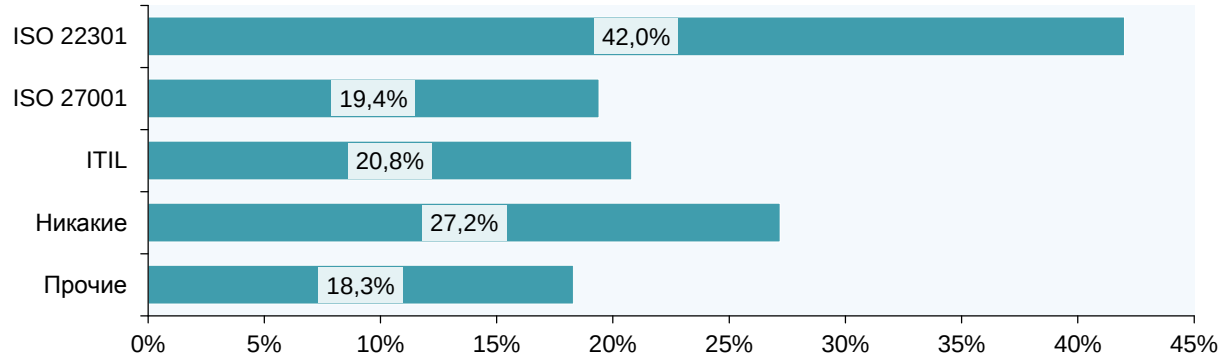
Несертификационные стандарты. Однако, иногда клиенты запрашивают у провайдеров независимую оценку по данным стандартам вместо сертификации по ISO 27001.

Источник: ISO 2015 Survey.

Сфокусированность на общих подходах к управлению информационной безопасностью, нежели на эффективности отдельных контролей, недоверие к другим сертификатам ISO, дороговизна сертификации – возможные причины непопулярности стандарта в СНГ, который де-факто является «must-have» на Западе.

Непрерывность бизнеса представлена в ISO 27001, но более полно охвачена в выпущенном в 2014 г. стандарте ISO 22301

Стандарты, используемые при развитии системы управления непрерывностью бизнеса (помимо регуляторных положений)



Источник: The 2013 – 2014 Continuity Insights and KPMG Global BCM Program Benchmarking Study.

В первый год действия стандарта:

1757 выданных сертификатов в мире

1 выданный сертификат в СНГ

«Удивляет и вдохновляет, что более 42% респондентов обозначили ISO 22301 как стандарт, влияющий на их программы [по BCP]. Особенно если учесть, что исследование 2011–2012 показало общее влияние стандартов BS25999-2 и ASIS/BSI BCM.01:2010 на уровне всего 16%».

Тим Мэтью, исполнительный директор, Eterprise Resiliency, Educational Testing Service (ETS)

«[Результаты] показывают, что влияние ISO 22301 даже выше, чем многие в Америке могли подумат

Линдон Бёрд, технический директор BSI

«Очевидно, сертификация рассматривается полезным шагом – более 50% респондентов отметили, что их организация собирается получить сертификацию от DRI, еще 34% - от BCI…».

Майк Джанко, менеджер, The Goodyear Tire & Rubber Co.

SOC – аттестационные стандарты среды внутреннего контроля поставщиков услуг

Аббревиатура SOC расшифровывается как Service Organization Control reports (Отчеты сервисных организаций о системе контроля). Существуют три типа SOC-отчетов: SOC1 (более известны как ISAE 3402/SSAE 16 – ранее SAS 70), SOC2, SOC3. Появление данных стандартов стало ответом на эволюцию аутсорсинговых моделей.

	Контроли над процессами формирования финансовой отчетности (ICOFR)	**Любые операционные контроли**	
	SOC1 (ISAE 3402 / SSAE 16)	**SOC2 (ISAE 3000, Trust Services)**	**SOC3 (ISAE 3000, Trust Services)**
Общие сведения	Подробный отчет для пользователей услуг и их финансовых аудиторов	Подробный отчет для пользователей услуг, их аудиторов и других определенных сторон (например, руководства, регуляторов, консультантов по сделкам слияния-поглощения)	Короткий отчет, который может публично распространяться. При этом обязательно должна быть выполнена проверка операционной эффективности контролей.
Применимость	Риски неправильного формирования финансовой отчетности пользователей услуг и контроли, покрывающие эти риски. Риски и контроли формулируются провайдером. Наиболее применимо для провайдеров, занимающихся обработкой финансовых транзакций или поддерживающих финансовые системы.	Фокус на доменах: – Безопасность – Доступность – Конфиденциальность – Целостность обработки данных – Защита персональных данных. Применимо для широкого круга провайдеров.	

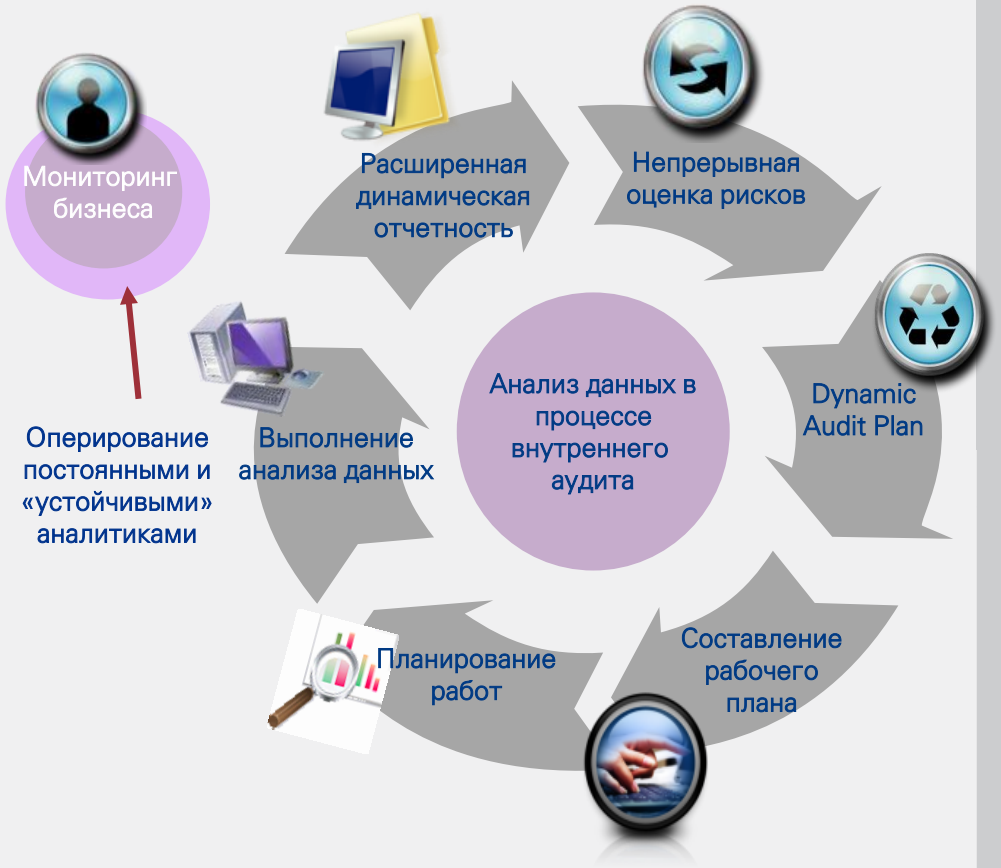
Отчеты SOC2/3 были выделены для возможности охватить контроли, не относящиеся к фин. отчетности клиентов провайдеров услуг

Домены, покрываемые отчетами SOC2/3				
Безопасность (обязательный домен)	**Доступность**	**Конфиденциальность**	**Целостность обработки**	**Защита персональных данных**
▪ Политика ИБ ▪ Осведомленность пользователей и коммуникации ▪ Оценка рисков ▪ Логический доступ ▪ Физический доступ ▪ Защита окружающей среды ▪ Мониторинг ▪ Аутентификация пользователей ▪ Управление инцидентами ▪ Управление активами ▪ Разработка и поддержка систем ▪ Защита персонала ▪ Управление конфигурациями ▪ Управление изменениями ▪ Комплайенс	▪ Политика непрерывности ▪ Резервное копирование ▪ Восстановление деятельности ▪ Управление непрерывностью бизнеса	▪ Политика конфиденциальности ▪ Сбор конфиденциальных данных ▪ Обработка конфиденциальных данных ▪ Раскрытие информации ▪ Обеспечение конфиденциальности при разработке информационных систем	▪ Политики целостности обработки ▪ Полнота, корректность, своевременность и авторизация при выполнении операции ввода/ вывода данных и их обработки	▪ Управление персональными данными ▪ Уведомление сторон ▪ Получение согласий на обработку ▪ Сбор данных ▪ Использование, хранение и уничтожение ▪ Ограничение доступа ▪ Раскрытия ▪ Контроль качества ▪ Мониторинг процессов обработки персональных данных и законодательства

Анализ данных и непрерывный (дистанционный) аудит

Анализ данных в аудите

Анализ данных и непрерывный аудит повышает уровень качества результатов аудита и его общую ценность для бизнеса.



Ключевые задачи:

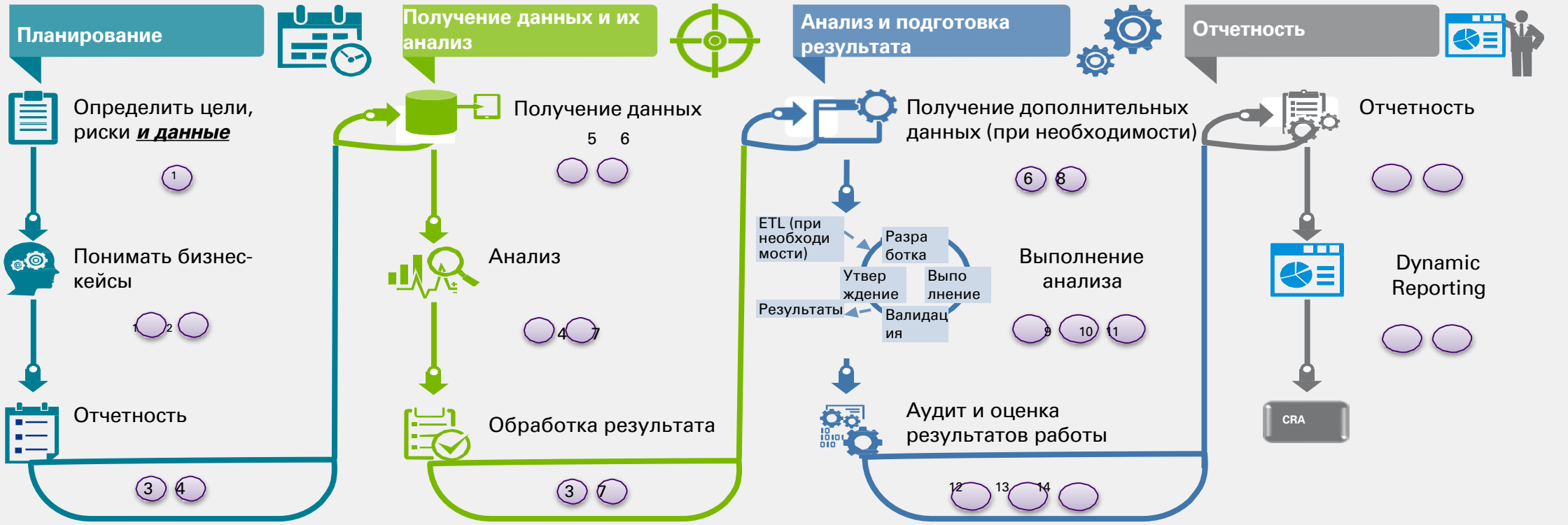
- Увеличение общей эффективности проведения аудитов (частота, объем работ и т.д.)
- Непрерывное управление рисками.
- Фокус внимания на ключевые зоны риска с помощью анализа данных.
- Снижение затрат на проведение аудитов и мониторинга.
- Обеспечение своевременного обнаружения фактов злоупотребления или ошибок.

Использование **традиционных методов аудита** базируется на циклическом процессе, который предполагает «ручное» определение целей контроля, оценку, определение небольшой выборки для тестирования операционной эффективности контролей.

Современный метод предполагает использование непрерывного анализа данных для риск-ориентированного подхода: можно отследить каждую транзакцию, а не толь ко те, которые были включены в выборку, что повышает общую эффективность аудита с учетом большого количества данных.

Преимущества комплексного подхода использования данных в процессе аудита

Процесс анализа данных



Инструменты (например)

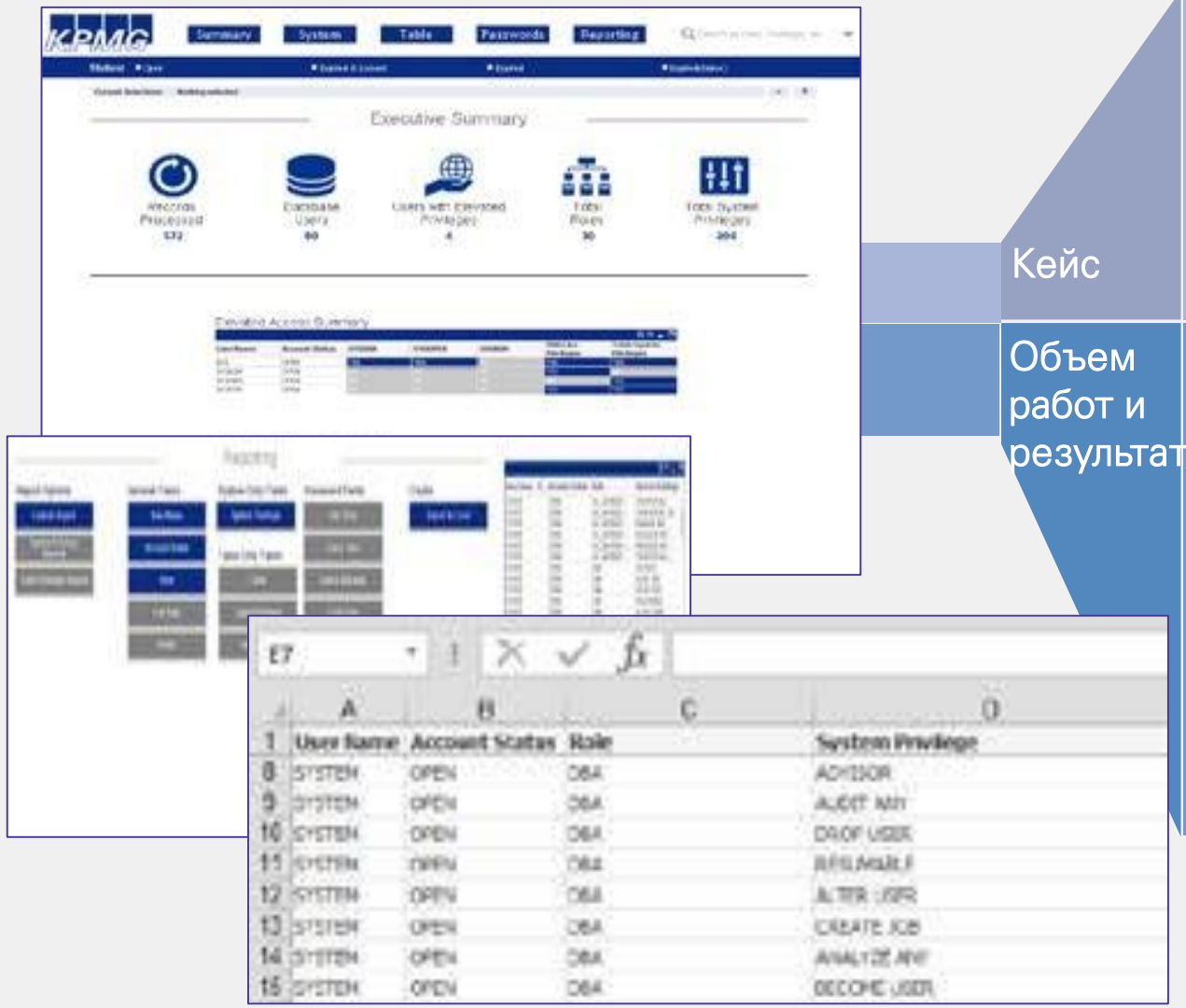
D&A-enabled программы
alteryx (или эквивалент)
QlikView (или Sense)

alteryx
QlikView
Qlik Sense
(или эквивалент)

QlikView
Qlik Sense
(или эквивалент)

Пример использования анализа данных

Панель отчетности



Кейс

Компания работает в Oracle и AS40 с несколькими базами данных, что требует трудоемкого ручного манипулирования большими объемами данных для достижения эффективности процесса, безопасности и контроля доступа. Лицензии на сканирование безопасности программного обеспечения (Nessus, AppDetective) дороги и требуют непосредственной установки на клиентских средах.

Объем работ и результат

Команда KPMG разработала приложение на основе Alteryx, QlikView для обзора и оценки ключевых инстанций Oracle, AS400 на основании принятых аудитом программ и стандартных скриптов.

Использование автоматически подготовленных данных в результате исполнения стандартных скриптов, приложений экономит время по сравнению традиционного подхода анализа данных.
Созданные панели отчетности позволяют пользователей обучить рискам, связанных с каждым уровнем доступа и настройкам безопасности.

Оксана Борисова

Директор, Консультирование в области ИТ

oborisova@kpmg.kz

Константин Аушев

Менеджер, Консультирование в области ИТ

kaushev@kpmg.kz