

Как интегрировать основные принципы управления в функцию **информационной безопасности?**



Анастасия Харыбина

Руководитель АКТИВ.CONSULTING
Председатель Ассоциации АБИСС

Три кита управления

1. Постановка целей и задач

SMART: конкретный, измеримый, достижимый, значимый, ограниченный по времени

2. Выделение ресурсов

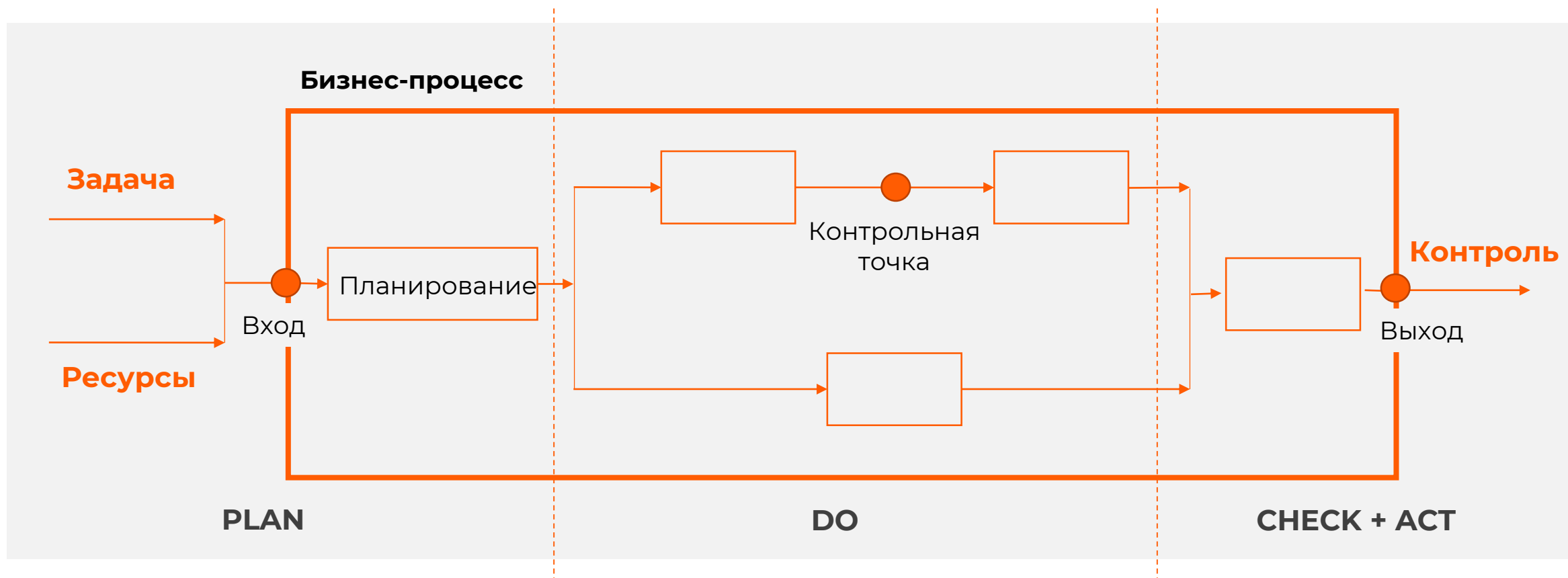
Деньги, люди, время, процессы, регламенты, полномочия, экспертиза, инструменты, методики и т.д.

3. Контроль результатов

Соответствие поставленной цели, в том числе, через ключевые показатели эффективности

Управление организацией, структурной единицей, функцией, процессом, проектом, сотрудниками и т.д.

Управление как процесс



Процесс состоит из совокупности подпроцессов и является частью верхнеуровневого процесса



Процесс представляет собой черный ящик, определяемый владельцем процесса

Постановка целей и задач

РИСК-ориентированный подход

Мотивация через **страхи**

Постановка целей и задач **на основе ИБ-экспертизы** (модель угроз, уязвимости, киберриски, комплаенс и т.д.)

Принцип «**необходимого**»

VS or &

БИЗНЕС-ориентированный подход

Мотивация через **развитие**

Постановка целей и задач на основе **дерева целей всей организации**

Принцип «**достаточного**»

Принцип «необходимого и достаточного» – базовый принцип для достижения эффективности

Ключевые показатели «эффективности»

Системы сбалансированных показателей (*Balanced Scorecard, BSC*) разработана Нортон и Капланом



BSC позволяет отслеживать реализацию стратегических целей по четырем «перспективам»: финансы, клиенты, процессы, персонал (*декомпозиция целей*)



KPI часть BSC помогает оценить производительность (*результативность + эффективность*) процессов достижения целей

Основные ошибки при внедрение KPI:

- ✘ Не определены цели, и/или слабо сформулированы, и/или не согласованы (*дерево целей*)
- ✘ Не применяется процессный подход к управлению (KPI в первую очередь для процессов)
- ✘ Не внедрена система контроля результатов, и/или она манкируется

Резюме

01

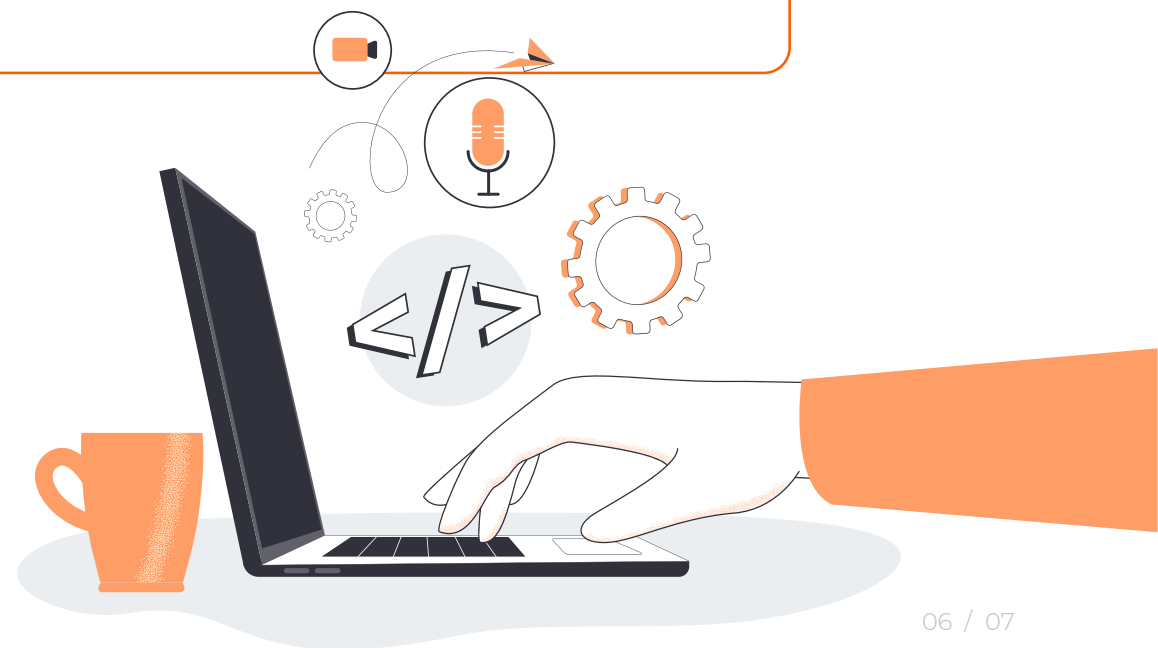
Любое управление, в том числе функцией ИБ, состоит из постановки целей, выделения ресурсов и контроля результатов

02

Цели ИБ должны учитывать риск- и бизнес ориентированные подходы и соотносится с деревом целей организации

03

Оценка результативности и эффективности процессов ИБ - инструмент определения участия ИБ в достижении бизнес-целей





Анастасия Харыбина

Руководитель АКТИВ.CONSULTING
Председатель Ассоциации АБИСС

✉ kharybina@aktiv.consulting