AKTIV.
CONSULTING

Подходы к формированию процессов управления киберрисками в рамках СУОР

Александр Моисеев
Ведущий консультант по информационной безопасности AKTIV.CONSULTING

О чем сегодня пойдет речь

Блок I

Формирование СУОР
в организации

Блок II

Управление киберрисками
в рамках процессов СУОР

AKTIV.
CONSULTING

Блок I

Формирование СУОР в организации

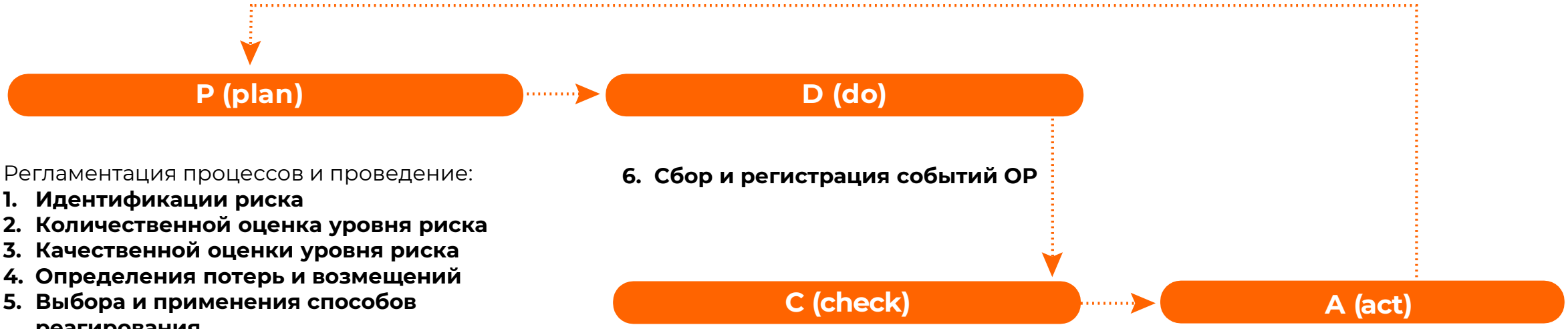
Состав системы управления операционными рисками (СУОР)

	ЭЛЕМЕНТ СУОР	СОДЕРЖАНИЕ ЭЛЕМЕНТА	ОСНОВНЫЕ ТРЕБОВАНИЯ
1	Подразделения	СУР, ЦК, СП, УП, КИО, СД, ИБ, ИТ	Определяются организацией
2	Информационные системы	SGRC, СЭД, IRP-платформы	Определяются организацией
3	База событий	(В составе элемента 2) Набор регистрируемых параметров	(Гл. 6) Требования к консолидированному и раздельному ведению, порогу регистрации
4	Классификатор	(В составе элемента 2) Признаки классификации и атрибуты	(Гл. 3 + Пр.4 и 5) Требования к делению на классы
5	Процедуры управления ОР	Идентификация рисков, ..., реагирование	(Гл. 2) Требования к оперативности реагирования и оповещения
6	Контрольные показатели уровня риска (КПУР)	Количественные и качественные показатели	(Гл. 5 + Пр. 1) Требования к установлению сигнальных и контрольных значений
7	Дополнительные элементы СУОР	Политик, регламенты и методики, а также вспомогательные процессы	(Гл. 4) Требования к периодичности пересмотра и актуализации

Основные процедуры управления ОР по 716-П

ОСНОВНЫЕ ПРОЦЕДУРЫ УПРАВЛЕНИЯ РИСКОМ	ОСНОВНЫЕ ТРЕБОВАНИЯ К ПРОЦЕДУРАМ
I. Процедуры расчета показателей для организации на плановый период	
1. Идентификация	Аналитическая работа, работа с персоналом
2. Количественная оценка уровня риска	Проведение оценки: агрегированной, ожидаемых потерь, объема капитала на покрытие потерь
3. Качественная оценка уровня риска	Проведение оценки: профессиональной, самооценки, сценарного анализа
4. Определение потерь и возмещений	Определение порядка и методов: учета потерь, недополученных доходов, потенциальных потерь, стоимости возмещений
5. Выбор и применение способа реагирования	Стратегия обработки, меры снижения негативного влияния
II. Процедуры оперативной обработки конкретных событий ОР (или группы событий)	
6. Сбор и регистрация рисковых событий	• Ввод информации в Базу событий и ее обновление • Классификация • Определение потерь и стоимости возмещений
7. Мониторинг	• Установление и отслеживание ключевых индикаторов риска (КИР) • Осуществление контроля: повышения качества самой СУОР, соблюдения выбранных способов реагирования

Процессы управления ОР в ходе внедрения



Регламентация процессов и проведение:

1. **Идентификации риска**
2. **Количественной оценка уровня риска**
3. **Качественной оценки уровня риска**
4. **Определения потерь и возмещений**
5. **Выбора и применения способов реагирования**

A. Разработка ВНД
B. Подготовка Базы событий
C. Разработка классификатора
D. Распределение ролей
E. Определение КПУР (СЗ, КЗ)
F. Выбор методики и проведение расчета резервируемого капитала

6. **Сбор и регистрация событий ОР**

G. Определение процедур мониторинга
H. Установление требований к КИР

7. **Мониторинг**

I. Направление отчетности КИО

J. Тестирование плана ОНиВД
K. Проведение аудитов (внутренних и внешних)
L. Оценка эффективности СУОР
M. Повышения качества СУОР

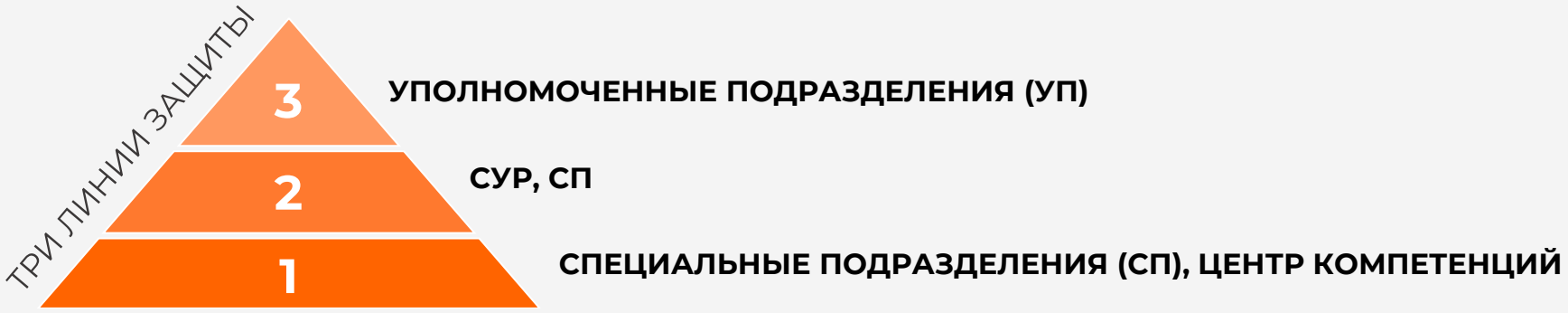
AKTIV.
CONSULTING

Блок II

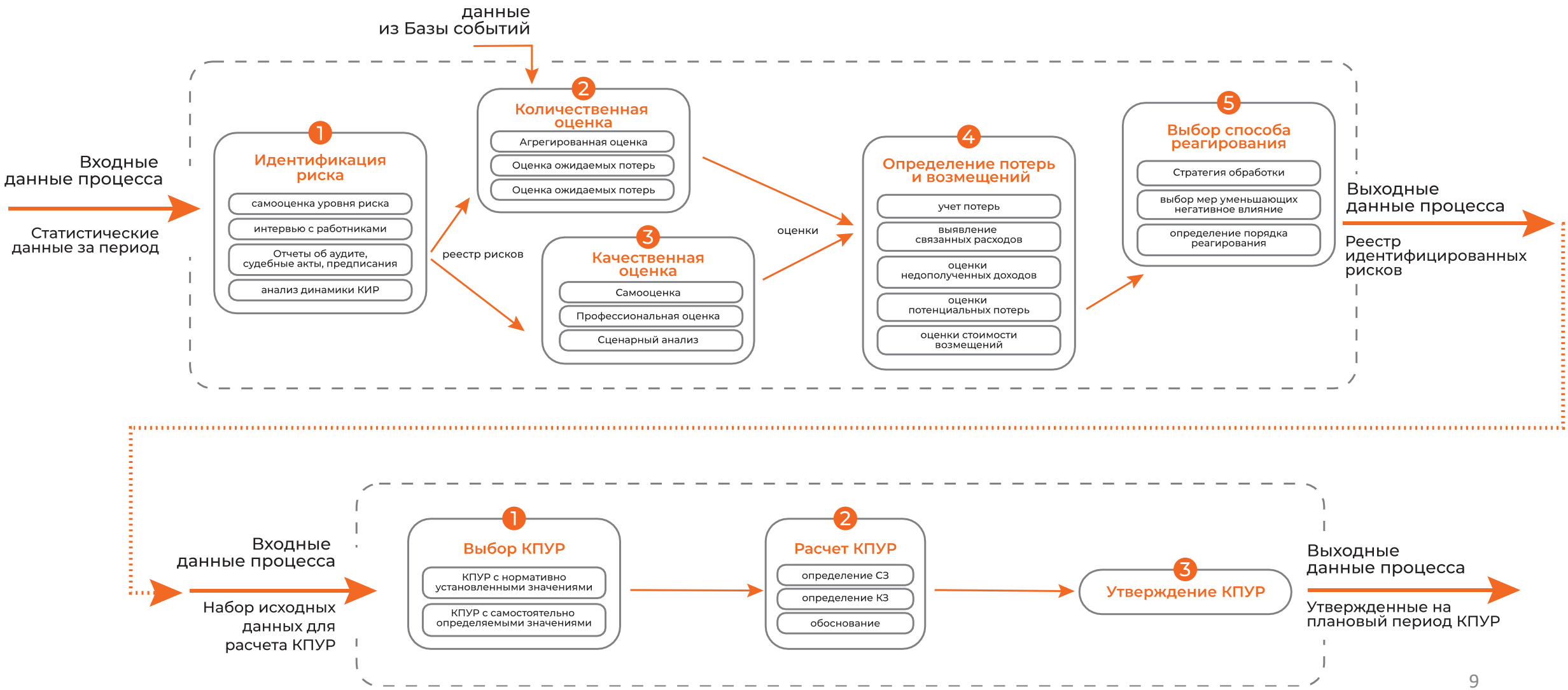
Управление киберрисками в рамках процессов СУОР

Дополнительные требования в управлении КР

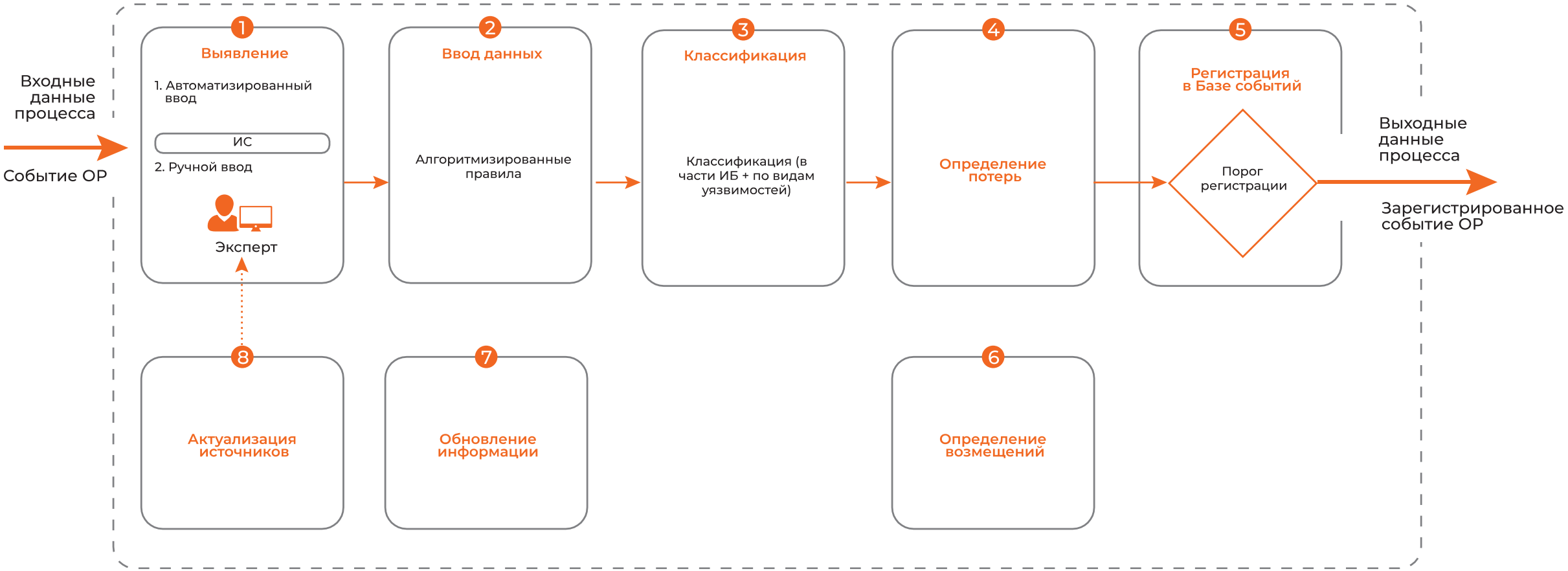
- **Значение КПУР рискам ИБ принятым в КО значениям**
- **Идентификация и оценка КР**
- **Участие совета директоров и КИО в управлении КР**
- Исключение конфликта интересов
- Защита от угроз ИБ при аутсорсинге
- Выявление компьютерных атак
- Порядок реагирования
- Обмен с ФинЦЕРТ
- Ресурсное обеспечение
- Осведомленность и обучение работников
- Аудит
- Актуальность политики ИБ
- PDCA повышения управления риском ИБ
- Порядок применения прикладного ПО
- Пентест и анализ уязвимостей
- Независимая оценка соответствия



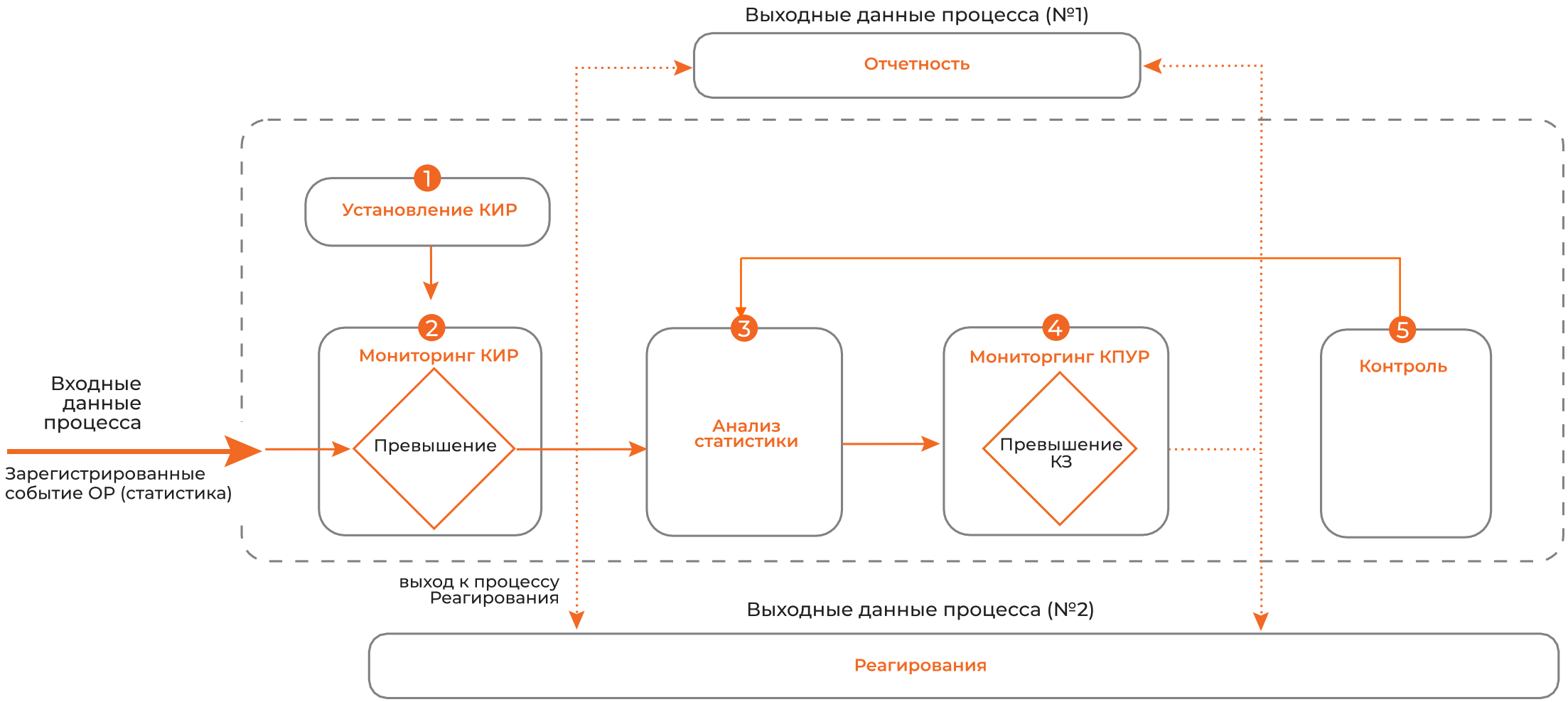
Процессы управления КР
(установление показателей на плановый период)



Процессы управления КР
(обработка событий КР: регистрация)



Процессы управления КР
(обработка событий КР: мониторинг)



AKTIV.
CONSULTING

В качестве резюме

1 Отчитываться по внедренным процессам в рамках 716-П придется в самое ближайшее время

2 Даже если в ФО нет СУОР, внедрение процесса управления киберрисками по 716-П входит в зону ответственности службы ИБ

AKTIV.
CONSULTING

Александр Моисеев

Ведущий консультант
по информационной безопасности

moiseev@aktiv.consulting