AKTIV.
CONSULTING

Управление рисками ИБ и обеспечение операционной надежности 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 рисками ИБ
Блок III	Обеспечение операционной надежности

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	Определяются организацией
3	**База событий (new)**	(В составе элемента 2) Набор регистрируемых параметров	(Гл. 6) Требования к консолидированному и раздельному ведению, установлению порога регистрации
4	**Классификатор (new)**	(В составе элемента 2) Признаки классификации и атрибуты	(Гл. 3 + Пр.4 и 5) Требования к делению классификационных признаков
5	**Контрольные показатели уровня риска (КПУР) (new)**	Количественные и качественные показатели	(Гл. 5 + Пр. 1) Требования к установлению целевых, сигнальных и контрольных значений
6	Процедуры управления ОР	Идентификация ОР, количественная и качественная оценка, определение потерь и возмещений, реагирование	(Гл. 2) Требования к оперативности реагирования и оповещения, к периодичности проведения процедур
7	Дополнительные элементы СУОР	Политики, регламенты и методики, а также вспомогательные процессы	(Гл. 4) Требования к периодичности аудита, пересмотру процедур и актуализации

Основные процедуры управления ОР по 716-П

I. Процедуры расчета показателей для организации на плановый период (на год)

1. Идентификация риска
2. Количественная оценка уровня риска
3. Качественная оценка уровня риска
4. Определение потерь и возмещений
5. Выбор и применение способа реагирования

Реестр идентифицированных рисков

Установление КПУР

Значения КПУР

II. Процедуры оперативной обработки конкретных событий ОР (в течении года)

Событие риска

6. Сбор и регистрация рисковых событий

Зарегистрированные события риска

7. Мониторинг (КИР, КПУР)

Примеры КПУР и КИР

КПУР
на плановый период по организации
по направлению деятельности
информационной безопасности

«Общая сумма валовых прямых потерь от реализации событий риска ИБ за отчетный период (год) с нарастающим итогом с начала календарного года»

Целевое значение: 5 млн руб.

Сигнальное значение: 0,25 млн руб.

Контрольное значение: 1 млн руб.

КИР
на конкретный
идентифицированный риск ИБ
или инцидент ОН

«Превышение средней мощности DDoS-атаки на веб-сайт в 10 Гбит/с»

AKTIV.
CONSULTING

Важное по первому блоку

1 Новые для ИБ сущности 716-П: база событий, классификатор, КПУР

2 Процедуры делятся на:

- установление значений показателей на год
- оперативную обработку событий риска в течении года

3 КПУР: финансовая характеристика ожидаемых результатов воздействия событий риска на всю организацию

КИР: техническая характеристика конкретного события риска

AKTIV. CONSULTING

AKTIV.
CONSULTING

Блок II

Управление рисками ИБ

Дополнительные требования для управлении рисками ИБ

Глава 7 716-П

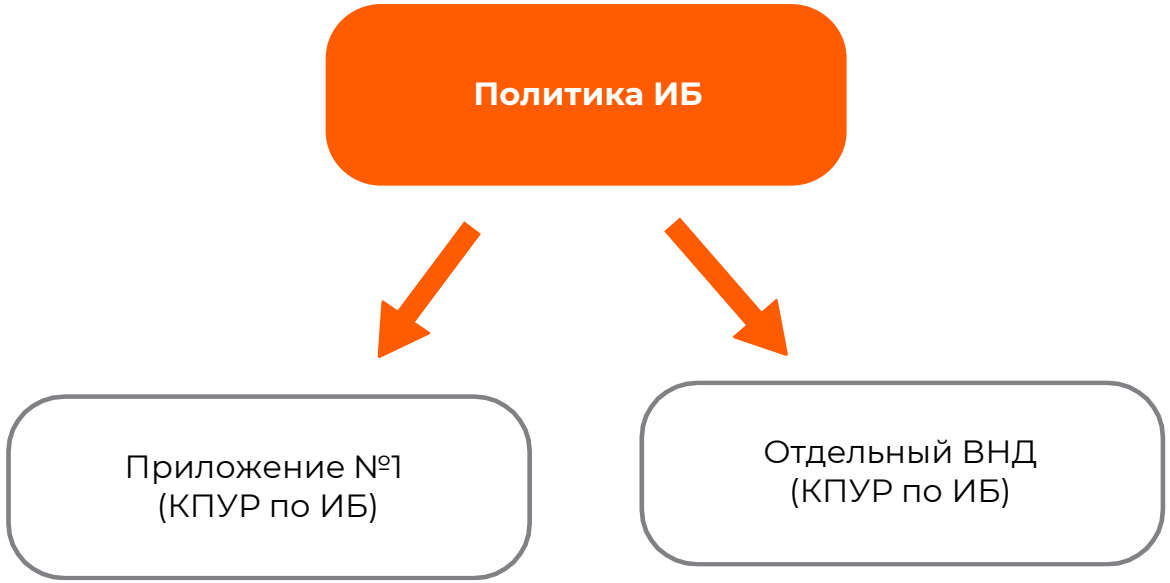
- **Идентификация и оценка рисков ИБ**
- **Значение КПУР рискам ИБ принятым в КО значениям**
- **Участие совета директоров и КИО в управлении рисками ИБ**
- Исключение конфликта интересов
- Защита от угроз ИБ при аутсорсинге
- Выявление компьютерных атак
- Порядок реагирования
- Обмен с ФинЦЕРТ
- Ресурсное 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

ГОСТ УР (проект)

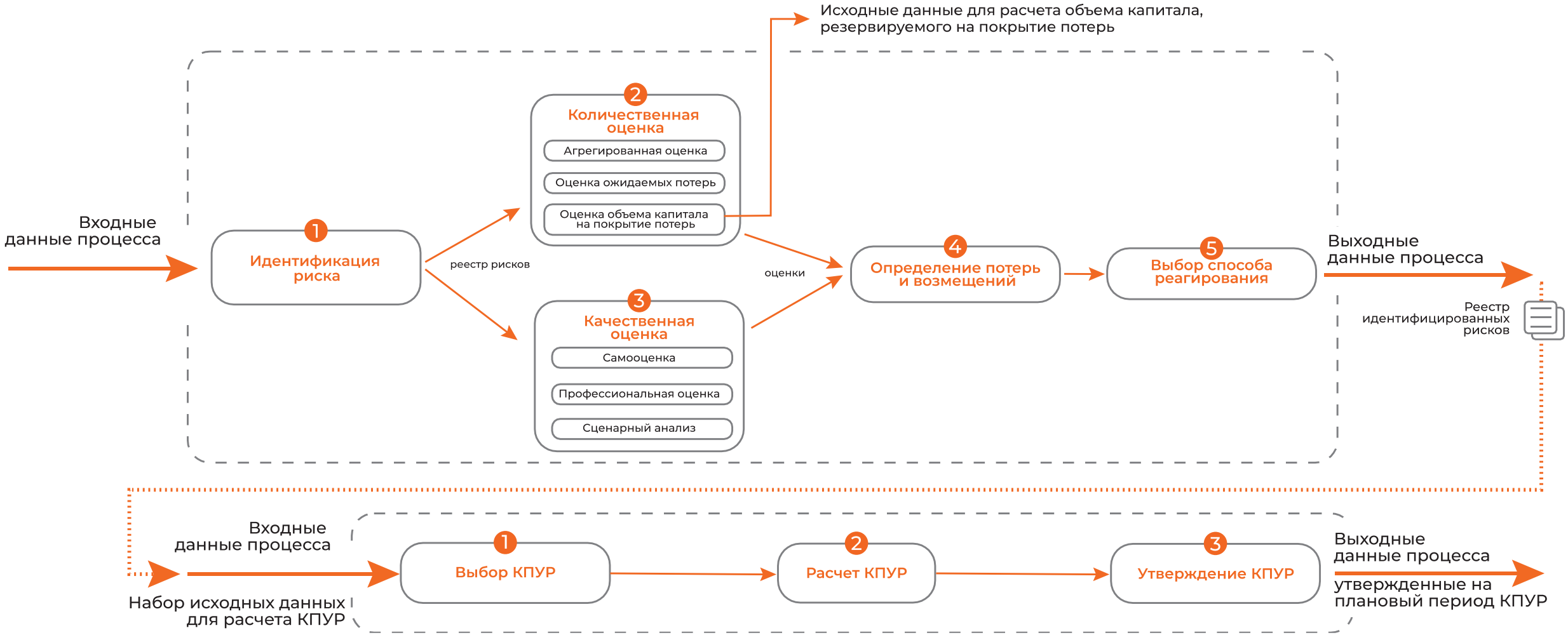
Дополнение Политики ИБ

1 Функциями и ответственностью работников, участвующих в управлении рисками ИБ

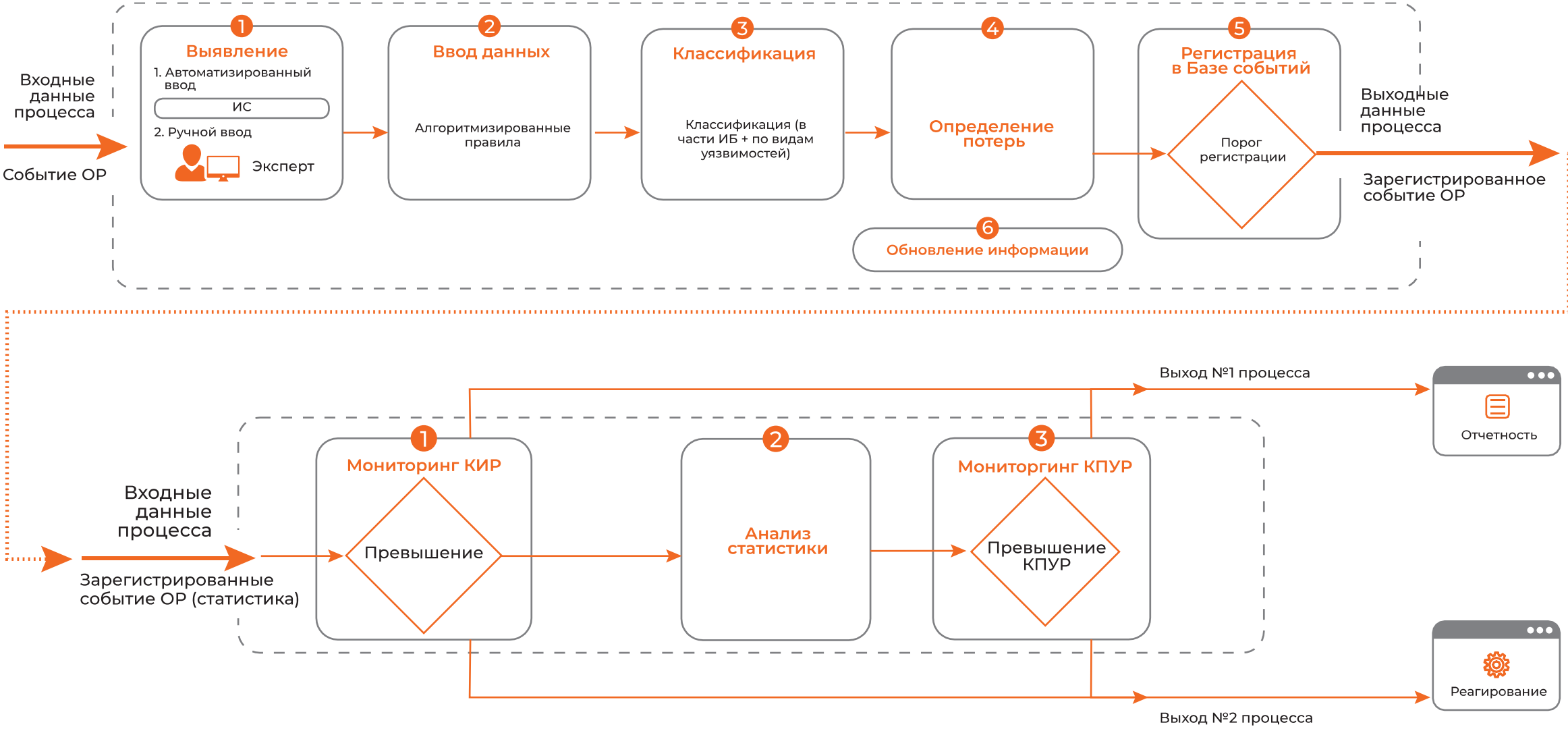
2 Вынести в отдельные приложения, либо ВНД установленные сигнальные и контрольные значения контрольных показателей уровня риска ИБ



Установление показателей на плановый период



Оперативная обработка событий риска ИБ



Важное по второму блоку

1. Существующие процессы управления рисками ИБ можно адаптировать к требованиям 716-П

2. Распределение ролей и обязанностей по управлению рисками ИБ по концепции «трех линий защиты»

AKTIV. CONSULTING

AKTIV.
CONSULTING

Блок III

Обеспечение операционной надежности

Различия инцидентов ЗИ и ОН, событий риска ИБ

Инциденты ЗИ

нарушение требований к обеспечению ЗИ

ВПО было обнаружено и удалено на почтовом шлюзе

Событие риска ИБ

инцидент ЗИ, который привел к прямым и непрямым потерям

ВПО прошло механизмы защиты почтового шлюза, было обнаружено и удалено на хосте

Инцидент ОН

произошедший в рамках события ОР: совершенный во время нарушения ТП, вызванный угрозами или сбоями ИТ-инфраструктуры привел к неоказанию (ненадлежащему оказанию) банковских услуг

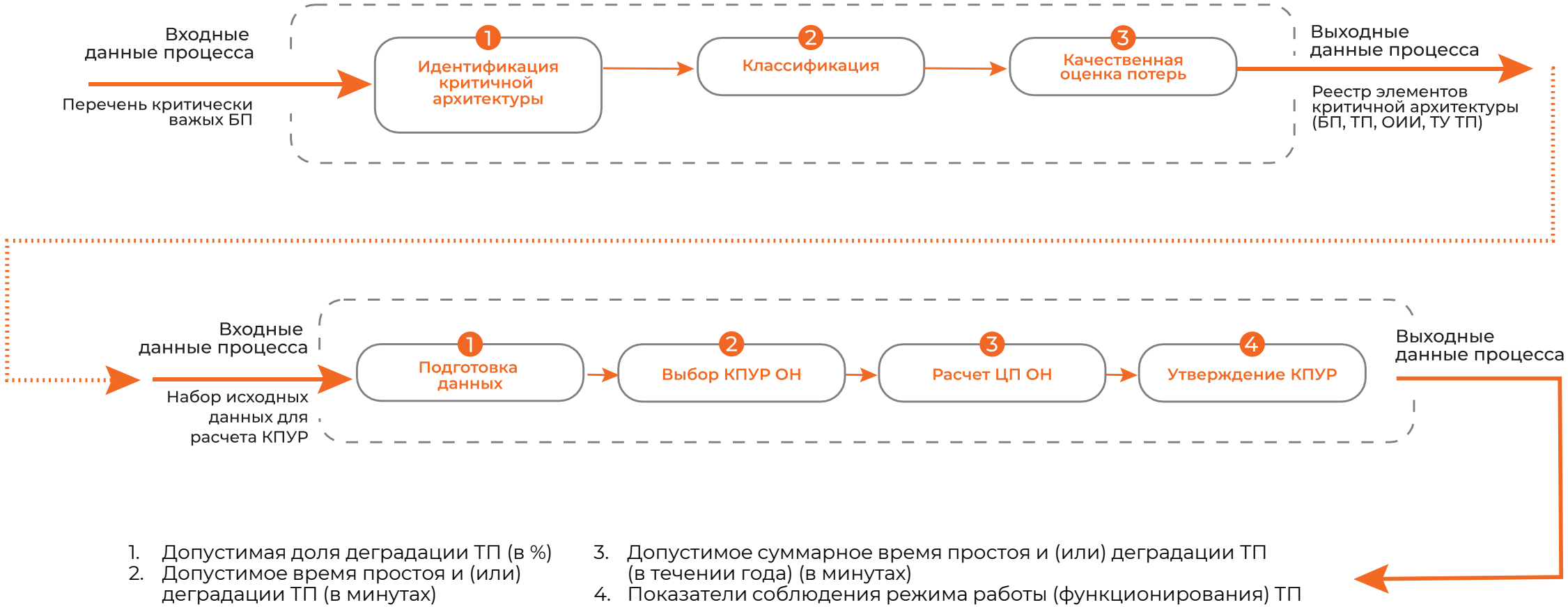
Попытка удаления ВПО не была успешной и отработала политика изоляции хоста на 4 часа

Основные процессы обеспечения ОН

ПРОЦЕССЫ	ОСНОВНЫЕ МОМЕНТЫ
Идентификация критичной архитектуры	Составление: ▪ Перечней БП (в т.ч. на аутсорисинге) ▪ Реестра элементов критичной архитектуры А также их классификация и инвентаризация
Управление изменениями	▪ Планирование конфигурации и анализ влияния изменений (BIA) ▪ Разделение сред (разработки, тестирования, эксплуатации) ▪ Протоколирование изменений и возможность их отката ▪ Проверка обновлений ПО (в т.ч. code review, SAST, DAST) ▪ Сканирование на уязвимости, пентест, Red team
Обработка инцидентов и восстановление	Установление целевых показателей: ▪ Реагирования (ЦПР) ▪ Восстановления (ЦПВ) ▪ Анализа свидетельств (ЦПАС) ▪ Оценка эффективности реагирования и восстановления (ЦПЭРВ)
Взаимодействие с поставщиками услуг	SLA, внешний аудит цепи поставок, проработка альтернативных поставщиков, контроль удаленного технического обслуживания
Тестирование ОН БП и ТП	Киберучения, тестирование восстановления в периоды целевого времени восстановления (ЦВВ), стресс-тестирование, оценка подготовки персонала
Защита критичной архитектуры при удаленной работе	План ОНиВД (на период удаленной работы), планирование пропускной способности сети и средств защиты информации, безопасность мобильных устройств

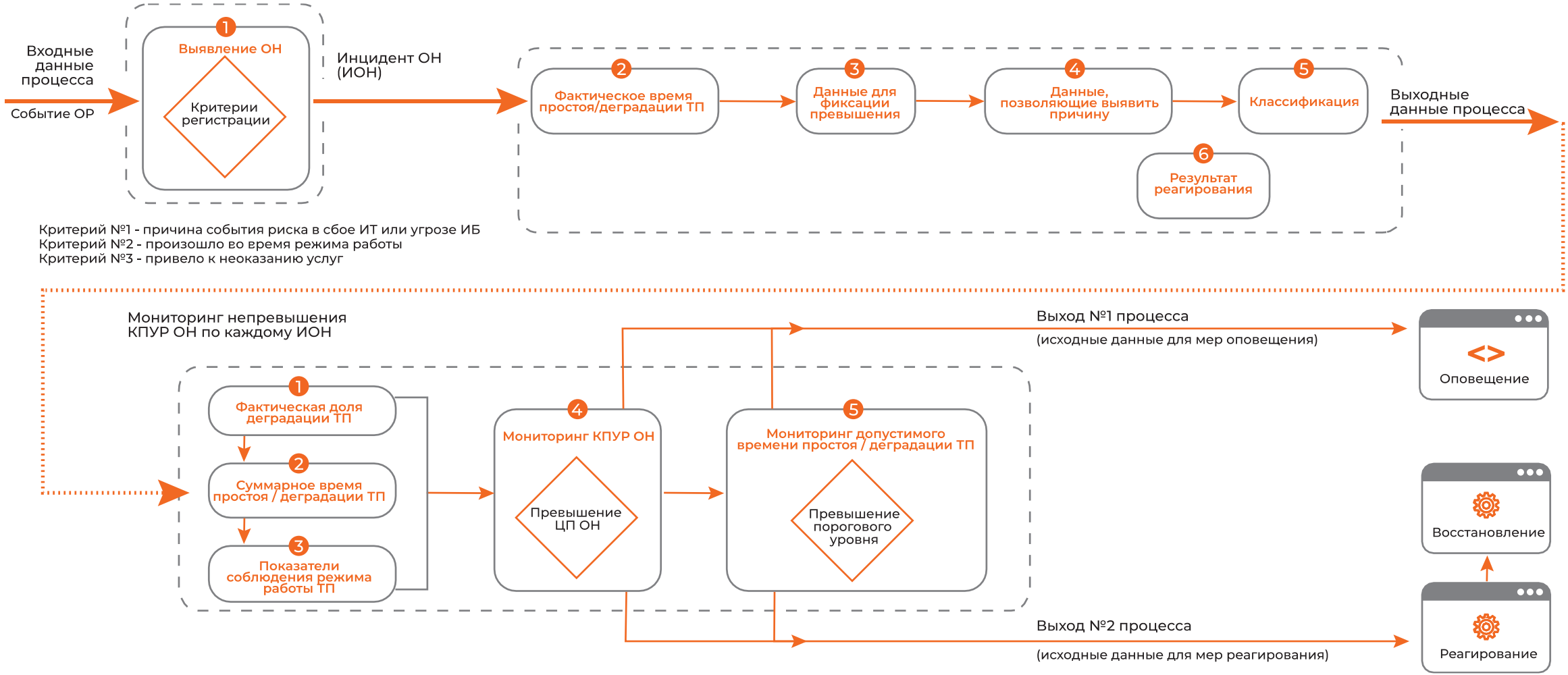
Идентификация критичной архитектуры и установление КПУР ОН

Процесс 1. Идентификация критической архитектуры



1. Допустимая доля деградации ТП (в %)
2. Допустимое время простоя и (или) деградации ТП (в минутах)
3. Допустимое суммарное время простоя и (или) деградации ТП (в течении года) (в минутах)
4. Показатели соблюдения режима работы (функционирования) ТП

Регистрация и мониторинг инцидентов ОН



Важное по третьему блоку

1. Процесс обеспечения ОН тесно связан с управлением рисками ИБ и оптимально функционирует в рамках СУОР по 716-П.

2. Требуется обеспечение фиксации метрик «времени» и «доли» простоя или деградации ТП в банковских ИС.

3. Повышаются требования по скорости реакции на события ОН, а также оповещения ЦБ, партнеров и поставщиков, клиентов.

AKTIV. CONSULTING

В качестве резюме

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

2. Обеспечение операционной надежности оптимальней всего организовывать на базе элементов СУОР.

3. Обеспечение операционной надежности и управление рисками ИБ имеют много точек пересечения, рекомендуем при внедрении актуализации процессов ИБ взаимоувязывать ИБ и ОН.

AKTIV.
CONSULTING

Александр Моисеев

Ведущий консультант
по информационной безопасности

moiseev@aktiv.consulting