

Построение системы управления ИБ (СУИБ) на промышленных предприятиях



Владислав Крылов

Консультант по информационной
безопасности



О чем будет речь?

1

СУИБ – понятие,
регулирование,
отличие от
СОИБ

2

Цели
внедрения
СУИБ

3

Ключевые
составляющие
СУИБ

4

Жизненный
цикл СУИБ

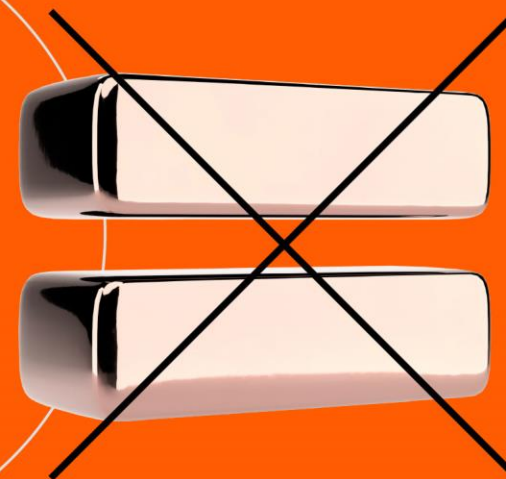


Что такое СУИБ?



Система управления информационной безопасностью — это комплекс организационной структуры и ресурсов, направленных на безопасность информации и управление ею с учетом требований и рисков.

СУИБ

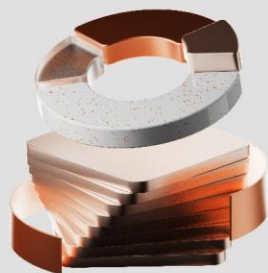


СОИБ

СУИБ / СОИБ – в чем разница?

СОИБ

СУИБ представляет собой комплексный подход к управлению информационной безопасностью, который охватывает все уровни организации.



СОИБ, в свою очередь, фокусируется на технических и операционных аспектах защиты информации. Она включает в себя набор инструментов, технологий и процессов, направленных на защиту информационных активов от угроз.



Цели внедрения СУИБ

Цели внедрения СУИБ

Управление
рисками



Цели внедрения СУИБ

Управление
рисками



Устойчивость
к инцидентам



Цели внедрения СУИБ

Управление
рисками



Устойчивость
к инцидентам



Усиление процессов
безопасности

Цели внедрения СУИБ

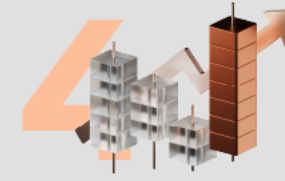
Управление
рисками



Устойчивость
к инцидентам



Усиление процессов
безопасности



Оптимизация
бизнес-процессов

Цели внедрения СУИБ

Управление
рисками



Устойчивость
к инцидентам



Ключевая задача СУИБ:
Без усложнения процессов
сделать их безопасными
и управляемыми!

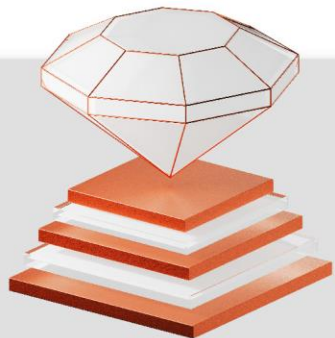


Усиление процессов
безопасности



Оптимизация
бизнес-процессов

На что опираться?



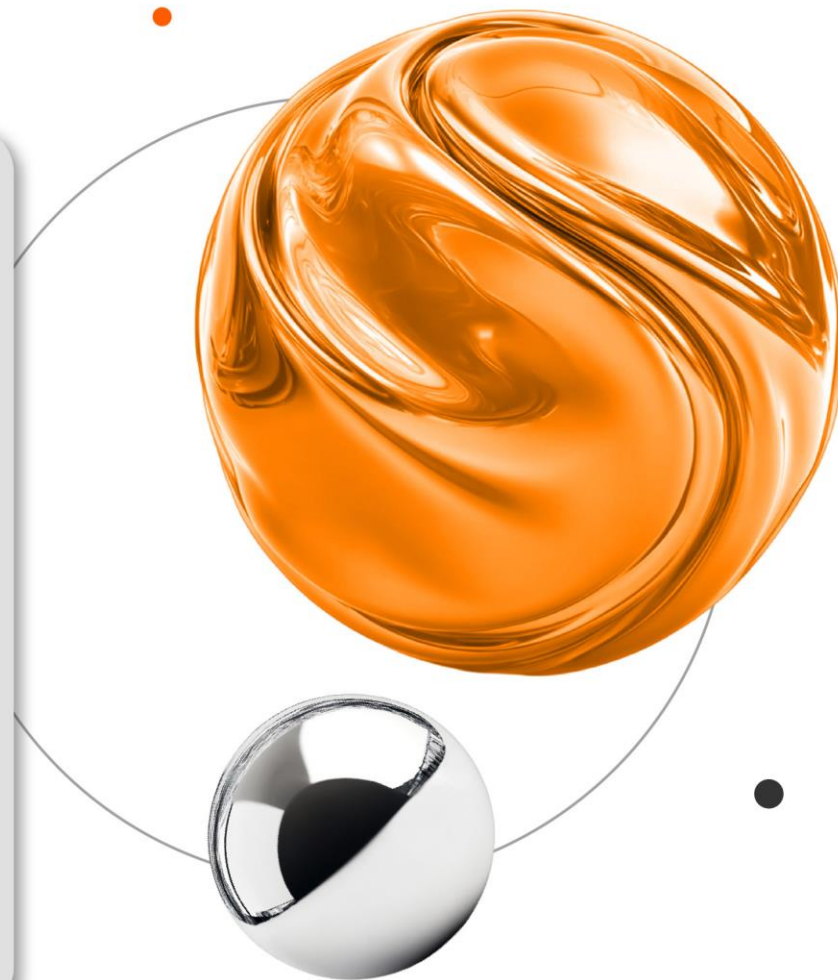
Отечественные документы:

- 📍 ГОСТ Р ИСО/МЭК 27000-2021 (идентичен международному стандарту ИСО/МЭК 27000:2018)

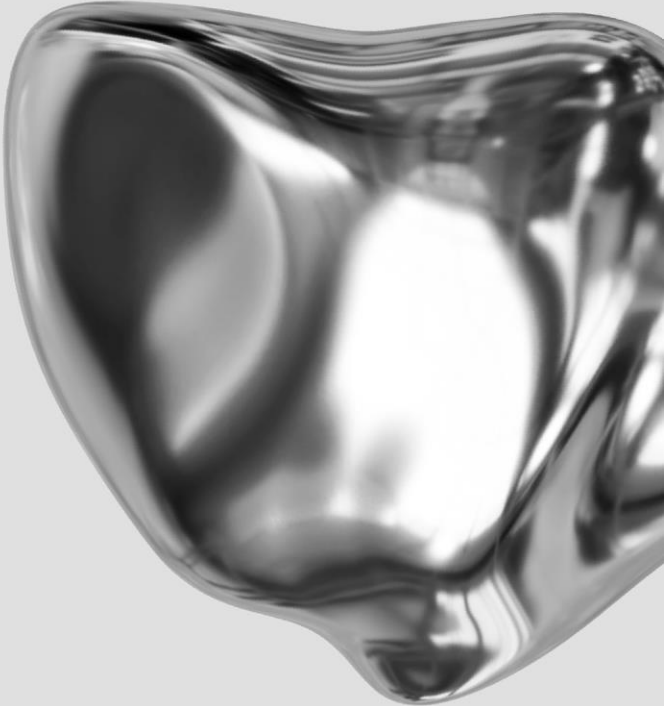
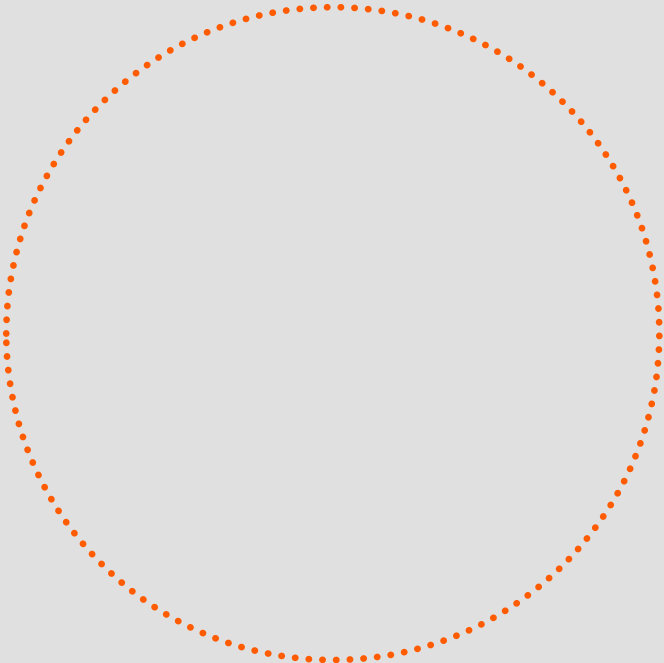
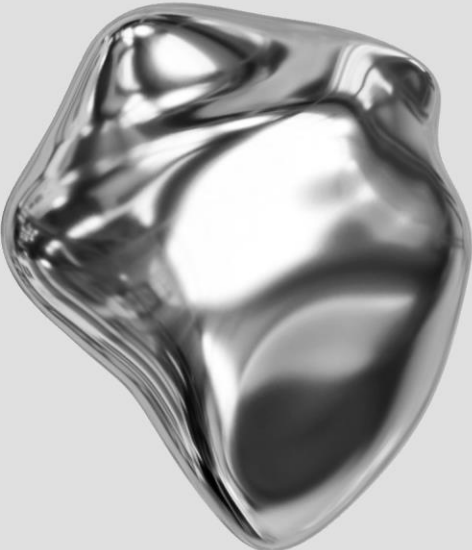


Международные стандарты и рекомендации:

- 📍 ISO/IEC 27001
- 📍 NIST SP 800-53
- 📍 GDPR



Ключевые составляющие **СУИБ**



Ключевые составляющие **СУИБ**

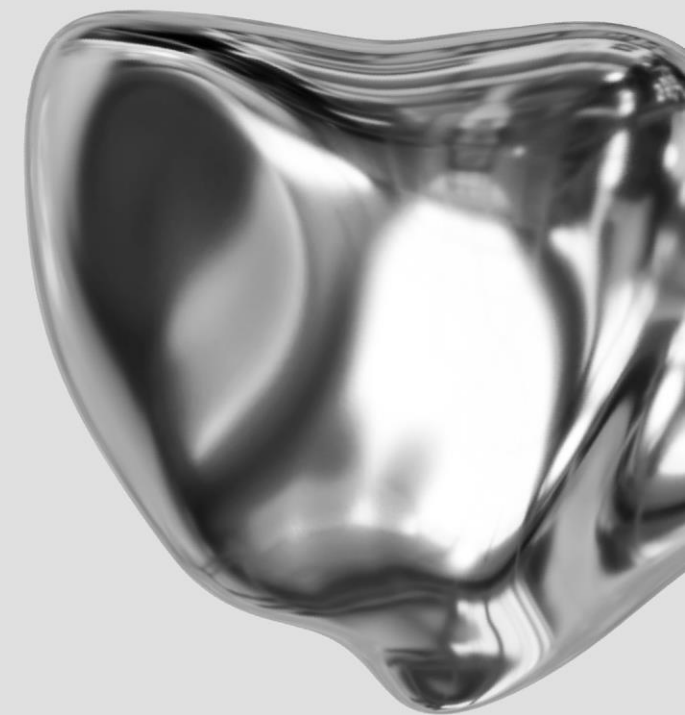
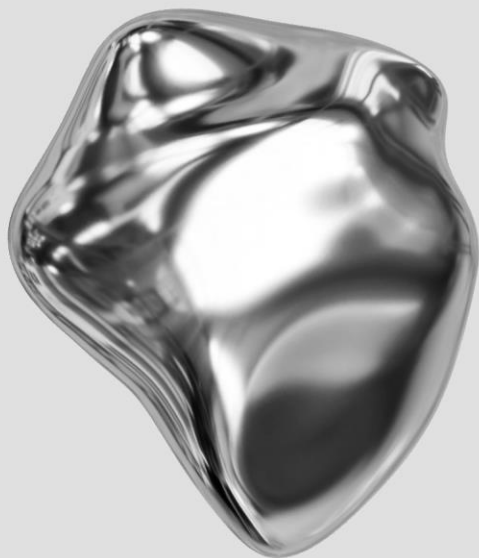


Регламенты

Процедуры

Персонал

**Технические
средства**



Ключевые составляющие **СУИБ**



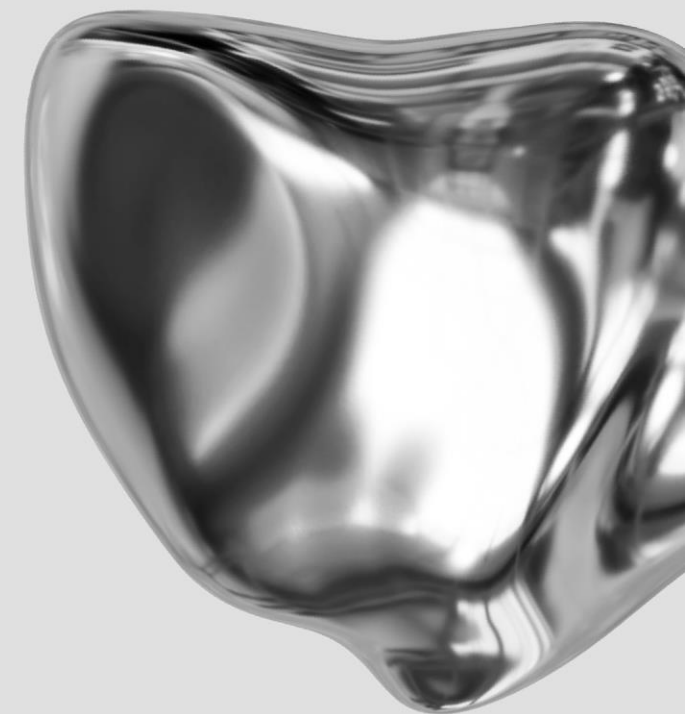
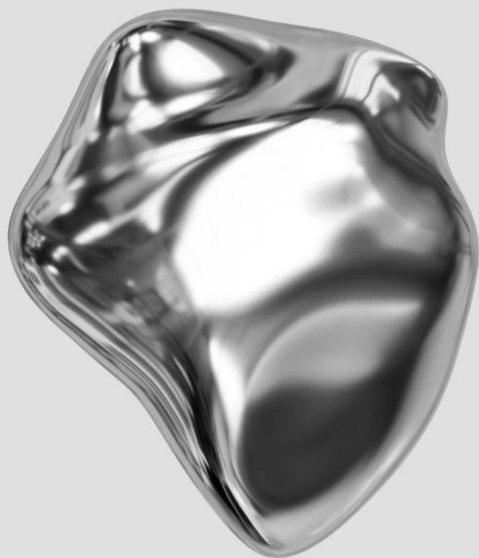
- 📍 Инструмент, а не формальная «бумажка»
- 📍 Соответствие реалиям и бизнес-целям компании

Регламенты

Процедуры

Персонал

Технические средства



Ключевые составляющие СУИБ



- Инструмент, а не формальная «бумажка»
- Соответствие реалиям и бизнес-целям компании

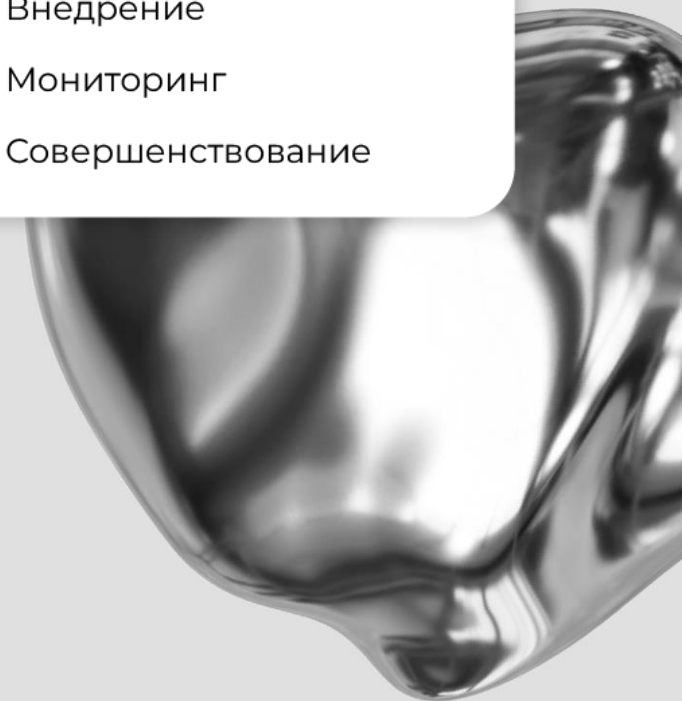
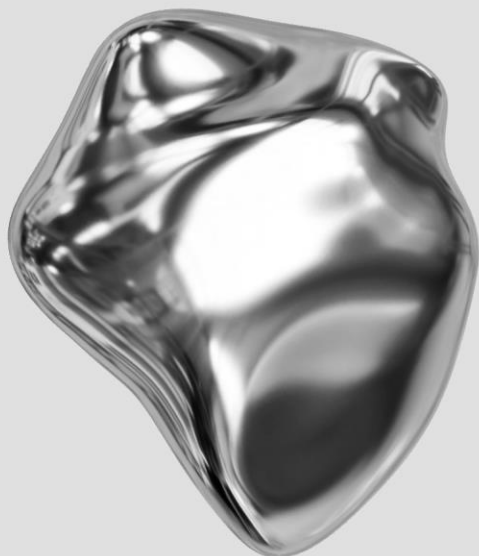
Регламенты

Процедуры

- Планирование
- Внедрение
- Мониторинг
- Совершенствование

Персонал

Технические средства



Ключевые составляющие СУИБ



- Инструмент, а не формальная «бумажка»
- Соответствие реалиям и бизнес-целям компании

Регламенты

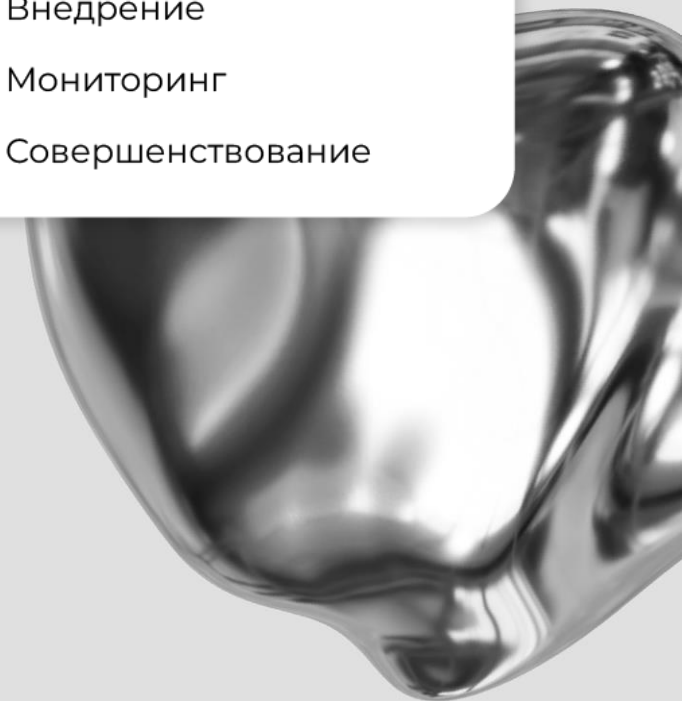
Процедуры

- Планирование
- Внедрение
- Мониторинг
- Совершенствование

- Создание культуры безопасности
- Реализация регламентов

Персонал

Технические средства



Ключевые составляющие СУИБ



- Инструмент, а не формальная «бумажка»
- Соответствие реалиям и бизнес-целям компании

Регламенты

Процедуры

- Планирование
- Внедрение
- Мониторинг
- Совершенствование

- Создание культуры безопасности
- Реализация регламентов

Персонал

Технические средства

- Инструменты для осуществления контроля и управления

Жизненный цикл СУИБ



Жизненный цикл СУИБ

Подготовка

- ⦿ Определение целей и задач
- ✓ Оценка текущего состояния



Жизненный цикл СУИБ

Подготовка

- ⦿ Определение целей и задач
- ✓ Оценка текущего состояния

Внедрение

- ⚙️ Разработка политик и регламентация процессов
- ✨ Обучение сотрудников (контроль компетенций)
- 📦 Внедрение технических средств



Жизненный цикл СУИБ

Подготовка

- ⦿ Определение целей и задач
- ✓ Оценка текущего состояния

Внедрение

- ⚙️ Разработка политик и регламентация процессов
- ✨ Обучение сотрудников (контроль компетенций)
- 📦 Внедрение технических средств

Сопровождение

- ☆ Мониторинг и оценка
- 🔊 Аудит и улучшение



Жизненный цикл СУИБ

Подготовка

- ⦿ Определение целей и задач
- ✓ Оценка текущего состояния

Внедрение

- ⚙️ Разработка политик и регламентация процессов
- ✨ Обучение сотрудников (контроль компетенций)
- 📦 Внедрение технических средств

Сопровождение

- ☆ Мониторинг и оценка
- 🔊 Аудит и улучшение

Жизненный цикл СУИБ

Подготовка

- ⦿ Определение целей и задач
- ✓ Оценка текущего состояния

Внедрение

- ⚙️ Разработка политик и регламентация процессов
- ✨ Обучение сотрудников (контроль компетенций)
- 📦 Внедрение технических средств

Сопровождение

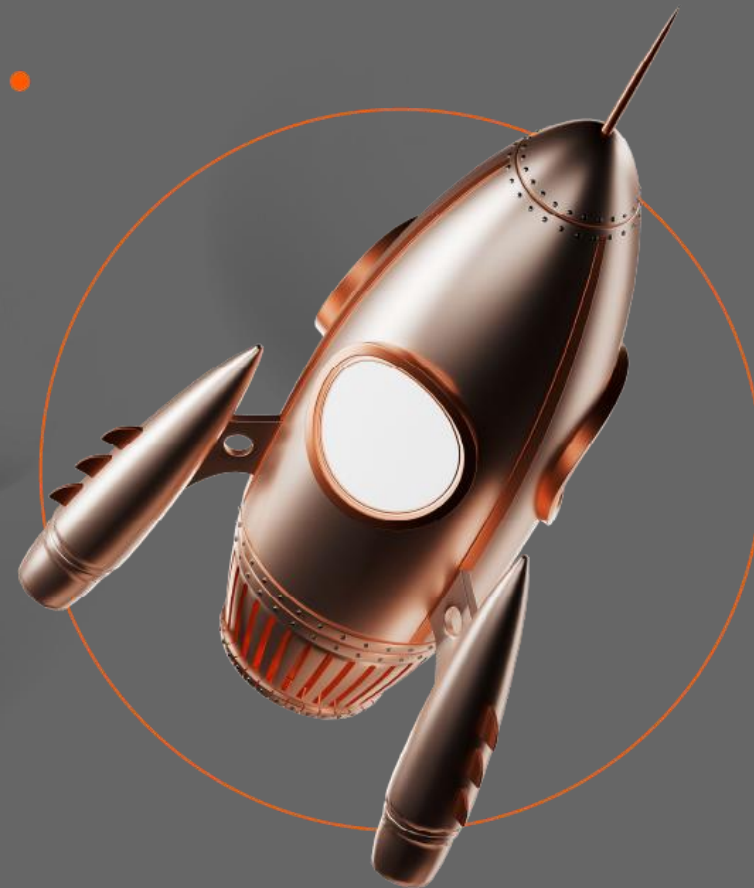
- ☆ Мониторинг и оценка
- 🔊 Аудит и улучшение

СУИБ



Жизненный цикл СУИБ.

Этап 1. Подготовка



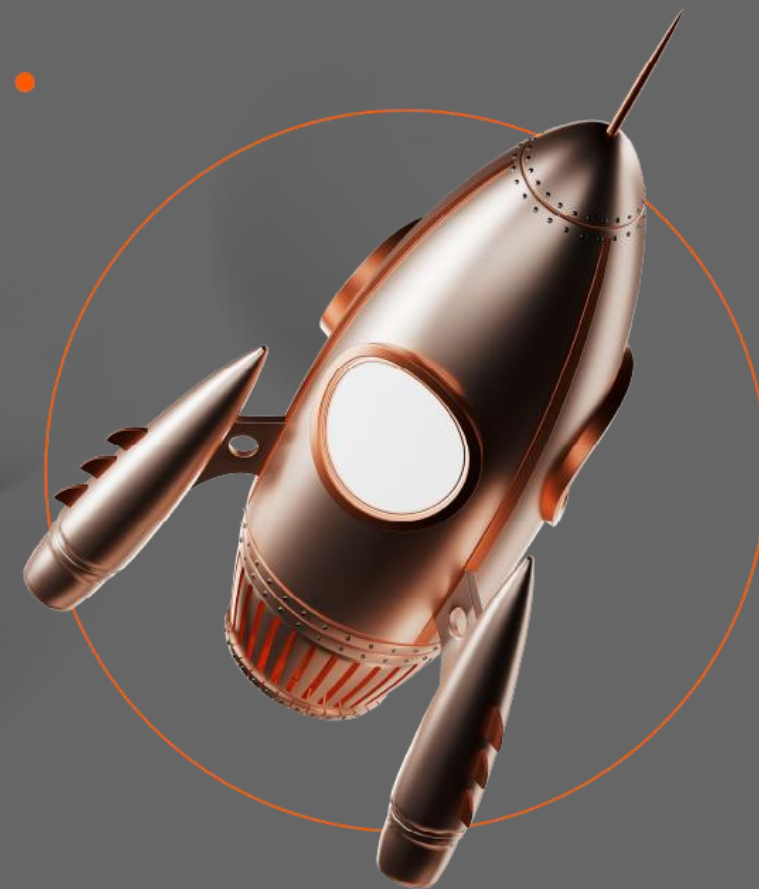
Жизненный цикл СУИБ.

Этап 1. Подготовка

Постановка
задач СУИБ

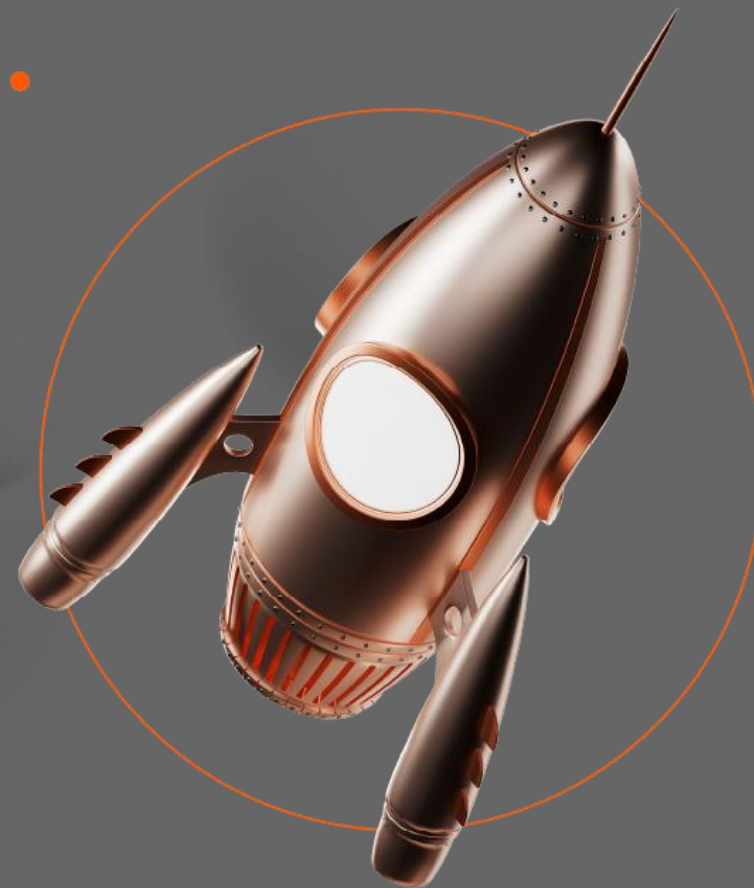
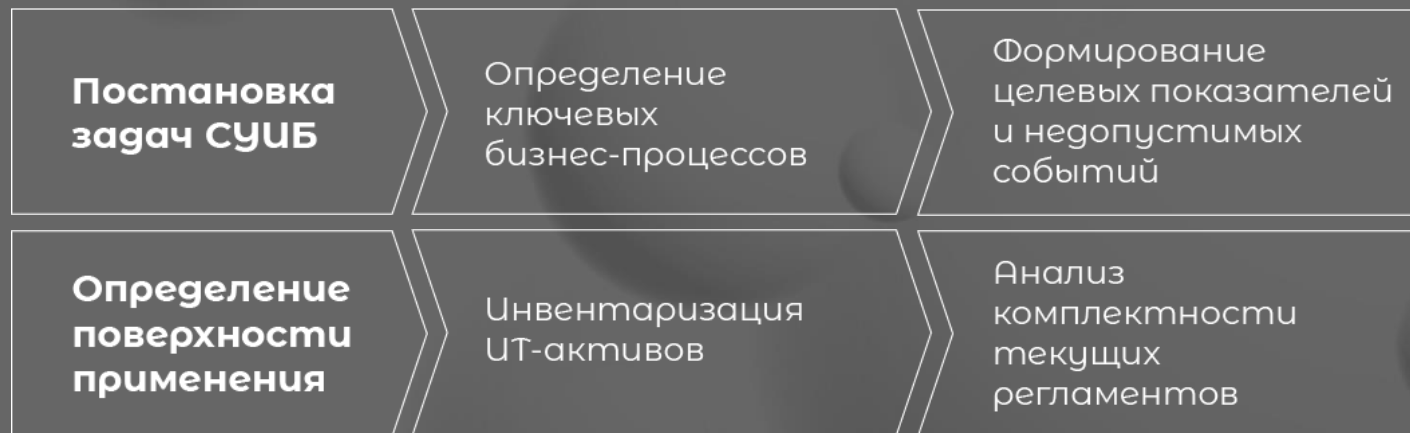
Определение
ключевых
бизнес-процессов

Формирование
целевых показателей
и недопустимых
событий



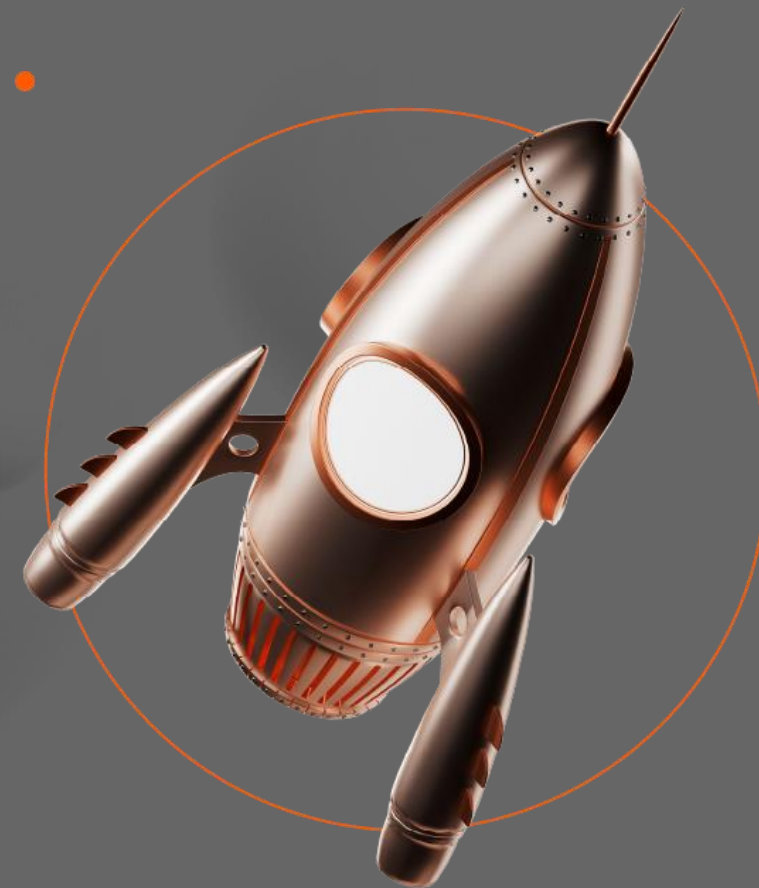
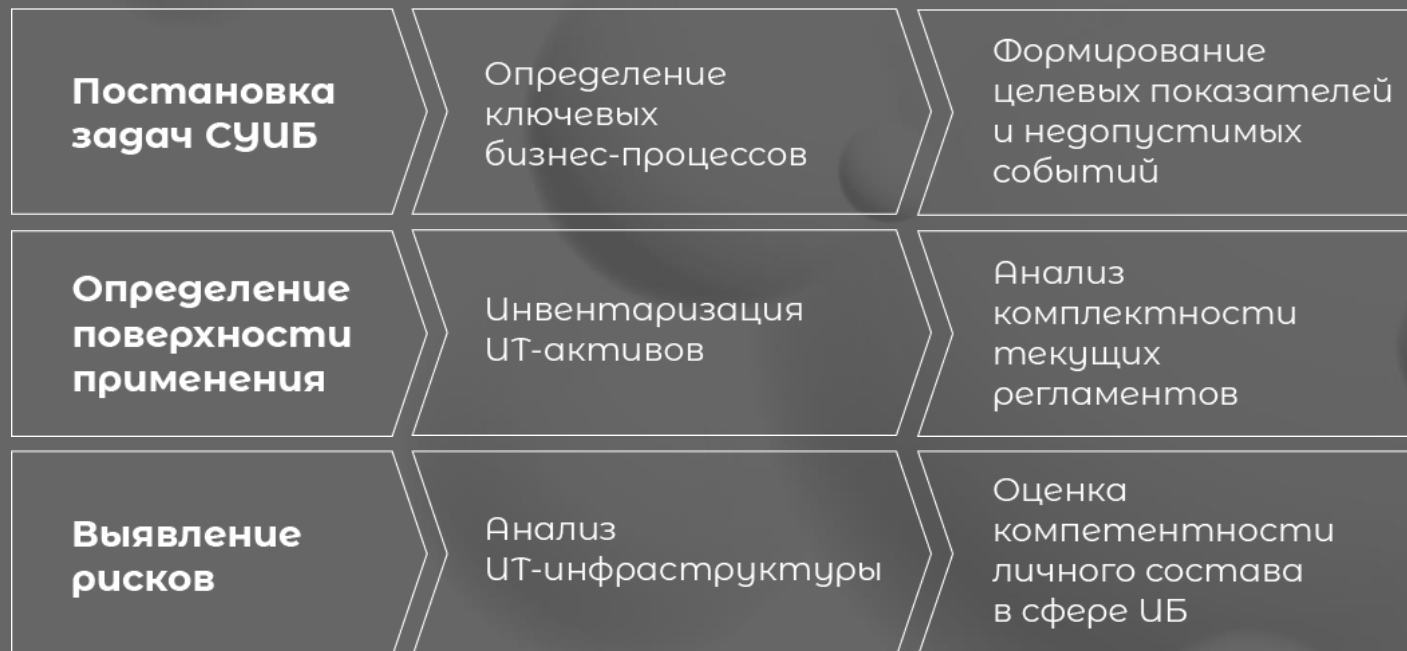
Жизненный цикл СУИБ.

Этап 1. Подготовка



Жизненный цикл СУИБ.

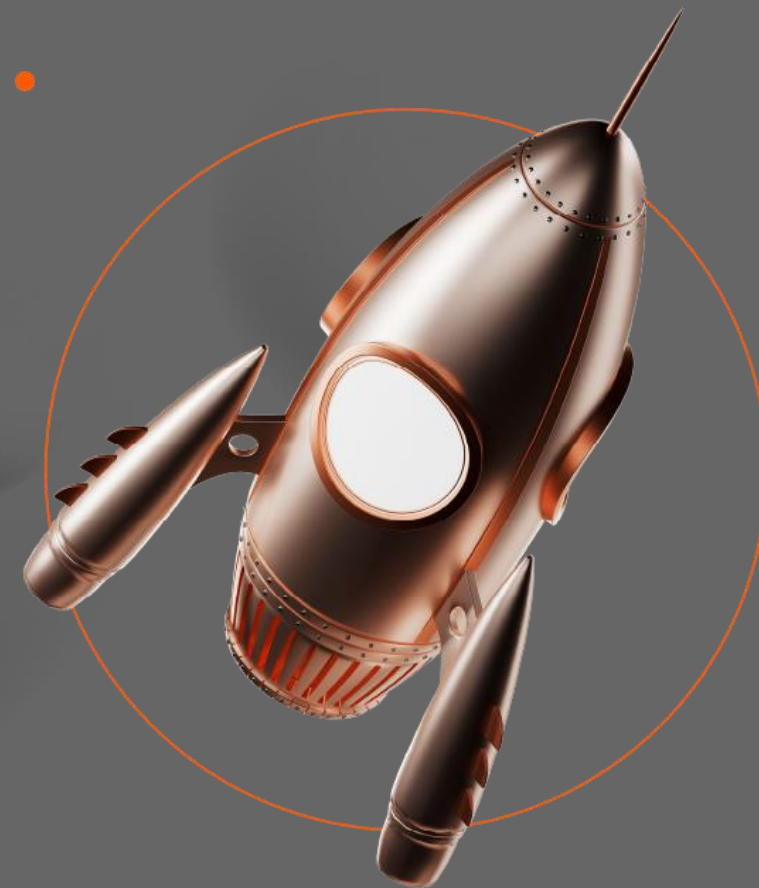
Этап 1. Подготовка



Жизненный цикл СУИБ.

Этап 1. Подготовка

Постановка задач СУИБ	Определение ключевых бизнес-процессов	Формирование целевых показателей и недопустимых событий
Определение поверхности применения	Инвентаризация ИТ-активов	Анализ комплектности текущих регламентов
Выявление рисков	Анализ ИТ-инфраструктуры	Оценка компетентности личного состава в сфере ИБ
Распределение ролей	Назначение ответственных лиц	Определение зон ответственности сотрудников





СТАЛЕЛИТЕЙНЫЙ ЗАВОД

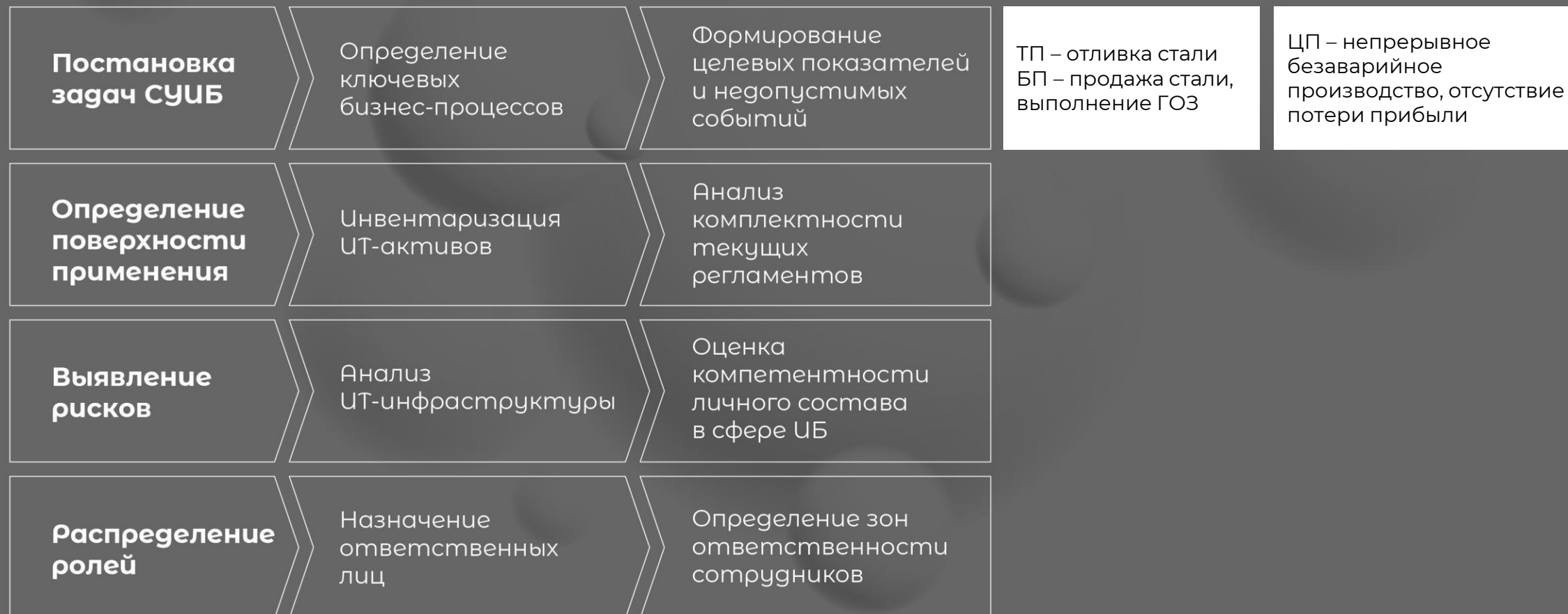
Жизненный цикл СУИБ.

Этап 1. Подготовка



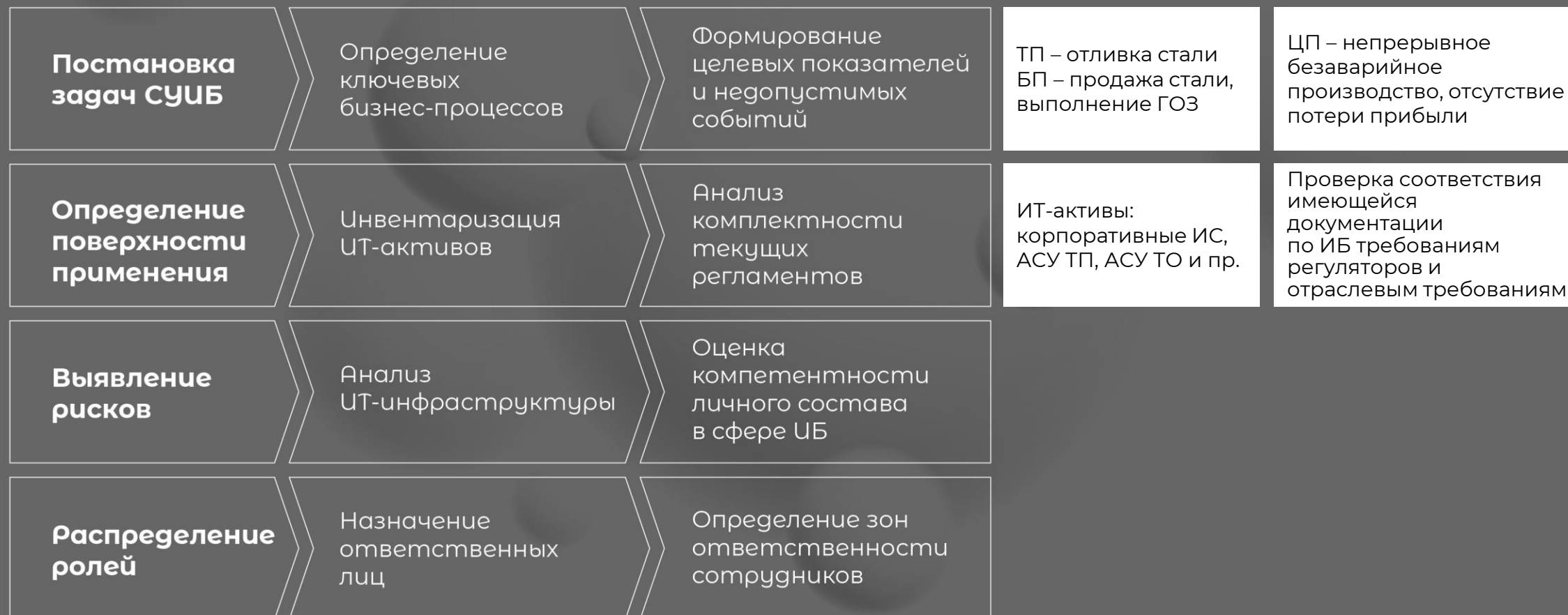
Жизненный цикл СУИБ.

Этап 1. Подготовка



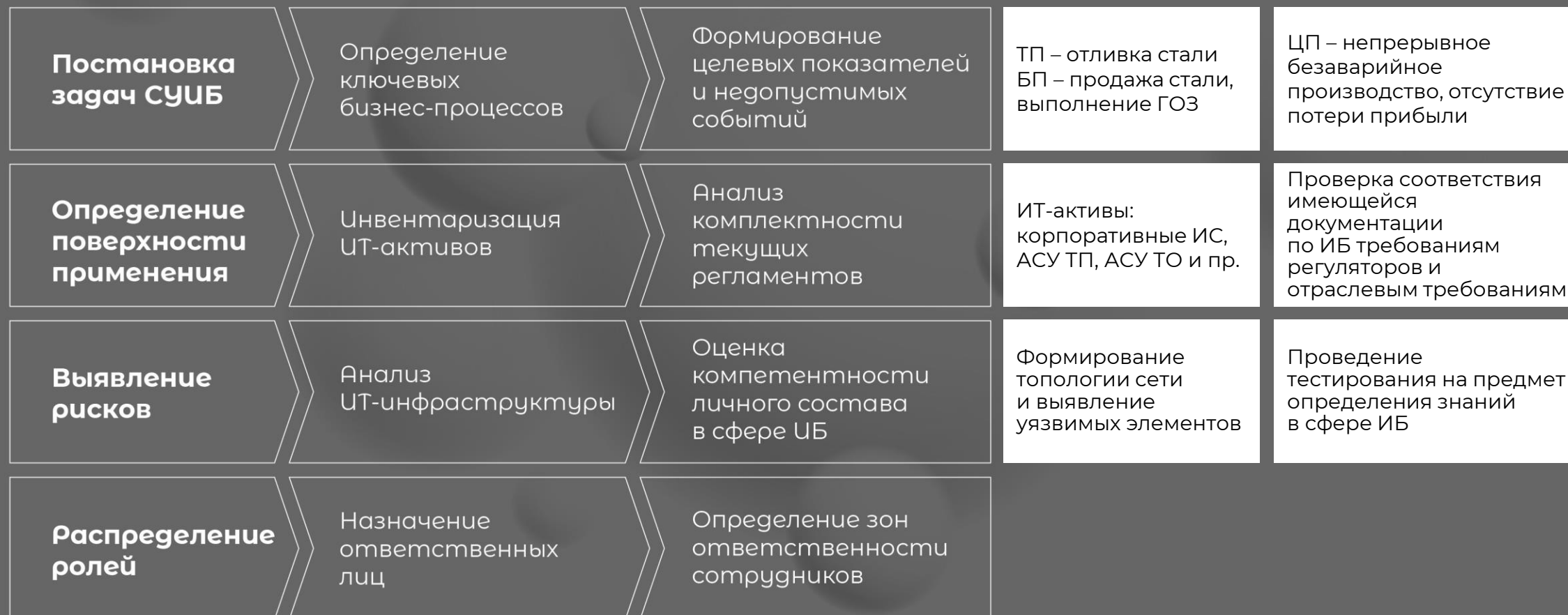
Жизненный цикл СУИБ.

Этап 1. Подготовка



Жизненный цикл СУИБ.

Этап 1. Подготовка



Жизненный цикл СУИБ.

Этап 1. Подготовка

Постановка задач СУИБ	Определение ключевых бизнес-процессов	Формирование целевых показателей и недопустимых событий	ТП – отливка стали БП – продажа стали, выполнение ГОЗ	ЦП – непрерывное безаварийное производство, отсутствие потери прибыли
Определение поверхности применения	Инвентаризация ИТ-активов	Анализ комплектности текущих регламентов	ИТ-активы: корпоративные ИС, АСУ ТП, АСУ ТО и пр.	Проверка соответствия имеющейся документации по ИБ требованиям регуляторов и отраслевым требованиям
Выявление рисков	Анализ ИТ-инфраструктуры	Оценка компетентности личного состава в сфере ИБ	Формирование топологии сети и выявление уязвимых элементов	Проведение тестирования на предмет определения знаний в сфере ИБ
Распределение ролей	Назначение ответственных лиц	Определение зон ответственности сотрудников	Определение должностей, заинтересованных в реализации СУИБ	Формирование ролевой модели по подразделениям исходя из обрабатываемой информации

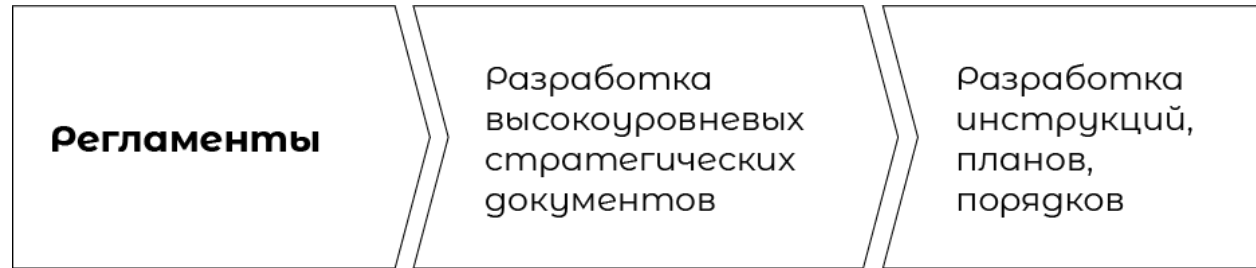
Жизненный цикл СУИБ.

Этап 2. Внедрение



Жизненный цикл СУИБ.

Этап 2. Внедрение



Жизненный цикл СУИБ.

Этап 2. Внедрение



Жизненный цикл СУИБ.

Этап 2. Внедрение

Регламенты	Разработка высокоуровневых стратегических документов	Разработка инструкций, планов, порядков
Обучение	Внешнее	Внутреннее
Технические средства	Средства мониторинга	Средства управления



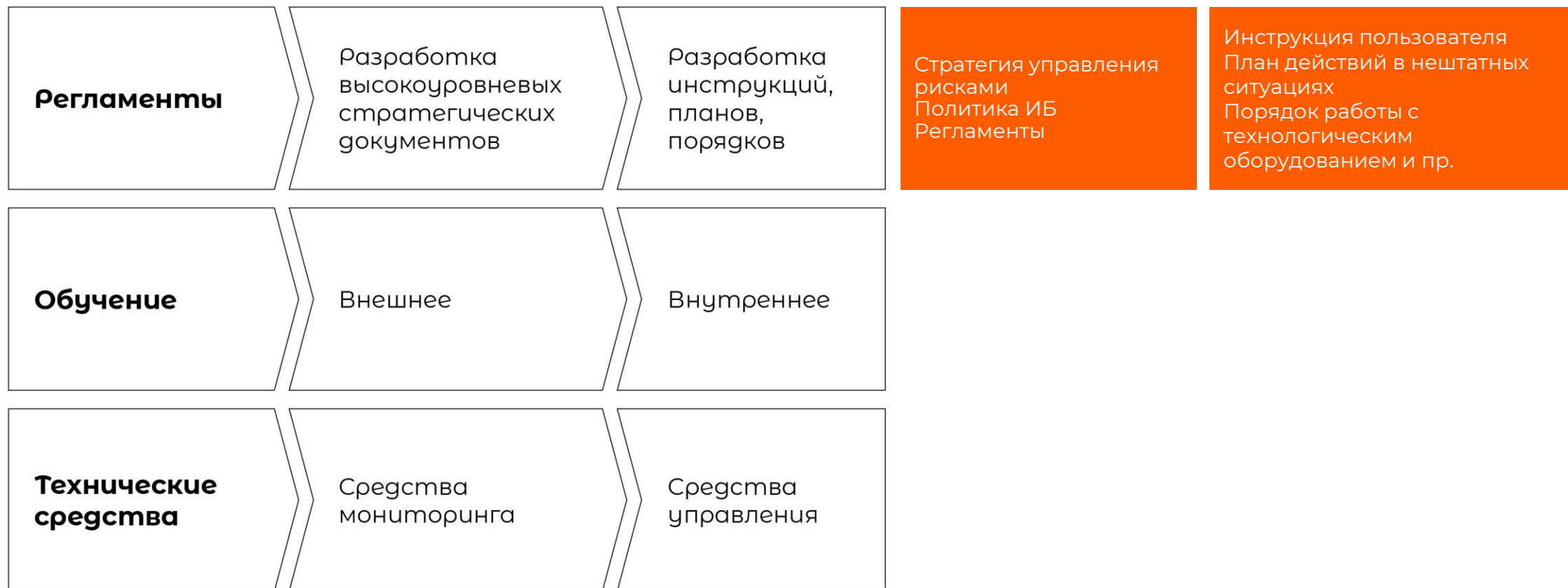
Жизненный цикл СУИБ.

Этап 2. Внедрение



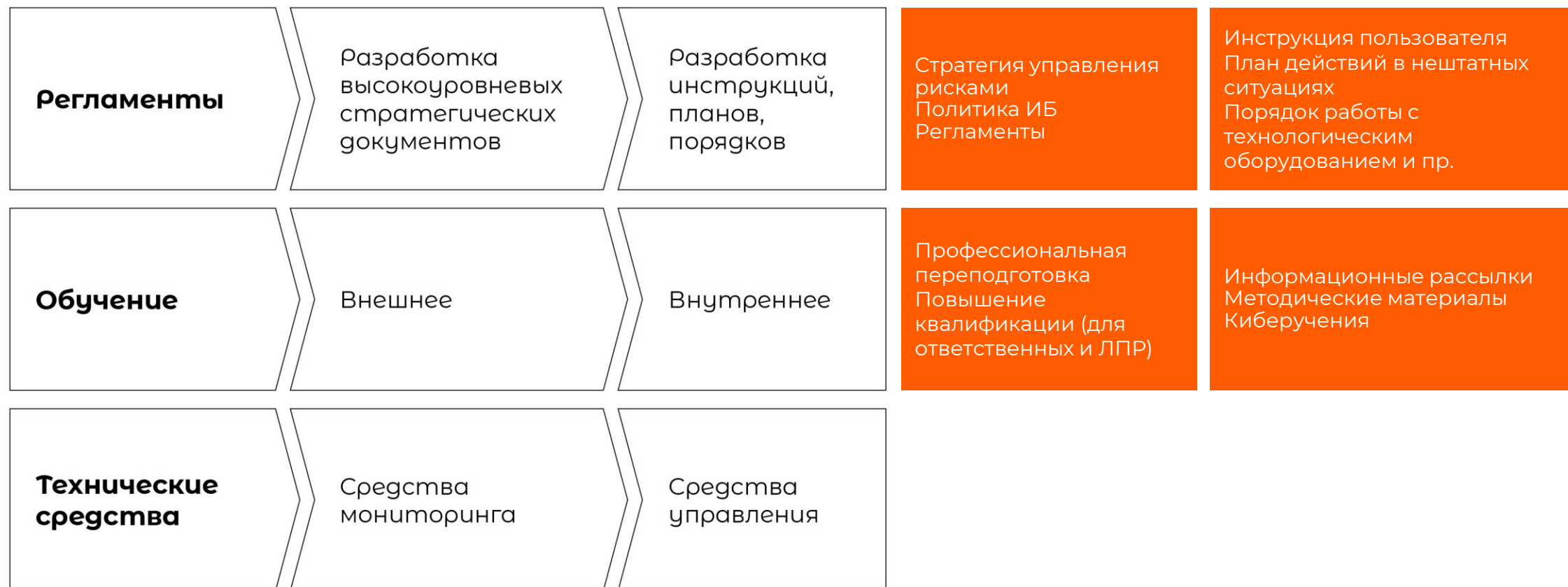
Жизненный цикл СУИБ.

Этап 2. Внедрение



Жизненный цикл СУИБ.

Этап 2. Внедрение



Жизненный цикл СУИБ.

Этап 2. Внедрение



Жизненный цикл СУИБ.

Этап 3. Сопровождение



Жизненный цикл СУИБ.

Этап 3. Сопровождение

**Мониторинг
и оценка**

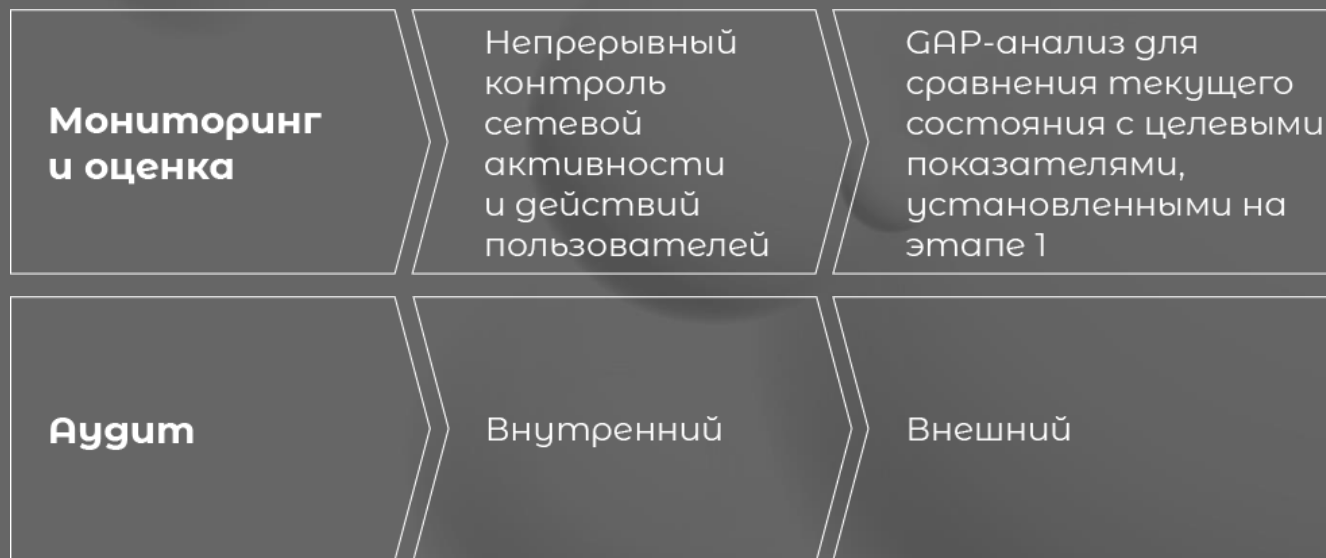
Непрерывный контроль сетевой активности и действий пользователей

GAP-анализ для сравнения текущего состояния с целевыми показателями, установленными на этапе 1



Жизненный цикл СУИБ.

Этап 3. Сопровождение



Жизненный цикл СУИБ.

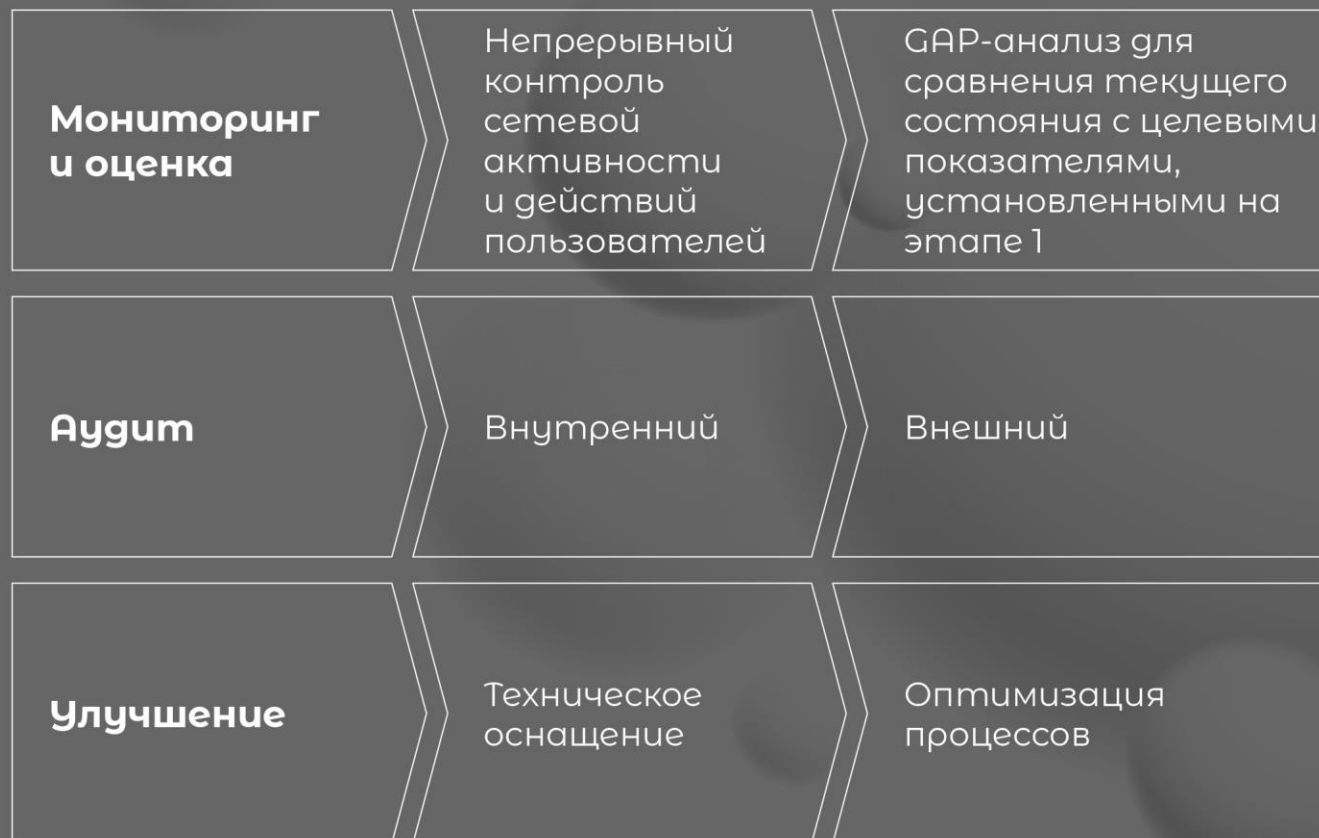
Этап 3. Сопровождение

Мониторинг и оценка	Непрерывный контроль сетевой активности и действий пользователей	GAP-анализ для сравнения текущего состояния с целевыми показателями, установленными на этапе 1
Аудит	Внутренний	Внешний
Улучшение	Техническое оснащение	Оптимизация процессов



Жизненный цикл СУИБ.

Этап 3. Сопровождение



Жизненный цикл СУИБ.

Этап 3. Сопровождение



Жизненный цикл СУИБ.

Этап 3. Сопровождение



Жизненный цикл СУИБ.

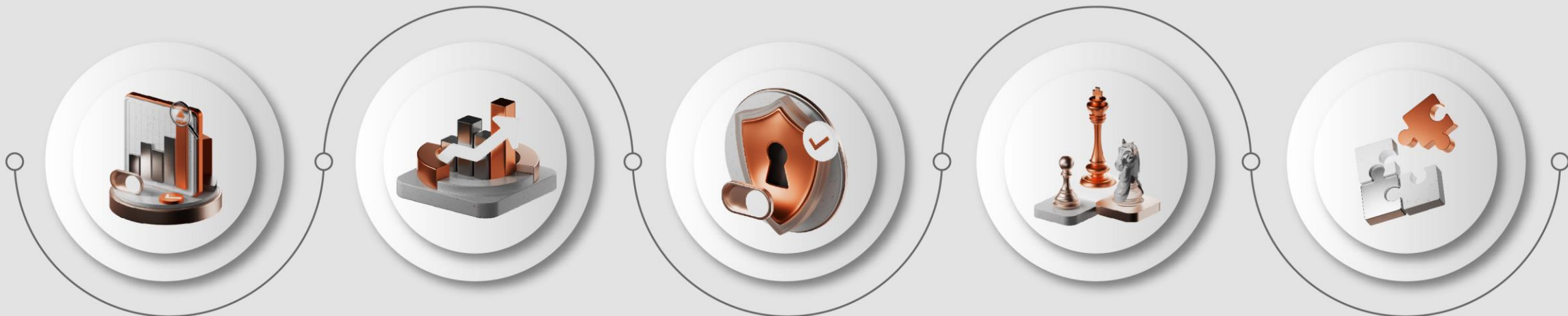
Этап 3. Сопровождение



Положительные аспекты внедрения СУИБ

Минимизация
рисков

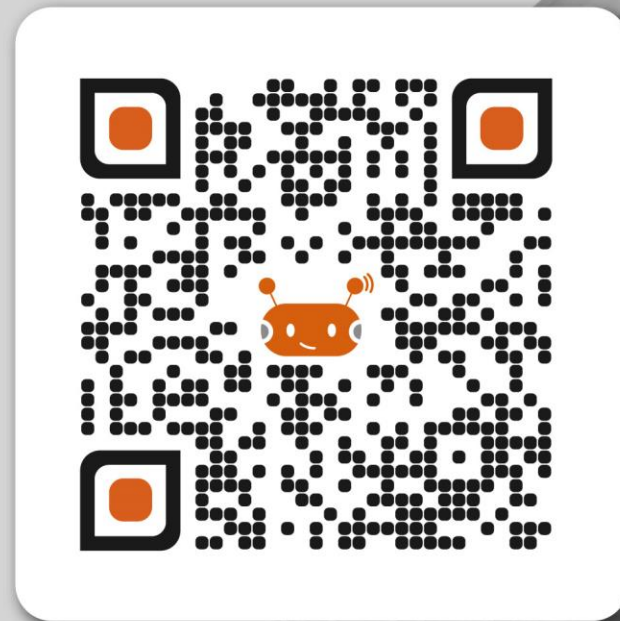
Доверие
клиентов
и партнеров



Системный
подход к ИБ

Культура
безопасности
в компании

Динамичность
и адаптивность



БЛАГОДАРЮ ЗА ВНИМАНИЕ!

AKTIV.
CONSULTING



Владислав Крылов

Консультант по информационной
безопасности

krylov@aktiv.consulting

