



## Создание системы обеспечения безопасности ОКИИ (АСУ ТП). Типовые ошибки на этапах категорирования, проектирования и внедрения

---

Алексей Орехов

Руководитель производственно-  
технологического управления

[www.ntc-vulkan.ru](http://www.ntc-vulkan.ru)

# ИТЦ «ВУЛКАН» - НЕЗАВИСИМЫЙ ЭКСПЕРТ И ИНТЕГРАТОР ТЕХНОЛОГИЙ ИБ



На рынке с **2010** года



**150+** сотрудников в штате



Комплексные решения в сфере экономической и информационной безопасности



Сертифицированная система менеджмента качества



**500+** реализованных проектов в ИБ



Входит в **40** крупнейших компаний РФ в сфере защиты информации

*По версии TAdviser, 2022*



**20+** проектов внедрения SIEM



Допуски и лицензии ФСТЭК, ФСБ, Минобороны, Минпромторг

# ОБЩАЯ ПРОБЛЕМАТИКА «НА ВХОДЕ»

- Построенная бессистемно, «по наитию», непрозрачная и недокументированная инфраструктура, где годами наслаивались решения разных производителей
- Продолжительность жизненного цикла систем (прежде всего АСУ ТП) превышает продолжительность цикла обновления нормативных требований
- Проприетарность ПО АСУ ТП и монополизм производителей ведут к незаинтересованности в изменениях
- Отсутствие единой мотивации и несовпадение «целей» для подразделений эксплуатирующих АСУ ТП и подразделений ИБ
- Большой временной лаг между завершением проектных работ и началом внедрения
- «Осложнения», связанные со слияниями, поглощениями и формированием сложных структур владения

## Обеспечение безопасности ЗОКИИ

- ✓ Прозрачность инфраструктуры
- ✓ Ревизия присвоенных категорий
- ✓ Анализ критических процессов
- ✓ Авторитетные рекомендации

# КАНОНИЧЕСКИЙ ПОДХОД К СОЗДАНИЮ СИСТЕМЫ

Этап  
**1**

Предпроектное обследование

Этап  
**2**

Разработка проектной документации

Этап  
**3**

Разработка организационно-распорядительной документации

Этап  
**4**

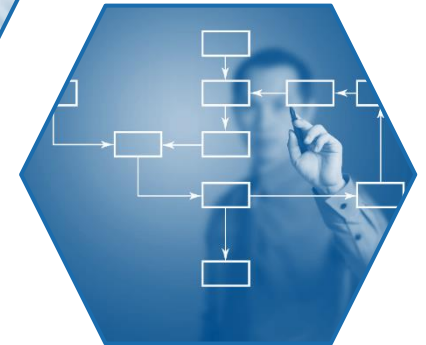
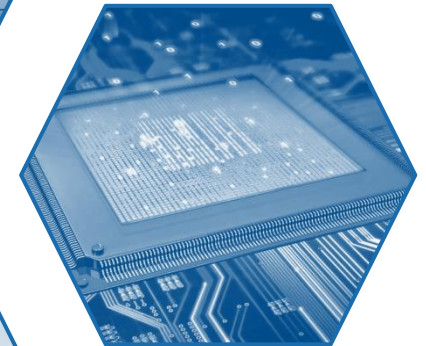
Поставка, установка и настройка СрЗИ

Этап  
**5**

Внедрение мер по защите информации, в т.ч. организационных

Этап  
**6**

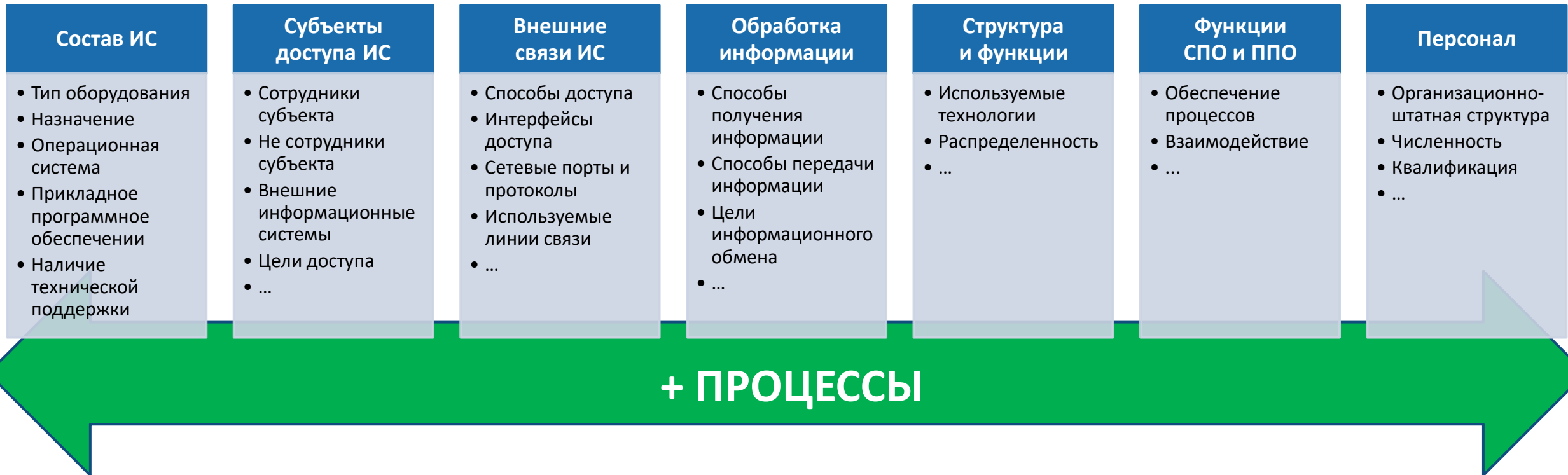
Проведение испытаний / Оценка соответствия / Оценка эффективности



# КОМПЛЕКСНОЕ ОБСЛЕДОВАНИЕ



# ИСХОДНЫЕ ДАННЫЕ ДЛЯ ПРОЕКТИРОВАНИЯ



**Более 150 метрик !**

# ТИПОВЫЕ ОШИБКИ

- Неверное определение границ ЗОКИИ
- Отсутствие контроля сетевого трафика
- Отсутствие сегментации сети
- Использование открытых протоколов передачи
- «Плоские» права доступа в ЗОКИИ
- Отсутствие управления идентификаторами/аутентификаторами
- Отсутствие контроля интерфейсов ввода-вывода
- Осуществляются не все процессы обеспечения информационной безопасности
- Неполные процессы обеспечения информационной безопасности

## На разных этапах жизненного цикла

- ✓ Категорирование
- ✓ Проектирование
- ✓ Внедрение
- ✓ Эксплуатация

# НЕВЕРНОЕ ОПРЕДЕЛЕНИЕ ГРАНИЦ ЗОКИИ

Состав ИС

Субъекты  
доступа ИС

Внешние  
связи ИС

Обработка  
информации

Функции  
СПО и ППО

Персонал

## «Распиливание» ППО на модули

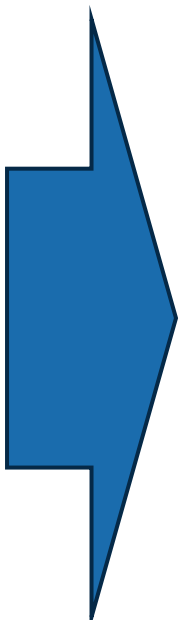
- Отсутствие необходимых механизмов защиты
- Необходимость контроля соединений между модулями
- Множество взаимодействующих/обеспечивающих ИС

## Широкие границы объекта

- Большие затраты на создание системы защиты
- Отсутствие средств защиты для некоторых компонент
- «Зоопарк» технических средств

## Узкие границы объекта

- Появление множества взаимодействующих ИС
- «Разрыв» технологического (критического) процесса

- 
- ✓ Программные и аппаратные компоненты, осуществляющие критический процесс
  - ✓ Средства защиты информации
  - ✓ Инфраструктурные компоненты



# «ПЛОСКИЕ» ПРАВА ДОСТУПА В ЗОКИИ

Состав ИС

Субъекты  
доступа ИС

Внешние  
связи ИС

Обработка  
информации

Функции  
СПО и ППО

Персонал

- Отсутствие разграничение прав между администраторами
- Пользователи с одинаковыми правами
- Пользователи с правами администраторов



- ✓ Разграничение прав доступа встроенными механизмами
- ✓ «Терминирование» доступа
- ✓ Использование РАМ-систем

# ОТСУТСТВИЕ УПРАВЛЕНИЯ ИДЕНТИФИКАТОРАМИ/АУТЕНТИФИКАТОРАМИ

Состав ИС

Субъекты  
доступа ИС

Внешние  
связи ИС

Обработка  
информации

Функции  
СПО и ППО

Персонал

Топ 20 паролей

Gmail

123456  
password  
123456789  
qwerty  
12345678  
111111  
abc123  
123123  
1234567  
1234567890  
iloveyou  
password1  
000000  
zaq12wsx  
tinkle  
qwerty123  
monkey  
target123  
dragon  
1q2w3e4r

Yandex

123456  
123456789  
111111  
qwerty  
1234567890  
1234567  
7777777  
123321  
000000  
123123  
666666  
12345678  
555555  
654321  
ghijkl  
777777  
112233  
121212  
987654321  
159753

Mail.ru

qwerty  
123456  
qwertyuiop  
qwe123  
qweqwe  
klaster  
1qaz2wsx  
1q2w3e4r  
qazwsx  
1q2w3e  
123qwe  
1q2w3e4r5t  
123456789  
111111  
zxcvbnm  
1234qwer  
qwer1234  
asdfgh  
marina  
q1w2e3r4t5



- ✓ Управление формированием идентификатора
- ✓ Управление сложностью аутентификатора
- ✓ Управление сменой аутентификатора
- ✓ Блокирование учетных записей (в том числе по неактивности)

# КОНТРОЛЬ СЕТЕВЫХ СОЕДИНЕНИЙ

Состав ИС

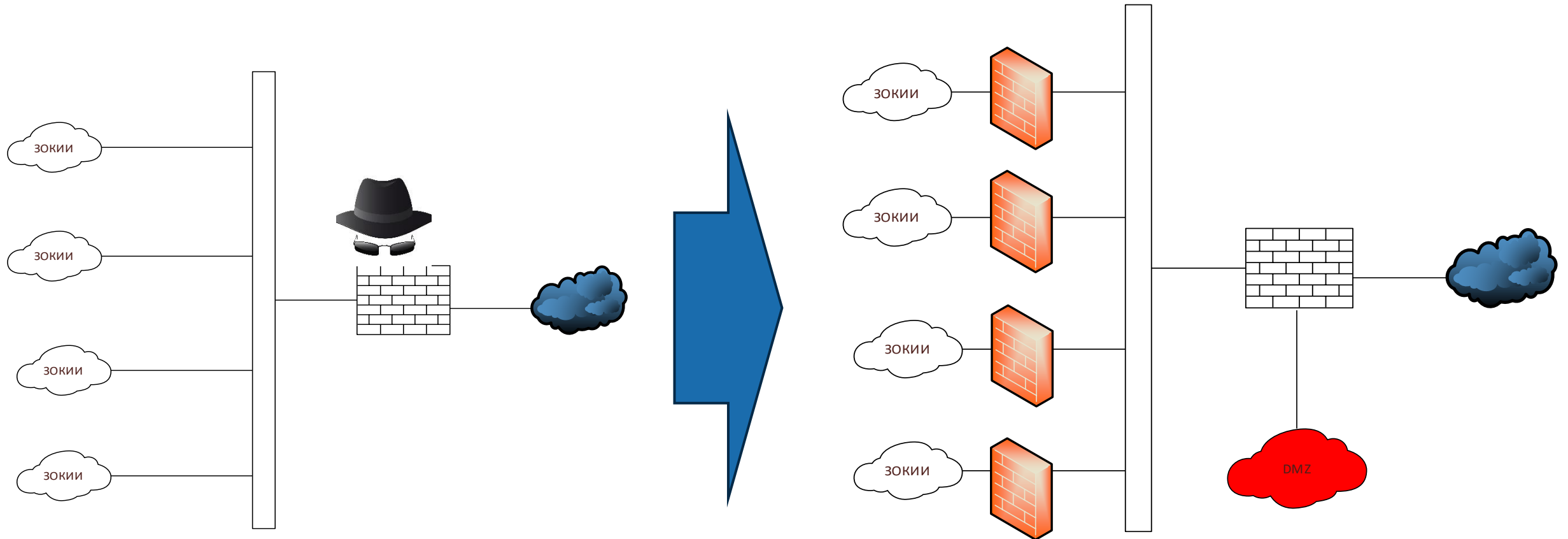
Субъекты  
доступа ИС

Внешние  
связи ИС

Обработка  
информации

Функции  
СПО и ППО

Персонал



# ОТСУТСТВИЕ СЕГМЕНТАЦИИ СЕТИ

Состав ИС

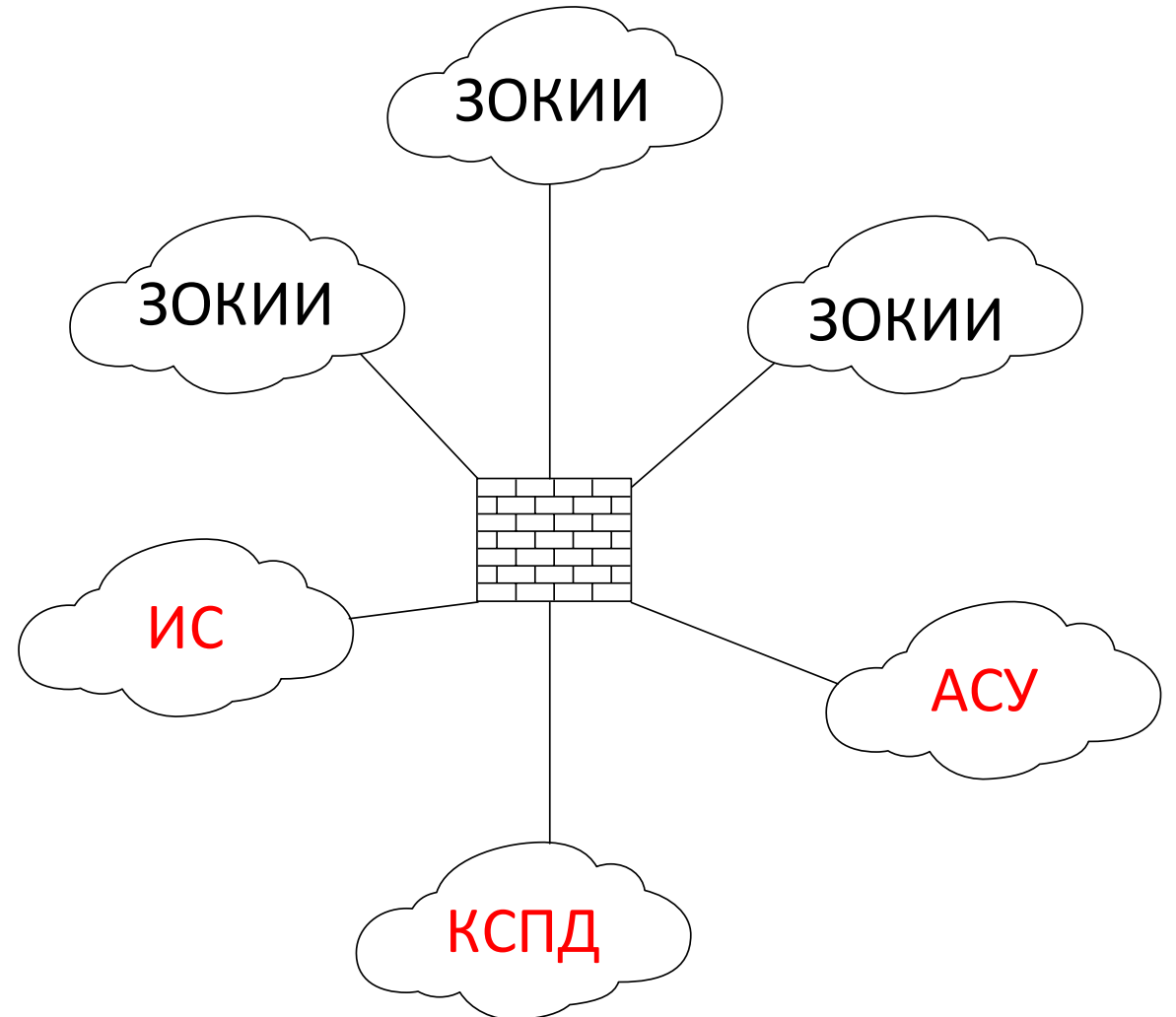
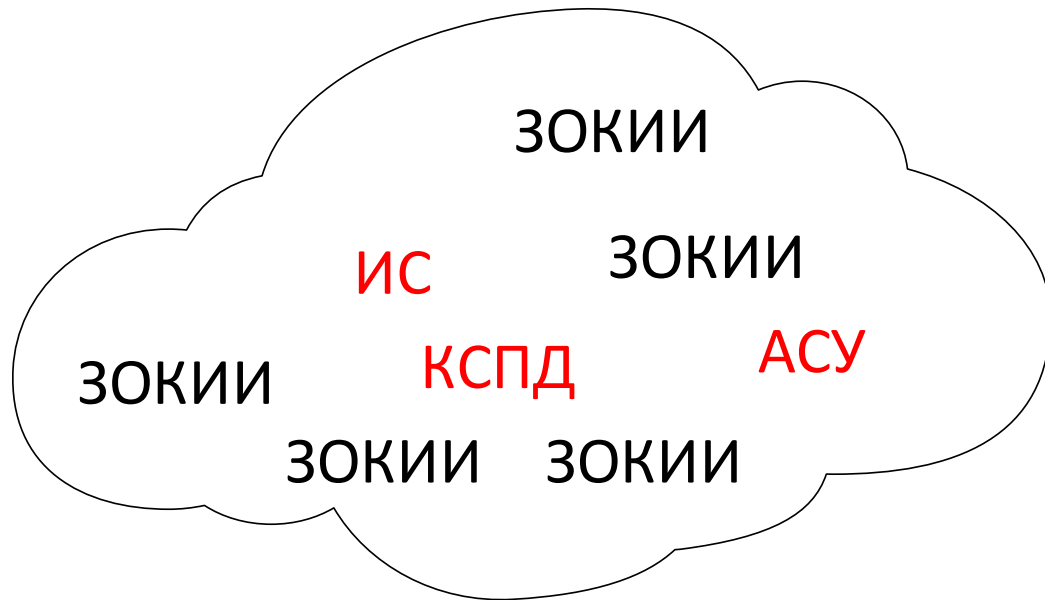
Субъекты  
доступа ИС

Внешние  
связи ИС

Обработка  
информации

Функции  
СПО и ППО

Персонал



# ОТСУТСТВИЕ КОНТРОЛЯ ИНТЕРФЕЙСОВ ВВОДА-ВЫВОДА

Состав ИС

Субъекты  
доступа ИС

Внешние  
связи ИС

Обработка  
информации

Функции  
СПО и ППО

Персонал

Осуществляется контроль  
не всех интерфейсов ввода вывода



Контроль входящей информации на предмет:

- ✓ наличия вредоносного кода
- ✓ полноты
- ✓ корректности
- ✓ источника поступления

# ИСПОЛЬЗОВАНИЕ ОТКРЫТЫХ ПРОТОКОЛОВ ПЕРЕДАЧИ

Состав ИС

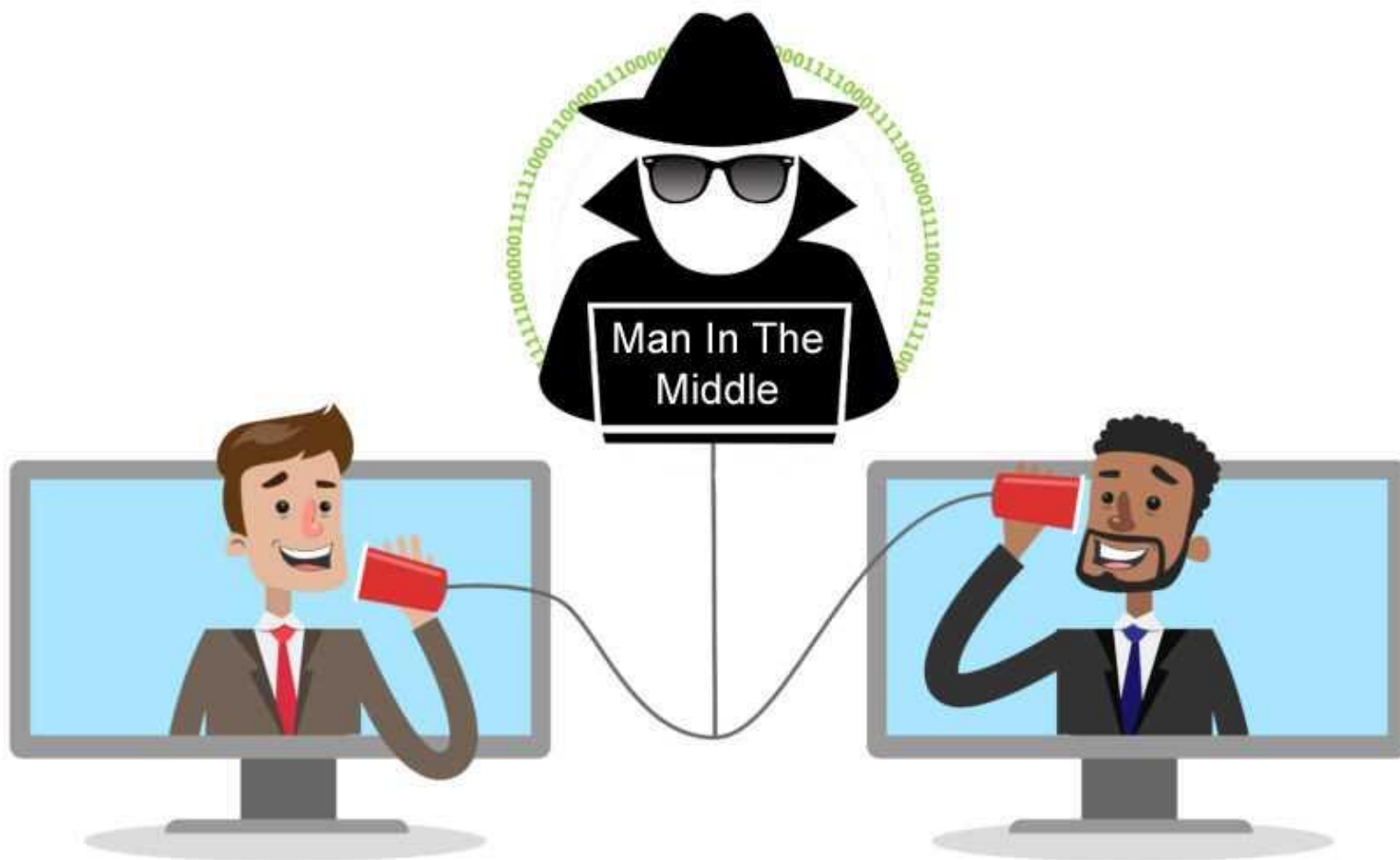
Субъекты  
доступа ИС

Внешние  
связи ИС

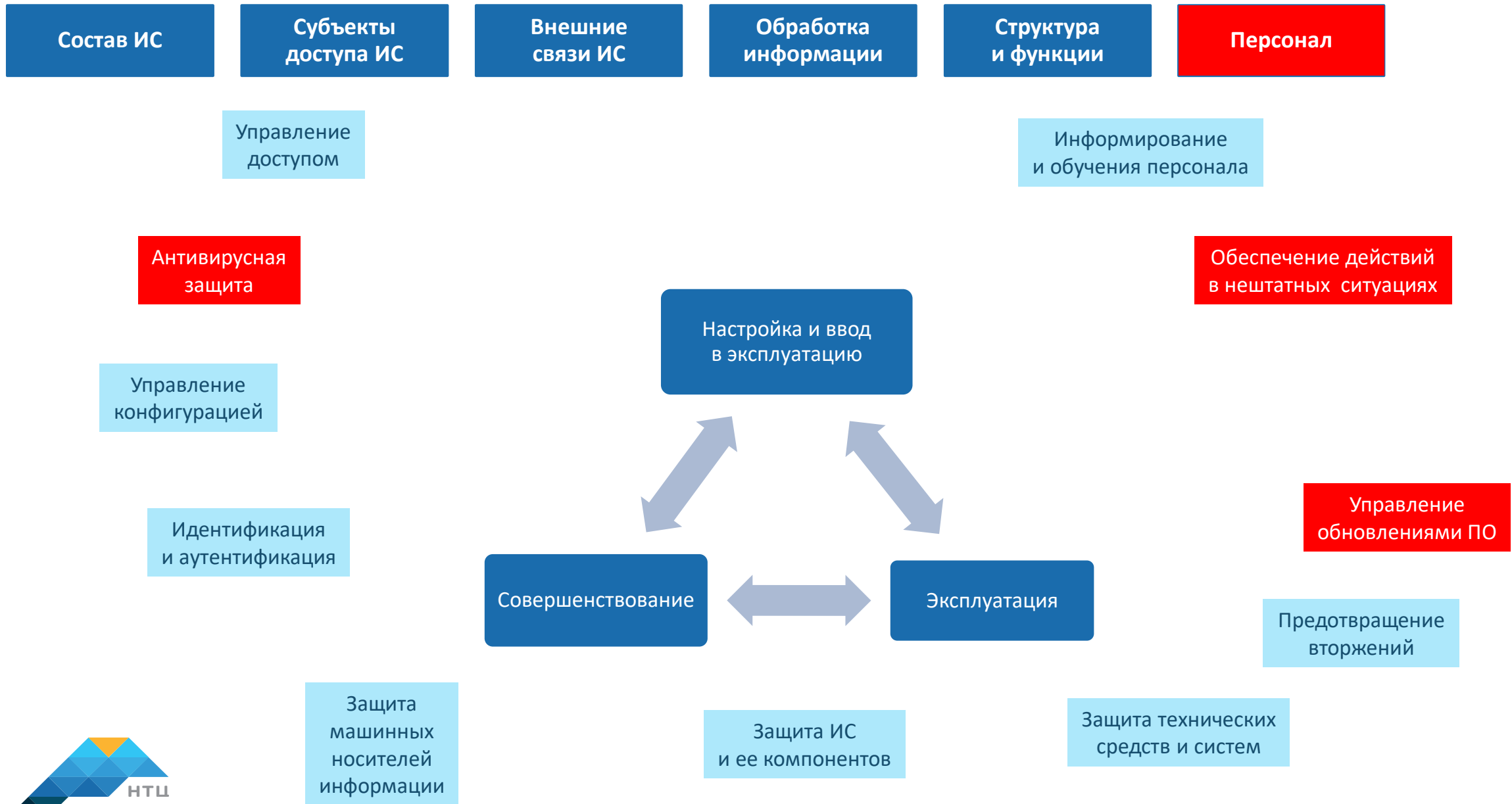
Обработка  
информации

Функции  
СПО и ППО

Персонал



# НЕПОЛНЫЕ ПРОЦЕССЫ ОБЕСПЕЧЕНИЯ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ



# ПРОЕКТИРОВАНИЕ

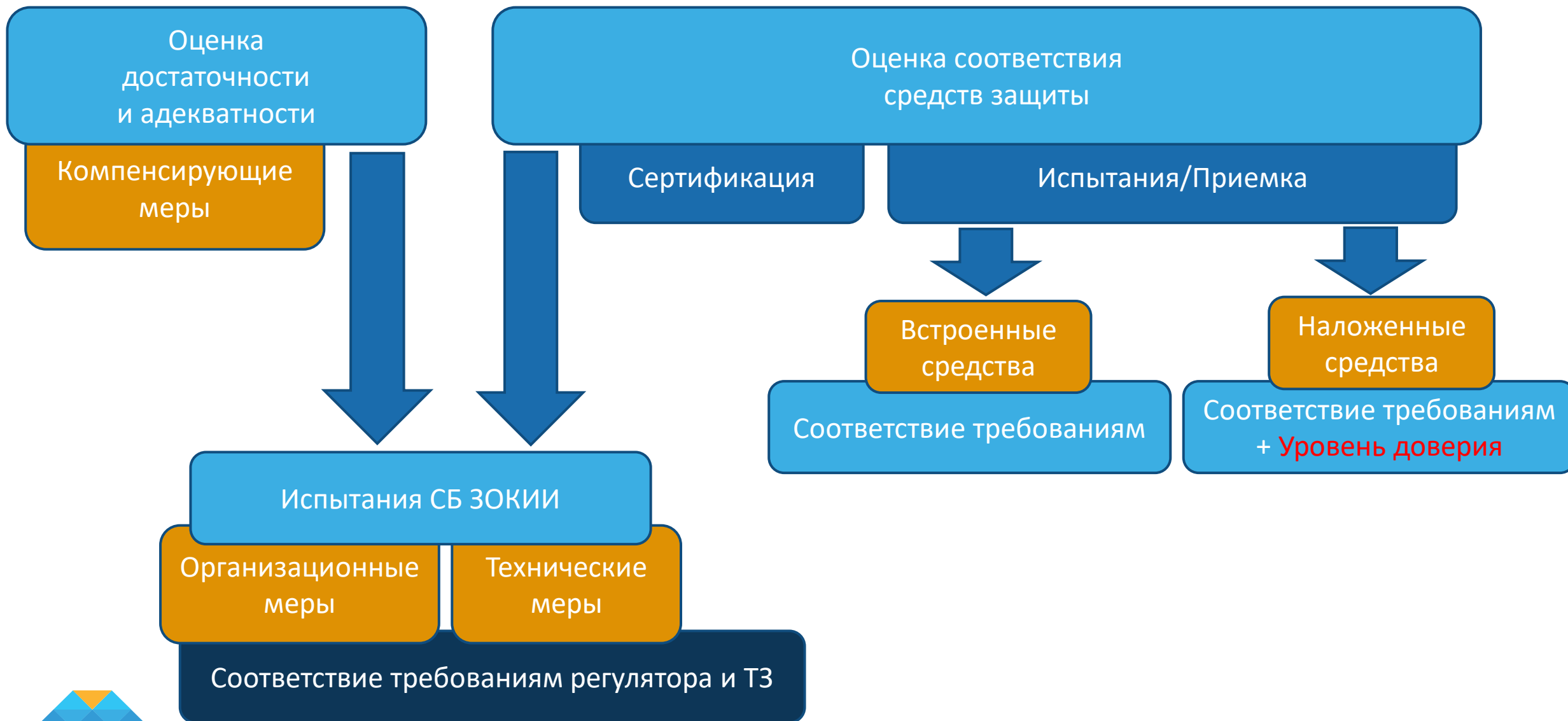




# ПОЛНЫЕ ПРОЦЕССЫ ОБЕСПЕЧЕНИЯ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ



# ВВОД В ЭКСПЛУАТАЦИЮ



# РЕЗУЛЬТАТ - КОМПЛЕКСНАЯ СИСТЕМА ЗАЩИТЫ ЗОКИИ



**СПАСИБО ЗА ВНИМАНИЕ!**



Научно-технический центр «Вулкан»  
г. Москва, ул. Ибрагимова, д. 31  
+7 495 777-13-10  
marketing@ntc-vulkan.ru

[www.ntc-vulkan.ru](http://www.ntc-vulkan.ru)