AKTIV.
CONSULTING

Практика идентификации и управления изменениями элементов критичной архитектуры **для финансовых организаций**

Александр Моисеев

Ведущий консультант по информационной безопасности AKTIV.CONSULTING

Система НПА и НМД
для обеспечения ОН

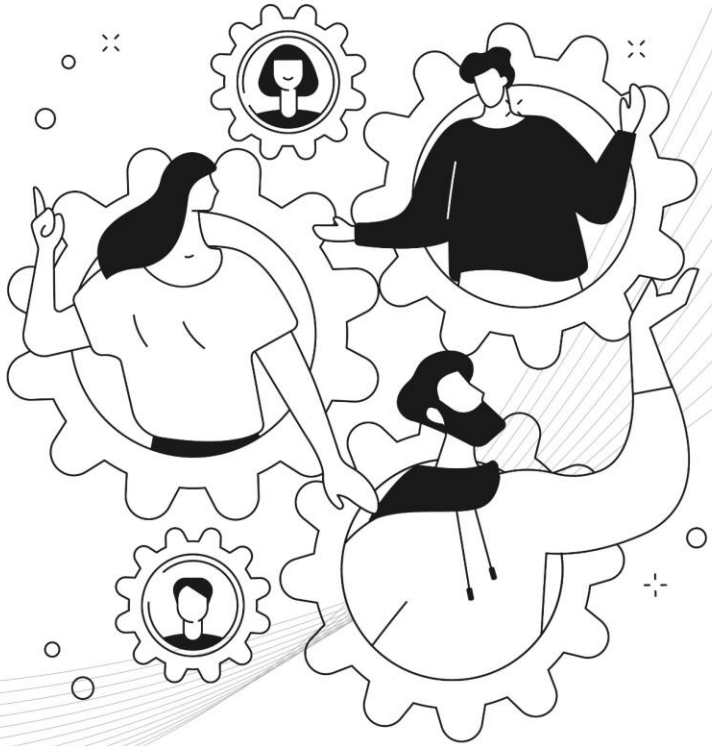
О чем сегодня пойдет речь

Процесс №1

Идентификация

Процесс №2

Управление изменениями

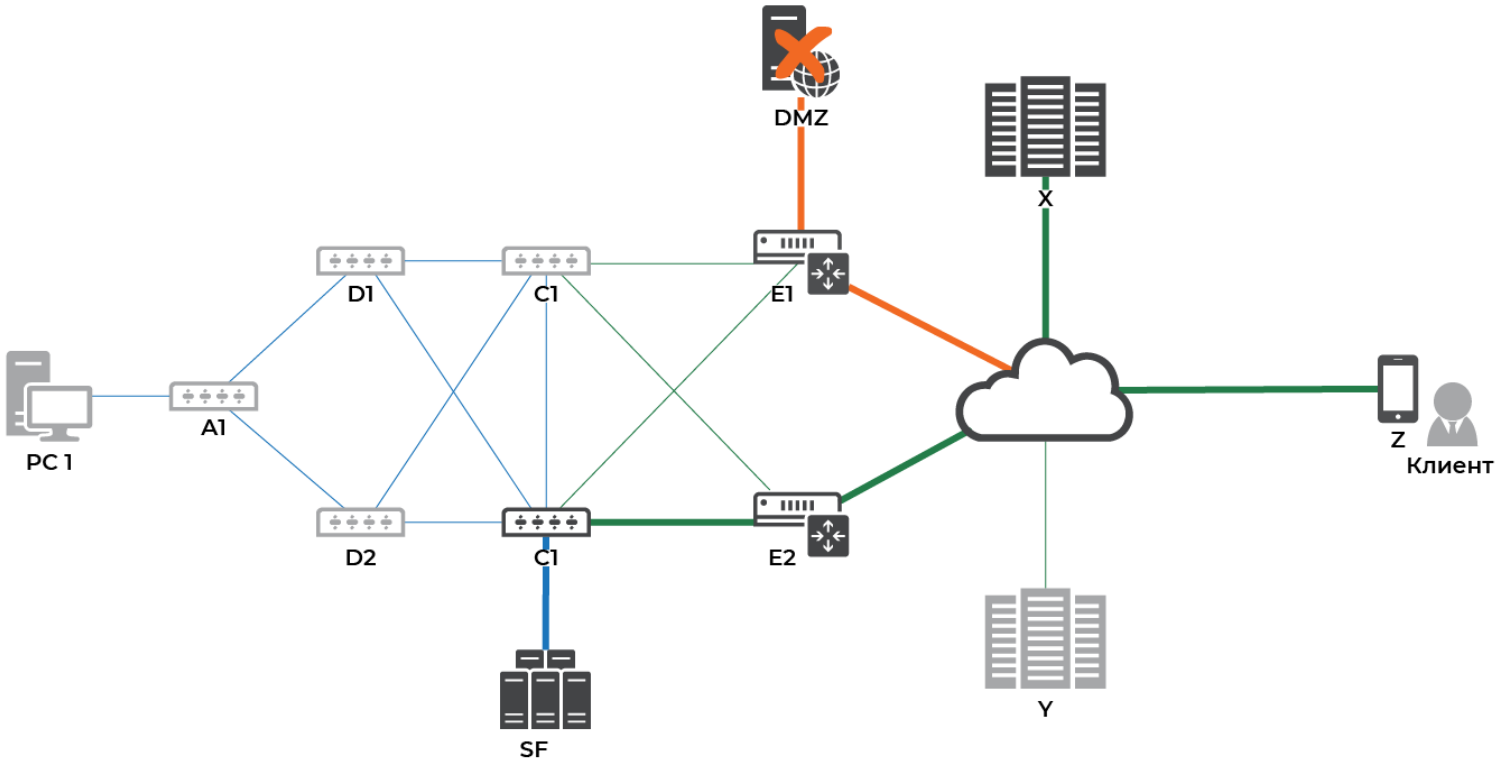


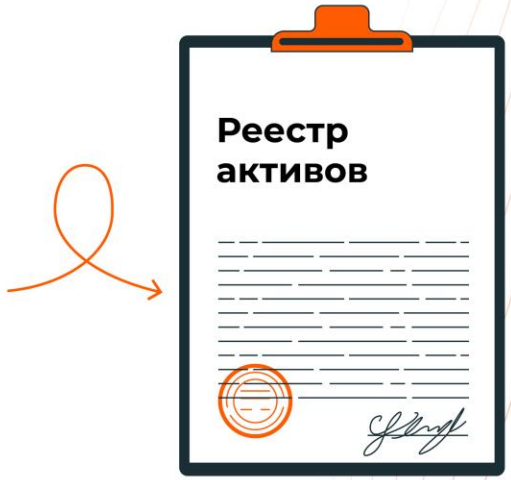
Процесс №1
«Идентификация»

01

- Выявление элементов КА
- Классификация
- Учет элементов КА

Выявление элементов КА 1/3





Модель данных

Технологический процесс №1
проведение организованных торгов

Технологический участок ТП №1
идентификация клиента

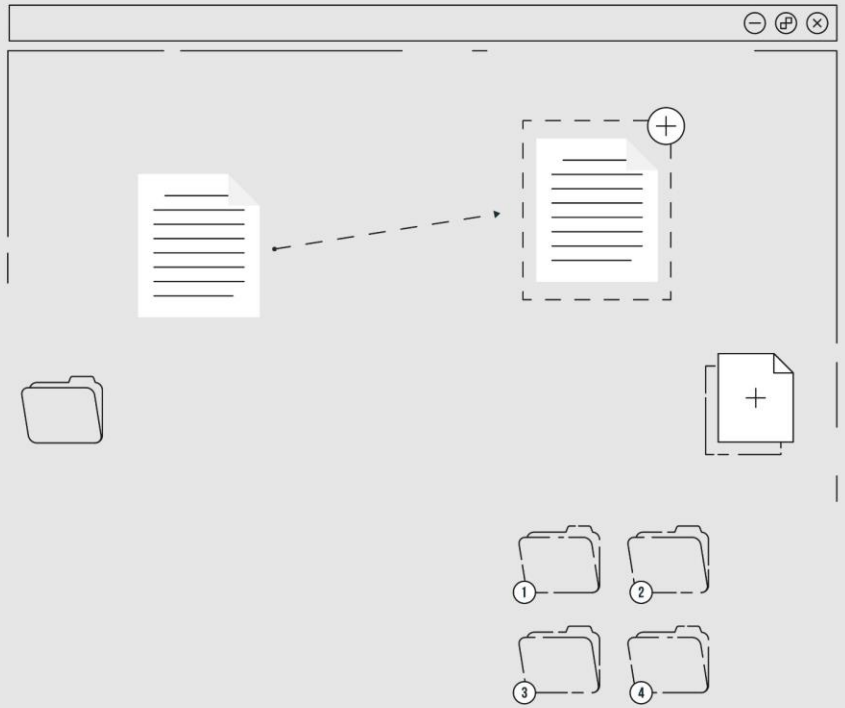
ОИИ №1
торговая система

ОИИ №2
пул серверных ресурсов

Набор данных №1
классификационная метка

Документ №1
стандарт конфигурирования

Технологический участок ТП №2
хранение информации

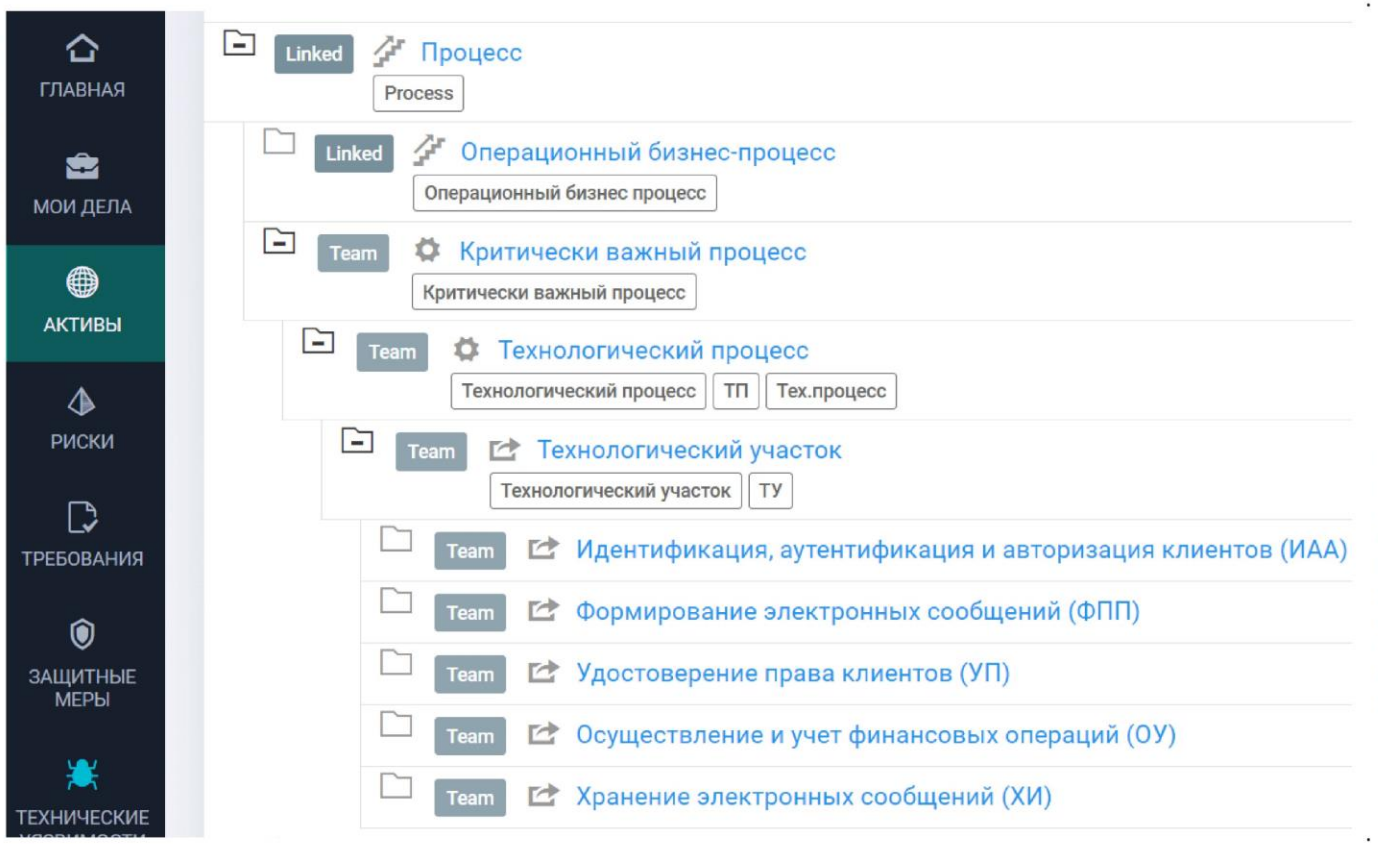


Классификация 2 / 3

Пример классификации из СТО БР 1.5

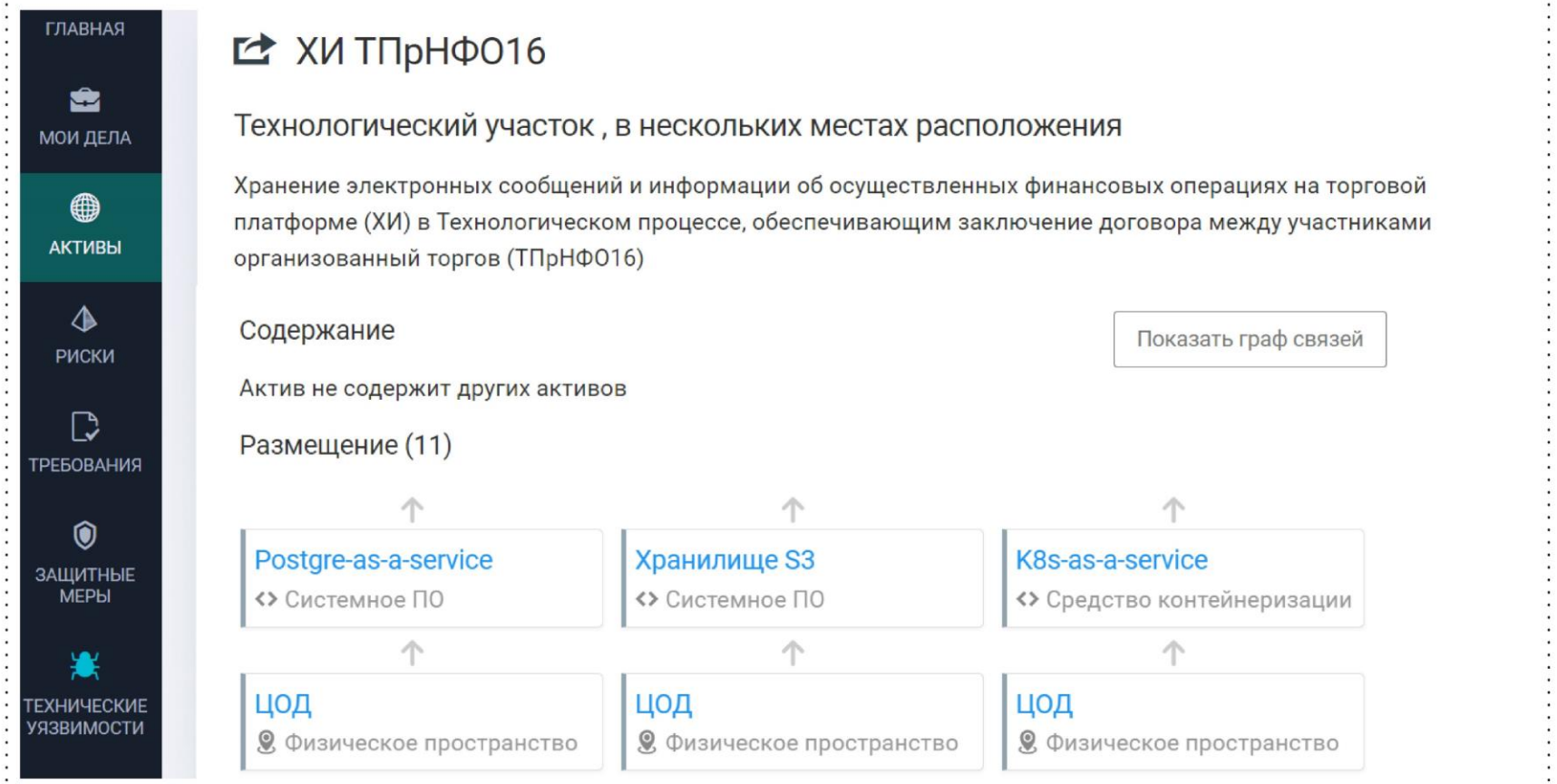
Код ТУ	Наименование ТУ
[ИАА]	Идентификация, аутентификация и авторизация клиентов
[ФПП]	Формирование, передача и прием электронных сообщений
[УП]	Удостоверение права клиентов распоряжаться
[ОУ]	Осуществление финансовой операции
[ХИ]	Хранение информации

Пример реализации в ИС класса «SGRC»



Учет элементов КА 3 / 3

Пример реализации учета активов



Процесс №2 «Управление изменениями»

02

- Управление изменениями
- Управление конфигурацией ОИИ
- Управление уязвимостями
- Управление обновлениями

Управление изменениями 1 / 4

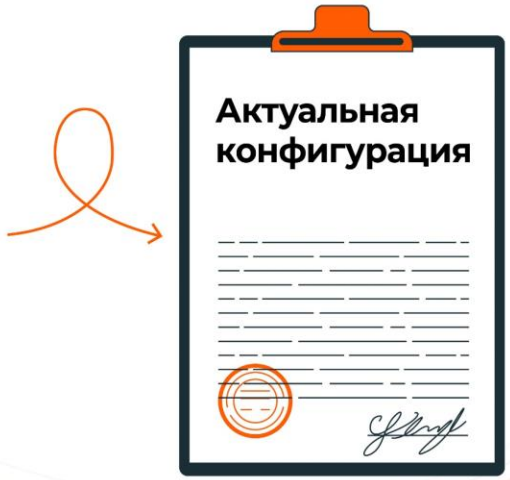
Управление конфигурацией 2 / 4

ПЛАНИРОВАНИЕ КОНФИГУРАЦИИ

ИДЕНТИФИКАЦИЯ КОНФИГУРАЦИИ

АУДИТ КОНФИГУРАЦИИ

МОНИТОРИНГ



Управление уязвимостями 3 / 4

Пример схемы процесса управления уязвимостями

Полезные ссылки:

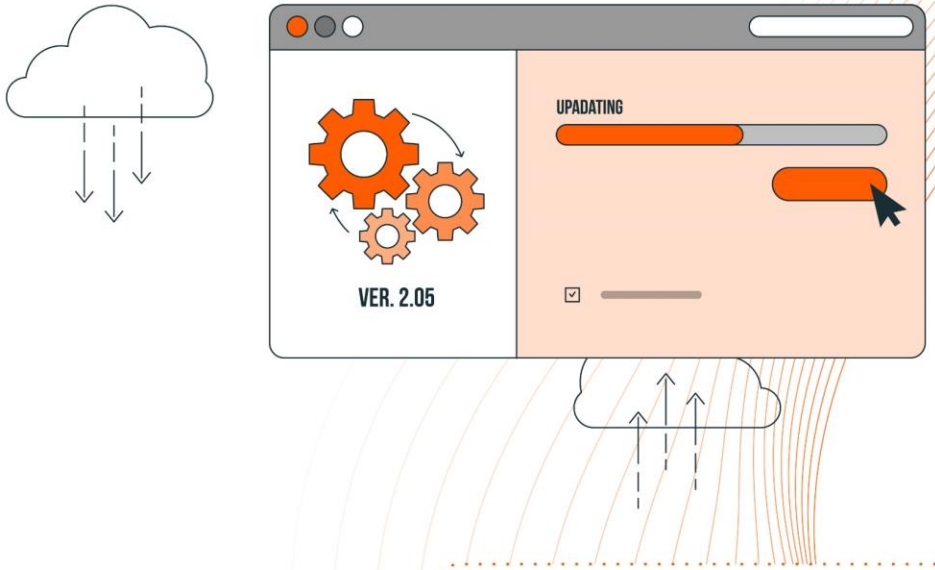
https://bdu.fstec.ru/vul
https://bdu.fstec.ru/calc31
https://bdu.fstec.ru/scanoval

*Руководство по организации процесса управления уязвимостями (ФСТЭК России, 2023)

Управление обновлениями 4 / 4

Тестирование обновлений

- поиск актуальных обновлений
- проверка корректности их работы



Тестирование безопасности обновлений

- сверка идентичности (T001*)
- проверка подлинности (T002)
- антивирусный контроль (T003)
- поиск опасных конструкций (T004)
- мониторинг активности в среде функционирования (T005)
- ручной анализ (T006)

*Методика тестирования обновлений безопасности ПО, ПАК (ФСТЭК России, 2022)

Полезные ссылки:

https://bdu.fstec.ru/software-section/updates

Выводы:

01

Разработка и адаптация методологии **под конкретное ФО**

02

Реализация процессов потребует **дополнительные ресурсы** для взаимодействия с ФинЦЕРТ

03

Цифровизация процессов сократит трудоемкость формирования отчетности для Банка России

04

Управление уязвимостями и обновлениями ПО с использованием **методологий ФСТЭК России**

AKTIV.
CONSULTING

Александр Моисеев

Ведущий консультант по информационной безопасности AKTIV.CONSULTING

moiseev@aktiv.consulting