AKTIV.
CONSULTING

ВНЕДРЕНИЕ ТРЕБОВАНИЙ ГОСТ Р 57580.4-2022

ПО ОБЕСПЕЧЕНИЮ ОПЕРАЦИОННОЙ НАДЕЖНОСТИ

Александр Моисеев

Ведущий консультант
по информационной безопасности
AKTIV.CONSULTING

ОРГАНИЗАЦИОННЫЙ ВОПРОС

01

Всем участникам будет выслана презентация и запись видео

02

Задавайте вопросы на вкладке «Вопросы»

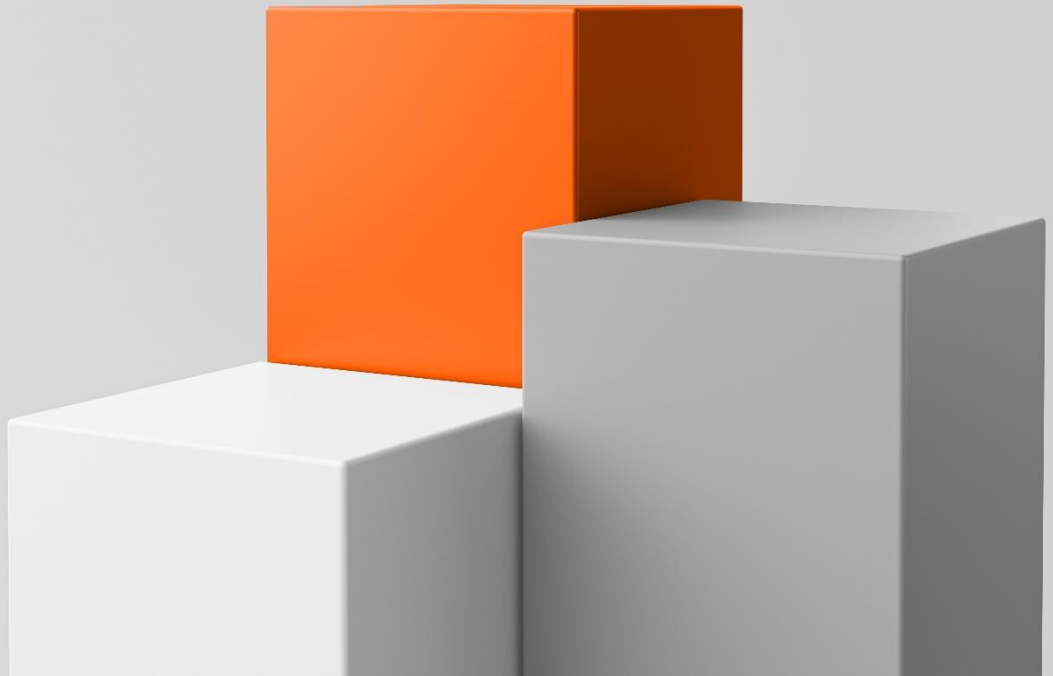
03

Автор самого лучшего вопроса получит подарок от **AKTIV.**CONSULTING

ЧТО СЕГОДНЯ РАССМОТРИМ

1. Структуру ГОСТ ОН
и основные сложности первых трех
процессов

2. Рекомендации
по преодолению
сложностей



СТРУКТУРА ГОСТ И ОСНОВНЫЕ СЛОЖНОСТИ

СТРУКТУРА СТАНДАРТА И СВЯЗЬ С ОСТАЛЬНЫМИ СТАНДАРТАМИ

57580.4 («ГОСТ ОН»)	57580.1 («ГОСТ ЗИ»)	57580.3 («ГОСТ УР ИУ»)
Процесс 1 «Идентификация критичной архитектуры»	ИУ.1-6, РД.1-7	ВСР.2, ВИО.10-11,13, РМ.9
Процесс 2 «Управление изменениями»	УЗП.11-12,27, РД.16,43, ФД.19-20, ИУ.7-8, СМЭ.21, ЗБС.10, ЗВК.20, МАС.23, ЗСВ.33,35,37-38,42-43, РЗИ.5, КЗИ.11, ЖЦ.4,10,22-23,25	ОПР.13.1, ОСЗ.1.5
Процесс 3 «Выявление, реагирование и восстановление после инцидентов»	МАС.1-7	ВИО.7,16,22, РМ,13, ВСР.1-6, ОПР.7, РМ.1-5, 8.3.1.3, УПК.13
Процесс 4 «Взаимодействие с поставщиками услуг»	А.5-8	ОПР.15, ВИО.11.3, ЗИУ.12-17, ОСЗ.1.6,2
Процесс 5 «Тестирование ОН БП и ТП»	ЦЗИ.14, РЗИ.3, КЗИ.4, ЖЦ.5,9,13	ВИО.14, УПК.9.4, ОСЗ.3.2
Процесс 6 «Защита при удаленной работе»	ЗУД.1-12	—
Процесс 7 «УР внутреннего нарушителя»	ПУИ.1-33	8.3.1.2
Процесс 8 «Обеспечение осведомленности»	РЗИ.16	ОПР.5.2, 8.3.3

Подробнее про процессы ГОСТ ОН: в статье https://aktiv.consulting/ekspertiza/623 подготовленной для журнала BIS Journal

ОСНОВНЫЕ СЛОЖНОСТИ ПРОЦЕССОВ 1–3 «ГОСТ ОН»

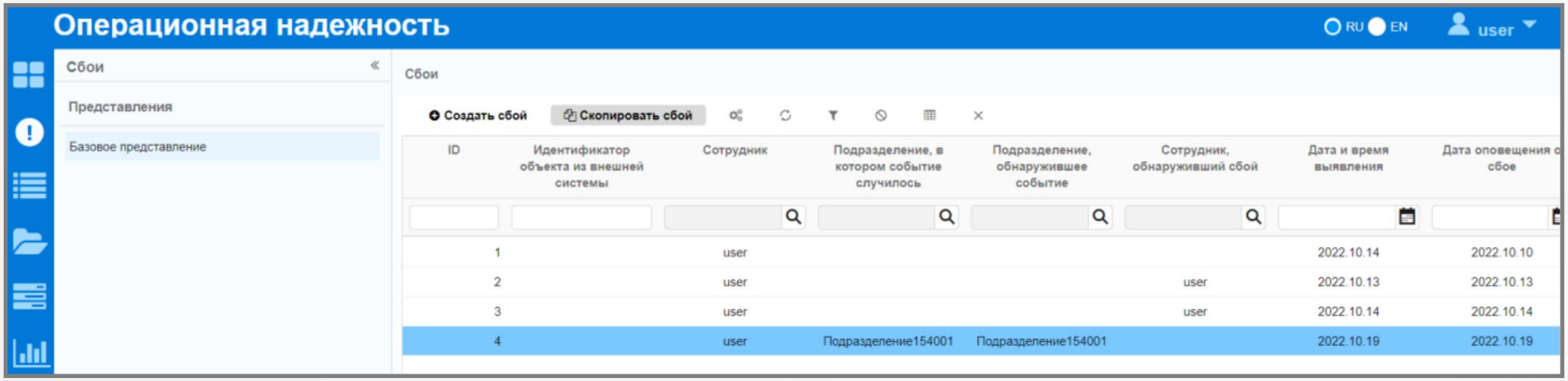
ПРОЦЕСС	СЛОЖНОСТИ
1 «Идентификация элементов критичной архитектуры»	Низкое качество данных. Трудно управлять связью элементов друг с другом, классификационными признаками, статусами
2 «Управление изменениями»	Долгий цикл согласования изменений. Поддержание в актуальном состоянии данных об элементах
3 «Выявление, реагирование и восстановление после инцидентов»	Трудности в определении целевых и вспомогательных показателей ОН

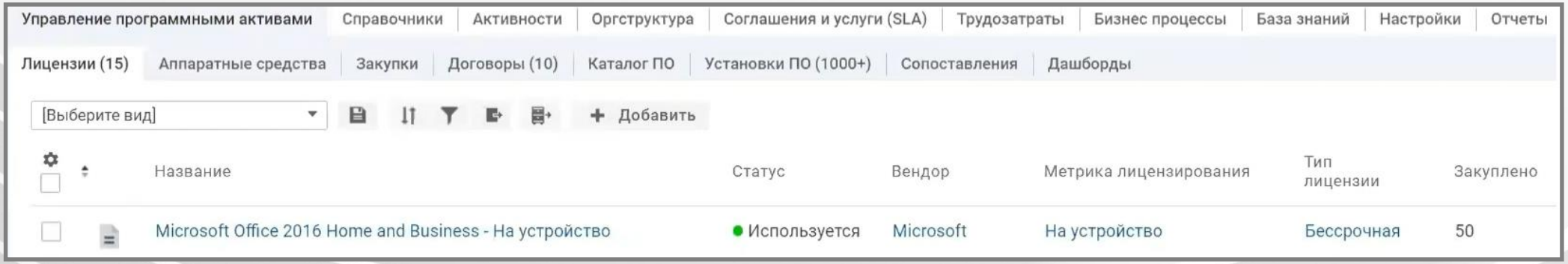
РЕКОМЕНДАЦИИ

РЕКОМЕНДАЦИИ ПО МЕТОДОЛОГИЯМ ПРОЦЕССОВ

ПРОЦЕСС	РЕКОМЕНДАЦИИ
1 «Идентификация элементов критичной архитектуры»	Специализированные платформы, сочетание решений класса: ITAM, SAM, DCIM, CMDB, IPAM, SGRC, IRP
2 «Управление изменениями»	Методологии и стандарты CMII, ITIL, COBIT, ГОСТ Р 59193
3 «Выявление, реагирование и восстановление после инцидентов»	**NIST SP 800-160:** Раздел С.4: «… анализ воздействия на бизнес (BIA), анализ дерева отказов (FTA), анализ видов, последствий и критичности отказов (FMECA)..» **Системы стандартов «Надежность в технике»:** анализ древа событий (ETA), анализ надежности человеческого фактора (HRA), software reliability engineering (SRE) **Лучшие практики из ИТ-отрасли:** DevOps, SRE, DBRE, PE

СЛОЖНОСТЬ №1:
РЕКОМЕНДАЦИИ ПО ИДЕНТИФИКАЦИИ И УЧЕТУ АКТИВОВ



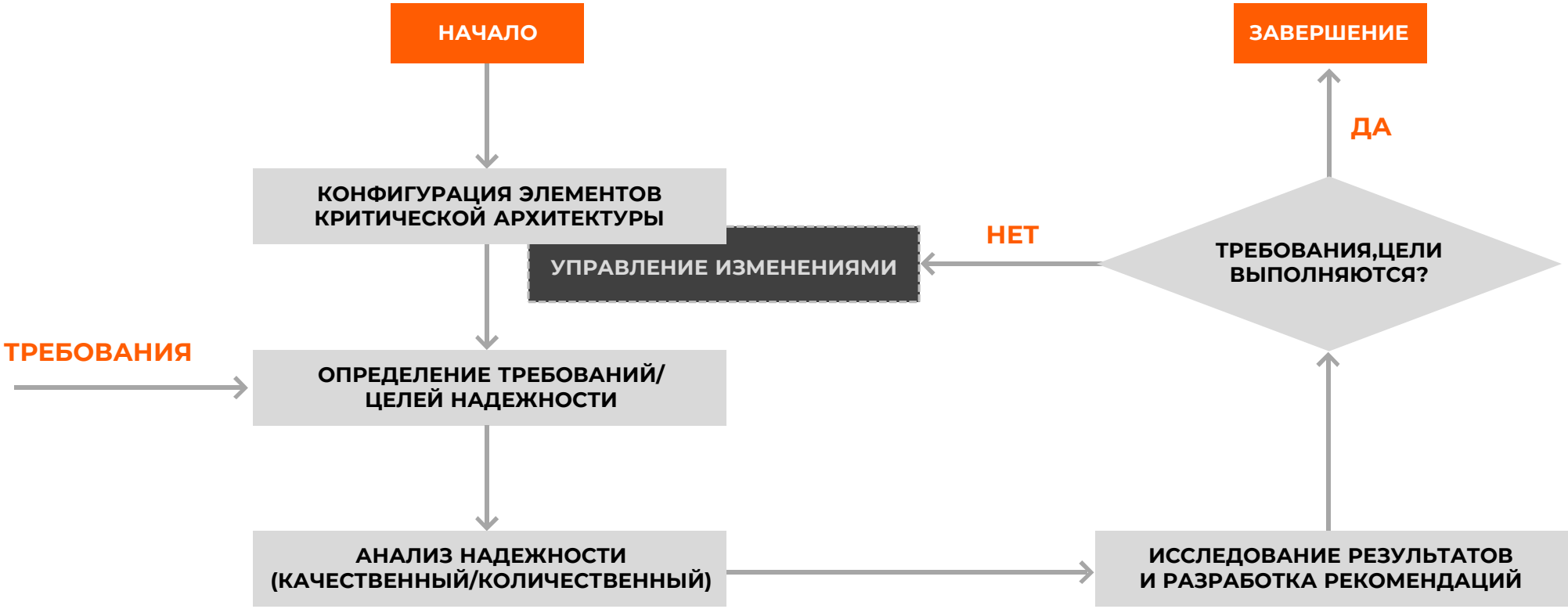


- Пример информационных систем

СЛОЖНОСТЬ №2:
РЕКОМЕНДАЦИИ ПО ОРГАНИЗАЦИИ ПРОЦЕССА УПРАВЛЕНИЯ ИЗМЕНЕНИЯМИ

Пример схемы процесса управления изменениями

СЛОЖНОСТЬ №3:
ОБЩИЕ РЕКОМЕНДАЦИИ ПО ПРОВЕДЕНИЮ АНАЛИЗА НАДЕЖНОСТИ



СЛОЖНОСТЬ №3:
МЕТОД АНАЛИЗА ВЛИЯНИЯ НА БИЗНЕС (BIA)

БИЗНЕС ПОДРАЗДЕЛЕНИЯ

БИЗНЕС ПРОЦЕСС	ПОТЕНЦИАЛЬНОЕ ВОЗДЕЙСТВИЕ	МДВП	КОМПОНЕНТ ИС	ЦВВ	ЦТВД
Обработка заявок	Блокировка БП 300 сотрудников	4	Сервер приложений **A**	1,5	0,5
Подготовка отчётов	Репутационные потери	72	Веб-сервер **B**	6	12
Корректировка бюджета	Блокировка БП	48	Сервер БД **C**	14	24

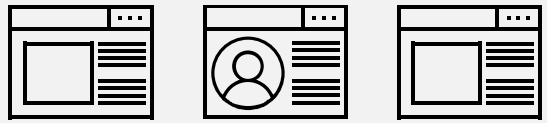
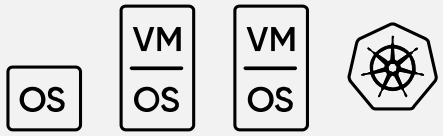
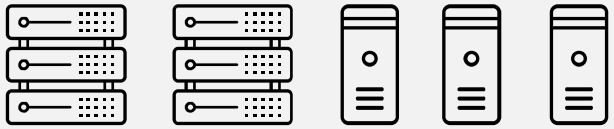
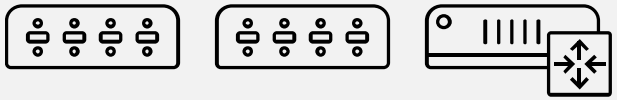
ЗАВИСИМОСТЬ

СЛОЖНОСТЬ №3:
МЕТОД «ГАЛСТУК-БАБОЧКА» (КОМБИНАЦИЯ FTA И ETA)

ПРИЧИНЫ	МЕРЫ УМЕНЬШАЮЩИЕ СВР	ОПАСНОЕ СОБЫТИЕ	МЕРЫ СНИЖАЮЩИЕ СТП	ПОСЛЕДСТВИЯ
1 ЗАМЫКАНИЕ ПОРТА	1 АГРЕГАЦИЯ КАНАЛОВ	**ОТКАЗ КОММУТАТОРА №1**	1 АЛЬТЕРНАТИВНЫЕ МАРШРУТЫ	1 ПОТЕРЯ ДОСТУПНОСТИ ИС №2
2 ОШИБКА СЕТЕВОГО ИНЖЕНЕРА В КОНФИГУРАЦИИ	2 УИ.19 ПРОВЕРКА КОНФИГУРАЦИИ	FTA	2 УИ.10 ОТКАТ ИЗМЕНЕНИЙ	2 ПРОСТОЙ СОТРУДНИКОВ В РАБОТЕ
N ПОДБОР АТАКУЮЩИМ ПАРОЛЯ	N РД.24 ПАРОЛЬНАЯ ПОЛИТИКА		N ВРВ.16.2 УПРАВЛЯЕМАЯ ДЕГРАДАЦИЯ	N БЛОКИРОВАНИЕ SPAN-ПОРТА НА СЕТЕВОЙ СЕНСОР

ETA

ПРИМЕНЕНИЕ ПРИ АНАЛИЗ ИНФРАСТРУКТУРЫ ФО

УРОВНИ		ПОВЫШЕНИЕ НАДЕЖНОСТИ	МОНИТОРИНГ	РЕАГИРОВАНИЕ
5 ПРИКЛАДНОЕ ПО (БИЗНЕС-ПРИЛОЖЕНИЯ)		**ТЕСТИРОВАНИЕ, СКАНИРОВАНИЕ**	**NEW RELIC**	**ЦК, ИТ, ИБ**
4 ОБЩЕСИСТЕМНОЕ ПО, ВИРТУАЛИЗАЦИЯ		**НА, DR РАБОЧИХ НАГРУЗОК**	**ELK, ZIPKIN, TANZU**	**ИТ, ИБ**
3 СЕРВЕРНОЕ ОБОРУДОВАНИЕ		**СЕРВИСНЫЕ КОНТРАКТЫ, ЗИП**	**ZABBIX, GRAFANA, PROMETHEUS**	**ИТ**
2 СЕТЕВОЕ ОБОРУДОВАНИЕ		**ENTERCHANEL, VRRP, БАЛАНСИРОВКА**	**SYSLOG, SNMP, NETFLOW**	**ИТ, ИБ**
1 ХРАНЕНИЕ ДАННЫХ		**RAID, БЭКАПИРОВАНИЕ, РЕЗЕРВНАЯ СХД**	**iSCSI MANAGER, VEEAM, VELERO**	**ИТ**
0 ОБЕСПЕЧИВАЮЩАЯ ИНФРАСТРУКТУРА		**ИБП, АВР, ДГУ, МОБИЛЬНЫЙ КОНДИЦИОНЕР**	**IOT-УСТРОЙСТВА, ОПС, CCTV**	**СЕРВИСНЫЕ СЛУЖБЫ**

В КАЧЕСТВЕ РЕЗЮМЕ

- Начинать планирование внедрения процессов ОН необходимо как можно раньше
- Меры мониторинга, реагирования и тестирования должны быть унифицированы с 57580.1 и .3
- Для первых трех мер из 57580.4 можно использовать методы и решения из смежных отраслей.
- Рекомендуем внедрять цифровые процессы идентификации и управления изменениями для снижения объема ручного труда и повышения качества данных

AKTIV.
CONSULTING

БЛАГОДАРЮ
ЗА ВНИМАНИЕ!

Александр Моисеев

Ведущий консультант
по информационной безопасности

moiseev@aktiv.consulting