AKTIV.CONSULTING

2023

# Внедрение требований ГОСТ Р 57580.3-4

**Александр Моисеев,**
ведущий консультант по ИБ

# ОСНОВНАЯ ПРОБЛЕМА

Участие руководства в управлении рисками ИУ и обеспечении ОН закреплены в ГОСТ (требования по ЗИ также есть в Указе президента №250), но зачастую это игнорируется топ-менеджментом

**ПРИЧИНЫ ВОЗНИКНОВЕНИЯ ПРОБЛЕМЫ:**

1. Низкий приоритет вопросов ИБ/ИТ по сравнению с операционной деятельностью
2. Трудность коммуникации между ИБ и Бизнесом
3. Низкая осведомленность об актуальных информационных угрозах
4. Восприятие требований регулятора как «очередной compliance»

# ОСНОВНАЯ ПРОБЛЕМА

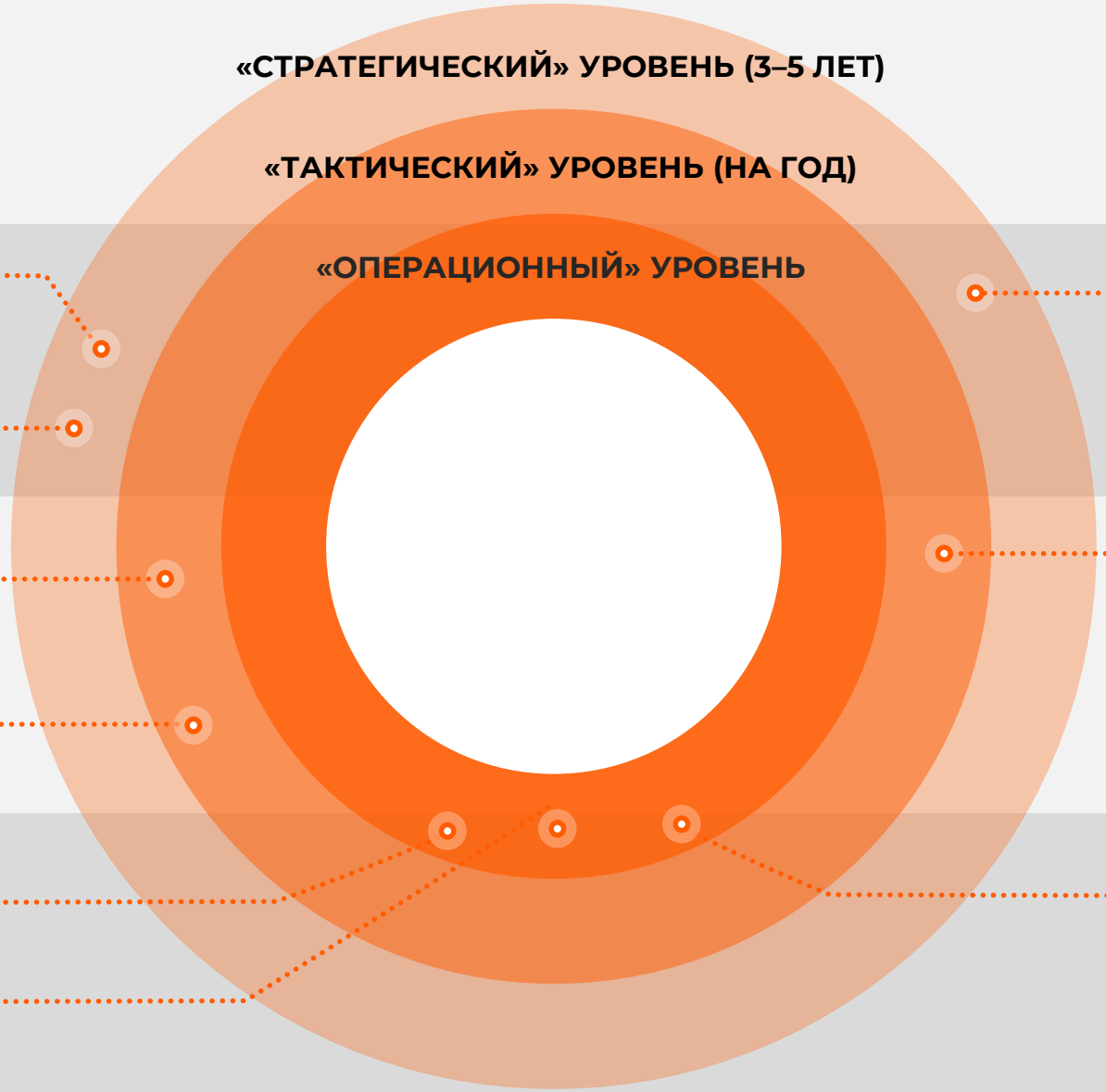
**ЧТО БУДЕТ, ЕСЛИ ПРОБЛЕМОЙ НЕ ЗАНИМАТЬСЯ:**

- возникновение реальных финансовых и репутационных потерь
- атака на всю цепочку поставок – пострадают и партнеры и клиенты

**ЧТО МОЖЕТ ПОМОЧЬ:**

1. Формирование картины целевого состояния процессов – «как должно быть»
2. Обоснование на понятном бизнесу языке (BIA, ТЭО, ROI)
3. Обучение руководства аспектам ИБ
4. Внедрение изменений через проектный подход

# УЧАСТИЕ ТОП-МЕНЕДЖМЕНТА




## ОБЯЗАТЕЛЬНЫЕ ТРЕБОВАНИЯ

- Учет рисков информационных угроз в рамках общей стратегии развития ФО
- Утверждение политики управления риском
- Рассмотрение отчетности по управлению рисками
- Утверждение контрольных показателей уровня риска
- Контроль процедур реагирования и восстановления
- Контроль результатов аудитов

## РЕКОМЕНДАЦИИ КОНСУЛЬТАНТОВ

- Включение ИБ в цикл стратегического планирования
- Повышение осведомленности
- Обеспечение ситуационного осведомленности

# «ОПЕРАЦИОННЫЙ» УРОВЕНЬ: СИТУАЦИОННАЯ ОСВЕДОМЛЕННОСТЬ

Постепенное включение вопросов ИБ в повестку операционной деятельности ответственного куратора по направлению ИБ от руководства

МЕРОПРИЯТИЯ:

1. Оперативное оповещение об инцидентах и угрозах
2. Аналитика по отраслевым инцидентам на основе реальных данных
3. Информирование о значимых инцидентах у клиентов и партнеров

# ТАКТИЧЕСКИЙ УРОВЕНЬ: ПОВЫШЕНИЕ ОСВЕДОМЛЕННОСТИ

МЕРОПРИЯТИЯ:

1. Разработка программ обучения сотрудников и руководства
2. Отработка навыков и проверка знаний инженерно-технического персонала
3. Планирование и проведение киберучений

Поддержание в высокой готовности навыков взаимодействия в кризисной ситуации

# ВЗАИМОДЕЙСТВИЕ РУКОВОДСТВА И СЛУЖБЫ ИБ ПРИ СТРАТЕГИРОВАНИИ

1. Инициация стратегирования

2. Разработка стратегии
   - оценка драфта стратегии на стоп-факторы
   - сведение реестра рисков
   - разработка нескольких конфигураций мер
   - разработка подраздела по ИБ

3. Согласование и утверждение
   - обязательное акцептование службой ИБ перед утверждением

4. Реализация стратегии
   - создание дорожной карты в части ИБ и ее реализация
   - консультирование других подразделений

5. Контроль соответствия
   - плановый контроль со стороны службы ИБ
   - участие в формировании сводного отчета по реализации

6. Внеплановый пересмотр стратегии
   - ИБ может стать инициатором

# В КАЧЕСТВЕ РЕЗЮМЕ

- Проблема недостаточного вовлечения топ-менеджмента в процессы решаема
- Если не начинать разъяснять и обосновывать на систематической основе, то ситуация не изменится
- Лидерство в данном вопросе оптимально возложить на ИБ
- Итоговые решения по обеспечению операционной надежности и управлению рисками - это задача менеджмента
- Комплаенс – это давно не про документы, а про процессы

AKTIV.
CONSULTING

# БЛАГОДАРЮ
# ЗА ВНИМАНИЕ!


**Александр Моисеев**

Ведущий консультант
по информационной безопасности

moiseev@aktiv.consulting