

ОУЗ: самооценка или аудит?

Как не обмануть себя и регулятора



Владислав Крылов

Ведущий консультант по ИБ
AKTIV.CONSULTING



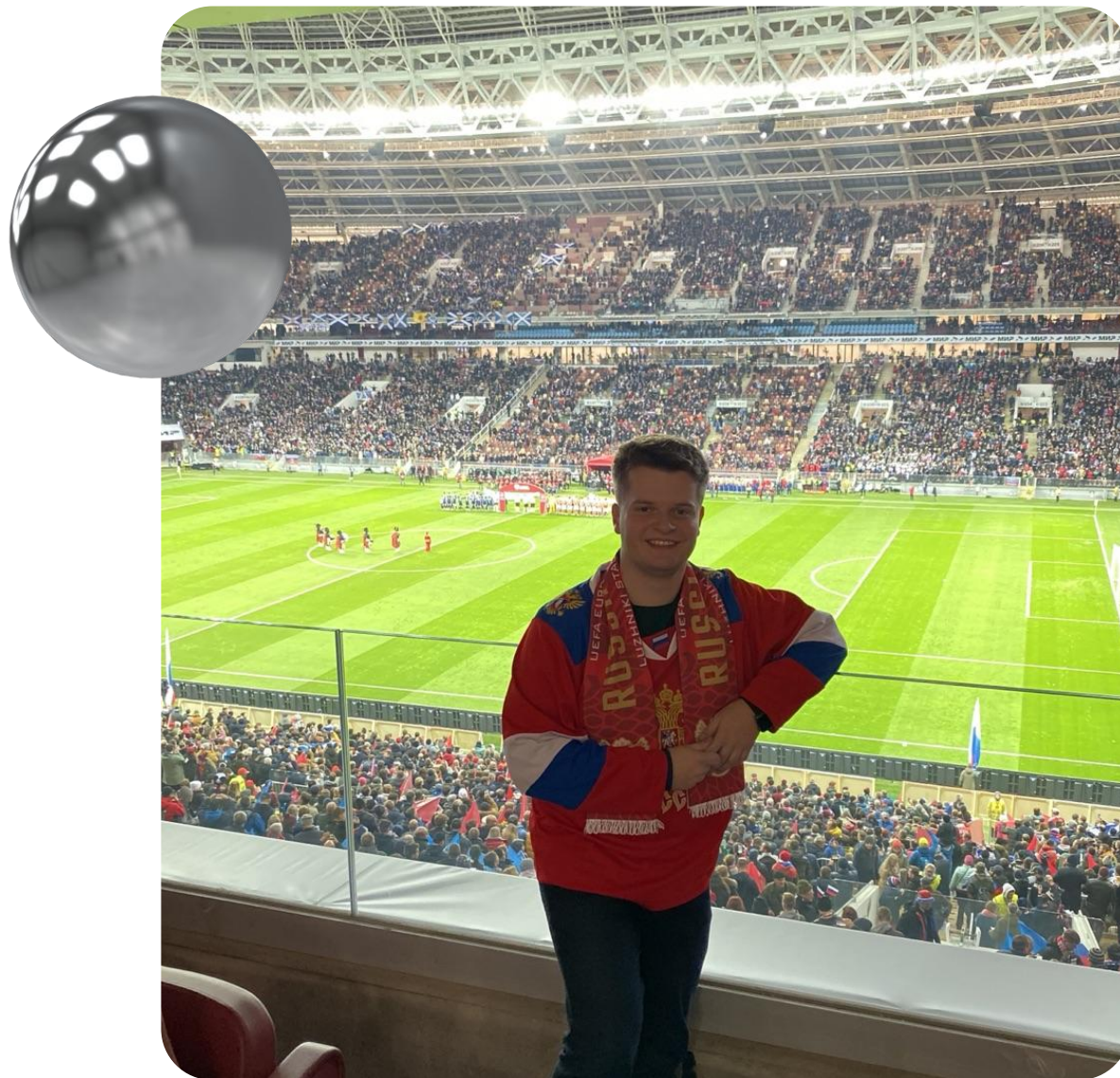
Немного о себе

Уровень зрелости – 30
(через неделю будет 31)

Ех. МГТУ им. Н.Э. Баумана.
Задействован в проектах
в сферах КИИ, РБПО

**Участвовал в рабочей группе
по рецензированию первых
итераций Методики ОУЗ**

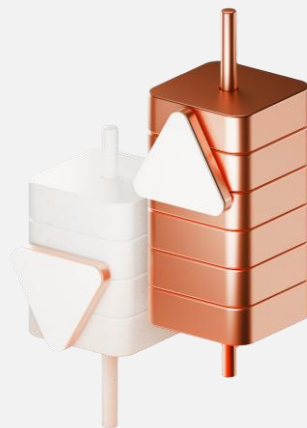
Болельщик футбольного клуба
«Ливерпуль», любитель мопсов



Содержание



Кратко
о новой методике



Самооценка **vs**
сторонний аудит



Как выбрать
свой путь

Выводы

Как жили раньше

- У каждого вендора и консультанта – **своя методика**
- **Результаты несопоставимы:** каждый считал по своей шкале
- Регулятор не имел **единого входа**
- Заказчики не могли **корректно сравнить** себя с рынком



Как живем теперь

Утвержден ФСТЭК России
7 августа 2026 г.

МЕТОДИЧЕСКИЙ ДОКУМЕНТ

МЕТОДИКА
ОЦЕНКИ УРОВНЯ ЗРЕЛОСТИ ДЕЯТЕЛЬНОСТИ В ОБЛАСТИ
ТЕХНИЧЕСКОЙ ЗАЩИТЫ ИНФОРМАЦИИ В ИНФОРМАЦИОННЫХ
СИСТЕМАХ И ОБЕСПЕЧЕНИЯ БЕЗОПАСНОСТИ ЗНАЧИМЫХ
ОБЪЕКТОВ КРИТИЧЕСКОЙ ИНФОРМАЦИОННОЙ ИНФРАСТРУКТУРЫ
РОССИЙСКОЙ ФЕДЕРАЦИИ

Кейс оценки **уровня зрелости ИБ**

Крупная страховая компания

ДИБ – 60+ чел.

ДИТ – 700+ чел.



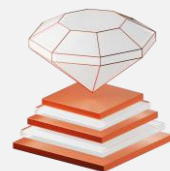
Проект стартовал
до выхода методики
ФСТЭК России



Проект под специфику
бизнеса, **без оглядки**
на регуляторный шаблон

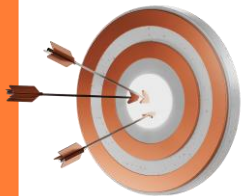


Запрос не единичный,
но подходы адаптивны;
статистика **недостаточно**
объективна



Вывод: рыночная
потребность в единой
методике назрела давно

Что изменилось: новая Методика



Единый
обязательный
подход



4 уровня зрелости:
начальный →
управляемый →
определенный →
верифицируемый



21 направление
оценки



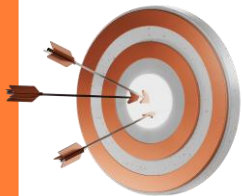
8 видов
требований
с весовыми
коэффициентами



Охват:
ГИС, КИИ, ИСПДн,
подрядные
организации



Что изменилось новая Методика



Единый
обязательный
подход



21 направлений
оценки

**Робот может оценить
уровень зрелости ИБ
компаний?**



**А ты без Методики
ФСТЭК России
сможешь?**



Охват:
ГИС, КИИ, ИСПДн,
подрядные
организации



Уровни зрелости ИБ согласно Методике

Уровень 1	Уровень 2	Уровень 3	Уровень 4
Начальный	Управляемый	Определенный	Верифицируемый
Процессы не формализованы	Базовые процессы есть, без системности	Процессы формализованы, документированы, измеряются	Системный уровень управления ИБ, реализованы все требования
Допустима самооценка	Допустима самооценка	Допустима самооценка	Необходима внешняя организация

Связь с действующими приказами ФСТЭК России

3. Настоящая Методика применяется для оценки уровня зрелости деятельности в области защиты информации ... в соответствии с законодательством Российской Федерации

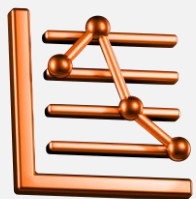
- о безопасности критической информационной инфраструктуры,
- об информации, информационных технологиях и о защите информации,
- о персональных данных



Самооценка: **что это и когда допустима**



Ловушки самооценки



Ответственные
оценивают
собственную
работу – конфликт
интересов



Подгонка баллов
под желаемый
уровень

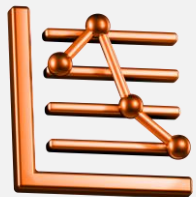


Нет внешнего
калибра –
верификация
под вопросом



Игнорирование
«слабых»
направлений

Ловушки самооценки



Ответственные
оценивают
собственную
работу – конфликты
интересов

Sourcee?

Подгонка баллов
под желаемый
уровень



Нет внешнего
калибра
верификации
под волю

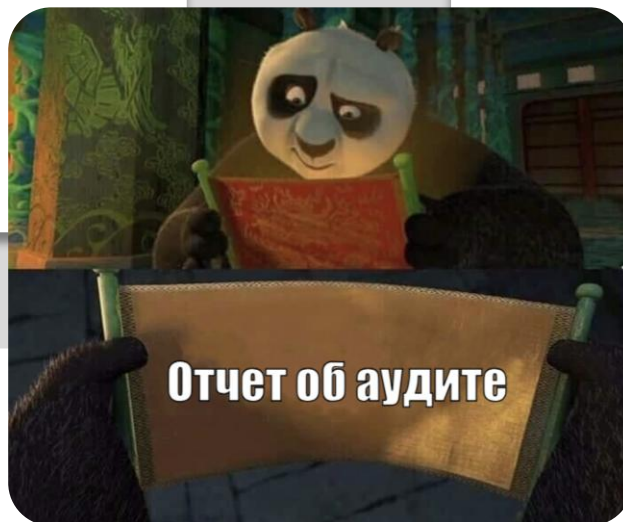
Trust me bro

Игнорирование
«слабых»
направлений

Сторонний аудит: **что дает и чего стоит**



Независимая
верификация,
которую
регулятор
считает
надежнее



Стоит
дороже,
требуется
подготовки



Для Уровня 4
фактически
обязателен

Внешний
контрагент
не связан
внутренней
политикой



С чем столкнулись при реализации **внешнего аудита?**



Артефакты есть,
а практика
**отличается
от документации**



**Смещенная
выборка:**
показываем
лучшее, скрываем
проблемное



Время на то,
чтобы вникнуть
в инфраструктуру –
при внутренней
проверке
отсутствует

Сравнение

Самооценка

Стоимость: околонулевая

Трудозатраты заказчика:
умеренные

Объективность: риск искажения

Доказательная сила: для локального
использования

Уровень зрелости: 1-3 уровни

Скорость: оперативно

Сторонний аудит

Стоимость: высокая

Трудозатраты заказчика: высокие
(интервью, опросные листы, верификация)

Объективность: независимая оценка

Доказательная сила: пригодна
для регулятора

Уровень зрелости: 4, но можно на любом

Скорость: может затягиваться

Матрица выбора: когда и какой формат достаточен

Бюджет ограничен:

самооценка + точечный
внешний аудит

**Уровень 1-2,
внутренние
цели:**
самооценка

**Уровень 3,
внутренние
цели:**
самооценка с внутренним
аудитом качества

**Уровень 3,
демонстрация
регулятору:**
внешний
аудит

Уровень 4:
внешний аудит
обязателен

Решение – не «или/или»,
а комбинация под цель



Практические ориентиры: как выбрать формат

Я, понимающий, что помимо
категории ОКИИ, класса
защищенности ИСПДн и т.д

Теперь придется еще и считать
уровень защищенности

1

Определите
целевой
уровень

2

Оцените
бюджет
и сроки

3

Проверьте
артефакты
по 21
направлению

4

Уровень 4 –
сразу
внешний аудит

5

Уровень 3 –
не все так
просто

6

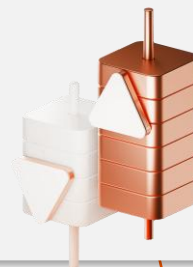
Самооценку
всегда полезно
провести
первой – как
«репетицию»

Выводы

Методика ФСТЭК России впервые дает **единый подход**. Выбор формата определяется целевым уровнем, не только бюджетом



Самооценка – полезный инструмент с осознанием ограничений



Считать **Узи** – не цель. Цель – **понимать**, где вы на самом деле, и **куда двигаться**



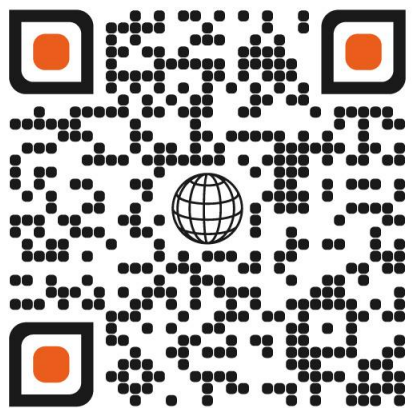
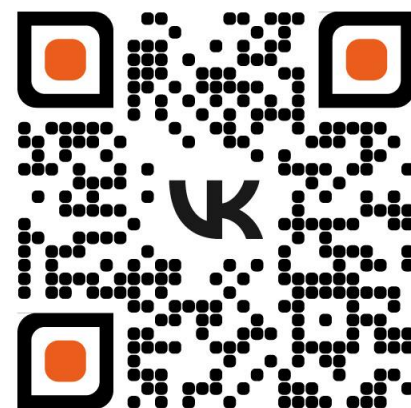
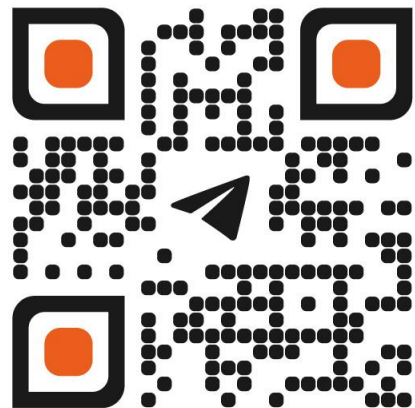
Защищаться нужно не от **регулятора**, а от **инцидента**. Ваш **Узи** – дополнительный **рубеж защиты**



Вот такие вот дела, слушатели



Спасибо за внимание!



БЛАГОДАРЮ ЗА ВНИМАНИЕ!

AKTIV.
CONSULTING



Владислав Крылов

Ведущий консультант по ИБ
AKTIV.CONSULTING

krylov@aktiv.consulting

