

СТАТИСТИКА ОЦЕНОК СООТВЕТСТВИЯ

КАК Я МОГ БЫ ПОЛУЧИТЬ «ХОРОШО»
И ПРИ ЧЕМ ТУТ ИНФОРМАЦИОННЫЕ СИСТЕМЫ

Александр Митрохин
Руководитель направления АО «ДиалогНаука»

10 октября 2023 года, Москва

Обобщенные результаты оценки соответствия

Основания для проведения оценки соответствия требованиям ГОСТ Р 57580.1-2017

46%

Положение 683-П

53%

Положение 802- П
(747-П)

35%

Положение 757-П
(684-П)

90%

Положение 719-П

16%

Приказ 453
(930, 321)
Минцифры

5%

Рассматривалось 2 нормативных документа
для формирования контуров оценки

40%

Рассматривалось 3 нормативных документа
для формирования контуров оценки

5%

Рассматривалось 4 нормативных документа
для формирования контуров оценки

Рассматриваемый уровень защиты в соответствии с
ГОСТ Р 57580.1-2017

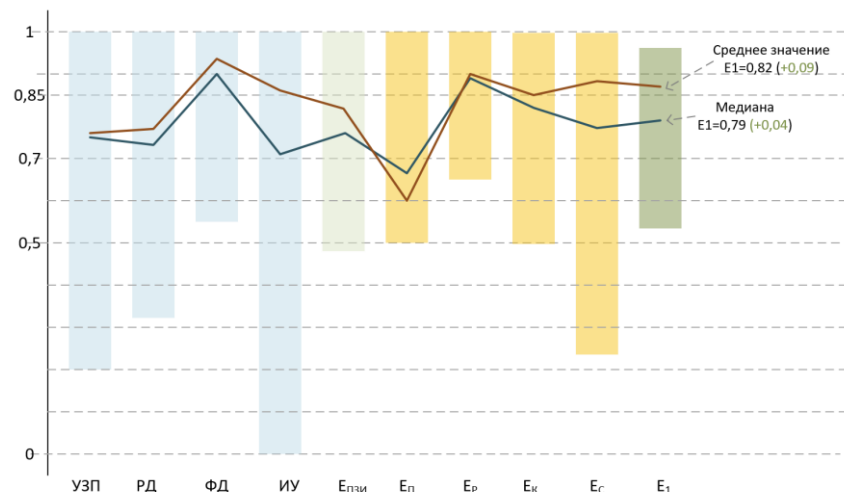


Обобщенные результаты оценки соответствия



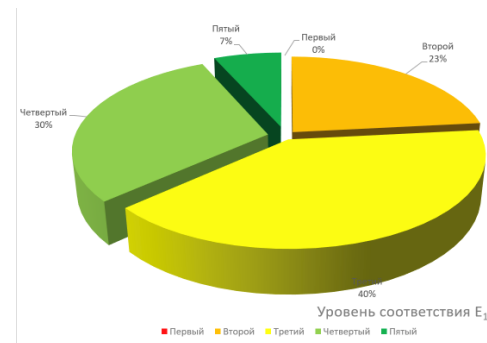
Результаты оценки соответствия по направлениям

Процесс 1 «Обеспечение защиты информации при управлении доступом»



Топ 5 часто встречающихся несоответствий:

- ✓ УЗП.1 – Работа под неперсонифицированными УЗ
- ✓ УЗП.14 (УЗП.15) – Установление фактов неиспользования предоставленных прав доступа
- ✓ РД.2 (РД.4) – Многофакторная аутентификация
- ✓ РД.12 – Запрет множественной аутентификации
- ✓ ИУ.4 (ИУ.6) – Контроль состава ресурсов доступа (объектов доступа) и их корректного размещения



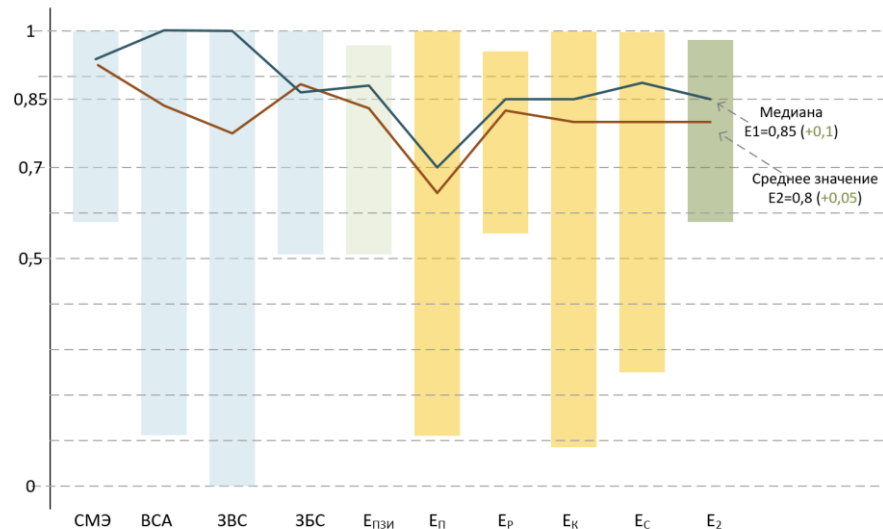
В сравнении с результатами 2021-2022 гг.

E₁ (медиана) +0,04

E₁ (среднее) +0,09

Результаты оценки соответствия по направлениям

Процесс 2 «Обеспечение защиты вычислительных сетей»



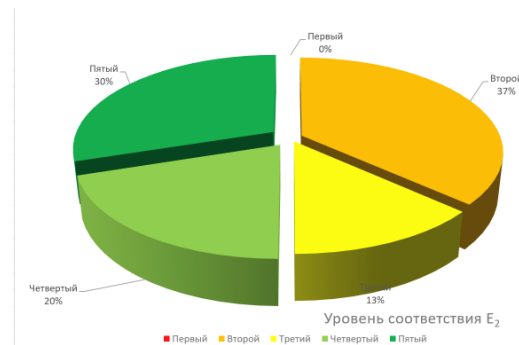
Топ 5 часто встречающихся несоответствий:

- ✓ СМЭ.7 – Сегментирование (выделение и контроль сегмента разработки и тестирования)
- ✓ СМЭ.8 (СМЭ.9) – Сегментирование (АРМ пользователей и эксплуатационного персонала)
- ✓ ВСА.9 – Блокирование атак типа «отказ в обслуживании»
- ✓ ЗБС.4 – Сетевая изоляция wi-fi
- ✓ ЗБС.8 – Контроль доступа к wi-fi

В сравнении с результатами 2021-2022 гг.

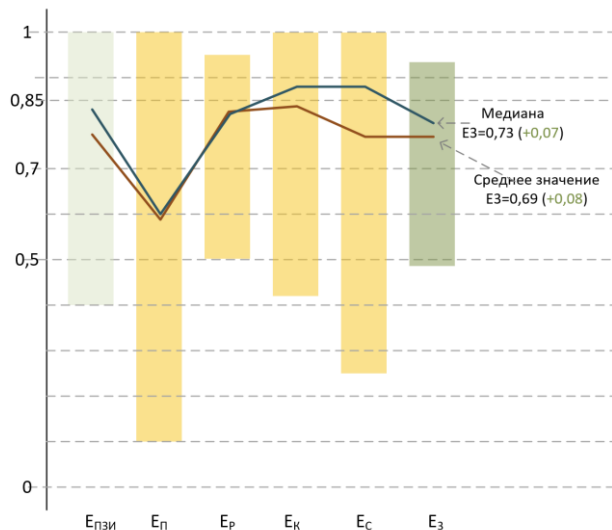
E_2 (медиана) **+0,1**

E_2 (среднее) **+0,05**



Результаты оценки соответствия по направлениям

Процесс 3 «Контроль целостности и защищенности информационной инфраструктуры»



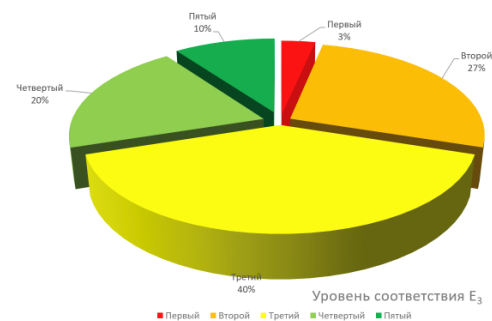
Топ часто встречающихся несоответствий:

- ✓ ЦЗИ.7-10 – Сканирование и анализ конфигурации
- ✓ ЦЗИ.22 – Контроль состава ПО серверного оборудования

В сравнении с результатами 2021-2022 гг.

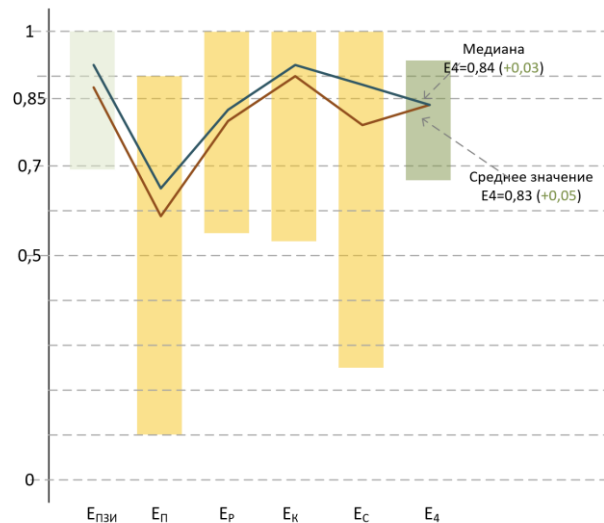
E_З (медиана) **+0,07**

E_З (среднее) **+0,08**



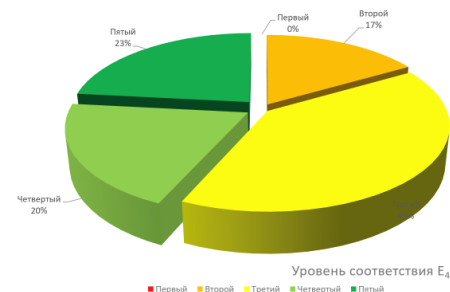
Результаты оценки соответствия по направлениям

Процесс 4 «Защита от вредоносного кода»



Топ 5 часто встречающихся несоответствий:

- ✓ ЗВК.7 – АВПО на банкоматах и платежных терминалах
- ✓ ЗВК.12 – Еженедельная проверка серверов
- ✓ ЗВК.13 (ЗВК.14) – Многовендорность защиты
- ✓ ЗБС.19 – Входной контроль переносных носителей информации
- ✓ ЗБС.20 – Проверка до и после установки ПО



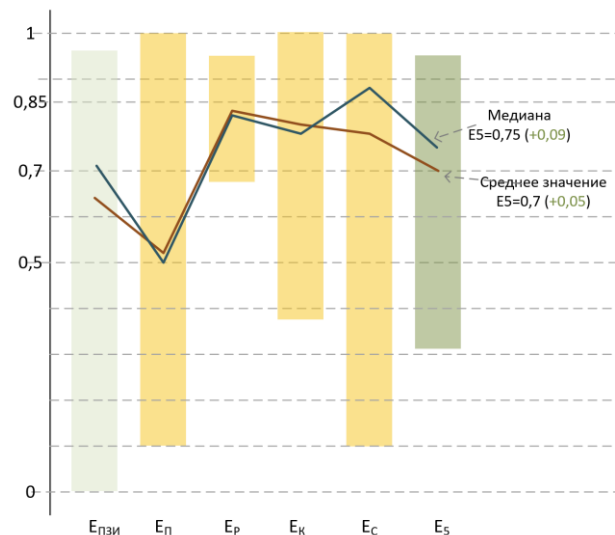
В сравнении с результатами 2021-2022 гг.

E₄ (медиана) +0,03

E₄ (среднее) +0,05

Результаты оценки соответствия по направлениям

Процесс 5 «Предотвращение утечек информации»



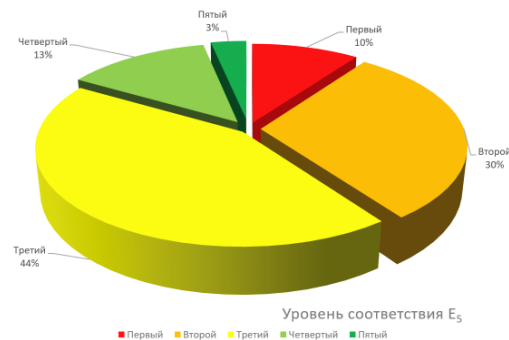
Топ часто встречающихся несоответствий:

- ✓ ПУИ.1-4 – недостаточно работы DLP системы в режиме «Мониторинга»
- ✓ ПУИ.11 (ПУИ.15, ПУИ.17) – контентный анализ передаваемой информации

В сравнении с результатами 2021-2022 гг.

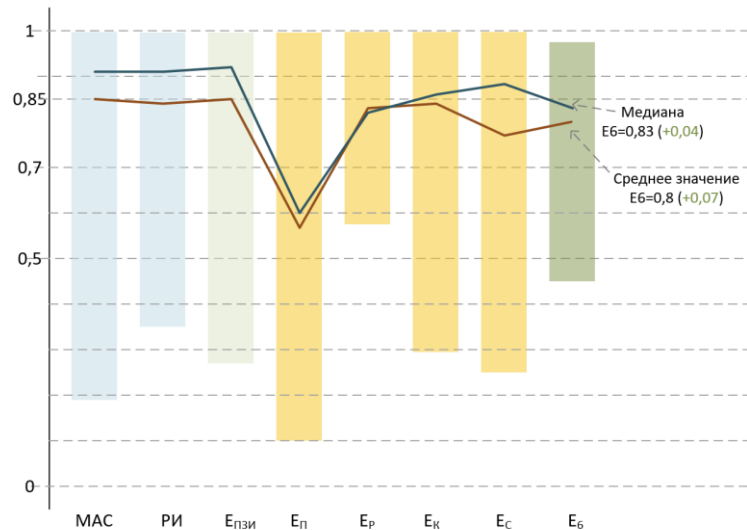
E_5 (медиана) **+0,09**

E_5 (среднее) **+0,05**



Результаты оценки соответствия по направлениям

Процесс 6 «Управление инцидентами защиты информации»



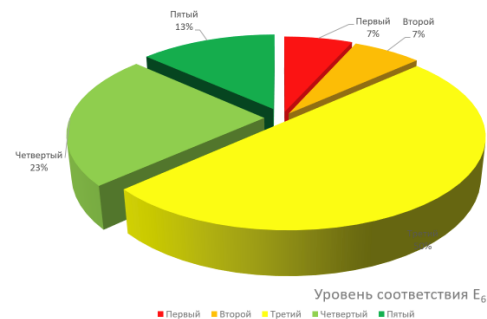
Топ 5 часто встречающихся несоответствий:

- ✓ MAC.8 – Централизованный сбор данных о событиях
- ✓ MAC.15 (MAC.16) – Сроки хранения событий
- ✓ MAC.17 - Нормализация, фильтрация, агрегация и классификация данных регистрации
- ✓ РИ.9 – корректное определение состава ГРИЗИ
- ✓ РИ.11 – полномочия ГРИЗИ

В сравнении с результатами 2021-2022 гг.

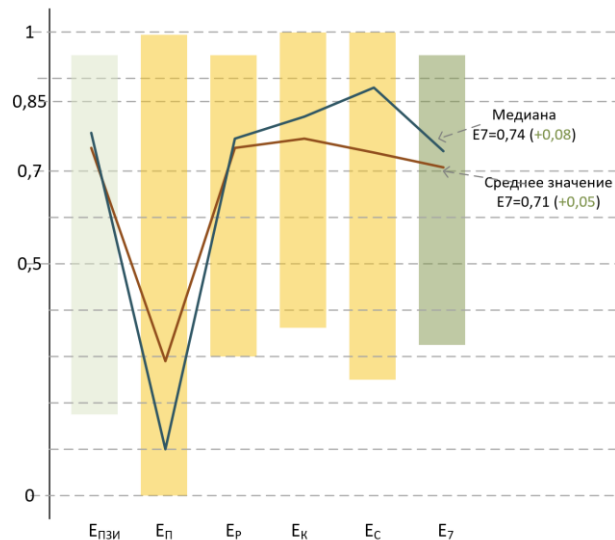
E_6 (медиана) **+0,04**

E_6 (среднее) **+0,07**



Результаты оценки соответствия по направлениям

Процесс 7 «Защита среды виртуализации»



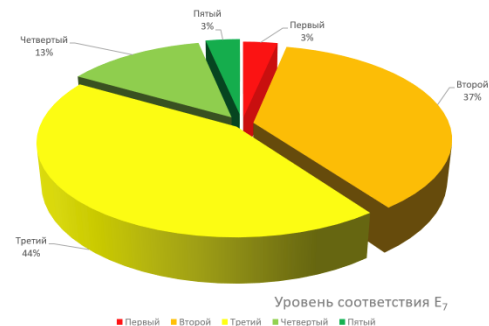
Топ часто встречающихся несоответствий:

✓ Все???

В сравнении с результатами 2021-2022 гг.

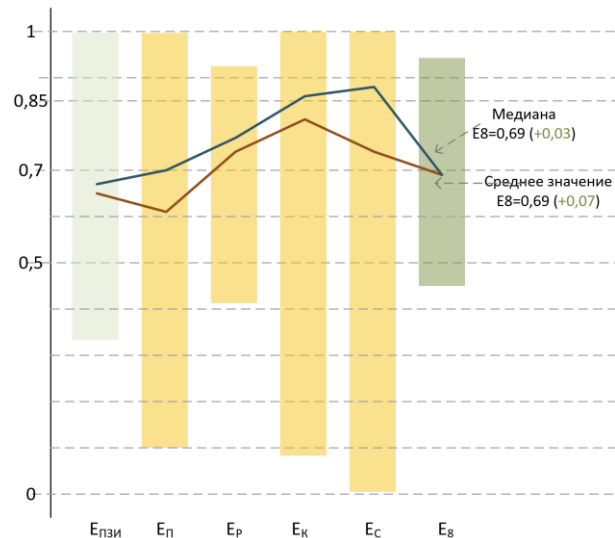
E_7 (медиана) **+0,08**

E_7 (среднее) **+0,05**



Результаты оценки соответствия по направлениям

Процесс 8 «Защита информации при осуществлении удаленного логического доступа с использованием мобильных (переносных) устройств»



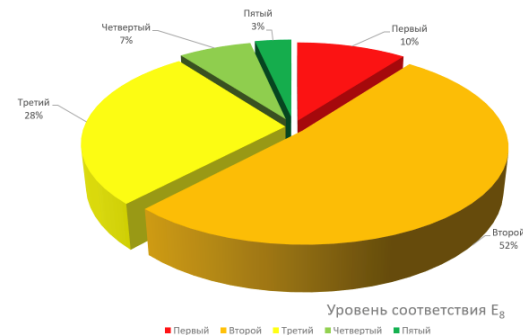
Топ часто встречающихся несоответствий:

- ✓ ЗУД.2 – Аутентификация устройств (мобильных/переносных)
- ✓ ЗУД.5 – Многофакторная аутентификация
- ✓ ЗУД.7 – Контроль трафика при удаленной работе

В сравнении с результатами 2021-2022 гг.

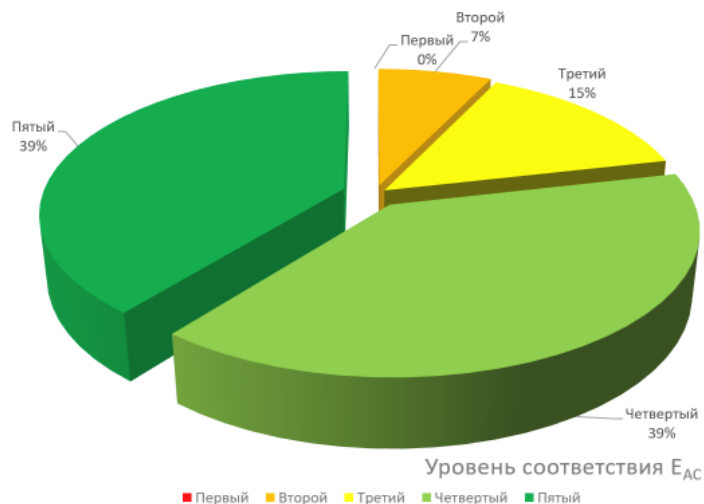
E₇ (медиана) **+0,03**

E₇ (среднее) **+0,07**



Результаты оценки соответствия по направлениям

Защита информации на этапах жизненного цикла автоматизированных систем и приложений



Топ часто встречающихся несоответствий:

- ✓ ЖЦ.3 – Определение параметров настроек технических мер системы защиты информации АС
- ✓ ЖЦ.8 – ОУД 4...
- ✓ ЖЦ.14 – Тестирование на проникновение при вводе в эксплуатацию АС

Результаты оценки соответствия по направлениям



Планирование:

- ✓ ПЗИ.2 (ПЗИ.4) – Во внутренних нормативных документах отсутствует отсылка к ГОСТ Р 57580.1-2017
- ✓ ПЗИ.5 – Не определены параметры настроек технических мер защиты информации и информационной инфраструктуры

Реализация:

- ✓ РЗИ.11 (РЗИ.12, РЗИ.13) – Применение сертифицированных по требованиям безопасности информации СЗИ

Контроль:

- ✓ КЗИ.8 – Фиксация результатов контроля

Совершенствование:

- ✓ СЗИ.2 – Анализ необходимости совершенствования при изменении политики в отношении целевых показателей величины допустимого остаточного операционного риска (риск-аппетита)

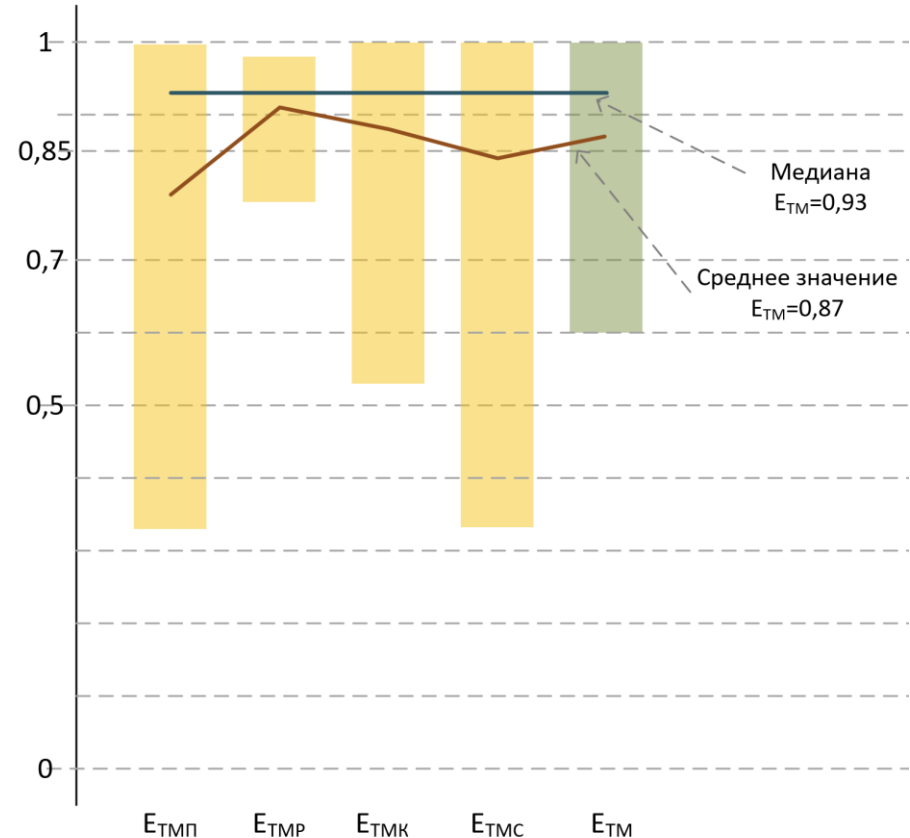
Результаты оценки соответствия

Положение Банка России 683-П

- ✓ Качественная оценка:
 - ✓ Проверяется 35 требований (качественная оценка)
 - ✓ Определение методики выставления оценки
 - ✓ Результаты на текущий момент только для внутреннего использования
- ✓ Количественная оценка (12-МР)
 - ✓ Проверяется 15 требований (в соответствии с 12-МР) в части технологических мер и 2 требования по ППО
 - ✓ Целевые показатели не заданы
 - ✓ Результаты включаются в форму 0409071

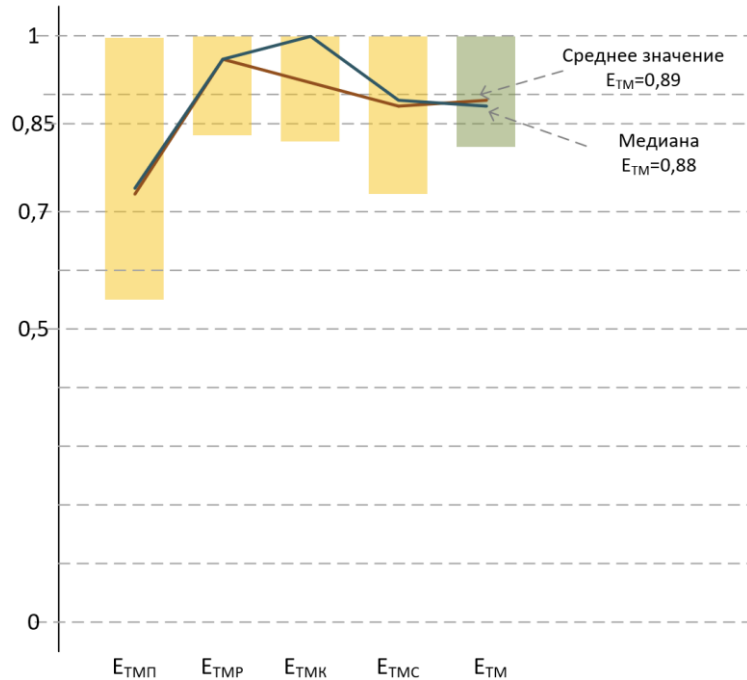
Топ часто встречающихся несоответствий:

- ✓ Неполное выполнение требований 152-ФЗ «О персональных данных» (п.1)
- ✓ Документированность области применения технологических мер
- ✓ Сертифицированное ПО или ОУД 4 (п.4.1)
- ✓ Регистрация событий (п.5.2.3)
- ✓ Классификация событий как инциденты (п.8)

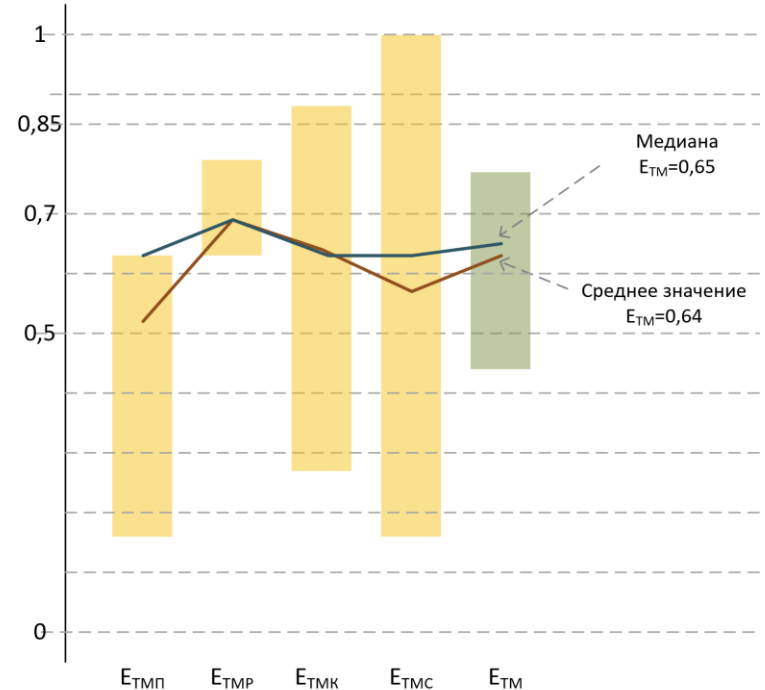


Результаты оценки соответствия

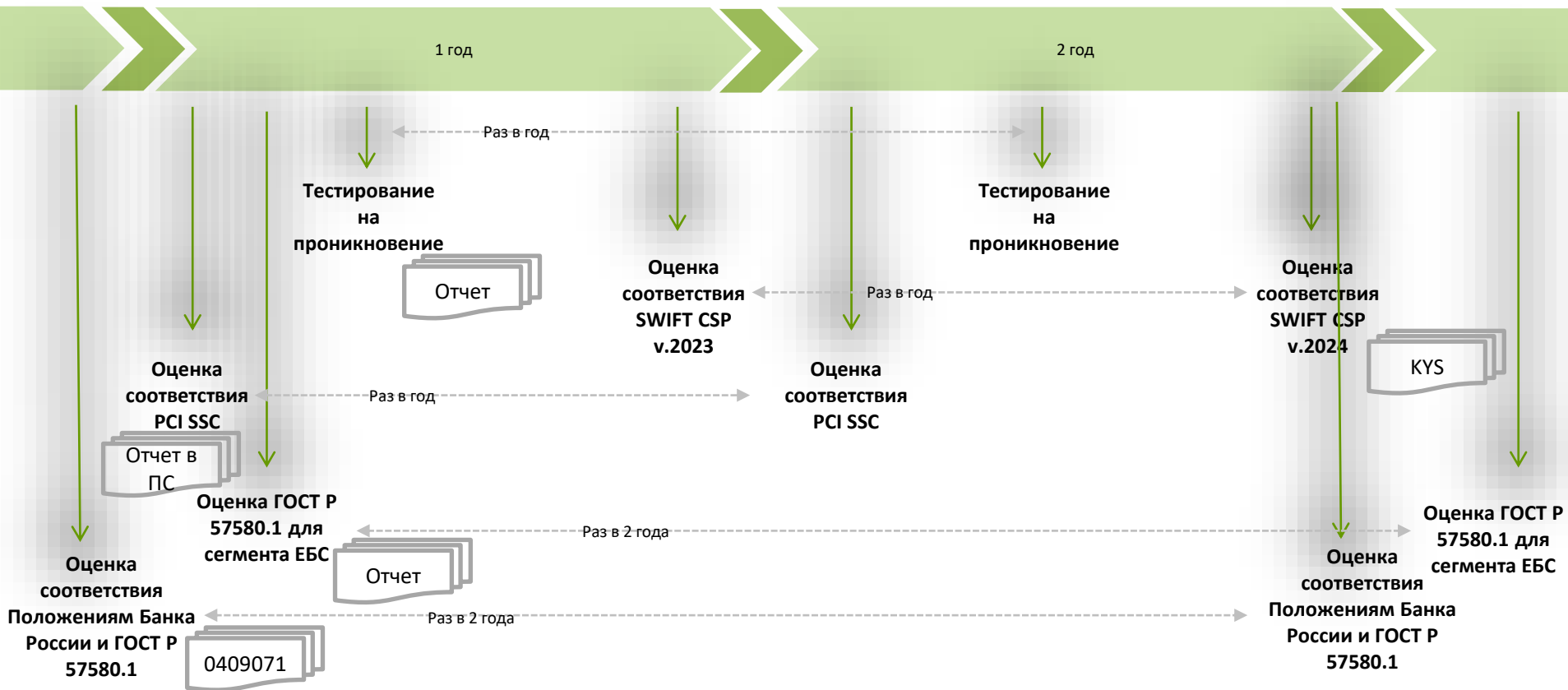
Положение 802-П (в части 12-МР)



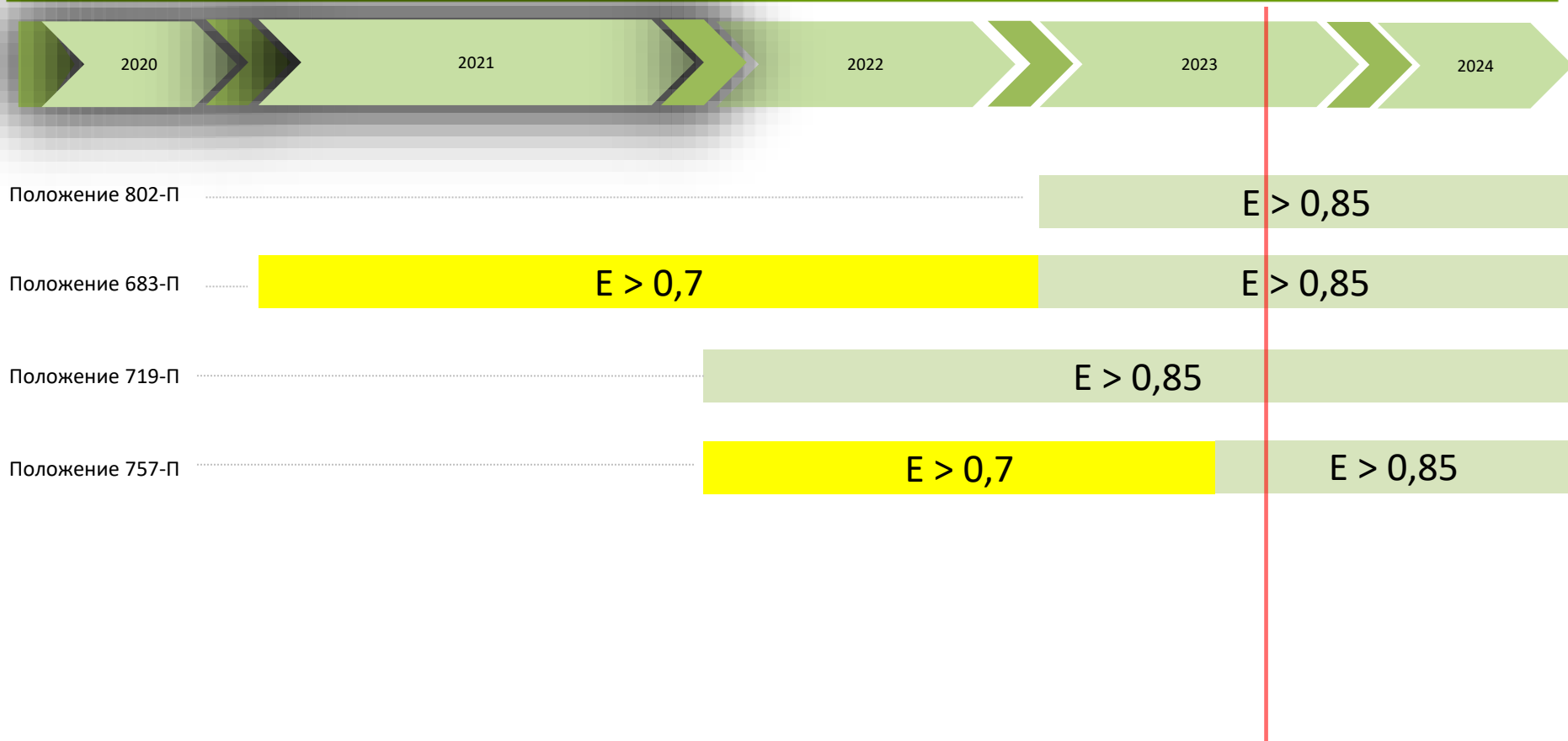
Положение 719-П (в части 12-МР)



В помощь для финансовой организации



Положения Банка России по защите информации



Успеть за 60 дней?

- ✓ системы ДБО для физических и юридических лиц
- ✓ АБС
- ✓ АРМ КБР-Н, АРМ СПФС
- ✓ процессинговые системы
- ✓ MS Active Directory Service



около 8 АС, каждая оценивается
по 50 параметрам

+

Интервью по описанию технологических процессов

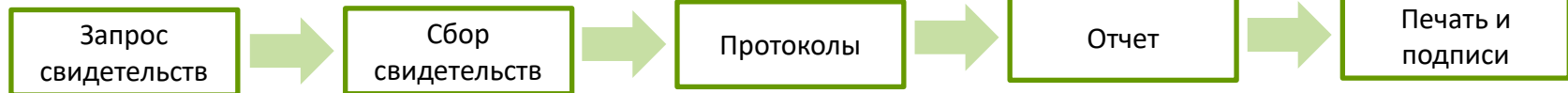
- ✓ средства защиты информации
- ✓ процессы обеспечения ИБ
- ✓ физическая безопасность



около 10 интервью по процессам защиты
информации

+

СЗИ



Спасибо за внимание!

Вопросы?

АО «ДиалогНаука»

Телефон: +7 (495) 980-67-76

Факс: +7 (495) 980-67-75

E-mail: A.Mitrokhin@dialognauka.ru

<http://www.DialogNauka.ru>