ОЦЕНКА СООТВЕТСТВИЯ

ЦИФРЫ И ТОЛЬКО ЦИФРЫ

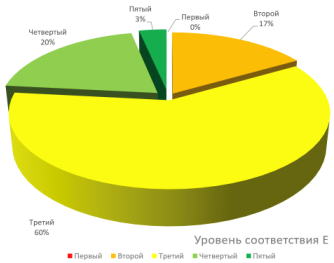
Антон Свинцицкий
Директор по консалтингу

20 мая 2025 года, Москва

ДиалОгНаука

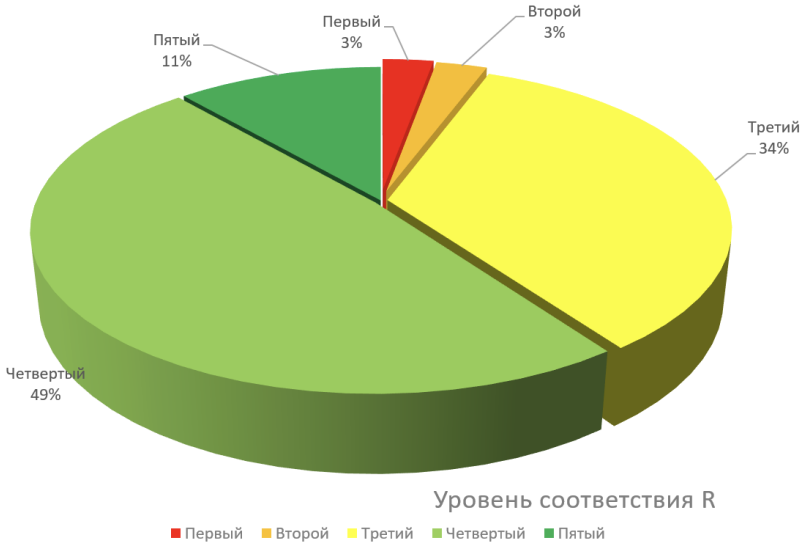
Обобщенные результаты оценки соответствия

2018-2021



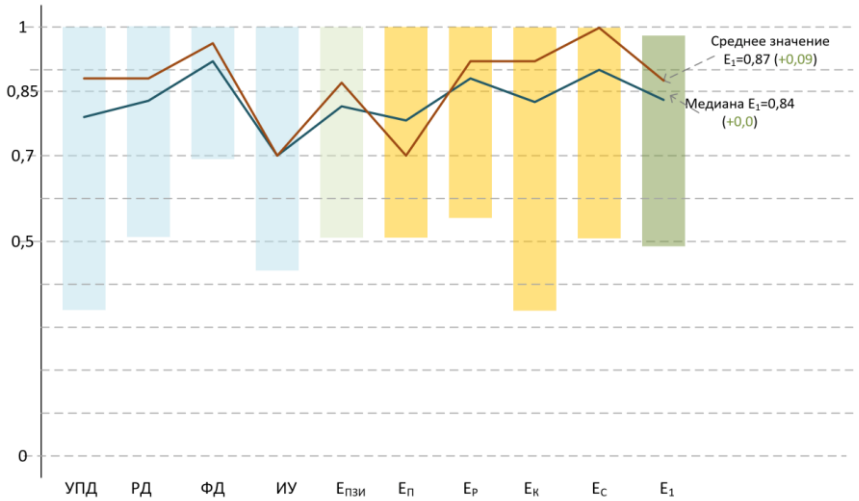
2021-2023

2023-2025



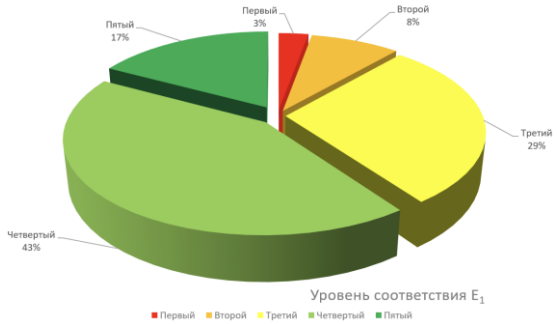
Результаты оценки соответствия по направлениям

Процесс 1 «Обеспечение защиты информации при управлении доступом»



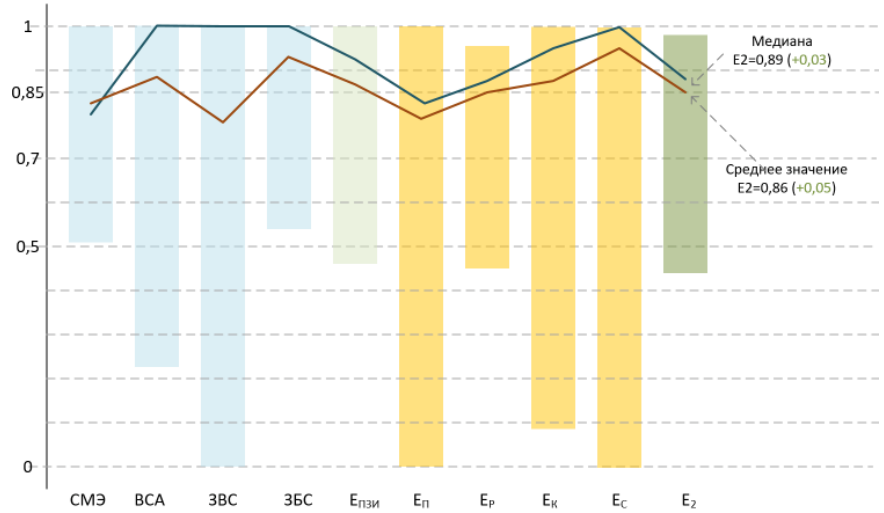
Топ 5 часто встречающихся несоответствий:

- ✓ УЗП.9 (Контроль прав) – реализовано с использованием организационных мер
- ✓ УЗП.14 (УЗП.15) – Установление фактов неиспользования предоставленных прав доступа
- ✓ УЗП.21 – Отстутствие квалифицированных кадров
- ✓ РД.2 (РД.4) – Многофакторная аутентификация
- ✓ РД.12 – Запрет множественной аутентификации
- ✓ ИУ.4 (ИУ.6) – Контроль состава ресурсов доступа (объектов доступа)



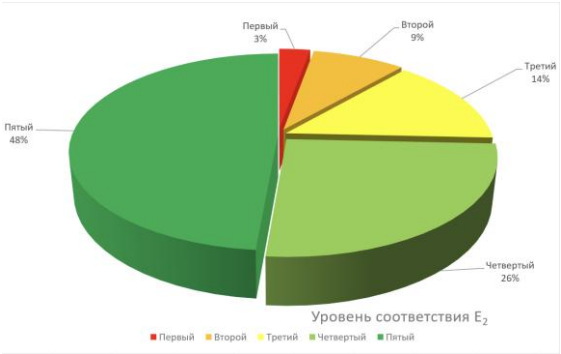
Результаты оценки соответствия по направлениям

Процесс 2 «Обеспечение защиты вычислительных сетей»



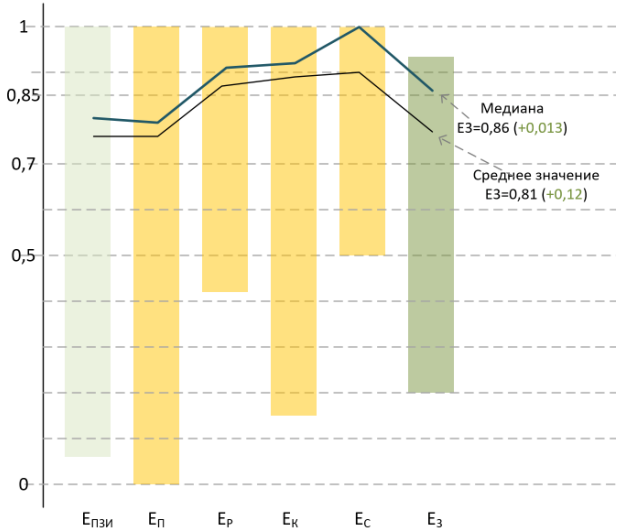
Топ 5 часто встречающихся несоответствий:

- ✓ СМЭ.7 – Сегментирование (выделение и контроль сегмента разработки и тестирования)
- ✓ СМЭ.8 (СМЭ.9) – Сегментирование (АРМ пользователей и эксплуатационного персонала)
- ✓ СМЭ.3 (СМЭ.16) – фильтрация на прикладном уровне
- ✓ ЗВС – Отсутствие защиты трафика на оптических линиях связи



Результаты оценки соответствия по направлениям

Процесс 3 «Контроль целостности и защищенности информационной инфраструктуры»

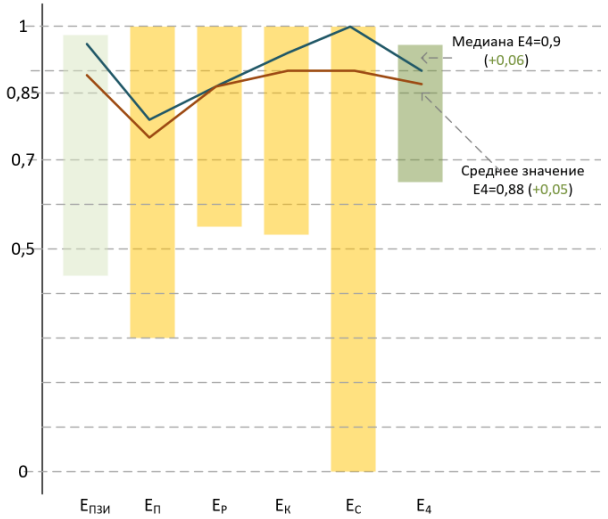


Топ часто встречающихся несоответствий:

- ✓ ЦЗИ.7-10 – Сканирование и анализ конфигурации
- ✓ ЦЗИ.12 (ЦЗИ.13) – неподдерживаемые версии ПО
- ✓ ЦЗИ.22 – Контроль состава ПО серверного оборудования

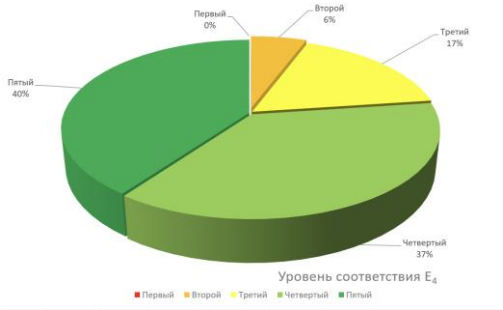
Результаты оценки соответствия по направлениям

Процесс 4 «Защита от вредоносного кода»



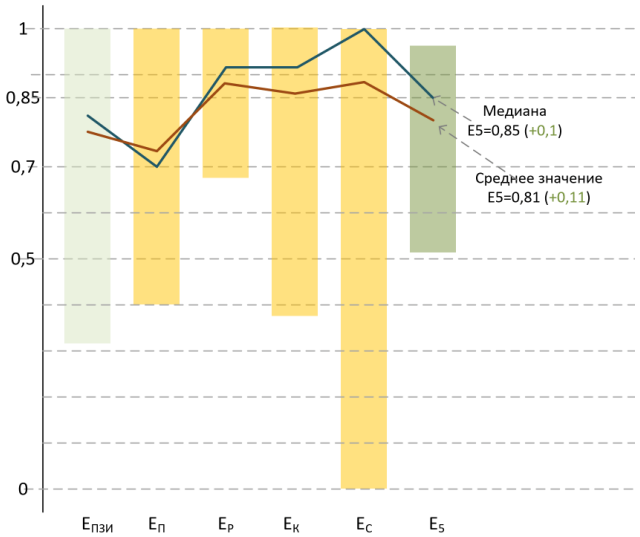
Топ 5 часто встречающихся несоответствий:

- ✓ 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



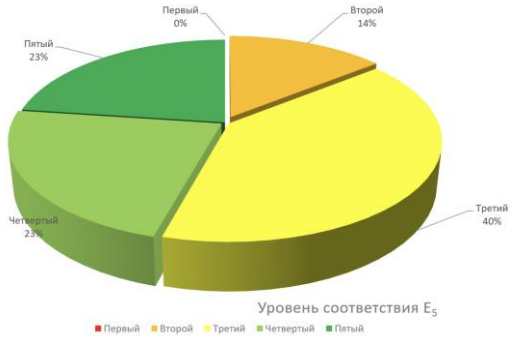
Результаты оценки соответствия по направлениям

Процесс 5 «Предотвращение утечек информации»



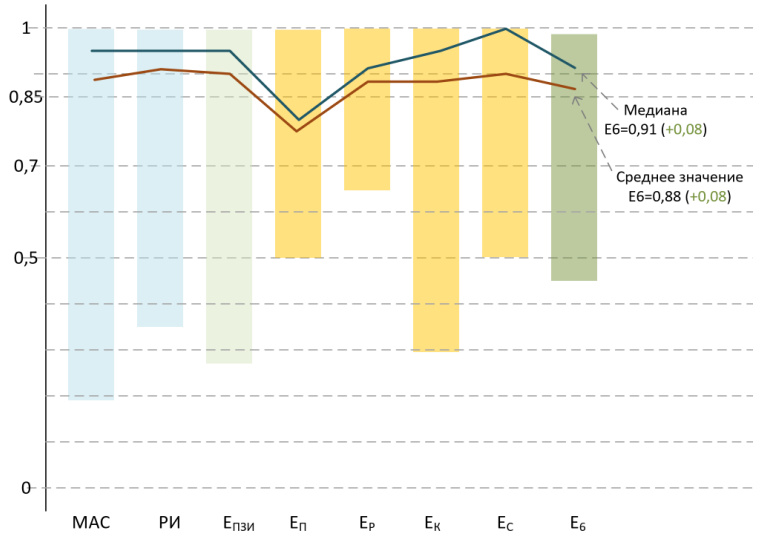
Топ часто встречающихся несоответствий:

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



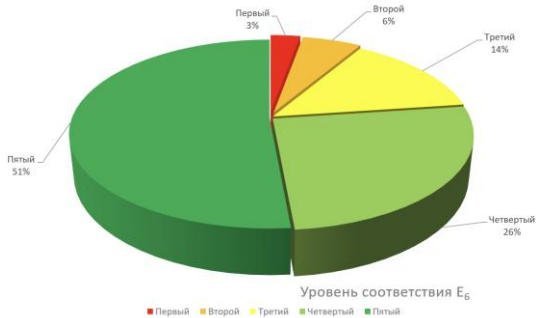
Результаты оценки соответствия по направлениям

Процесс 6 «Управление инцидентами защиты информации»



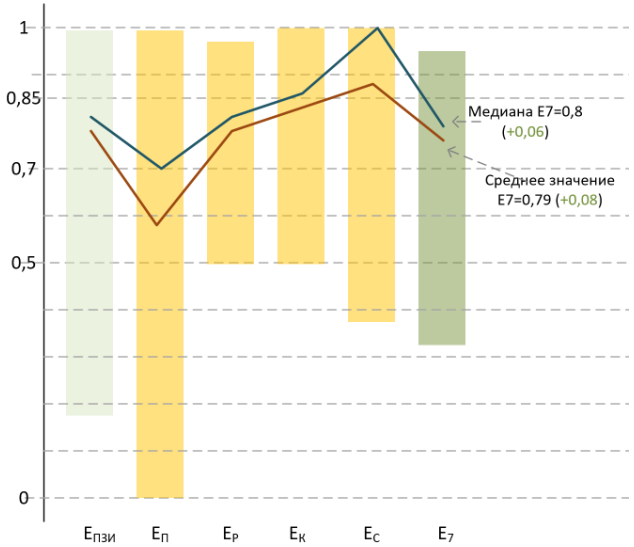
Топ 5 часто встречающихся несоответствий:

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



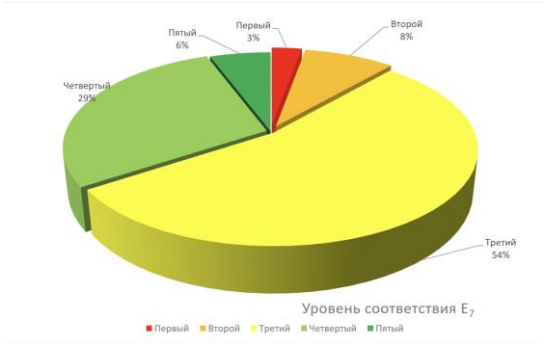
Результаты оценки соответствия по направлениям

Процесс 7 «Защита среды виртуализации»



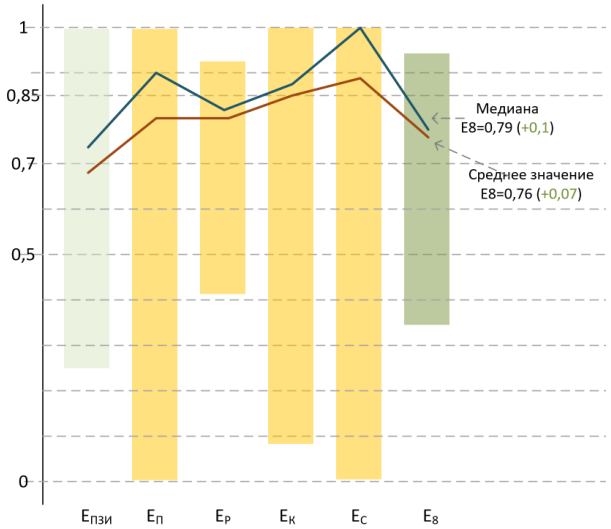
Топ часто встречающихся несоответствий:

- ✓ ЗСВ.9 – двухфакторная аутентификация
- ✓ ЗСВ.11 – разделение ролей
- ✓ ЗСВ.35 - протоколирование



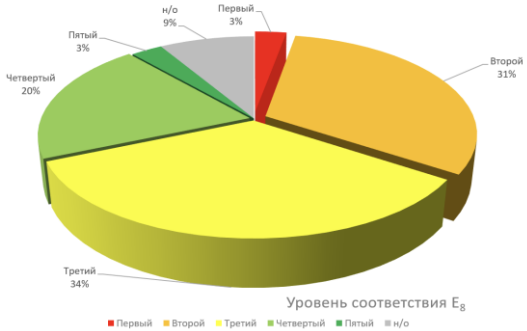
Результаты оценки соответствия по направлениям

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



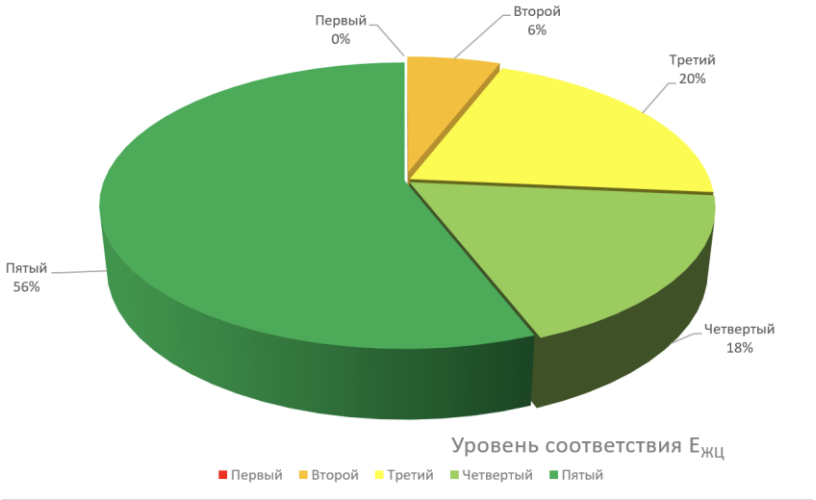
Топ часто встречающихся несоответствий:

- ✓ ЗУД.3 – MDM
- ✓ ЗУД.5 – Многофакторная аутентификация
- ✓ ЗУД.7 – Контроль трафика при удаленной работе



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 по направлениям

Ключевые несоответствия по Положениям Банка России:

- ✓ не определены и не формализированы Технологические участки и автоматизированные системы на этих участках (все положения)
- ✓ не определены применимые меры защиты на каждом технологическом участке (все положения)
- ✓ не реализованы меры в соответствии с PDCA циклом (методические рекомендации 3-МР)
- ✓ отсутствие ОУД 4 для используемых версий прикладного ПО (Положение 821-П, Положение 851-П)
- ✓ не установлены ограничения по параметрам операций (Положение 821-П)
- ✓ отсутствие кода технологического участка при регистрации событий (Положение 821-П, Положение 851-П)
- ✓ подпись электронных сообщений с использованием СКЗИ или имитозащита для систем дистанционного банковского обсуждения физических лиц (Положение 851-П)
- ✓ верификация адреса электронной почты (Положение 821-П)

2021 → 2022 → 2023 → 2024

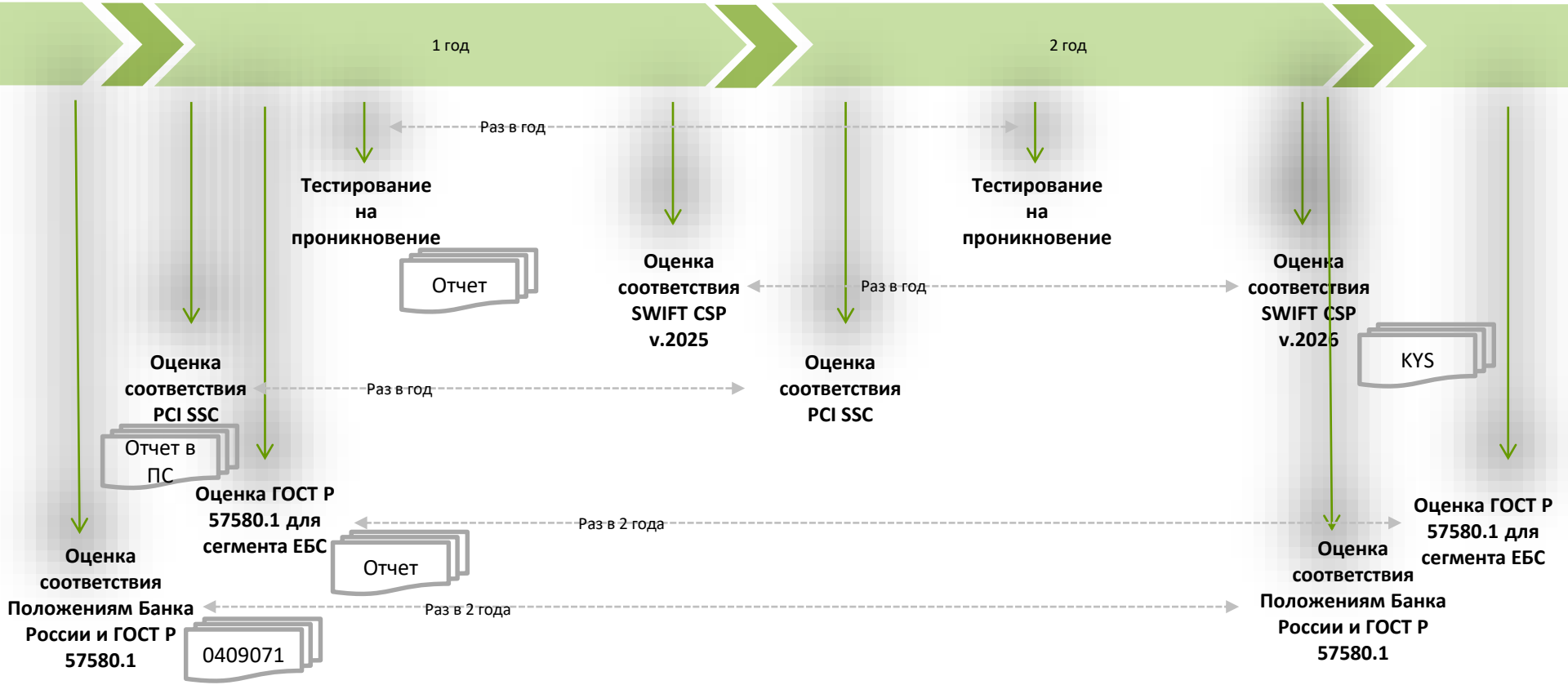
	E1	E2	E3	E4	E5	E6	E7	E8	ЖЦ
2024	0,87	0,89	0,86	0,9	0,85	0,92	0,8	0,80	0,92
2023	0,84	0,86	0,8	0,85	0,77	0,83	0,75	0,69	0,88
2022	0,82	0,86	0,8	0,84	0,75	0,83	0,74	0,69	0,88
2021	0,75	0,74	0,73	0,81	0,66	0,79	0,66	0,66	0,85

2021 → 2022 → 2023 → 2024

	E1	E2	E3	E4	E5	E6	E7	E8	ЖЦ
2024	0,87	0,89	0,86	0,9	0,85	0,92	0,8	0,80	0,92
2023	0,84	0,86	0,8	0,85	0,77	0,83	0,75	0,69	0,88
2022	0,82	0,86	0,8	0,84	0,75	0,83	0,74	0,69	0,88
2021	0,75	0,74	0,73	0,81	0,66	0,79	0,66	0,66	0,85

КПУР!!!

В помощь для финансовой организации



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