

# ОЦЕНКА СООТВЕТСТВИЯ

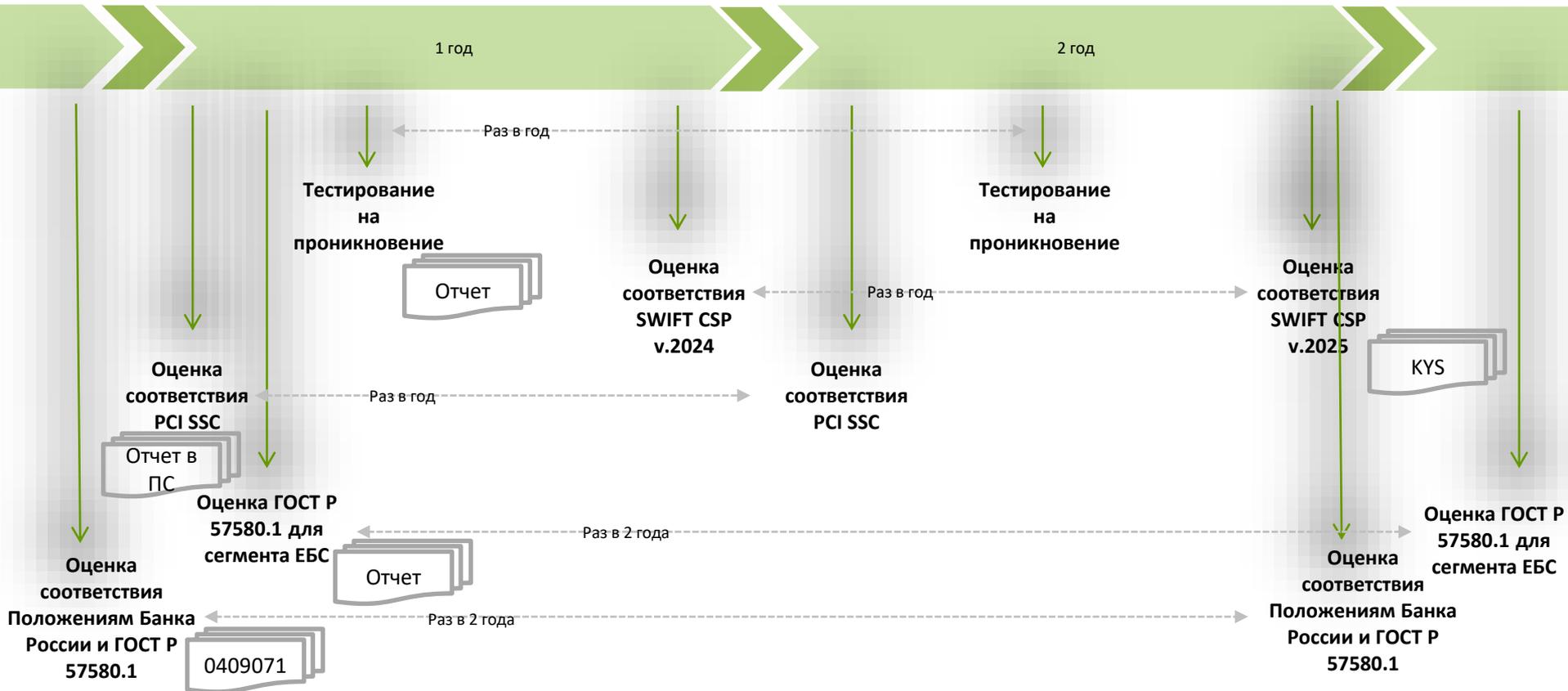
КАК СДЕЛАТЬ ПРОЦЕСС БЫСТРЫМ И ПРОЗРАЧНЫМ ДЛЯ ЗАКАЗЧИКОВ

Антон Свинцицкий  
Директор по консалтингу

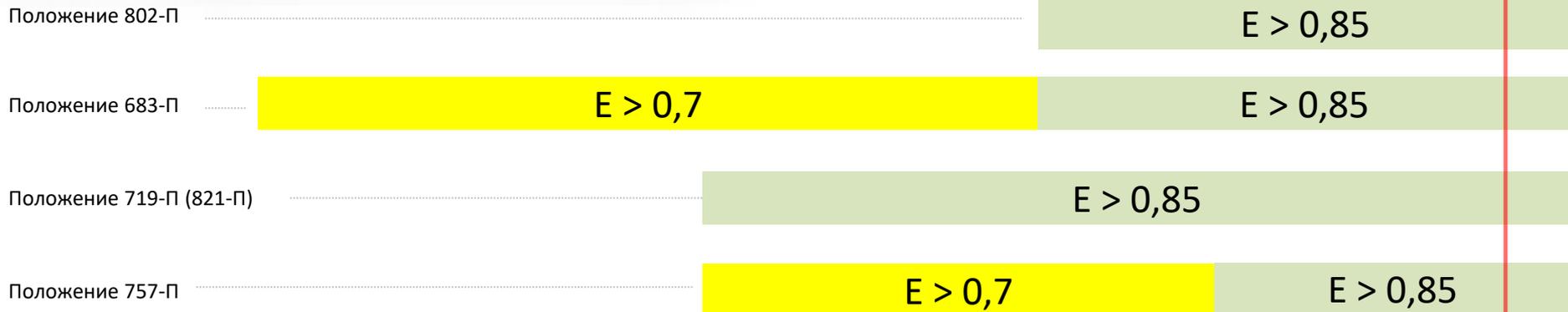
4 июня 2024 года, Москва

**ДиалОГНаука**

# В помощь для финансовой организации

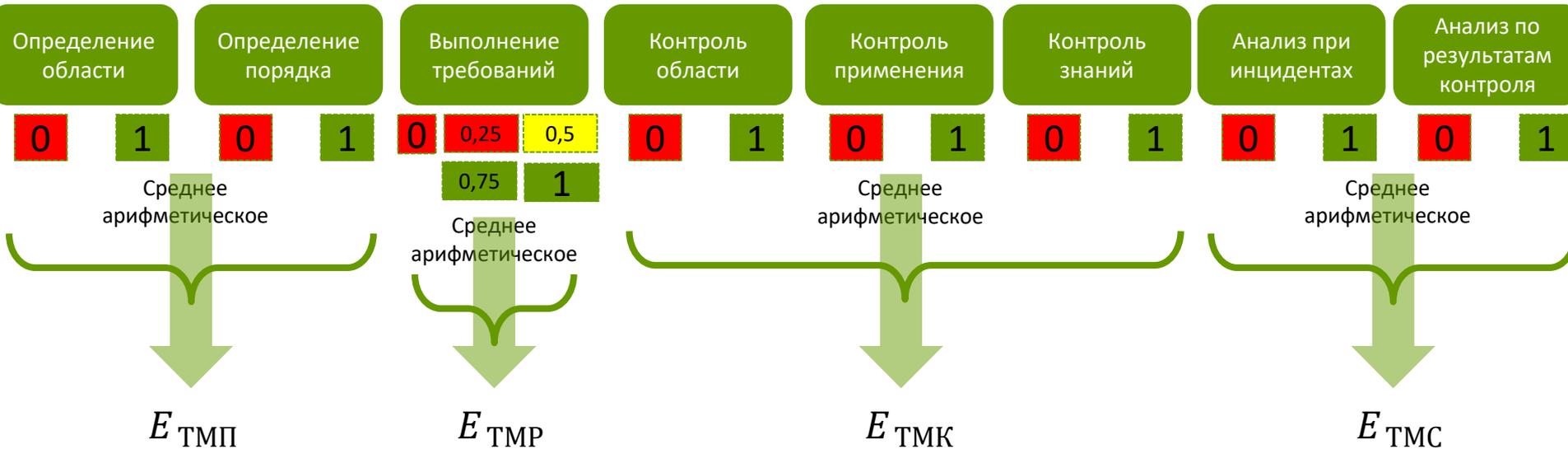


# Положения Банка России по защите информации



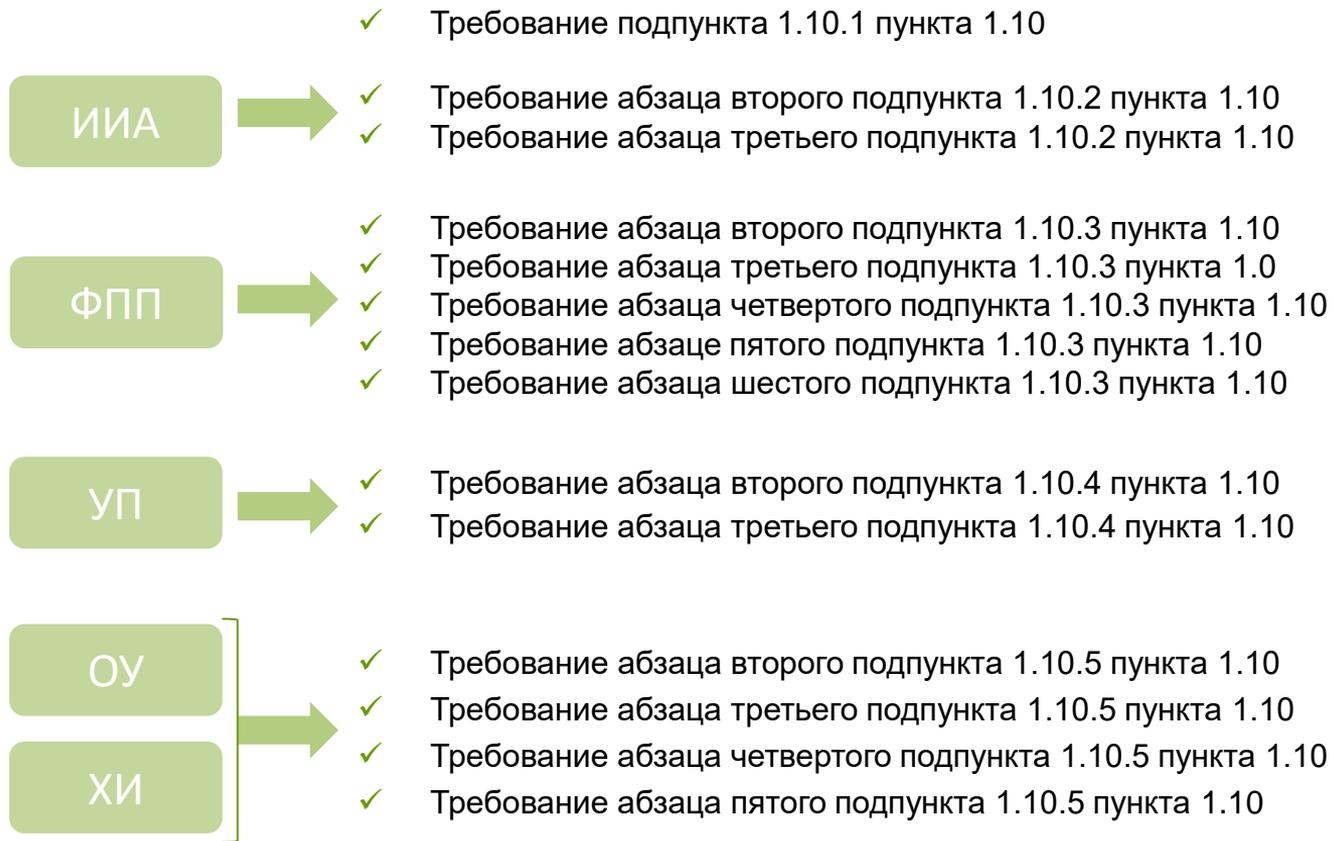
# Новое в методологии. Методика 12-МР (8-МР)

## Оценка мер защиты информации



$$E_{ТМ} = 0,2 E_{ТМП} + 0,4 E_{ТМР} + 0,25 E_{ТМК} + 0,15 E_{ТМС}$$

# Оценка требований Положения 757-П (8-МР)



→ 14 требований по 8 направлениям

+ 6 требований для операторов финансовых платформ (ведется ЦБ, входит 9 операторов)

+ 11 требований для операторов информационных систем, в которых осуществляется выпуск цифровых финансовых активов, операторов обмена цифровых финансовых активов (реестр ведет ЦБ, входит 11 операторов)

# Новое в методологии. Методика 12-МР и 8-МР

Положение 802-П

12 требований (всего 96 проверок)

Положение 683-П

15 требований (всего 120 проверок)

Положение 757-П

14 требований (всего 112 проверок)  
ОИС: + 11 требований (88 проверок)  
ОФП: + 6 требований (48 проверок)

Положение 719-П (821-П)

ОПДС: 8 требований (всего 64 проверки)  
РЦ: 13 требований (104 проверки)  
ОЦ: 6 требований (48 проверок)  
ПКЦ: 30 требований (240 проверок)



Дополнительных проверок для кредитной организации:  
не менее 49 требований (392 проверки)

Для информации:  
В ГОСТ Р 57580.1-2017 проверяется 606 мер для «Усиленного уровня» и 542 меры для «Стандартного уровня»

# Оценка соответствия и Положения Банка России 716-П

Приложение 1 к Положению Банка России от 8 апреля 2020 года № 716-П «О требованиях к системе управления операционным риском в кредитной организации и банковской группе» (в актуальной редакции) устанавливает следующие КПУР информационной безопасности:

	Сигнальное значение	Контрольное значение	Текущее значение
✓ оценка соответствия уровню ЗИ в отношении процесса 1 «Обеспечение защиты информации при управлении доступом»	0,9	0,85	
✓ оценка соответствия уровню ЗИ в отношении процесса 5 «Предотвращение утечек информации»	0,9	0,85	
✓ оценка выполнения Положений 719-П, 683-П, 747-П в части требований к защите объектов информационной инфраструктуры по ГОСТ Р 57580.2-2018			

# Обобщенные результаты оценки соответствия

## Основания для проведения оценки соответствия требованиям ГОСТ Р 57580.1-2017 за 2021-2023гг

45%

Положение 683-П

53%

Положение 802- П  
(747-П)

37%

Положение 757-П  
(684-П)

80%

Положение 719-П  
(821-П)

23%

Приказ 453  
(930, 321)  
Минцифры

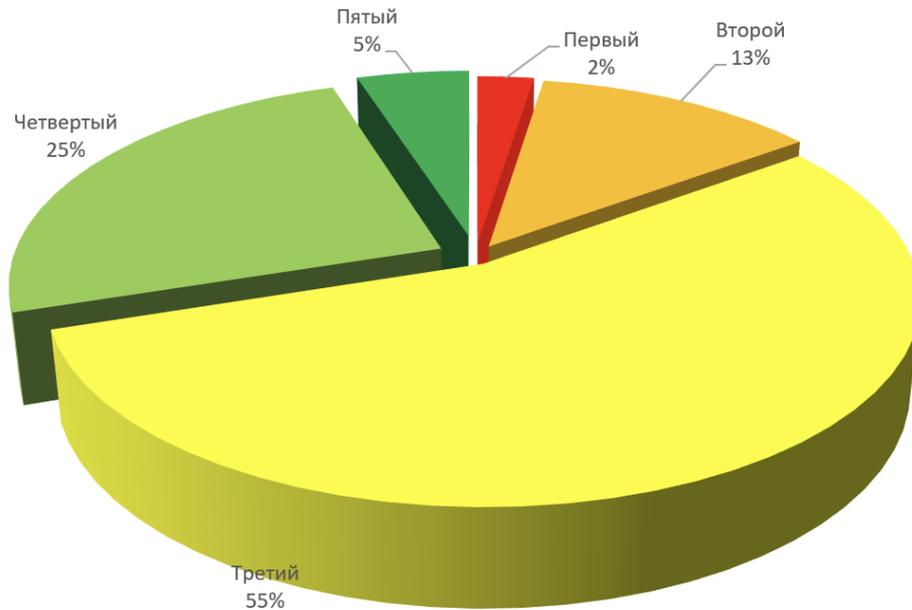
- 53% Рассматривался 1 нормативный документ для формирования контуров оценки
- 6% Рассматривалось 2 нормативных документа для формирования контуров оценки
- 32% Рассматривалось 3 нормативных документа для формирования контуров оценки
- 6% Рассматривалось 4 нормативных документа для формирования контуров оценки
- 3% Рассматривалось 5 нормативных документов для формирования контуров оценки

Рассматриваемый уровень защиты в соответствии с  
ГОСТ Р 57580.1-2017



# Обобщенные результаты оценки соответствия

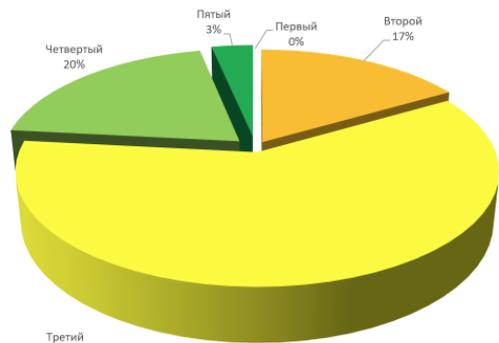
2022-2023



Уровень соответствия E

■ Первый ■ Второй ■ Третий ■ Четвертый ■ Пятый

2020-2021

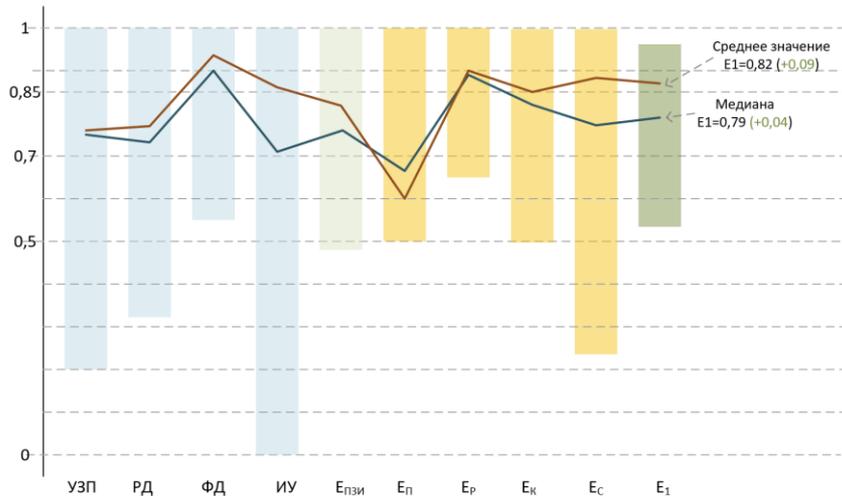


Уровень соответствия E

■ Первый ■ Второй ■ Третий ■ Четвертый ■ Пятый

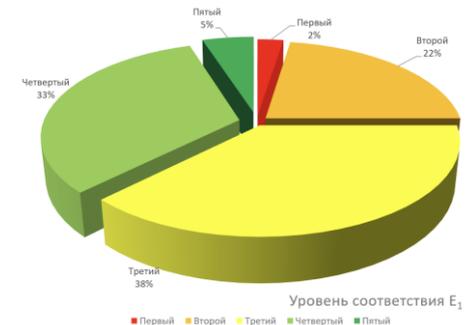
# Результаты оценки соответствия по направлениям

## Процесс 1 «Обеспечение защиты информации при управлении доступом»



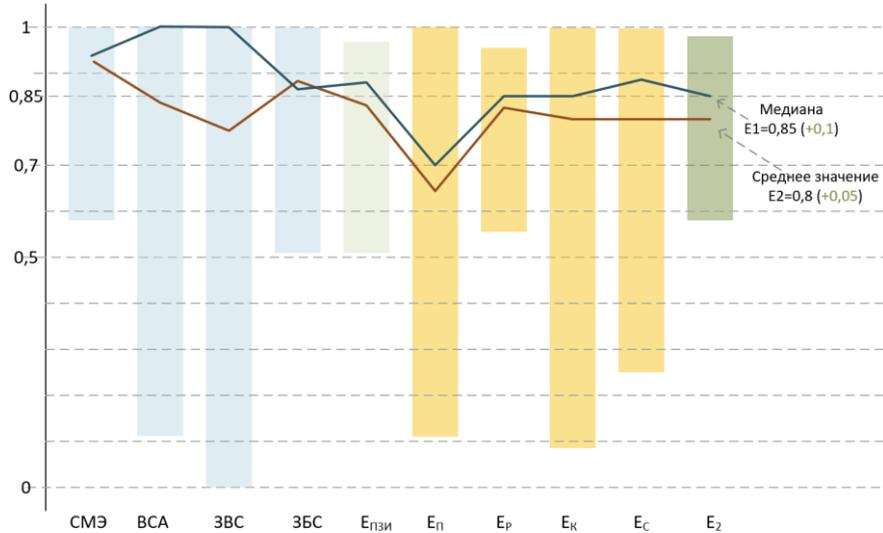
### Топ 5 часто встречающихся несоответствий:

- ✓ 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



# Результаты оценки соответствия по направлениям

## Процесс 2 «Обеспечение защиты вычислительных сетей»



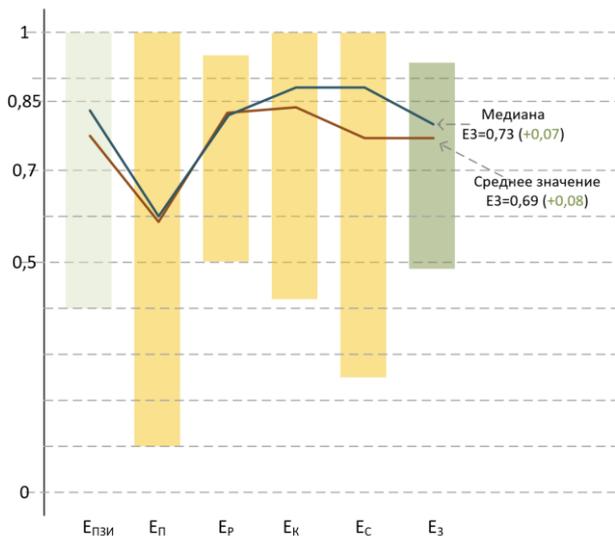
### Топ 5 часто встречающихся несоответствий:

- ✓ 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



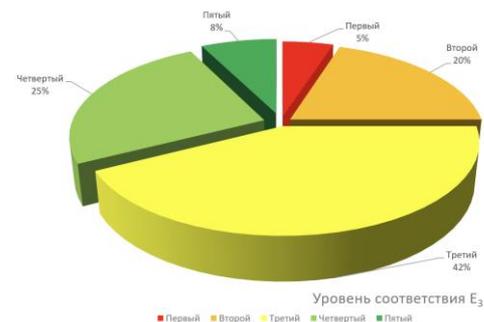
# Результаты оценки соответствия по направлениям

## Процесс 3 «Контроль целостности и защищенности информационной инфраструктуры»



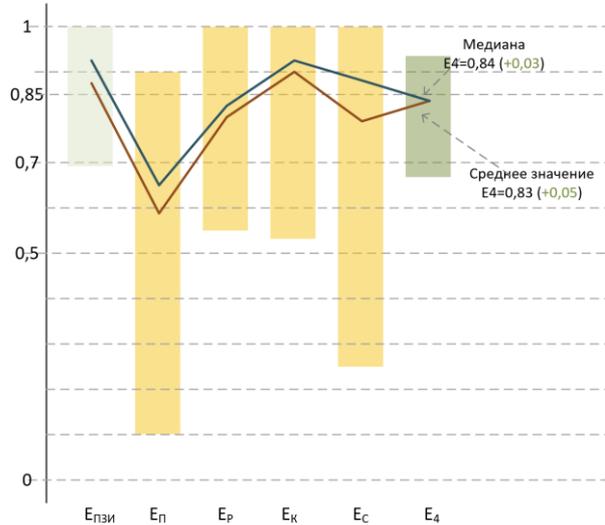
**Топ** часто встречающихся несоответствий:

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



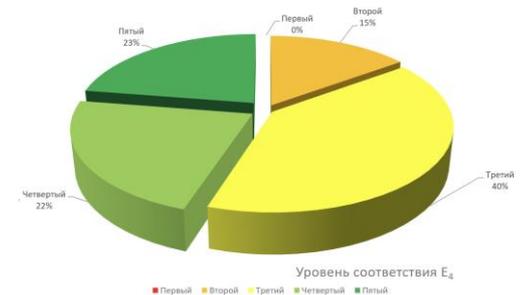
# Результаты оценки соответствия по направлениям

## Процесс 4 «Защита от вредоносного кода»



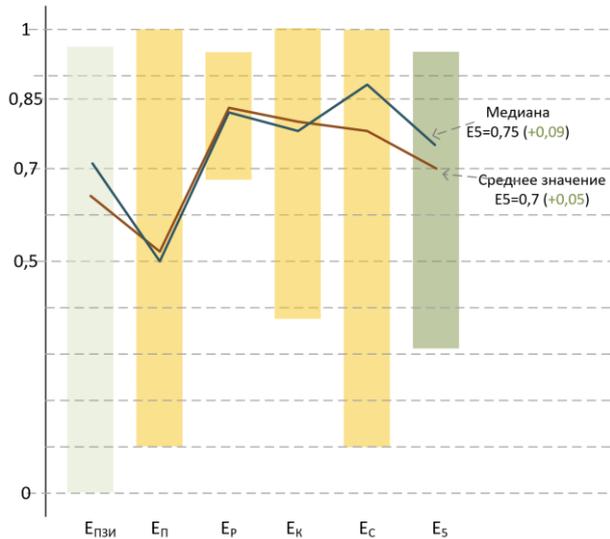
### Топ 5 часто встречающихся несоответствий:

- ✓ 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



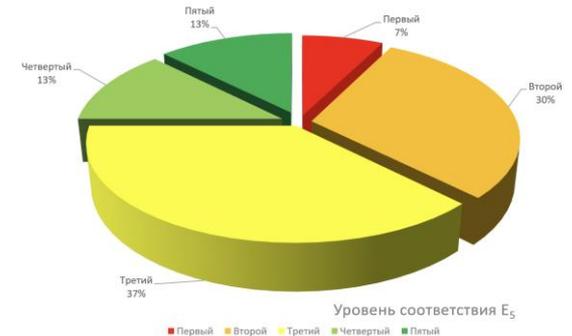
# Результаты оценки соответствия по направлениям

## Процесс 5 «Предотвращение утечек информации»



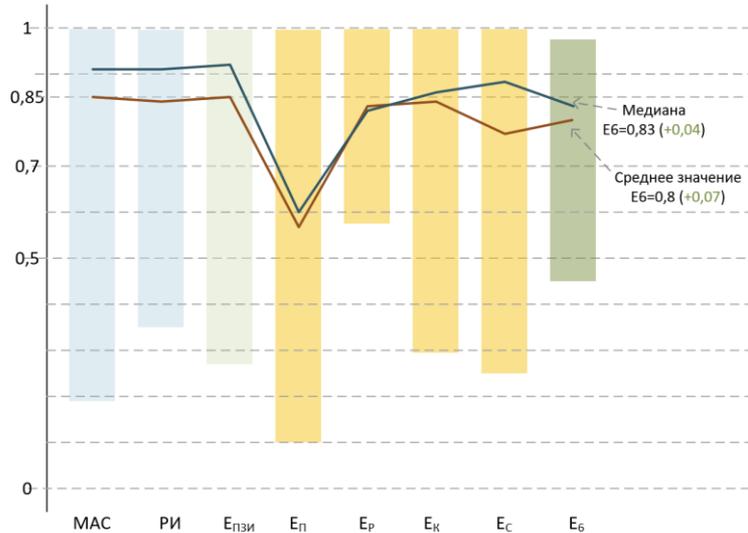
**Топ** часто встречающихся несоответствий:

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



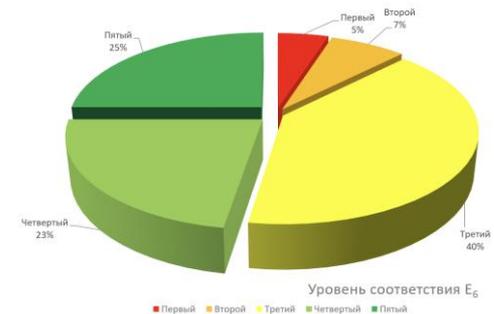
# Результаты оценки соответствия по направлениям

## Процесс 6 «Управление инцидентами защиты информации»



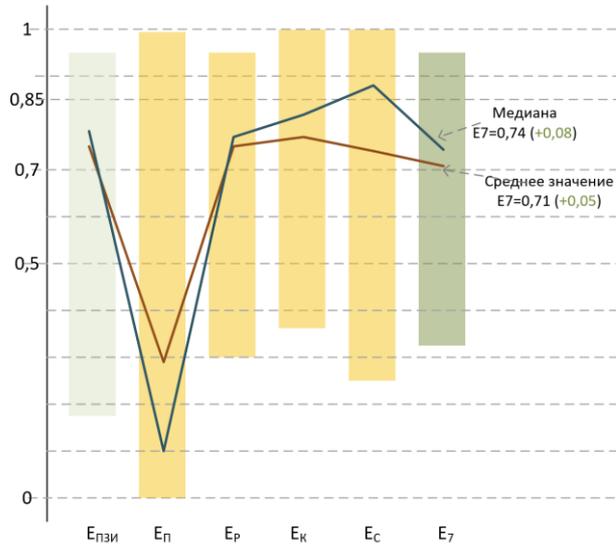
**Топ 5** часто встречающихся несоответствий:

- ✓ 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



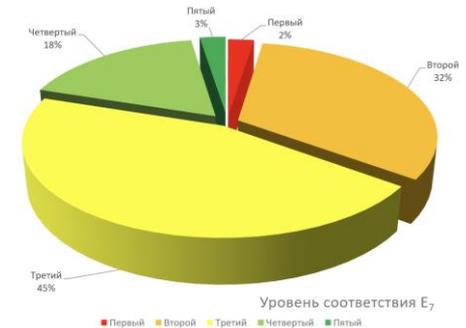
# Результаты оценки соответствия по направлениям

## Процесс 7 «Защита среды виртуализации»



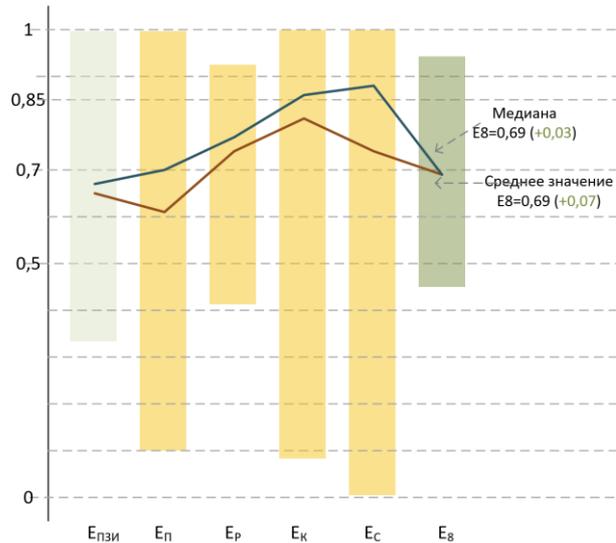
**Топ** часто встречающихся несоответствий:

- ✓ ЗСВ.6 – «один логин – один виртуальный АРМ»
- ✓ ЗСВ.9 – двухфакторная аутентификация
- ✓ ЗСВ.11 – разделение ролей
- ✓ ЗСВ.35 - протоколирование



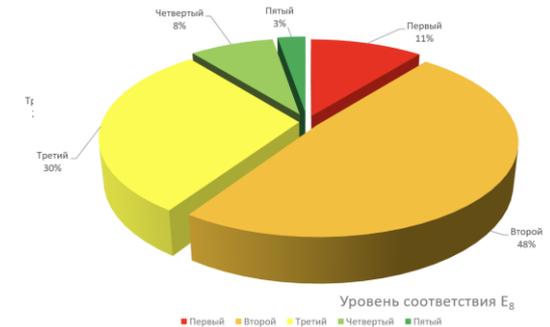
# Результаты оценки соответствия по направлениям

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



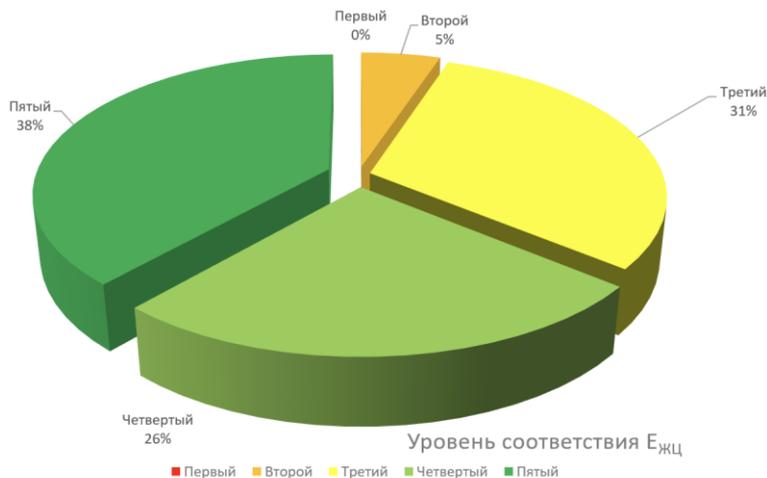
**Топ** часто встречающихся несоответствий:

- ✓ ЗУД.2 – Аутентификация устройств (мобильных/переносных)
- ✓ 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)

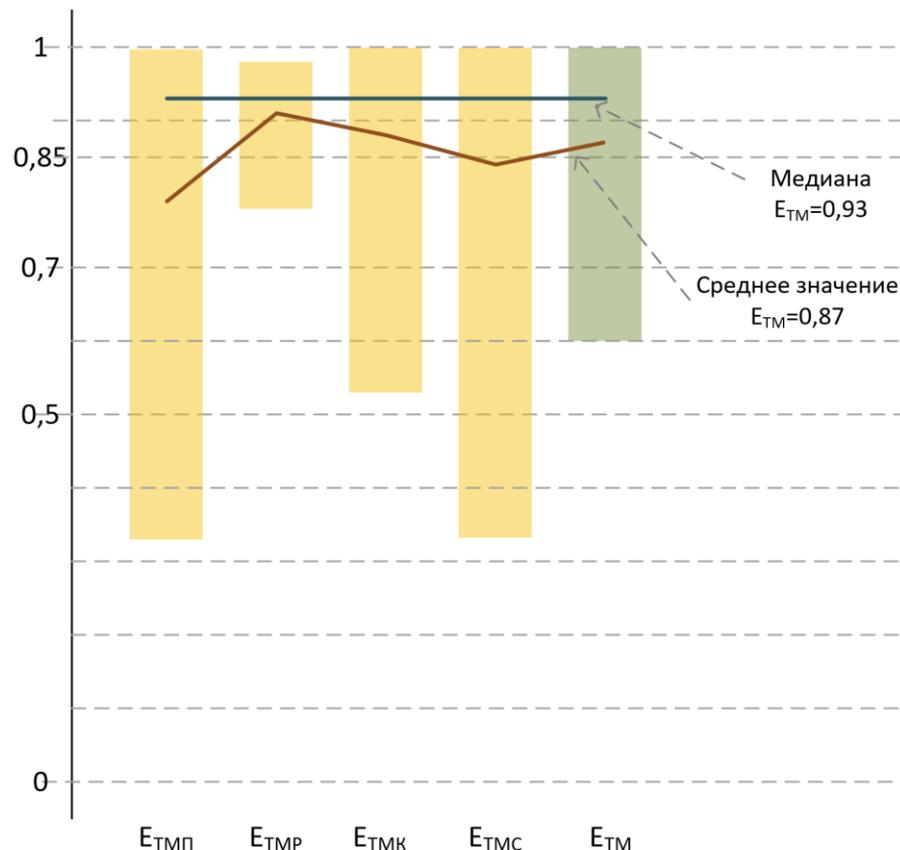
# Результаты оценки соответствия

## 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)



# 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





## ✓ Стандартизация информационной безопасности

Требования



### Регистрация событий защиты информации

Необходимо выполнить настройки в файле конфигурации `/etc/.../config/opensearch.yml`:

```
plugins.security.audit.type: internal_opensearch
plugins.security.audit.enable_rest: true
plugins.security.audit.enable_transport: true
plugins.security.audit.ignore_users: NONE
```

Убедитесь, что в файле `/etc/.../audit.yml` установлены следующие параметры:

```
config:
  enable: true
  audit:
    enable_rest: true
    enable_transport: true
    disabled_transport_categories: NONE
    ignore_users: NONE
  compliance:
    enabled: true
    internal_config: true
    write_ignore_users: NONE
```



Автоматизация



```
# Check audit.yml for required settings
describe yaml('/etc/...-security/audit.yml') do
  its(['config', 'enable']) { should eq true }
  its(['config', 'audit', 'enable_rest']) { should eq true }
  its(['config', 'audit', 'enable_transport']) { should eq true }
  its(['config', 'audit', 'disabled_transport_categories']) { should eq 'NONE' }
  its(['config', 'audit', 'ignore_users']) { should eq 'NONE' }
  its(['config', 'compliance', 'enabled']) { should eq true }
  its(['config', 'compliance', 'internal_config']) { should eq true }
  its(['config', 'compliance', 'write_ignore_users']) { should eq 'NONE' }
end

# Check for required files to be monitored

describe file('/etc/.../config.yml') do
  it { should exist }
end

...
describe file('/etc/opensearch/opensearch-security/audit.yml') do
  it { should exist }
end
end
```

## ✓ Большие языковые модели

Требования

### Регистрация событий защиты информации:

- Доступ пользователей;
- Изменение в перечне пользователей

### Промт:

Должен проверить настройки логирования событий безопасности в FreeBSD 14.0.

Какие команды надо выполнить чтобы проверить:

1. регистрацию событий доступа пользователей.
2. регистрацию изменений в перечень пользователей

Проверка

```
Для проверки настроек логирования (логирование) событий безопасности в FreeBSD 14.0, связанных с регистрацией событий доступа пользователей и регистрацией изменений в перечне пользователей, можно использовать утилиту "audit". Она позволяет контролировать и анализировать события безопасности.
```

```
1. Для проверки регистрации событий доступа пользователей:
Необходимо проверить конфигурацию аудита для пользовательских сессий. Для этого надо проверить файл конфигурации "/etc/security/audit_control".
Выполните следующую команду, чтобы просмотреть настройки аудита:
```

```
sh
cat /etc/security/audit_control
```

Обратите внимание на ключ "Flags", в котором должны быть указаны события, связанные с доступом пользователей (например, "lo", "ea"). Вы можете отредактировать этот файл, чтобы убедиться, что все необходимые события регистрируются.

```
2. Для проверки регистрации изменений в перечне пользователей:
Нужно, чтобы аудиторная система записывала события, связанные с изменением системных файлов, таких как "/etc/passwd", "/etc/group" и других файлов конфигурации пользователей. Эти события обычно именуются как "fa" (Вс по умолчанию).
Просмотрите файл конфигурации аудита "/etc/security/audit_control":
```

```
sh
cat /etc/security/audit_control
```

Убедитесь, что в ключе "Flags" присутствуют необходимые метки, например:

```
flags:fa
```

Вы также можете просмотреть текущие события аудита, чтобы проверить, что они действительно регистрируются:

```
sh
auditreduce -u AUE_USER | gaudit
```

Эта команда извлекает и форматирует записи аудита, связанные с событиями изменения пользователей.

Постоянное улучшение процесса (Kaizen)

---

**Спасибо за внимание!**  
**Вопросы?**

АО «ДиалогНаука»

Телефон: +7 (495) 980-67-76

Факс: +7 (495) 980-67-75

E-mail: Svintsitskii@dialognauka.ru

<http://www.DialogNauka.ru>