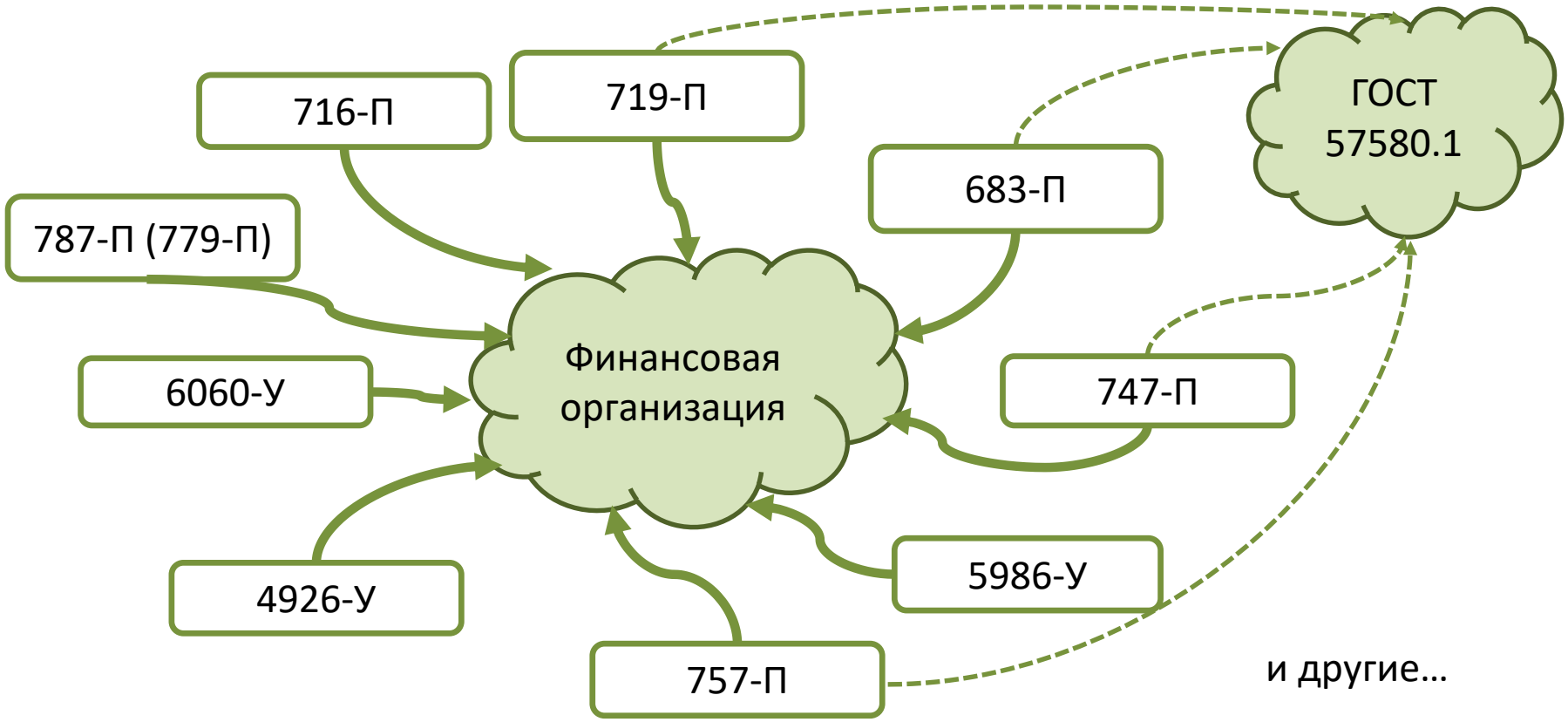
ОБЗОР ПОЛОЖЕНИЙ БАНКА РОССИИ ПО ЗАЩИТЕ ИНФОРМАЦИИ

Антон Свинцицкий
Директор по консалтингу
АО «ДиалогНаука»

17 мая 2022 года, Москва

ДиалогНаука

Нормативные требования по защите информации



Нормативные требования. Где мы сейчас находимся?

01.01.2020
Необходимость сертификации прикладного ПО АС

01.01.2021
1. Необходимость выполнения требований ГОСТ Р 57580.1-2017
2. Уровень не ниже 3 для КО
3. Проведение тестирований на проникновение
4. Проведение оценки соответствия

25.02.2021
Вступило в силу 747-П

01.07.2021
Дополнительные требования 747-П

02.07.2021
Вступило в силу 757-П

01.01.2022
Необходимость обеспечения не ниже 3 уровня соответствия ГОСТ Р 57580.1-2017 для НФО
Вступает в силу 719-П (уровень соответствия не ниже 4!!!)
Дополнительные требования 747-П
Требования 757-П
Готовность к 716-П

01.07.2022
Дополнительные требования 747-П
Дополнительные требования 757-П

01.10.2022
Вступает в силу Положение 787-П
Вступают в силу изменения в части формы отчетности 0409071

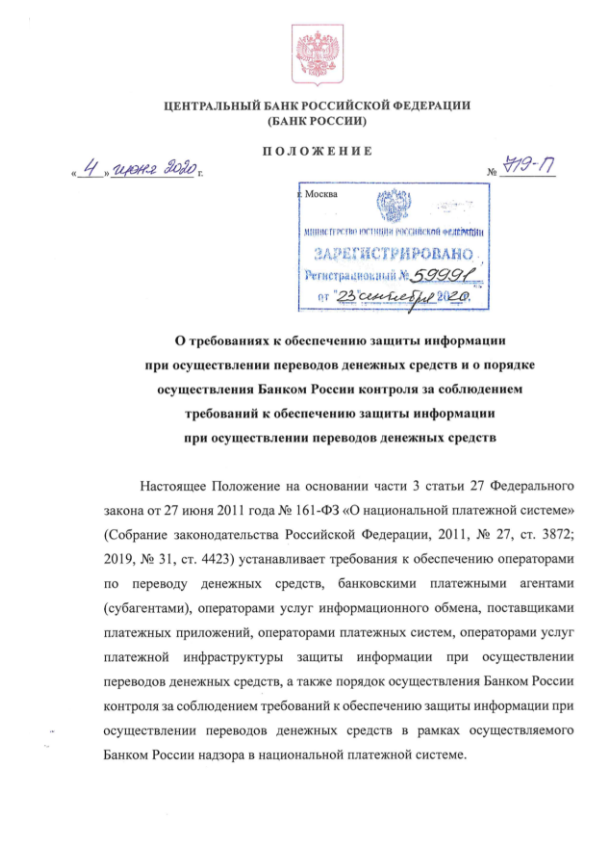
01.01.2023
Необходимость обеспечения не ниже 4 уровня соответствия ГОСТ Р 57580.1-2017 для КО
Дополнительные требования 747-П

Вступают в силу изменения в части формы отчетности 0403202

01.07.2023
Необходимость обеспечения не ниже 4 уровня соответствия ГОСТ Р 57580.1-2017 для НФО
Дополнительные требования 757-П

01.01.2024
Дополнительные требования 757-П
Дополнительные требования 719-П

Положение Банка России 719-П



ЦЕНТРАЛЬНЫЙ БАНК РОССИЙСКОЙ ФЕДЕРАЦИИ
(БАНК РОССИИ)

ПОЛОЖЕНИЕ

«4» июня 2020 г. № 719-П

г. Москва

МИНИСТЕРСТВО ЮСТИЦИИ РОССИЙСКОЙ ФЕДЕРАЦИИ
ЗАРЕГИСТРИРОВАНО
Регистрационный № 59991
от 23 сентября 2020

О требованиях к обеспечению защиты информации при осуществлении переводов денежных средств и о порядке осуществления Банком России контроля за соблюдением требований к обеспечению защиты информации при осуществлении переводов денежных средств

Настоящее Положение на основании части 3 статьи 27 Федерального закона от 27 июня 2011 года № 161-ФЗ «О национальной платежной системе» (Собрание законодательства Российской Федерации, 2011, № 27, ст. 3872; 2019, № 31, ст. 4423) устанавливает требования к обеспечению операторами по переводу денежных средств, банковскими платежными агентами (субагентами), операторами услуг информационного обмена, поставщиками платежных приложений, операторами платежных систем, операторами услуг платежной инфраструктуры защиты информации при осуществлении переводов денежных средств, а также порядок осуществления Банком России контроля за соблюдением требований к обеспечению защиты информации при осуществлении переводов денежных средств в рамках осуществляемого Банком России надзора в национальной платежной системе.

23.09.2020
Зарегистрировано

01.01.2022
Вступает в силу
(за исключением отдельных пунктов по СКЗИ)

Утрачивает силу:
Положение Банка России 382-П

Положение Банка России 719-П

Федеральный закон № 161-ФЗ «О национальной платежной системе»

Субъекты НПС

(в рамках Положения Банка России 382-П):

- ✓ Операторы по переводу денежных средств (ОПДС)
- ✓ Банковские платежные агенты (субагенты) (БПА)
- ✓ Операторы платежных систем (ОПС)
- ✓ Операторы услуг платежной инфраструктуры (ОУПИ):
  - ✓ Операционный центр (ОЦ)
  - ✓ Платежный клиринговый центр (ПКЦ)
  - ✓ Расчетный центр (РЦ)

Субъекты НПС

(в рамках Положения Банка России 719-П):

- ✓ Операторы по переводу денежных средств (ОПДС)
- ✓ Операторы платежных систем (ОПС)
- ✓ Операторы услуг платежной инфраструктуры (ОУПИ):
  - ✓ Операционный центр (ОЦ)
  - ✓ Платежный клиринговый центр (КЦ)
  - ✓ Расчетный центр (РЦ)
- ✓ Банковские платежные агенты (субагенты) (БПА)
- ✓ **Оператор услуг информационного обмена (ОУИО)**
- ✓ **Поставщик платежных приложений (ППП)**

Положение Банка России 719-П

Федеральный закон № 161-ФЗ «О национальной платежной системе»

Субъекты НПС

(в рамках Положения Банка России 382-П):

- ✓ Операторы по переводу денежных средств (ОПДС)
- ✓ Банковские платежные агенты (субагенты) (БПА)
- ✓ Операторы платежных систем (ОПС)
- ✓ Операторы услуг платежной инфраструктуры (ОУПИ):
  - ✓ Операционный центр (ОЦ)
  - ✓ Платежный клиринговый центр (ПКЦ)
  - ✓ Расчетный центр (РЦ)

Субъекты НПС

(в рамках Положения Банка России 719-П):

- ✓ Операторы по переводу денежных средств (ОПДС)
- ✓ Операторы платежных систем (ОПС)
- ✓ Операторы услуг платежной инфраструктуры (ОУПИ):
  - ✓ Операционный центр (ОЦ)
  - ✓ Платежный клиринговый центр (КЦ)
  - ✓ Расчетный центр (РЦ)
- ✓ Банковские платежные агенты (субагенты) (БПА)
- ✓ **Оператор услуг информационного обмена (ОУИО)**
- ✓ **Поставщик платежных приложений (ППП)**

Положение Банка России 719-П

Подход к формированию требований по защите информации:

1. **Требования к ИТ-инфраструктуре, задействованной при осуществлении переводов денежных средств**:
   - ✓ Выполнение требований ГОСТ Р 57580.1-2017
   - ✓ Оценка соответствия на периодической основе

2. **Требования к прикладному программному обеспечению автоматизированных систем и приложений**:
   - ✓ Сертификация **или(?)** оценка соответствия по ОУД 4

3. **Требования организационного характера**:
   - ✓ Проведение тестирования на проникновение
   - ✓ Информирование об инцидентах
   - ✓ Защита ПДн
   - ✓ Использование СКЗИ
   - ✓ Валидация email адресов

4. **Требования к реализации функций защиты информации на технологических участках выполнения операций по переводу денежных средств**:
   - ✓ Идентификация, аутентификация и авторизация клиентов ОПДС (ИАА)
   - ✓ Формирование (подготовка), передача и прием ЭС (ФПП)
   - ✓ Удостоверение права клиентов ОПДС распоряжаться денежными средствами (УП)
   - ✓ Осуществление операций и учет результатов осуществление переводов денежных средств (ОУ)
   - ✓ Хранение ЭС и информации об осуществлённых переводах денежных средств (ХИ)

Положение Банка России 719-П

Требования к ИТ-инфраструктуре, задействованной при осуществлении переводов денежных средств

Категория субъектов НПС	Уровень защиты информации в соответствии с ГОСТ Р 57580.1-2017		
	Минимальный	Стандартный	Усиленный
Операторы по переводу денежных средств (ОПДС)		+	+ Для системно значимых КО
Банковские платежные агенты (субагенты) (БПА)	+		
Оператор услуг информационного обмена (ОУИО)		+	
Поставщик платежных приложений (ППП)			
Операторы платежных систем (ОПС)			
Операторы услуг платежной инфраструктуры (ОУПИ)		+	+ Для системно значимых ПС

Положение Банка России 719-П

Требования к прикладному программному обеспечению автоматизированных систем и приложений

Категория субъектов НПС	Способ реализации требований для отдельных типов автоматизированных систем и приложений	
	Сертификация	Оценка соответствия по ОУД 4
Операторы по переводу денежных средств (ОПДС)	Не ниже 4 уровня доверия для системно значимых КО и КО, признанных значимыми на рынке платежных услуг Не ниже 5 уровня для остальных КО	+
Банковские платежные агенты (субагенты) (БПА)	Не ниже 6 уровня доверия	+
Оператор услуг информационного обмена (ОУИО)	Не ниже 5 уровня доверия	+
Поставщик платежных приложений (ППП) и Операторы платежных систем (ОПС)		
Операторы услуг платежной инфраструктуры (ОУПИ)	Не ниже 4 уровня доверия в случае выполнения требований ГОСТ Р 57580.1 по усиленному уровню защиты Не ниже 5 уровня в иных случаях	+

Положение Банка России 719-П

Категория субъектов НПС	Другие требования Положения 719-П			
	Защита ПДн	Использование СКЗИ в соответствии с требованиями законодательства РФ	Тестирование на проникновение (на ежегодной основе)	Информирование Банка России об инцидентах
Операторы по переводу денежных средств (ОПДС)	+	+	+	+
Банковские платежные агенты (субагенты) (БПА)	+	+	+ На основе критериев определяемых ОПДС	
Оператор услуг информационного обмена (ОУИО)	+	+	+	
Поставщик платежных приложений (ППП)	+			
Операторы платежных систем (ОПС)	+	+		
Операторы услуг платежной инфраструктуры (ОУПИ)	+	+	+	+

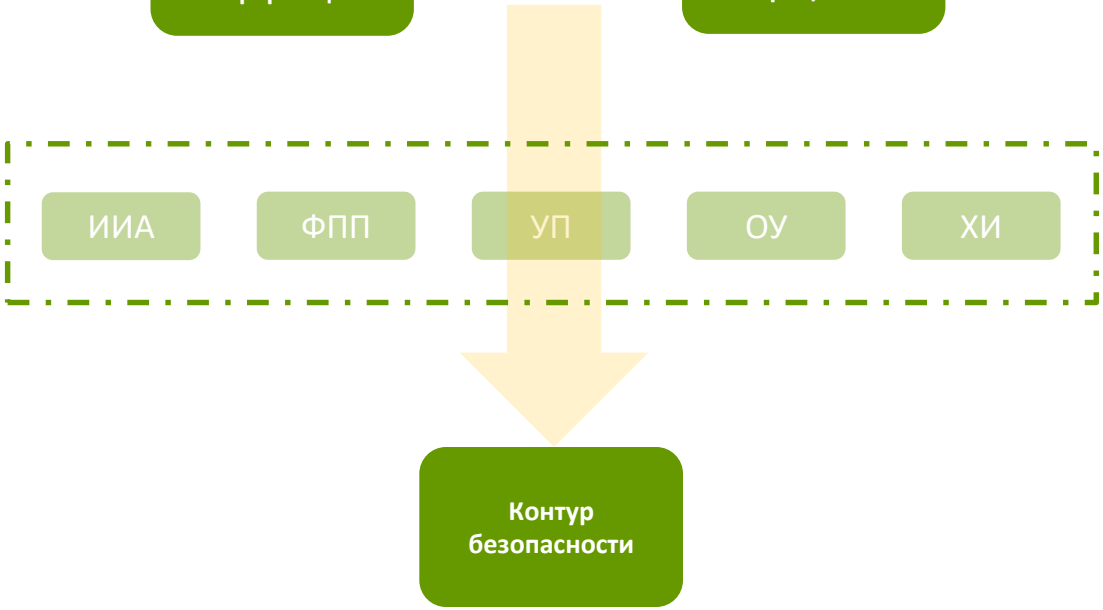
Контуры безопасности

- ✓ п.1 Положения 683-П
- ✓ п.2.1, п.2.2 Положения 719-П
- ✓ Приложение 2 к Положению 719-П

Типы защищаемой информации

Банковские технологические процессы

- ✓ Перечень процессов
- ✓ Владельцы процессов
- ✓ АС, реализующие процессы



Контуры безопасности. Вариант 1

- ✓ п.1 Положения 683-П
- ✓ п.2.1, п.2.2 Положения 719-П
- ✓ Приложение 2 к Положению 719-П

Типы защищаемой информации

Банковские технологические процессы

- ✓ Перечень процессов
- ✓ Владельцы процессов
- ✓ АС, реализующие процессы

- ✓ ССНП
- ✓ СБП

объект информатизации

- ✓ АРМ пользователей
- ✓ Серверное оборудование
- ✓ Сетевое оборудование
- ✓ СХД
- ✓ HSM
- ✓ Принтеры и копиры
- ✓ ТУ ДБО

объект доступа

ресурс доступа

- ✓ АС
- ✓ БД
- ✓ Сетевые ресурсы
- ✓ Виртуальные машины
- ✓ Сервисы (электронная почта, WEB)

Физический доступ

Логический доступ

субъект доступа

- ✓ Пользователь
- ✓ Клиент
- ✓ Эксплуатационный персонал
- ✓ Технический персонал
- ✓ Программный сервис

Контуры безопасности. Вариант 2

Нормативные требования	Уровень обработки информации	Тип автоматизированных систем
Положение 747-П	✓ Уровень взаимодействия с клиентами (ФЛ) ✓ Уровень взаимодействия с клиентами (ЮЛ) ✓ Обработка ЭС в кредитной организации ✓ Работы с карточными данными	✓ Системы ДБО, устанавливаемые на АРМ клиентов ✓ Системы ДБО, доступ к которым предоставляется через WEB интерфейс ✓ Системы мобильного банкинга ✓ Формирование ЭС при личном обращении клиента в офис Банка
Положение 683-П	✓ Управление банкоматной сетью и ТУ ДБО ✓ Системы взаимодействия с платежными системами	✓ Система быстрых переводов ✓ Система срочных и несрочных переводов ✓ Система взаимодействия с SWIFT ✓ Платежные системы из реестра ЦБ
Положение 719-П	✓ Автоматизация функций оператора услуг платежной инфраструктуры ✓ Инфраструктура ✓ Системы защиты информации	

Реализация базовых мер или их адаптация

Базовая мера:

Шаг 1. Выбор

Шаг 2. Формализация (планирование)

Шаг 3. Реализация

Шаг 4. Контроль и совершенствование (в рамках КЗИ и СЗИ)

Шаг 5. Проверка в рамках оценки соответствия

Адаптированная мера:

Шаг 1. Обоснование адаптации базовой меры

Шаг 2. Формализация (планирование)

Шаг 3. Реализация

Шаг 4. Контроль и совершенствование (в рамках КЗИ и СЗИ) + подтверждение уровней рисков

Шаг 5. Проверка в рамках оценки соответствия

- ✓ Предоставление аудитору свидетельств адаптации
- ✓ Оценка аудитором соответствия адаптированной меры
- ✓ Оценка соответствия

ОСОБЕННОСТИ ПРОВЕДЕНИЯ ОЦЕНКИ СООТВЕТСТВИЯ ПО ГОСТ Р 57580.2-2018

Антон Свинцицкий
Директор по консалтингу
АО «ДиалогНаука»

17 мая 2022 года, Москва

ДиалогНаука

Нормативная база проведения оценки соответствия

Схема оценки

Шаг 1.

1. Определение области оценки (должна совпадать с областью применения ГОСТ Р 57580.1)

- Типы защищаемой информации в соответствии с требованиями нормативных документов
- Банковские технологические процессы
- Объекты информационной инфраструктуры

  - Уровень взаимодействия с клиентами кредитной организации (ФЛ и ЮЛ)
  - Обработка ЭС в кредитной организации
  - Работы с карточными данными
  - Управление банкоматной сетью и платежными терминалами
  - Системы взаимодействия с платежными системами (ССНП, СБП и иные ПС)
  - Автоматизация функций оператора услуг платежной инфраструктуры (РЦ, ОЦ, КЦ)
  - и другие...

  - Инфраструктура
  - Системы защиты информации
  - Объекты и ресурсы доступа (объекты информационной инфраструктуры)

Область применения требований → **Репрезентативная выборка!!!**

Схема оценки

Шаг 1.

1. Определение области оценки (должна совпадать с областью применения ГОСТ Р 57580.1)

Шаг 2.

1. Формирование перечня неоцениваемых показателей:
   - ✓ связанные с неиспользуемыми информационными технологиями (например, беспроводные сети)
   - ✓ реализация которых не является необходимой для нейтрализации актуальных угроз безопасности, определенных в модели угроз и нарушителей
   - ✓ добавление в реестр оценки компенсирующих мер

Схема оценки

Шаг 1.

1. Определение области оценки (должна совпадать с областью применения ГОСТ Р 57580.1)

Шаг 2.

1. Формирование перечня неоцениваемых показателей:
   - ✓ связанные с неиспользуемыми информационными технологиями (например, беспроводные сети)
   - ✓ реализация которых не является необходимой для нейтрализации актуальных угроз безопасности, определенных в модели угроз и нарушителей
   - ✓ добавление в реестр оценки компенсирующих мер

методика проверки модели угроз?

Схема оценки

Шаг 1.

1. Определение области оценки (должна совпадать с областью применения ГОСТ Р 57580.1)

Шаг 2.

1. Формирование перечня неоцениваемых показателей:
   - ✓ связанные с неиспользуемыми информационными технологиями (например, беспроводные сети)
   - ✓ реализация которых не является необходимой для нейтрализации актуальных угроз безопасности, определенных в модели угроз и нарушителей
   - ✓ добавление в реестр оценки компенсирующих мер

методика проверки модели угроз?

как оценить полноту компенсирующих мер?

Схема оценки

Шаг 3.

1. Сбор информации и свидетельств выполнения (реализации) мер:

- ✓ документы проверяемой организации и иные материалы проверяемой организации в бумажном или электронном виде (при необходимости, документы третьих лиц)
- ✓ устные высказывания сотрудников проверяемой организации в процессе проводимых опросов в области оценки соответствия ЗИ;
- ✓ результаты наблюдений членов проверяющей группы за процессами системы ЗИ и деятельностью сотрудников проверяемой организации в области оценки соответствия ЗИ;
- ✓ параметры конфигураций и настроек технических объектов информатизации и средств ЗИ;
- ✓ технические методы, технические и программные средства сбора свидетельств полноты реализации мер ЗИ (анализ электронных журналов регистрации, анализ фактических настроек, **анализ уязвимостей, проведение тестирования на проникновение** и т.п.)

Схема оценки

Перечень типовых тем интервью:

1 очередь:

- ✓ Организация и функционирование ИБ
- ✓ Реализация банковского платежного технологического процесса (банковских операций)
- ✓ Выполнение требований по защите информации в АС
- ✓ Обеспечение защиты вычислительных сетей
- ✓ Защита инфраструктуры

2 очередь:

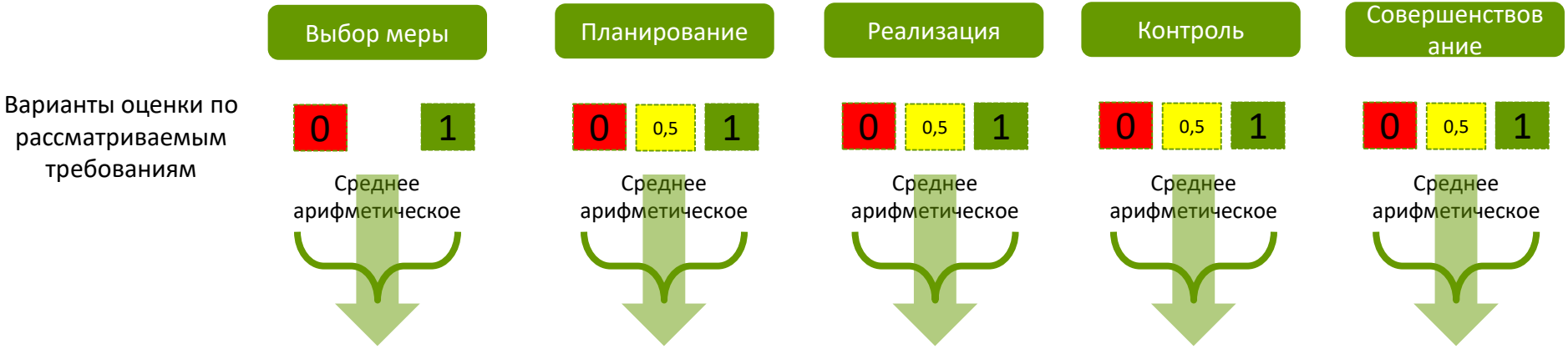
- ✓ Применяемые СЗИ
- ✓ Защита платформы виртуализации
- ✓ Управление уязвимостями
- ✓ Защита от вредоносного кода
- ✓ Управление инцидентами информационной безопасности
- ✓ Предотвращение утечек защищаемой информации
- ✓ Мониторинг и контроль состояния информационной безопасности
- ✓ …

3 очередь:

- ✓ Повышение осведомленности в области обеспечения ИБ
- ✓ Анализ и совершенствование мер защиты информации
- ✓ Защита персональных данных
- ✓ …

Методика оценки соответствия (расчет итоговых показателей)

Оценка процесса защиты информации



$$E_i = 0{,}5\ E_{\text{пзи}} + 0{,}1\ E_{\text{П}} + 0{,}2\ E_{\text{Р}} + 0{,}125\ E_{\text{К}} + 0{,}075\ E_{\text{С}}$$

Итоговая оценка $$R = \frac{E_1 + E_2 + E_3 + E_4 + E_5 + E_6 + E_7 + E_8 + E_{\text{ЖЦ}}}{9} - 0{,}01 \times Z$$

Z – количество нарушений

Методика оценки соответствия

Требования к системе защиты информации

$$\text{Е}_{\text{ПЗИ}_i} = \frac{\sum_{j=1}^{N} E_{\text{МЗИ}_j}}{N} \Rightarrow E_i = \frac{\text{Е}_{\text{ПЗИ}_i} + (0{,}2 * \text{Е}_{\text{П}_i} + 0{,}4 * \text{Е}_{\text{Р}_i} + 0{,}25 * \text{Е}_{\text{К}_i} + 0{,}15 * \text{Е}_{\text{С}_i})}{2}$$

Если в область оценки соответствия входят несколько контуров безопасности разного уровня

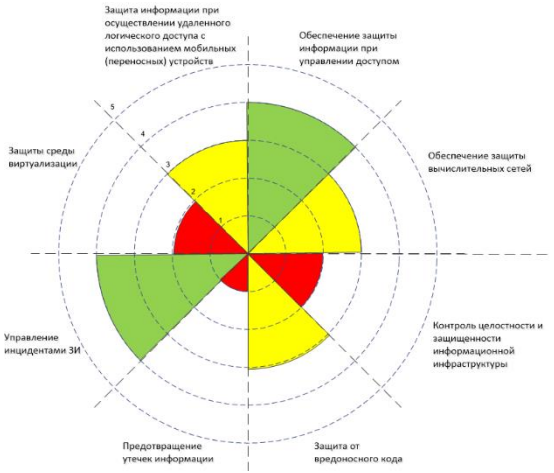
$$E_i = k_1 E_{1i} + k_2 E_{2i} + k_3 E_{3i}$$

Наличие контура заданного уровня			Корректирующий коэффициент		
3	2	1	E_{3i}	E_{2i}	E_{1i}
+	+	+	0,1	0,3	0,6
	+	+		0,3	0,7
+		+	0,2		0,8
+	+		0,4	0,6	

Интерпретация результатов оценки

Уровни соответствия	Результаты оценки E_i
Нулевой уровень соответствия	0
Первый уровень соответствия	$0 < E_i \leq 0{,}5$
Второй уровень соответствия	$0{,}5 < E_i \leq 0{,}7$
Третий уровень соответствия	$0{,}7 < E_i \leq 0{,}85$
Четвертый уровень соответствия	$0{,}85 < E_i \leq 0{,}9$
Пятый уровень соответствия	$0{,}9 < E_i$

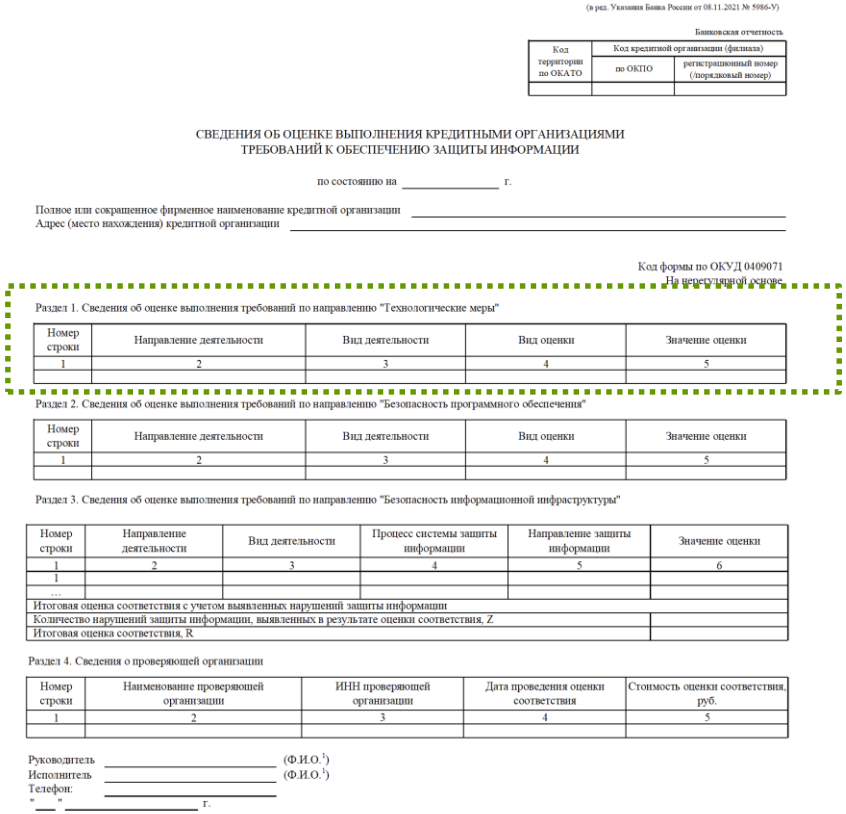
Рекомендуемый ЦБ



Итоговая оценка соответствия ЗИ ***R***

$$R = \frac{\sum_{i=1}^{T} E_i + E_{\text{AC}}}{T+1} - 0{,}01 * Z$$

Форма отчетности 0409071



(в ред. Указания Банка России от 08.11.2021 № 5986-У)

Банковская отчетность

Код территории по ОКАТО	Код кредитной организации (филиала)	
	по ОКПО	регистрационный номер (/порядковый номер)

СВЕДЕНИЯ ОБ ОЦЕНКЕ ВЫПОЛНЕНИЯ КРЕДИТНЫМИ ОРГАНИЗАЦИЯМИ ТРЕБОВАНИЙ К ОБЕСПЕЧЕНИЮ ЗАЩИТЫ ИНФОРМАЦИИ

по состоянию на _____ г.

Полное или сокращенное фирменное наименование кредитной организации _____

Адрес (место нахождения) кредитной организации _____

Код формы по ОКУД 0409071

На регулятивной основе

Раздел 1. Сведения об оценке выполнения требований по направлению "Технологические меры"

Номер строки	Направление деятельности	Вид деятельности	Вид оценки	Значение оценки
1	2	3	4	5

Раздел 2. Сведения об оценке выполнения требований по направлению "Безопасность программного обеспечения"

Номер строки	Направление деятельности	Вид деятельности	Вид оценки	Значение оценки
1	2	3	4	5

Раздел 3. Сведения об оценке выполнения требований по направлению "Безопасность информационной инфраструктуры"

Номер строки	Направление деятельности	Вид деятельности	Процесс системы защиты информации	Направление защиты информации	Значение оценки
1	2	3	4	5	6
1					
…					
Итоговая оценка соответствия с учетом выявленных нарушений защиты информации					
Количество нарушений защиты информации, выявленных в результате оценки соответствия, Z					
Итоговая оценка соответствия, R					

Раздел 4. Сведения о проверяющей организации

Номер строки	Наименование проверяющей организации	ИНН проверяющей организации	Дата проведения оценки соответствия	Стоимость оценки соответствия, руб.
1	2	3	4	5

Руководитель _____ (Ф.И.О.[1])

Исполнитель _____ (Ф.И.О.[1])

Телефон: _____

"__" _____ г.

Направление деятельности (Оценка выполнения требований Положений Банка России):

- ✓ N 683-П
- ✓ N 719-П
- ✓ N 747-П
- ✓ N 757-П

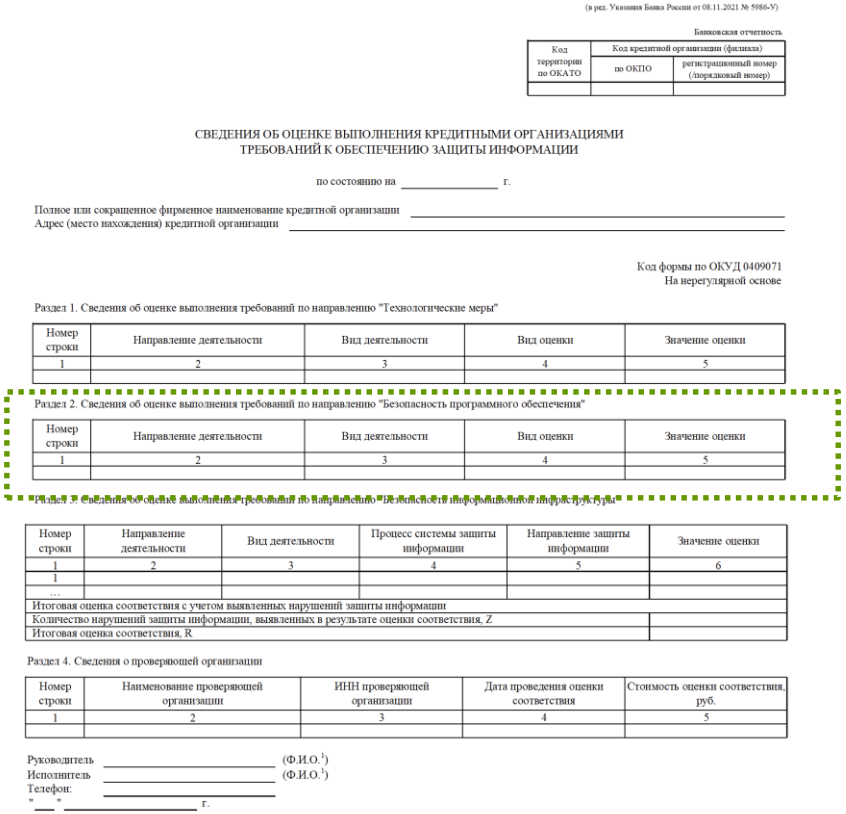
Вид деятельности:

- ✓ Банк
- ✓ ОПДС
- ✓ ОУПИ
- ✓ Участник ПС БР
- ✓ Брокер
- ✓ Депозитарий
- ✓ и другие…

Вид оценки:

- ✓ $E_{ТМП}$
- ✓ $E_{ТМР}$
- ✓ $E_{ТМК}$
- ✓ $E_{ТМС}$
- ✓ $E_{ТМ}$

Форма отчетности 0409071



(в ред. Указания Банка России от 08.11.2021 № 5986-У)

Банковская отчетность

Код территории по ОКАТО	Код кредитной организации (филиала)	
	по ОКПО	регистрационный номер (/порядковый номер)

СВЕДЕНИЯ ОБ ОЦЕНКЕ ВЫПОЛНЕНИЯ КРЕДИТНЫМИ ОРГАНИЗАЦИЯМИ ТРЕБОВАНИЙ К ОБЕСПЕЧЕНИЮ ЗАЩИТЫ ИНФОРМАЦИИ

по состоянию на _____ г.

Полное или сокращенное фирменное наименование кредитной организации _____

Адрес (место нахождения) кредитной организации _____

Код формы по ОКУД 0409071
На нерегулярной основе

Раздел 1. Сведения об оценке выполнения требований по направлению "Технологические меры"

Номер строки	Направление деятельности	Вид деятельности	Вид оценки	Значение оценки
1	2	3	4	5

Раздел 2. Сведения об оценке выполнения требований по направлению "Безопасность программного обеспечения"

Номер строки	Направление деятельности	Вид деятельности	Вид оценки	Значение оценки
1	2	3	4	5

Раздел 3. Сведения об оценке выполнения требований по направлению "Безопасность информационной инфраструктуры"

Номер строки	Направление деятельности	Вид деятельности	Процесс системы защиты информации	Направление защиты информации	Значение оценки
1	2	3	4	5	6
1					
…					
Итоговая оценка соответствия с учетом выявленных нарушений защиты информации					
Количество нарушений защиты информации, выявленных в результате оценки соответствия, Z					
Итоговая оценка соответствия, R					

Раздел 4. Сведения о проверяющей организации

Номер строки	Наименование проверяющей организации	ИНН проверяющей организации	Дата проведения оценки соответствия	Стоимость оценки соответствия, руб.
1	2	3	4	5

Руководитель _____ (Ф.И.О.[1])
Исполнитель _____ (Ф.И.О.[1])
Телефон: _____
"__" _____ г.

Направление деятельности (Оценка выполнения требований Положений Банка России):

- ✓ N 683-П
- ✓ N 719-П
- ✓ N 757-П

Вид деятельности:

- ✓ Банк
- ✓ ОПДС
- ✓ ОУПИ
- ✓ Участник ПС БР
- ✓ Брокер
- ✓ Депозитарий
- ✓ и другие…

Вид оценки:

- ✓ $E_{поп}$
- ✓ $E_{пор}$
- ✓ $E_{пок}$
- ✓ $E_{пос}$
- ✓ $E_{по}$
- ✓ ППО ОС

Форма отчетности 0409071

(в ред. Указания Банка России от 08.11.2021 № 5986-У)

Банковская отчетность

Код территории по ОКАТО	Код кредитной организации (филиала)	
	по ОКПО	регистрационный номер (/порядковый номер)

СВЕДЕНИЯ ОБ ОЦЕНКЕ ВЫПОЛНЕНИЯ КРЕДИТНЫМИ ОРГАНИЗАЦИЯМИ ТРЕБОВАНИЙ К ОБЕСПЕЧЕНИЮ ЗАЩИТЫ ИНФОРМАЦИИ

по состоянию на _____ г.

Полное или сокращенное фирменное наименование кредитной организации _____

Адрес (место нахождения) кредитной организации _____

Код формы по ОКУД 0409071
На нерегулярной основе

Раздел 1. Сведения об оценке выполнения требований по направлению "Технологические меры"

Номер строки	Направление деятельности	Вид деятельности	Вид оценки	Значение оценки
1	2	3	4	5

Раздел 2. Сведения об оценке выполнения требований по направлению "Безопасность программного обеспечения"

Номер строки	Направление деятельности	Вид деятельности	Вид оценки	Значение оценки
1	2	3	4	5

Раздел 3. Сведения об оценке выполнения требований по направлению "Безопасность информационной инфраструктуры"

Номер строки	Направление деятельности	Вид деятельности	Процесс системы защиты информации	Направление защиты информации	Значение оценки
1	2	3	4	5	6
1					
…					
Итоговая оценка соответствия с учетом выявленных нарушений защиты информации					
Количество нарушений защиты информации, выявленных в результате оценки соответствия, Z					
Итоговая оценка соответствия, R					

Раздел 4. Сведения о проверяющей организации

Номер строки	Наименование проверяющей организации	ИНН проверяющей организации	Дата проведения оценки соответствия	Стоимость оценки соответствия, руб.
1	2	3	4	5

Руководитель _____ (Ф.И.О.[1])
Исполнитель _____ (Ф.И.О.[1])
Телефон: _____
"__" _____ г.

Наименование процесса системы ЗИ, направления ЗИ	Оценка за выбор организационных и технических мер ЗИ, входящих в систему ЗИ	Оценки за направления				Качественная оценка уровня соответствия процесса системы ЗИ	Итоговая оценка за процесс системы ЗИ/Количество нарушений ЗИ/Итоговая оценка соответствия ЗИ
		Планирование процесса системы ЗИ	Реализация процесса системы ЗИ	Контроль процесса системы ЗИ	Совершенствование процесса системы ЗИ		
Процесс 1 «Обеспечение защиты информации при управлении доступом»	0,86	0,60	0,90	0,91	1,00	Четвертый	0,86
Процесс 2 «Обеспечение защиты вычислительных сетей»	0,61	0,60	0,73	0,82	1,00	Второй	0,69
Процесс 3 «Контроль целостности и защищенности информационной инфраструктуры»	0,83	0,60	0,77	0,92	1,00	Третий	0,82
Процесс 4 «Защита от вредоносного кода»	0,92	0,83	0,89	1,00	1,00	Пятый	0,92
Процесс 5 «Предотвращение утечек информации»	0,59	0,50	0,77	0,95	1,00	Второй	0,69
Процесс 6 «Управление инцидентами защиты информации»	0,95	0,70	0,82	0,95	1,00	Четвертый	0,90
Процесс 7 «Защита среды виртуализации»	0,82	0,70	0,91	1,00	1,00	Четвертый	0,86
Процесс 8 «Защита информации при осуществлении удаленного логического доступа с использованием мобильных (переносных) технических	0,67	0,70	0,73	0,96	1,00	Третий	0,75
организационных и технических мер ЗИ на этапах жизненного цикла							0,87
Итоговая оценка соответствия ЗИ с учетом выявленных нарушений ЗИ							
Количество нарушений ЗИ, выявленных в результате оценки соответствия ЗИ							
Итоговая оценка соответствия ЗИ							**0,82**

Форма отчетности 0409071

(в ред. Указания Банка России от 08.11.2021 № 5986-У)

Банковская отчетность

Код территории по ОКАТО	Код кредитной организации (филиала)	
	по ОКПО	регистрационный номер (/порядковый номер)

СВЕДЕНИЯ ОБ ОЦЕНКЕ ВЫПОЛНЕНИЯ КРЕДИТНЫМИ ОРГАНИЗАЦИЯМИ ТРЕБОВАНИЙ К ОБЕСПЕЧЕНИЮ ЗАЩИТЫ ИНФОРМАЦИИ

по состоянию на _____ г.

Полное или сокращенное фирменное наименование кредитной организации _____

Адрес (место нахождения) кредитной организации _____

Код формы по ОКУД 0409071
На нерегулярной основе

Раздел 1. Сведения об оценке выполнения требований по направлению "Технологические меры"

Номер строки	Направление деятельности	Вид деятельности	Вид оценки	Значение оценки
1	2	3	4	5

Раздел 2. Сведения об оценке выполнения требований по направлению "Безопасность программного обеспечения"

Номер строки	Направление деятельности	Вид деятельности	Вид оценки	Значение оценки
1	2	3	4	5

Раздел 3. Сведения об оценке выполнения требований по направлению "Безопасность информационной инфраструктуры"

Номер строки	Направление деятельности	Вид деятельности	Процесс системы защиты информации	Направление защиты информации	Значение оценки
1	2	3	4	5	6
1					
...					
Итоговая оценка соответствия с учетом выявленных нарушений защиты информации					
Количество нарушений защиты информации, выявленных в результате оценки соответствия, Z					
Итоговая оценка соответствия, R					

Раздел 4. Сведения о проверяющей организации

Номер строки	Наименование проверяющей организации	ИНН проверяющей организации	Дата проведения оценки соответствия	Стоимость оценки соответствия, руб.
1	2	3	4	5

Руководитель _____ (Ф.И.О.)

Исполнитель _____ (Ф.И.О.[1])

Телефон: _____

"___" _____ г.

Обобщенные результаты оценки соответствия

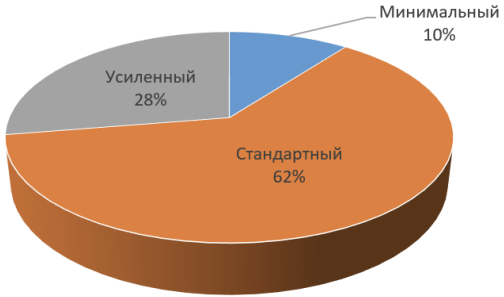
Основания для проведения оценки соответствия требованиям ГОСТ Р 57580.1-2017

38%	41%	38%	-	28%
Положение 683-П	Положение 747-П (672-П)	Положение 684-П (757-П)	Положение 719-П	Приказ 321 (930) Минцифры

25% Рассматривалось 2 нормативных документа для формирования контуров оценки

10% Рассматривалось 3 нормативных документа для формирования контуров оценки

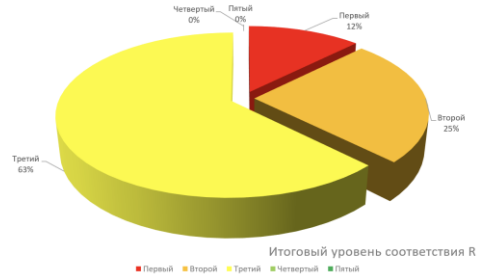
Рассматриваемый уровень защиты в соответствии с ГОСТ Р 57580.1-2017



Обобщенные результаты оценки соответствия

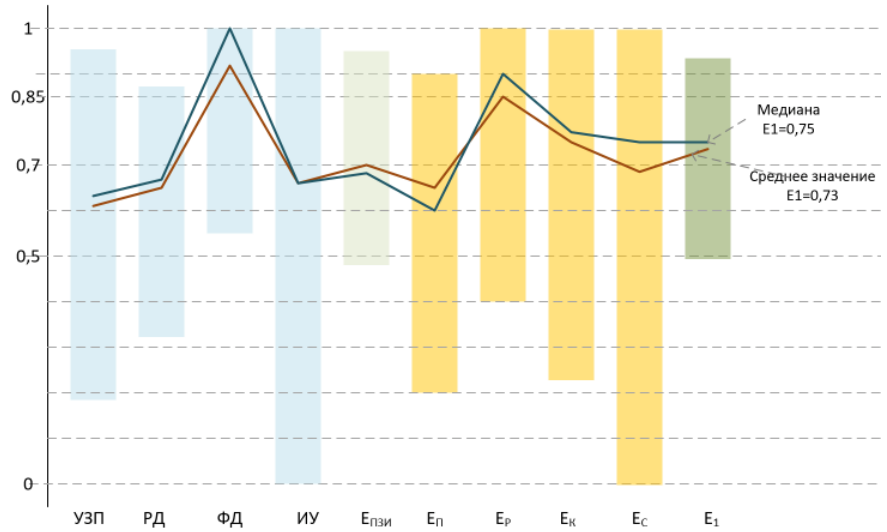
Для выбранного уровня защиты «Стандартный»

Для выбранного уровня защиты «Усиленный»



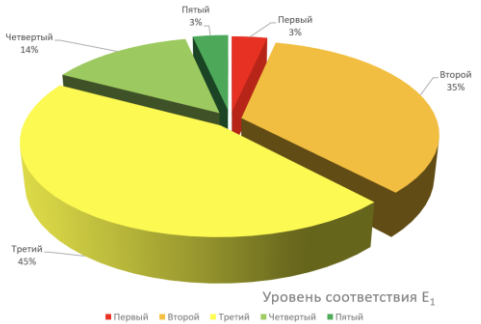
Результаты оценки соответствия по направлениям

Процесс 1 «Обеспечение защиты информации при управлении доступом»



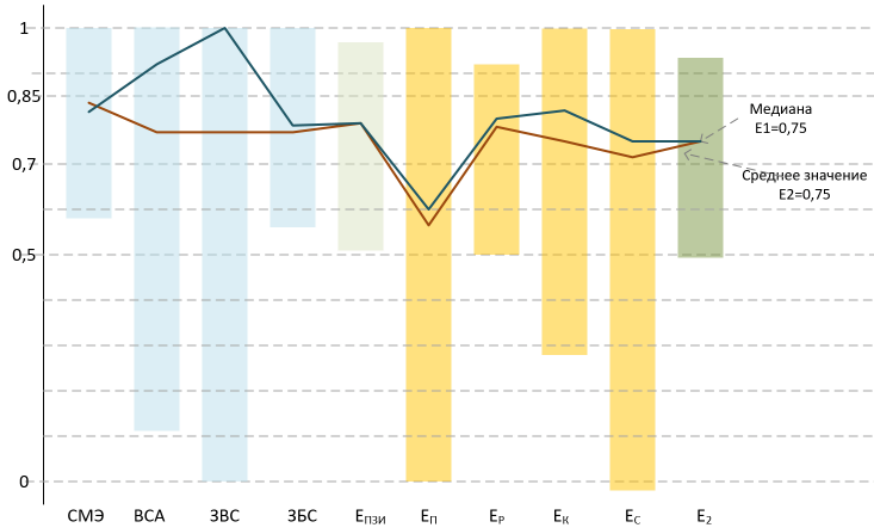
Топ 5 часто встречающихся несоответствий:

- ✓ 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



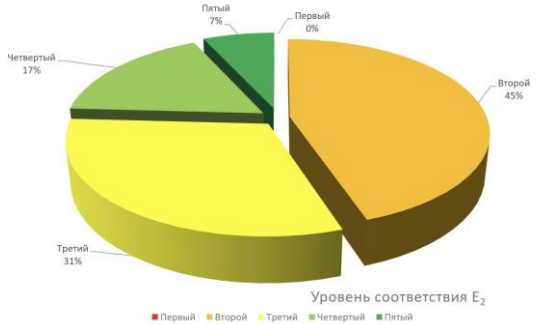
Результаты оценки соответствия по направлениям

Процесс 2 «Обеспечение защиты вычислительных сетей»



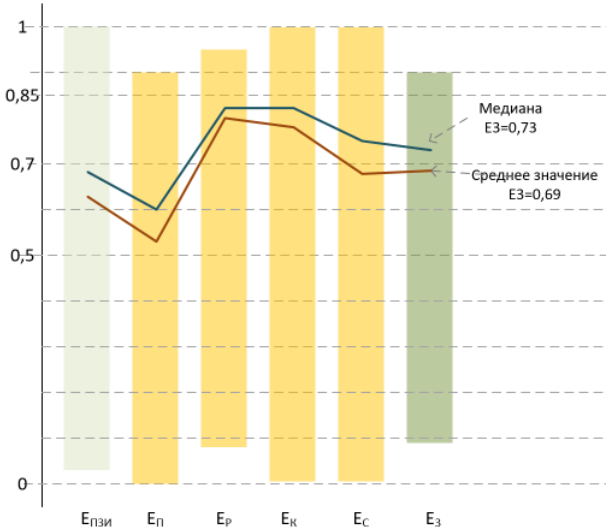
Топ 5 часто встречающихся несоответствий:

- ✓ 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



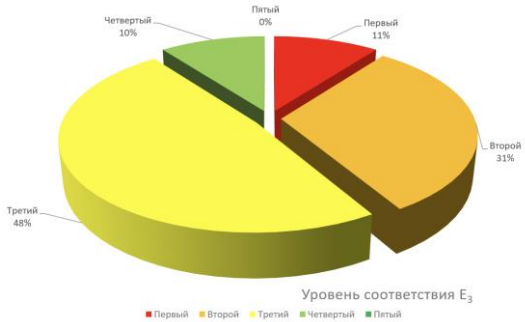
Результаты оценки соответствия по направлениям

Процесс 3 «Контроль целостности и защищенности информационной инфраструктуры»



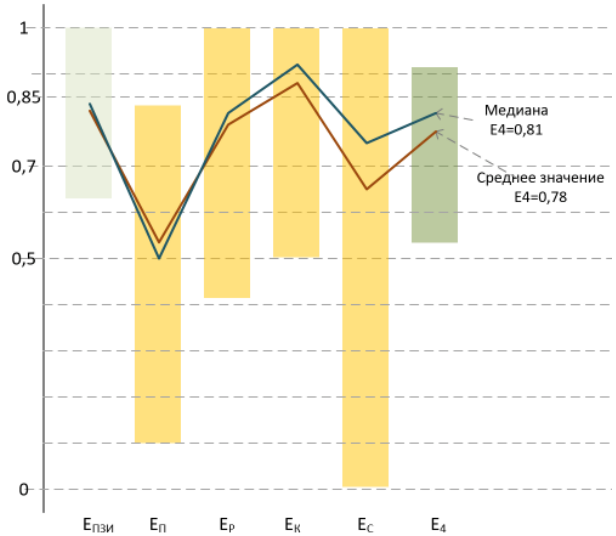
Топ часто встречающихся несоответствий:

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



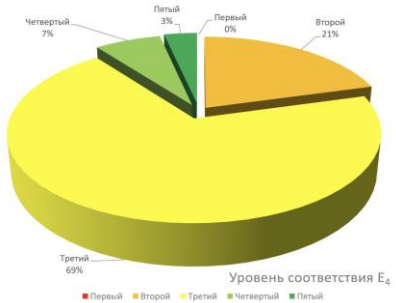
Результаты оценки соответствия по направлениям

Процесс 4 «Защита от вредоносного кода»



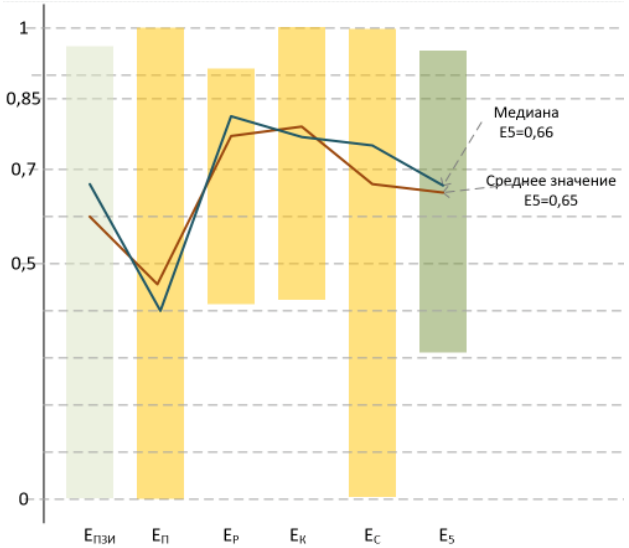
Топ 5 часто встречающихся несоответствий:

- ✓ 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



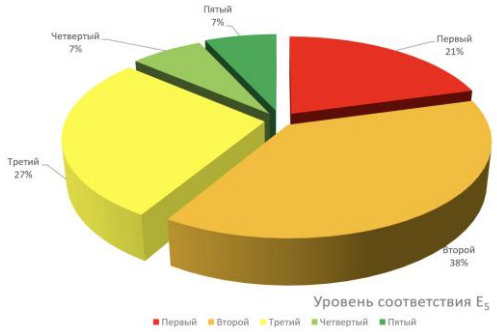
Результаты оценки соответствия по направлениям

Процесс 5 «Предотвращение утечек информации»



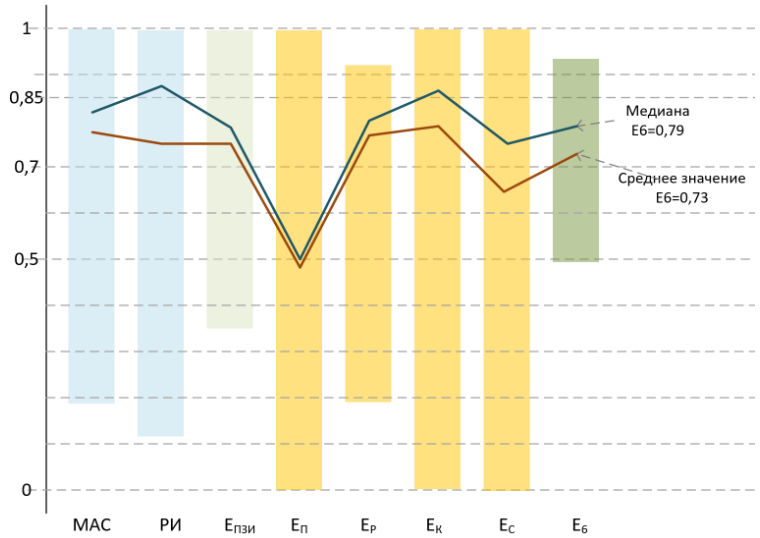
Топ часто встречающихся несоответствий:

- ✓ 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»

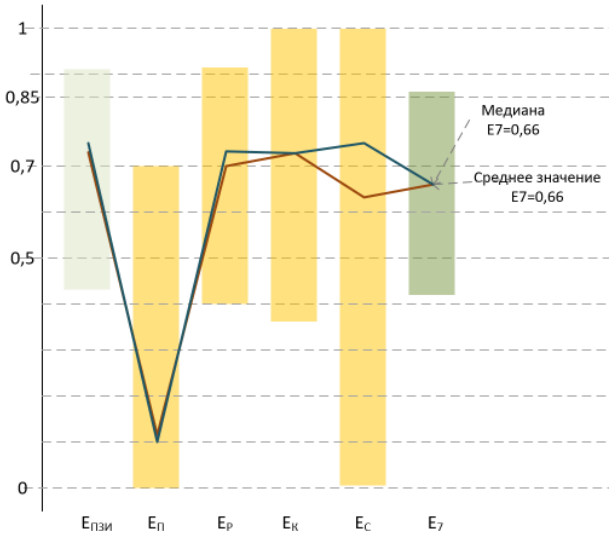


Топ 5 часто встречающихся несоответствий:

- ✓ 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»



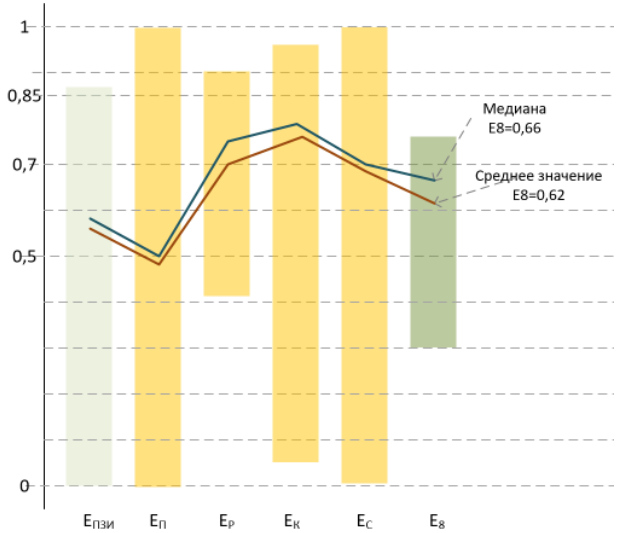
Топ часто встречающихся несоответствий:

✓ Все???

5% организаций не использовали средства виртуализации

Результаты оценки соответствия по направлениям

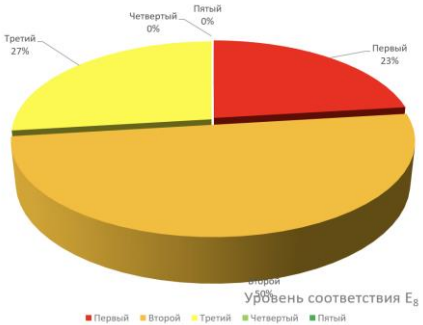
Процесс 8 «Защита информации при осуществлении удаленного логического доступа с использованием мобильных (переносных) устройств»



Топ часто встречающихся несоответствий:

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

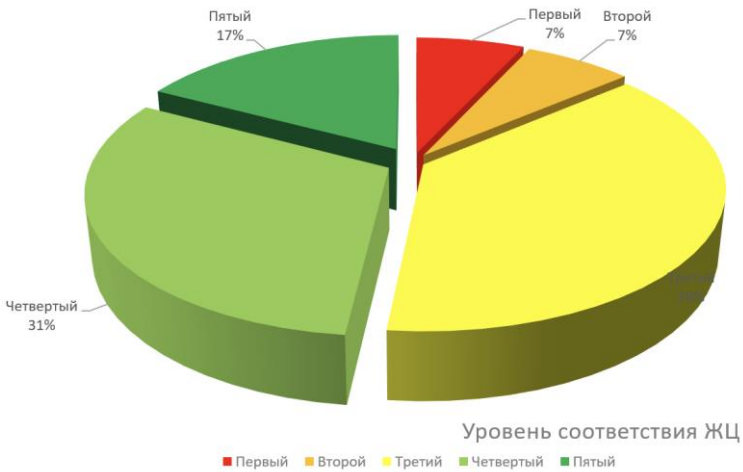
НЕТ адаптации мер из ГОСТ 57580.1 под специфику предоставления удаленного доступа в организации!!!



10% организаций не имели удаленного доступа

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)

Обобщенные результаты оценки соответствия

Основания для проведения оценки соответствия требованиям ГОСТ Р 57580.1-2017

Результаты оценки соответствия по направлениям

Положение Банка России 683-П

- ✓ Проверяется 35 требований
- ✓ Определение методики выставления оценки
- ✓ Результаты на текущий момент только для внутреннего использования

Топ часто встречающихся несоответствий:

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

Спасибо за внимание!
Вопросы?

Свинцицкий Антон Игоревич

Директор по консалтингу
АО «ДиалогНаука»
Телефон: +7 (495) 980-67-76
Факс: +7 (495) 980-67-75
E-mail: svintsitskii@dialognauka.ru

http://www.DialogNauka.ru