ОБЗОР ТРЕБОВАНИЙ БАНКА РОССИИ ПО ЗАЩИТЕ ИНФОРМАЦИИ

(ПОЛОЖЕНИЯ БАНКА РОССИИ, ГОСТ Р 57580.X, РЕКОМЕНДАЦИИ 12-МР)

Антон Свинцицкий
Директор по консалтингу
АО «ДиалогНаука»

27 апреля 2023 года, Москва

ДиалогНаука

Положения Банка России по защите информации

Центральный банк Российской Федерации

787-П (779-П)

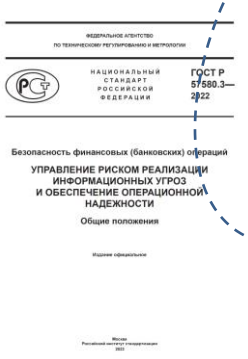
716-П

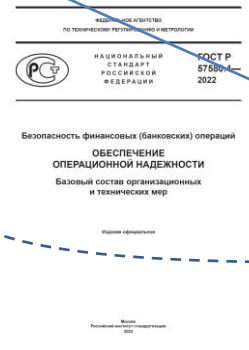
683-П

719-П

757-П

802-П





Положения Банка России по защите информации

01.01.2020
Необходимость сертификации прикладного ПО АС

01.01.2021
1. Необходимость выполнения требований ГОСТ Р 57580.1-2017
2. Проведение тестирований на проникновение
3. Проведение оценки соответствия

25.02.2021
Вступило в силу 747-П

01.07.2021
Дополнительные требования 747-П

03.07.2021
Вступило в силу 757-П

01.01.2022
1. Вступает в силу 719-П
2. Дополнительные требования 747-П
3. Требования 757-П
4. Готовность к 716-П

01.10.2022
1. Форма отчетности 0409071
2. «обновленная» редакция Положения 716-П
3. Изменения в 683-П
4. Вступает в силу 787-П
5. Вступает в силу 779-Р

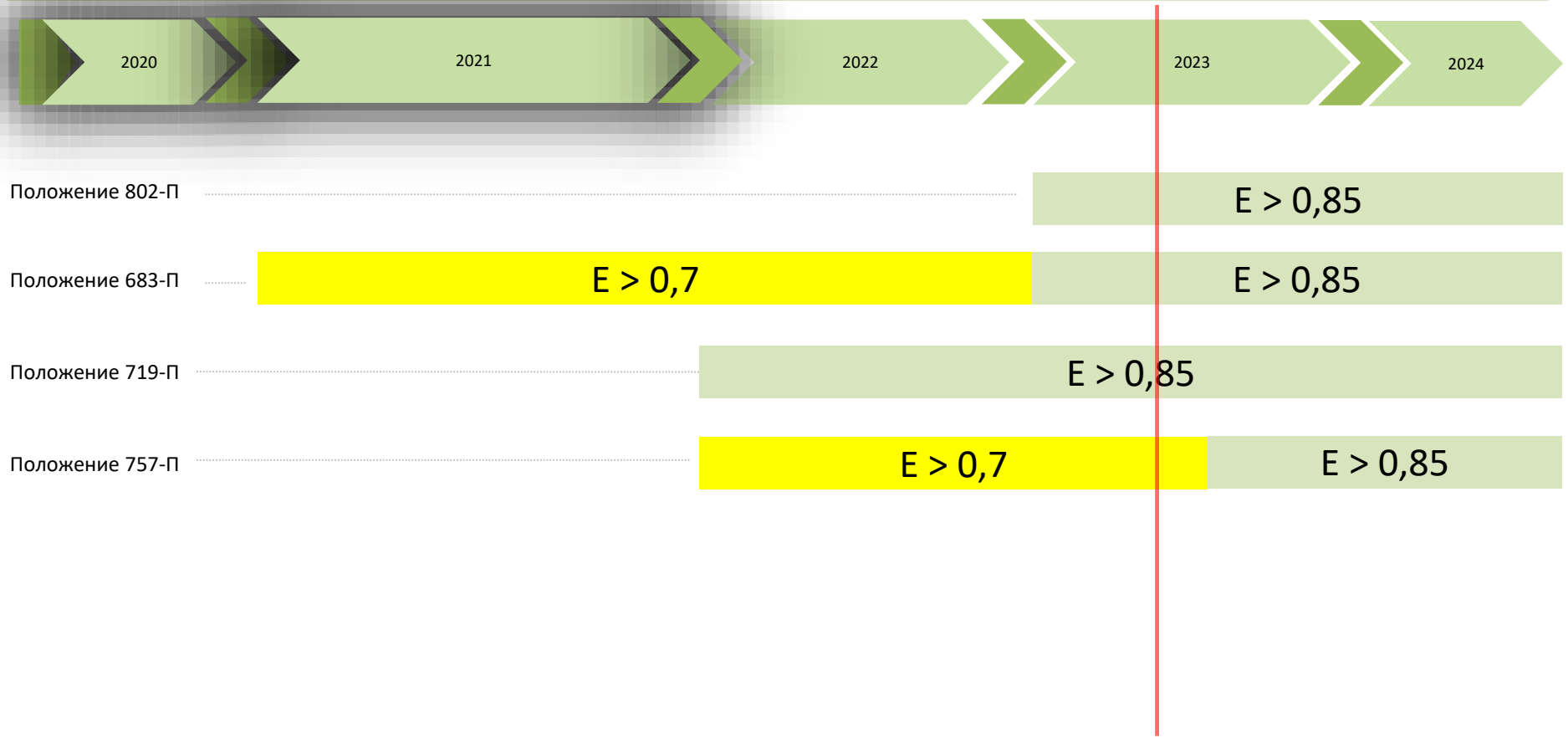
05.12.2022
1. Вступило в силу 802-П (вместо 747-П)

01.01.2023
1. Форма отчетности 0403202

01.07.2023
Дополнительные требования 757-П

01.01.2024
1. Дополнительные требования 757-П
2. Дополнительные требования 719-П

Положения Банка России по защите информации



Положение Банка России 802-П

Ключевые требования:

1. Выделение отдельных сегментов (не контуров!!!) для размещения объектов информационной инфраструктуры.

2. Реализация **второго уровня защиты** (стандартный) в соответствии с ГОСТ Р 57580.1-2017 для указанных сегментов (за исключением ОПКЦ – усиленный уровень).

3. Определены требования к мерам защиты информации на основных этапах обработки ЭС (аналогичные требованиям Положению Банка России 747-П).

4. Оценка соответствия должна проводиться не реже 1 раза в 2 года в соответствии с ГОСТ Р 57580.2-2018.

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

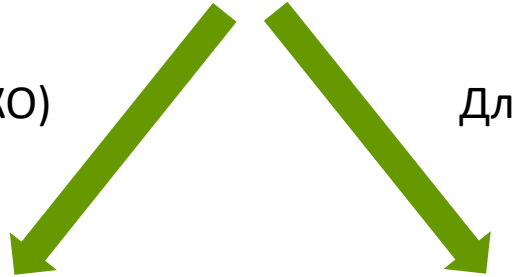
2. **Требования к прикладному программному обеспечению автоматизированных систем и приложений**:
   - ✓ Сертификация или **оценка соответствия** по ОУД 4

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 реализации функций защиты информации на технологических участках выполнения операций по переводу денежных средств



Для ОПДС (КО)

Положение Банка России 683-П
п.5.2.1

Для других субъектов НПС

Положение Банка России 719-П
Приложение 2

ИИА | ФПП | УП | ОУ | ХИ

Положение Банка России 683-П

Подход к формированию требований по защите информации:

1. **Определяет состав защищаемой информации в кредитных организациях**

2. **Требования к ИТ-инфраструктуре, задействованной ~~при осуществлении переводов денежных средств~~ при осуществлении банковской деятельности в целях противодействия осуществлению переводов денежных средств без согласия клиента**:
   - ✓ Выполнение требований ГОСТ Р 57580.1-2017:
     - ✓ системно значимые КО - усиленный уровень (уровень 1) защиты информации по ГОСТ Р 57580.1-2017;
     - ✓ остальные КО - стандартный уровень (уровень 2) защиты информации ГОСТ Р 57580.1-2017
   - ✓ Оценка соответствия на периодической основе

3. **Требования к прикладному программному обеспечению автоматизированных систем и приложений**:
   - ✓ Сертификация или **оценка соответствия** по ОУД 4 (в предыдущей редакции был анализ уязвимостей по ОУД 4)

4. **Требования к обеспечению защиты информации при осуществлении банковской деятельности, применяемые в отношении технологии обработки защищаемой информации**:
   - ✓ идентификация, аутентификация и авторизация клиентов при совершении действий в целях осуществления банковских операций (ИАА)
   - ✓ Формирование (подготовка), передача и прием ЭС (ФПП)
   - ✓ Удостоверение права клиентов распоряжаться денежными средствами (УП)
   - ✓ осуществление банковской операции, учет результатов ее осуществления (ОУ)
   - ✓ хранение электронных сообщений и информации об осуществленных банковских операциях (ХИ)

5. **Иные требования**:
   - ✓ Проведение тестирования на проникновение
   - ✓ Информирование об инцидентах
   - ✓ Защита ПДн
   - ✓ Использование СКЗИ (в том числе для обеспечения целостности электронных сообщений и подтверждения их составления)
   - ✓ Валидация email адресов

Положение Банка России 757-П

- ✓ **Информирование клиентов** о рисках информационно безопасности
- ✓ **Использование СКЗИ** в соответствии с:
  - законодательством Российской Федерации;
  - нормативными документами ФСБ России;
  - технической документации
- ✓ **Выполнение требований ГОСТ Р 57580.1-2017**

Определение уровня защиты

Примечание: пересмотр применимого уровня защиты ежегодно не позднее первого рабочего дня календарного года

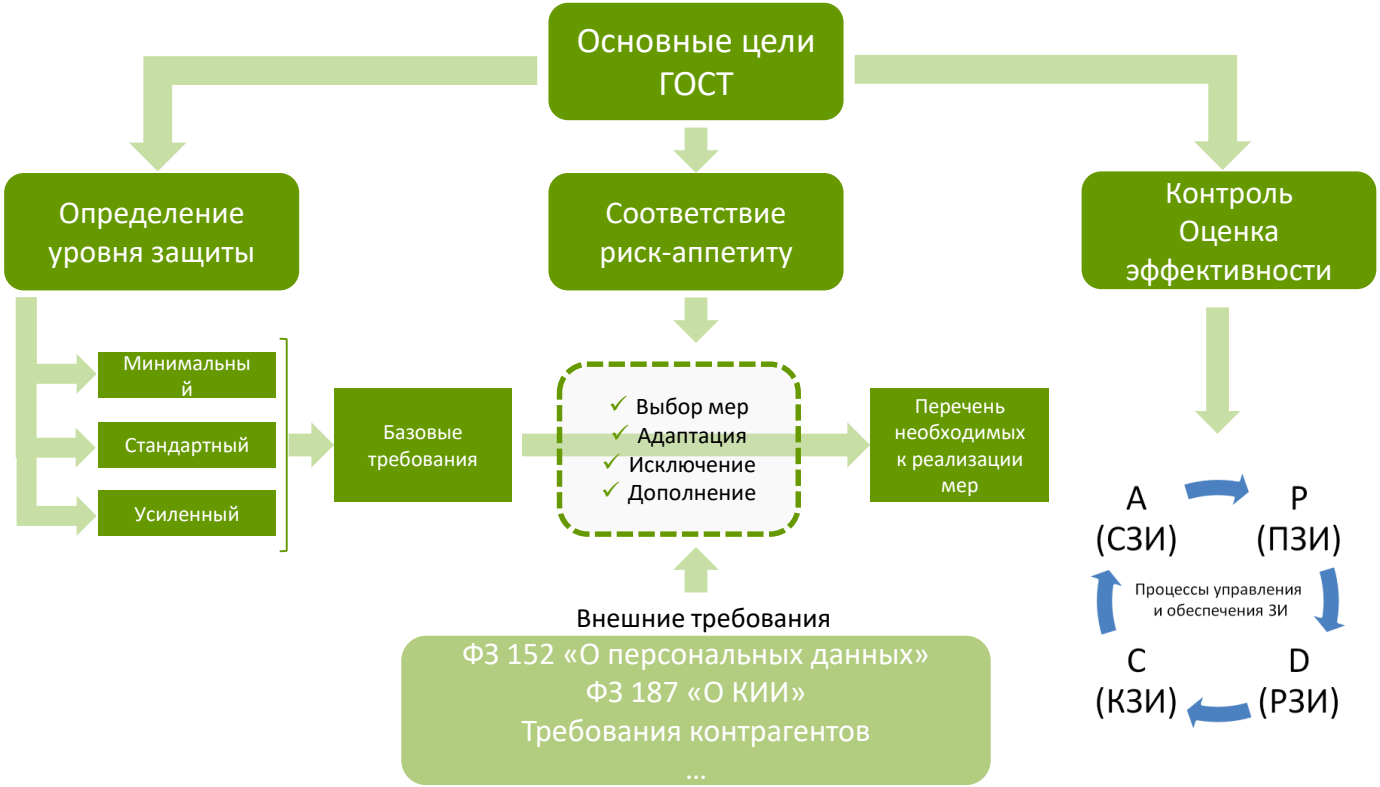
центральные контрагенты, центральный депозитарий	Усиленный
соответствующие критериям, описанным в п.5.3	Стандартный
остальные некредитные финансовые организации	Минимальный

Положение Банка России 757-П

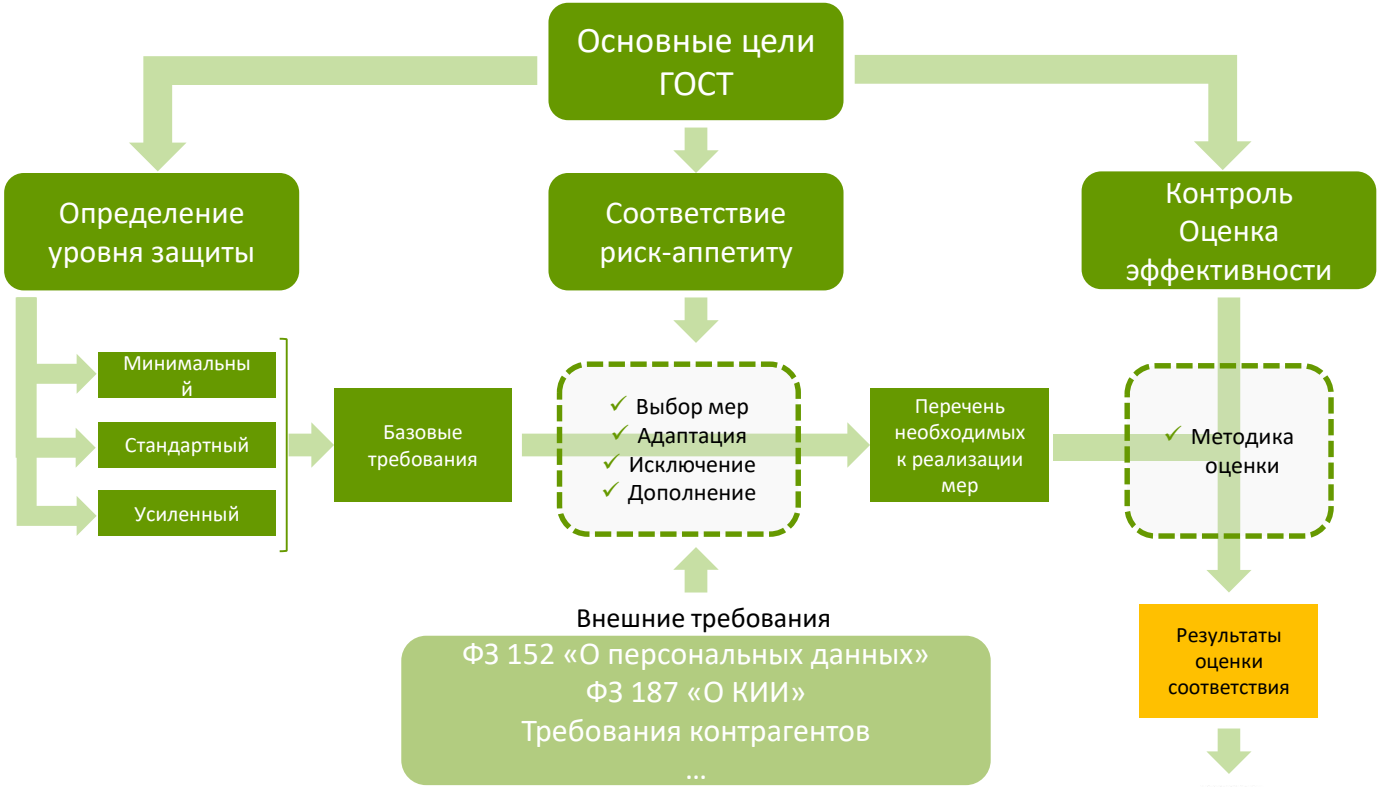
Требование	Ссылка	Период.
Проведение тестирования на проникновение	п.1.4.5 757-П ЖЦ.20 ГОСТ 57580	ежегодно
Сертификация прикладного ПО АС или оценка соответствия по ОУД 4	п.1.8 757-П	разово (а также в случаях предусмотренных выданным сертификатом)
Подписание электронных сообщений способом, позволяющим обеспечить их целостность и подтвердить их составление уполномоченным на это лицом	п.1.9 757-П	постоянно
Регламентация, реализация, контроль (мониторинг) технологии безопасной обработки защищаемой информации: ▪ ИИА ▪ ФПП ▪ УП ▪ ОУ ▪ ХИ	п.1.10 757-П	постоянно
Регистрация событий информационной безопасности	п.1.11 757-П	постоянно
Внедрение процесса управления инцидентами информационной безопасности	п.1.14 757-П	постоянно
Оценка выполнения требований ГОСТ Р 57580.1	п.1.5.3 757-П	ежегодно (для 1 уровня) раз в 3 года (для 2 уровня)

ГОСТ Р 57580.1-2017

ГОСТ Р 57580.1-2017



ГОСТ Р 57580.1-2017



Контуры безопасности

- ✓ п.1 Положения 683-П
- ✓ п.1 Положения 757-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

Контур безопасности

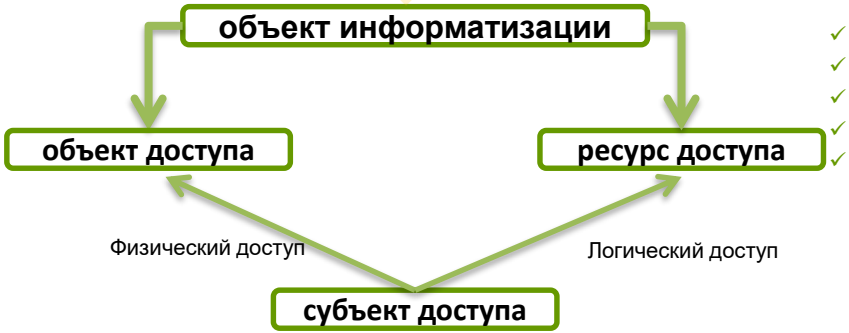
Контуры безопасности

- ✓ 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



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

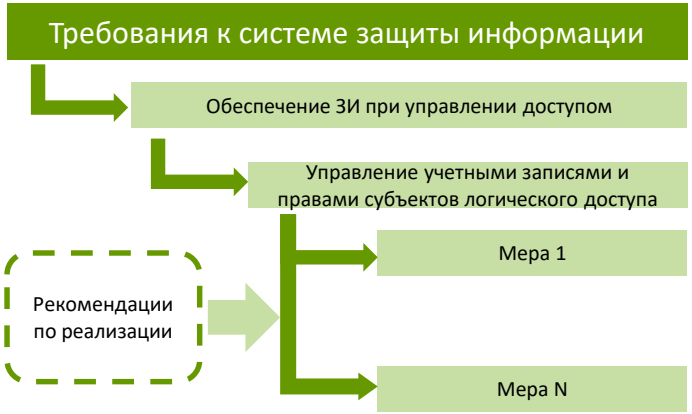
- ✓ АС
- ✓ БД
- ✓ Сетевые ресурсы
- ✓ Виртуальные машины
- ✓ Сервисы (электронная почта, WEB)

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

Контуры безопасности. Вариант 2

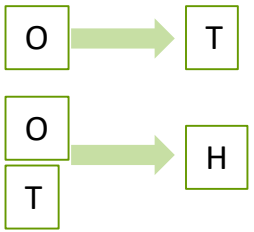
Нормативные требования	Уровень обработки информации	Тип автоматизированных систем
Положение 802-П	✓ Уровень взаимодействия с клиентами (ФЛ) ✓ Уровень взаимодействия с клиентами (ЮЛ)	✓ Системы ДБО, устанавливаемые на АРМ клиентов ✓ Системы ДБО, доступ к которым предоставляется через WEB интерфейс ✓ Системы мобильного банкинга ✓ Формирование ЭС при личном обращении клиента в офис Банка
Положение 683-П	✓ Обработка ЭС в кредитной организации ✓ Работы с карточными данными ✓ Управление банкоматной сетью и ТУ ДБО	
Положение 757-П	✓ 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	

Базовые требованиям ГОСТ Р 57580.1-2017



Направление	3 направления
Процесс	8 процессов
Подпроцесс	
Меры системы защиты информации	343 меры

Примечание:



Условное обозначение и номер меры	Содержание мер системы защиты информации	Уровень защиты информации		
		3	2	1
УЗП.5	Документарное определение правил предоставления (отзыва) и блокирования логического доступа	Н	О	О
УЗП.6	Назначение для всех ресурсов доступа распорядителя логического доступа (владельца ресурса доступа)	О	О	О
УЗП.7	Предоставление прав логического доступа по решению распорядителя логического доступа (владельца ресурса доступа)	О	О	О
УЗП.8	Хранение эталонной информации о предоставленных правах логического доступа и обеспечение целостности указанной информации	О	Т	Т

Раздел 8 ГОСТ Р 57580.1-2017

Организационные меры защиты информации

ПЗИ.1 Область применения процесса

ПЗИ.2 Состав и содержание

ПЗИ.4 Порядок применения

Технические меры защиты информации

ПЗИ.3 Состав и содержание

ПЗИ.5 Порядок применения

Раздел 8 ГОСТ Р 57580.1-2017

Реализация организационных мер защиты информации

РЗИ.1 Учет объектов доступа и ресурсов доступа

РЗИ.7 Применения мер

РЗИ.16 Повышение осведомленности

РЗИ.4 Назначение на роли

РЗИ.15 Обучение

Реализация технических мер защиты информации

РЗИ.2 Размещение и настройка

РЗИ.3 Контроль (тестирование)

РЗИ.11-14 Сертифицированные СЗИ

РЗИ.9 Обеспечение доступности

РЗИ.8 Централизованное управление

Раздел 8 ГОСТ Р 57580.1-2017

Организационные меры защиты информации

Технические меры защиты информации

Раздел 8 ГОСТ Р 57580.1-2017

- ✓ обнаружения инцидентов защиты информации;
- ✓ обнаружения недостатков в рамках контроля системы защиты информации;
- ✓ изменения политики финансовой организации;
- ✓ изменений требований к защите информации, определенных правилами платежной системы;
- ✓ изменений, внесенных в законодательство Российской Федерации, в том числе нормативные акты Банка России

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

Нормативная база проведения оценки соответствия

Методика оценки соответствия

- ✓ Оценка выбора и реализации финансовой организацией организационных и технических мер ЗИ в соответствии с требованиями ГОСТ Р 57580.1-2017 проводится независимой организацией:
  - обладающей необходимой компетенцией
  - обладающей лицензией на деятельность по технической защите конфиденциальной информации

- ✓ Оценка осуществляется по следующим основным направлениям:
  - выбор финансовой организацией организационных и технических мер ЗИ, направленных на непосредственное обеспечение ЗИ (раздел 7 ГОСТ)
  - полнота реализации организационных и технических мер ЗИ, направленных на непосредственное обеспечение ЗИ и входящих в систему организации и управления ЗИ (раздел 8 ГОСТ)
  - обеспечение ЗИ на этапах жизненного цикла АС (раздел 9 ГОСТ)

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
- ✓ Реализация деятельность некредитной финансовой организации (в том числе совмещение)

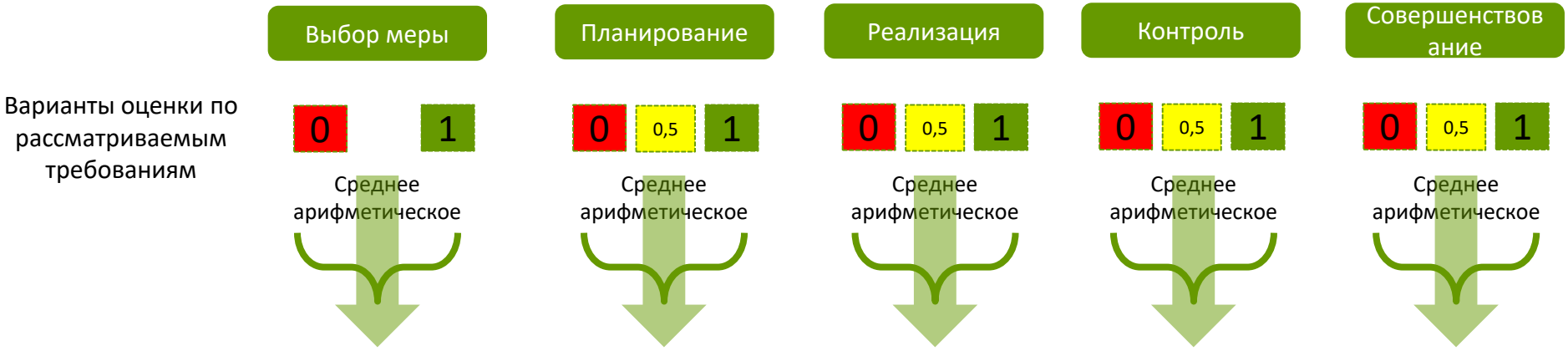
2 очередь:

- ✓ 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
- ✓ …

Оценка процесса защиты информации



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

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

$$\mathrm{E}_{\mathrm{ПЗИ}_i} = \frac{\sum_{j=1}^{N} E_{\mathrm{МЗИ}_j}}{N}$$

$$E_i = \frac{\mathrm{E}_{\mathrm{ПЗИ}_i} + (0{,}2 * \mathrm{E}_{\mathrm{П}_i} + 0{,}4 * \mathrm{E}_{\mathrm{Р}_i} + 0{,}25 * \mathrm{E}_{\mathrm{К}_i} + 0{,}15 * \mathrm{E}_{\mathrm{С}_i})}{2}$$

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	

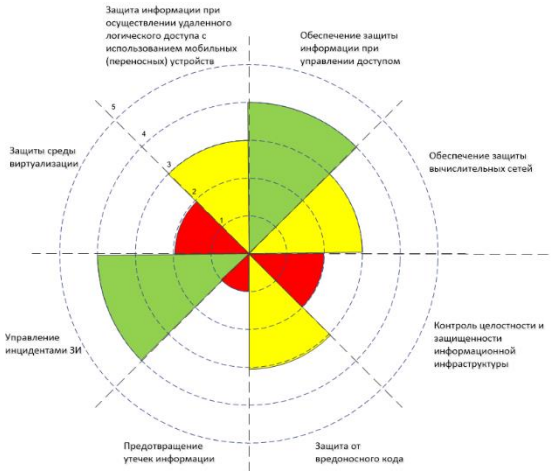
Интерпретация результатов оценки

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 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"

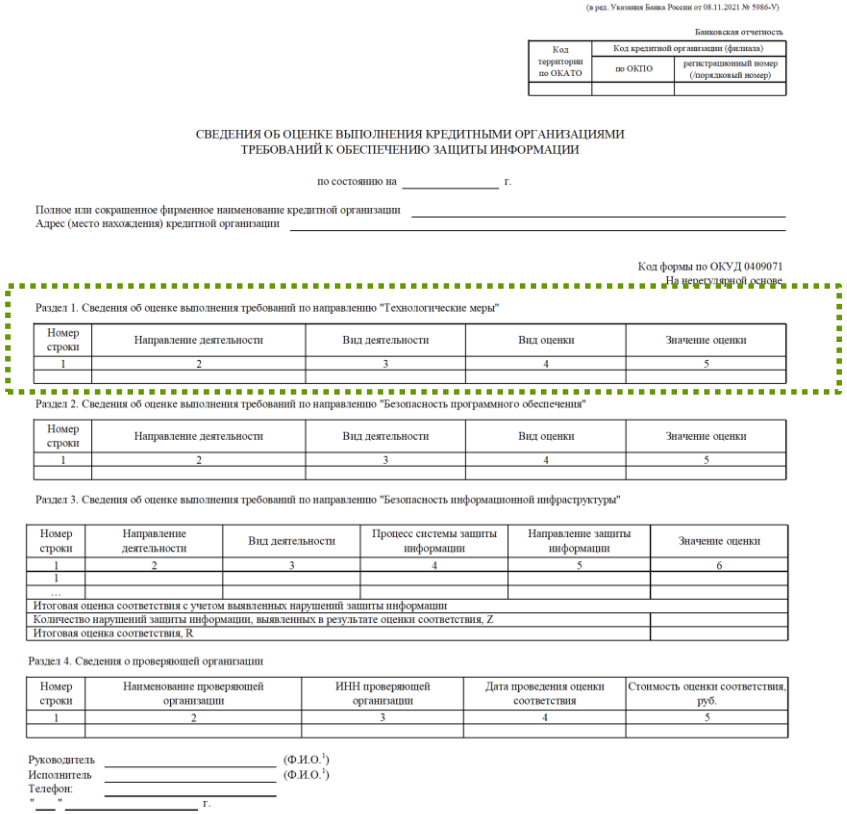
Номер строки	Направление деятельности	Вид деятельности	Процесс системы защиты информации	Направление защиты информации	Значение оценки
1	2	3	4	5	6
1					
...					
Итоговая оценка соответствия с учетом выявленных нарушений защиты информации					
Количество нарушений защиты информации, выявленных в результате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

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 747-П
- ✓ N 757-П

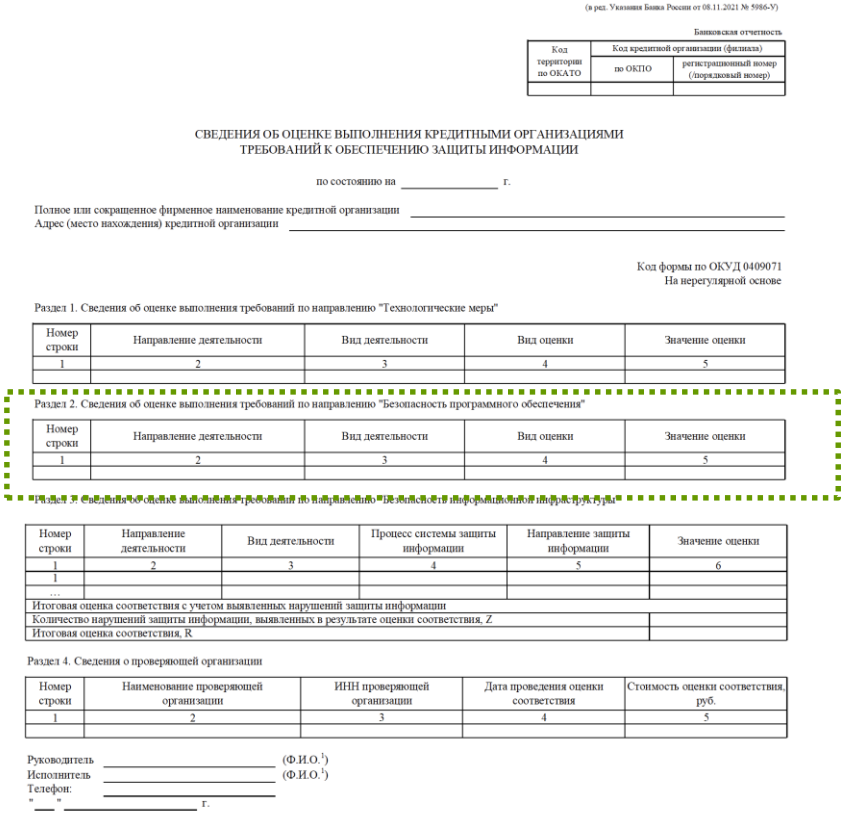
Вид деятельности (в том числе при совмещении):

- ✓ 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					

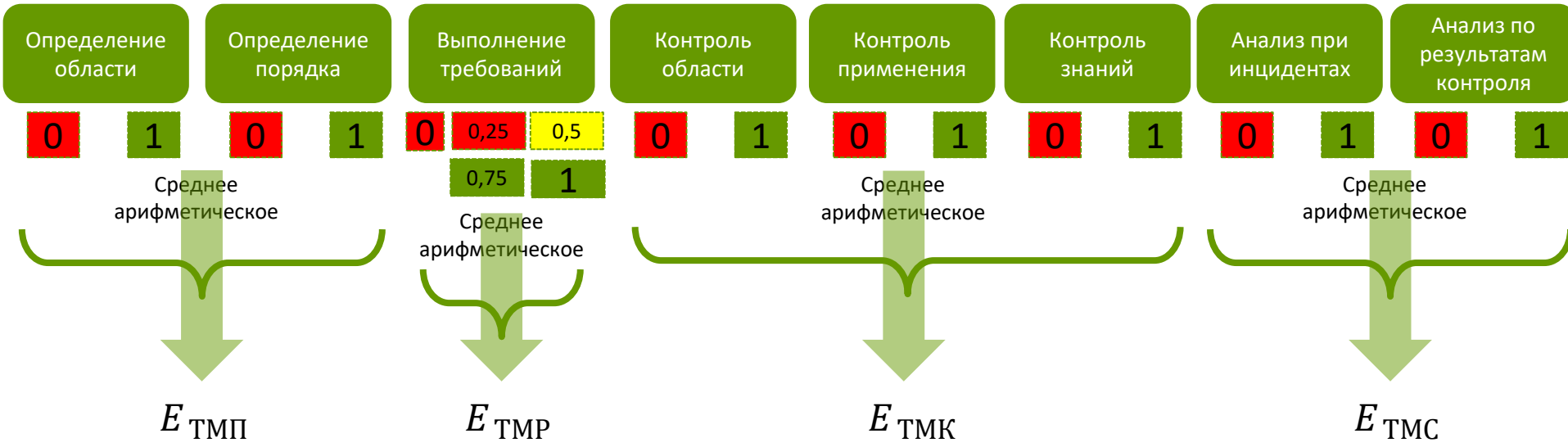
Раздел 4. Сведения о проверяющей организации

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.

Новое в методологии. Методика 12-MP

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

- ✓ Требование подпункта 1.10.1 пункта 1.10

ИИА

- ✓ Требование абзаца второго подпункта 1.10.2 пункта 1.10
- ✓ Требование абзаца третьего подпункта 1.10.2 пункта 1.10

ФПП

- ✓ Требование абзаца второго подпункта 1.10.3 пункта 1.10
- ✓ Требование абзаца третьего подпункта 1.10.3 пункта 1.0
- ✓ Требование абзаца четвертого подпункта 1.10.3 пункта 1.10
- ✓ Требование абзаце пятого подпункта 1.10.3 пункта 1.10
- ✓ Требование абзаца шестого подпункта 1.10.3 пункта 1.10

УП

- ✓ Требование абзаца второго подпункта 1.10.4 пункта 1.10
- ✓ Требование абзаца третьего подпункта 1.10.4 пункта 1.10

ОУ

ХИ

- ✓ Требование абзаца второго подпункта 1.10.5 пункта 1.10
- ✓ Требование абзаца третьего подпункта 1.10.5 пункта 1.10
- ✓ Требование абзаца четвертого подпункта 1.10.5 пункта 1.10
- ✓ Требование абзаца пятого подпункта 1.10.5 пункта 1.10

→ 14 требований по 8 направлениям

Новое в методологии. Методика 12-МР

Определение области:

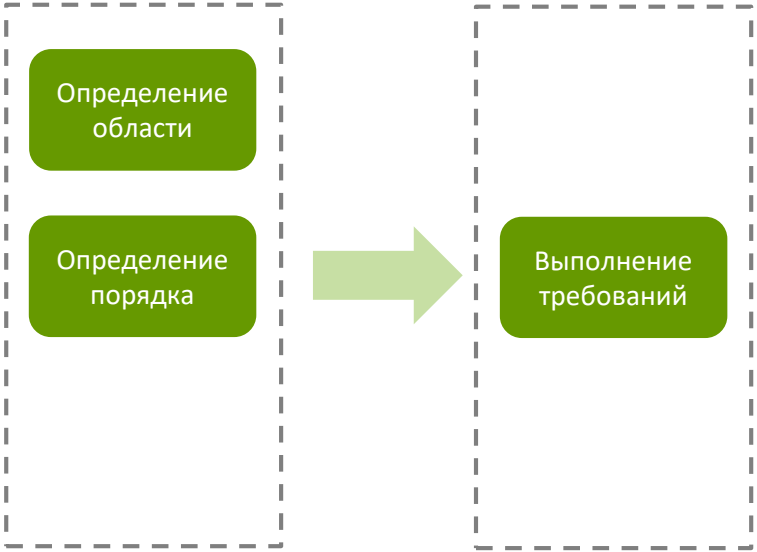
✓ Определение реестра технологических участков и АС (ИС), обеспечивающих реализацию процессов на указанных участках

Определение порядка:

✓ Определение требований в локальных ВНД (ОРД) организации

✓ Детализация требований в проектной документации на АС (ИС)

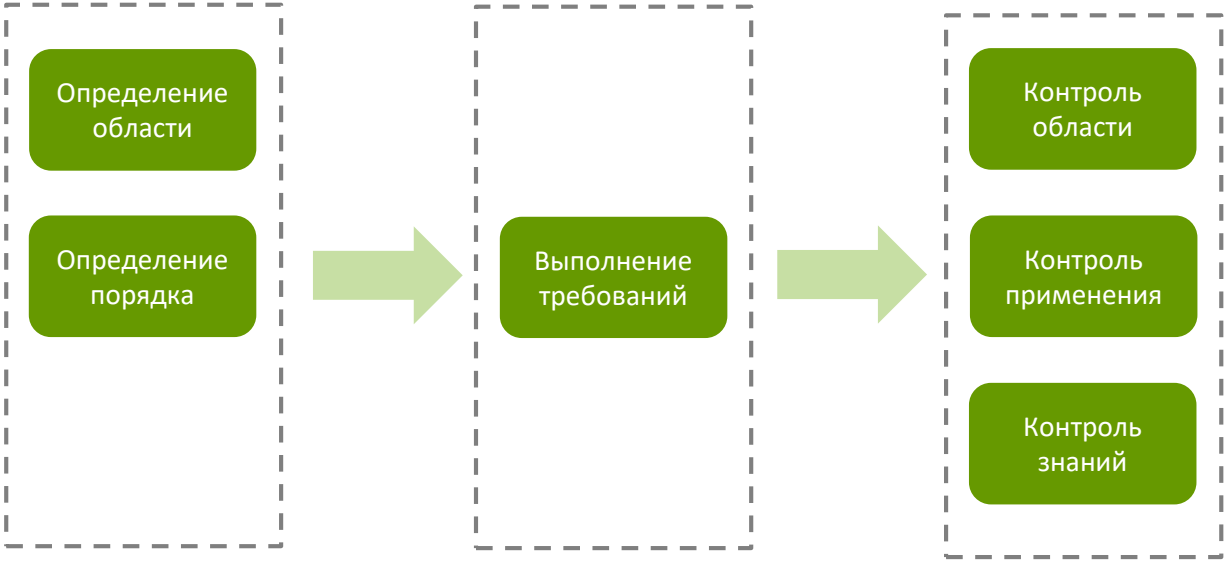
Новое в методологии. Методика 12-МР



Выполнение требований:

✓ Проверка реализации требований (сбор свидетельств) для АС (ИС)

Новое в методологии. Методика 12-МР



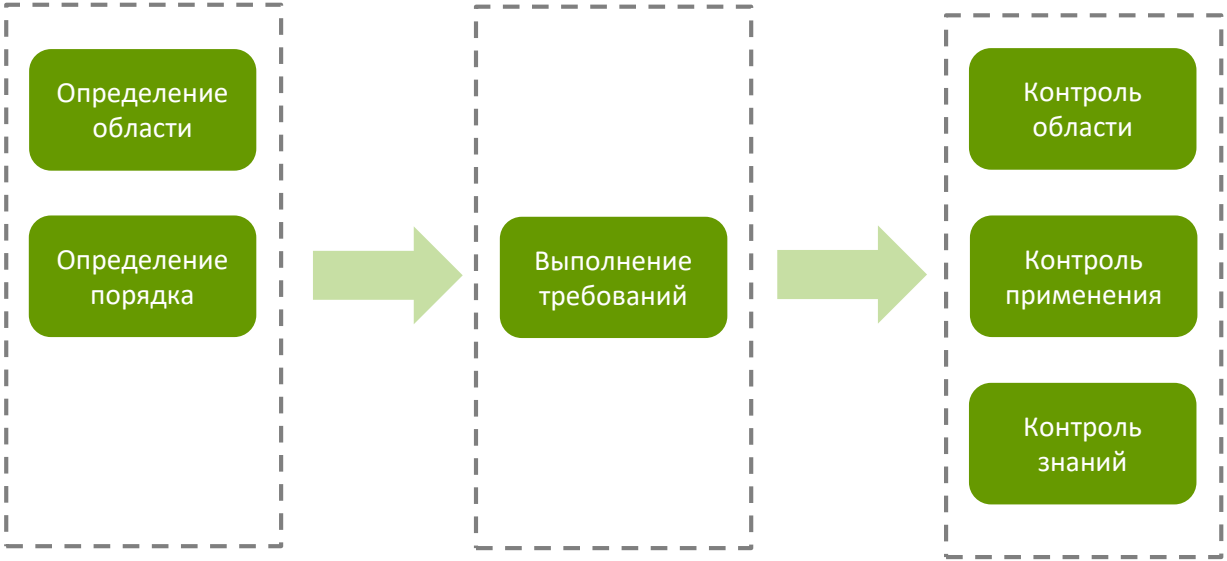
Контроль области:

✓ Проверка, что реестр технологических участков и АС (ИС) пересматривается на периодической основе

Контроль применения:

✓ Проведение внутренних процедур контроля, направленных на обеспечение соответствия реализуемых мер защиты информации мерам, описанных в проектной документации на АС (ИС)

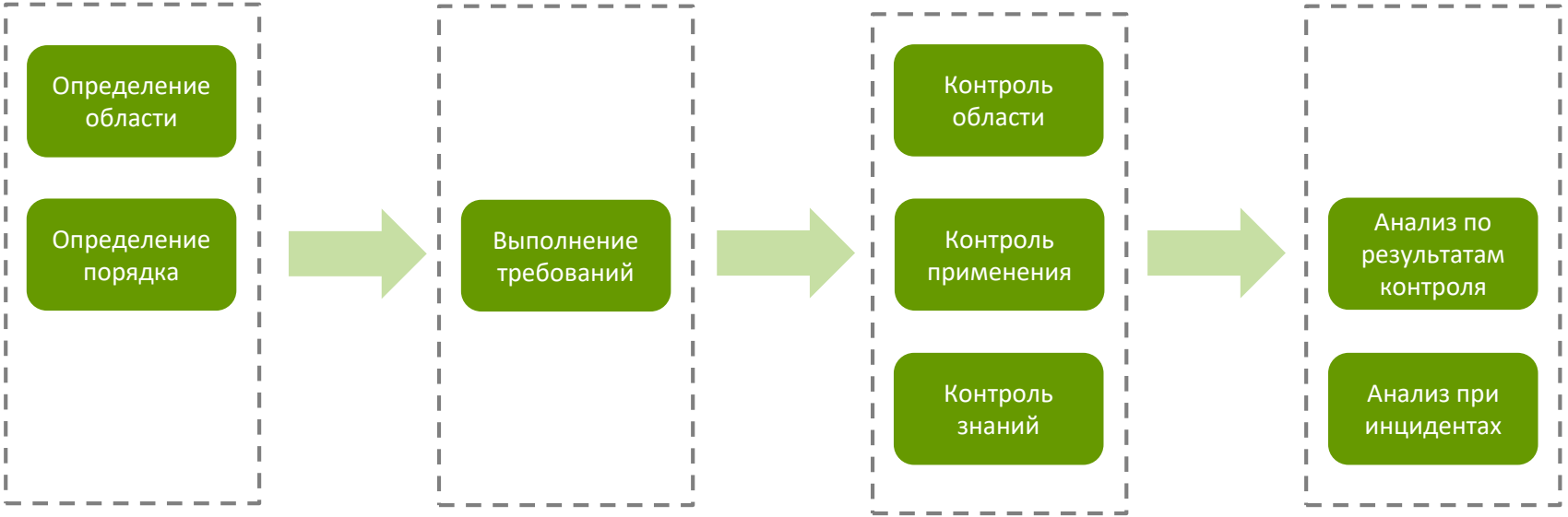
Новое в методологии. Методика 12-МР



Контроль знаний:

✓ аналог меры КЗИ.7 из ГОСТ Р 57580.1-2017 «Проведение проверок знаний работников финансовой организации в части применения мер защиты информации в рамках процесса системы защиты информации»

Новое в методологии. Методика 12-МР



Анализ по результатам контроля:

✓ Аналог требований СЗИ.2 - СЗИ.4 из ГОСТ Р 57580.1-2017

Анализ при инцидентах:

✓ Аналог требований СЗИ.1 ГОСТ Р 57580.1-2017

Новое в методологии. Методика 12-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)
Положение 719-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:

49 требований (392 проверки)

Для информации:

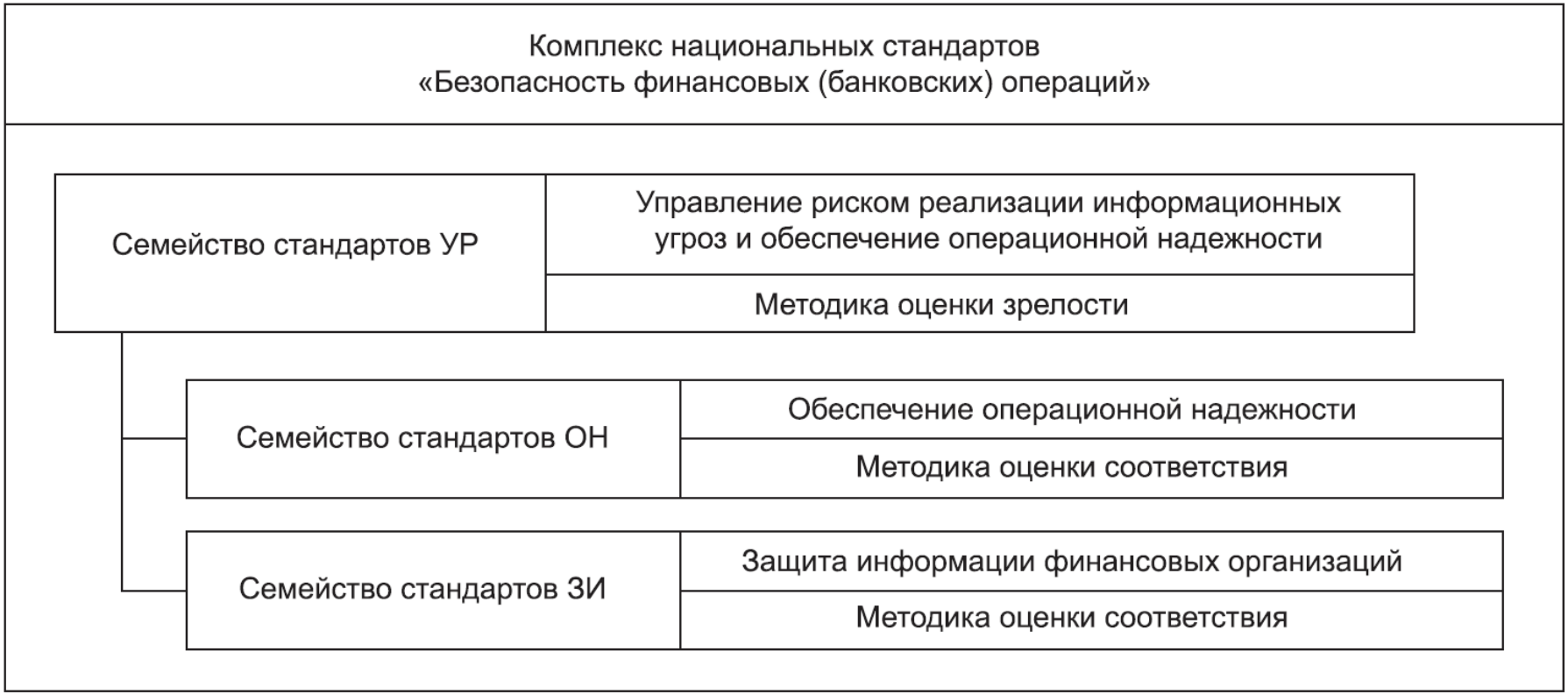
В ГОСТ Р 57580.1-2017 проверяется 606 мер для «Усиленного уровня» и 542 меры для «Стандартного уровня»

Оценка соответствия и Положения Банка России 716-П

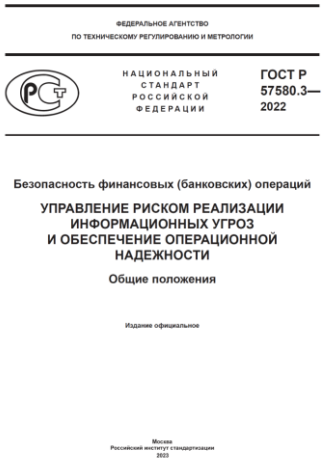
Приложение 1 к Положению Банка России от 8 апреля 2020 года № 716-П «О требованиях к системе управления операционным риском в кредитной организации и банковской группе» (в актуальной редакции) устанавливает следующие КПУР информационной безопасности:

	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			

Комплекс стандартов ГОСТ Р 57580.х



ГОСТ Р 57580.3-2022


ФЕДЕРАЛЬНОЕ АГЕНТСТВО
ПО ТЕХНИЧЕСКОМУ РЕГУЛИРОВАНИЮ И МЕТРОЛОГИИ

НАЦИОНАЛЬНЫЙ СТАНДАРТ РОССИЙСКОЙ ФЕДЕРАЦИИ

ГОСТ Р 57580.3— 2022

Безопасность финансовых (банковских) операций

УПРАВЛЕНИЕ РИСКОМ РЕАЛИЗАЦИИ ИНФОРМАЦИОННЫХ УГРОЗ И ОБЕСПЕЧЕНИЕ ОПЕРАЦИОННОЙ НАДЕЖНОСТИ

Общие положения

Издание официальное

Москва
Российский институт стандартизации
2022

Устанавливает требования к системе управления риском реализации информационных угроз

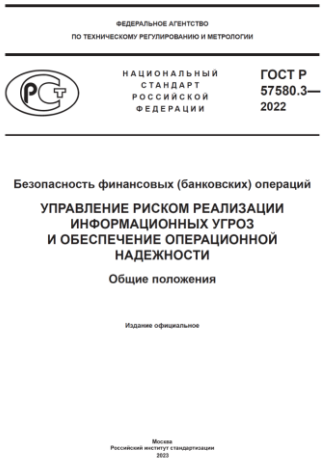
Направлено на обеспечение операционной надежности

Связано с бизнес-процессами (технологическими процессами) и объектами информатизации

Реализуется в «классической» модели PDCA

Интегрировано в общую систему управления операционным риском

ГОСТ Р 57580.3-2022



ФЕДЕРАЛЬНОЕ АГЕНТСТВО
ПО ТЕХНИЧЕСКОМУ РЕГУЛИРОВАНИЮ И МЕТРОЛОГИИ

НАЦИОНАЛЬНЫЙ СТАНДАРТ РОССИЙСКОЙ ФЕДЕРАЦИИ

ГОСТ Р 57580.3— 2022

Безопасность финансовых (банковских) операций

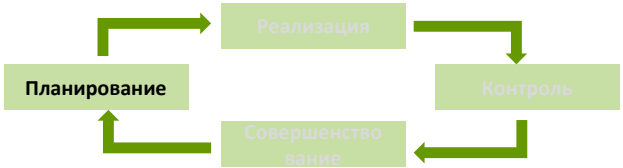
УПРАВЛЕНИЕ РИСКОМ РЕАЛИЗАЦИИ ИНФОРМАЦИОННЫХ УГРОЗ И ОБЕСПЕЧЕНИЕ ОПЕРАЦИОННОЙ НАДЕЖНОСТИ

Общие положения

Издание официальное

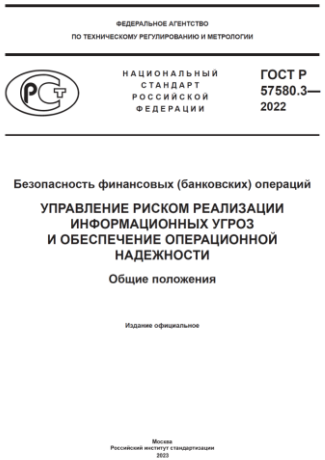
Москва
Российский институт стандартизации
2023

Требования к системе управления риском реализации информационных угроз



- ✓ определение политики управления риском реализации информационных угроз (с учетом требований ГОСТ Р 57580.3-2022 и Положения Банка России 716-П)
  - ✓ установление структуры и организации системы управления риском реализации информационных угроз, а также распределение функций, ролей и ответственности в рамках управления риском реализации информационных угроз;
  - ✓ установление политики управления риском реализации информационных угроз;
  - ✓ участие совета директоров (наблюдательного совета) и коллегиального исполнительного органа финансовой организации в решении вопросов управления риском реализации информационных угроз
- ✓ выявление и идентификацию риска реализации информационных угроз, а также его оценку;
  - ✓ идентификация критичной архитектуры;
  - ✓ идентификация риска реализации информационных угроз;
  - ✓ выявление и моделирование информационных угроз;
  - ✓ оценка риска реализации информационных угроз
- ✓ организация ресурсного (кадрового и финансового) обеспечения:
  - ✓ организация ресурсного (кадрового и финансового) обеспечения процессов системы управления риском реализации информационных угроз;
  - ✓ организация ресурсного (кадрового и финансового) обеспечения функционирования службы ИБ;
  - ✓ организация целевого обучения по вопросам выявления и противостояния реализации информационных угроз

ГОСТ Р 57580.3-2022



ФЕДЕРАЛЬНОЕ АГЕНТСТВО
ПО ТЕХНИЧЕСКОМУ РЕГУЛИРОВАНИЮ И МЕТРОЛОГИИ

НАЦИОНАЛЬНЫЙ СТАНДАРТ РОССИЙСКОЙ ФЕДЕРАЦИИ

ГОСТ Р 57580.3— 2022

Безопасность финансовых (банковских) операций

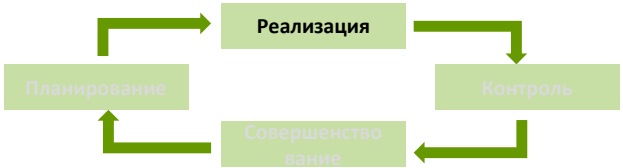
УПРАВЛЕНИЕ РИСКОМ РЕАЛИЗАЦИИ ИНФОРМАЦИОННЫХ УГРОЗ И ОБЕСПЕЧЕНИЕ ОПЕРАЦИОННОЙ НАДЕЖНОСТИ

Общие положения

Издание официальное

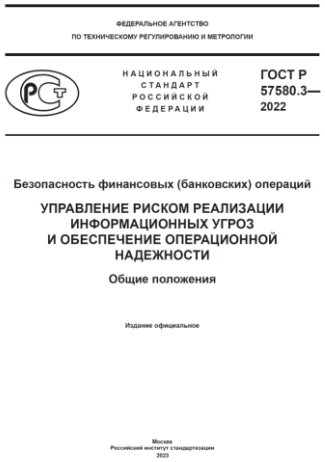
Москва
Российский институт стандартизации
2022

Требования к системе управления риском реализации информационных угроз



- ✓ разработка мероприятий, направленных на уменьшение негативного влияния риска реализации информационных угроз
  - ✓ выбор и применение способа реагирования на риск реализации информационных угроз;
  - ✓ разработка мероприятий, направленных на снижение СВР инцидентов;
  - ✓ разработка мероприятий, направленных на ограничение СТП инцидентов
- ✓ защита от информационных угроз (рекомендуется использовать меры из ГОСТ Р 57580.1-2017)
  - ✓ защита информации финансовой организации;
  - ✓ операционная надежность;
  - ✓ управление риском реализации информационных угроз при аутсорсинге и взаимодействии с поставщиками услуг;
  - ✓ управление риском внутреннего нарушителя;
  - ✓ управление риском реализации информационных угроз в финансовой экосистеме;
  - ✓ выполнение мероприятий, направленных на предотвращение утечек информации
- ✓ реагирование на инциденты, связанные с реализацией информационных угроз, и восстановление после их реализации;
- ✓ выявление событий риска реализации информационных угроз:
  - ✓ сбор и регистрацию информации о внутренних событиях риска реализации информационных угроз и потерях;
  - ✓ выявление и фиксацию инцидентов, в том числе обнаружение реализации компьютерных атак и выявление фактов (индикаторов) компрометации объектов информатизации;
  - ✓ ведение претензионной работы
- ✓ обеспечение осведомленности об актуальных информационных угрозах

ГОСТ Р 57580.3-2022



ФЕДЕРАЛЬНОЕ АГЕНТСТВО
ПО ТЕХНИЧЕСКОМУ РЕГУЛИРОВАНИЮ И МЕТРОЛОГИИ

НАЦИОНАЛЬНЫЙ СТАНДАРТ РОССИЙСКОЙ ФЕДЕРАЦИИ

ГОСТ Р 57580.3— 2022

Безопасность финансовых (банковских) операций

УПРАВЛЕНИЕ РИСКОМ РЕАЛИЗАЦИИ ИНФОРМАЦИОННЫХ УГРОЗ И ОБЕСПЕЧЕНИЕ ОПЕРАЦИОННОЙ НАДЕЖНОСТИ

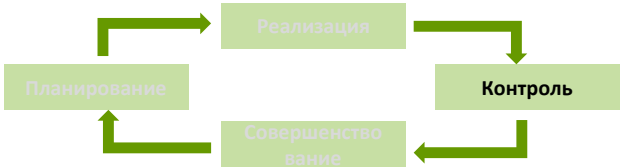
Общие положения

Издание официальное

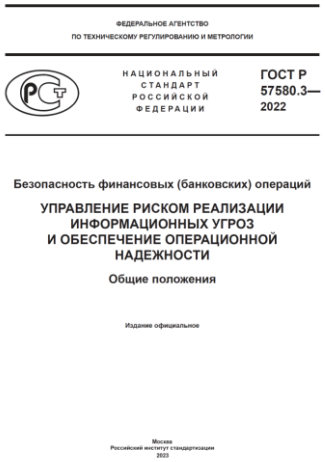
Москва
Российский институт стандартизации
2023

- ✓ установление и реализация программ контроля и аудита
  - ✓ проведение самооценки и профессиональной независимой оценки зрелости процессов обеспечения операционной надежности и защиты информации (самооценка для организаций по минимальному ровню);
  - ✓ проведение сценарного анализа (в части возможной реализации информационных угроз) и тестирования с использованием его результатов готовности финансовой организации противостоять реализации информационных угроз в отношении критичной архитектуры (киберучения)
  - ✓ оценка эффективности функционирования системы управления риском реализации информационных угроз
  - ✓ организацию внутренней отчетности в рамках управления риском реализации информационных угроз
- ✓ мониторинг риска реализации информационных угроз

Требования к системе управления риском реализации информационных угроз



ГОСТ Р 57580.3-2022



ФЕДЕРАЛЬНОЕ АГЕНТСТВО
ПО ТЕХНИЧЕСКОМУ РЕГУЛИРОВАНИЮ И МЕТРОЛОГИИ

НАЦИОНАЛЬНЫЙ СТАНДАРТ РОССИЙСКОЙ ФЕДЕРАЦИИ

ГОСТ Р 57580.3— 2022

Безопасность финансовых (банковских) операций

УПРАВЛЕНИЕ РИСКОМ РЕАЛИЗАЦИИ ИНФОРМАЦИОННЫХ УГРОЗ И ОБЕСПЕЧЕНИЕ ОПЕРАЦИОННОЙ НАДЕЖНОСТИ

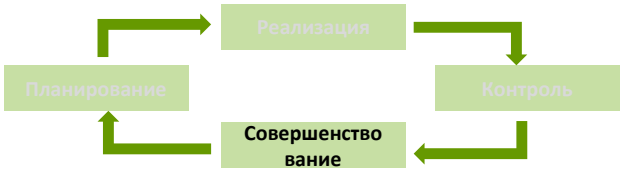
Общие положения

Издание официальное

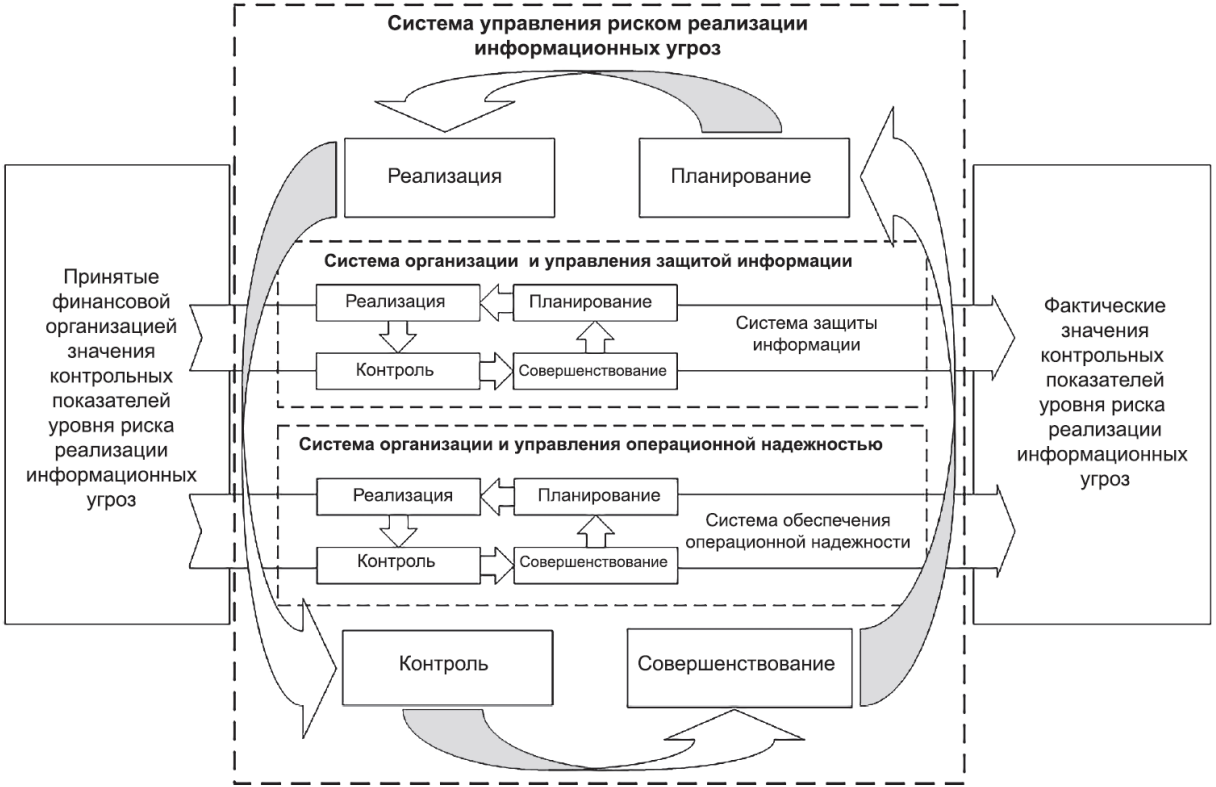
Москва
Российский институт стандартизации
2022

- ✓ обеспечение соответствия фактических значений КПУР принятым
  - ✓ проведение анализа необходимости совершенствования системы управления риском реализации информационных угроз;
  - ✓ принятие решений по совершенствованию системы управления риском реализации информационных угроз

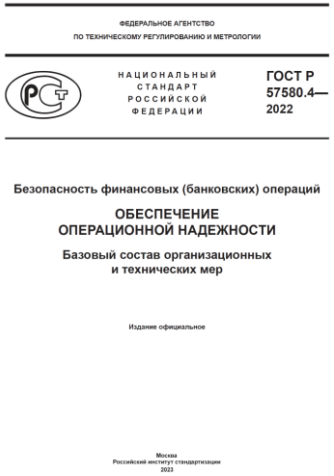
Требования к системе управления риском реализации информационных угроз



ГОСТ Р 57580.3-2022



ГОСТ Р 57580.4-2022


ФЕДЕРАЛЬНОЕ АГЕНТСТВО
ПО ТЕХНИЧЕСКОМУ РЕГУЛИРОВАНИЮ И МЕТРОЛОГИИ

НАЦИОНАЛЬНЫЙ СТАНДАРТ РОССИЙСКОЙ ФЕДЕРАЦИИ

ГОСТ Р 57580.4— 2022

Безопасность финансовых (банковских) операций

ОБЕСПЕЧЕНИЕ ОПЕРАЦИОННОЙ НАДЕЖНОСТИ

Базовый состав организационных и технических мер

Издание официальное

Москва
Российский институт стандартизации
2023

Часть системе управления риском реализации информационных угроз

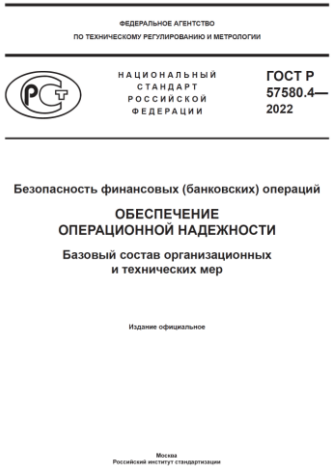
Определяет базовые меры обеспечения операционной надежности (по 8 направлениям)

Связано с бизнес-процессами (технологическими процессами) и объектами информатизации

Реализуется в «классической» модели PDCA

Интегрировано в общую систему управления операционным риском

ГОСТ Р 57580.4-2022


ФЕДЕРАЛЬНОЕ АГЕНТСТВО
ПО ТЕХНИЧЕСКОМУ РЕГУЛИРОВАНИЮ И МЕТРОЛОГИИ

НАЦИОНАЛЬНЫЙ СТАНДАРТ РОССИЙСКОЙ ФЕДЕРАЦИИ

ГОСТ Р 57580.4— 2022

Безопасность финансовых (банковских) операций

ОБЕСПЕЧЕНИЕ ОПЕРАЦИОННОЙ НАДЕЖНОСТИ

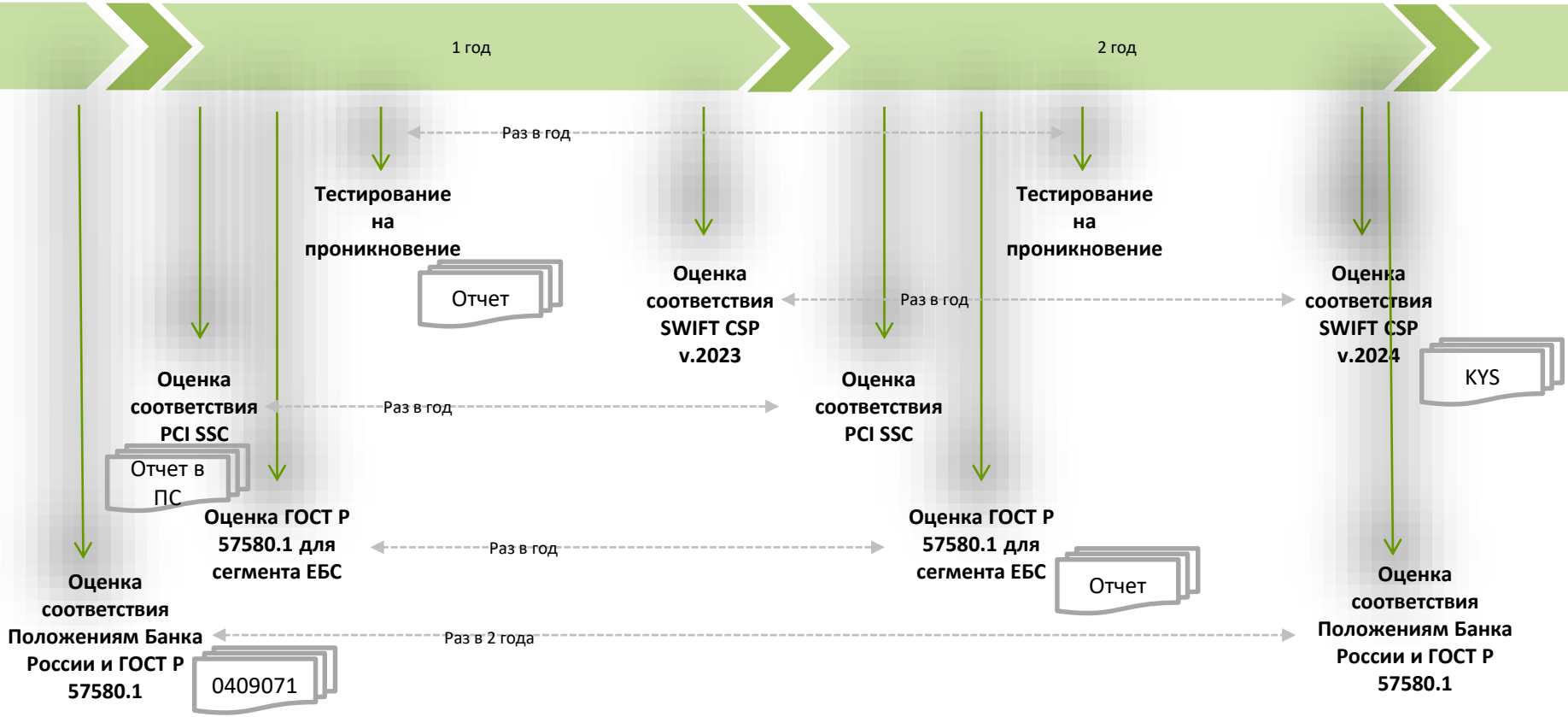
Базовый состав организационных и технических мер

Издание официальное

Москва
Российский институт стандартизации
2023

- ✓ процесс 1 «Идентификация критичной архитектуры» (детализирует требования п.6.1 Положения Банка России 787-П)
- ✓ процесс 2 «Управление изменениями» (детализирует требования п.6.2 Положения Банка России 787-П)
  - ✓ организация и выполнение процедур управления изменениями в критичной архитектуре
  - ✓ управление конфигурациями объектов информатизации
  - ✓ управление уязвимостями и обновлениями (исправлениями) объектов информатизации (**не только на уровне объектов информации, но и на уровне технологических процессов**)
- ✓ процесс 3 «Выявление, регистрация, реагирование на инциденты, связанные с реализацией информационных угроз, и восстановление после их реализации» (детализирует требования п.6.3 Положения Банка России 787-П)
- ✓ процесс 4 «Взаимодействие с поставщиками услуг» (детализирует требования п.6.4 Положения Банка России 787-П)
  - ✓ управление риском реализации информационных угроз при привлечении поставщиков услуг
  - ✓ управление риском технологической зависимости функционирования объектов информатизации финансовой организации от поставщиков услуг
- ✓ процесс 5 «Тестирование операционной надежности бизнес- и технологических процессов» (детализирует требования п.6.5 Положения Банка России 787-П)
- ✓ процесс 6 «Защита критичной архитектуры от возможной реализации информационных угроз при организации удаленной работы» (детализирует требования п.7Положения Банка России 787-П + отсылка к Процессу 8 ГОСТ Р 57580.1-2017)
- ✓ процесс 7 «Управление риском внутреннего нарушителя» (детализирует требования п.6.6 Положения Банка России 787-П)
- ✓ процесс 8 «Обеспечение осведомленности об актуальных информационных угрозах» ((детализирует требования п.6.7 Положения Банка России 787-П)

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: svintsitskii@dialognauka.ru

http://www.DialogNauka.ru