ОБЗОР ТРЕБОВАНИЙ БАНКА РОССИИ ПО ЗАЩИТЕ ИНФОРМАЦИИ

(ПОЛОЖЕНИЯ БАНКА РОССИИ, ГОСТ Р 57580.1-2017)

Антон Свинцицкий
Директор по консалтингу
АО «ДиалогНаука»

26 октября 2022 года, Москва

ДиалогНаука

Положения Банка России по защите информации

Центральный банк Российской Федерации

787-П (779-П)

716-П

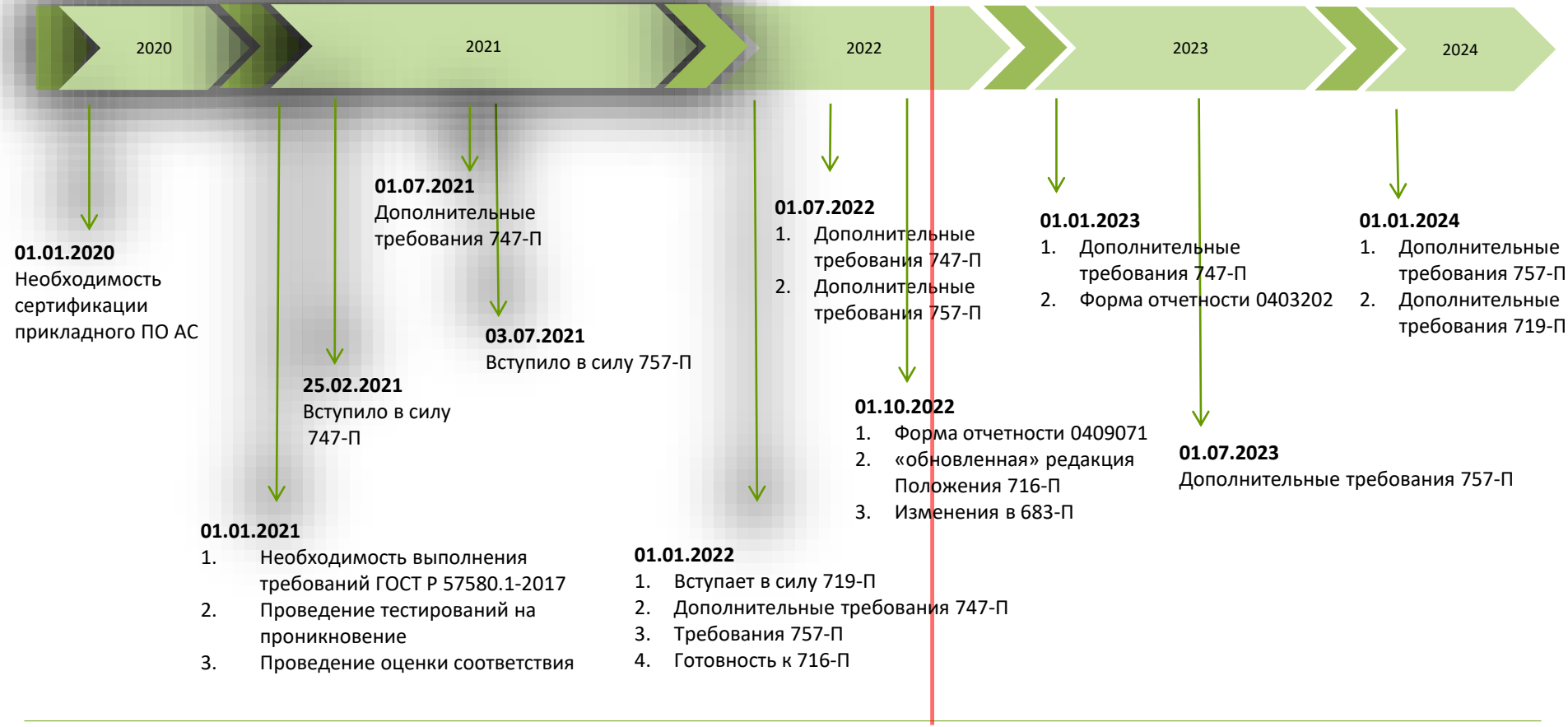
683-П

719-П

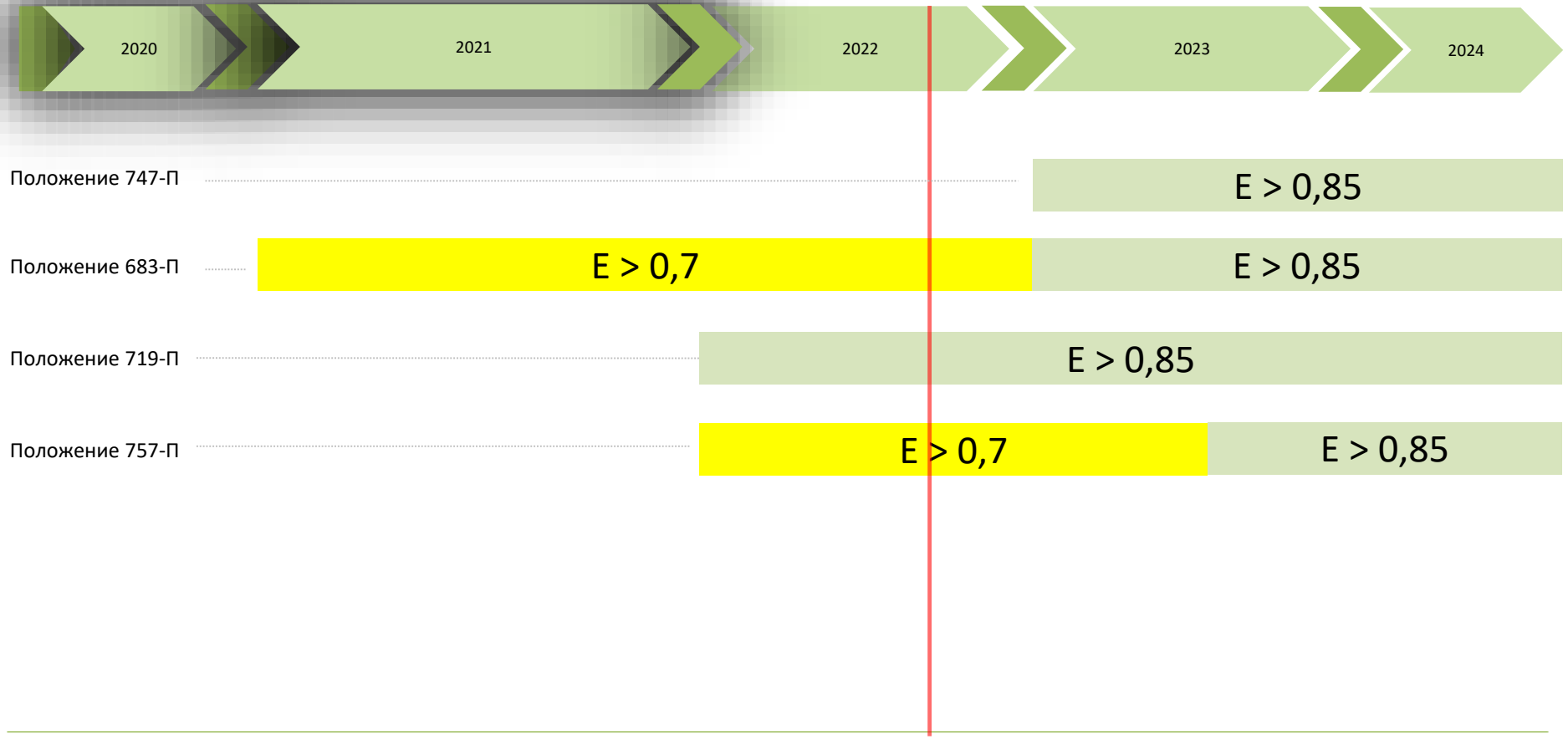
757-П

747-П

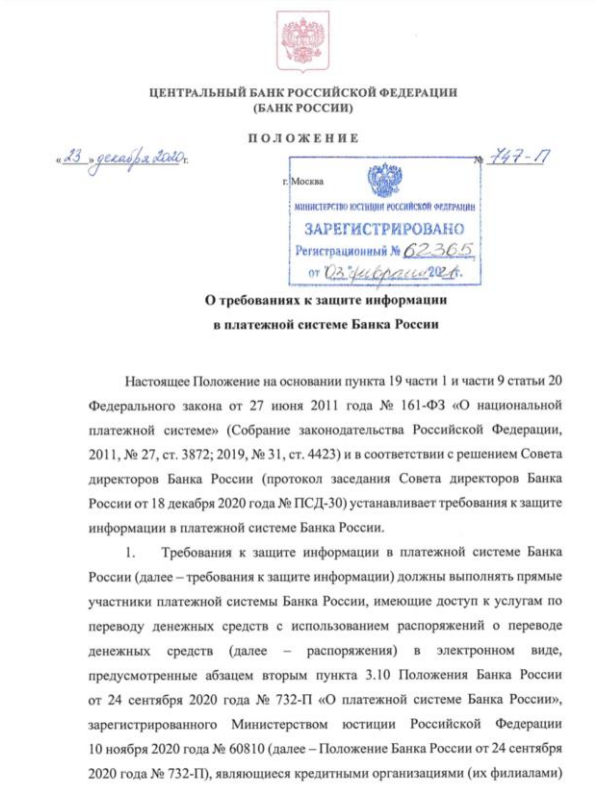
Положения Банка России по защите информации



Положения Банка России по защите информации



Положение Банка России 747-П



ЦЕНТРАЛЬНЫЙ БАНК РОССИЙСКОЙ ФЕДЕРАЦИИ
(БАНК РОССИИ)

ПОЛОЖЕНИЕ

«23» декабря 2020 г. № 747-П

г. Москва

МИНИСТЕРСТВО ЮСТИЦИИ РОССИЙСКОЙ ФЕДЕРАЦИИ
ЗАРЕГИСТРИРОВАНО
Регистрационный № 62365
от 03 февраля 2021 г.

О требованиях к защите информации в платежной системе Банка России

Настоящее Положение на основании пункта 19 части 1 и части 9 статьи 20 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) и в соответствии с решением Совета директоров Банка России (протокол заседания Совета директоров Банка России от 18 декабря 2020 года № ПСД-30) устанавливает требования к защите информации в платежной системе Банка России.

1. Требования к защите информации в платежной системе Банка России (далее – требования к защите информации) должны выполнять прямые участники платежной системы Банка России, имеющие доступ к услугам по переводу денежных средств с использованием распоряжений о переводе денежных средств (далее – распоряжения) в электронном виде, предусмотренные абзацем вторым пункта 3.10 Положения Банка России от 24 сентября 2020 года № 732-П «О платежной системе Банка России», зарегистрированного Министерством юстиции Российской Федерации 10 ноября 2020 года № 60810 (далее – Положение Банка России от 24 сентября 2020 года № 732-П), являющиеся кредитными организациями (их филиалами)

Положение Банка России от 23.12.2020 «О требованиях к защите информации в платежной системе Банка России»

- ✓ Зарегистрировано 03.02.2021
- ✓ Расширяет требования по защите информации на новые субъекты в рамках национальной платежной системы

Положение Банка России 747-П

Ключевые требования:

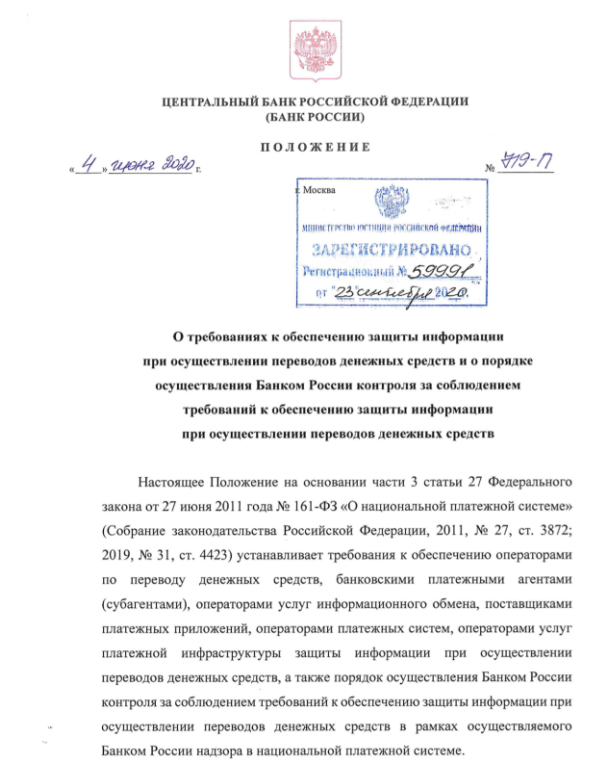
1. Выделение отдельных сегментов (не контуров!!!) для размещения объектов информационной инфраструктуры.

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 672-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



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

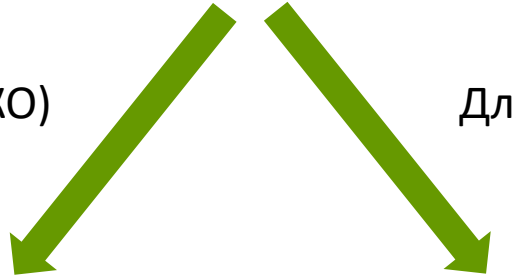
Категория субъектов НПС	Способ реализации требований для отдельных типов автоматизированных систем и приложений	
	Сертификация	Оценка соответствия по ОУД 4
Операторы по переводу денежных средств (ОПДС)	Не ниже 4 уровня доверия для системно значимых КО и КО, признанных значимыми на рынке платежных услуг 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)	+	+	+	+

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

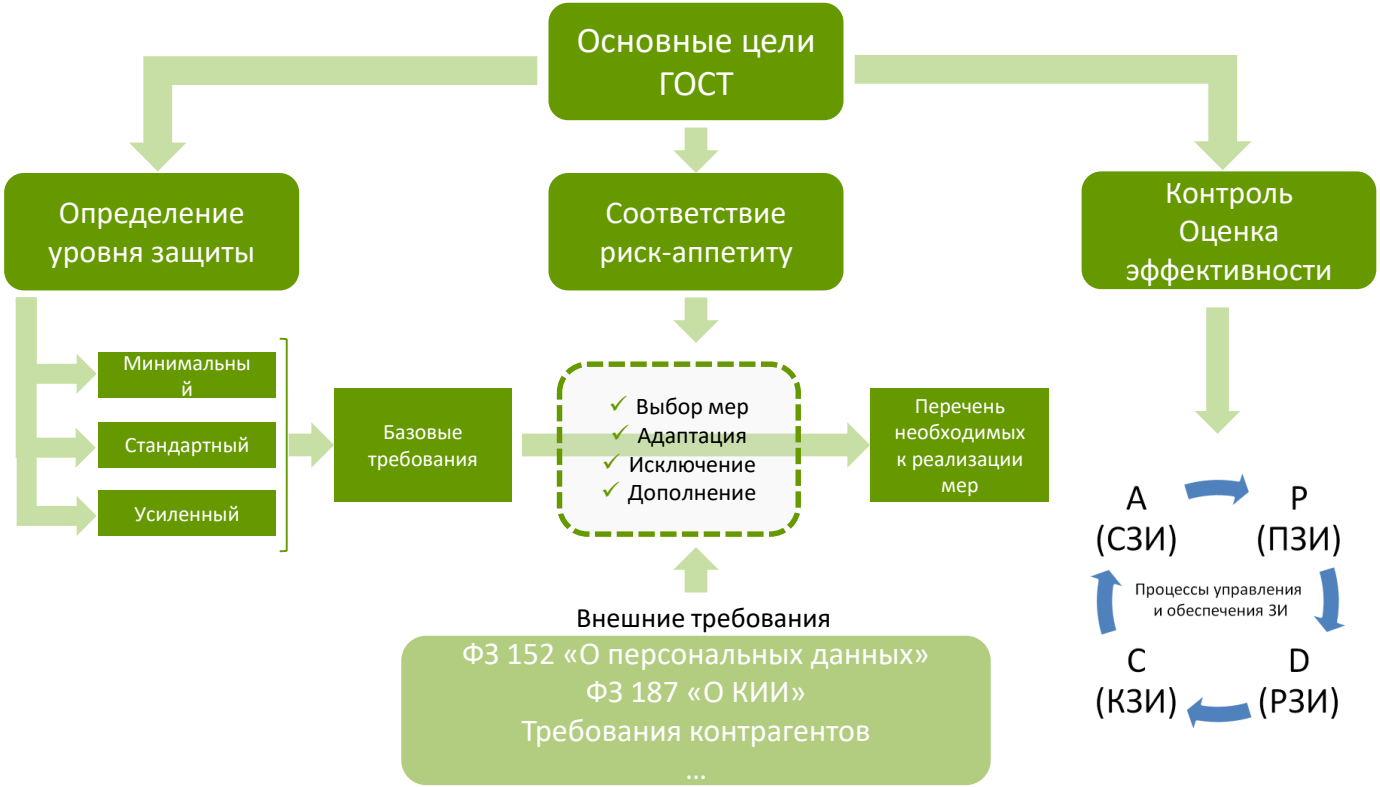
центральные контрагенты, центральный депозитарий	Усиленный
соответствующие критериям, описанным в п.5.3	Стандартный
остальные некредитные финансовые организации	Минимальный

Положение Банка России 757-П

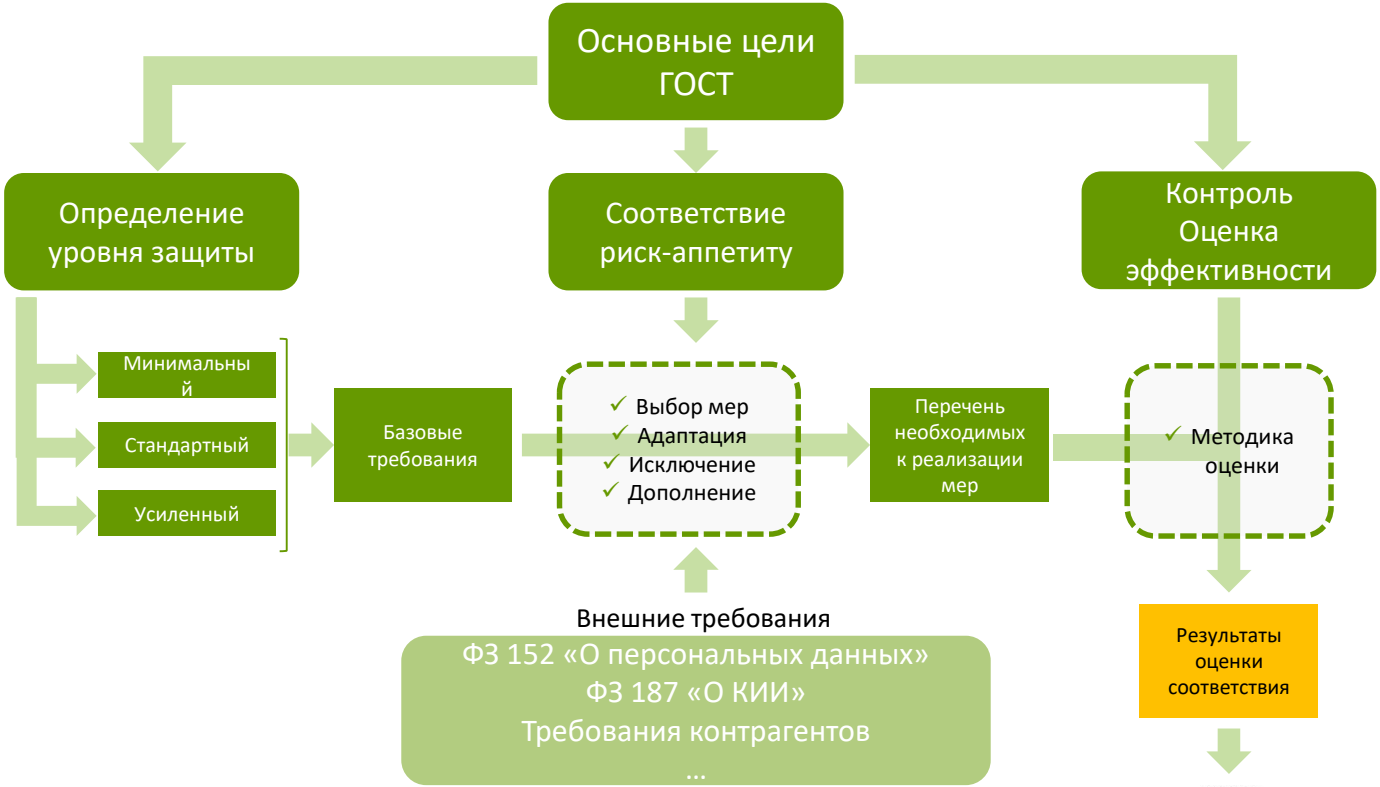
Требование	Ссылка	Период.
Проведение тестирования на проникновение	п.1.4.5 757-П ЖЦ.20 ГОСТ 57580	ежегодно
Сертификация прикладного ПО АС или оценка соответствия по ОУД 4	п.1.8 757-П	разово (а также в случаях предусмотренных выданным сертификатом)
Подписание электронных сообщений способом, позволяющим 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

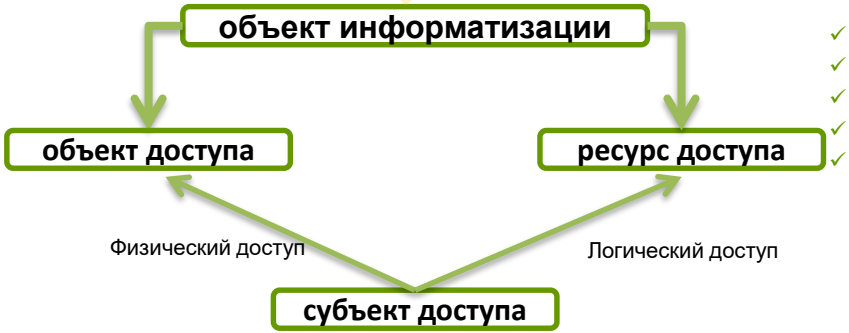
Контуры безопасности

- ✓ 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

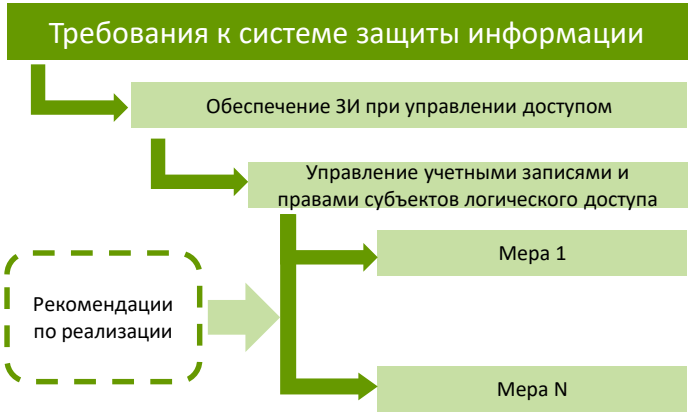
- ✓ АС
- ✓ БД
- ✓ Сетевые ресурсы
- ✓ Виртуальные машины
- ✓ Сервисы (электронная почта, WEB)

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

Контуры безопасности. Вариант 2

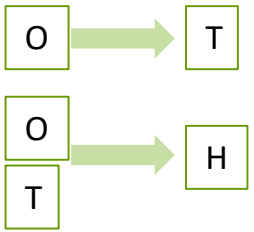
Нормативные требования	Уровень обработки информации	Тип автоматизированных систем
Положение 747-П	✓ Уровень взаимодействия с клиентами (ФЛ) ✓ Уровень взаимодействия с клиентами (ЮЛ)	✓ Системы ДБО, устанавливаемые на АРМ клиентов ✓ Системы ДБО, доступ к которым предоставляется через WEB интерфейс ✓ Системы 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

ГОСТ Р 57580.2-2018

ФЕДЕРАЛЬНОЕ АГЕНТСТВО

ПО ТЕХНИЧЕСКОМУ РЕГУЛИРОВАНИЮ И МЕТРОЛОГИИ

НАЦИОНАЛЬНЫЙ СТАНДАРТ РОССИЙСКОЙ ФЕДЕРАЦИИ

ГОСТ Р 57580.2– 2018

Безопасность финансовых (банковских) операций

ЗАЩИТА ИНФОРМАЦИИ ФИНАНСОВЫХ ОРГАНИЗАЦИЙ

Методика оценки соответствия

Издание официальное

УТВЕРЖДЕН И ВВЕДЕН В ДЕЙСТВИЕ
Приказом Федерального агентства по техническому регулированию и метрологии от 28 марта 2018 г. № 156-ст

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

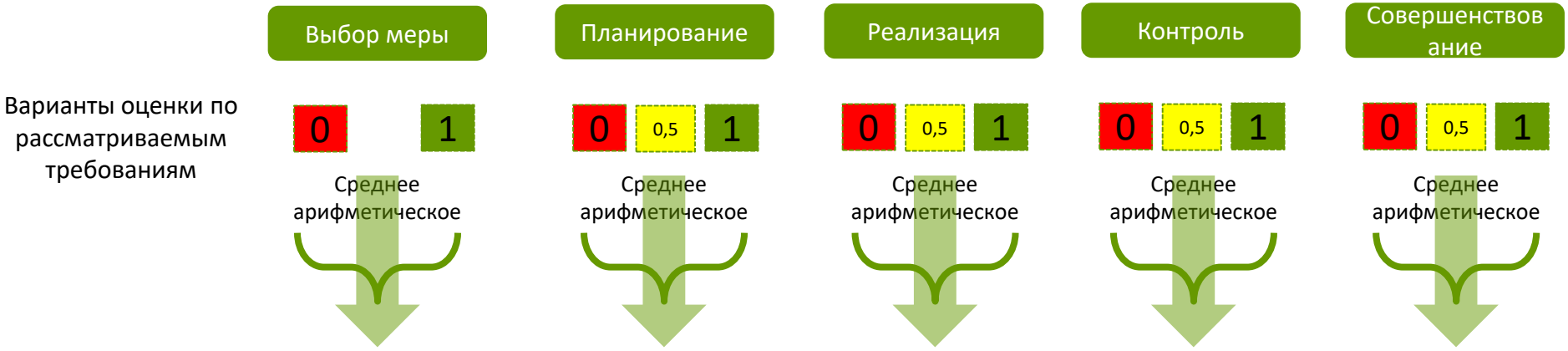
2 очередь:

- ✓ 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	

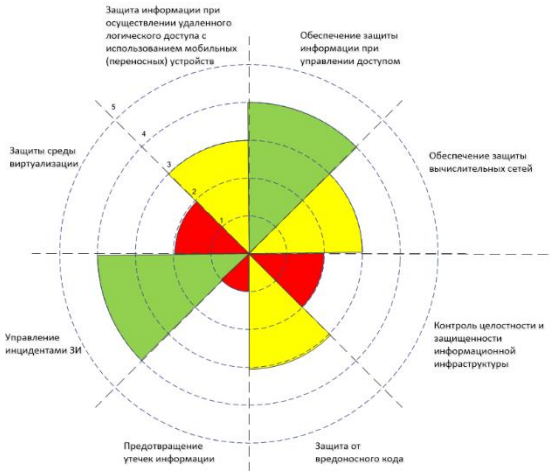
Интерпретация результатов оценки

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"

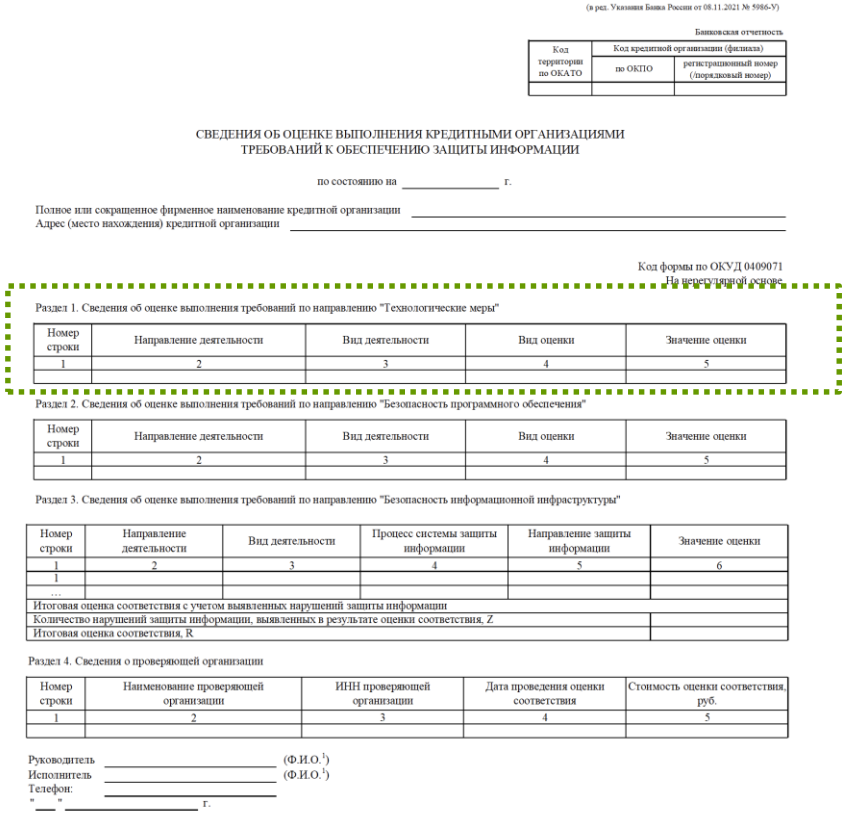
Номер строки	Направление деятельности	Вид деятельности	Процесс системы защиты информации	Направление защиты информации	Значение оценки
1	2	3	4	5	6
1					
...					
Итоговая оценка соответствия с учетом выявленных нарушений защиты информации					
Количество нарушений защиты информации, выявленных в результате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

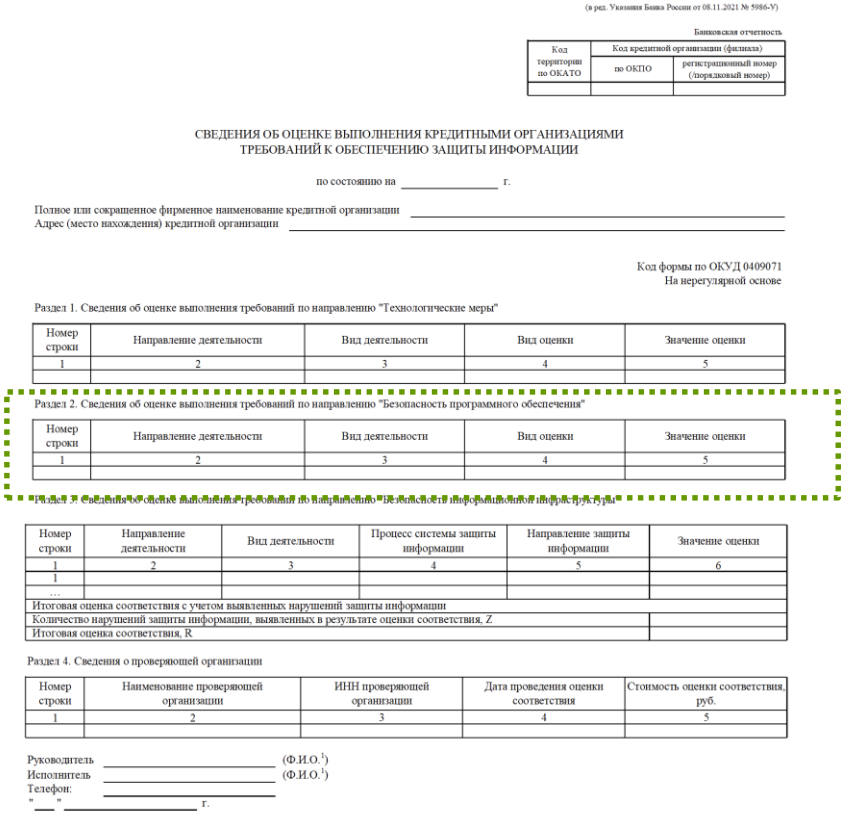
Вид деятельности (в том числе при совмещении):

- ✓ 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"

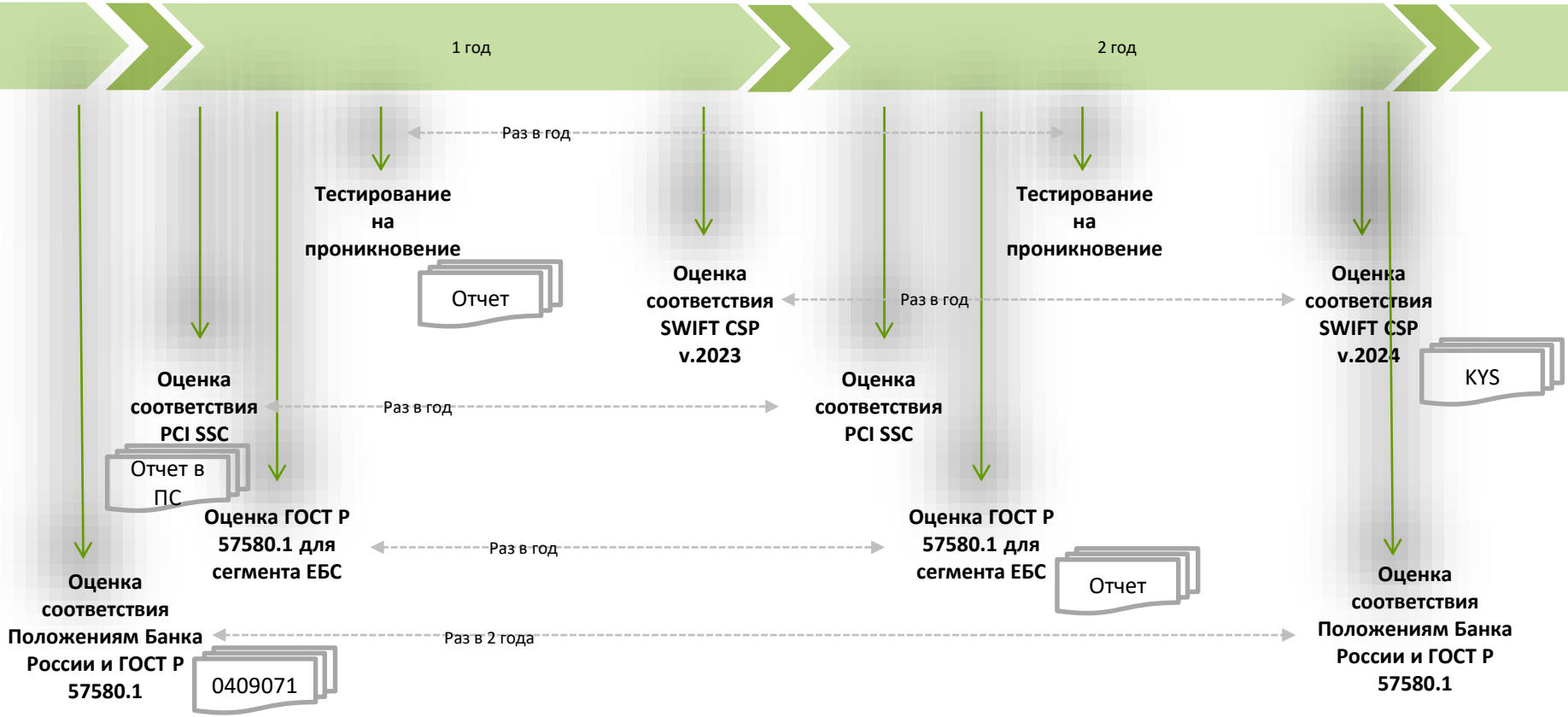
Номер строки	Направление деятельности	Вид деятельности	Процесс системы защиты информации	Направление защиты информации	Значение оценки
1	2	3	4	5	6
1					
…					
Итоговая оценка соответствия с учетом выявленных нарушений защиты информации					
Количество нарушений защиты информации, выявленных в результате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

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