СТАНДАРТИЗАЦИЯ

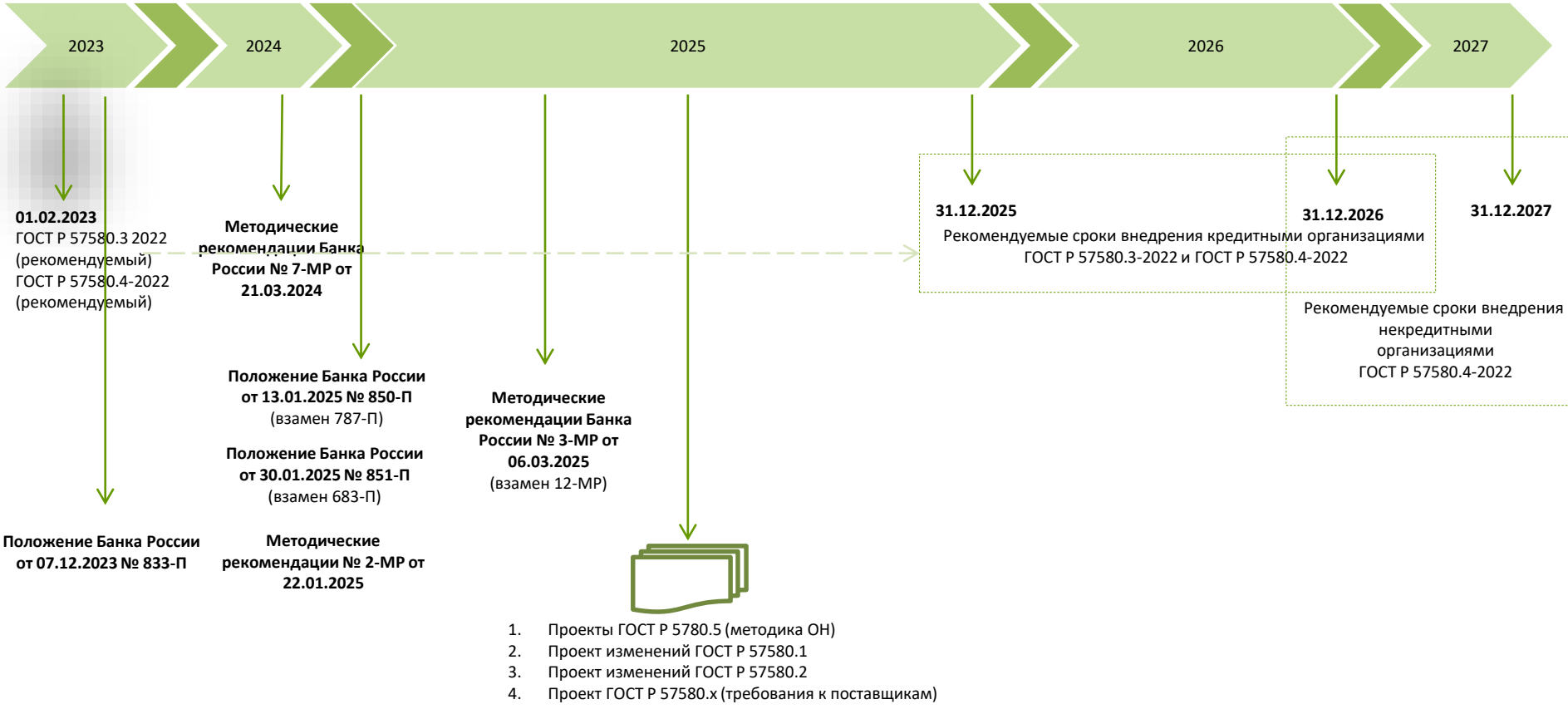
ОБЗОР ИЗМЕНЕНИЙ ТРЕБОВАНИЙ БАНКА РОССИИ ПО ЗАЩИТЕ ИНФОРМАЦИИ

Антон Свинцицкий
Директор по консалтингу
АО «ДиалогНаука»

20 мая 2025 года, Москва

ДиалогНаука

Положения Банка России

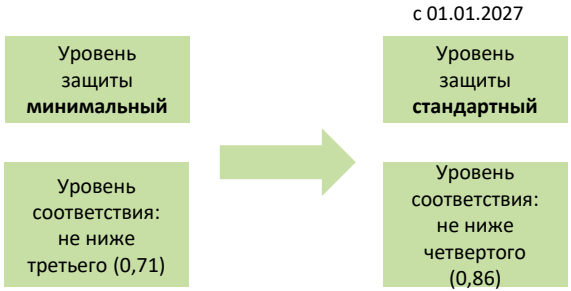


Положение Банка России 821-П. Ключевые изменения

1. Область действия Положения
2. Общие требования
3. Требования
4. Отчетность в Банк России

Новый тип субъектов:

✓ филиалы иностранных банков, осуществляющие деятельность на территории Российской Федерации



Положение Банка России 851-П. Ключевые изменения

1. Область действия Положения
2. Общие требования
3. Требования
4. Отчетность в Банк России

- ✓ в явном виде закреплена необходимость реализации цикла PDCA (Планирование – Реализация – Контроль – Совершенствование)
- ✓ к защищаемой информации в явном виде отнесена банковская тайна
- ✓ в явном виде появилось требование к сертификации / ОУД в отношении ПО при внесении изменений в исходный код (раздел 4)
- ✓ при использовании УНЭП должны применяться сертифицированные средства ЭП и УЦ

Положение Банка России 851-П. Ключевые изменения

1. Область действия Положения
2. Общие требования
3. Требования
4. Отчетность в Банк России

- ✓ при использовании УНЭП должны применяться сертифицированные средства ЭП и УЦ (п.5.1)
- ✓ контроль изменения идентификационного модуля устройства клиента (SIM-карты) (п.5.2.1)
- ✓ изменены и уточнены требования к регистрации данных о действиях клиентов и срокам их хранения (п.5.2.4, п.5.2.5)
- ✓ новое требование по ограничению по параметрам операций по приему наличных ДС (п.9)
- ✓ уведомление родителей несовершеннолетних о выданных картах и об операциях, которые дети совершают с их использованием (п.11)

Положение Банка России 851-П. Ключевые изменения

1. Область действия Положения
2. Общие требования
3. Требования
4. Отчетность в Банк России

- ✓ синхронизация с Положением Банка России 821-П в части инцидентов защиты информации и определение сроков уведомления в Приложении 2 к Положению 851-П (п.12)
- ✓ установлена периодичность проведения оценки по ГОСТ Р 57580.1, технологических мер и безопасности прикладного ПО (не реже 1 раза в 2 года) (п.13.4)
- ✓ добавлена прямая отсылка к форме отчетности 0409071 (п.13.5)

Рекомендации 3-МР. Ключевые изменения

- ✓ убраны отсылки к Положению Банка России 747-П (изменено на Положение Банка России 802-П)
- ✓ в перечень технологических мер добавлены меры из Положения Банка России 802-П, применимые к ОПКЦ СБП
- ✓ в перечень технологических мер добавлены меры из Положения Банка России 833-П (цифровой рубль)
- ✓ + редакционные правки

Проект изменений ГОСТ Р 57580.1

1. Общие требования
2. Требования к процессам защиты информации
3. Требования к PDCA-циклу

- ✓ скорректирована область применения стандарта (не только для финансовых организаций)
- ✓ Уточнены основные понятия (в том числе «Мобильное устройство»)
- ✓ Убрана отсылка к Приложению по мерам защиты ПДн (надо просто выполнять Федеральный закон «О персональных данных»)
- ✓ Скорректирован подход к выбору мер защиты информации и необходимости отражения в ВНД результатов выбора мер

Проект изменений ГОСТ Р 57580.1

1. Общие требования
2. Требования к процессам защиты информации
3. Требования к PDCA-циклу

Процесс 1

- ✓ определены требования к управлению технологическими УЗ и заданными по умолчанию УЗ
- ✓ уточнены формулировки по контролю прав доступа и контролю действий пользователей
- ✓ пароль пользователя не менее 10 символов
- ✓ использование менеджеров хранения паролей
- ✓ добавлены требования к организации резервного копирования в подпроцесс ИУ

Проект изменений ГОСТ Р 57580.1

1. Общие требования

Процесс 2

2. Требования к процессам защиты информации

3. Требования к PDCA-циклу

- ✓ уточнены требования к определению и контролю сетевого взаимодействия с сетью Интернет и использованию протоколов почтового обмена
- ✓ уточнены требования к сегменту разработки и тестирования

Проект изменений ГОСТ Р 57580.1

1. Общие требования
2. Требования к процессам защиты информации
3. Требования к PDCA-циклу

Процесс 3

- ✓ установлена необходимость определения правил выявления и устранения уязвимостей;
- ✓ добавлены ссылки на БДУ ФСТЭК России
- ✓ устранение уязвимостей разного уровня критичности (критичный, высокий, средний, низкий) оценивается независимо друг от друга

Проект изменений ГОСТ Р 57580.1

1. Общие требования
2. Требования к процессам защиты информации
3. Требования к PDCA-циклу

Процесс 4

- ✓ уточнены формулировки использования АВПО на уровне виртуальной инфраструктуры
- ✓ реализация работы АВПО в резидентном режиме на АРМ, серверах и виртуальной инфраструктуре

Проект изменений ГОСТ Р 57580.1

1. Общие требования

2. Требования к процессам защиты информации

3. Требования к PDCA-циклу

Процесс 5

- ✓ уточнены отдельные формулировки
- ✓ определена необходимость контентного анализа при передачи графических файлов (сканов, фотографий)

Проект изменений ГОСТ Р 57580.1

1. Общие требования

2. Требования к процессам защиты информации

3. Требования к PDCA-циклу

Процесс 6

- ✓ уточнены отдельные формулировки

Проект изменений ГОСТ Р 57580.1

1. Общие требования

2. Требования к процессам защиты информации

3. Требования к PDCA-циклу

Процесс 7

- ✓ уточнено название процесса защиты информации «Защита сред виртуализации и контейнеризации»
- ✓ добавлены требования по защите операционных систем с системами контейнеризации и контейнеров
- ✓ уточнены отдельные формулировки

Проект изменений ГОСТ Р 57580.1

1. Общие требования

2. Требования к процессам защиты информации

3. Требования к PDCA-циклу

Процесс 8

- ✓ уточнено название процесса защиты информации «Защита информации при осуществлении удаленного доступа»
- ✓ уточнены формулировки по сегментированию
- ✓ уточнены формулировки по требованиям к MDM-решениям
- ✓ добавлено требование к шифрованию данных на устройствах, с которых осуществляется удаленный доступ

Проект изменений ГОСТ Р 57580.2

- ✓ уточнение определения «Проверяющей организации»
- ✓ уточнение качественных уровней соответствия (от «нулевого» до «пятого»)
- ✓ уточнение понятия шкалы оценки выбора меры»:
  - 1 – мера выбрана (при предъявлении проверяющей организации свидетельств выбора в виде фактического применения)
  - 0 – мера не выбрана (при отсутствии у проверяемой организации свидетельств выбора, состояния и срока применения и порядка применения выбранных мер, отсутствия технической возможности применения меры, необоснованного превышения сроков реализации применения меры либо невозможности обеспечения в организации условий, необходимых для применения меры
- ✓ определение порядка обоснования применения компенсирующих мер
- ✓ уточнены требования к содержанию отчета (в том числе определена возможность передачи в электронном виде с УКЭП)
- ✓ определены требования к срокам передачи отчетных материалов
- ✓ уточнен перечень нарушений. Новые нарушения:
  - не проведение или некорректное проведение (без обоснования границ и модели нарушителя) тестирования на проникновение и анализа уязвимостей
  - отсутствие реализации требований к безопасности удаленного доступа, мобильных (переносных) устройств
  - выявление на момент проверки отсутствия фактов реализации выбранных (запланированных к реализации) мер ЗИ (для каждой установленной меры)
  - неустранение уязвимостей критичного и высокого уровня в установленные сроки
- ✓ уточнен порядок формирования оценки для нескольких контуров безопасности

Проект национального стандарта ГОСТ Р 57580.х

1. Область действия Стандарта
2. Требования к проверяющей организации
3. Требования к лицам, входящим в проверяющую группу
4. Требования к процессу оценки соответствия

✓ **объект стандартизации**: деятельность проверяющих организаций и процесс проведения оценки соответствия требованиям ГОСТ Р 57580.1 и иным (например, ГОСТ Р 57580.4)

Проект национального стандарта ГОСТ Р 57580.х

1. Область действия Стандарта
2. Требования к проверяющей организации
3. Требования к лицам, входящим в проверяющую группу
4. Требования к процессу оценки соответствия

- ✓ **Общие требования:**
  - ✓ нет в реестрах недобросовестных поставщиков и банкротства;
  - ✓ лицензия ТЗКИ;
  - ✓ подтверждения участия в СДС
- ✓ **Наличие документированных политик:**
  - ✓ управление риском возникновения конфликта интересов;
  - ✓ управление ресурсами;
  - ✓ повышения профессиональных навыков работников;
- ✓ **Аттестованные в рамках СДС работники, привлекаемые к оценке соответствия**
- ✓ **Требования к привлечению соисполнителей**

Проект национального стандарта ГОСТ Р 57580.х

1. Область действия Стандарта
2. Требования к проверяющей организации
3. Требования к лицам, входящим в проверяющую группу
4. Требования к процессу оценки соответствия

- ✓ **Требования к руководителям проверяющей группы**
  - ✓ образование;
  - ✓ подтверждения опыта работы
  - ✓ подтверждения квалификации по одному из национальных или международных стандартов в области информационной безопасности
- ✓ **Требования к участникам проверяющей группы**
  - ✓ образование;
- ✓ **Требования СДС (если установлены)**

Проект национального стандарта ГОСТ Р 57580.х

1. Область действия Стандарта
2. Требования к проверяющей организации
3. Требования к лицам, входящим в проверяющую группу
4. Требования к процессу оценки соответствия

- ✓ **Планирование:**
  - ✓ область оценки;
  - ✓ требования к Заказчику (ресурсы, документы и т.д.);
  - ✓ недопустимость установление целей (количественных или качественных)
- ✓ **Проведение**
  - ✓ требование к выборке;
  - ✓ обязательность включения областей, отданных на аутсорсинг (и предоставления соответствующих свидетельств);
  - ✓ хранение свидетельств (сроки и порядок)
- ✓ **Требования к отчету, содержанию и срокам хранения**

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