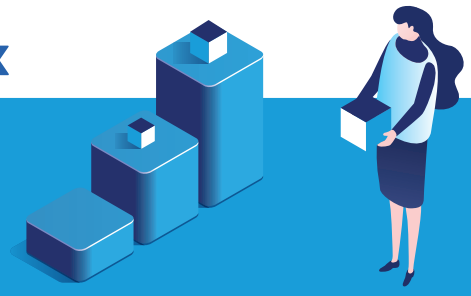
ПОЛОЖЕНИЕ №684-П. ПЛАН МЕРОПРИЯТИЙ ПО РЕАЛИЗАЦИИ ТРЕБОВАНИЙ ЦБ РФ.

8-800-333-27-53 | sale@ec-rs.ru | www.ec-rs.ru

Действует для всех



01/17 ☐

Что делать:

Предварительно определить уровень защиты информации

п. 5.1-5.3 Положения №684-п

02/17 ☐

Что делать:

Необходимо разработать и обеспечить доведение до своих клиентов рекомендаций по защите информации. Состав информации, которая должна содержаться в данных рекомендациях, указана в п.2 Положения №684-п

п. 2 Положения №684-п

03/17 ☐

Что делать:

Обеспечить работу с криптографией в соответствии с требованиями законодательства РФ

п. 3-4 Положения №684-п

04/17 ☐

Что делать:

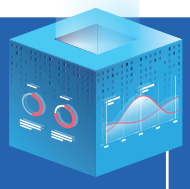
Применение мер защиты информации в соответствии с №152-ФЗ «О персональных данных»

Наш продукт:

Аудит защиты ПДн

п. 1-2 Положения №684-п

Усиленный и стандартный уровень защиты



05/17 ☐

Что делать:

Хранение информации о финансовых операциях, о регистрации данных, об инцидентах

п. 14 Положения №684-п

06/17 ☐

Что делать:

Регистрация инцидентов, связанных с нарушением требований к обеспечению ИБ

п. 13 Положения №684-п

07/17 ☐

Что делать:

Регистрация действия работников и клиентов, выполняемый с использованием ИС

п. 12 Положения №684-п

08/17 ☐

Что делать:

Информировать Банк России о выявленных инцидентах защиты информации и о планируемых мероприятиях в отношении инцидентов ИБ

п. 15 Положения №684-п

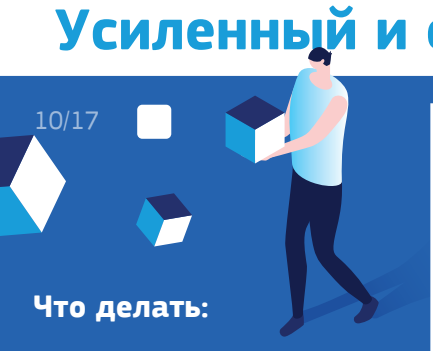
09/17 ☐

Что делать:

Регламентация, реализация, контроль (мониторинг) технологии безопасной обработки защищаемой информации

п. 11 Положения №684-п

Усиленный и стандартный уровень защиты



10/17 ☐

Что делать:

Организовать подписание электронных сообщений способом, позволяющим обеспечить их целостность и возможность подтверждения отправителя

п. 10 Положения №684-п

11/17 ☐

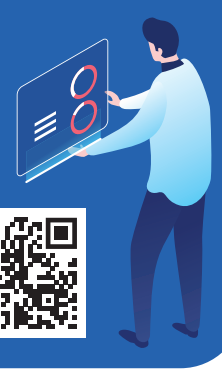
Вступает в силу: 01.01.20

Что делать:

Сертифицировать либо провести анализ уязвимости по требованиям ОУД 4:

- прикладного программного обеспечения АС и приложений, распространяемых клиентам для совершения финансовых операций;
- программного обеспечения, обрабатывающего защищаемую информацию при приеме электронных сообщений к исполнению в АС с использованием Интернет.

Наш продукт: Проведение анализа уязвимости приложений по требованиям к оценочному уровню доверия



п. 9 Положения №684-п

Кроме усиленного и стандартного уровня

12/17 ☐

Вступает в силу: 01.01.21

Что делать:

Самостоятельно определить необходимость проведения сертификации или анализа уязвимостей

п. 9 Положения №684-п

13/17

Вступает в силу: 01.01.20

Что делать:

Ежегодно проводить мероприятия по определению уровня защиты информации

п. 5.1 Положения №684-п

Усиленный и стандартный уровень защиты

14/17 ☐

01.01.21

Что делать:

Тестирование на проникновение и анализ уязвимостей объектов информационной инфраструктуры

Наш продукт: Пентест

п. 5.4 Положения №684-п

15/17 ☐

Вступает в силу: 01.01.21

Что делать:

Оценка соответствия защиты информации в соответствии с ГОСТ Р 57580.2-2018 не реже 1 раза в год для усиленного уровня защиты и не реже в 1 раза в 3 года для стандартного уровня защиты

Наш продукт: Оценка соответствия защиты информации в соответствии с ГОСТ Р 57580.2-2018

п. 6 Положения №684-п

16/17 ☐

Вступает в силу: 01.01.22

Что делать:

Обеспечение уровня соответствия системы защиты информации не ниже 3 уровня соответствия, предусмотренного подпунктом «г» пункта 6.9 ГОСТ Р 57580.2-2018

Наш продукт: Модернизация системы защиты информации

п. 8 Положения №684-п

17/17 ☐

Вступает в силу: 01.07.23

Что делать:

Обеспечение уровня соответствия системы защиты информации не ниже 4 уровня соответствия, предусмотренного подпунктом «д» пункта 6.9 ГОСТ Р 57580.2-2018

Наш продукт: Модернизация системы защиты информации

п. 8 Положения №684-п