Вебинар

Выполнение требований ЦБ РФ по информационной безопасности некредитных финансовых организаций

«ИЦ РЕГИОНАЛЬНЫЕ СИСТЕМЫ»
Умницын Михаил

Положение 684-п и его место в экосистеме нормативных актов по ИБ

Банк России
Семейство
СТО БР ИББС,
СТО БР БФБО

Банк России
684-П

«…требования к обеспечению защиты информации при осуществлении деятельности **в сфере финансовых рынков**…»

ФЗ №152
«ПДн»

ФЗ №187
«КИИ»

Регуляторы

ЦБ РФ

ФСТЭК

684-п. Основные требования

- Оценка соответствия по ГОСТ 57580.х
- Модернизация системы защиты информации (2 этапа)
- Тестирование на проникновение и анализ уязвимостей
- Сертификация или анализ уязвимостей по ОУД 4
- Применение мер по защите персональных данных
- Рекомендации для клиентов по ИБ
- Регистрация инцидентов защиты информации
- Требование ИБ к бизнес-процессам (подписание электронных сообщений ЭП, использование СКЗИ; регламентация, реализация, контроль технологии обработки информации; регистрация событий и инцидентов)

684-П. Уровни защиты.

К каким организациям применяется Положение 684-П:

Усиленный уровень защиты:
- центральные контрагенты;
- центральный депозитарий.

Стандартный уровень защиты:
- специализированные депозитарии инвестиционных фондов, паевых инвестиционных фондов и негосударственных пенсионных фондов;
- клиринговые организации;
- организаторы торговли;
- страховые организации (с условиями);
- негосударственные пенсионные фонды, осуществляющие деятельность по обязательному пенсионному страхованию;
- негосударственные пенсионные фонды, осуществляющие деятельность по негосударственному пенсионному обеспечению (с условиями);
- репозитарии;
- Брокеры (с условиями);
- Дилеры (с условиями);
- Депозитарии (в том числе расчетные депозитарии) (с условиями);
- Регистраторы (с условиями);
- Управляющие (с условиями).

?

Иные организации:
- Организации, не попадающие под требования по обороту или количеству клиентов для стандартного уровня защиты;
- Прочие организации, определенные статьей 76.1 федерального закона от 10.07.2002 № 86-ФЗ.

684-П. «Минимальный» уровень защиты.

К каким организациям применяется Положение 684-П:

В Положении 684-П в явном виде упоминаются только организации, реализующие усиленный и стандартный уровни защиты информации.
Но в п.6.7 ГОСТ 58580.1-2017 определен минимальный уровень защиты информации.

соответствии с методикой, приведенной в соответствующем национальном стандарте.
6.7 Настоящий стандарт определяет три уровня защиты информации:
- уровень 3 — минимальный;
- уровень 2 — стандартный;
- уровень 1 — усиленный.

В финансовой организации формируются один или несколько контуров безопасности

Согласно п.5.1 Положения 684-П определение уровня защиты информации должно осуществляться некредитной финансовой организацией ежегодно.

?

- Какой уровень определить «иным организациям»?
- Тогда требуется выполнять требования ГОСТ 57580.1-2017?
- Как трактовать требование п.5 Положения 684-П?

В п.6.8 ГОСТ 57580.1-2017 рекомендуется реализовывать меры защиты информации уровней защиты информации для обеспечения выполнения требований к защите персональных данных в ИСПДн.

Минимальный уровень	↔	УЗ-4
Стандартный уровень	↔	УЗ-3, УЗ-2
Усиленный уровень	↔	УЗ-1

?

- Моей организации нет п.5.2 и п.5.3 Положения 684-П, но у меня свыше 100000 клиентов! Какой уровень защиты информации определить?

684-п. Основные требования

Что обязаны выполнять все организации, независимо от уровня защиты информации:

- Осуществление защиты информации, обрабатываемой в АС (п.1).
- Разработка и доведение до клиентов рекомендаций по защите информации (п.2);
- Обеспечение защиты информации с помощью СКЗИ, в т.ч. ПДн (п.3, п.4);
- Ежегодно определять уровень защиты (п.5.1).

Что обязаны выполнять организации, реализующие стандартный и усиленный уровень:

- Провести тестирование на проникновение и анализ уязвимостей информационной безопасности объектов информационной инфраструктуры (п.5.4).
- Оценка определенного уровня защиты информации (оценка соответствия), обеспечение хранения отчета об оценке соответствия (п.6, п.7);
- Обеспечить уровень соответствия не ниже третьего / четвертого уровня соответствия защиты информации (п.8);
- Сертификация или анализ уязвимостей по требования к ОУД, не ниже чем ОУД4 для ПО (п.9);
- Выполнить требования к Технология обработки защищаемой информации (п.10 – п.12);
- Осуществлять регистрацию инцидентов защиты информации, обеспечить хранение сведений об инцидентах, производить информирование Банка России об инцидентах (п.13 – п.14).

Анализ уязвимостей по требованиям к ОУД 4 (п. 9)

Вступил в силу, но ЦБ не штрафует до 01 июля 2021.
Информационное письмо от 14 мая 2020 г. № ИН-014-56/88

Что делать

Сертифицировать или
провести анализ 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.

Состав работ

Подготовка стенда, развертывание ПО

Оценка уязвимостей программного обеспечения

Функциональное, статическое, динамическое тестирование, тестирование на проникновение

Оценка документации (на ПО, организации процесса разработки, тестирования и т.д.)

! Для анализа нужно подготовить очень большой объем документации

Какие документы необходимы для успешного прохождения ОУД

Что передается Оценщику в электронном виде:

- Инсталляционная версия программного обеспечения;
- Исходный код программного обеспечения ;
- Программные утилиты, используемые для компиляции программного обеспечения из исходных текстов программных модулей.

Что передается Оценщику в электронном или печатном виде:

- Сведения о программном обеспечении;
- Проектная документация;
- Эксплуатационная документация;
- Дополнительная документация, содержащая сведения о ПО;
- Документация по безопасной разработке.

Документы должны быть оформлены официально, с указанием версии, регистрационного номера и датой утверждения каждого из документов.

Что дополнительно надо учесть при разработке:

- Методический документ «Профиль защиты прикладного программного обеспечения автоматизированных систем и приложений кредитных организаций и некредитных финансовых организаций».

! Данный документ до сих пор находится в стадии проекта в ТК 122 и может претерпеть изменения!

Какие сложности при прохождении ОУД:

- Отсутствует документация на программное обеспечение;
- Отсутствует документация по безопасной разработке;
- Сложность получения исходного кода (заявитель на анализ уязвимостей не является разработчиком ПО).

! Общий вердикт по анализу уязвимостей «положительный тогда и только тогда, когда все составляющие вердикта положительные»! (ГОСТ Р ИСО/МЭК 18045-2013, п.7.2.5.)

Какие документы необходимы для успешного прохождения ОУД

Документация на программное обеспечение:

- Описания объекта оценки;
- Функциональная спецификация;
- Задание по безопасности;
- Руководство пользователя;
- Руководство администратора;
- Формуляр;
- Технические условия;
- Регламент передачи ПО пользователю;
- Регламент отслеживания и исправления обнаруженных ошибок ПО и уязвимостей программы;
- Регламент приема и обработки сообщений от пользователей об ошибках ПО и уязвимостях программы;
- Регламента доведения до пользователей информации об уязвимости программы и рекомендаций по их устранению;
- Регламент управления конфигурацией;
- Регламента регистрации событий изменений конфигурации ПО;
- Регламент экстренного выпуска обновлений ПО;
- Регламент маркировки версий ПО;
- Журнала регистрации изменений конфигурации ПО;
- Журнал ошибок и уязвимостей программы;
- Регламента поддержки жизненного цикла; Описание архитектуры безопасности;
- Регламент и протоколы тестирования программы;
- Регламент и протоколы экспертизы исходного кода программы;
- Регламент и протоколы тестирования на проникновение;
- Регламент, протоколы, журналы поиска уязвимостей программы;
- Отчет по анализу уязвимостей и тестированию на проникновение.

Документация по реализации процесса безопасной разработки:

- Руководство по разработке безопасного ПО;
- Перечень инструментальных средств разработки ПО;
- Порядок оформления исходного кода программы;
- Регламент защиты инфраструктуры среды разработки ПО;
- Программа обучения сотрудников в области разработки безопасного ПО;
- Журнал обучения сотрудников в области разработки безопасного ПО.

Требования к документам

- ГОСТ ИСО/МЭК 15408: Общие критерии.
- ГОСТ ИСО/МЭК 15408-1: Введение и общая модель.
- ГОСТ ИСО/МЭК 15408-2: Функциональные компоненты безопасности.
- ГОСТ ИСО/МЭК 15408-3: Компоненты доверия к безопасности.
- ГОСТ ИСО/МЭК 18045: Методология оценки.
- ГОСТ Р 58142: Использование источников для идентификации уязвимостей.
- ГОСТ Р 56545: Правила описания уязвимостей.
- ГОСТ Р 56546: Классификация уязвимостей.
- ГОСТ Р 58143: Тестирование проникновения.
- ГОСТ ИСО/МЭК ТО 20004: Уточнённый анализ уязвимости программного обеспечения.
- ГОСТ Р 57628-2017: Руководство по разработке профилей защиты и заданий по безопасности.
- ГОСТ Р 56939-2016 Защита информации. Разработка безопасного программного обеспечения. Общие требования.
- ГОСТ Р 58412-2019 Защита информации. Разработка безопасного программного обеспечения. Угрозы безопасности информации при разработке программного обеспечения.
- ГОСТ 19.501-78 Единая система программной документации (ЕСПД). Формуляр. Требования к содержанию и оформлению.
- ГОСТ 2.114-2016 «Единая система конструкторской документации (ЕСКД). Технические условия».
- ГОСТ Р 56920-2016/ISO/IEC/IEEE 29119-1:2013 Системная и программная инженерия. Тестирование программного обеспечения. Часть 1. Понятия и определения.
- ГОСТ Р 56921-2016/ISO/IEC/IEEE 29119-2:2013 Системная и программная инженерия. Тестирование программного обеспечения. Часть 2. Процессы тестирования.
- ГОСТ Р 56922-2016/ISO/IEC/IEEE 29119-3:2013 Системная и программная инженерия. Тестирование программного обеспечения. Часть 3. Документация тестирования.
- ГОСТ Р ИСО 10007 Менеджмент организации. Руководящие указания по управлению конфигурацией.
- ГОСТ Р ИСО/МЭК 12207 Информационная технология. Системная и программная инженерия. Процессы жизненного цикла программных средств.

! Перечень документов, который необходимо изучить при самостоятельной разработки документации.

Реальный кейс. ОУД-4

Исходные данные:	Анализ уязвимостей по требованиям к ОУД	Разработка проектов документов и консультации по заполнению	Общая длительность работ
1 ПО **2 языка ПО** **~ 500 000 строк кода**	Стоимость услуг: **1,9 млн. руб.** Длительность работ: **90 дней**	Стоимость услуг: **1,6 млн. руб.** Длительность работ: **100 дней**	**~ 120-140 дней**

Оценка соответствия уровню защиты информации (п. 6)

Что делать

Не реже **одного раза в 3 года** для некредитных организаций реализующих **стандартный уровень**, не реже **одного раза в год** для некредитных организаций реализующих **усиленный уровень** защиты проводить оценку соответствия уровню защиты информации **для объектов информационной инфраструктуры** с привлечением лицензированной организации.

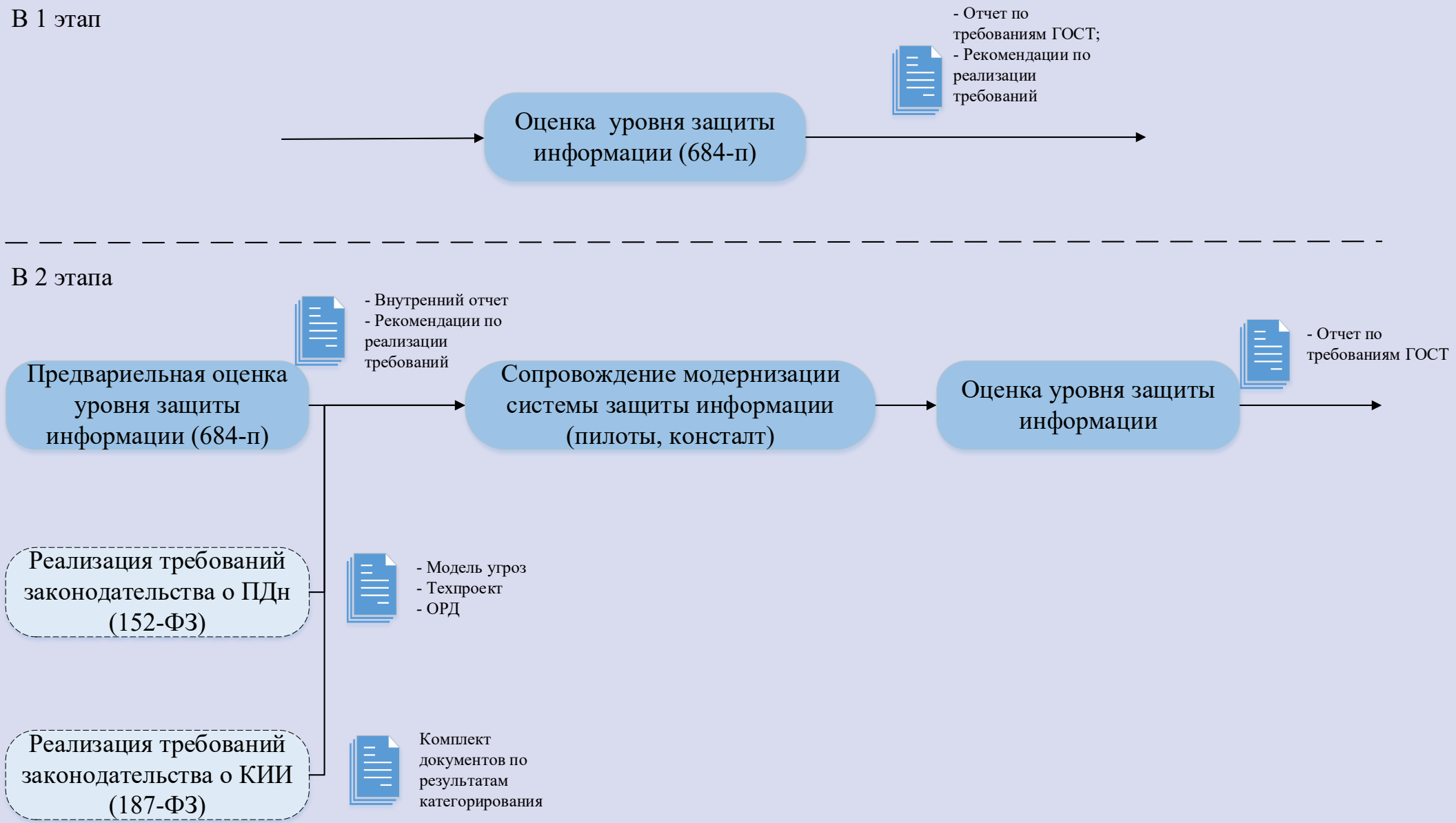
Почему оценку соответствия нужно проводить сейчас, а не в следующем году

Система защиты информации некредитной финансовой организации должна обеспечивать 3 уровень соответствия уже с **01.01.2022 г.** Поэтому, необходимо уже сейчас понимать текущую оценку и планировать мероприятия по модернизации системы защиты.

Что мы предлагаем

Оценка уровня защиты информации в соответствии с ГОСТ Р 57580.2-2018

Этапы оценки соответствия уровню защиты информации (п. 6)



Результаты оценки соответствия уровня защищенности (п.6)

Требования ГОСТ:

Текущая оценка соответствия

Отчет об оценке, уровня защиты информации по требованиям ГОСТ

Внутренний отчет (дополнительно) включает в себя:

Предложения по корректировке ОРД Заказчика

Различные варианты модернизации системы защиты информации по требованиям Положения 684-п по этапам (с указанием стоимости):

- с учётом числового значения оценки соответствия каждого типа СрЗИ.
- с учетом различных производителей СрЗИ.

Реальные кейсы. Оценка соответствия

1

1 контур

11 филиалов

Оценка соответствия:

Стоимость услуг – **800 тыс. руб**.

Длительность работ **– 50 дней.**

2

1 контур

7 филиалов

Оценка в 2 этапа

Оценка соответствия:

Стоимость услуг – **1,2 млн. руб.**

Длительность работ **– 196 дней.**

Модернизация системы защиты информации

! План и оценку мы делаем в рамках оценки соответствия

Что делать

Некредитная организация должна обеспечить уровень соответствия уровню защиты информации:

- не ниже 3-го с 1 января 2022 г.
- не ниже 4-го с 1 июля 2023 г.

Состав работ

- План модернизации системы защиты информации
- Оценка стоимости системы защиты информации
- Запуск процессов бюджетирования
- Пилотирование отдельных решений по ИБ (при необходимости)
- Модернизация системы защиты информации до 3го уровня соответствия
- Модернизация системы защиты информации до 4го уровня соответствия

Реальный кейс

70 сотрудников

11 филиалов

1 ЦОД

1 AD-домен

МЭ с IDS/IPS, AppControl, без AV

AV-Endpoint решения (АРМ, сервера), AV-Mail.

Виртуализация с централизованным управлением

VPN (ГОСТ VPN)

Средства инвентаризации и мониторинга

Исходный бал: 0,645

1

ЭТАП (3й уровень соответствия)

- Настройка существующих СрЗИ;
- SIEM;
- Покупка лицензий AV на МЭ;

Выходной бал по результатам этапа: + 0,081 (Итого: 0,726)

Стоимость реализации мер ~ 8,5 млн. руб.

2

ЭТАП (4й уровень соответствия)

- DLP;
- Корректировка ОРД.
- Контроль привилегированных пользователей;

Выходной бал по результатам этапа: + 0,156 (Итого: 0,882)

Стоимость реализации мер ~ 10 млн. руб.

Тестирование на проникновение и анализ уязвимостей (п.5.4)

С 01 января 2021 г.

Что делать

Проводить тестирование на проникновение и анализ уязвимостей информационной безопасности объектов информационной инфраструктуры.

Что мы предлагаем

Тестирование на проникновение ИТ инфраструктуры согласно рекомендациям ЦБ РФ

На что обратить внимание

Положение 684-П не определяет «Что включить в состав подлежащих тестированию объектов и как проводить тестирование на проникновение?». Но рекомендуется обратить внимание на **Приложение 3 нормативного документа «**РС БР ИББС-2.6-2014».

Реализация мер по защите персональных данных (п. 1)

Вступил в силу!

Что делать

Некредитные организации должны применять меры по обеспечению безопасности персональных данных

Что мы предлагаем

- Аудит на соответствие требованиям
- Разработка модели угроз и нарушителя
- Разработка организационно-распорядительной документации
- Разработка технического проекта на ИСПДн
- Аттестационные испытания
- Внедрение системы защиты персональных данных

684-п. План на 2020 год

№ п/п	Мероприятие	Рекомендуемый срок	Требование ЦБ	Примечание
1	Анализ уязвимостей ПО по требованиям ОУД4	Заключение договора в ближайшее время	Январь 2020	Санкции за несоблюдение с 01 июля 2021
2	(Предварительная) оценка соответствия	Июнь – Август 2020	-	Понять текущий уровень защиты
3	Модернизация технических средств защиты	Июнь – Декабрь 2020	-	Цель - выйти на 3 уровень соответствия к 01.01.2022 г.
4	Корректировка ОРД			
5	Тестирование на проникновение	Декабрь 2020	Январь 2021	
6	Применение мер по защите ПДн	Аудит ПДн с июня 2020	Апрель 2019	
7	Оценка соответствия	Ноябрь – Декабрь 2020	Январь 2021	Полноценная оценка по требованиям ГОСТ

Инфографика

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 дов
до своих клиентов рекомендаций по защит
информации. Состав информации, которая
содержаться в данных рекомендациях, ука
п.2 Положения №684-п

п. 2 Положения №684-п

Усиленный и стандартный уровен

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 И

п. 12 Положения №684-п

Спасибо за внимание!

Региональные системы
Инжиниринговый центр

+7 (800) 333 27 53

resp@ec-rs.ru

www.ec-rs.ru