Приложение

**Вопросы кредитных организаций:**

1. Требуется ли при выполнении процедур оценки соответствия ГОСТ Р 57580.1 оценивать только выполнение базовых мер защиты информации, описанных в ГОСТ Р 57580.1? Следует ли при проведении оценки учитывать дополнительные меры защиты информации, применяемые в организации в соответствии с пунктом 6.3 ГОСТ Р 57580.1?
2. Пункт 1.1 Приложения 1 к Положению № 672-П[[1]](#footnote-1) требует от участника сервиса срочного перевода и сервиса несрочного перевода (ССНП) привлечения отдельных работников для каждого из двух контуров: контура формирования электронных сообщений и контура контроля реквизитов. Это требование определено мерой УЗП.19 (пункт 7.2.1.3 ГОСТ Р 57580.1**)**. Допустимо ли при определенных условиях совмещение одним работником функционала обоих контуров, например:
* при работе в разных сменах в разных контурах;
* при реализации в ролевой модели автоматизированной системы запрета на выполнение функции контроля для электронных сообщений, созданных этим же работником?
1. Какое количество сотрудников необходимо для реализации требования, указанного в УЗП.21 (пункт 7.2.1.3 ГОСТ Р 57580.1)?
2. В пунктах 7.3 и 7.4 ГОСТ Р 57580.1 содержатся требования к процессу разработки, а также к разделению сред разработки и тестирования программного обеспечения. Должны ли в область применимости ГОСТ Р 57580.1 включаться АРМ разработчиков в случае, если организация сама разрабатывает для себя программное обеспечение?
3. Какое программное обеспечение обеспечивает возможности, требуемые в ЦЗИ.7-ЦЗИ.10 (пункт 7.4.2 ГОСТ Р 57580.1)?
4. В пункт 7.9 ГОСТ Р 57580.1 включены требования по обеспечению безопасности при удаленном доступе с использованием мобильных устройств. Какие требования применимы к компьютерам и ноутбукам, с которых осуществляется удаленный доступ? Должны ли эти ноутбуки включаться в область применимости стандарта ГОСТ Р 57580.1? Считается ли доступ к корпоративной почте с мобильного телефона удаленным доступом, для которого требуется выполнять меры защиты, определенные пунктом 7.9 ГОСТ Р 57580.1?
5. Обязательно ли для кредитной организации выполнение требований Положения № 684-П, если в ней есть подразделение, осуществляющее деятельность в сфере финансовых рынков с соответствующей лицензией (специализированный депозитарий, брокер, дилер и др.), не являющееся отдельным юридическим лицом и использующее объекты информационной инфраструктуры кредитной организации?

При этом кредитная организация, следуя нормам Положений № 683-П и № 684-П, дублирует функции по информированию об инцидентах и проведению периодической оценки уровня информационной безопасности с привлечением сторонних организаций. Кроме того, возникает ситуация неопределенности в части формирования отчетов по оценке соответствия положениям ГОСТ Р 57580.1:

* возможно ли формирование разных независимых отчетов по Положениям № 683-П и № 684-П?
* какой уровень защиты информации должен выполнятся по Положению № 684-П, если по Положению № 683-П кредитная организация реализует усиленный уровень защиты информации?
1. Возможно ли использование персональных ноутбуков работников организации, которые в нерабочее время находятся вне контроля организации? Например, при условии предварительной проверки мер защиты ноутбука перед подключением к безопасному контуру?
2. Что считать финансовыми операциями согласно Положению № 684-П? Будет ли считаться выплата заработной платы сотрудникам страховой компании финансовой операцией?
3. Требование пункта 10 Положения № 684-П по обеспечению контроля целостности электронного сообщения имеет отношение только к финансовым операциям?
4. Страховая компания принимает платежи за полисы в общедоступном веб-приложении у себя на сайте. Непосредственно за прием платежа отвечает эквайринговая система банка-партнера. Клиент перенаправляется на нее, проводит платеж, затем возвращается обратно в веб-приложение страховой компании. Будет ли это веб-приложение обрабатывать финансовые операции, и будет ли оно подлежать анализу на уязвимости по ОУД4 (или сертификации ФСТЭК России), если фактически платежами занимается банк-партнер?
1. Положение Банка России от 09.01.2019 № 672*-*П «О требованиях к защите информации в платежной системе Банка России». [↑](#footnote-ref-1)