**Приложение**

**Вопросы кредитных организаций по реализации положений ГОСТ Р 57580.1-2017 «Безопасность финансовых (банковских) операций. Защита информации финансовых организаций. Базовый состав организационных и технических мер» (далее – ГОСТ Р 57580.1) и ГОСТ Р 57580.2-2018 «Безопасность финансовых (банковских) операций. Защита информации финансовых организаций. Методика оценки соответствия» (далее – ГОСТ Р 57580.2)**

1. Пункт 6.4 ГОСТ Р 57580.1 определяет возможность применения компенсирующих мер защиты информации в связи с невозможностью технической реализации и (или) экономической целесообразностью:
* каковы критерии оценки экономической целесообразности реализации мер, определенных ГОСТ Р 57580.1?
* могут ли в качестве причин невозможности технической реализации меры рассматриваться: отсутствие на рынке технических решений российского производства, обеспечивающих необходимую эффективность и функциональность; возможные западные санкции и опасность/невозможность использования решений иностранных производителей?
* можно ли в связи с невозможностью технической реализации и (или) экономической целесообразностью вместо технической меры реализовывать организационную меру/меры?
1. Что подразумевается под хранением эталонной информации о предоставленных правах логического доступа и обеспечением целостности указанной информации (пункт 7.2.1.3 ГОСТ Р 57580.1)? Это таблица в MS Excel или что-то другое?
2. Как правильно организовать установление фактов неиспользования субъектами логического доступа предоставленных им прав на осуществление логического доступа на протяжении периода времени (пункт 7.2.1.3 ГОСТ Р 57580.1)? Теоретически можно проверять учетные записи по дате последнего входа в систему, но проверить неиспользование доступов, скорее всего, получится только из логов системы. Реализация данной процедуры вручную слишком трудоемкая. Как Банк России рекомендует реализовать данный вид проверки на практике?
3. Подразумевает ли мера РД.4 (пункт 7.2.2.2 ГОСТ Р 57580.1), что многофакторная аутентификация администраторов должна быть реализована на всех объектах доступа в рамках контура защиты, включая сетевое оборудование, банкоматы и платежные терминалы, а также все применяемые технические меры защиты (антивирусные средства, прокси-серверы, SIEM-системы, DLP-системы, системы резервного копирования информации т.д.)?
4. Каким образом необходимо реализовывать меру РД.6 (пункт 7.2.2.2 ГОСТ Р 57580.1):
* какими средствами можно реализовать аутентификацию АРМ эксплуатационного персонала?
* должна ли обеспечиваться аутентификация АРМ администраторов всех объектов доступа, включая применяемые технические меры защиты (антивирусные средства, прокси-серверы, SIEM-системы, DLP-системы, системы резервного копирования информации т.д.), или данное требование распространяется только на АРМ администраторов ресурсов доступа?
1. Что подразумевается под использованием на АРМ субъектов логического доступа встроенных механизмов контроля изменения базовой конфигурации оборудования (пункт 7.2.2.2 ГОСТ Р 57580.1)? Имеется в виду пароль на CMOS, опечатывание системных блоков и составление паспорта на АРМ с описанием того, что входит в конфигурацию? Что делать, если в организации используются преимущественно «тонкие клиенты»?
2. Как следует организовать хранение копий аутентификационных данных эксплуатационного персонала (пункт 7.2.2.3 ГОСТ Р 57580.1): на выделенных МНИ или на бумажных носителях? Необходимо хранить связку логин-пароль в таблице (или только логин), ФИО, должность и т.п.? Можно ли хранить данную информацию в зашифрованном виде в сети (например, с помощью ПО «KeePass Password Safe») или это уже будет считаться нарушением?
3. Что подразумевается под регистрацией персонификации, выдачи (передачи) и уничтожения персональных технических устройств аутентификации (пункт 7.2.2.3 ГОСТ Р 57580.1)? Имеются в виду токены для входа в систему? Если организация их не использует, то нужен ли подобный учет в виде пустого журнала на бумажном носителе или достаточно в документации по информационной безопасности написать, что данный учет не ведется, поскольку нет необходимости?
4. Как правильно организовать контроль перечня лиц, которым предоставлено право самостоятельного физического доступа в помещения (пункт 7.2.3.2 ГОСТ Р 57580.1)? Как рекомендуется это реализовать, если у организации нет своего СКУД, доступ в помещение контролируется на уровне арендодателя? Необходимо ли учитывать заявки на предоставление доступа? Как контролировать доступ в помещение организации представителей самого арендодателя и технических служб? Технические специалисты управляющей компании имеют свободный вход на этаж организации в технические помещения, которые принадлежат арендодателю. Кроме того, по ночам совершается обход помещений организации сотрудниками охраны управляющей компании.
5. Может ли мера ИУ.1 (пункт 7.2.4.2 ГОСТ Р 57580.1) быть реализована посредством применения системы управления заявками на доступ, позволяющей вести учет ресурсов доступа, к которым в соответствии с установленной процедурой пользователи могут запрашивать доступ?
6. Какими техническими средствами (класс решений) можно контролировать фактический состав созданных, используемых и (или) эксплуатируемых ресурсов доступа (баз данных, сетевых файловых ресурсов, виртуальных машин) и их корректное размещение в сегментах вычислительных сетей организации (мера ИУ.4, пункт 7.2.4.2 ГОСТ Р 57580.1)?
7. Какими техническими средствами (класс решений) можно контролировать создание и удаление ресурсов доступа (мера ИУ.5, пункт 7.2.4.2 ГОСТ Р 57580.1)?
8. На предмет чего должно контролироваться содержимое информации при ее переносе из сегментов или в сегменты контуров безопасности с использованием переносных (отчуждаемых) носителей информации (мера СМЭ.13, пункт 7.3.1.2 ГОСТ Р 57580.1)?
9. Какими техническими средствами может быть реализована мера СМЭ.14 (пункт 7.3.1.3 ГОСТ Р 57580.1)?  Достаточно ли будет применения межсетевого экрана или маршрутизатора на границе сети организации и сети Интернет?
10. Что подразумевается под обеспечением возможности восстановления эталонных копий ПО АС, ПО средств и систем защиты информации, системного ПО в случаях нештатных ситуаций (пункт 7.4.3 ГОСТ Р 57580.1)? Имеется в виду восстановление из резервных копий?
11. Что подразумевается под требованием ЦЗИ.26 (пункт 7.4.4 ГОСТ Р 57580.1, контроль (выявление) использования технологии мобильного кода)? Нужно запрещать такой код? Или вести списки разрешенных приложений? Или достаточно фиксировать использование?
12. Будет ли считаться, что мера ЗВК.19 (пункт 7.5.3 ГОСТ Р 57580.1) реализована, если мобильные устройства запрещено подключать к сети организации, а все переносные носители проверяются на выделенном автономном АРМ?
13. Какими техническими средствами (класс решений) может быть реализовано выявление и регистрация неконтролируемого использования технологии мобильного кода (мера ЗВК.24, пункт 7.5.4 ГОСТ Р 57580.1)?
14. Относятся ли требования раздела 7.8 ГОСТ Р 57580.1 к контейнерам Docker?
15. Как необходимо реализовать следующие требования и в чем их практический смысл (пункт 7.8.3 ГОСТ Р 57580.1)?
* ЗСВ.6 Реализация необходимых методов предоставления доступа к виртуальным машинам, обеспечивающим возможность доступа с использованием одних аутентификационных данных только к одной виртуальной машине;
* ЗСВ.7 Реализация необходимых методов предоставления доступа к виртуальным машинам, обеспечивающим возможность доступа с использованием одних аутентификационных данных только к одной виртуальной машине с одного АРМ пользователя или эксплуатационного персонала.

При наличии 1000 виртуальных машин иметь 1000 учетных записей администратора невозможно.

1. Просим привести примеры в каких случаях необходимо применение сертифицированных по требованиям безопасности информации средств защиты информации не ниже 6 класса (пункт 8.3.2 ГОСТ Р 57580.1).
2. Пункт 6.2 ГОСТ Р 57580.2 (методика оценки) говорит об оценке выбора мер защиты информации, если организация выбрала какую-то меру, зафиксировала выбор в своих НПА, но не реализовала ее, следует ли оценивать меру как выполненную?
3. Термин «проверяющая организация» ГОСТ Р 57580.2 устанавливает, что организация, проводящая оценку соответствия, не должна осуществлять оказание услуг проверяемой организации в области реализации информатизации и защиты информации. Будет ли как-то отслеживаться такой конфликт интересов и какие санкции планируется предусмотреть для нарушителей этого правила?
4. Положения Банка России № 683-П[[1]](#footnote-1), № 684-П[[2]](#footnote-2), № 672-П[[3]](#footnote-3) требуют от финансовых организаций обеспечить определенный уровень соответствия в соответствии с ГОСТ Р 57580.2. По ГОСТ Р 57580.2 уровень соответствия определен только для процессов защиты информации (далее – ЗИ). Для итоговой оценки шкала уровней соответствия не установлена. Правильно ли понимать требование об обеспечении уровня соответствия ЗИ как требование к уровню соответствия каждого из 8 процессов ЗИ ГОСТ Р 57580.1?
5. Планируется ли организовать разработку методички по применению ГОСТ Р 57580.2 и критериям принятия решений по оценке мер ЗИ ГОСТ Р 57580.1 для обеспечения сходных и повторяемых результатов оценки соответствия?
6. Положение Банка России № 382-П[[4]](#footnote-4) устанавливает требования по защите информации при осуществлении переводов денежных средств. Положение Банка России № 683-П устанавливает требования к обеспечению защиты информации при осуществлении банковской деятельности в целях противодействия осуществлению переводов денежных средств без согласия клиента, которые направлены на обеспечение защиты информации, подготавливаемой, обрабатываемой и хранимой в автоматизированных системах, входящих в состав объектов информационной инфраструктуры и используемых для осуществления банковских операций, связанных с осуществлением перевода денежных средств. Учитывая, что в первом и втором случаях в обработке будут задействованы одни и те же автоматизированные системы (в первом и во втором случаях – перевод денежных средств), какова будет разница между областями оценки? Какие контуры безопасности будут актуальны для первого и второго случаев?
7. В финансовой организации в область оценки могут войти десятки автоматизированных систем и тысячи автоматизированных рабочих мест. Объем аудиторской выборки напрямую влияет на трудоемкость и стоимость работ. Какого размера будет достаточна аудиторская выборка объектов информационной инфраструктуры, задействованных в осуществлении переводов денежных средств для вынесения корректного заключения аудита?
8. Могут ли результаты оценки соответствия требованиям Положений Банка России № 683-П и № 672‑П быть оформлены в виде одного отчета с учетом различных контуров безопасности?
9. Как правильно устанавливать значение коэффициента, отражающего количество нарушений ЗИ, выявленных членами проверяющей группы в процессе оценки соответствия ЗИ: по выявленным типам нарушений или по каждому отдельному нарушению? Например, выявление факта «Наличия незаблокированных учетных записей уволенных работников» или количество таких выявленных учетных записей?
10. Планируется ли разработать методологию оценки выполнения требований к технологическим мерам и требованиям к СКЗИ, предусмотренных Положениями Банка России № 683-П, № 684-П, № 672-П?
11. В соответствии с подпунктом 9.2 Положения Банка России № 683-П кредитные организации должны соответствовать 3 уровню защиты к 1 января 2021. Наличие соответствия подтверждается результатами внешнего аудита. То есть аудит необходимо пройти до 31.12.2020?
1. Положение Банка России от 17.04.2019 № 683-П «Об установлении обязательных для кредитных организаций требований к обеспечению защиты информации при осуществлении банковской деятельности в целях противодействия осуществлению переводов денежных средств без согласия клиента». [↑](#footnote-ref-1)
2. Положение Банка России от 17.04.2019 № 684-П «Об установлении обязательных для некредитных финансовых организаций требований к обеспечению защиты информации при осуществлении деятельности в сфере финансовых рынков в целях противодействия осуществлению незаконных финансовых операций». [↑](#footnote-ref-2)
3. Положение Банка России от 09.01.2019 № 672-П «О требованиях к защите информации в платежной системе Банка России». [↑](#footnote-ref-3)
4. Положение Банка России от 09.06.2012 № 382-П «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». [↑](#footnote-ref-4)