RTM GROUP

Внедрение и оценка ГОСТ Р 57580.1-2017: частные случаи

RTM TECHNOLOGIES — первая экспертная компания специализирующаяся на проведении нормативных и нормативно - технических экспертиз в области ИБ и ИТ.

rtmtech.ru

ПРОГРАММА

01 Обсуждение комментариев ЦБ

02 Разбор вариантов исключения мер

03 Разбор вариантов применения компенсирующих мер

Обсуждение комментариев ЦБ

Исполнение мер

Общие вопросы проведения оценки

Вопрос 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:

1.1 Каковы критерии оценки экономической целесообразности реализации мер, определенных ГОСТ Р 57580.1?

Ответ

» *Применение компенсирующих мер должно сопровождаться обоснованием их применения финансовой организацией. Дополнительных критериев, обосновывающих реализацию компенсационных мер ЗИ, ГОСТ Р 57580.1-2017 не предусмотрено. Вместе с тем рекомендуется при определении экономической целесообразности производить оценку и* ***сравнение вероятности и величины потенциальных потерь*** *от реализации информационных угроз при применении компенсирующих мер и мер из базового состава.*

Вопрос 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:

1.2. 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?

Ответ

Обоснование причин невозможности технической реализации мер ЗИ:

1. *отсутствие **на рынке** технических решений российского производства, обеспечивающих необходимую эффективность и функциональность;*
2. *возможные западные санкции и опасность/невозможность использования решений иностранных производителей.*

При этом такие обоснования должны базироваться на подтвержденных фактах, обуславливающих невозможность технической реализации мер ЗИ, а не на предположениях.

Вопрос 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:

1.3. Можно ли в связи с невозможностью технической реализации и (или) экономической целесообразностью вместо технической меры реализовывать организационную меру/меры?

Ответ

» *Организационные меры ЗИ можно рассматривать в качестве компенсационных при условии, что их применение направлено на **обработку операционного риска**, связанного с реализацией тех же угроз безопасности информации, на нейтрализацию которых направлены меры из базового состава мер защиты информации настоящего стандарта, не применяемые финансовой организацией в связи с невозможностью технической реализации и (или) экономической целесообразностью*.

Вопрос 2

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?

Ответ

» *способ хранения эталонной информации (т.е. совокупности настроек управления правами логического доступа в отношении каждого субъекта) может отличаться в зависимости от реализации механизма управления правами логического доступа (например, посредством реализации механизмов резервного копирования в отношении информационной системы, задействованной при управлении правами логического доступа).*

Вопрос 3

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?

Ответ

» Реализация может быть осуществлена, например, посредством настройки автоматического блокирования учетной записи пользователя в случае, если тот не производил авторизацию в системе в течение заданного периода времени, с возможностью разблокировки только с привлечением представителя подразделения информатизации.

Вопрос 4

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.)?

Ответ

» *Каких-либо исключений при реализации данной меры, в том числе по объектам доступа, в ГОСТ Р 57580.1-2017 не установлено. Однако в случае технической невозможности реализации меры РД.4 финансовой организацией могут быть реализованы компенсирующие меры, направленные на обработку операционного риска, связанного с реализацией тех же угроз безопасности информации, на нейтрализацию которых направлена мера РД.4.*

Вопрос 5

Каким образом необходимо реализовывать меру РД.6 (пункт 7.2.2.2 ГОСТ Р 57580.1):

5.1. Какими средствами можно реализовать аутентификацию АРМ эксплуатационного персонала?
5.2. 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?

Ответ

» *Каких-либо исключений при реализации данной меры, в том числе по объектам доступа, в ГОСТ Р 57580.1-2017 не установлено. При этом аутентификация АРМ эксплуатационного персонала, используемого для осуществления логического доступа, может быть реализована с помощью механизма двухсторонней аутентификации, в том числе с использованием сторонних средств защиты информации, обладающих соответствующим функционалом.*

Вопрос 6

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»?

Ответ

» *При реализации меры РД.16 предполагается достаточным использование на АРМ субъектов логического доступа пароля на изменение параметров конфигурации системы, хранящихся в энергонезависимой памяти, штатными средствами или с использованием сторонних СЗИ.*

Вопрос 7

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.?

Ответ

» *При реализации меры РД.26 финансовой организации необходимо обеспечить выполнение меры РД.27 по реализации защиты копий аутентификационных данных эксплуатационного персонала от НСД при их хранении на МНИ или бумажных носителях. Набор параметров, формат и способ защиты от НСД хранимых данных финансовая организация определяет самостоятельно, при этом учитывая, что выбранный набор и формат должны обеспечивать возможность восстановления учетных записей эксплуатационного персонала.*

Вопрос 7

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.?

7.1. Можно ли хранить данную информацию в зашифрованном виде в сети (например, с помощью ПО «KeePass Password Safe») или это уже будет считаться нарушением?

Ответ

» *Исходя из содержания меры РД.26, полагаем, что копии аутентификационных данных эксплуатационного персонала подлежат хранению исключительно на выделенных МНИ или на бумажных носителях. Это, в свою очередь, не предполагает размещение таких данных в сети даже в зашифрованном виде.*

Вопрос 8

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?

Ответ

» Реализация данной меры предполагает использование токена либо других персональных технических устройств аутентификации, реализующих многофакторную аутентификацию. В случае неиспользования таких устройств отсутствует необходимость ведения пустого журнала на бумажном носителе.

Вопрос 9

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.

Ответ

» Финансовая организация самостоятельно определяет порядок реализации меры ФД.2. Вместе с тем полагаем возможным рекомендовать в описанной Вами ситуации осуществлять контроль посредством сопровождения третьих лиц работниками финансовой организации, обладающими правом самостоятельного доступа в помещения, а также использования различных охранных систем, в том числе сигнализации и видеонаблюдения. Кроме того, определенный в финансовой организации порядок реализации меры ФД.2 целесообразно отразить в том или ином виде в договоре аренды.

Вопрос 10

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?

Ответ

» *Финансовая организация самостоятельно определяет порядок реализации меры ИУ.1.*
Вместе с тем обращаем внимание, что помимо учета ресурсов доступа, создаваемых, используемых и (или) эксплуатируемых на пользовательском уровне по оформленным ими заявкам, мера ИУ.1 предполагает реализацию учета также иных активов финансовой организации, относящихся к ресурсам доступа, которые создаются, используются и (или) эксплуатируются на уровне финансовой организации в целом, в рассматриваемом контуре безопасности.

Вопросы 11-12

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)?

Какими техническими средствами (класс решений) можно контролировать создание и удаление ресурсов доступа (мера ИУ.5, пункт 7.2.4.2 ГОСТ Р 57580.1)?

Ответ

» *Финансовая организация самостоятельно определяет порядок реализации мер ИУ.4 и ИУ.5. При этом полагаем, что в качестве технического средства может выступать программный продукт, реализующий необходимый функционал для управления ИТ-активами финансовой организации, в том числе заявками на предоставление ИТ-услуг для работников внутри финансовой организации.*

Вопрос 13

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)?

Ответ

» *Предметом контроля меры СМЭ.13 является выявление информации, не разрешенной к переносу из сегментов или в сегменты контуров безопасности с использованием переносных (отчуждаемых) носителей информации.*

Вопрос 14

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?

Ответ

» *Для реализации меры СМЭ.14 применение на границе внутренних вычислительных сетей организации и сети Интернет только технического решения, обеспечивающего реализацию сетевого взаимодействия и сетевой изоляции на уровне не выше второго (канальный) по семиуровневой стандартной модели взаимодействия открытых систем.*

Вопрос 15

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?

Ответ

» Реализация меры ЦЗИ.16 предполагает обеспечение возможности восстановления эталонных копий ПО АС, ПО средств и систем защиты информации, системного ПО из резервных копий, способных обеспечить возвращение АС, а также средств и систем защиты информации к штатному функционированию.

Вопрос 16

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?

Ответ

» *Реализация меры ЦЗИ.26 предполагает ведение списков разрешенных приложений, использующих технологии мобильного кода, и фиксирование их использования*

Вопрос 17

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?

Ответ

» *Как реализацию меры ЗВК.19 можно рассматривать запрет на подключение мобильных устройств к сети финансовой организации, а также проверку всех переносных носителей на выделенном автономном АРМ (т.е. когда исключаются возможности информационного взаимодействия данного АРМ и иных сегментов вычислительных сетей финансовой организации, кроме управляющего информационного взаимодействия по установленным правилам и протоколам).*

Вопрос 18

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)?

Ответ

» *Финансовая организация самостоятельно определяет порядок реализации меры ЗВК.24. Вместе с тем полагаем, что факты неконтролируемого использования технологии мобильного кода могут регистрироваться системой обнаружения вторжений.*

Вопрос 19

Относятся ли требования раздела 7.8 ГОСТ Р 57580.1 к контейнерам Docker?

Ответ

- *Учитывая, что технология виртуализации программного обеспечения (в частности, контейнерная виртуализация Docker) является одной из технологий виртуализации, полагаем, что положения раздела 7.8 ГОСТ Р 57580.1-2017 распространяются на данное программное обеспечение.*
- *Организационные и технические меры, приведенные в разделе 7.8 ГОСТ Р 57580.1-2017, являются дополнительными и применяются в совокупности с иными мерами защиты информации, установленными ГОСТ Р 57580.1-2017.*
- *Дополнительно сообщаем, что рекомендации по обеспечению информационной безопасности при использовании технологии виртуализации, включающей виртуализацию программного обеспечения, приведены в ГОСТ Р 56938-2016.*

Вопрос 20

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.

Ответ

Сложность практической реализации мер ЗСВ.6 и ЗСВ.7 позволяет рекомендовать реализовывать их по аналогии с пунктами 10.10 и 10.11 РС БР ИББС-2.8-2015, а именно:

- *при реализации технологии виртуализации рабочих мест пользователей для каждого пользователя рекомендуется единовременно обеспечивать возможность работы только с одной виртуальной машиной в каждом из контуров безопасности (пункт 10.10 РС БР ИББС-2.8-2015);*
- *техническими средствами рекомендуется исключить возможность доступа пользователей к нескольким разным экземплярам виртуальных машин, включенных в один контур безопасности, с использованием одних (общих) аутентификационных данных (пункт 10.11 РС БР ИББС-2.8-2015).*

Вопрос 21

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).

Ответ

- *Мера РЗИ.13 реализуется в случаях, когда применение таких средств необходимо для нейтрализации угроз безопасности, определенных в модели угроз и нарушителей безопасности информации финансовой организации.*
- *Кроме того, согласно абзацу первому пункта 6.12 ГОСТ Р 57580.1-2017 финансовая организация самостоятельно определяет необходимость использования средств криптографической защиты информации, если иное не предусмотрено федеральными законами и иными нормативными правовыми актами Российской Федерации, в том числе нормативными актами Банка России, стандартами, правилами профессиональной деятельности и (или) правилами платежной системы.*

Вопрос 22

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?

Ответ

В соответствии с пунктом 6.2 ГОСТ Р 57580.2-2018 оценку соответствия ЗИ осуществляют по следующим направлениям:

- *выбор финансовой организацией организационных и технических мер ЗИ, направленных на непосредственное обеспечение ЗИ и входящих в систему ЗИ финансовой организации (ГОСТ Р 57580.1-2017, раздел 7);*
- *полнота реализации организационных и технических мер ЗИ, направленных на непосредственное обеспечение ЗИ и входящих в систему организации и управления ЗИ финансовой организации (ГОСТ Р 57580.1-2017, раздел 8);*
- *обеспечение ЗИ на этапах жизненного цикла АС финансовой организации (ГОСТ Р 57580.1-2017, раздел 9).*

При этом исходя из положений пункта 6.10 ГОСТ Р 57580.2-2018 оценку соответствия направлений ЗИ осуществляют отдельно в соответствии с подходом, изложенным в пунктах 6.10.1 - 6.10.3 ГОСТ Р 57580.2-2018.

Вопрос 23

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?

Ответ

» *В соответствии с пунктом 3.2 ГОСТ Р 57580.2-2018 под проверяющей организацией понимается организация, проводящая оценку соответствия ЗИ финансовой организации и являющаяся независимой от проверяемой организации и от организаций, осуществлявших или осуществляющих оказание услуг проверяемой организации в области реализации информатизации и защиты информации (в части внедрения и/или сопровождения систем, средств, процессов информатизации и защиты информации, используемых в финансовой организации в период проведения проверки и входящих в область оценки соответствия ЗИ).*

Вопрос 24

Положения Банка России № 683-П , № 684-П , № 672-П 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?

Ответ

» *Дополнительно проводить качественную оценку вычисленного числового значения итоговой оценки соответствия ЗИ (R) с использованием таблицы 1 «Качественная оценка уровня соответствия процессов системы ЗИ» ГОСТ Р 57580.2-2018 для определения уровня соответствия ЗИ ГОСТ Р 57580.1-2017. Полученный результат также должен приниматься во внимание наряду с оценками, полученными в отношении каждого из восьми процессов ЗИ отдельно.*

Вопрос 26

Положение Банка России № 382-П 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?

Ответ

- *Положение Банка России № 382-П устанавливает требования, в соответствии с которыми операторы по переводу денежных средств, банковские платежные агенты (субагенты), операторы платежных систем, операторы услуг платежной инфраструктуры обеспечивают защиту информации при осуществлении переводов денежных средств.*
- *Положение Банка России № 683-П устанавливает обязательные для кредитных организаций требования к обеспечению защиты информации при осуществлении банковской деятельности в целях противодействия осуществлению переводов денежных средств без согласия клиента.*

Полагаем, что в указанном в вопросе в область оценки соответствия ЗИ в соответствии с Положением Банка России № 683-П входят в том числе автоматизированные системы, используемые при осуществлении как переводов денежных средств, так и иных банковских операций, предусмотренных Федеральным законом от 02.12.1990 № 395-1 «О банках и банковской деятельности».

Вопрос 27

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?

Ответ

- *Согласно пункту 6.1 ГОСТ Р 57580.2-2018 количество и выборку проверяемых подразделений, объектов информатизации, АС и СВТ, входящих в область оценки соответствия ЗИ, проверяющая организация **определяет самостоятельно** с учетом предложений проверяемой организации и обеспечения достоверности итоговой оценки соответствия ЗИ.*
- *Кроме того, для определения объема выборки могут быть использованы соответствующие положения ГОСТ Р ИСО/МЭК 27006-2008 «Информационная технология. Методы и средства обеспечения безопасности. Требования к органам, осуществляющим аудит и сертификацию систем менеджмента информационной безопасности».*

Вопрос 28

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?

Ответ

» *Положение Банка России № 672-П , Положение Банка России № 683-П, и ГОСТ Р 57580.2-2018* ***не содержат ограничений*** *на возможность оформления одного отчета по результатам оценки соответствия ЗИ с учетом различных контуров безопасности.*

Вопрос 29

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?

Ответ

» *Каждый выявленный факт нарушения (например, каждая незаблокированная учетная запись уволенных работников) следует учитывать для определения итоговой оценки соответствия ЗИ.*

Вопрос 31

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?

Ответ

» *Кредитные организации должны обеспечить проведение оценки соответствия данному уровню защиты информации **до** указанной даты.*

ч.2 Вопрос 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?

Ответ

- *1.1.В случае если в соответствии с пунктом 6.4 ГОСТ Р 57580.1-2017 вместо организационных и технических мер защиты информации (ЗИ), предусмотренных ГОСТ Р 57580.1-2017, применяются иные (компенсирующие) меры ЗИ, при определении оценок Емш, Ешу и £МАС для соответствующих процессов (подпроцессов) системы ЗИ и направлений ЗИ оценку компенсирующих мер следует осуществлять* ***в соответствии с подходом, изложенным в пунктах 6.10.1 - 6.10.3*** *ГОСТ Р 57580.2-2018.*
- *1.2.Если используемые финансовой организацией дополнительные меры не являются неотъемлемой составляющей базовых или компенсирующих мер, то применительно к таким случаям ГОСТ Р 57580.2-2018* ***не содержит требования*** *о необходимости проведения процедур оценки соответствия ЗИ.*

ч.2 Вопрос 2

Пункт 1.1 Приложения 1 к Положению № 672-П 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?

Ответ

- *В соответствии с пунктом 1.1 приложения к Положению Банка России № 672-П контур формирования электронных сообщений и контур контроля реквизитов электронных сообщений в информационной инфраструктуре участника ССНП должны быть реализованы с использованием разных рабочих мест, разных криптографических ключей и с привлечением отдельных работников для каждого из контуров.*
- *При этом каких-либо исключений из вышеуказанной нормы, в том числе в ситуации, описанной в Вашем письме, не предусмотрено. Разграничение должно быть отражено в соответствующих внутренних документах организации, в том числе в приказах о назначении работников.*

ч.2 Вопрос 3

Какое количество сотрудников необходимо для реализации требования, указанного в УЗП.21 (пункт 7.2.1.3 ГОСТ Р 57580.1)?

Ответ

- *Финансовая организация самостоятельно определяет порядок реализации меры УЗП.21. При этом каждую функцию, предусмотренную мерой УЗП.21, следует рассматривать отдельно для каждого субъекта логического доступа при управлении его правами логического доступа.*
- *Вместе с тем при реализации меры УЗП.21 также рекомендуется принимать во внимание пункт 7.2.3 СТО БР ИББС-1.0-2014, предусматривающий с целью предупреждения возникновения и снижения рисков нарушения ИБ недопущение совмещения в рамках одной роли следующих функций: разработки и сопровождения АБС/ПО, их разработки и эксплуатации, сопровождения и эксплуатации, администратора системы и администратора ИБ, выполнения операций в АБС и контроля их выполнения.*

ч.2 Вопрос 4

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?

Ответ

» *ГОСТ Р 57580.1-2017 не содержит каких-либо исключений в отношении неприменения отдельных мер, в том числе по разработке и тестированию программного обеспечения в случае, когда финансовая организация самостоятельно разрабатывает ПО.*

ч.2 Вопрос 5

Какое программное обеспечение обеспечивает возможности, требуемые в ЦЗИ.7-ЦЗИ.10 (пункт 7.4.2 ГОСТ Р 57580.1)?

Ответ

» *Финансовая организация самостоятельно определяет ПО, позволяющее обеспечить реализацию мер ЦЗИ.7 - ЦЗИ.10.*

ч.2 Вопрос 6

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?

Ответ

» *Для целей пункта 7.9 ГОСТ Р 57580.1-2017 к категории мобильных (переносных) устройств следует отнести компьютеры и ноутбуки, с которых осуществляется удаленный логический доступ работников финансовой организации.*

*Следовательно, при использовании таких компьютеров и ноутбуков финансовая организация должна обеспечить защиту информации от раскрытия и модификации при осуществлении удаленного доступа; защиту внутренних вычислительных сетей при осуществлении удаленного доступа; защиту информации от раскрытия и модификации при ее обработке и хранении на мобильных (переносных) устройствах (**в том числе в случае использования таких мобильных (переносных) устройств для доступа к корпоративной почте**).*

ч.2 Вопрос 7

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?

Ответ

- Положение Банка России № 684-П3 устанавливает требования к обеспечению защиты информации исключительно в отношении некредитных финансовых организаций.
- Таким образом, на кредитные организации распространяются установленные Положением Банка России № 683-П требования к обеспечению защиты информации, в том числе при осуществлении ими деятельности в сфере финансовых рынков.

ч.2 Вопрос 8

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?

Ответ

» *Нормативные правовые акты Банка России в области защиты информации и ГОСТ Р 57580.1-2017 не содержат ограничений на возможность использования персональных ноутбуков работников финансовых организаций, которые в нерабочее время находятся вне контроля этих финансовых организаций, при условии обеспечения всех требований к защите информации.*

ч.2 Вопрос 9

Что считать финансовыми операциями согласно Положению № 684-П? Будет ли считаться выплата заработной платы сотрудникам страховой компании финансовой операцией?

Ответ

» *Полагаем, что выплата заработной платы не относится к категории финансовых операций, поскольку под действие Положения Банка России № 684-П подпадают финансовые операции, осуществляемые в рамках деятельности в сфере финансовых рынков.*

ч.2 Вопрос 10

Требование пункта 10 Положения № 684-П по обеспечению контроля целостности электронного сообщения имеет отношение только к финансовым операциям?

Ответ

» *Для целей Положения Банка России № 684-П под электронными сообщениями понимается информация, содержащаяся в документах, составляемых при осуществлении финансовых операций в электронном виде работниками некредитных финансовых организаций и (или) клиентами некредитных финансовых организаций (абзац второй пункта 1 Положения Банка России № 684-П).*

Принимая во внимание изложенное, полагаем, что выполнение требования абзаца первого пункта 10 Положения Банка России № 684-П должно быть обеспечено при осуществлении финансовых операций в рамках деятельности в сфере финансовых рынков.

ч.2 Вопрос 11

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?

Ответ

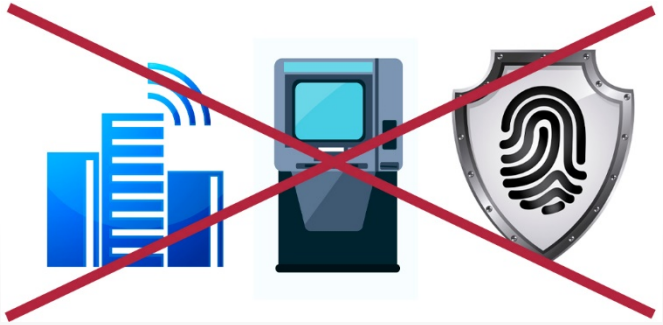
» *Совершение страховой компанией в целях осуществления финансовых операций действий по перенаправлению клиента из своего веб-приложения, а также последующему учету оплаты полиса, по мнению Департамента, обуславливает необходимость соответствия ее программного обеспечения требованиям, предусмотренным пунктом 9 Положения Банка России № 684-П.*

Вопросы

Разбор вариантов исключения мер

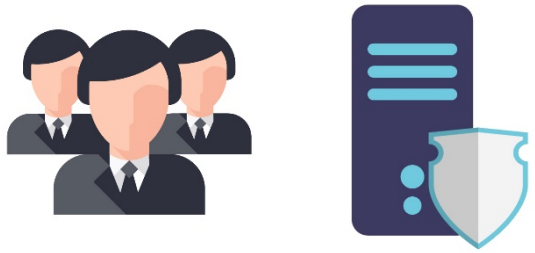
На основании отсутствия технологий

Как правило, не применяются WiFi, в ряде случаев отсутствуют банкоматы, в сегменте ЕБС зачастую нет виртуализации.



Разбор вариантов исключения мер

На основании модели угроз



- Банк имеет незначительный штат сотрудников.
- В АБС и ДБО всего 3 роли.
- Администраторы ИС являются доверенными лицами.

Вероятность неправомерного расширения прав минимальна. Меры, направленные на минимизацию данной угрозы, не применяются. А именно: хранение эталонной информации (УЗП.8), регистрация действий администраторов (УЗП.24).

Разбор вариантов исключения мер

На основании модели угроз

- Банк применяет самописные системы ДБО и АБС.
- ДБО является модулем АБС.
- Взаимодействие происходит в изолированном сетевом сегменте.

Угроза НСД к процедуре обмена не актуальна. Необходимость аутентификации программного сервиса отсутствует (РД.5).

Разбор вариантов исключения мер

На основании модели угроз

- Расчетный центр обрабатывает обезличенные данные.
- Финансовые показатели тайны не составляют.

Утечка конфиденциальной информации посредством печати на бумажном носителе невозможна, и соответствующие меры (ПУИ.3) не имеют смысла.

Разбор вариантов применения компенсирующих мер

На основании экономической целесообразности

При наличии прибыли в 50 млн. в год, ежедневных операциях в 20 млн. и остатках на счетах клиентов больше 10 млн.

*решение за 10 млн. **не** может считаться дорогим!*

Разбор вариантов применения компенсирующих мер

На основании экономической целесообразности

Решения по защите среды виртуализации, удовлетворяющее требованиям пункта 7.8 ГОСТ 57580, имеет:

- стоимость внедрения, согласно коммерческим предложениям от 5.5 до 7 млн. рублей.

Дополнительно переход требует принятия в штат специалиста (либо оплаты аутсорсингу), а также затрат на обновление и поддержку в объеме порядка:

- 1 млн. рублей в год.

Суммы подтверждены коммерческими предложениями от 3-х интеграторов и справкой отдела подбора персонала. С учетом ежегодной прибыли Банка в 30 млн. рублей, принято решение об изоляции серверного сегмента Банка посредством МЭ 5 класса, а также ввести в штат сотрудника, на ежедневной основе исполняющего контроль настроек и активности компонент среды виртуализации.

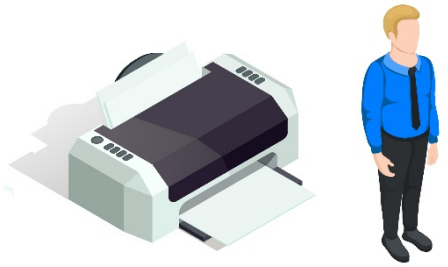
Разбор вариантов применения компенсирующих мер

На основании экономической целесообразности

Решение по защите информации, передаваемой по внутренним сетям (IPS, IDS, МЭ) для расчетного центра стоит 4 млн. рублей.
Максимально возможная **сумма хищения** составляет 1.5 млн. рублей (по максимальной ежедневной сумме операций).
Внедрение подобных решений экономически нецелесообразно, и компенсируется имеющимися средствами межсетевого экранирования с анализом трафика и антивирусными средствами.

Разбор вариантов применения компенсирующих мер

На основании оценки рисков

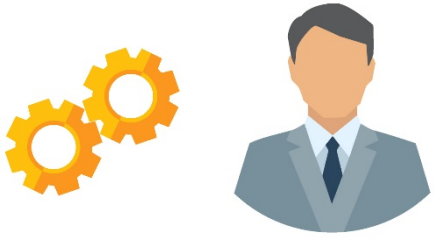


- Принтеры Банка находятся в зоне, контролируемой доверенными лицами.
- Все бумажные носители проходят контроль.
- Риск утечки данных по данному каналу минимален, обрабатывается сотрудниками, заинтересованными в устойчивой деятельности Банка.

Технические меры контроля печати (ПУИ.3) заменены организационными.

Разбор вариантов применения компенсирующих мер

На основании оценки рисков

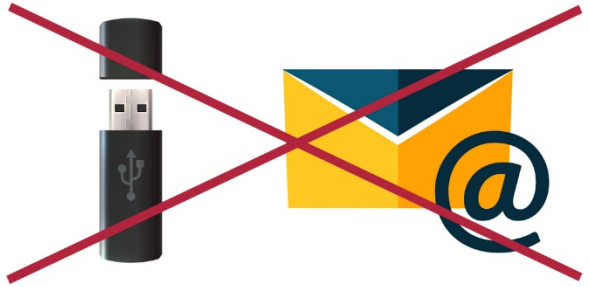


Отсутствие в Банке системы управления инцидентами, компенсируется дублированием обязанностей по взаимодействию ГРИЗИ. Риск несвоевременного реагирования на инцидент минимален.

Техническая мера (РИ.10) компенсирована организационно.

Разбор вариантов применения компенсирующих мер

На основании оценки рисков



Для снижения вероятностей утечки информации через съемные носители, либо электронную почту, в сегменте Банка, принимающем участие в платежном процессе, запрещены отправка email и подключение съемных носителей, а также организован выход в сеть Internet по "белому списку" доверенных ресурсов.

Компенсированы меры (ПУИ.1,2,4-11,17,19) по предотвращению утечек информации по соответствующим каналам.

Вопросы

СПАСИБО ЗА ВНИМАНИЕ!

Фёдор Музалевский

Кандидат физико-математических наук

Ведущий судебный эксперт

Директор технического департамента RTM Group

+79081472741

f.muzalevsky@rtmtech.ru

https://rtmtech.ru

GroupRTM

rtm.group

@GroupRtm

rtm.group.Russia

t.me/kurilka_ib