56-1-11

ЦЕНТРАЛЬНЫЙ БАНК
РОССИЙСКОЙ ФЕДЕРАЦИИ
(Банк России)

Департамент информационной безопасности

107016, Москва, ул. Неглинная, 12
www.cbr.ru
тел.: (499) 300-30-00

От 22.05.2020 № 56-1-11/265

На № 02-05/236 от 24.03.2020

О рассмотрении обращения

Президенту
Ассоциации банков России

Г.И. Лунтовскому

asros@asros.ru

Уважаемый Георгий Иванович!

Департамент информационной безопасности (далее – Департамент) рассмотрел письмо Ассоциации банков России (Ассоциация «Россия») от 22.04.2020 № 02-05/236, содержащее вопросы кредитных организаций по реализации положений ГОСТ Р 57580.1-2017[1] и ГОСТ Р 57580.2-2018[2], и сообщает следующее.

По вопросу 1.

1.1. Пунктом 6.4 ГОСТ Р 57580.1-2017 предусмотрена возможность применения компенсационных мер защиты информации в случае невозможности технической реализации отдельных выбранных мер защиты информации (ЗИ) и/или в случае отсутствия экономической целесообразности.

При этом 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

[1] Национальный стандарт Российской Федерации ГОСТ Р 57580.1-2017 «Безопасность финансовых (банковских) операций. Защита информации финансовых организаций. Базовый состав организационных и технических мер».

[2] Национальный стандарт Российской Федерации ГОСТ Р 57580.2-2018 «Безопасность финансовых (банковских) операций. Защита информации финансовых организаций. Методика оценки соответствия».

вероятности и величины потенциальных потерь от реализации информационных угроз при применении компенсирующих мер и мер из базового состава.

1.2. В качестве обоснования причин невозможности технической реализации мер ЗИ полагаем допустимым указывать такие, как: 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.

1.3. Полагаем, что 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 (абзац третий пункта 6.4 ГОСТ Р 57580.1-2017).

По вопросу 2.

Мера по хранению эталонной информации о предоставленных правах логического доступа и обеспечению целостности указанной информации (УЗП.8) включена в базовый состав мер по организации, контролю предоставления (отзыва) и блокированию логического доступа (пункт 7.2.1.3 ГОСТ Р 57580.1-2017).

При этом 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).

По вопросу 3.

Меры по установлению фактов неиспользования субъектами логического доступа предоставленных им прав на осуществление логического доступа на протяжении определенного периода времени (УЗП.14 и УЗП.15) включены в базовый состав мер по организации, контролю предоставления (отзыва) и блокированию логического доступа (пункт 7.2.1.3 ГОСТ Р 57580.1-2017).

При этом их 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.

По вопросу 4.

Мера по идентификации и многофакторной аутентификации эксплуатационного персонала (РД.4) включена в базовый состав мер по идентификации и аутентификации субъектов логического доступа (пункт 7.2.2.2 ГОСТ Р 57580.1-2017).

При этом 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.

По вопросу 5.

Мера по аутентификации АРМ эксплуатационного персонала, используемых для осуществления логического доступа (РД.6), включена в базовый состав мер по идентификации и аутентификации субъектов логического доступа (пункт 7.2.2.2 ГОСТ Р 57580.1-2017).

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.

По вопросу 6.

Мера, предусматривающая использование на АРМ субъектов логического доступа встроенных механизмов контроля изменения базовой конфигурации оборудования (пароль на изменение параметров конфигурации системы, хранящихся в энергонезависимой памяти) (РД.16), включена в базовый состав мер по идентификации и аутентификации субъектов логического доступа (пункт 7.2.2.2 ГОСТ Р 57580.1-2017).

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 средств защиты информации.

По вопросу 7.

1.1. Мера по хранению копий аутентификационных данных эксплуатационного персонала на выделенных машинных носителях информации (МНИ) или на бумажных носителях (РД.26) включена в базовый состав мер по организации управления и организации защиты идентификационных и аутентификационных данных (пункт 7.2.2.3 ГОСТ Р 57580.1-2017).

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.

1.2. 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.

По вопросу 8.

Мера по регистрации персонификации, выдачи (передачи) и уничтожения персональных технических устройств аутентификации, реализующих многофакторную аутентификацию (РД.28), включена в базовый состав мер по организации управления и организации защиты идентификационных и аутентификационных данных (пункт 7.2.2.3 ГОСТ Р 57580.1-2017).

При этом 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.

По вопросу 9.

Мера, предусматривающая осуществление контроля перечня лиц, которым предоставлено право самостоятельного физического доступа в помещения (ФД.2), включена в базовый состав мер по организации и контролю физического доступа в помещения (пункт 7.2.3.2 ГОСТ Р 57580.1-2017).

При этом 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.

По вопросу 10.

Мера по учету созданных, используемых и (или) эксплуатируемых ресурсов доступа (ИУ.1) включена в базовый состав мер по организации учета и контроля состава ресурсов и объектов доступа (пункт 7.2.4.2 ГОСТ Р 57580.1-2017).

При этом 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.

По вопросам 11 и 12.

Меры по контролю фактического состава созданных, используемых и (или) эксплуатируемых ресурсов доступа (баз данных, сетевых файловых ресурсов, виртуальных машин) и их корректному размещению в сегментах вычислительных сетей финансовой организации (ИУ.4), а также по контролю выполнения операций по созданию, удалению и резервному копированию ресурсов доступа (баз данных, сетевых файловых ресурсов, виртуальных машин) (ИУ.5) включены в базовый состав мер по организации учета и контроля состава ресурсов и объектов доступа (пункт 7.2.4.2 ГОСТ Р 57580.1-2017).

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.

По вопросу 13.

Мера, предусматривающая осуществление контроля содержимого информации при ее переносе из сегментов или в сегменты контуров безопасности с использованием переносных (отчуждаемых) носителей информации (СМЭ.13), включена в базовый состав мер по сегментации и межсетевому экранированию внутренних вычислительных сетей (пункт 7.3.1.2 ГОСТ Р 57580.1-2017).

При этом 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.

По вопросу 14.

Мера, предусматривающая реализацию сетевого взаимодействия и сетевой изоляции на уровне не выше второго (канальный) по семиуровневой стандартной модели взаимодействия открытых систем, определенной в ГОСТ Р ИСО/МЭК 7498-1[3], внутренних вычислительных сетей финансовой организации и сети Интернет (СМЭ.14), включена в базовый состав мер по сегментации и межсетевому экранированию внутренних вычислительных сетей (пункт 7.3.1.3 ГОСТ Р 57580.1-2017).

При этом полагаем возможным 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, определенной в ГОСТ Р ИСО/МЭК 7498-1.

По вопросу 15.

Мера, предусматривающая обеспечение возможности восстановления эталонных копий ПО АС, ПО средств и систем защиты информации, системного ПО в случаях нештатных ситуаций (ЦЗИ.16), включена в базовый состав мер по организации и контролю размещения, хранения и обновления ПО (пункт 7.4.3 ГОСТ Р 57580.1-2017).

При этом 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.

---

[3] Государственный стандарт Российской Федерации ГОСТ Р ИСО/МЭК 7498-1-99 «Информационная технология. Взаимосвязь открытых систем. Базовая эталонная модель. Часть 1. Базовая модель».

По вопросу 16.

Мера, предусматривающая осуществление контроля (выявления) использования технологии мобильного кода (ЦЗИ.26), включена в базовый состав мер по контролю состава и целостности ПО информационной инфраструктуры (пункт 7.4.4 ГОСТ Р 57580.1-2017).

При этом реализация меры ЦЗИ.26 предполагает ведение списков разрешенных приложений, использующих технологии мобильного кода, и фиксирование их использования.

По вопросу 17.

Мера, предусматривающая осуществление входного контроля устройств и переносных (отчуждаемых) носителей информации перед их использованием в вычислительных сетях финансовой организации, в выделенном сегменте вычислительной сети с исключением возможности информационного взаимодействия указанного сегмента и иных сегментов вычислительных сетей финансовой организации (кроме управляющего информационного взаимодействия по установленным правилам и протоколам) (ЗВК.19), включена в базовый состав мер по организации и контролю применения средств защиты от вредоносного кода (пункт 7.5.3 ГОСТ Р 57580.1-2017).

При этом полагаем, что 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).

По вопросу 18.

Мера по регистрации неконтролируемого использования технологии мобильного кода (ЗВК.24) включена в базовый состав мер по регистрации событий защиты информации, связанных с реализацией защиты от вредоносного кода (пункт 7.5.4 ГОСТ Р 57580.1-2017).

При этом 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.

По вопросу 19.

Раздел 7.8 ГОСТ Р 57580.1-2017 содержит требования к содержанию базового состава мер защиты информации для процесса 7 «Защита среды виртуализации».

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.

По вопросу 20.

Меры по реализации необходимых методов предоставления доступа к виртуальным машинам, обеспечивающих возможность доступа с использованием одних аутентификационных данных только к одной виртуальной машине (ЗСВ.6) и только к одной виртуальной машине с одного АРМ пользователя или эксплуатационного персонала (ЗСВ.7), включены в базовый состав мер по организации идентификации, аутентификации, авторизации (разграничения доступа) при осуществлении логического доступа к виртуальным машинам и серверным компонентам виртуализации (пункт 7.8.3 ГОСТ Р 57580.1-2017).

При этом 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[4], а именно:

---

[4] Рекомендации в области стандартизации Банка России «Обеспечение информационной безопасности организаций банковской системы Российской Федерации. Обеспечение информационной безопасности при

- 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).

По вопросу 21.

Мера по применению сертифицированных по требованиям безопасности информации средств защиты информации не ниже шестого класса (РЗИ.13) включена в базовый состав мер по реализации процесса системы защиты информации (пункт 8.3.2 ГОСТ Р 57580.1-2017).

При этом 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.

По вопросу 22.

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);

использовании технологии виртуализации» РС БР ИББС-2.8-2015» (приняты и введены в действие Приказом Банка России от 19.02.2015 № ОД-393).

- 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.

По вопросу 23.

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).

При этом соблюдение пункта 3.2 ГОСТ Р 57580.2-2018 является предметом контроля со стороны Банка России наравне с контролем за соблюдением иных положений ГОСТ Р 57580.2-2018.

По вопросу 24.

Нормативными правовыми актами Банка России в области защиты информации установлен ряд требований к финансовым организациям об обеспечении определенных уровней соответствия, предусмотренных ГОСТ Р 57580.2-2018.

При этом исходя из положений ГОСТ Р 57580.2-2018 уровень соответствия оценивается в отношении каждого из восьми процессов ЗИ отдельно.

Однако в таком случае оценка соответствия требованиям, установленным ГОСТ Р 57580.1-2017, не реализуется финансовыми организациями в полном объеме, поскольку на этапе качественной оценки процессов системы ЗИ в ГОСТ Р 57580.2-2018 не учитывается оценка полноты применения организационных и технических мер ЗИ на этапах жизненного цикла АС финансовой организации (E_{AC}), а также нарушения ЗИ, выявленные членами проверяющей группы в процессе оценки соответствия ЗИ (Z), которые влияют на показатели итоговой оценки соответствия ЗИ (R).

Принимая во внимание изложенное, полагаем возможным рекомендовать 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.

По вопросу 25.

Планом работы Департамента на 2020 год не предусмотрена разработка каких-либо методических рекомендаций в развитие ГОСТ Р 57580.1-2017 и ГОСТ Р 57580.2-2018.

По вопросу 26.

Положение Банка России № 382-П[5] 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[6] устанавливает обязательные для кредитных организаций требования к обеспечению защиты информации при

---

[5] 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».

[6] 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

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».

По вопросу 27.

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».

По вопросу 28.

Положение Банка России № 672-П[7], 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.

По вопросу 29.

В соответствии с пунктом 7.10 ГОСТ Р 57580.2-2018 при выявлении самостоятельно членами проверяющей группы в процессе оценки соответствия ЗИ фактов нарушений ЗИ, в результате которых имелась или имеется возможность наступления инцидентов ЗИ, наносящих ущерб финансовой

противодействия осуществлению переводов денежных средств без согласия клиента».

[7] Положение Банка России от 09.01.2019 № 672-П «О требованиях к защите информации в платежной системе Банка России».

организации или ее клиентам, числовую итоговую оценку соответствия ЗИ R снижают на числовую величину, равную 0,01, за каждый выявленный факт нарушения.

С учетом изложенного полагаем, что каждый выявленный факт нарушения (например, каждая незаблокированная учетная запись уволенных работников) следует учитывать для определения итоговой оценки соответствия ЗИ.

По вопросу 30.

Планом работы Департамента на 2020 год не предусмотрена разработка методологии оценки выполнения требований к технологическим мерам и требованиям к СКЗИ, предусмотренных Положением Банка России № 672-П, Положением Банка России № 683-П, Положением Банка России № 684-П[8].

По вопросу 31.

Согласно абзацу первому пункта 9.2 Положения Банка России № 683-П кредитные организации должны обеспечить уровень соответствия не ниже третьего в соответствии с ГОСТ Р 57580.2-2018 с 1 января 2021 года.

Следовательно, кредитные организации должны обеспечить проведение оценки соответствия данному уровню защиты информации до указанной даты.

Директор В.А. Уваров

[8] 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».