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 № 56-1-11/264

На № 02-05/245 от 26.03.2020

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 26.03.2020 № 02-05/245, 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. 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 $E_{\text{МЗИ}}$, $E_{\text{МОУ}}$ и $E_{\text{МАС}}$ 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,

---

[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».

то применительно к таким случаям ГОСТ Р 57580.2-2018 не содержит требования о необходимости проведения процедур оценки соответствия ЗИ.

По вопросу 2.

В соответствии с пунктом 1.1 приложения к Положению Банка России № 672-П[3] 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.

По вопросу 3.

Мера по реализации правил управления правами логического доступа, обеспечивающая запрет совмещения одним субъектом логического доступа функций, предусмотренных данной мерой (УЗП.21), включена в базовый состав мер по организации, контролю предоставления (отзыва) и блокированию логического доступа (пункт 7.2.1.3 ГОСТ Р 57580.1-2017).

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[4], 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

---

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

[4] Стандарт Банка России СТО БР ИББС-1.0-2014 «Обеспечение информационной безопасности организаций банковской системы Российской Федерации. Общие положения» (принят и введен в действие распоряжением Банка России от 17.05.2014 № Р-399).

эксплуатации, сопровождения и эксплуатации, администратора системы и администратора ИБ, выполнения операций в АБС и контроля их выполнения.

По вопросу 4.

В пунктах 7.3 и 7.4 ГОСТ Р 57580.1-2017 определены требования к содержанию базового состава мер по обеспечению защиты вычислительных сетей, а также по контролю целостности и защищенности информационной инфраструктуры (соответственно).

При этом 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.

По вопросу 5.

Пункт 7.4.2 ГОСТ Р 57580.1-2017 содержит ряд требований (меры ЦЗИ.7 – ЦЗИ.10) к процедуре реализации мер по контролю отсутствия и обеспечения оперативного устранения известных (описанных) уязвимостей, предусмотренных мерами ЦЗИ.1 – ЦЗИ.6.

При этом финансовая организация самостоятельно определяет ПО, позволяющее обеспечить реализацию мер ЦЗИ.7 – ЦЗИ.10.

По вопросу 6.

Пунктом 7.9 ГОСТ Р 57580.1-2017 определены требования к содержанию базового состава мер по защите информации при осуществлении удаленного логического доступа работников финансовой организации с использованием мобильных (переносных) устройств.

При этом полагаем, что 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).

По вопросу 7.

Положение Банка России № 684-П[5] устанавливает требования к обеспечению защиты информации исключительно в отношении некредитных финансовых организаций.

Таким образом, на кредитные организации распространяются установленные Положением Банка России № 683-П[6] требования к обеспечению защиты информации, в том числе при осуществлении ими деятельности в сфере финансовых рынков.

По вопросу 8.

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.

По вопросу 9.

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.

По вопросу 10.

В соответствии с абзацем первым пункта 10 Положения Банка России № 684-П некредитные финансовые организации, реализующие усиленный и стандартный уровни защиты информации, должны обеспечивать подписание электронных сообщений способом, позволяющим обеспечить их целостность и подтвердить их составление уполномоченным на это лицом.

---

[5] 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».

[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 противодействия осуществлению переводов денежных средств без согласия клиента».

При этом 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.

По вопросу 11.

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.

Директор В.А. Уваров