Банк России

«МЕТОДИЧЕСКИЕ РЕКОМЕНДАЦИИ ПО НЕЙТРАЛИЗАЦИИ БАНКАМИ УГРОЗ БЕЗОПАСНОСТИ, АКТУАЛЬНЫХ ПРИ ОБРАБОТКЕ, ВКЛЮЧАЯ СБОР И ХРАНЕНИЕ, БИОМЕТРИЧЕСКИХ ПЕРСОНАЛЬНЫХ ДАННЫХ, ИХ ПРОВЕРКЕ И ПЕРЕДАЧЕ ИНФОРМАЦИИ О СТЕПЕНИ ИХ СООТВЕТСТВИЯ ПРЕДОСТАВЛЕННЫМ БИОМЕТРИЧЕСКИМ ПЕРСОНАЛЬНЫМ ДАННЫМ ГРАЖДАНИНА РОССИЙСКОЙ ФЕДЕРАЦИИ»

2019 г.

Вопрос 1.

Что подразумевается под термином «обработанные биометрические персональные данные», возможно ли исключить указанную терминологию, так как банк не обрабатывает, а именно не вносит изменения в данные физических лиц, а только собирает и передает?

Ответ:

В Методических рекомендациях под термином «обработанные биометрические персональные данные» не подразумевается внесение изменений в биометрию физических лиц, в данное понятие вкладываются только действия необходимые для их передачи, а именно: сбор, объединение в упаковку и подписание.

Слова «обработанных» исключены из последнего абзаца пункта 1.2.1, пунктов 2.3.10, 2.4, 2.4.1.

В остальных случаях остается пояснение терминологии.

Вопрос 2.

Требуется ли дополнить Методические рекомендации дополнительными технологическими участками, в случае взаимодействия АРМ сбора биометрии с центральным хранилищем и сервером обработки запросов в периметре банка (это не обязательно между структурными подразделениями происходит) и АРМ оператора ЦО ЕСИА/ЕБС?

Ответ:

В указанном случае передача собранных биометрических персональных данных осуществляется внутри банка, но защищается таким же образом, в соответствии с рекомендациями, указанными на участках сбора и обработки биометрических персональных данных перед отправкой в ЕБС. Добавление дополнительных технологических участков считаем нецелесообразным.

Вопрос 3.

Возможно ли уточнить спецификацию рекомендуемых средств защиты безопасности (межсетевой экран и антивирусное ПО). Также просим сообщить, проработан ли со ФСТЭК вопрос о сертификации прикладного ПО в системе сертификации средств защиты информации и имеется ли подтверждение ФСТЭК о готовности принять на себя сертификацию прикладного ПО?

Ответ:

Банк России не имеет возможности уточнить спецификацию конкретных средств защиты информации, однако данный перечень указан на официальном сайте ФСТЭК России.

Вопрос по сертификации ФСТЭК России прикладного ПО проработан в рамках нормативного регулирования и отражен в пункте 2.5.5.1 Положения Банка России № 382-П.

Вопрос 4.

Как соотносятся рекомендуемые СЗИ и их классы с Приказом ФСТЭК России от 18.02.2013 №21?

Ответ:

Рекомендуемый класс и перечень средств защиты информации определяется на основании требований, предъявляемых к средствам криптографической защиты информации.

Вопрос 5.

Зачем для установления факта подписания электронных сообщений конкретным сотрудником использовать УКЭП для сотрудника, если 63-ФЗ признает юридически значимым использование ПЭП? Использование УКЭП очень затратно для банков, при этом необходимо учесть, что для идентификации оператора, снявшего БО, в ЕСИА-ЕБС используется СНИЛС, а доступ к ИС Банка предоставляется на основании логина и пароля, а также 2-го фактора аутентификации.

Ответ:

В указанном случае УКЭП применяется для идентификации сотрудника в целях усиления информационной безопасности на участке сбора, с учетом того, что если применение УКЭП невозможно, то для идентификации остаются требования, указанные в Приказе Минкомсвязи № 321.

Вопрос 6.

Просим уточнить, регистрацию каких именно действий необходимо обеспечить, которые описаны в абзаце третьем и пятом пункта 2.1.8?

Ответ:

В абзаце третьем рекомендуется обеспечить регистрацию действий сотрудника, осуществляющего сбор параметров биометрических персональных данных физических лиц в процессе их сбора.

В абзаце пятом рекомендуется обеспечить регистрацию событий формирования пакета данных (успешных/неуспешных попыток формирования пакета с учетом проверки качества собранных биометрических данных с помощью библиотеки проверки качества данных), собранных на АРМ сбора биометрии уполномоченным сотрудником, до его подписания УКЭП банка.

Вопрос 7.

Допускается ли использование одного устройства, сертифицированного ФСТЭК России на соответствие требованиям к разным категориям средств защиты информации (например, СОВ (ИТ.СОВ.С3.ПЗ) - по 3 классу и МЭ (ИТ.МЭ.А3.ПЗ) по 3 классу или выше)?

Ответ:

Допускается использование одного устройства, сертифицированного по нескольким категориям средств защиты информации, если оно имеет сертификацию по каждой из категорий.

Вопрос 8.

Для чего необходимо сравнение входящих и исходящих сообщений для подтверждения целостности, если для этой цели предлагалось ранее использовать УКЭП? Логично оставить данный пункт при условии использования ПЭП уполномоченного сотрудника.

Ответ:

В процессе где осуществляется переподписание электронного сообщения, содержащего биометрические персональные данные рекомендуется применять сверку входящих электронных сообщений с исходящими.

Вопрос 9.

Предусматривается ли возможность использования собственного и типового решения при взаимодействии с ЕСИА/ЕБС при выполнении биометрической верификации по аналогии с пунктом 2.3.8 в случае сбора?

Ответ:

Возможность использования всех типов решения при взаимодействии с ЕСИА/ЕБС предусмотрена в пункте 3.2.2 Методических рекомендаций.

Вопрос 10.

Будет ли являться вывозом СКЗИ, в случае выезда клиента за границу с установленным на его мобильном устройстве приложением для удаленной идентификации?

Ответ:

Выезд клиента с установленным на его устройстве приложением и применяемым в его личных целях не является вывозом СКЗИ.

Вопрос 11.

Каков технический порядок информирования Банка России об инцидентах в ЕБС?

Ответ:

Информирование об инцидентах осуществляется по существующим каналам (например, АСОИ ФинЦЕРТ), информация о которых указана на сайте Банка России.

Банком России ведется подготовка документов, в которых будут отражены вопросы претензионной работы с банками, а также в последующем будет доработан стандарт Банка России СТО-БФБО-1.5-2018 в части уведомления об инцидентах связанных с нарушением защиты информации в ЕБС.

Вопрос 12.

Предусмотрено ли применение мер (санкций) к банкам в случае полного или частичного неисполнения Методических рекомендаций?

Ответ:

Банки должны реализовывать меры защиты информации, направленные на нейтрализацию угроз безопасности в ЕБС, определенные в Указании Банка России № 4859-У. Методические рекомендации являются одним из вариантов реализации мер, направленных на нейтрализации угроз. Банк России предусматривает меры (санкции) к банкам в случае отсутствия принятия указанных мер.

Банк России

СПАСИБО
ЗА ВНИМАНИЕ

Пункт приема корреспонденции:
Москва, Сандуновский пер., д. 3, стр. 1, телефон +7 495 621-09-61
Почтовый адрес: 107016, Москва, ул. Неглинная, д. 12
Контактный центр: 8 800 250-40-72, +7 495 771-91-00
Факс: +7 495 621-64-65, +7 495 621-62-88
Сайт: www.cbr.ru
Электронная почта: fps@cbr.ru