Руководителям организаций,
участвующих в электронном
обмене с Банком России
(по списку, кроме ДПУ, ПУ)

О планируемых изменениях, предоставляемого Банком России участникам обмена программного обеспечения, применяемого при передаче финансовых сообщений через СПФС

От: 13.11.2018

Информационное сообщение № ВН-16-4-6-1/9608

Центр эксплуатации платежной системы Департамента информационных технологий Банка России (далее - ЦЭПС ДИТ) в дополнение к информационным сообщениям от 14.03.2018 № 20 и от 05.06.2018 №51 информирует участников обмена (далее - УО), являющихся пользователями системы передачи финансовых сообщений (далее – СПФС), о планируемых изменениях в предоставляемом Банком России УО программном обеспечении, применяемом при передаче финансовых сообщений через СПФС о программного комплекса «Автоматизированное рабочее место клиента Банка России пользователя передачи финансовых сообщений» (далее – ПК АРМ КБР-СПФС).

ЦЭПС ДИТ обращает внимание, что пользователям СПФС необходимо до 29.06.2019 перейти на ПК АРМ КБР-СПФС, т.к. из программных комплексов (далее - ПК), переданных Банком России УО для взаимодействия с использованием электронных сообщений (далее - ЭС) при переводе денежных в рамках платежной системы Банка России и при передаче финансовых сообщений через СПФС, в том числе из ПК «Автоматизированное программное место Клиента Банка России Новое» (далее – ПК АРМ КБР-Н) будет исключена возможность обмена ЭС при передаче финансовых сообщений через СПФС.

При обмене ЭС с Банком России при передаче финансовых сообщений через СПФС:

- применяется первый вариант защиты ЭС согласно Альбому УФЭБС;

- используются ключи, предназначенные для СПФС.

Тестирование ПК АРМ КБР-СПФС на стенде совмещенного тестирования подсистем РАБИС-НП уровня КЦОИ пользователь СПФС может проводить после получения тестовых ключевых документов в установленном порядке.

Данное сообщение размещено на сайте Банка России по адресу www.cbr.ru/mcirabis/ в разделе «Информация о новых версиях программного обеспечения».

Контактные данные Единой службы поддержки пользователей Департамента информационных технологий:

многоканальный телефон - 8 (495) 957-80-01;

адрес электронной почты - helpdeskmci@cbr.ru.

Приложения:

1.«Общее описание ПК АРМ КБР-СПФС» - 11 л;

2. «Описание проверок целостности ПК АРМ КБР-СПФС» - 2 л.

Заместитель директора Департамента
информационных технологий –
директор Центра эксплуатации
платежной системы М.Н. Шашлов

Приложение 1

Общее описание ПК АРМ КБР-СПФС

1. Условия эксплуатации

1.1 Условия применения

Условия применения ПК АРМ КБР-СПФС предусматривают наличие у пользователя СПФС:

– собственной АС обработки информации, реализующей интерфейс обмена в соответствии с Альбомом УФЭБС в форматах swift или в собственных форматах участников электронного обмена (далее - УЭО) ;

– сетевого соединения с транспортной подсистемой Банка России;

– необходимого для эксплуатации ПК АРМ КБР-СПФС комплекса технических средств;

– необходимого для эксплуатации ПК АРМ КБР-СПФС квалифицированного персонала.

1.2 Технические средства

ПК АРМ КБР-СПФС функционирует на ПЭВМ с процессором семейства Intel с архитектурой x86 (32-bit) или x64 (64-bit).

Объём жёсткого диска и оперативной памяти должен удовлетворять минимальным требованиям для установленной на данной ПЭВМ версии операционной системы (ОС) Microsoft Windows, СКАД «Сигнатура», IBM WebSphere MQ Client.если взаимодействие с СВК осуществляется клиентом с использованием протокола IBM WebSphere MQ.

Компьютер должен быть оснащён считывателем ключевых носителей в соответствии с требованиями СКАД «Сигнатура», клавиатурой, дисплеем и манипулятором «мышь». Видеоадаптер должен обеспечивать разрешение не менее 1280x800 пикселей.

1.3 Программные средства

ПК АРМ КБР-СПФС функционирует в среде семейства ОС Windows версии Windows 7 и выше, как в 32-битной, так и 64-битной реализации.

Дополнительно должно быть установлено следующее программное обеспечение (ПО):

– Microsoft Windows Installer версия 3.0 или выше;

– Microsoft .NET Framework версия 4.5.2 и выше;

– СКАД «Сигнатура»;

– ПО IBM WebSphere MQ (IBM WebSphere MQ Client) версии 7.0.1 или выше при взаимодействии с Унифицированной транспортной средой электронного взаимодействия территориальных учреждений Банка России с клиентами Банка России (далее – СВК) по протоколам IBM WebSphere MQ (далее – IBM MQ);

– веб-консоль оператора СВК.

1.4Квалификация персонала

Эксплуатационный персонал ПК АРМ КБР-СПФС, выполняющий технологические операции по загрузке ключей шифрования и мониторингу процессов обработки ЭС, должен обладать квалификацией, необходимой для понимания и использования технологических процессов обмена ЭС между АС пользователя СПФС и Центром обработки сообщений (ЦОС) Банка России, а также для обращения с ключевой информацией.

Эксплуатационный персонал ПК АРМ КБР-СПФС, выполняющий административные функции, должен обладать квалификацией, необходимой для выполнения операций по установке и настройке ПК, поддержке бесперебойной работы ПО, обеспечению информационной безопасности.

Эксплуатационный персонал ПК АРМ КБР-СПФС всех категорий должен иметь навыки работы в ОС Microsoft Windows на уровне опытного пользователя.

1.5 Телекоммуникационная система

ПК АРМ КБР-СПФС взаимодействует с СВК. Взаимодействие с СВК осуществляется по следующим протоколам:

– IBM MQ;

– HTTP 1.1 [RFC 2616].

При использовании IBM MQ обмен ЭС СВК, размещенными в транспортных сообщениях формата IBM MQ, осуществляется путем передачи сообщений через очереди, созданные на локальном менеджере очередей IBM MQ. Под термином «локальный менеджер очередей» подразумевается менеджер, расположенный на том же хосте, что и ПК АРМ КБР-СПФС, или на другом хосте в пределах той же локальной сети. Подключение с помощью ПО WebSphere MQ Client непосредственно к внешнему менеджеру СВК не предусмотрено.

Комплекс технических средств ПК АРМ КБР-СПФС должен быть подключен в локальную вычислительную сеть пользователя СПФС через защищенное соединение, предполагающее отсутствие технической возможности доступа к ПК АРМ КБР-СПФС из внешних, по отношению к ЛВС пользователя СПФС, сетей.

2. Описание функционирования ПК АРМ КБР-СПФС

2.1 Интерфейс обмена ЭС ПК АРМ КБР-СПФС с АС пользователя СПФС

ПК АРМ КБР-СПФС предоставляет файловый интерфейс для обмена ЭС с АС пользователя СПФС, при котором обмен ЭС с АС пользователя СПФС осуществляется путем передачи файлов, содержащих ЭС, через разделяемые каталоги обмена. К именам файлов, кроме файлов в собственных форматах УЭО, предъявляется требование – уникальность. Уникальность должна быть обеспечена на время нахождения файлов ЭС в разделяемых каталогах обмена ПК АРМ КБР-СПФС (для исключения перезаписи файлов ЭС). Обработка файлов ЭС должна выполняться в порядке поступления их в каталог обмена либо, если таковой порядок не может быть определен, в хронологическом порядке по времени создания файла.

2.2 Интерфейс обмена ЭС ПК АРМ КБР-СПФС с СВК

ПК АРМ КБР-СПФС взаимодействует с СВК Банка России. Взаимодействие с СВК Банка России осуществляется по следующим протоколам:

1) IBM MQ;
2) HTTP 1.1 [RFC 2616].

При использовании IBM MQ обмен ЭС с СВК Банка России, размещенными в транспортных сообщениях формата IBM MQ, осуществляется путем передачи сообщений через очереди, созданные на менеджере очередей IBM MQ на стороне АС клиента.

2.3 Особенности пользовательского интерфейса

В ПК АРМ КБР – СПФС предусмотрена возможность выбора языка интерфейса из русского и английского вариантов.

3. Описание обработки ЭС

ПК АРМ КБР-СПФС обрабатывает ЭС в формате Альбома УФЭБС, в формате SWIFT и в собственных форматах УЭО.

В ПК АРМ КБР – СПФС реализована возможность работы только с ключами, предназначенными для обмена с ЦОС СПФС и исключена возможность обработки ЭС, не предназначенных для обработки в СПФС. Для этого, при загрузке ключа проверятется расширенная область применения сертификата ключа (OID). В случае, если OID не соответствует ключам, предназначенными для обмена с ЦОС СПФС, работа ПК АРМ КБР-СПФС завершается.

3.1 Обработка исходящих ЭС из АС пользователя СПФС

3 1.1. Обработка ЭС в формате УФЭБС (ED5**)

При получении ЭС из соответствующего каталога обмена в формате УФЭБС (ED501, ED503, ED512, ED540, ED542, ED573, ED599), направляемых пользователем СПФС на обработку в СПФС, ПК АРМ КБР-СПФС:

1) выполняет структурный контроль (валидацию по схемам УФЭБС);

2) помещает ЭС в хранилище введенных, удаляет из входного каталога обмена;

3) формирует КА на ЭС;

4) упаковывает ЭС в соответствии с требованиями Альбома УФЭБС;

5) шифрует ЭС с использованием открытого ключа шифрования контура контроля ЦОС в адрес СПФС Банка России в соответствии с требованиями Альбома УФЭБС;

6) формирует ЭС в формате служебного конверта (СК) (SoapEnvelope) в соответствии с требованиями Альбома УФЭБС;

7) помещает ЭС в формате СК в хранилище отправленных;

8) передает сформированный СК в СВК.

3.1.2 Обработка ЭС в формате УФЭБС (SigEnvelope)

При получении ЭС из соответствующего каталога обмена в формате УФЭБС (SigEnvelope), направляемых клиентом на обработку в СПФС, ПК АРМ КБР-СПФС:

1) выполняет структурный контроль (валидацию по схемам УФЭБС);

2) выполняет проверку КА и проверку на соответствие OID КА списку разрешенных для подписи OID;

3) извлекает ЭС из конверта КА, выполняет структурный контроль (валидацию по схемам УФЭБС) извлеченного ЭС;

4) помещает ЭС в хранилище введенных, удаляет из входного каталога обмена;

5) упаковывает ЭС в соответствии с требованиями Альбома УФЭБС;

6) шифрует ЭС с использованием открытого ключа шифрования контура контроля ЦОС в адрес СПФС Банка России в соответствии с требованиями Альбома УФЭБС;

7) формирует ЭС в формате СК в соответствии с требованиями Альбома УФЭБС;

8) помещает ЭС в формате СК в хранилище отправленных;

9) передает сформированный СК в СВК.

3.2 Обработка ЭС в формате SWIFT

При получении ЭС из соответствующего каталога обмена в формате SWIFT, направляемых пользователем СПФС на обработку в СПФС, ПК АРМ КБР-СПФС:

1) осуществляет разбор информационных блоков {1:} и {2:} сообщения, определение SWIFTBIC отправителя и SWIFTBIC получателя;

2) группирует сообщения по SWIFTBIC отправителя и SWIFTBIC получателя;

3) определяет по справочнику пользователей СПФС уникального идентификатора составителя (УИС) отправителя и УИС получателя;

4) формирует сообщения ED503 из каждой группы сообщений.

Правила формирования ED503 приведены в таблице 1.

Таблица 1 - Правила заполнения реквизитов ED503

Реквизит ED503	**Правило заполнения**
EDNo	Уникальный номер в течение операционного дня (ОД)
EDDate	Дата ОД
EDAuthor	Осуществить поиск УИС в справочнике пользователей СПФС по значению атрибута SenderSWIFTBIC
SenderSWIFTBIC	Идентификационный код отправителя в системе SWIFT. Формируется как подстрока субполя (d) информационного блока {1:} по правилу: 8 символов слева + 3 символа справа
ActualReceiver	Осуществить поиск УИС в справочнике пользователей СПФС по значению атрибута ReceiverSWIFTBIC

ReceiverSWIFTBIC	Идентификационный код получателя в системе SWIFT. Формируется как подстрока субполя (d) информационного блока {2:} по правилу: 8 символов слева + 3 символа справа
SWIFTContainerQuantity	Количество SWIFT-сообщений, помещаемых в ED503
FormatType@ed:SWIFTDocument	«MT» + субполе (c) информационного блока {2:}
TerminalSessionNum@ed:SWIFT Document	Субполе (e) информационного блока {1:} + субполе (f) информационного блока {1:}
ed:SWIFTDocument	Содержимое информационных блоков {1:}{2:}{3:}{4: -}{5:} SWIFT-сообщения, закодированных по base64

Дальнейшая обработка сообщений ED503 в ПК АРМ КБР - СПФС осуществляется по алгоритмам обработки УФЭБС- сообщений (см. п. 3.1.1), в зависимости от установленных режимов работы и других параметров конфигурации.

3.3 Обработка ЭС в собственных форматах УЭО

При получении ЭС в собственных форматах УЭО, направляемого пользователем СПФС на обработку в СПФС БР, ПК АРМ КБР-СПФС:

1) определяет имя файла сообщения. Имя файла должно быть следующим - <**УИС получателя**[10]><**уникальный в течение ОД для УИС номер**[0-9]>.ED501;

2) формирует сообщение ED501 «Конверт для ЭС в собственных форматах участников электронного обмена». Файл, содержащий сообщение в собственных

форматах УЭО, кодируется в одно ED501. Правила формирования реквизитов для ED501 приведены в таблице 2;

3) дальнейшая обработка осуществляется по алгоритмам обработки УФЭБС-сообщений (см. п.3.1.1).

Таблица 2 - Правила заполнения реквизитов ED501

Реквизит ED501	**Правило заполнения**
EDNo	Уникальный в течение ОД для УИС номер, определяется по 11-19 символам имени файла
EDDate	Дата ОД, определяется настройками
EDAuthor	УИС, определяется настройками
ActualReceiver	УИС получателя, определяется по первым 10 символам имени файла
ed: ProprietoryDocument	Документ собственного формата
ed: ProprietoryAttachment	Приложение к документу собственного формата. Не заполняется
ed:InitialED	Идентификаторы исходного ЭС. Не заполняется

4. Обработка входящих ЭС для АС пользователя СПФС

При получении из СВК ЭС формата СК, направленного СПФС Банка России в адрес пользователя СПФС, ПК АРМ КБР-СПФС:

1) помещает полученное ЭС в хранилище поступивших;

2) выполняет структурный контроль СК (валидацию по схемам УФЭБС);

3) извлекает ЭС формата SigEnvelope из ЭС в формате СК;

4) расшифровывает ЭС с использованием закрытого ключа шифрования клиента Банка России;

5) распаковывает ЭС;

6) выполняет валидацию по схемам УФЭБС расшифрованных и распакованных ЭС;

7) проверяет КА и ЗК расшифрованных и распакованных ЭС;

8) в случае успешной проверки помещает расшифрованное и распакованное ЭС в хранилище принятых, передает его в соответствующий каталог обмена.

4.1 Прием и обработка ЭС, содержащих финансовые сообщения или результаты обработки отправленных ED503

Прием и обработка ЭС, поступивших в адрес пользователя СПФС и содержащих финансовые сообщения или результаты обработки отправленных в СПФС ED503, выполняются в порядке, установленном для сообщений УФЭБС (см. п. 0) . Дополнительно ПК АРМ КБР-СПФС выполняет следующие действия:

1) определяет тип принятого сообщения и его реквизиты;
2) если полученное сообщение является ответным на переданные ED503, выполняет поиск в хранилище отправленных сообщений соответствующего начального ED503;
3) на основе полученной информации формирует сообщение в формате SWIFT

Для возможности идентификации сообщения в формате SWIFT на стороне АС пользоваткля СПФС при формировании извещения о результатах контроля ЭС ED503 для каждого SWIFT-сообщения из ed:SwiftDocument в составе начального ED503 формируется реквизит «Идентификатор входящего сообщения» по алгоритму <SenderSWIFTBIC 8 символов слева> + «X» + < SenderSWIFTBIC 3 символа справа> + значение атрибута TerminalSessionNum@ed:SWIFTDocument.

Прием и обработка ED508

Получение из ЦОС ED508 трактуется как положительный результат контроля ED503, результатом которого является формирование SWIFT-извещения вида:

{1:F21<Идентификатор входящего сообщения>}
{4:{177:yymmddhhmi}
{451:0}
}

Прием и обработка ED201

Получение из ЦОС ED201 трактуется как отрицательный результат контроля ED503, результатом которого является формирование SWIFT-извещения вида:

{1:F21<Идентификатор входящего сообщения>}

{4:{177:yymmddhhmi}

{451:1}

}

Прием и обработка ED503

Сообщение формата SWIFT извлекается из элемента ed:SWIFTDocument сообщения ED503 и передается в соответствующий каталог обмена.

4.2 Прием и обработка ЭС ED501

Прием и обработка ЭС ED501, поступивших в адрес пользователя СПФС и содержащих сообщения в собственных форматах УЭО, выполняются в порядке, установленном для сообщений УФЭБС (см. п. 0). Дополнительно ПК АРМ КБР-СПФС формирует сообщение в собственных форматах УЭО. Для каждого полученного ED501 формируется отдельный файл. В содержимое файла помещается значение элемента ProprietoryDocument после раскодирования по base64.

5. Ручной ввод ЭС

В ПК АРМ КБР-СПФС реализована возможность ручного ввода ЭС:

– ручной ввод оператором реквизитов ЭС типа ED512, ED540, ED542, ED573, ED599 в соответствии с требованиями Альбома УФЭБС;

– формирование ED503 на базе файлов в формате SWIFT. Правила формирования приведены выше (таблица 1);

– формирование ED501 на базе файлов в собственных форматах УЭО. Правила формирования приведены выше (таблица 2).

6. Описание сервисных функций

ПК АРМ КБР-СПФС в качестве вспомогательных операций выполняет следующие функции:

1) обеспечение визуального контроля процессов обработки ЭС;

2) просмотр, печать и выгрузку протоколов выполненных операций (с опциональной возможностью их автоматической очистки после выгрузки) в архивные файлы;

3) преобразование файлов ЭС формата конверта КА, СК и содержащих ЗК в формат АРМ разбора конфликтных ситуаций (РКС) СКАД «Сигнатура»;

4) обеспечение визуального контроля проверки целостности ПО при запуске ПК АРМ КБР-СПФС.

Приложение 2

Описание проверок целостности ПК АРМ КБР-СПФС

Проверка целостности ПК АРМ КБР-СПФС осуществляется автоматически при запуске ПК АРМ КБР-СПФС пользователем АРМ с функциональной ролью «Оператор» и, в дальнейшем, периодически в процессе его работы. Период самоконтроля равен 60 минутам.

В ПК АРМ КБР-СПФС реализована возможность проведения контроля состава и целостности следующих информационных объектов:

1) ПО ПК АРМ КБР-СПФС;
2) конфигурации ПК АРМ КБР-СПФС;
3) протокола выполненных операций;
4) учетных записей персонала.

В случае отрицательного результата контроля автоматически формируется электронное служебно-информационное сообщение (ЭСИС) ED997 с информацией о нарушении целостности при условии, что не повреждены конфигурационные данные, необходимые для его формирования. ЭСИС должно включать в себя версию ПК АРМ КБР-СПФС, УИС пользователя СПФС, у которого установлен ПК АРМ КБР-СПФС, кодовое описание обнаруженного нарушения, время проведения контроля состава и целостности. Сформированное ED997 не снабжается КА.

Информация о нарушении целостности направляется в Банк России средствами ПК АРМ КБР-СПФС эксплуатационным персоналом с функциональной ролью «Оператор». При этом автоматически выполняются следующие операции:

– формирование ЭС в формате СК, включающем в себя сформированное ED997 с информацией о нарушении целостности. Выполняется шифрование и упаковка содержимого тела СК. Шифрование выполняется с использованием открытого ключа контура контроля ЦОС, сертификат которого содержит OID расширенной области использования "1.3.6.1.4.1.3670.5.10.28".

– запись сформированного ЭС в формате СК в выходной ресурс ПК АРМ КБР-СПФС, предназначенный для отправки ЭС в Банк России.

После обнаружения нарушения целостности ПО и данных и формирования сообщения о нарушении целостности работа ПК АРМ КБР-СПФС блокируется средствами ПК АРМ КБР-СПФС до восстановления целостности.

В случае положительного результата контроля автоматически выполняются следующие операции:

– формирование ЭСИС ED997. ЭСИС должно включать в себя версию ПК АРМ КБР-СПФС, УИС пользователя СПФС, у которого установлен ПК АРМ КБР-СПФС, код события контроля целостности – «00», время проведения контроля состава и целостности. Сформированное ED997 не снабжается КА;

– формирование ЭС в формате СК, включающем в себя сформированное ED997. Должно быть выполнено шифрование и упаковка содержимого тела СК. Шифрование выполняется с использованием открытого ключа контура контроля ЦОС, сертификат которого содержит OID расширенной области использования «1.3.6.1.4.1.3670.5.10.28».

– запись сформированного ЭС в формате СК в выходной ресурс ПК АРМ КБР-СПФС, предназначенный для отправки ЭС в Банк России.

– Обращаем внимание, что логический адрес получателя СК, содержащего ED997 с информацией мониторинга, устанавливается в "uic:458300199900", если адрес получателя СК, указанный в реквизите служебного конверта «Адрес получателя (ЦОС)» принимает значение uic:777777700000, иначе логический адрес получателя СК, содержащего ЭС ED997 устанавливается в "uic:458300199911".