ЦВЦБ

Стандарт. Порядок подключения Финансового посредника к Платформе Цифрового Рубля

Версия 1.2

Лист изменений

ЦВЦБ. Стандарт. Порядок подключения Финансового посредника к Платформе Цифрового Рубля.		
Версия	**Дата изменения**	**Содержание изменений**
0.1	15.08.2021	Начальная версия документа для описания мероприятий, выполняемых на этапе пилота
0.2	21.11.2021	Добавлен новый раздел 7 с описанием настроек и правил взаимодействия с ТШ КБР. Скорректирован п.3.5, удалены 3.6, 3.7 (изменена нумерация) в связи с появлением раздела 7. Скорректирован п.4.3 с целью актуализации перечня СКЗИ.
0.3	09.03.2022	Скорректированы п.3.1, 3.5, 3.6 в части уточнения о разных ключевых системах на тестовом стенде ПлЦР и среде пилотирования. Скорректирован Раздел 2 в части уточнения о возможности проведения плановых работ на технической инфраструктуре. Скорректирован Раздел 4 в части общих требований к информационной безопасности и требований, предъявляемых к АС ФП. Скорректирован п.7.4 в части содержания ответа на запрос статуса узла ТШ КБР. Иные редакционные правки.
1.0	10.08.2022	Подготовлена версия для подключения к тестовому стенду ПлЦР, внесены соответствующие редакционные правки. Приложение 1. Схема бизнес-процесс скорректирована. Приложение 2. Внесены редакционные правки. Приложение 3. Внесены редакционные правки. Раздел 4. Внесены редакционные правки. В список передаваемого ПО добавлены СКЗИ «DiSec-W» и СКЗИ «МГК-3». Добавлен пункт 7.2. по настройке подключения к КС ТШ КБР. Изменена нумерация пунктов раздела 7.
1.1	28.10.2022	Раздел 3: добавлен этап пользовательского тестирования Раздел 4: уточнены требования к организации двух контуров на стороне ФП; уточнен порядок тиражирования СКЗИ Раздел 7: скорректирован, добавлена информация по требованиям к защите каналов Внесены редакционные правки по всему документу

1.2	11.01.2023	Изменено название документа. Добавлена информация по подключению к промышленному контуру ПлЦР, уровню доступности и временным регламентам. В п.3.5.1 указаны настройки для подключения к тестовому контуру ПлЦР. Ряд требований Раздела 4. Обеспечение безопасности в рамках информационного обмена перенесен в документ «ЦВЦБ. Требования по обеспечению информационной безопасности для Финансового посредника» Раздел 4.3. Порядок тиражирования СКЗИ перенесен в документ «Условия передачи программного обеспечения Клиенту Банка России» Внесены уточнения в раздел 7. Добавлен новый раздел 8 Мероприятия по предоставлению доступа представителям КО к ППУ ПлЦР. Добавлены приложения 4 и 5 (форма заявки на создание/отключение учетных записей уполномоченных пользователей ППУ ПлЦР и пример заполнения заявки). Уточнена информация о тестовом контуре – добавлен стенд «Песочница». Раздел 3 разделен на подразделы: добавлены 3.5 Подключение к тестовому контуру, 3.6 Выполнение ТИВ и пользовательского тестирования, 3.7 Подключение к промышленному контуру.

Оглавление

1. Общие положения

1.1. Назначение и область применения документа

Цель документа – установить:

- порядок и параметры подключения кредитной организации к ПлЦР в качестве Финансового посредника;
- порядок получения услуг ПлЦР.

Настоящий документ предназначен для специалистов кредитных организаций, выполняющих или планирующих подключение к ПлЦР в качестве Финансового посредника:

- службы информационных технологий и эксплуатации;
- команды разработки, вовлеченной в проект интеграции с ПлЦР;
- службы информационной безопасности;
- операционной службы.

Данная редакция документа описывает порядок и параметры подключения КО к тестовому и промышленному контурам ПлЦР.

Также в документе представлена информация, касающаяся комплекта документов, регламентирующих взаимодействие с ПлЦР в рамках промышленной эксплуатации.

1.2. Термины и сокращения

В рамках настоящего документа применяются следующие термины и сокращения.

АКС	Администратор ключевой системы
АС	Автоматизированная система
АС ФП	Автоматизированная система финансового посредника, обеспечивающая выполнение операций на ПлЦР
ГУ по ЦФО	Главное управление Центрального банка Российской Федерации по Центральному федеральному округу г. Москва
ДИТ	Департамент информационных технологий Банка России
КДБО	Комплексный договор банковского обслуживания, в рамках которого (а также в рамках отдельных документов, на которые КДБО ссылается) описаны Условия обслуживания, подключения и взаимодействия с ПлЦР[1]

[1] До 01.01.2024 договорные отношения Банка России и кредитной организации будут определены отдельным договором цифрового счета.

Клиент	Пользователь ПлЦР (физическое лицо, юридическое лицо или индивидуальный предприниматель), доступ к кошельку которого на ПлЦР обеспечивается ФП
КО	Кредитная организация
Контур контроля	Подсистема (компонент), реализующая прием ЭС, их проверку, помещение в архивы АС и передачу в контур обработки, а также прием сформированных в контуре обработки ЭС, контроль результатов обработки, проверку и отправку сформированных в контуре обработки ЭС
Контур обработки	Подсистема (компонент), реализующая прием ЭС из контура контроля, их проверку, обработку защищаемой информации, содержащейся в ЭС, а также формирование ЭС, содержащих результат обработки защищаемой информации, и передачу ЭС, сформированных по результатам обработки в контур контроля
КПКИ	Комплекс передачи ключевой информации
КС	Криптографическая сеть
ЛК	Личный кабинет участника информационного обмена на сайте Банка России
МП ФП	Мобильное приложение финансового посредника – ПО для мобильных устройств, предназначенное для обработки и формирования ЭС Клиента
Оператор ПлЦР	Организация (Банк России), обеспечивающая функционирование ПлЦР, а также выполняющая регистрацию ФП, управление статусом кошелька ФП, устанавливающая максимальное значение суммы операций с цифровыми рублями и (или) суммы остатка цифровых рублей на цифровых счетах
ОС	Операционная система
Подразделение Банка России, ПБР	Территориальное учреждение Банка России, на подведомственной территории которого расположена КО
ПК	Программный комплекс

ПлЦР	Платформа цифрового рубля – информационная система, посредством которой взаимодействуют Оператор, ФП и Клиенты в соответствии с Правилами ПлЦР, установленными Оператором ПлЦР
ПО	Программное обеспечение
Пользовательское тестирование	Тестирование МП ФП, имеющее целью подтвердить корректность реализации, оптимальность клиентского пути и эргономичность МП ФП
ППУ ПлЦР	Портал поддержки участников ПлЦР
Программный модуль Банка России (ПМ БР)	Программное обеспечение, встраиваемое в МП ФП, имеющее в своем составе встроенное сертифицированное СКЗИ для осуществления криптографических преобразований
ПС БР	Платежная система Банка России
Регистрационная карточка сертификата ключа	Документ, содержащий распечатку сертификата ключа проверки электронной подписи, включая распечатку в шестнадцатеричной системе счисления ключа проверки электронной подписи, наименование и иные реквизиты, идентифицирующие владельца ключа электронной подписи, подпись руководителя (лица, его замещающего) владельца ключа электронной подписи, а также оттиск печати (при ее наличии)
САС	Список аннулированных сертификатов
Сертификат ключа	Сертификат ключа проверки электронной подписи
СКАД	Система криптографической авторизации электронных документов
СКЗИ	Средство криптографической защиты информации
ССТ	Стенд совмещенного тестирования платежной системы Банка России
Система ЦР, Система	Совокупность услуг, ИТ-систем ФП и Оператора ПлЦР
Тестовый контур ПлЦР	Предоставляемая Банком России среда для проведения отладки на ПлЦР «Песочница», ПлЦР стенда совмещенного тестирования (ССТ) – ТИВ и пользовательского тестирования ФП
ТИВ	Тестовые испытания взаимодействия с ПлЦР, проводимые ФП на ПлЦР ССТ и имеющие целью подтвердить готовность АС ФП к

	интеграционному взаимодействию с ПлЦР, а также пользовательского тестирования ФП
ТУ	Территориальное учреждение Банка России
ТШ КБР	Транспортный шлюз Банка России для обмена платежными и финансовыми сообщениями с клиентами Банка России - участниками электронного обмена
УППИ	Участок передачи платежной информации (промышленный контур)
УПТИ	Участок передачи тестовой информации (тестовый контур)
УЦ БР	Удостоверяющий центр Банка России
УЦ ФП	Удостоверяющий центр Финансового посредника
Финансовый посредник (ФП)	Кредитная организация, предоставляющая доступ к сервисам ПлЦР своим Клиентам, либо использующая сервисы ПлЦР для выполнения своих финансовых операций – (Участник ПлЦР)
ЦВЦБ	Цифровая валюта Центрального Банка
ЦК ПС	Централизованная компонента ПС БР, обеспечивающая осуществление переводов денежных средств в платежной системе Банка России в валюте Российской Федерации в электронном виде
ЭП	Электронная подпись
ЭС	Электронное сообщение
UUID	Universally unique identifier, глобальный уникальный идентификатор
TLS	Transport Layer Security

1.3. Способы и правила взаимодействия КО, осуществляющих подключение к ПлЦР в качестве ФП, и Оператора ПлЦР

1.3.1. Взаимодействие между КО и Оператором ПлЦР в процессе подключения к ПлЦР в качестве ФП, а также дальнейшее взаимодействие между ФП и Оператором ПлЦР осуществляется следующими способами:

- путем создания запросов на ППУ ПлЦР;
- путем направления сообщений на адрес электронной почты cbdc_pilot@cbr.ru (резервный способ в случае недоступности ППУ ПлЦР);
- путем направления сообщений на адрес электронной почты на cbdc_ux@cbr.ru (резервный способ согласования макетов интерфейсов в случае недоступности ППУ ПлЦР);
- путем регулярных встреч при участии выделенного менеджера Центра операций с Цифровым рублем Департамента национальной платежной системы;
- путем обращения в обслуживающее ПБР с использованием ЛК;
- путем официальной переписки и обмена юридически значимыми документами на бумажном носителе;
- путем обмена ЭС, составленными в соответствии с требованиями документа [5], при совершении операций на ПлЦР, а также при выполнении процедуры сверки данных в системах ФП с данными на ПлЦР.

1.3.2. Обмен документами осуществляется в соответствии с порядком, установленным Соглашением о неразглашении конфиденциальной информации, заключенным между КО и Банком России.

1.4. Нормативные ссылки

[1] *ЦВЦБ. Процедура проведения тестовых испытаний взаимодействия.*

[2] *ЦВЦБ. Регламент взаимодействия Финансового посредника и Банка России при управлении криптографическими ключами Платформы Цифрового рубля.*

[3] *Платформа Цифрового рубля. Правила заполнения полей сертификатов.*

[4] *ЦВЦБ. Требования и рекомендации к пользовательским интерфейсам*

[5] *Альбом электронных сообщений, используемых для взаимодействия субъектов Платформы Цифрового рубля.*

[6] *ЦВЦБ. Требования по обеспечению информационной безопасности для Финансового посредника*

[7] *Условия передачи программного обеспечения Клиенту Банка России*

[8] *Порядок проведения пользовательского тестирования*

2. Уровень доступности ПлЦР

ПлЦР доступна 24x7 в тестовом и промышленном контурах, за исключением технологических окон проведения плановых работ. Оповещение КО о проведении плановых работ на ПлЦР будет осуществляться заблаговременно. При этом операции пополнения цифрового счета (кошелька) ФП и вывода средств с цифрового счета (кошелька) ФП могут осуществляться только в рамках стандартного периода регулярного сеанса ПС БР.

В промышленном контуре поддержка осуществляется в режиме 24x7; в тестовом контуре – в рабочие дни в период с 8.00 до 21.00 МСК, за исключением времени проведения плановых работ на технической инфраструктуре и обновления системного и прикладного ПО.

Показатель доступности ПлЦР в промышленном контуре устанавливается 99,5% (включающий плановый простой).

Требования к уровню доступности ПлЦР в тестовом контуре не предъявляются.

3. Мероприятия по подключению КО к ПлЦР

Порядок действий КО для подключения к ПлЦР в роли ФП приведен на схеме в Приложении №1.

Для подключения к ПлЦР КО необходимо выполнить мероприятия, перечисленные ниже.

3.1. Обеспечение функционирования подчиненного Удостоверяющего центра ФП

3.1.1. Для организации работы подчиненного УЦ ФП, осуществляющего процедуру выпуска сертификатов ключей клиентов КО (физических лиц, юридических лиц и индивидуальных предпринимателей), КО необходимо выполнить действия по изготовлению ключей подчиненного УЦ ФП в соответствии с п. 3.1.3.

3.1.2. Выполнить организационные и технические мероприятия для обеспечения функционирования подчиненного УЦ ФП с целью выпуска сертификатов ключей клиентов КО, используемых для совершения операций на ПлЦР, в соответствии с документами [2]-[6].

3.1.3. Для организации работы подчиненного УЦ ФП должно применяться СКЗИ, имеющее действующий сертификат ФСБ России. Для обеспечения данного требования Банком России допускается (в качестве одной из возможных опций) передача ПК СКЗИ «Сигнатура-сертификат L» версия 6 и «Сигнатура-клиент L» версия 6 в соответствии с порядком, описанным в документе [7].

3.2. Регистрация на ПлЦР и открытие кошелька ФП

3.2.1. Для регистрации на ПлЦР в качестве ФП КО предоставляет в обслуживающее ПБР комплект документов, включающий:

С использованием ЛК:

- обращение об открытии цифрового счета (кошелька) по форме Приложения №2 к настоящему документу (далее – Заявление). На Заявлении проставляется подпись единоличного исполнительного органа КО и оттиск печати (при наличии);
- заявку на создание учетных записей уполномоченных пользователей ППУ ПлЦР (в соответствии с разделом 8 документа) по форме Приложения №4.

На бумажном носителе:

- доверенность на право осуществления функций администратора ключевой системы ФП по форме Приложения №3 (далее – Доверенность АКС ФП). На доверенности проставляется подпись единоличного исполнительного органа КО и оттиск печати (при наличии).

Внимание! Допускается подписание Заявления, Доверенности АКС ФП и заявки на создание учетных записей уполномоченных пользователей ППУ ПлЦР иным представителем КО (не единоличным исполнительным органом КО) на основании выданной представителю КО доверенности за подписью единоличного исполнительного органа КО. В этом случае одновременно с указанными выше документами, подписанными иным представителем КО, КО должна предоставить также доверенность на представителя КО.

3.2.2. По итогам рассмотрения представленных документов:

- при отрицательном результате проверки обслуживающее ПБР направляет в КО письмо об отказе в приеме документов с указанием причины отказа с использованием ЛК;
- при положительном результате проверки обслуживающее ПБР готовит проект договора цифрового счета (кошелька) и, после подписания КО этого договора, Оператор ПлЦР присваивает идентификатор ФП и идентификатор цифрового счета (кошелька) ФП в тестовом контуре ПлЦР и в промышленном контуре ПлЦР и направляет данную информацию в обслуживающее ПБР, которое доводит ее до КО с использованием ЛК. Значения идентификаторов в тестовом контуре ПлЦР и в промышленном контуре ПлЦР идентичны.

3.2.3. В целях изготовления ключей для организации подписи и шифрования на прикладном уровне при взаимодействии с ПлЦР в тестовом и промышленном контурах ПлЦР, а также ключей подчиненного УЦ ФП, КО осуществляет взаимодействие с АКС УЦ БР ПлЦР согласно порядку и правилам, описанным в документах [2] и [3].

Внимание! Для взаимодействия ФП с ПлЦР в тестовом контуре ПлЦР и в промышленном контуре изготавливаются два отдельных комплекта ключей в двух отдельных ключевых системах.

При изготовлении ключей для взаимодействия с тестовым контуром ПлЦР направление в Банк России заверенных регистрационных карточек сертификатов ключей Контура контроля ФП и Контура обработки ФП, а также ключа подчиненного УЦ ФП не требуется.

3.2.4. После выполнения процедуры сертификации открытых ключей ФП Оператор ПлЦР завершает процедуру открытия кошелька ФП на ПлЦР в тестовом и промышленном контурах ПлЦР и уведомляет об этом ФП.

3.3. Доработка автоматизированных систем КО

3.3.1. Получить сертификат ключа для организации подписи и шифрования на прикладном уровне при взаимодействии с ПлЦР в соответствии с п. 3.1.3.

3.3.2. Доработать АС ФП для обеспечения выполнения операций на ПлЦР и соответствия требованиям к криптографической защите информации при выполнении операций на ПлЦР согласно требованиям документов [4-6] и раздела 4 настоящего документа.

3.4. Доработка мобильного приложения ФП

3.4.1. Согласовать с Оператором ПлЦР макеты пользовательских интерфейсов МП ФП, доработанные с учетом требований документов [4] и [6]:

3.4.1.1. Направить в адрес Оператора ПлЦР макеты пользовательских интерфейсов МП ФП, разработанные с учетом требований документа [4] в составе сообщения электронной почты с темой «<Краткое наименование КО>. ПлЦР. Макеты UI» в соответствии с правилами, указанными в п. 1.3.

3.4.1.2. Получить в ответном сообщении, направленном Оператором ПлЦР, подтверждение о допустимости использования указанных макетов в разработке.

3.4.1.3. В случае получения от Оператора ПлЦР замечаний к макетам, устранить их и направить на повторное рассмотрение Оператору ПлЦР.

3.4.2. Получить и выполнить встраивание ПМ БР в МП ФП в соответствии с порядком и требованиями, описанными в технической документации на встраиваемый ПМ БР и в документе [6].

3.4.3. Выполнить доработку МП ФП в соответствии с разработанными макетами пользовательских интерфейсов согласно требованиям документа [4], требованиями по обеспечению информационной безопасности документа [6] и раздела 4 настоящего документа для обеспечения возможности совершения операций на ПлЦР клиентами КО.

3.5. Подключение к тестовому контуру

По завершении действий, указанных в пп. 3.1- 3.4. выполнить подключение к тестовому контуру ПлЦР в соответствии с разделом 7.

Внимание! При взаимодействии ПлЦР с ЦК ПС, для ЦК ПС используется существующее (тестовое либо промышленное, в зависимости от контура) подключение КО к ТШ КБР.

Внимание! Для обмена ЭС между АС ФП и ПлЦР в тестовом контуре ПлЦР используется комплект ключей, изготовленный для работы в тестовом контуре ПлЦР.

При направлении ЭС в адрес ЦК ПС тестового контура ПлЦР в соответствующих настройках ПК АРМ КБР-Н должны указываться:

Для тестового контура – стенд ПлЦР «Песочница»:

- «Адрес отправителя (АРМ)» uic:XXXXXXXXXX**31** (где XXXXXXXXXX уникальный идентификатор составителя –УИС, 10 знаков и номер АРМ = **31** (поле <FROM:> служебного конверта)
- «Адрес получателя (ЦОИ)» uic: 458300199**31** (поле <TO:> служебного конверта).
- Также для всех исходящих ЭС из ЦК ПС среды ТИВ (ответы на ЭС, регламентные ЭС) в поле <FROM…> служебного конверта, логический адрес отправителя будет указываться uic:458300199**31**.

Для тестового контура – ПлЦР ССТ:

- «Адрес отправителя (АРМ)» uic:XXXXXXXXXX**11** (где XXXXXXXXXX уникальный идентификатор составителя –УИС, 10 знаков и номер АРМ = **11** (поле <FROM:> служебного конверта)
- «Адрес получателя (ЦОИ)» uic: 458300199**11** (поле <TO:> служебного конверта).
- Также для всех исходящих ЭС из ЦК ПС ПлЦР ССТ (ответы на ЭС, регламентные ЭС) в поле <FROM…> служебного конверта, логический адрес отправителя будет указываться uic:458300199**11**.

3.6. Выполнение ТИВ и пользовательского тестирования

3.6.1. После успешной апробации на тестовом стенде ПлЦР «Песочница» сценариев взаимодействия с ПлЦР в соответствии с документом [1] КО способами, указанными в п.1.3.1, информирует Оператора ПлЦР о готовности начать прохождение официальной процедуры ТИВ с подписанием протокола по результатам.

3.6.2. КО в согласованный с Оператором ПлЦР период прохождения ТИВ осуществляет выполнение программы ТИВ на ПлЦР ССТ в соответствии с документом [1].

3.6.3. После успешного прохождения ТИВ Оператор ПлЦР оформляет Протокол ТИВ и доводит его до КО с использованием ЛК.

3.6.4. КО в согласованный с Оператором ПлЦР период осуществляет прохождение пользовательского тестирования в соответствии с актуальной редакцией документа [8]. Пользовательское тестирование проводится на ПлЦР ССТ.

3.6.5. После успешного прохождения пользовательского тестирования Оператор ПлЦР оформляет Протокол пользовательского тестирования и доводит его до КО с использованием ЛК.

3.6.6. Оператор ПлЦР определяет Дату активации цифрового счета (кошелька) ФП в промышленном контуре ПлЦР, направляет с использованием ЛК письмо о возможности осуществления взаимодействия с ПлЦР в промышленном контуре с Даты активации.

3.7. Подключение к промышленному контуру

3.7.1. Подключение к промышленному контуру ТШ КБР осуществляется в соответствии с разделом 7.

3.7.2. При направлении ЭС в адрес ЦК ПС промышленного контура ПлЦР в соответствующих настройках ПК АРМ КБР-Н должны указываться:

Для промышленного контура ПлЦР:

- «Адрес отправителя (АРМ)» uic:XXXXXXXXXX**00** (где XXXXXXXXXX уникальный идентификатор составителя –УИС, 10 знаков и номер АРМ = **00** (поле <FROM:> служебного конверта)
- «Адрес получателя (ЦОИ)» uic: 458300199**00** (поле <TO:> служебного конверта);
- Также для всех исходящих ЭС из ЦК ПС промышленного контура ПлЦР (ответы на ЭС, регламентные ЭС) в поле <FROM…> служебного конверта, логический адрес отправителя будет указываться uic:458300199**00**.

3.7.3. Перед началом работы в промышленном контуре для проверки правильности работы транспорта, средств защиты и проверки подлинности ЭС требуется направить в промышленный контур «Зонд» (cbdc.999 Probe) и получить на него ЭС «Ответ на сообщение – зонд» (cbdc.777 ProbeNotification).

3.7.4. У КО сохраняется постоянный доступ к тестовому контуру ПлЦР (стенд ПлЦР «Песочница» и ПлЦР ССТ) для апробации доработок АС ФП и МП ФП во взаимодействии с ПлЦР перед их внедрением в промышленный контур.

3.8. Правила взаимодействия КО со сторонним разработчиком при подключении к ПлЦР

КО может привлекать стороннего разработчика для разработки ПО и выполнения иных работ. При передаче стороннему разработчику документов, указанных в п. 1.4. и иной информации, полученной от Оператора ПлЦР, необходимо руководствоваться порядком и требованиями,

установленными Соглашением о неразглашении конфиденциальной информации, заключенным между КО и Банком России.

4. Обеспечение безопасности в рамках информационного обмена

4.1. Общие требования.

4.1.1. Для обеспечения безопасности в рамках информационного обмена ФП должны осуществлять выполнение требований Положения 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» и документа [6].

4.1.2. Для обеспечения безопасности технологии обработки и передачи ЭС в ПлЦР на стороне ФП должны быть реализованы два разделенных контура: Контур контроля и Контур обработки.

4.1.3. На стороне ФП Контур контроля и Контур обработки должны быть реализованы с использованием разных рабочих мест, разных криптографических ключей и с привлечением отдельных работников для каждого из контуров.

4.1.4. Объекты информационной инфраструктуры Контура обработки и Контура контроля на стороне ФП должны быть размещены в разных сегментах вычислительных сетей.

4.2. Направление и обработка ЭС должны осуществляться ФП таким образом, чтобы все исходящие ЭС на ПлЦР поступали в Контур контроля только из Контура обработки, а все входящие ЭС от ПлЦР из Контура контроля передавались только в Контур обработки, в том числе для последующей передачи Клиенту (при необходимости).

4.2.1. Для исходящих ЭС, направляемых ФП на ПлЦР, в Контуре обработки должно быть реализовано:

- расшифрование ЭС;
- проверка ЭП ЭС;
- структурный контроль ЭС;
- проверка правильности заполнения полей ЭС;
- подписание ЭС ЭП;
- направление ЭС в Контур контроля.

4.2.2. Для исходящих ЭС, направляемых ФП на ПлЦР, в Контуре контроля должно быть реализовано:

- проверка ЭП ЭС;
- структурный контроль ЭС;
- проверка правильности заполнения полей ЭС;
- контроль отсутствия дублирования ЭС;
- подписание ЭС ЭП;
- шифрование ЭС, передаваемого на ПлЦР.

4.2.3. Для входящих ЭС от ПлЦР в Контуре контроля должны осуществляться:

- расшифрование ЭС;
- проверка ЭП ЭС;
- структурный контроль ЭС;
- подписание ЭС ЭП;
- направление ЭС в Контур обработки;

4.2.4. Для входящих ЭС от ПлЦР в Контуре обработки должны осуществляться:

- проверка ЭП ЭС;
- структурный контроль ЭС;
- проверка правильности заполнения полей ЭС;
- контроль отсутствия дублирования ЭС;
- шифрование ЭС, передаваемых клиенту ПлЦР.

4.2.5. Состав и виды ЭП, указанных в пунктах 4.2.1-4.2.4, определяются в соответствии с документом [5].

4.3. Порядок тиражирования ПМ БР и СКЗИ описан в документе [7]

5. Временные регламенты тестового контура ПлЦР

В тестовом контуре ПлЦР «Песочница» осуществляет прием и обработку ЭС от ФП в соответствии с регламентом работы ПлЦР «Песочница». Еженедельно, в последний рабочий день недели с 12:00 до 15:00 осуществляется смена операционного дня в тестовом экземпляре платежной системы Банка России стенда ПлЦР «Песочница». В качестве операционного дня устанавливается календарная дата, предшествующая календарной дате смены операционного дня.

В тестовом контуре ПлЦР ССТ осуществляет прием и обработку ЭС от ФП в соответствии с регламентом работы ССТ, регулярно обновляемом Банком России в сети Интернет по адресу http://www.cbr.ru/development/mcirabis/regl/

Взаимодействие ПлЦР с ЦК ПС осуществляется в дате операционного дня тестового экземпляра платежной системы Банка России согласно вышеуказанному регламенту.

Отдельная рассылка указанного регламента на ППУ ПлЦР, либо его рассылка по электронной почте не производится.

6. Справочники ПлЦР

При взаимодействии с ПлЦР нормативно-справочная информация в адрес ФП не направляется.

7. Протокол информационно-технического взаимодействия ФП с ТШ КБР

Обмен ЭС с ПлЦР осуществляется через отдельный контур ТШ КБР.

Данный раздел описывает подключение к тестовому и промышленному контурам ТШ КБР.

Сетевое подключение к ТШ КБР осуществляется с использованием имеющихся подключений к сетям операторов связи, предназначенных для телекоммуникационного взаимодействия с ТШ КБР.

Для организации подключения к ТШ КБР с целью взаимодействия с ПлЦР ФП должен создать запрос на ППУ ПлЦР или направить сообщение на адрес электронной почты, указанный в п.1.3.1, с темой «ПлЦР. ТШ КБР. Учетные данные <*Наименование КО*>», содержащее запрос, составленный в произвольной форме, на получение логина и пароля ФП, указываемых в заголовках HTTP-запросов, направляемых в ТШ КБР.

Учетные данные для подключения к ТШ КБР направляются ФП в ответном сообщении с соблюдением требований, установленных Соглашением о неразглашении конфиденциальной информации, заключенным между КО и Банком России.

В целях изготовления ключей для организации подключения к КС ТШ КБР КО осуществляет взаимодействие с АКС ТУ/ДИТ в соответствии с «Регламентом взаимодействия Банка России и Клиента (косвенного участника Клиента, Пользователя) при управлении криптографическими ключами», действующим в соответствующем ТУ/ДИТ.

7.1. Организация подключения к тестовому и промышленному контурам ТШ КБР средствами ПО Cisco AnyConnect

В период времени до перехода на защищённые по ГОСТ каналы связи (см. следующий раздел 7.2.) допускается использование ПО Cisco AnyConnect для установления VPN-соединения с

серверами доступа ТШ КБР. Инструкция «Порядок подключения к ТШ КБР» размещена по адресу http://cbr.ru/development/mcirabis/Involve_EM/

7.1.1 Тестовый контур

VPN-соединение средствами ПО Cisco AnyConnect может быть установлено с основным (172.16.20.42) или резервным (172.16.20.74) серверами доступа ТШ КБР. После установления VPN-соединения прикладное взаимодействие осуществляется по следующим адресам:

а) в случае организации VPN-туннеля с сервером доступа 172.16.20.42 прикладное подключение ФП должно осуществляться на адрес **172.16.19.93**;

б) в случае организации VPN-туннеля с сервером доступа 172.16.20.74 прикладное подключение ФП должно осуществляться на адрес **172.16.19.193**.

7.1.2 Промышленный контур

VPN-соединение средствами ПО Cisco AnyConnect может быть установлено с основным (172.16.20.34) или резервным (172.16.20.66) серверами доступа ТШ КБР. После установления VPN-соединения прикладное взаимодействие осуществляется по следующим адресам:

а) в случае организации VPN-туннеля с сервером доступа 172.16.20.34 прикладное подключение ФП должно осуществляться на адрес **172.16.18.93**;

б) в случае организации VPN-туннеля с сервером доступа 172.16.20.66 прикладное подключение ФП должно осуществляться на адрес **172.16.18.193**.

7.2. Организация подключения к тестовому и промышленному контурам ТШ КБР с использованием средств криптографической защиты каналов DiSec-W

7.2.1. После перехода на защищённые по ГОСТ каналы связи подключение ФП к КС ТШ КБР должно выполняться с использованием программных и/или технических средств криптографической защиты информации, обеспечивающих защиту каналов связи на основе криптографических алгоритмов, определенных национальными стандартами Российской Федерации.

7.2.2. Дата вступления указанного требования в силу – не ранее 30.06.2023 и будет сообщена дополнительно; до указанной даты возможно применение описанной в разделе 7.1. схемы подключения с использованием Cisco AnyConnect.

7.2.3. Банк России предоставляет ФП возможность выбора варианта реализации указанного требования:

- программный: при помощи установки и настройки СКЗИ «DiSec-W»; лицензии на СКЗИ «DiSec-W» предоставляются Банком России ФП на безвозмездной основе в рамках заключенного КДБО с учетом изменений, связанных с организацией взаимодействия КО с ПлЦР;

- программно-аппаратный: при помощи развертывания и настройки ПАК Dionis (далее – ПАК); в этом случае ФП должен самостоятельно и за свой счёт приобрести указанный ПАК у поставщика решения. Банк России предоставляет данные, необходимые для осуществления настроек ПАК, но не оказывает какой-либо технической поддержки по настройке и эксплуатации ПАК.

7.2.4. Используемое в программном варианте реализации СКЗИ «DiSec-W» предназначено только для защиты рабочих станций (построение криптографического туннеля от рабочей станции ФП до узлов ТШ КБР по технологии Remote Access), функционирующих под управлением ОС семейства Windows. СКЗИ «DiSec-W» должно быть установлено на каждой рабочей станции ФП, подключающейся к КС ТШ КБР, и снабжено индивидуальным набором ключевой информации. Порядок получения ключевой информации для контура ТШ КБР ПлЦР определяется каждым ТУ/ДИТ самостоятельно.

Инструкция «Порядок подключения участников обмена к автоматизированной системе «Транспортный шлюз Банка России для обмена платежными и финансовыми сообщениями с клиентами Банка России (ТШ КБР)» с использованием средств криптографической защиты каналов DiSec-W» размещена на официальном сайте Банка России по адресу:

http://www.cbr.ru/development/mcirabis/Involve_EM/

7.2.5. Для генерации ключевой информации, используемой СКЗИ «DiSec-W», должно использоваться дополнительное программное обеспечение средство криптографической защиты информации «Модуль генерации ключей - 3» (СКЗИ «МГК-3»), также распространяемое Банком России[2] на безвозмездной основе в рамках заключенного КДБО, с учетом изменений, связанных с организацией взаимодействия КО с ПлЦР.

Документ «Инструкция по изготовлению ключевой информации с использованием средства криптографической защиты информации «Модуль генерации ключей - 3» размещен на официальном сайте Банка России по адресу:

http://www.cbr.ru/development/mcirabis/Involve_EM/

В случае использования ПАК, ключевая информация может быть сгенерирована самим ПАК (см. документацию ПАК).

7.2.6. Для получения СКЗИ «DiSec-W» и СКЗИ «МГК-3» ФП подписывает акт передачи на предоставление СКЗИ согласно разделу 4.2, с указанием количества запрашиваемых экземпляров СКЗИ «DiSec-W». Количество экземпляров должно соответствовать количеству рабочих станций ФП, подключаемых к КС ТШ КБР, как в тестовом, так и в промышленном контурах.

[2] Правила эксплуатации данного ПО, включающие описание требований к отдельным техническим средствам, на которых оно должно функционировать, входят в состав дистрибутивного комплекта.

Внимание! Использование СКЗИ «DiSec-W» на ПЭВМ или серверах, выполняющих роль маршрутизаторов внутренних подсетей до ТШ КБР, не допускается.

Схема подключения с использованием СКЗИ «DiSec-W» приведена на рисунке 1, где:

- АРМ генерации ключевой информации – АРМ с установленным СКЗИ «МГК-3»;
- АРМ УППИ – программное средство КБР, используемое для обмена платежной информацией;
- АРМ УПТИ – программное средство КБР, используемое для обмена тестовой информацией;
- АРМ КПКИ УППИ – АРМ КПКИ, функционирующее в промышленном контуре;
- АРМ КПКИ УПТИ – АРМ КПКИ, функционирующее в тестовом контуре.

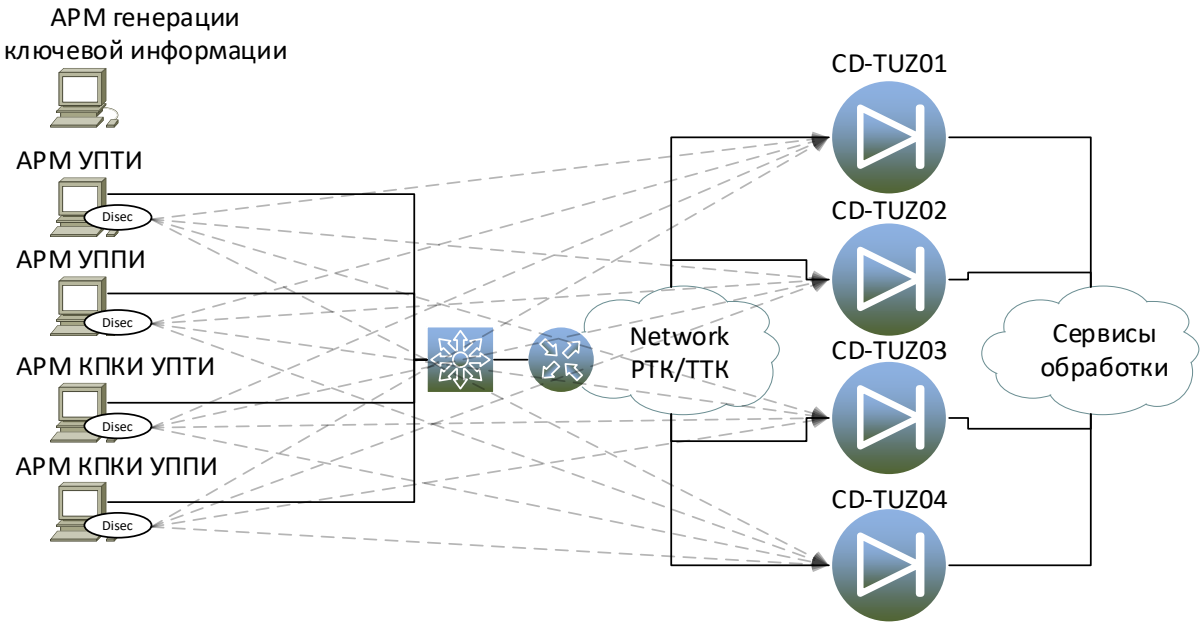


Рисунок 1 – Схема подключения с использованием СКЗИ «DiSec-W»

7.2.7. Перечень адресов УПТИ ТШ КБР (тестовый контур), разрешенных портов и протоколов взаимодействия приведён в Таблице 1.

Таблица 1. Перечень адресов УПТИ ТШ КБР, портов и протоколов взаимодействия (тестовый контур).

Наименование узла	**IP адрес в сети провайдера, до которого устанавливается VPN (узел доступа КС ТШ КБР)**	**IP адреса и порты прикладных сервисов (для ПС КБР, Личного кабинета ТШ КБР, сервиса САС и КПКИ и т.д.) внутри установленного туннеля**

Объект №1 «CD-TUZ01»	172.21.5.27 (UDP 500, UDP 4500, ESP, ICMP)	172.21.5.61 (ICMP, TCP 8888, TCP 8899, TCP 9099, TCP 9010, TCP 143, TCP 2525)
Объект №2 «CD-TUZ02»	172.21.5.35 (UDP 500, UDP 4500, ESP, ICMP)	172.21.5.62 (ICMP, TCP 8888, TCP 8899, TCP 9099, TCP 9010, TCP 143, TCP 2525)
Объект №3 «CD-TUZ03»	172.21.5.43 (UDP 500, UDP 4500, ESP, ICMP)	172.21.5.63 (ICMP, TCP 8888, TCP 8899, TCP 9099, TCP 9010, TCP 143, TCP 2525)
Объект №4 «CD-TUZ04»	172.21.5.51 (UDP 500, UDP 4500, ESP, ICMP)	172.21.5.64 (ICMP, TCP 8888, TCP 8899, TCP 9099, TCP 9010, TCP 143, TCP 2525)

Перечень адресов УППИ ТШ КБР (промышленный контур), разрешенных портов и протоколов взаимодействия приведён в Таблице 2.

Таблица 2. Перечень адресов УППИ ТШ КБР, портов и протоколов взаимодействия (промышленный контур).

Наименование узла	**IP адрес в сети провайдера, до которого устанавливается VPN (узел доступа КС ТШ КБР)**	**IP адреса и порты прикладных сервисов внутри установленного туннеля**
Объект №1 «CD-TUZ01»	172.21.1.27 (UDP 500, UDP 4500, ESP, ICMP)	172.21.1.61 (ICMP, TCP 8888, TCP 8899, TCP 9099, TCP 9010, TCP 143, TCP 2525)
Объект №2 «CD-TUZ02»	172.21.1.35 (UDP 500, UDP 4500, ESP, ICMP)	172.21.1.62 (ICMP, TCP 8888, TCP 8899, TCP 9099, TCP 9010, TCP 143, TCP 2525)
Объект №3 «CD-TUZ03»	172.21.1.43 (UDP 500, UDP 4500, ESP, ICMP)	172.21.1.63 (ICMP, TCP 8888, TCP 8899, TCP 9099, TCP 9010, TCP 143, TCP 2525)
Объект №4 «CD-TUZ04»	172.21.1.51 (UDP 500, UDP 4500, ESP, ICMP)	172.21.1.64 (ICMP, TCP 8888, TCP 8899, TCP 9099, TCP 9010, TCP 143, TCP 2525)

7.2.8. Номера TCP-портов сервисов ТШ КБР, предоставляемых после построения криптографического туннеля, приведены в Таблице 3.

Таблица 3. Номера TCP-портов сервисов ТШ КБР.

Номер TCP-порта	Сервис ТШ КБР
8888	сервис передачи ЭС по протоколу HTTPS
8899	сервис смены пароля прикладной учётной записи ФП
9010	сервис доступа к личному кабинету КПКИ по протоколу https
143	сервис доступа к почтовому серверу КПКИ по протоколу IMAP (при использовании почтового клиента)
2525	сервис доступа к почтовому серверу КПКИ по протоколу SMTP (при использовании почтового клиента)
9099	сервис централизованного распространения CAC

7.3. Порядок обмена

Инициатором обмена всегда выступает ФП.

Прикладное взаимодействие ПО ФП с ТШ КБР осуществляется по протоколу HTTP 1.1 [RFC 2616] поверх протокола TLS [RFC 5246].

Внимание! ФП в рамках установленных VPN-туннелей может быть доступно одновременно от одного до четырёх узлов ТШ КБР для осуществления обмена. ФП должен балансировать http-запросы между всеми доступными ему узлами ТШ КБР. При определении доступности узлов ТШ КБР необходимо учитывать, как сетевую видимость прикладного порта взаимодействия (TCP 8888), так и ответы, возвращаемые сервисом проверки статуса узла ТШ КБР (nodestate), подробнее см. раздел 7.6 ниже.

Внимание! В рамках обмена ЭС, при формировании URL HTTP-запросов, приведенных далее по тексту документа, следует использовать **суффикс**.

Суффикс для использования в промышленном контуре: **cbdc.**

Суффикс для использования в тестовом контуре CCT: **cbdc** (на CCT совпадает с суффиксом для использования в промышленном контуре).

Суффикс для использования в тестовом контуре «Песочница»: **sandbox.**

7.4. Отправка сообщения ФП

Отправка ФП ЭС на ТШ КБР осуществляется посылкой HTTP-запроса (HTTP request) методом POST по протоколу HTTP 1.1 [RFC 2616] на URL **https://хост:8888/<суффикс>/post**.

Заголовки HTTP-запроса должны содержать следующие обязательные значения:

Authorization	Authorization: Basic xxxxxxxxxxxxxxxxxx, где xxxxxxxxxxxxxxxxxx – данные ФП. Данные ФП формируются следующим образом: а) логин и пароль, разделённые двоеточием, пример: aladdin:opensesame; б) результирующая строка, закодированная в Base64 (RFC4648) пример: YWxhZGRpbjpvcGVuc2VzYW1l.

	При отсутствии данного заголовка ТШ КБР посылает HTTP-ответ (HTTP response) с телом служебного сообщения и кодом ответа 401- требования аутентификации
Content-type	*Content-type* – идентификатор сообщения ЦР: “application/xml”. Не кодируется в Base64.
Connection	Connection: keep-alive

Тело сообщения содержит XML сообщение - не кодируется в Base64. XML сообщение должно быть оформлено в соответствии с документом [5].

Максимальное время ожидания ответа на запрос ФП составляет 5 секунд с момента направления ФП POST-запроса.

В ответ на запрос ТШ КБР возвращает HTTP-ответ (HTTP response) с пустым телом и кодом ответа:

а) 20X, как факт успешного принятия сообщения:
   1) 202 – запрос принят в работу;

б) 30X, перенаправление запроса:
   1) 302 – следующий запрос направлять на другой узел, указанный в заголовке ответа в поле Location;

в) 40X – требования к пользовательским действиям:
   1) 400 – неправильный формат;
   2) 401 – необходима аутентификация;
   3) 404 – неправильный запрос;

г) 50X – ошибки системы:
   1) 501 – внутренняя ошибка.

Заголовок HTTP-ответа, в случае успешного принятия сообщения содержит следующие значения (но не ограничивается ими):

InstanceID	*InstanceID* - идентификатор, передаваемого сообщения. Используется для идентификации сообщения (формат random UUID). Не кодируется в Base64

7.5. Получение сообщения ФП

Получение ФП ЭС из ТШ КБР осуществляется посылкой HTTP-запроса (HTTP request) методом GET по протоколу HTTP 1.1 [RFC 2616] на URL **https://хост:8888/<суффикс>/get.**

Заголовки HTTP-запроса должны содержать следующие обязательные значения:

Authorization	Authorization: Basic `xxxxxxxxxxxxxxxxxx`, где `xxxxxxxxxxxxxxxxxx` – данные ФП. Данные ФП формируются следующим образом: а) логин и пароль, разделённые двоеточием, пример: `aladdin:opensesame`; б) результирующая строка, закодированная в Base64 (RFC4648) пример: `YWxhZGRpbjpvcGVuc2VzYW1l`.

	При отсутствии данного заголовка ТШ КБР посылает HTTP-ответ (HTTP response) с телом служебного сообщения и кодом ответа 401- требования аутентификации
Connection	Connection: keep-alive

Максимальное время ожидания ответа на запрос ФП составляет 2 секунды с момента направления ФП запроса.

Следующий запрос на получение сообщения должен быть направлен ФП сразу после получения ответа на предыдущий запрос.

При осуществлении взаимодействия в тестовом контуре направление запросов на получение сообщений от ТШ КБР осуществляется не более, чем в 10 потоков.

В ответ на запрос ТШ КБР возвращает HTTP-ответ (HTTP response) с телом, содержащим ЭС (при его наличии) и кодом ответа:

а) 20X, как факт успешной обработки запроса:
   1) 200 – сообщение обработано успешно
   2) 204 – нет сообщений

б) 30X, перенаправления сообщения:
   1) 302 – следующий запрос направлять на другой узел, указанный в заголовке ответа в поле Location:

в) 40X – требования к пользовательским действиям (требование аутентификации или сообщение об отсутствии сообщений в очереди):
   1) 401 – необходима аутентификация
   2) 404 – неправильный запрос

г) 50X – ошибки системы:
   1) 501 - внутренняя ошибка

В случае успешной обработки запроса ФП (код 200), заголовок HTTP-ответа содержит следующие значения (но не ограничивается ими):

Content-type	*Content-type* – идентификатор сообщения ЦР: application/xml. Не кодируется в Base64.
InstanceID	*InstanceID* – идентификатор, принимаемого сообщения. Используется для идентификации сообщения (формат random UUID). Не кодируется в Base64.

Тело сообщения содержит XML сообщение - не кодируется в Base64. XML сообщение оформлено в соответствии с документом [5].

7.6. Проверка ФП статуса узла ТШ КБР

ФП должен проверять статус каждого доступного ему узла ТШ КБР.

Получение ФП статуса узла ТШ КБР осуществляется посылкой HTTP-запроса (HTTP request) методом GET по протоколу HTTP 1.1 [RFC 2616] на URL **https://хост:8888/< суффикс>/nodestate.**

Заголовки HTTP-запроса содержат следующие значения:

Authorization	Authorization: Basic xxxxxxxxxxxxxxxxxx, где xxxxxxxxxxxxxxxxxx – данные ФП. Данные ФП формируются следующим образом: а) логин и пароль, разделённые двоеточием, пример: aladdin:opensesame; б) результирующая строка, закодированная в Base64 (RFC4648) пример: YWxhZGRpbjpvcGVuc2VzYW1l. При отсутствии данного заголовка ТШ КБР посылает HTTP-ответ (HTTP response) с телом служебного сообщения и кодом ответа 401 - требования аутентификации
Connection	Connection: keep-alive

Ответ (http-response) содержит статус узла в следующем виде:

а) заголовок ответа содержит код ответа 502 (Bad Gateway), тело содержит значение 0 – узел неработоспособен, либо планируется вывод узла из работы. Необходимо как можно скорее прекратить передачу сообщений через данный узел;

б) заголовок ответа содержит код ответа 200 (OK), тело содержит значение 1 – узел работает в штатном режиме.

Максимальное время ожидания ответа на запрос ФП статуса узла составляет 30 секунд с момента направления ФП запроса. Если в течении 30 секунд с момента направления ФП запроса ответ не получен, данный узел считается выведенным из эксплуатации и ФП не должен направлять на данный узел запросы на передачу и получение сообщений.

Следующий запрос на получение статуса узла ТШ КБР должен быть направлен ФП сразу после получения ответа на предыдущий запрос.

Направление запросов на получение статуса узла ТШ КБР должно осуществляться в один поток с каждого из АРМ ФП.

8. Мероприятия по предоставлению доступа представителям КО к ППУ ПлЦР

8.1. Общие сведения

8.1.1. ППУ ПлЦР предназначен для автоматизации процедур взаимодействия представителей ФП с Банком России по вопросам функционирования ПлЦР в части:

- запросов на техническую поддержку по работе компонентов ПлЦР;
- запросов на получение консультаций по правилам ПлЦР;
- запросов на получение консультаций по документарному обеспечению работы с ПлЦР;
- возможности получения (скачивания) инструктивных и нормативных документов по работе с ПлЦР;

- прочих вопросов, возникающих у ФП по работе с ПлЦР.

8.1.2. Доступ к ППУ ПлЦР для авторизованных пользователей осуществляется через сеть интернет по адресу https://support-dr.cbr.ru.

8.1.3. В рамках настоящего документа описывается только предоставление доступа к ППУ ПлЦР работникам ФП с ролью «Уполномоченный пользователь ФП» (см. п.8.2 ниже). Регистрация «обычных» пользователей ФП, как и работа с ППУ ПлЦР в целом, описана в инструкции по работе с ППУ ПлЦР, размещенной в разделе «Документы» на главной странице ППУ ПлЦР.

8.2. Описание ролевой модели

В процедурах предоставления и прекращения предоставления доступа к порталу поддержки ПлЦР участвуют следующие роли:

8.2.1. Уполномоченный пользователь ФП - сотрудник ФП, выполняющий регистрацию обращений в Банк России с использованием ППУ ПлЦР по вопросам подключения/отключения/смены пароля/разблокировки учетных записей Пользователей ФП на ППУ ПлЦР. Также включает в себя функции и права доступа роли «Пользователь ФП». На роль уполномоченного пользователя ФП требуется назначение 3 (трех) работников от каждого ФП.

8.2.2. Пользователь ФП - сотрудник ФП, выполняющий взаимодействие с Банком России с использованием ППУ ПлЦР.

8.2.3. Работник обслуживающего ПБР - сотрудник подразделения Банка России. Осуществляет прием заявок от ФП на предоставление его сотруднику прав доступа к ППУ ПлЦР с ролью «Уполномоченный пользователь ФП». Проверяет полноту и корректность заполнения заявки. Инициирует создание учетной записи уполномоченного сотрудника ФП.

8.3. Порядок предоставления доступа пользователям

8.3.1. Для получения доступа к ППУ ПлЦР с ролью «Уполномоченный пользователь ФП», ответственный представитель ФП направляет в обслуживающее ПБР комплект документов, содержащий заявку на создание учетных записей уполномоченных пользователей ППУ ПлЦР через ЛК. Форма заявки приведена в Приложении 4.

8.3.2. Работник обслуживающего ПБР проверяет полноту и корректность заполнения заявки, выполняет контроль количества пользователей, указанных в заявке, регистрирует заявку для регистрации нового пользователя ППУ ПлЦР.

8.3.3. После выполнения заявки по электронной почте на адреса пользователей, указанных в заявке, направляются сообщения, содержащие имена и пароли созданных пользователей и ссылку на вход в ППУ ПлЦР.

8.3.4. Заявку на подключение пользователя с ролью «Пользователь ФП» в ППУ ПлЦР регистрирует пользователь ППУ ПлЦР с ролью «Уполномоченный пользователь ФП» с использованием заявки «Регистрация пользователя» раздела «Управление пользователями портала поддержки».

8.3.5. При первом входе пользователя на ППУ ПлЦР пользователю будет предложено в обязательном порядке сменить первоначально установленный пароль на новый.

8.3.6. Требования к паролю содержатся в Инструкции по работе с ППУ ПлЦР, размещенной в разделе «Документы» на главной странице ППУ ПлЦР.

8.4. Изменение перечня сотрудников с ролью «Уполномоченный пользователь ФП»

8.4.1. Если у ФП меняются сотрудники, которым на основании ранее предоставленной Заявки уже был предоставлен доступ к ППУ ПлЦР, ФП повторно оформляет и направляет в ПБР заявку на подключение/отключение уполномоченных пользователей к ППУ ПлЦР с актуальным перечнем через ЛК. Форма заявки приведена в Приложении 4. Пример заполнения приведен в Приложении 5.

8.4.2. Существующие учетные записи пользователей ФП с ролью «Уполномоченный пользователь ФП», у которых в заявке в поле «Действие» указано «Отключить» - отключаются.

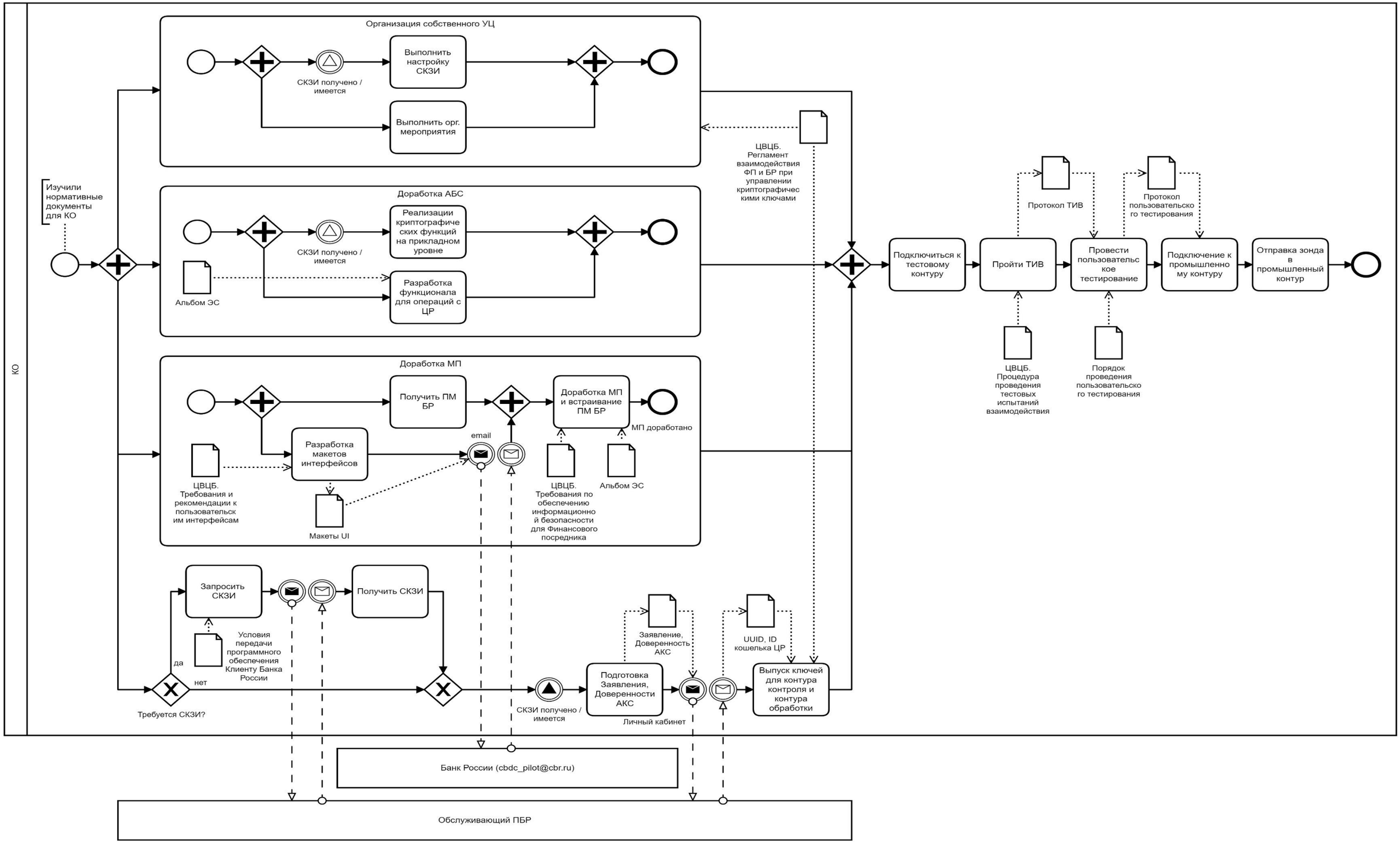
8.4.3. Для сотрудников ФП, у которых в заявке в поле «Действие» указано «Подключить» создаются новые учетные записи по аналогии с п.8.3. настоящего Регламента.

8.4.4. Для сотрудников ФП, у которых в заявке поле «Действие» не заполнено, никаких действий не выполняется, роль «Уполномоченный пользователь ФП» у них сохраняется.

8.4.5. Срок выполнения работ по предоставлению/изменению/прекращению доступа пользователей с ролью «Уполномоченный пользователь ФП» – 5 рабочих дней.

8.4.6. Действия, описанные в данном пункте Регламента, также выполняются при утрате доступа к ППУ ПлЦР всех пользователей с ролью «Уполномоченный пользователь ФП».

Приложение № 1. Порядок действий КО при подключении к тестовому и промышленному контурам ПлЦР



Приложение № 2. Форма Обращения об открытии цифрового счета (кошелька)

Руководителю
подразделения Банка России[3]

Обращение
об открытии цифрового счета (кошелька)

Прошу подключить к Платформе Цифрового рубля и открыть цифровой счет (кошелек)

_____

(указывается полное наименование кредитной организации, номер лицензии на осуществление банковских операций)

.

Сведения о кредитной организации:

1. _____
(наименование кредитной организации)

2. _____
(банковский идентификационный код)

3. _____
(номер корреспондентского счета)

Приложение на __ л.[4]

_____	_____	_____
(наименование должности лица, подписавшего обращение)	(личная подпись)	(инициалы, фамилия)

М.П.
«___» _____ _____ года

[3] Указываются должность руководителя подразделения Банка России, обслуживающего корреспондентский счет КО, наименование данного подразделения Банка России, инициалы и фамилия руководителя в дательном падеже.

[4] Копия доверенности лица, подписавшего настоящее обращение, если обращение подписывается лицом, действующим на основании доверенности.

Приложение № 3. Форма Доверенности АКС ФП

ДОВЕРЕННОСТЬ

на право осуществления функций администратора ключевой системы финансового посредника

Страна, город, число

Наименование организации, в лице *должность ФИО*, действующего на основании _____, настоящей доверенностью уполномочивает *должность, ФИО*[5] *(номер телефона, эл. почта*[6]*), должность, ФИО (номер телефона, эл. почта)* осуществлять функции ответственного за управление криптографическими ключами в рамках взаимодействия с Платформой Цифрового рубля.

Предоставленные полномочия могут осуществляться каждым из перечисленных сотрудников в отдельности.

Полномочия по настоящей доверенности не могут быть переданы другим лицам.

Подпись *ФИО* _____ удостоверяю
(подпись доверенного лица)

Подпись *ФИО* _____ удостоверяю
(подпись доверенного лица)

Настоящая доверенность выдана на срок по *<ДД.ММ.ГГГГ>*.

_____	_____	_____
(наименование должности лица, подписавшего доверенность)	(личная подпись)	(инициалы, фамилия)

М.П.

« » года

[5] Количество лиц, ответственных за управление криптографическими ключами, должно быть не менее двух.
[6] В доверенности должен быть указан один адрес электронной почты, доступный всем уполномоченным лицам.

Приложение № 4. Форма заявки на создание/отключение учетных записей уполномоченных пользователей Портала поддержки Платформы Цифрового рубля

Заявка на создание/отключение учетных записей уполномоченных пользователей
Портала поддержки Платформы Цифрового рубля

_____

(указывается полное наименование кредитной организации)

№	БИК организации	Фамилия[1]	Имя	Отчество	Email[2]	Действие[3]	Контактный телефон
1							
2							
3							

_____ _____ _____

(наименование должности лица, подписавшего заявку) (личная подпись) (инициалы, фамилия)

« » года

___ _____ _____ М.П.

[1] Необходимо указать суммарно трех сотрудников, для которых запрашивается и/или уже предоставлен доступ, в противном случае форма считается недействительной и требует исправления со стороны КО.

[2] В email должен использоваться корпоративный домен, использование адресов публичных почтовых сервисов недопустимо.

[3] Необходимо указать одно из значений:

- «Подключить», если необходимо предоставить доступ новому пользователю с ролью «Уполномоченный пользователь ФП»;
- «Отключить», если необходимо прекратить доступ существующему пользователю с ролью «Уполномоченный пользователь ФП»;
- Не заполнять, если по существующему пользователю с ролью «Уполномоченный пользователь ФП» никаких действий выполнять не требуется.

Приложение № 5. Пример заполнения заявки на создание/отключение учетных записей уполномоченных пользователей Портала поддержки Платформы Цифрового рубля

Заявка на создание/отключение учетных записей уполномоченных пользователей
Портала поддержки Платформы Цифрового рубля

Кредитная организация «Банк1»

(указывается полное наименование кредитной организации)

№	БИК организации	Фамилия	Имя	Отчество	Email	Действие	Контактный телефон
1	04XXXXXXXX	Иванов	Иван	Иванович	ivanovii@bank1.ru	Подключить	(495) 111-11-11
2	04XXXXXXXX	Петров	Петр	Петрович	petrovpp@bank1.ru		(495) 111-11-12
3	04XXXXXXXX	Сидоров	Дмитрий	Алексеевич	sidorovda@bank1.ru	Подключить	(495) 111-11-13
4	04XXXXXXXX	Морозов	Сергей	Григорьевич	morozovsg@bank1.ru	Отключить	
5	04XXXXXXXX	Федоров	Иван	Сергеевич	fedorovis@bank1.ru	Отключить	

В представленном примере для пользователей, входящих в роль «Уполномоченный пользователь ФП»:

1) запрашивается отключение существующих пользователей Морозова С.Г. и Федорова И.С.;

2) запрашивается предоставление доступа для новых пользователей ФП Иванова И.И. и Сидорова Д.А.;

3) для существующего пользователя Петрова П.П. никаких действий не запрошено (роль сохраняется).

В итоге в заявке содержится три сотрудника, которые после выполнения заявки будут иметь доступ к ППУ ПлЦР с ролью «Уполномоченный пользователь ФП», требование к максимальному количеству таких пользователей ролью «Уполномоченный пользователь ФП» соблюдено.