Порядок подключения участников обмена к автоматизированной системе «Транспортный шлюз Банка России для обмена платежными и финансовыми сообщениями с клиентами Банка России (ТШ КБР)» с использование средств криптографической защиты каналов DiSec-W

(версия 1.1 от 06.05.2024)

1. Введение

1.1. Назначение

ТШ КБР предназначен для обеспечения централизованного доступа участников обмена к платёжной системе Банка России и пользователей СПФС к СПФС путем обмена электронными сообщениями.

Для доступа к обмену электронными сообщениями на прикладном уровне необходимо установить защищенное VPN-соединение с использованием СКЗИ DiSec-W. При установлении соединениями используется метод двусторонней аутентификации на основе сертификатов. Генерация ключевой информации и получение сертификатов осуществляется в соответствии с инструкцией на СКЗИ МГК-3, получаемой в обслуживающем вас Территориальном учреждении.

На прикладном уровне обмен ЭС через ТШ КБР можно осуществлять по протоколам HTTP, WMQ с использованием, как специализированных программных комплексов в режиме «система-система» (например АРМ КБР-Н, АРМ КБР СПФС и т.д.), так и через Web-браузер из состава используемой на технических средствах участника обмена операционной системы для работы по протоколу HTTPS в режиме «клиент-система».

1.2. Программные средства, устанавливаемые на автоматизированном рабочем месте участника обмена

1) Операционная система MS Windows 10;

2) Web-браузер «Internet Explorer» (версии 11 и выше), Web-браузер «Google Chrome» (версии 66 и выше) или «Mozilla FireFox» (версии 56 и выше) для работы с личным кабинетом ТШ КБР (при обмене ЭС с ТШ КБР в режиме «клиент-система»);

3) СКЗИ DiSec-W, для построения защищённого VPN-соединения

4) Программный комплекс АРМ КБР-Н / АРМ КБР-СПФС версии не ниже 2020.3 при обмене ЭС с ТШ КБР в режиме «система-система».

1.3. Общий порядок действий участника обмена при настройке подключения к ТШ КБР

1) Установить системное и общее программное обеспечение на ПЭВМ участника обмена;

2) Убедиться в сетевой доступности серверов доступа ТШ КБР с которыми устанавливается VPN-соединение;

3) Установить и настроить СКЗИ МГК-3 (для генерации ключевой информации) в соответствии с инструкцией на СКЗИ МГК-3, получаемой в обслуживающем вас Территориальном учреждении;

4) Установить, активировать и настроить СКЗИ DiSec-W (для организации VPN-соединения) в соответствии с **Приложением 1;**

5) Убедиться в сетевой доступности прикладных сервисов ТШ КБР внутри установленных VPN-соединений;

6) Настроить специальное программное обеспечение на ПЭВМ участника обмена (ПК АРМ КБР-Н/ПК АРМ КБР-СПФС) для взаимодействия с промышленным/тестовым ТШ КБР в соответствии с **Приложением 2**;

Приложение 1

Инструкция по подключению Клиента Банка России к криптографической сети Транспортного шлюза для обмена платежными и финансовыми сообщениями с клиентами Банка России с использованием СКЗИ «Disec-W»

В настоящем документе приведено описание подключения клиента Банка Россиик криптографической сети Транспортного шлюза Банка России для обмена платежными и финансовыми сообщениями с клиентами Банка России с использованием СКЗИ «DiSec-W», а также настройки программных средств защиты информации клиентов Банка России для реализации данного подключения. Данная инструкция отменяет действие инструкции № ТРД-16-2-8-3/2094 от 13.08.2022.

Содержание

Обозначения и сокращения

Сокращение	Расшифровка сокращения
АРМ	Автоматизированное рабочее место
Банк	Банк России
Клиент	Клиент Банка России
КС	Криптографическая сеть
КПКИ	Комплекс передачи ключевой информации
МГК	Модуль генерации ключей
ОМНИ	Отчуждаемый машинный носитель информации
ПАК	Программно-аппаратный комплекс
ПС КБР	Программные средства клиента Банка России (ПК АРМ КБР, ПК АРМ КБР-Н, ПК АРМ КБР-СПФС)
ПЭВМ	Персональная электронно-вычислительная машина
САС	Список аннулированных сертификатов, в интерфейсе СКЗИ «DiSec-W» – список отозванных сертификатов (СОС)
СПО	Специализированное программное обеспечение
ТШ КБР	Транспортный шлюз Банка России для обмена платежными и финансовыми сообщениями с клиентами Банка России
УЗ	Учетная запись
УППИ	Участок передачи платежной информации (промышленная среда)
УПТИ	Участок передачи тестовой информации (тестовая среда)
УЦ	Удостоверяющий центр на базе СКЗИ «СКАД Сигнатура»

1 Общие сведения по подключению к КС ТШ КБР

Подключение Клиента к КС ТШ КБР должно выполняться с использованием программных и/или технических средств криптографической защиты информации.

В качестве программного средства криптографической защиты информации Банк России на безвозмездной основе передает Клиенту СКЗИ «DiSec-W»[1], распространяемое Банком на безвозмездной основе, используемого только для защиты рабочих станций (построение криптографического туннеля от рабочей станции Клиента до узлов ТШ КБР по технологии Remote Access), функционирующих под управлением операционных систем семейства Windows. Данное СКЗИ должно быть установлено на каждой рабочей станции Клиента, подключающейся к ТШ КБР, и снабжено индивидуальным набором ключевой информации: закрытый ключ, сертификат ключа, сертификаты центров сертификации и их CAC (далее – ключевая информация).

Клиент получает в Банке России дистрибутив и лицензии на установку СКЗИ «DiSec-W» Количество запрашиваемых лицензий соответствует количеству рабочих станций Клиента, подключаемых к ТШ КБР, как в тестовой, так и в промышленной среде.

Для генерации ключевой информации, используемой СКЗИ «DiSec-W», должно использоваться дополнительное программное обеспечение СКЗИ «Модуль генерации ключей - 3» (далее – МГК-3), также распространяемое Банком России (Правила эксплуатации данного ПО, включающие описание требований к отдельным техническим средствам, на которых оно должно функционировать, входят в состав дистрибутивного комплекта). Описание процедуры по генерации ключевой информации представлено в Инструкции по генерации ключевой информации с использованием СКЗИ «МГК-3».

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.

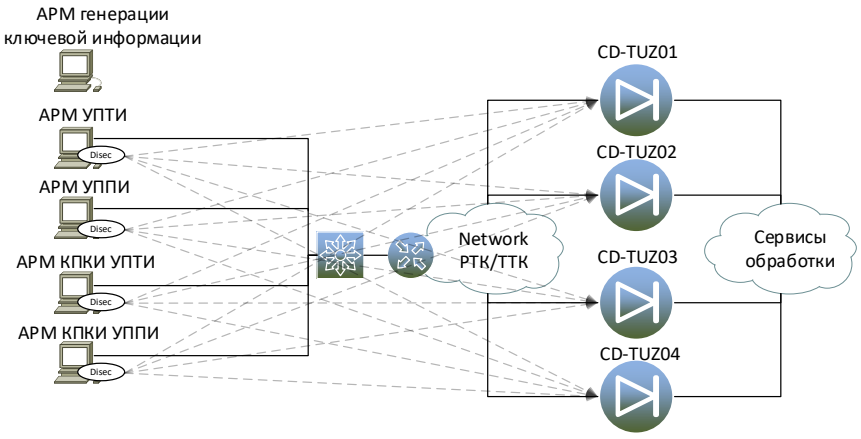


Рисунок 1 – Схема подключения с использованием СКЗИ «DiSec-W»

[1] Клиент может самостоятельно и за свой счёт приобрести программно-аппаратное решение для обеспечения защиты каналов связи. Перечень совместимого оборудования необходимо уточнять в ООО «Фактор-ТС». Банк России не оказывает технической поддержки по настройке и эксплуатации таких программно- аппаратных комплексов

Где: АРМ генерации ключевой информации – АРМ с установленным СКЗИ «МГК-3»;

АРМ УППИ – ПС КБР, функционирующее в промышленной среде;

АРМ УПТИ – ПС КБР, функционирующее в тестовой среде;

АРМ КПКИ УППИ – АРМ КПКИ, функционирующее в промышленной среде;

АРМ КПКИ УПТИ – АРМ КПКИ, функционирующее в тестовой среде;

Перечень адресов УПТИ ТШ КБР (тестовая среда), разрешенных портов и протоколов взаимодействия приведён в Таблице 1.

Таблица 1 – Перечень адресов УПТИ ТШ КБР (тестовая среда), разрешенных портов и протоколовзаимодействия

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, КПКИ и т.д.) внутри установленного туннеля**
Объект №1 «CD-TUZ01»	172.21.5.26 (UDP 500, UDP 4500, ESP, ICMP)	172.21.5.57 (ICMP, TCP 7777, TCP 8888, TCP 1414, TCP 9696, TCP 9697, TCP 9099, TCP 9010, TCP 143, TCP 2525)
Объект №2 «CD-TUZ02»	172.21.5.34 (UDP 500, UDP 4500, ESP, ICMP)	172.21.5.58 (ICMP, TCP 7777, TCP 8888, TCP 1414, TCP 9696, TCP 9697, TCP 9099, TCP 9010, TCP 143, TCP 2525)
Объект №3 «CD-TUZ03»	172.21.5.42 (UDP 500, UDP 4500, ESP, ICMP)	172.21.5.59 (ICMP, TCP 7777, TCP 8888, TCP 1414, TCP 9696, TCP 9697, TCP 9099, TCP 9010, TCP 143, TCP 2525)
Объект №4 «CD-TUZ04»	172.21.5.50 (UDP 500, UDP 4500, ESP, ICMP)	172.21.5.60 (ICMP, TCP 7777, TCP 8888, TCP 1414, TCP 9696, TCP 9697, TCP 9099, TCP 9010, TCP 143, TCP 2525)

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

Таблица 2 – Перечень адресов УППИ ТШ КБР (промышленная среда), разрешенных портов и протоколов взаимодействия

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 CAC, КПКИ и т.д.) внутри установленного туннеля**
Объект №1 «CD-TUZ01»	172.21.1.26 (UDP 500, UDP 4500, ESP, ICMP)	172.21.1.57 (ICMP, TCP 7777, TCP 8888, TCP 1414, TCP 9696, TCP 9697, TCP 9099, TCP 9010, TCP 143, TCP 2525)
Объект №2 «CD-TUZ02»	172.21.1.34 (UDP 500, UDP 4500, ESP, ICMP)	172.21.1.58 (ICMP, TCP 7777, TCP 8888, TCP 1414, TCP 9696, TCP 9697, TCP 9099, TCP 9010, TCP 143, TCP 2525)
Объект №3 «CD-TUZ03»	172.21.1.42 (UDP 500, UDP 4500, ESP, ICMP)	172.21.1.59 (ICMP, TCP 7777, TCP 8888, TCP 1414, TCP 9696, TCP 9697, TCP 9099, TCP 9010, TCP 143, TCP 2525)
Объект №4 «CD-TUZ04»	172.21.1.50 (UDP 500, UDP 4500, ESP, ICMP)	172.21.1.60 (ICMP, TCP 7777, TCP 8888, TCP 1414, TCP 9696, TCP 9697, TCP 9099, TCP 9010, TCP 143, TCP 2525)

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**
7777	сервис передачи ЭС по протоколу HTTP
8888	сервис передачи ЭС по протоколу HTTP
1414	сервис передачи ЭС по протоколу IBM MQ
9697	сервис доступа к личному кабинету КБР по протоколу https
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

2 Установка СКЗИ «DiSec-W»

2.1 Подготовительные работы

Во избежание некорректной работы программы перед СКЗИ «DiSec-W» необходимо: установить на АРМ:

а) Windows 10 LTSC (сборка должна быть не ниже 1809);

б) Windows 10 Pro (сборка должна быть не ниже 21H2);

в) обновления ОС Windows, выпущенные компанией Microsoft;

г) 32-разрядные библиотеки Microsoft Visual C++ (Visual Studio 2015-2022) по ссылке https://aka.ms/vs/17/release/vc_redist.x86.exe

д) 64-разрядные библиотеки Microsoft Visual C++ (Visual Studio 2015-2022) по ссылке https://aka.ms/vs/17/release/vc_redist.x64.exe

В случае конфликта устанавливаемых библиотек Microsoft Visual C++ (Visual Studio 2015-2022) с ранее установленными на компьютере отдельными библиотеками Microsoft Visual C++ 2015, 2017, 2019 или 2022 необходимо выполнить удаление таких отдельных библиотек и установить рекомендуемые.

Установка СКЗИ «Disec-W» выполняется на ПВЭМ, подключенной к телекоммуникационной сети и имеющей доступ через операторов связи к узлам КС ТШ КБР.

В Н И М А Н И Е ! Ниже будет описана настройка тестовой среды (УПТИ), промышленная среда (УППИ) настраивается аналогично, требуется только указатьсоответствующие IP-адреса узлов КС ТШ КБР промышленной среды.

Если между оператором связи и АРМ, на который устанавливается СКЗИ «Disec-W», функционирует промежуточное сетевое оборудование, то для корректной работы СКЗИ «Disec-W» на промежуточном сетевом оборудовании **в сторону узлов КС ТШ КБР и обратно** должны быть открыты следующие порты и протоколы:

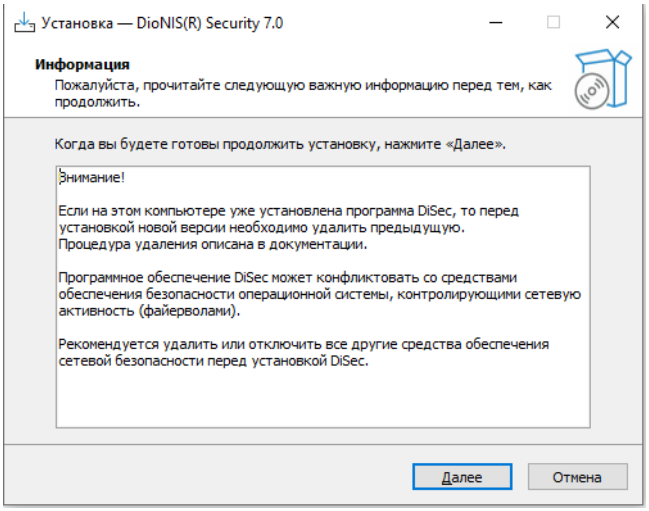
1) протокол UDP - порт 500;
2) протокол UDP - порт 4500;
3) протокол ESP.

2.2 Установка СКЗИ «Disec-W»

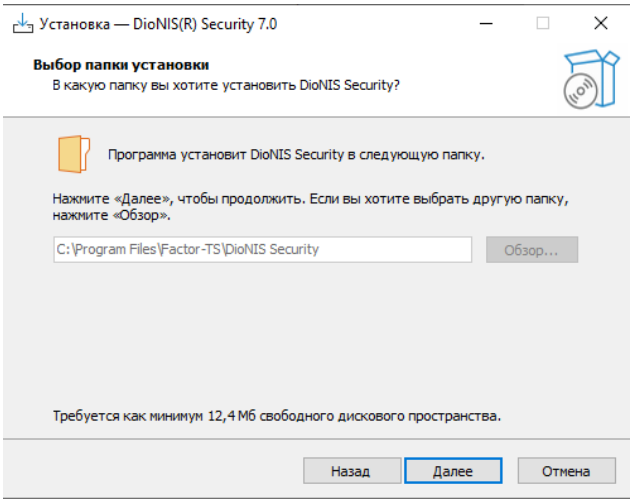
Для настройки работы нескольких Операторов с СКЗИ «Disec-W» на одном АРМ под своими учетными записями, но с общим закрытым ключом на одном ОМНИ, необходимо выполнить полную установку и настройку СКЗИ «Disec-W» под УЗ Администратора АРМ и затем после проверки и устранения всех ошибок в работе – импорт конфигурации отдельно для каждой УЗ Оператора. Функция экспорта/импорта конфигураций/подключений DiSec-W, требует УЗ Администратора или временное повышение полномочий УЗ Оператора до локального администратора.

Для установки СКЗИ «Disec-W» необходимо запустить файл инсталляции …\Disec-W\DiSecSetup.exe, находящийся на установочном диске. Программа запросит согласие на внесение изменений в компьютер, следует нажать «ОК».

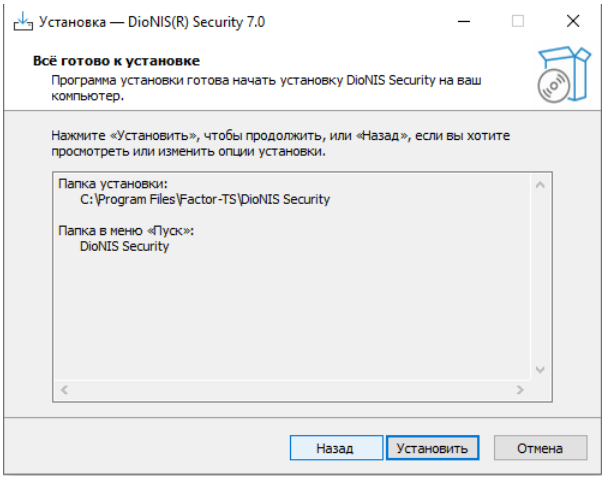
Нажать «Далее».



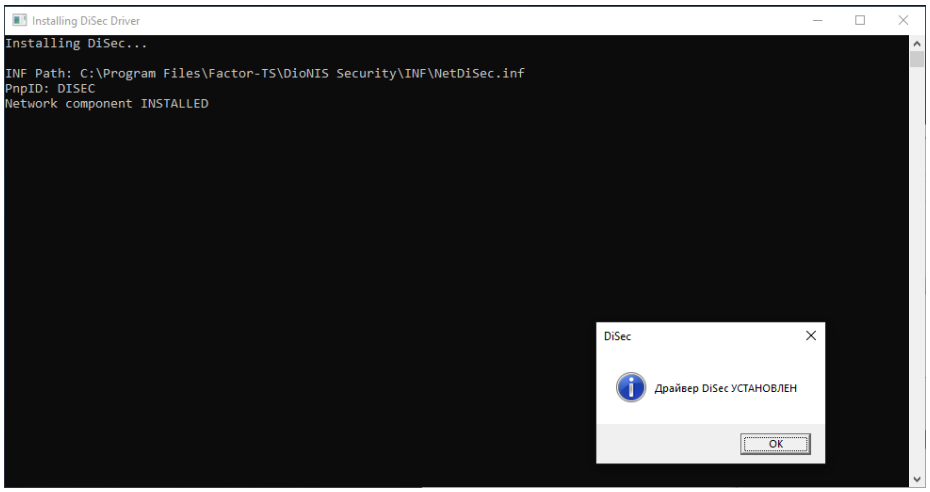
Нажать «Далее».

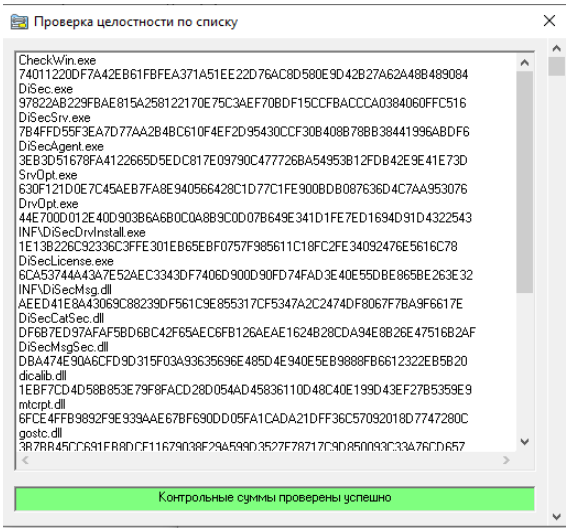


Нажать «Установить».



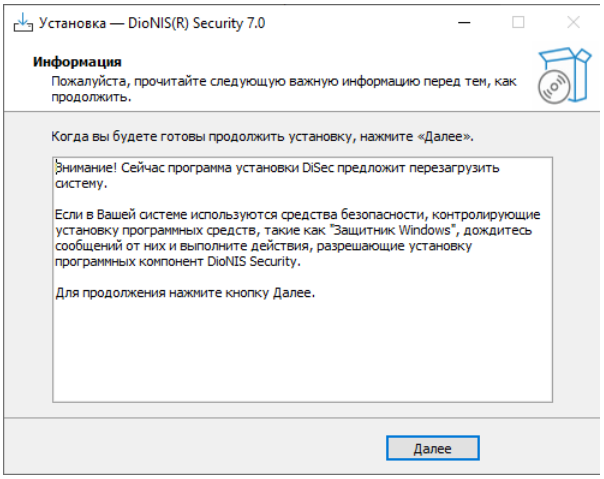
Информационное окно, сообщающее об успешной установке драйвера Disec. Нажать «ОК».



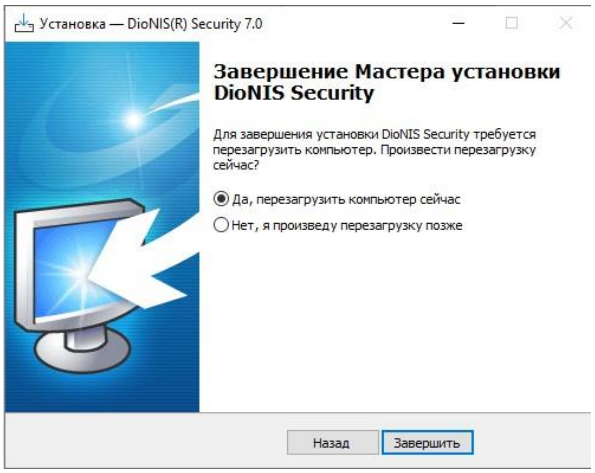


Если программа установилась корректно, в окне «Проверка целостности по списку» будет выдано уведомление «Контрольные суммы проверены успешно». Для продолжения установки необходимо закрыть окно. В случае некорректной установки, необходимо запросить через техническую поддержку эталонный экземпляр файла инсталляции и выполнить установку повторно.

Нажать «Далее».



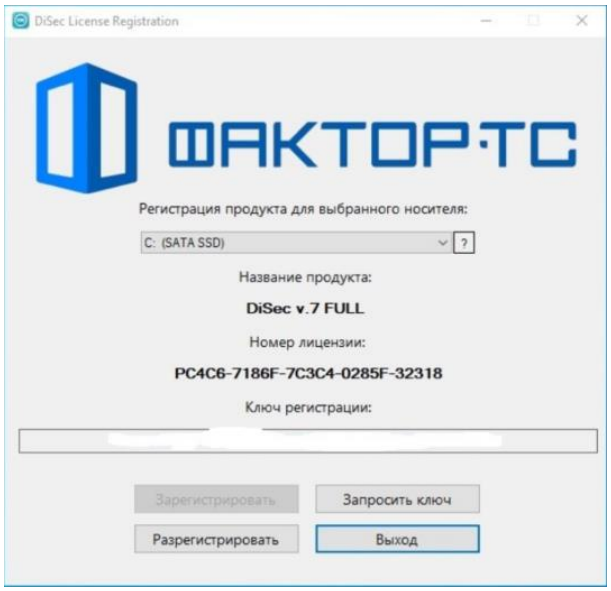
Нажать «Завершить», после чего ПЭВМ будет перезагружена.


Установка — DioNIS(R) Security 7.0
Завершение Мастера установки DioNIS Security
Для завершения установки DioNIS Security требуется перезагрузить компьютер. Произвести перезагрузку сейчас?
Да, перезагрузить компьютер сейчас
Нет, я произведу перезагрузку позже
Назад
Завершить

2.3 Активация СКЗИ «Disec-W»

После перезагрузки на рабочем столе необходимо найти ярлык 

и кликнуть по нему левой кнопкой мыши. Будет выведено окно активации:



Убедиться, что регистрация продукта будет запрошена для основного жесткого диска компьютера – его необходимо выбрать в предлагаемом списке носителей. Нажать «Запросить ключ». Будет выведено окно активации, где будут запрошены данные, которые необходимо отправить по адресу **helpdeskmci@cbr.ru** со следующим содержанием:

Тема письма: *Активация DiSec-W для <Наименование Клиента>, УИС <указать УИС>*;

В теле письма необходимо указать

а) учётный номер СКЗИ: *<указан на стр.8 из формуляра на **СКЗИ «Disec-W»** (не путать с формуляром на Модуль генерации ключей)>*;

б) номер лицензии: *XXXXX-XXXXX-XXXXX-XXXXX (показывается при первом запуске СКЗИ «DiSec-W»)*

В ответ на письмо будет отправлен ключ регистрации.

После получения ключа регистрации необходимо его внести в соответствующе поле и нажать «Зарегистрировать», после чего продукт будет готов к работе. Признаком правильной активации является отсутствие окна запроса лицензии при последующих запусках СКЗИ «Disec-W».

3 Настройка первого подключения СКЗИ «Disec-W» к узлам ТШ КБР

3.1 Подготовительные работы

Для настройки подключения СКЗИ «Disec-W» к узлам ТШ КБР, необходимо наличие у Клиента ОМНИ со следующей ключевой информацией:

а) закрытый ключ Клиента;

б) личный сертификат Клиента;

в) сертификат корневого УЦ;

г) список аннулированных сертификатов корневого УЦ;

д) сертификат подчиненного УЦ;

е) список аннулированных сертификатов подчиненного УЦ.

ВНИМАНИЕ! В СКЗИ «DiSec-W» существует ограничение при загрузке сертификатов и CAC, в наименовании которых используется символ «,» (запятая) или «@» (собачка) (например – CN=ROOTsvc-CA-test,OU=GUBZI,OU=PKI,DC=region,DC=cbr,DC=ru.cer; CLN=cln-9805001500@kpki.cbrgate.ru.cer). Для корректной загрузки сертификатов и CAC необходимо использовать следующий формат имени файла – CN=ROOTsvc-CA-test.cer; CLN=cln-9805001500.cer

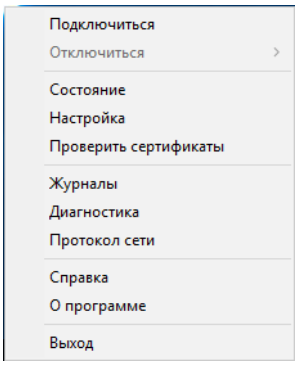
Для дальнейшей работы СКЗИ «Disec-W» необходимо, чтобы в ПЭВМ с установленным СКЗИ «Disec-W» был подключен ОМНИ, содержащий закрытый ключ Клиента и цепочку сертификатов.

3.2 Настройка первого подключения к ТШ КБР

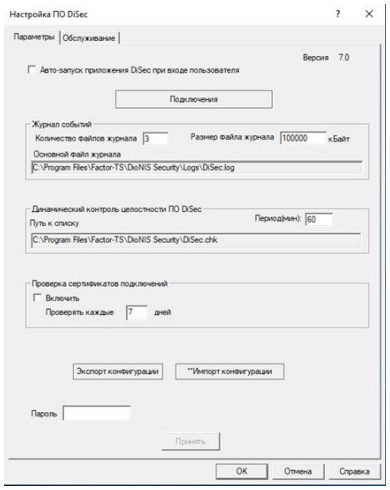
На рабочем столе необходимо найти ярлык 

и кликнуть по нему левой кнопкой мыши.

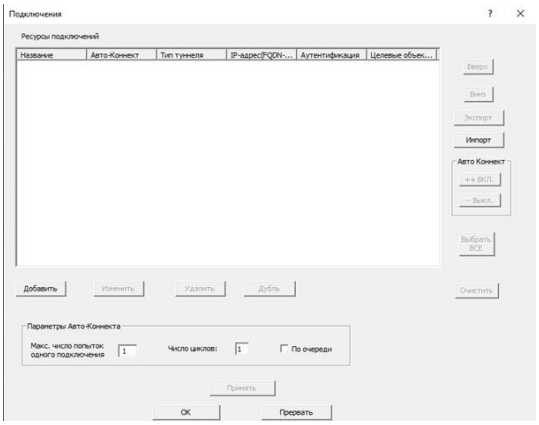
Справа внизу экрана появится значок  необходимо навести на него курсор мыши и правой кнопкой мыши вызвать контекстное меню.



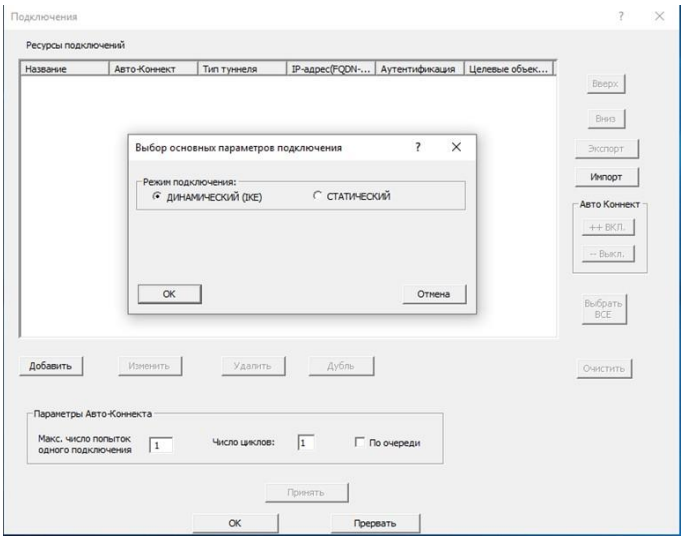
Далее левой кнопкой мыши выбрать пункт «Настройка», после чего откроется окно настроек программы.



Нажать на кнопку «Подключения» для дальнейшей настройки программы.

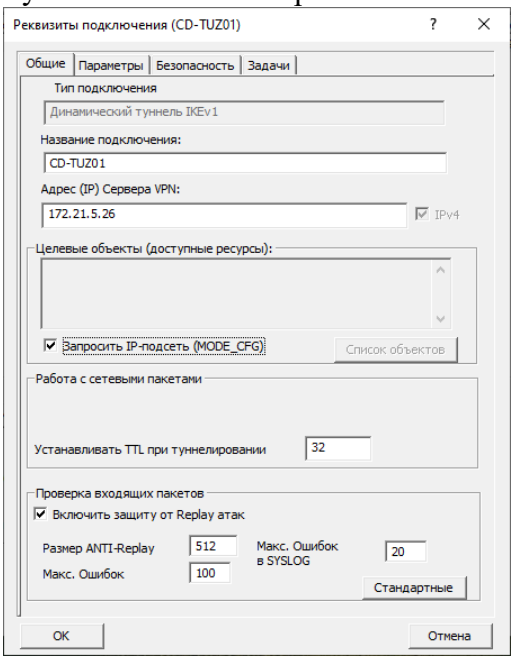


Нажать на кнопку «Добавить», после чего будет предположено выбрать типы соединений. Необходимо выбрать «Динамический» и начать «Ок».

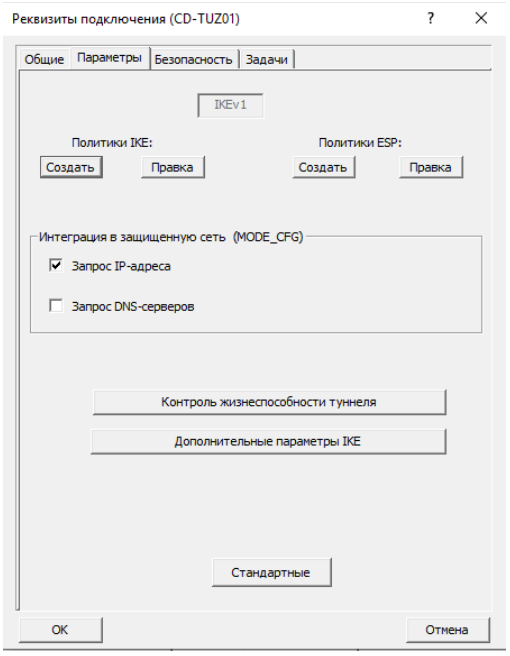


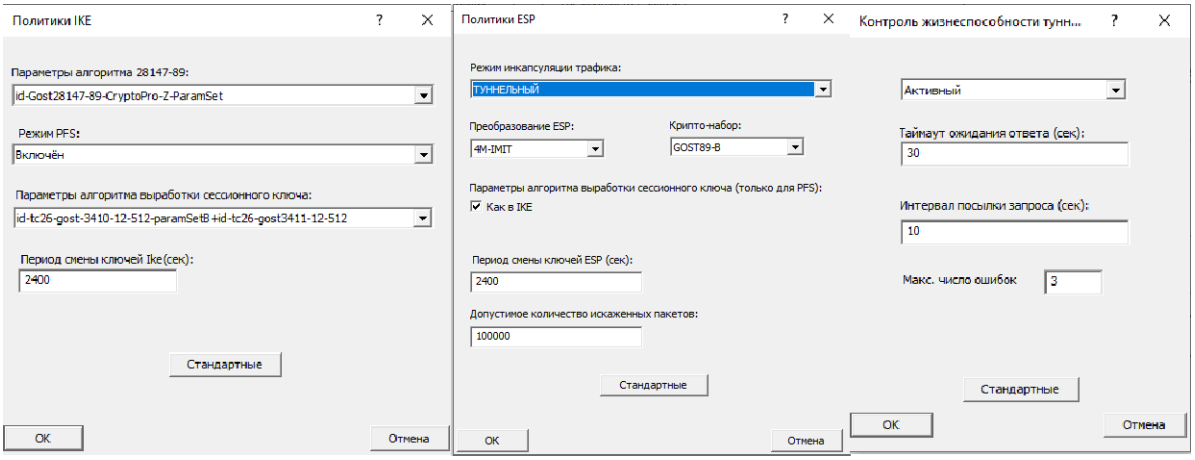
В окне «Реквизиты подключения» выполняются следующие настройки.

Вкладка *«Общие»* – для узла КС ТШ КБР первого объекта настройки будут следующими:



Вкладка *«Параметры»* – проверить следующие параметры:

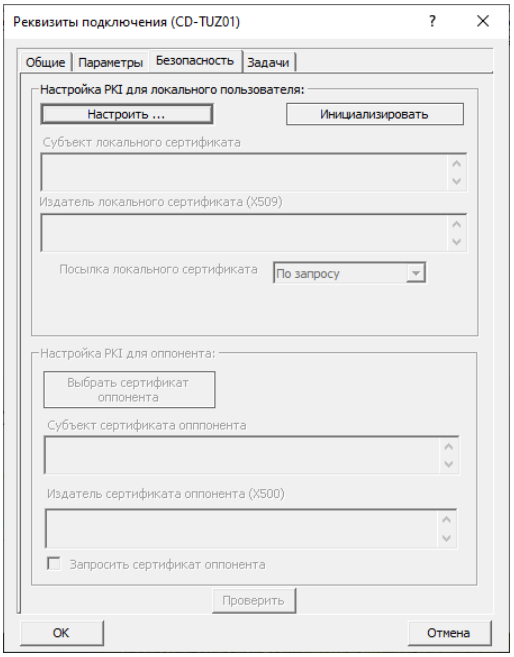




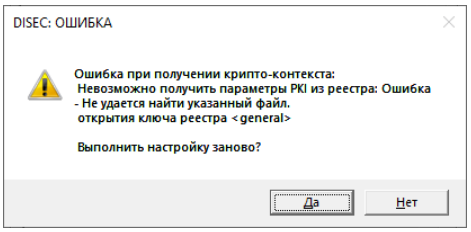
3.3 Загрузка цепочки сертификатов

3.3.1 Загрузка закрытого ключа Клиента

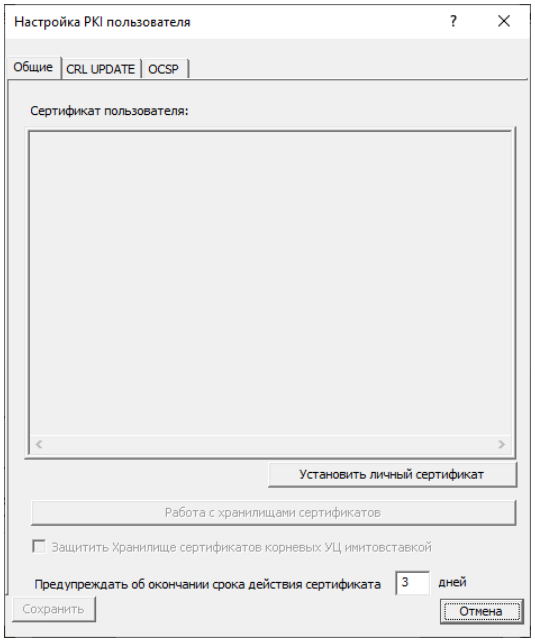
Вкладка «Безопасность»:



Выбрать «Настроить».



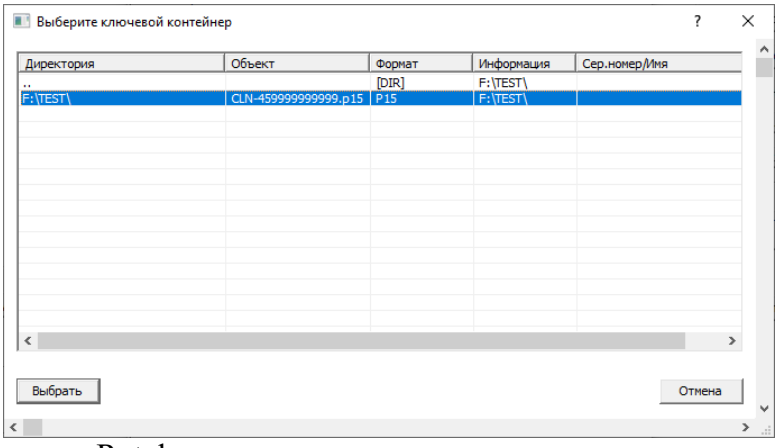
Сообщение "Ошибка получения криптоконтекста. Невозможно получить параметры PKI из реестра" может возникать при инициализации нового подключения. Не является ошибкой и после сохранения всей цепочки сертификатов в хранилище сертификатов больше не появляется. Нажать «Да».



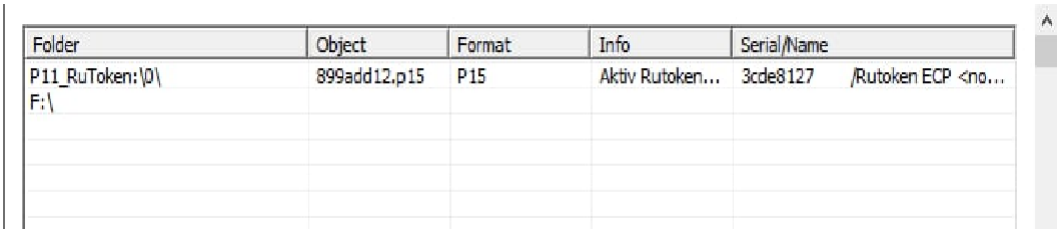
Выбрать «Установить личный сертификат».

Первым этапом будет предложено выбрать ОМНИ, на котором находится закрытый ключ.

Если ОМНИ является USB-flash:



Если ОМНИ является Rutoken:

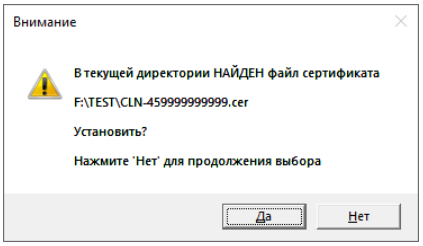


Необходимо найти и выделить мышью закрытый ключ – файл с расширением p15 и нажать

кнопку «Выбрать».

3.3.2 Загрузка личного сертификата Клиента

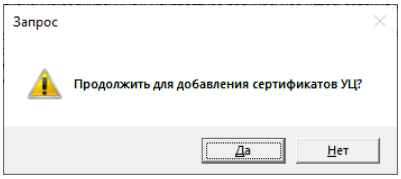
Если личный сертификат Клиента не расположен в каталоге с закрытым ключом, то программа запросит указать ОМНИ, содержащий личный сертификат Клиента. Далее программа сообщит, что был найден файл сертификата:



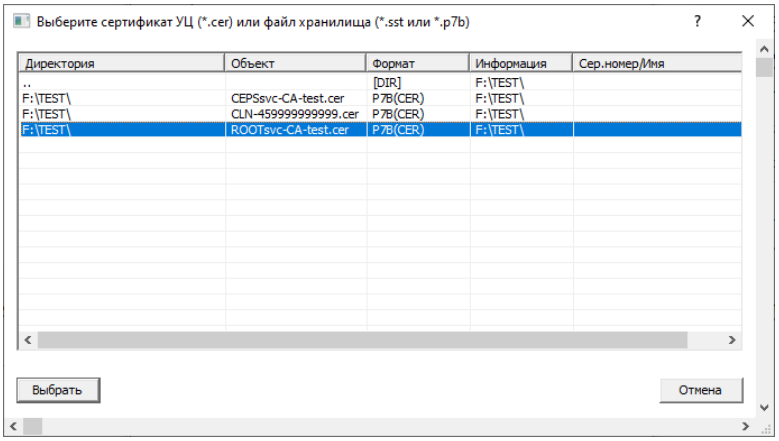
Убедиться, что предлагаемый к загрузке файл - личный сертификат Клиента и нажать «Да». В противном случае нажать «Нет» и продолжить выбор необходимого файла.

3.3.3 Загрузка сертификата корневого УЦ

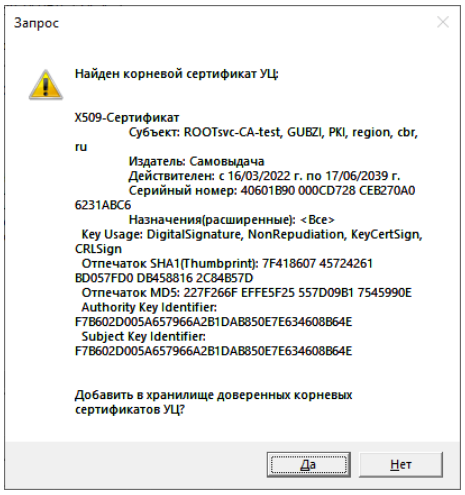
Далее будет выведено сообщение о начале этапа загрузки корневого сертификата УЦ:



Следует нажать «Да». Программа запросит указать ОМНИ, содержащий корневой сертификат УЦ:



Необходимо найти на ОМНИ и выделить мышью корневой сертификат УЦ – файл ROOTsvc-CA-test.cer и нажать кнопку «Выбрать»

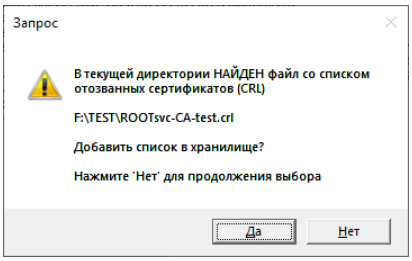


Убедиться, что предлагаемый к загрузке файл – Корневой сертификат УЦ и нажать «Да». В противном случае нажать «Нет» и продолжить выбор необходимого файла. Далее будет выведен запрос на добавление данного сертификата в контейнер доверенных корневых сертификатов, следует нажать «Да».

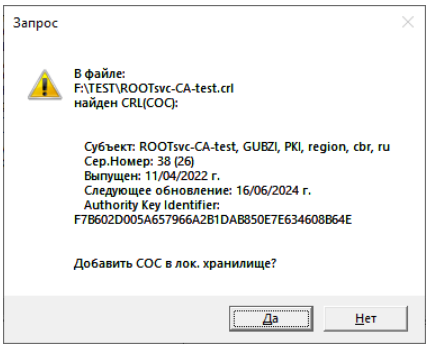
ВНИМАНИЕ! Если на этапе добавления сертификатов и CAC выпадает сообщение об ошибке, следует начать операцию заново, нажав «отмена» в настройках PKI пользователя, проверив все шаги настоящей инструкции.

3.3.4 Загрузка CAC корневого УЦ

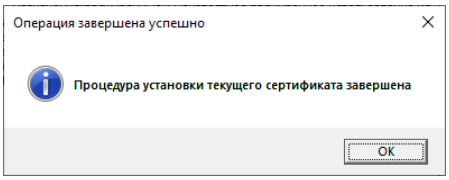
Далее будет выведено сообщение о том, что в данной директории найден CAC корневого УЦ:



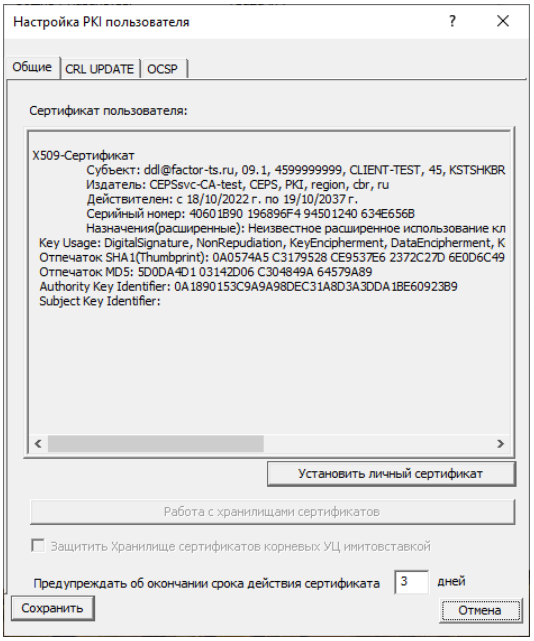
Убедиться, что предлагаемый к загрузке CAC корневого УЦ – файл ROOTsvc-CA-test.crl и нажать «Да». В противном случае нажать «Нет» и продолжить выбор необходимого файла.



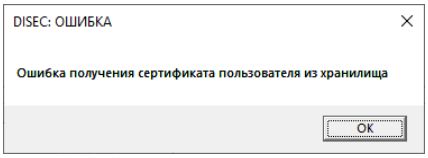
Далее программа сообщит о завершении процедуры установки текущего сертификата, следует нажать «ОК».



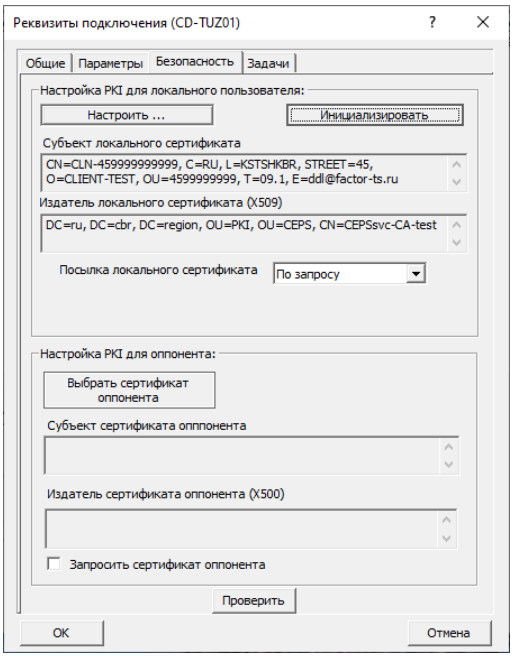
В окне «Настройка PKI пользователя» нажать «Сохранить».



Появившееся сообщение «Ошибка получения сертификата пользователя из хранилища» может возникать в процессе первичной настройки реквизитов подключения на этапе ввода сертификата и САС УЦ. Не является критической ошибкой и после сохранения всей цепочки сертификатов в хранилище сертификатов больше не появляется.



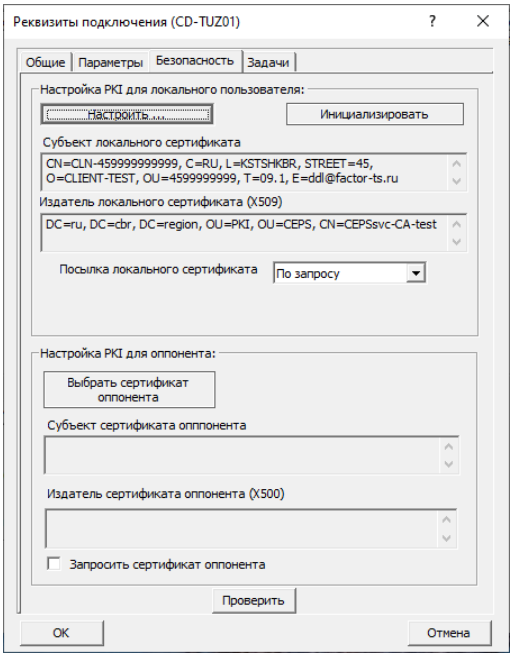
Нажать «Ок». Будет выполнен возврат в окно «Реквизиты подключения (CD-TUZ01)».



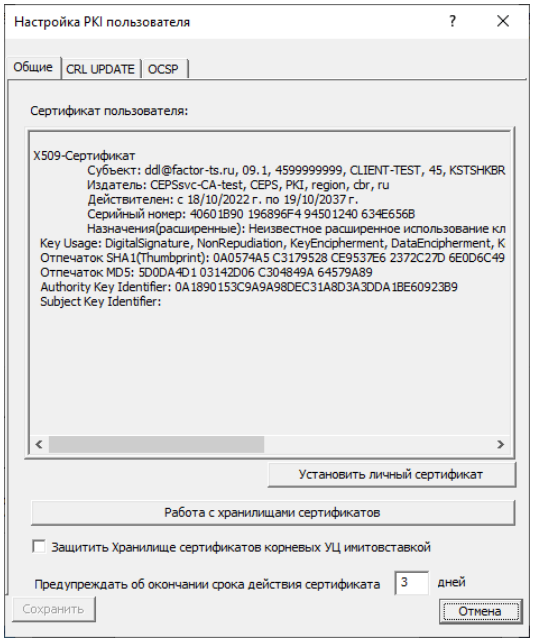
Нажать кнопку «Инициализировать».

3.3.5 Загрузка сертификата подчиненного УЦ

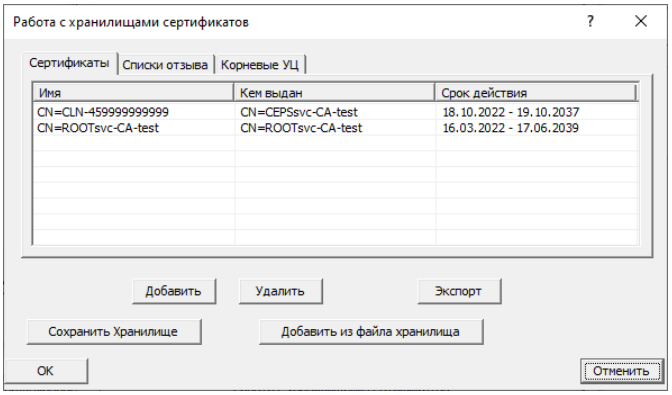
Для загрузки сертификата подчиненного УЦ следует снова в окне «Реквизиты подключения (CD-TUZ01)» нажать кнопку «Настроить»



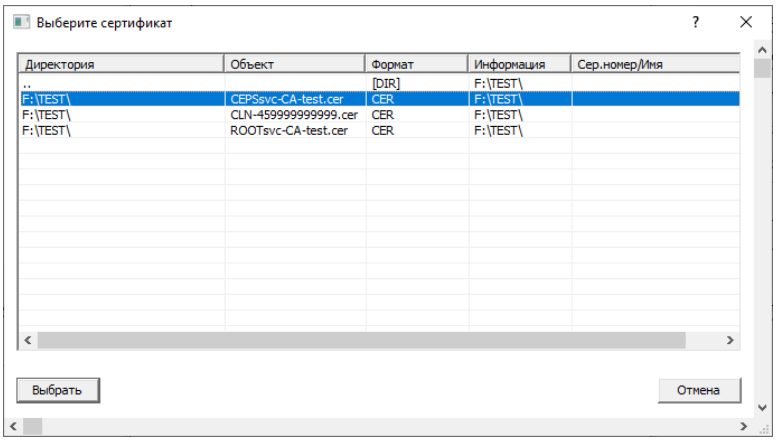
В открывшемся окне «Настройка PKI пользователя» станет доступна кнопка «Работа с хранилищами сертификатов»



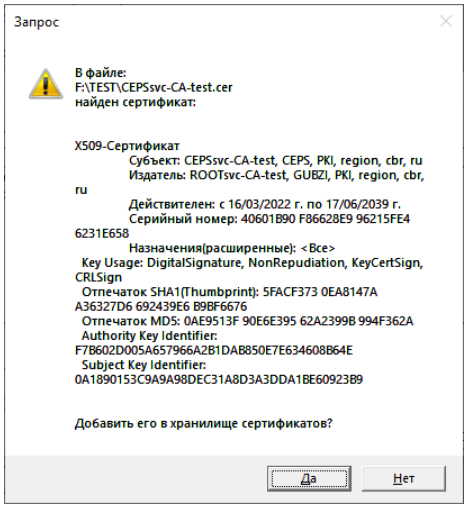
Нажать кнопку «Работа с хранилищами сертификатов».



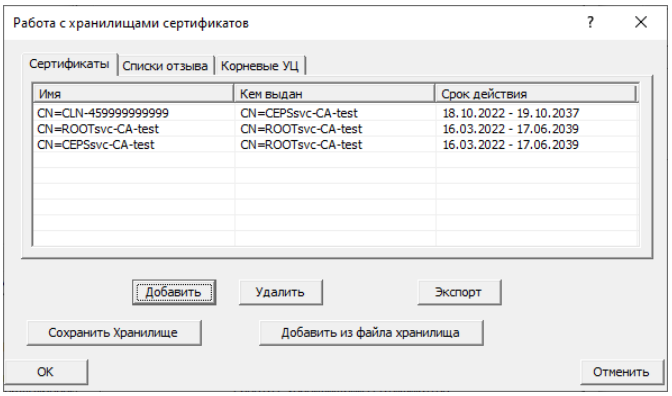
Следует нажать кнопку «Добавить», найти и выделить на ОМНИ файл сертификата подчинённого УЦ (в примере это CEPSsvc-CA-test.cer).



Далее следует нажать кнопку «Выбрать». Далее будет выведен запрос на добавление данного сертификата в хранилище доверенныхсертификатов, следует нажать «Да».

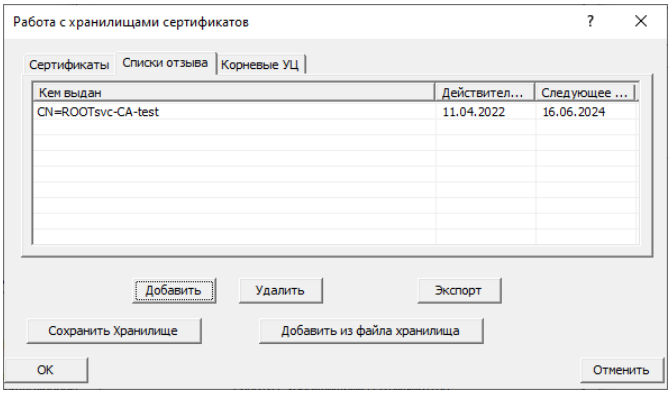


Сертификат подчинённого УЦ будет добавлен в хранилище. На вкладке «Сертификаты» должно быть 3 сертификата – личный сертификат Клиента, корневой сертификат УЦ и сертификат промежуточного УЦ.

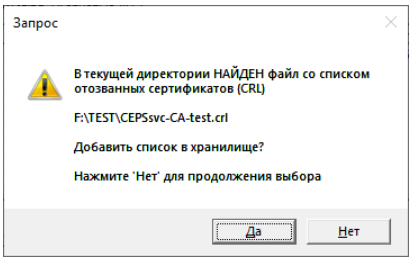


3.3.6 Загрузка CAC подчинённого УЦ

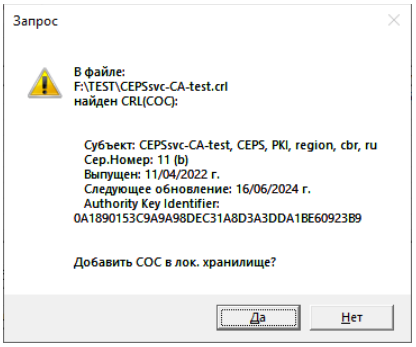
Для добавления CAC подчинённого УЦ следует перейти в закладку «Списки отзыва» окна «Работа с хранилищами сертификатов» и нажать кнопку «Добавить».



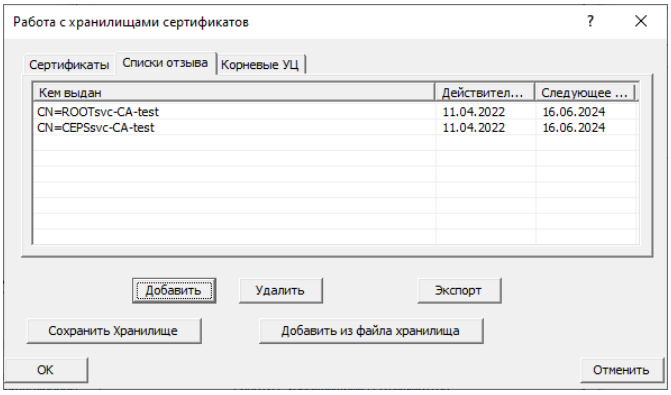
Будет выведено сообщение о том, что в каталоге найден CAC. Убедиться, что предлагаемый к загрузке CAC промежуточного УЦ – файл CEPSsvc-CA-test.crl и нажать «Да». В противном случае нажать «Нет» и продолжить выбор необходимого файла.



После этого программа сообщит о том, что в файле найден список аннулированных сертификатов подчиненного УЦ.



Следует нажать «Да».



На вкладке «Списки отзыва» должно быть 2 списка – CAC промежуточного УЦ и корневой CAC).

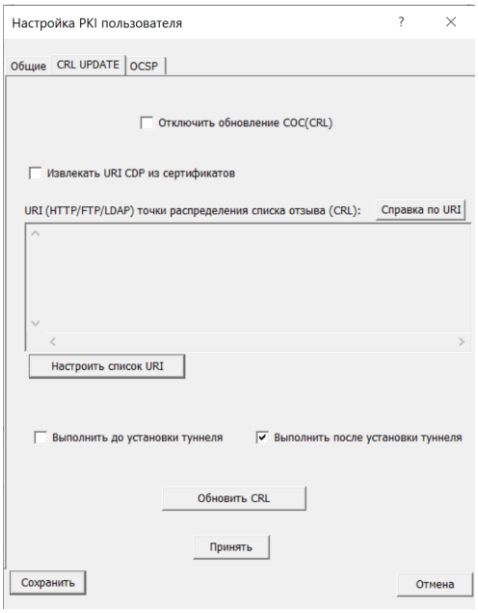
По окончании добавления сертификатов и CAC необходимо нажать «ОК» и далее

«Сохранить».

3.4 Настройка автоматического обновления CAC

Для настройки механизма автоматического обновления CAC необходимо перейти на вкладку «CRL UPDATE».

Для активации сервиса необходимо снять галку с пунктов «Отключить обновление COC(CRL)» и «Выполнить до установки туннеля».



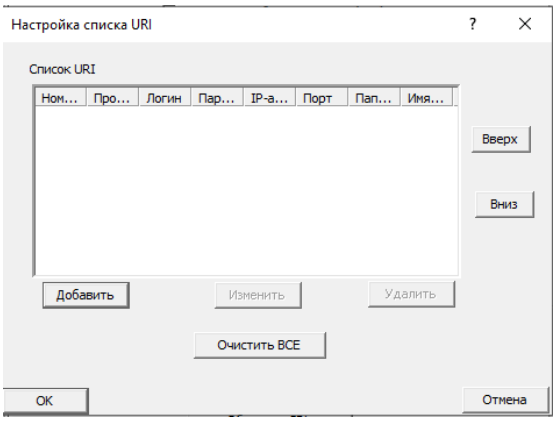
После активации механизма необходимо настроить узлы, с которых будут получены обновления списков отзыва. Для соединения с первым объектом URI будут следующими:

Наименование узла	Среда	Назначение сертификата	URI
КС ТШ КБР первого объекта	Тестовая	Корневой	http://172.21.5.57:9099/tsh/crl**YY**.crl
		Подчиненный	http://172.21.5.57:9099/**xx**/crl**YY**.crl

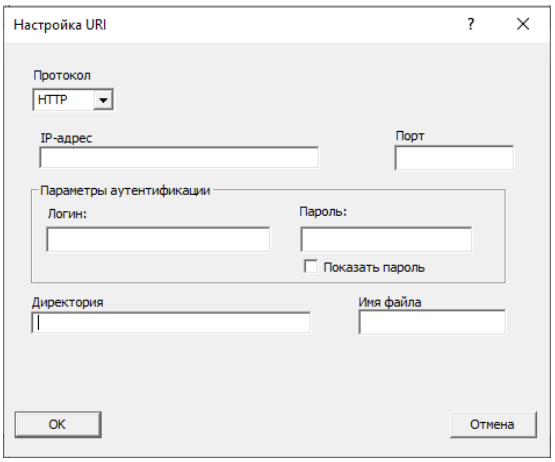
где XX - это номер региона. Далее по тексту в качестве примера будет использоваться номер московского региона (45).

где YY – это номер серии.

Для настройки данных URI необходимо нажать кнопку «Настроить список URI».



Нажать кнопку «Добавить».



При заполнении полей окна:

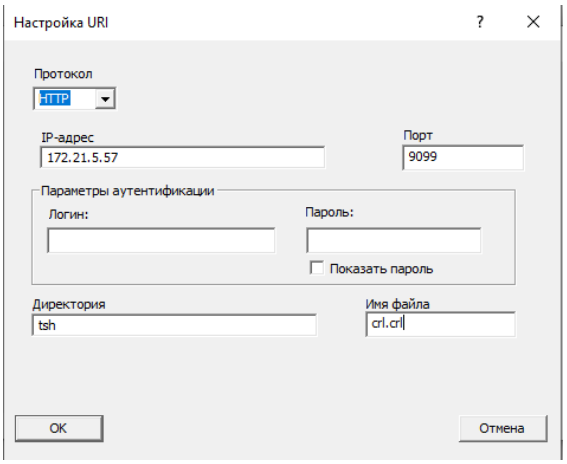
а) в поле «Протокол» необходимо указать **«HTTP»**;

б) в поле «IP-адрес» указать **«172.21.5.57»**.

в) в поле «Директория» указать **«tsh»**;

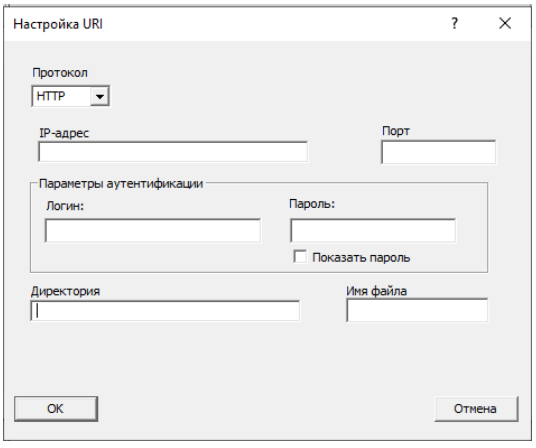
г) в поле «Имя файла» указать **«crlYY.crl»**, где ***YY*** номер серии;

д) в поле "Порт" указать **"9099".**



Нажать кнопку «ОК».

Нажать кнопку «Добавить».



При заполнении полей окна:

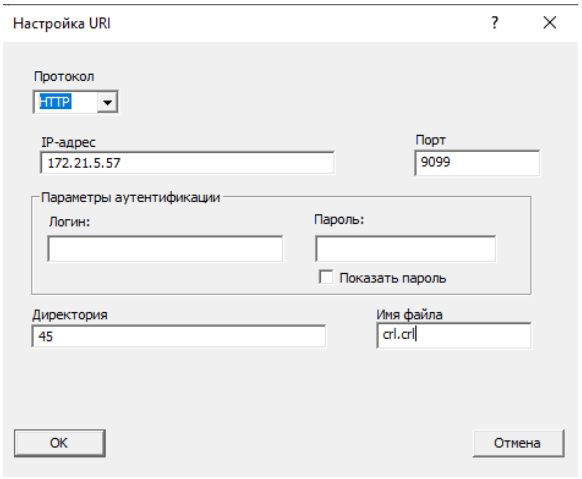
а) в поле «Протокол» необходимо указать **«HTTP»;**

б) в поле «IP-адрес» указать **«172.21.5.57»;**

в) в поле «Директория» указать **«45»;**

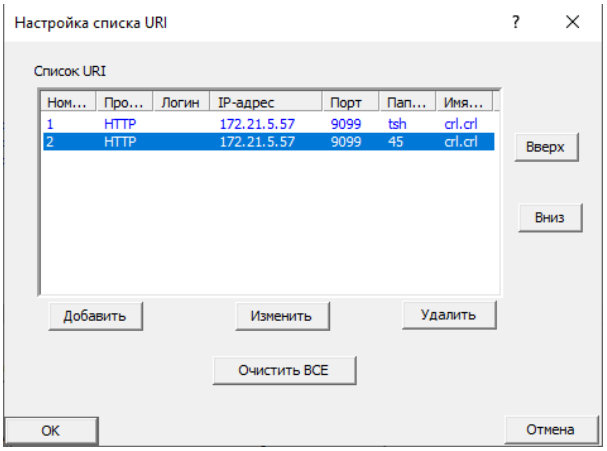
г) в поле «Имя файла» указать **«crlYY.crl»**, где ***YY*** номер серии**;**

д) в поле "Порт" указать **"9099".**



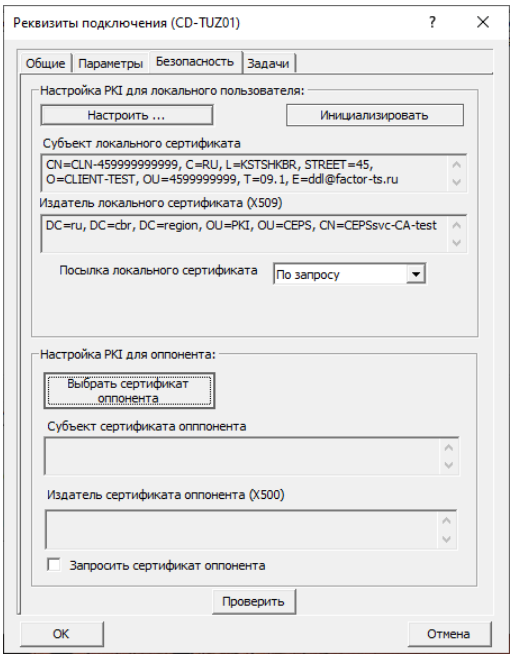
Нажать «ОК».

По окончании настройки должно иметь следующий вид.

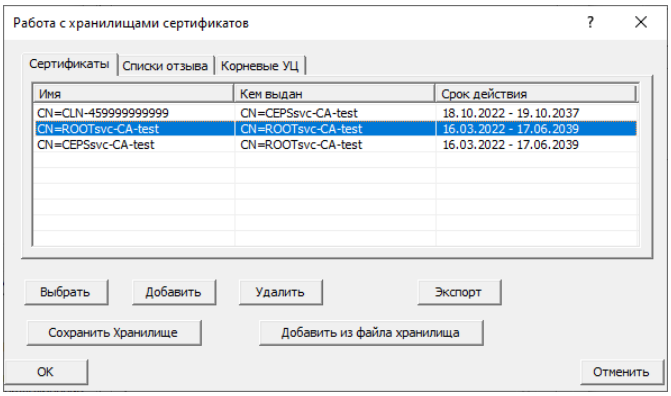


Нажать «Ок».

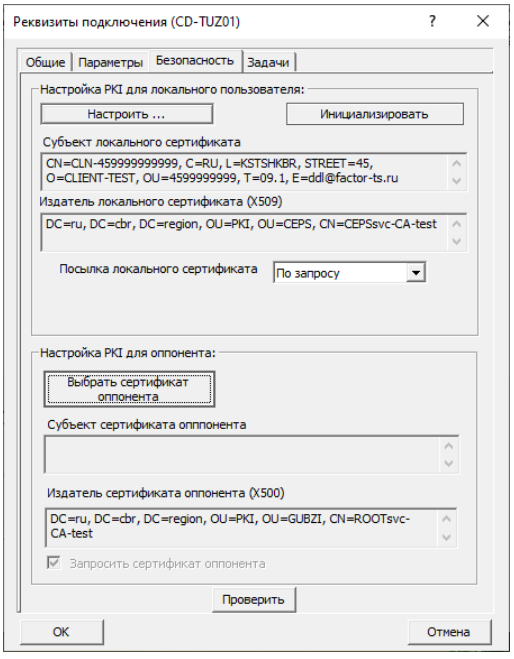
В разделе «Безопасность» необходимо указать сертификат оппонента. Для этого необходимо нажать кнопку «Выбрать сертификат оппонента».



В качестве сертификата оппонента будет использоваться **корневой сертификат УЦ.** Для этого следует в списке на закладке «Сертификаты» выбрать сертификат CN=ROOTsvc-CA-test левой кнопки мыши, нажать кнопку «Выбрать» и затем «ОК».

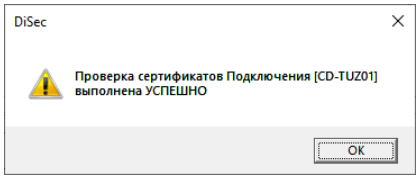


По окончании настройки вкладка «Безопасность» окна «Реквизиты подключения (CD-TUZ01)» должна иметь следующий вид:



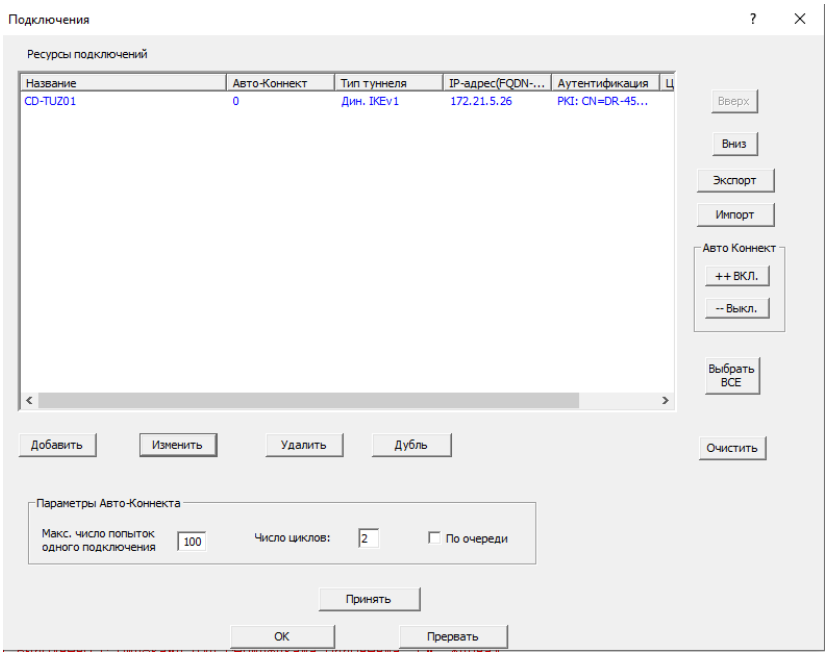
3.5 Проверка настроек

Следующим шагом необходимо проверить, что все настройки по добавлению сертификатов выполнены правильно. Для этого во вкладке «Безопасность» следует нажать кнопку «Проверить». После некоторого ожидания программа выдаст уведомление.



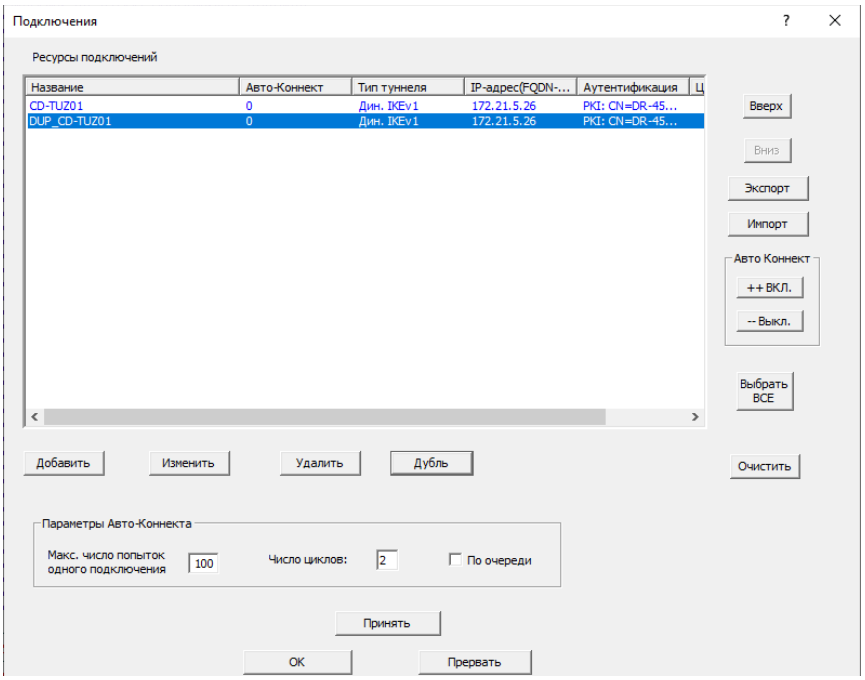
ВНИМАНИЕ! Если выдается сообщение об ошибке следует еще раз проверить все шаги настоящей инструкции.

Далее следует выйти из вкладки «Безопасность» нажав кнопку «Ок». Должен получится следующий результат.

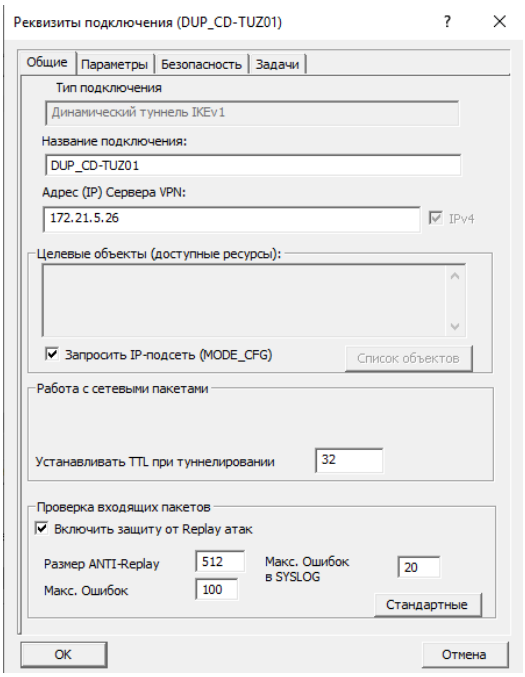


4 Настройка последующих подключений к узлам ТШ КБР.

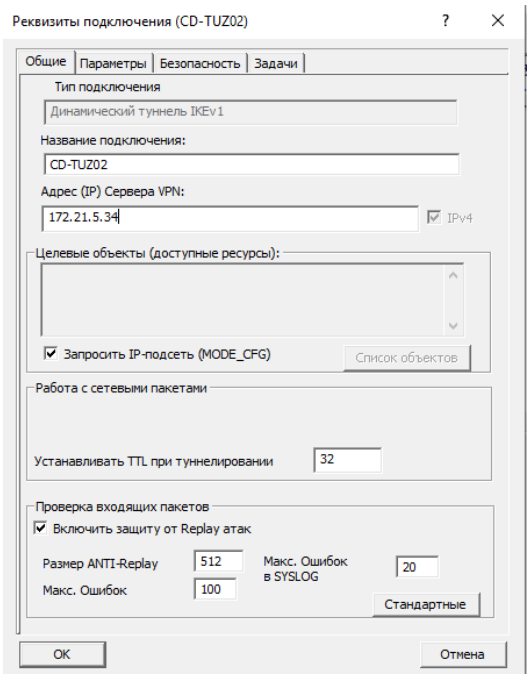
Левой кнопкой мыши выделить подключение и нажать «Дубль».



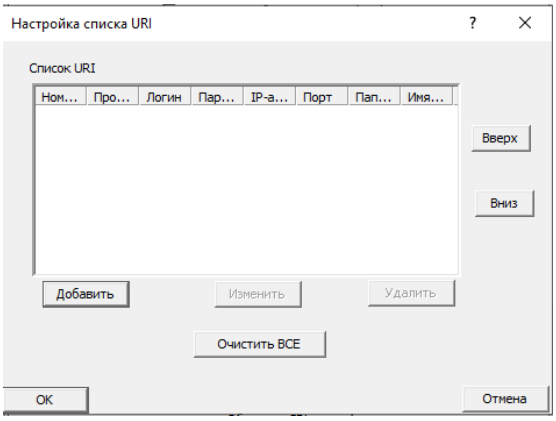
Нажать кнопку «Изменить».



Следует привести к следующему виду:



Далее необходимо перейти во вкладку «Безопасность» далее нажать кнопку «Настроить» и перейти во вкладку «CRL UPDATE» и нажать кнопку «Настроить список URI».



Далее необходимо произвести корректировку следующих настроек, корректировка настроек выполняется выбором объекта и нажать кнопку «Изменить».

Наименование узла	Среда	Назначение сертификата	URI
КС ТШ КБР второго объекта	тестовая	Корневой	http://172.21.5.58:9099/tsh/crl10.crl
		Подчиненный	http://172.21.5.58:9099/**45**/crl10.crl

Для корневого сертификата №1 указываются следующие настройки:

а) в поле «Протокол» необходимо указать **«HTTP»**;

б) в поле «IP-адрес» указать **«172.21.5.58»**;

в) в поле «Директория» указать **«tsh»**;

г) в поле «Имя файла» указать **«crlYY.crl»**, где ***YY*** номер серии;

д) в поле "Порт" указать **"9099".**

Для подчиненного сертификата №2 указываются следующие настройки:

а) в поле «Протокол» необходимо указать **«HTTP»**;

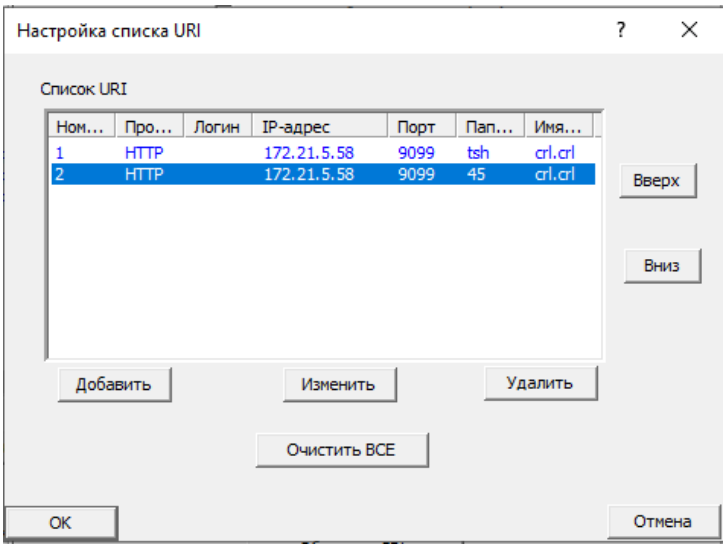
б) в поле «IP-адрес» указать **«172.21.5.58»**;

в) в поле «Директория» указать **«45»**;

г) в поле «Имя файла» указать **«crlYY.crl»**, где ***YY*** номер серии;

д) в поле "Порт" указать **"9099".**

По окончании настройки должен получится следующий результат:

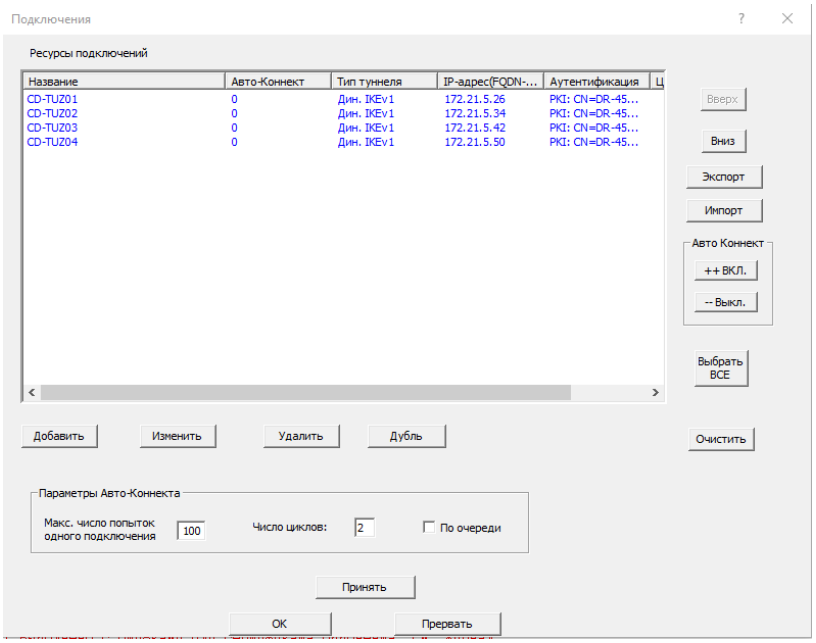


Нажать «ОК».

Нажать «Сохранить».

Нажать «ОК».

По окончании настройки должен быть следующий результат:

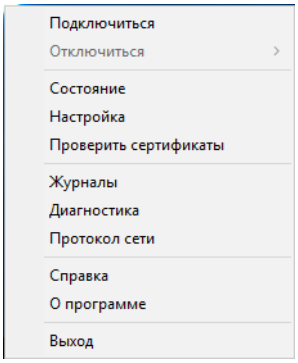


ВНИМАНИЕ! Остальные подключения настраиваются аналогичным способом. Все IP адреса подключений приведены в разделе «Общие сведения».

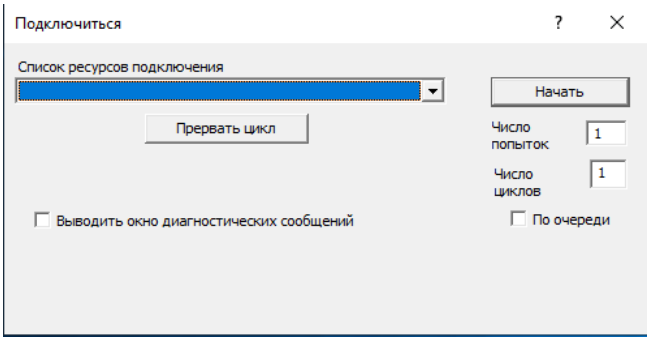
5 Запуск СКЗИ «DiSec-W»

После установки и настройки СКЗИ справа внизу экрана появится значок 

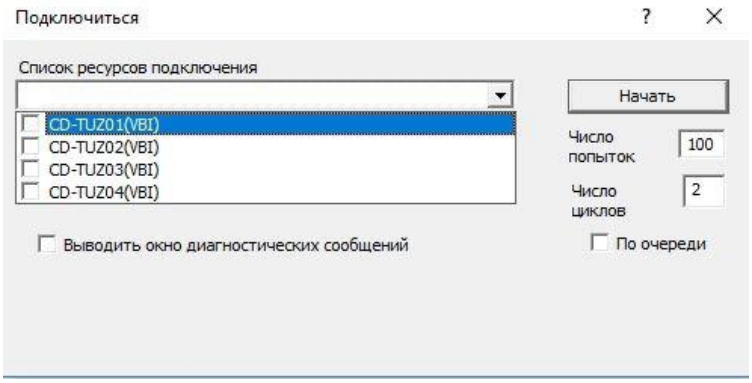
Необходимо навести на него курсор мыши и правой кнопкой мыши вызвать контекстное меню.



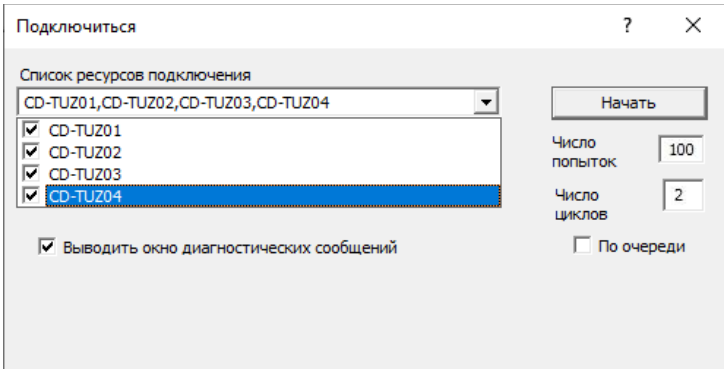
Выбрать пункт «Подключиться», после чего откроется окно «Подключиться».



Далее нужно указать какие подключения будут выполняться, для этого следует раскрыть поле «Список ресурсов подключения».



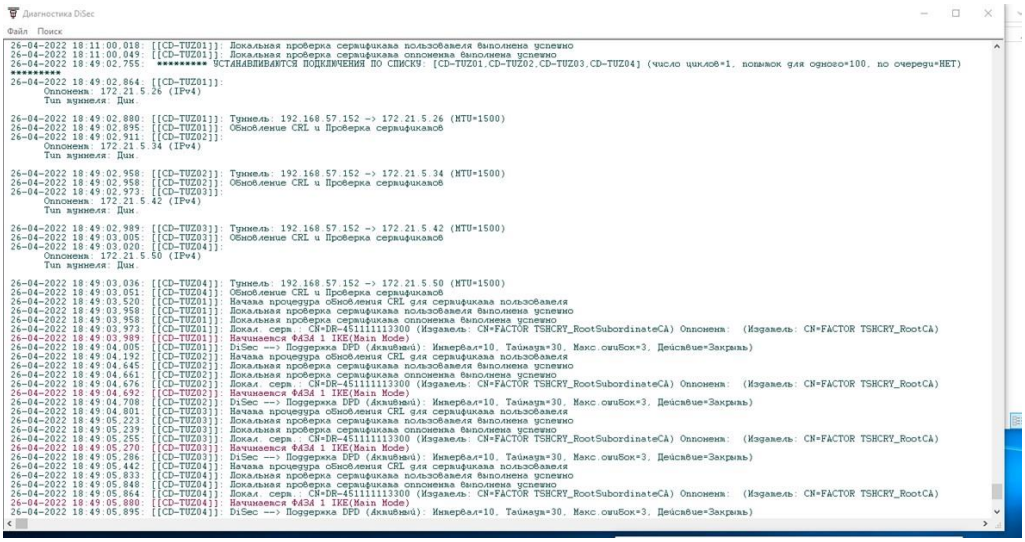
В раскрывшемся списке следует отметить все объекты (CD-TUZ01, CD-TUZ02, CDTUZ03, CD-TUZ04).



Далее в обязательном порядке необходимо указать в поле «Число попыток» количество переподключений (рекомендуется 100) на случай обрыва связи или сбоя в процессе обновления ключевой информации (*rekeying)*, который происходит автоматически каждые 40 минут. Значение поля «Число циклов» рекомендуется установить в 2. В случае, если установленное количество попыток и циклов будет исчерпано, то процедура подключения будет остановлена до повторного запуска Оператором.

Для визуального контроля состояния соединений рекомендуется установить галку «Выводить окно диагностических сообщений».

Далее необходимо нажать кнопку «Начать», после этого будет запущена процедура подключения к узлам ТШ КБР.



6 Смена ключевой информации в «DiSec-W»

Смена ключевой информации бывает двух типов.

1) В рамках текущей серии.

2) В рамках новой серии.

Если смена ключевой информации выполняется в рамках текущей серии, то достаточно выполнить только смену сертификата клиента, смена корневых и подчинённых сертификатов выполняется при необходимости.

При смене ключевой информации в рамках новой серии необходимо:

1) Войти в Настройка → Подключения.

2) Выбрать подключение и нажать кнопку «Дубль».

3) Выбрать вновь созданное подключение и нажать кнопку «Изменить».

4) Выбрать вкладку безопасность и нажать на кнопку «Настроить».

5) Нажать на кнопку «Работа с хранилищем сертификатов».

6) Во вкладке ***сертификаты*** выбрать сертификат (навести на сертификат курсор мыши и нажать левую кнопку мыши) и нажать на кнопку «Удалить», аналогично выполнить для всех сертификатов кроме сертификата клиента.

7) Перейти во ***вкладку списки*** отзыва выбрать CAC (навести на сертификат курсор мыши и нажать левую кнопку мыши) и нажать на кнопку «Удалить», аналогично выполнить для всех CAC.

8) Перейти во ***вкладку коневые УЦ*** выбрать сертификат (навести на сертификат курсор мыши и нажать левую кнопку мыши) и нажать на кнопку «Удалить», аналогично выполнить для всех сертификатов.

9) Нажать на кнопку «Ок».

10) Нажать на кнопку «Установить личный сертификат» и выполнить загрузку ключевой информации как описано выше (пункт 3.3).

11) Нажать на кнопку «Сохранить».

12) Повторно во вкладке безопасность и нажать на кнопку «Настроить».

13) Перейти во вкладку ***CRL UPDATE***.

14) Выбрать точку распространения (навести курсор мыши и нажать левую кнопку мыши).

15) В окне имя файла изменить имя на ***crlYY.crl***, где ***YY*** номер серии. Нажать кнопку «ОК».

16) Аналогично изменить имена файлов во всех точках.

17) Нажать кнопку «Сохранить».

18) Нажать кнопку «Ок».

19) Выполнить **подключение/отключение** к серверу доступа.

20) Аналогичные операции выполнить для оставшихся подключений (раздел 4) и выполнить проверку подключений.

21) После успешной проверки новых подключений на новой серии, подключения к ТШ КБР предыдущей серии необходимо удалить.

7 Диагностика работы СКЗИ «DiSec-W»

7.1 Лог файлы СКЗИ «Disec-W»

В каталоге C:\Program Files\Factor-TS\DioNIS Security\Logs находятся лог файлы СКЗИ «Disec-W», которые могут помочь в диагностике возникающих проблем:

Disec.log – файл журнала работы (выводится в окно Диагностика DiSec).

CrlUpd.log – файл журнала обновлений CAC.

7.2 Доступность узлов ТШ КБР

Для проверки наличия сетевого соединения с узлами ТШ КБР тестовой среды:

1) Запустить powershell

2) Выполнить командлеты:

Test-NetConnection -ComputerName "172.21.5.26" -TraceRoute -InformationLevel "Detailed"

Test-NetConnection -ComputerName "172.21.5.34" -TraceRoute -InformationLevel "Detailed"

Test-NetConnection -ComputerName "172.21.5.42" -TraceRoute -InformationLevel "Detailed"

Test-NetConnection -ComputerName "172.21.5.50" -TraceRoute -InformationLevel "Detailed"

3) Сохранить вывод в текстовом файле tracert-test.txt.

Все 4 узла ТШ КБР должны быть доступны.

Для проверки наличия сетевого соединения с узлами ТШ КБР промышленной среды:

1) Запустить powershell

2) Выполнить командлеты:

Test-NetConnection -ComputerName "172.21.1.26" -TraceRoute -InformationLevel "Detailed"

Test-NetConnection -ComputerName "172.21.1.34" -TraceRoute -InformationLevel "Detailed"

Test-NetConnection -ComputerName "172.21.1.42" -TraceRoute -InformationLevel "Detailed"

Test-NetConnection -ComputerName "172.21.1.50" -TraceRoute -InformationLevel "Detailed"

4) Сохранить вывод в текстовом файле tracert-prom.txt.

Все 4 узла ТШ КБР должны быть доступны.

7.3 Доступность сервисов ТШ КБР

На данный момент предоставление сервисов ТШ КБР при доступе с использованием СКЗИ «DiSec-W» организовано следующим образом: обработка платежной информации выполняется или на паре узлов «CD-TUZ01», «CD-TUZ02» или на паре «CD-TUZ03», «CD-TUZ04». Клиенту Банка России доступны 4 подключения одновременно, но АРМ КБР-Н/СПФС будет штатно функционировать только с первой парой подключений, или со второй. Остальные сервисы должны быть доступны на всех 4-х подключениях. Эти правила должны действовать для

тестовой и промышленной среды.

Для проверки доступа к сервисам ТШ КБР тестовой среды:

1) Запустить powershell

2) Запустить подключение «CD-TUZ01».

3) Выполнить командлеты:

Test-NetConnection -ComputerName "172.21.5.57" -Port 7777 -InformationLevel "Detailed"

Test-NetConnection -ComputerName "172.21.5.57" -Port 1414 -InformationLevel "Detailed"

Test-NetConnection -ComputerName "172.21.5.57" -Port 9697 -InformationLevel "Detailed"

Test-NetConnection -ComputerName "172.21.5.57" -Port 9099 -InformationLevel "Detailed"

Test-NetConnection -ComputerName "172.21.5.57" -Port 9010 -InformationLevel "Detailed"

4) Отключить подключение «CD-TUZ01».

5) В случае отсутствия возможности выполнить командлеты, использовать команды tracert и telnet.

6) Сохранить вывод в текстовом файле CD-TUZ01-test-diag.txt.

7) Выполнить шаги 2-6 для остальных узлов ТШ КБР. Перечень необходимых портов и адреса узлов ТШ КБР приведены в таблице 1 данной Инструкции.

7.4 Ошибка обновления CRL

Периодические сообщения в окне диагностики вида «Обновление CRL выполнено с ошибками для сертификата пользователя. См. Журнал» могут возникать из-за временной недоступности или загруженности сервиса распространения CAC.

Причину в каждом конкретном случае можно посмотреть в лог-файле C:\Program Files\Factor-TS\DioNIS Security\Logs\CrlUpd.log:

1. Если по всем 4-м подключениям сервис распространения CAC доступен, загрузка файлов crl выполняется и имеются лишь единичные сообщения вида «Время ожидания операции истекло» то никаких дополнительных действий предпринимать не стоит.

2. Если по всем 4-м подключениям сервис распространения CAC доступен, загрузка файлов crl выполняется, но имеются множественные сообщения вида «Время ожидания операции истекло» это может говорить о наличии сетевых проблем у Клиента или у его провайдера. Клиенту необходимо направить запрос на проверку стабильности сетевого взаимодействия с узлами ТШ КБР на подразделение информатизации своей организации и далее на провайдера услуг.

3. Если сервис распространения CAC недоступен на конкретном подключении, необходимо проверить правильность настройки URI для данного подключения, и в случае, если это не приведет к решению проблемы, Клиенту необходимо направить запрос на проверку и

организацию сетевого доступа к узлам ТШ КБР на подразделение информатизации своей организации. Перечень необходимых портов и адреса узлов ТШ КБР приведены в таблицах 1-2 данной Инструкции.

7.5 Направление данных в техническую поддержку

При направлении запроса в техническую поддержку на почтовый адрес helpdeskmci@cbr.ru, рекомендуется приложить к следующую информацию:

1) Подробное описание выполняемых действий, приводящих к появлению ошибки, с приложением скриншотов.
2) Файл экспорта конфигурации DiSec-W.
3) Файлы проверки доступности узлов и сервисов ТШ КБР.
4) Архив каталога C:\Program Files\Factor-TS\DioNIS Security\Logs.

Приложение 2

Инструкция по настройке ПК АРМ КБР-Н / АРМ КБР-СФПС для обмена платежными и финансовыми сообщениями с ТШ КБР в рамках криптографической сети ТШ КБР

Для обмена электронными сообщениями с ТШ КБР в рамках работы через защищённые каналы связи КС ТШ КБР необходимо настроить ПК АРМ КБР-Н / ПК АРМ КБР-СПФС.

Внимание! УО необходимо использовать ПК АРМ КБР-Н версии 2020.3 и ПК АРМ КБР-СФПС версии 2020.3 или выше.

С учётом того, что СКЗИ DiSec-W устанавливает одновременно четыре VPN - туннеля до серверов доступа ТШ КБР, то в рамках установленных туннелей УО доступны четыре независимых IP-адреса прикладных сервисов ТШ КБР для осуществления обмена электронными сообщениями. Банк России на своей стороне определяет доступность IP-адресов прикладных сервисов ТШ КБР, при этом ПК АРМ КБР-Н / ПК АРМ КБР-СПФС должен быть настроен на работу со всеми возможными IP-адресами.

Для этого необходимо настроить основной и резервные IP-адреса серверов ТШ КБР в параметрах настройки точки обмена на вкладке «Настройки обмена СВК / ТШ КБР» для ПК АРМ КБР-Н и на вкладке ««Настройки взаимодействия с СВК/ТШ КБР» для ПК АРМ КБР-СПФС

А) Для работы в <u>тестовом контуре по протоколу HTTP</u> должны использоваться следующие настройки (рис. 1а и 1б):

Сервер отправки: http://172.21.5.57:7777/in

Сервер получения: http://172.21.5.57:7777/get

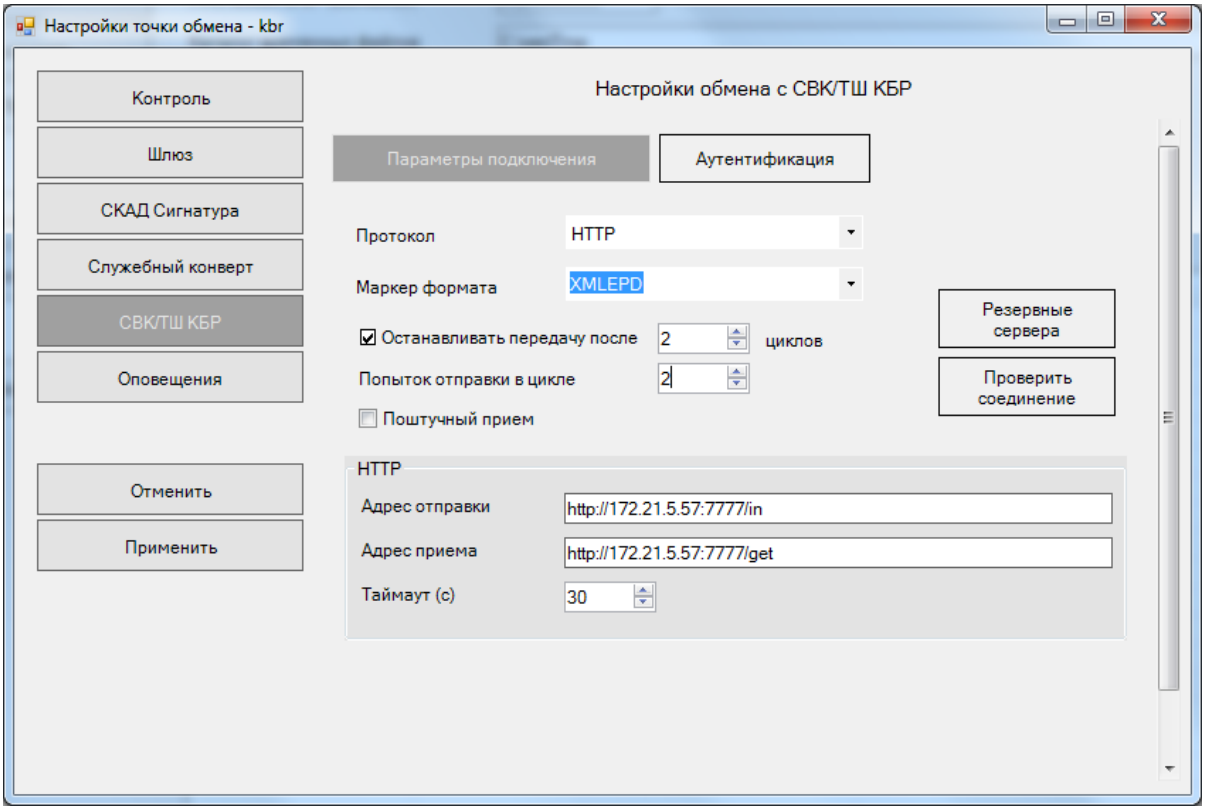


Рис 1а. Настройки обмена СВК / ТШ КБР для ПК АРМ КБР-Н
(Протокол HTTP, тестовый контур)

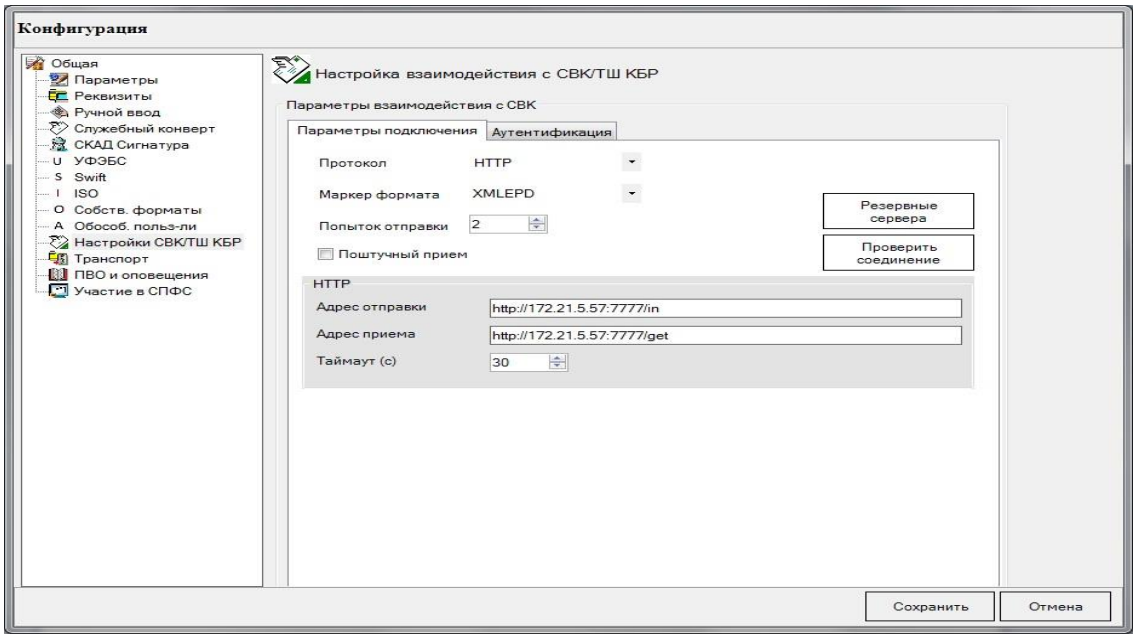


Рис 1б. Настройки взаимодействия с СВК / ТШ КБР для ПК АРМ КБР-СПФС (Протокол HTTP, тестовый контур)

Также необходимо указать резервные значения IP-адресов сервера:

172.21.5.58:7777

172.21.5.59:7777

172.21.5.60:7777

***Резервные сервера*–** по кнопке открывается окно, в котором нужно задать список IP адресов ТШ КБР, на которые будет перенаправляться соединение в случае отсутствия подключения к основному серверу.

Б) Для работы в <u>тестовом контуре по протоколу MQ</u> должны использоваться следующие настройки (рис. 2а и 2б):

WMQ / Сервер: 172.21.5.57

WMQ / Порт: 1414

WMQ / Канал: KBR.SVRCONN

WMQ / Менеджер: FRONTGATE

Отправка / Очередь: FROM.KBR

Отправка / Менеджер ответов: FRONTGATE

Отправка / Очередь ответов: INBOX.xxxxxx (уточняется через Единую службу поддержки пользователей при начале работы по MQ)

Опция Отправка / Запрашивать квитанции о доставке/получении устанавливается опционально при необходимости

Приём / Очередь: INBOX.xxxxxx (уточняется через Единую службу поддержки пользователей при начале работы по MQ)

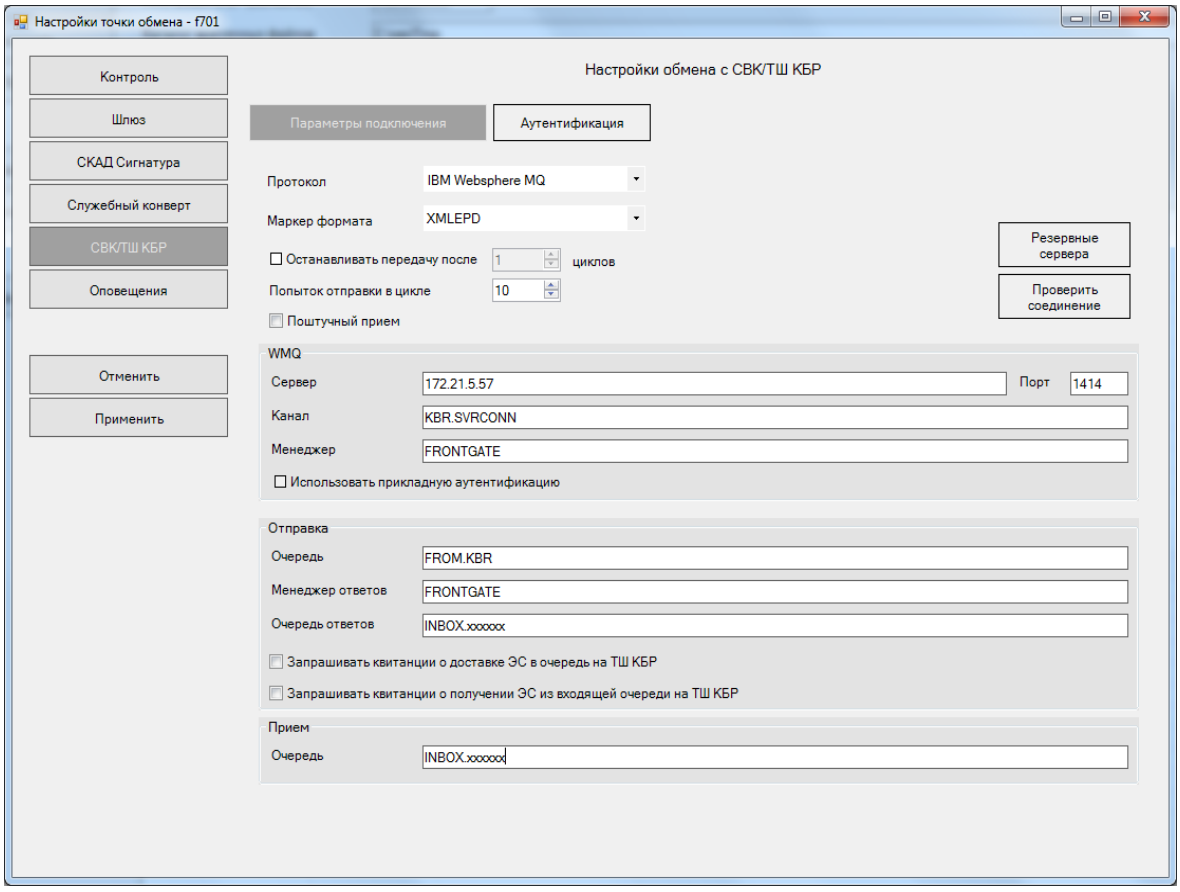


Рис 2а. Настройки обмена СВК / ТШ КБР для ПК АРМ КБР-Н
(Протокол MQ, тестовый контур)

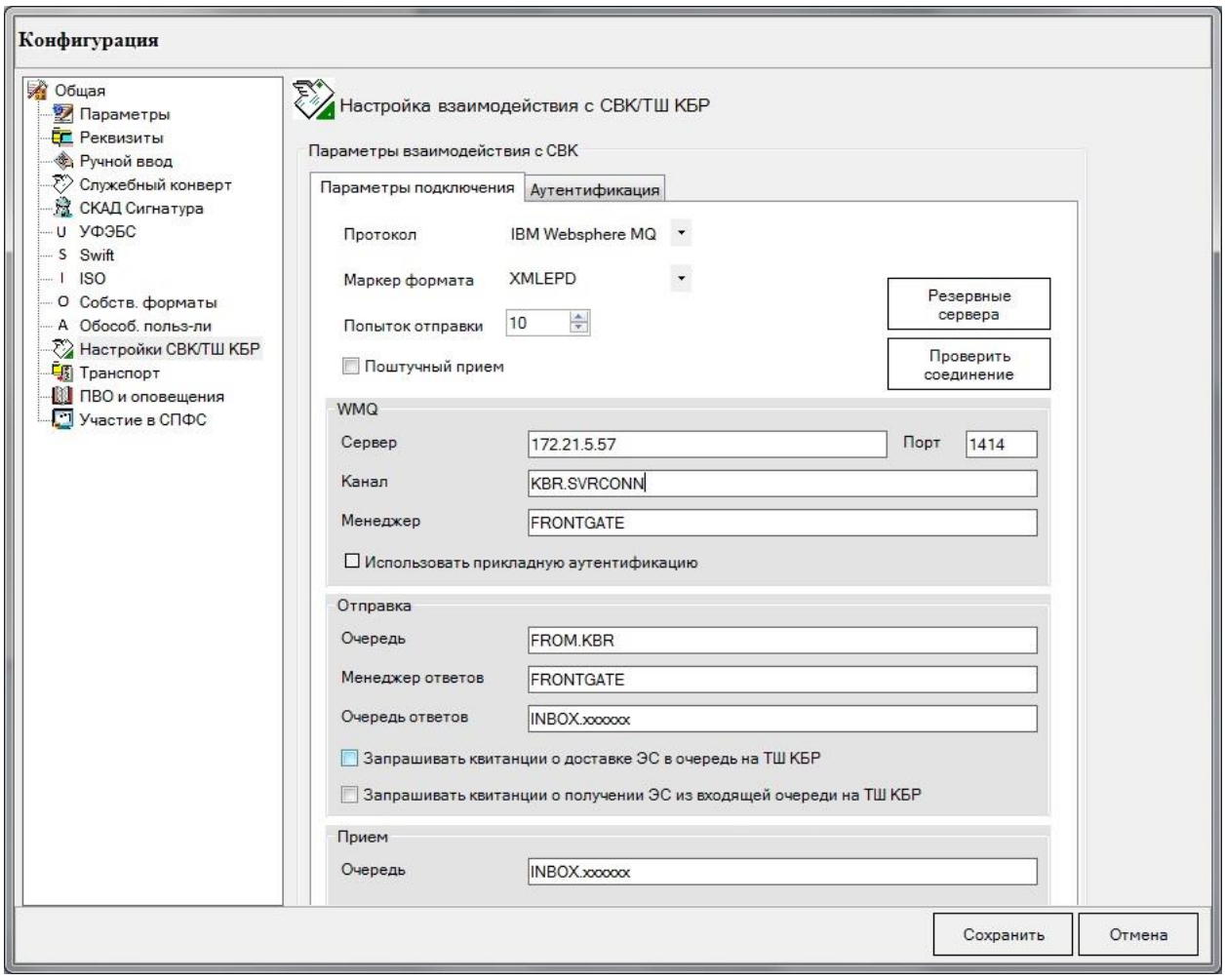


Рис 2б. Настройки взаимодействия СВК / ТШ КБР для ПК АРМ КБР- СПФС (Протокол MQ, тестовый контур)

Также необходимо указать резервные IP-адреса сервера:

172.21.5.58:1414

172.21.5.59:1414

172.21.5.60:1414

Резервные сервера– по кнопке открывается окно, в котором нужно задать список IP адресов ТШ КБР, на которые будет перенаправляться соединение в случае отсутствия подключения к основному серверу.

В) Для работы в <u>промышленном контуре по протоколу HTTP</u> должны использоваться следующие настройки (рис. 3а и 3б):

Сервер отправки: http://172.21.1.57:7777/in

Сервер получения: http://172.21.1.57:7777/get

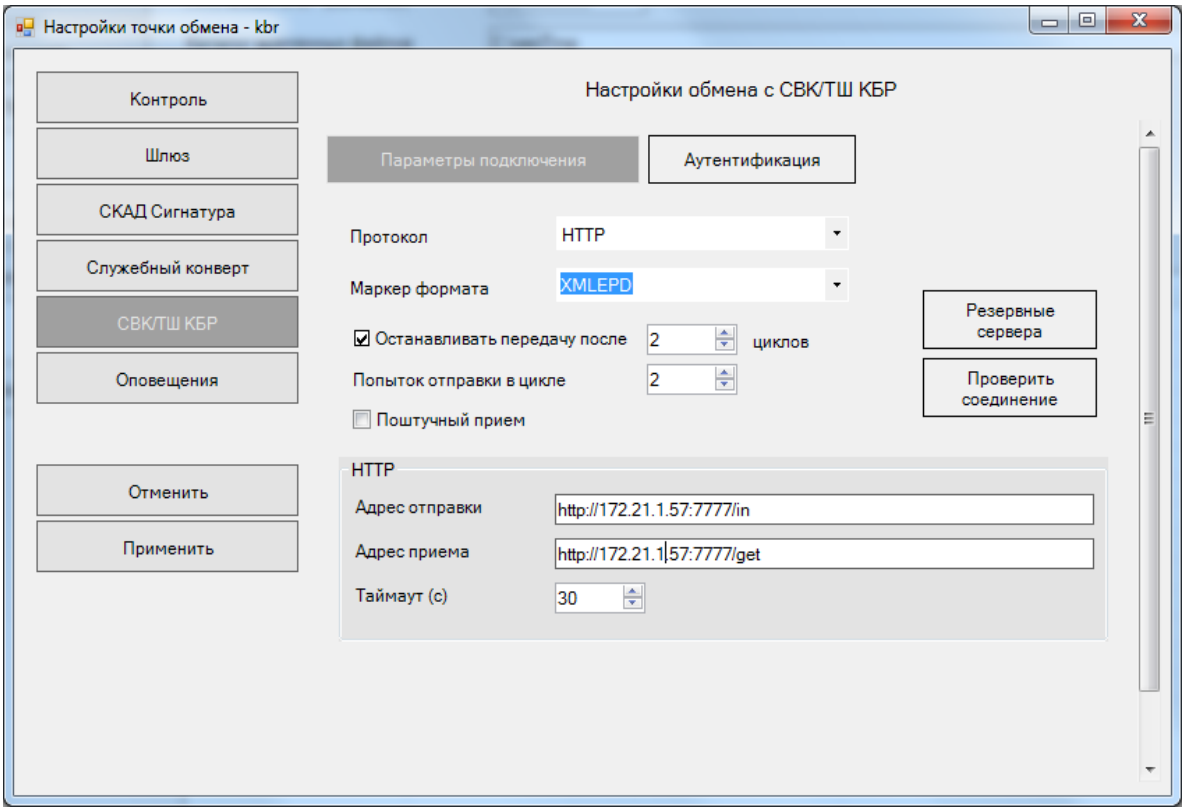


Рис 3а. Настройки обмена СВК / ТШ КБР для ПК АРМ КБР- Н
(Протокол HTTP, промышленный контур)

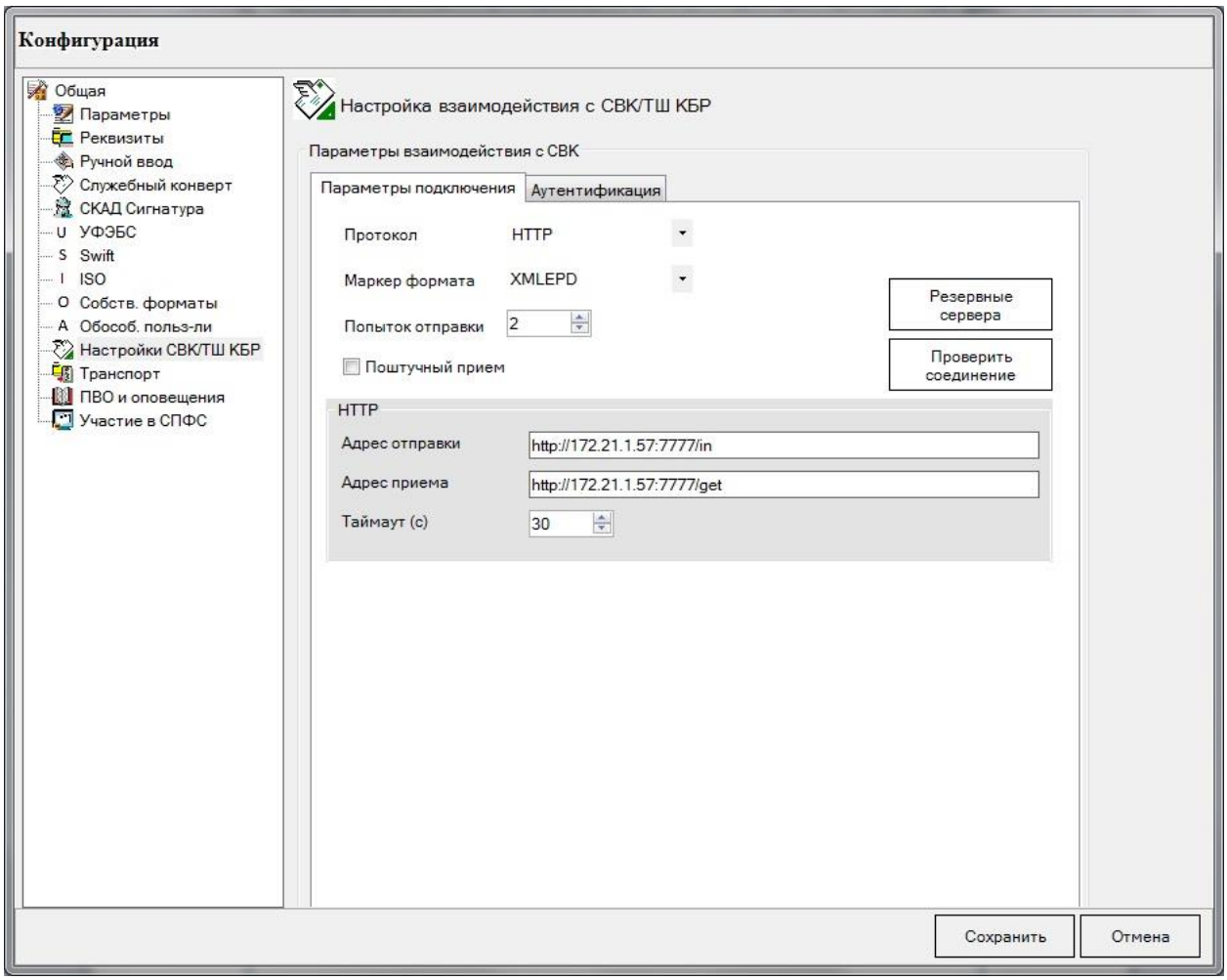


Рис 3б. Настройки взаимодействия с СВК / ТШ КБР для ПК АРМ КБР- СПФС (Протокол HTTP, промышленный контур)

Также необходимо указать резервные IP-адреса сервера:

172.21.1.58:7777

172.21.1.59:7777

172.21.1.60:7777

***Резервные сервера*–** по кнопке открывается окно, в котором нужно задать список IP адресов ТШ КБР, на которые будет перенаправляться соединение в случае отсутствия подключения к основному серверу.

Г) Для работы в <u>промышленном контуре по протоколу MQ</u> должны использоваться следующие настройки (рис.4а и 4б):

WMQ / Сервер: 172.21.1.57

WMQ / Порт: 1414

WMQ / Канал: KBR.SVRCONN

WMQ / Менеджер: FRONTGATE

Отправка / Очередь: FROM.KBR

Отправка / Менеджер ответов: FRONTGATE

Отправка / Очередь ответов: INBOX.xxxxxx (уточняется через Единую службу поддержки пользователей при начале работы по MQ)

Опция Отправка / Запрашивать квитанции о доставке/получении устанавливается опционально при необходимости

Приём / Очередь: INBOX.xxxxxx (уточняется через Единую службу поддержки пользователей при начале работы по MQ)

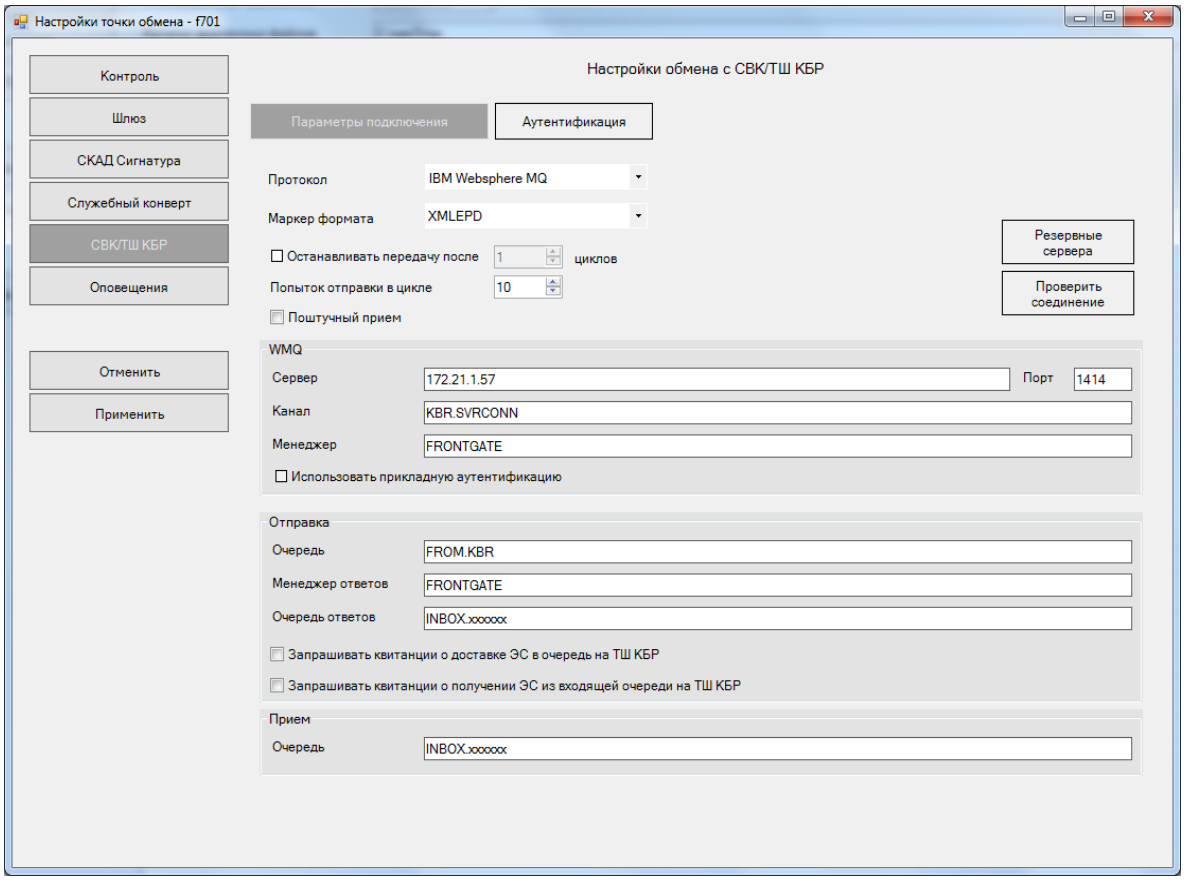


Рис 4а. Настройки обмена СВК / ТШ КБР для ПК АРМ КБР- Н
(Протокол MQ, промышленный контур)

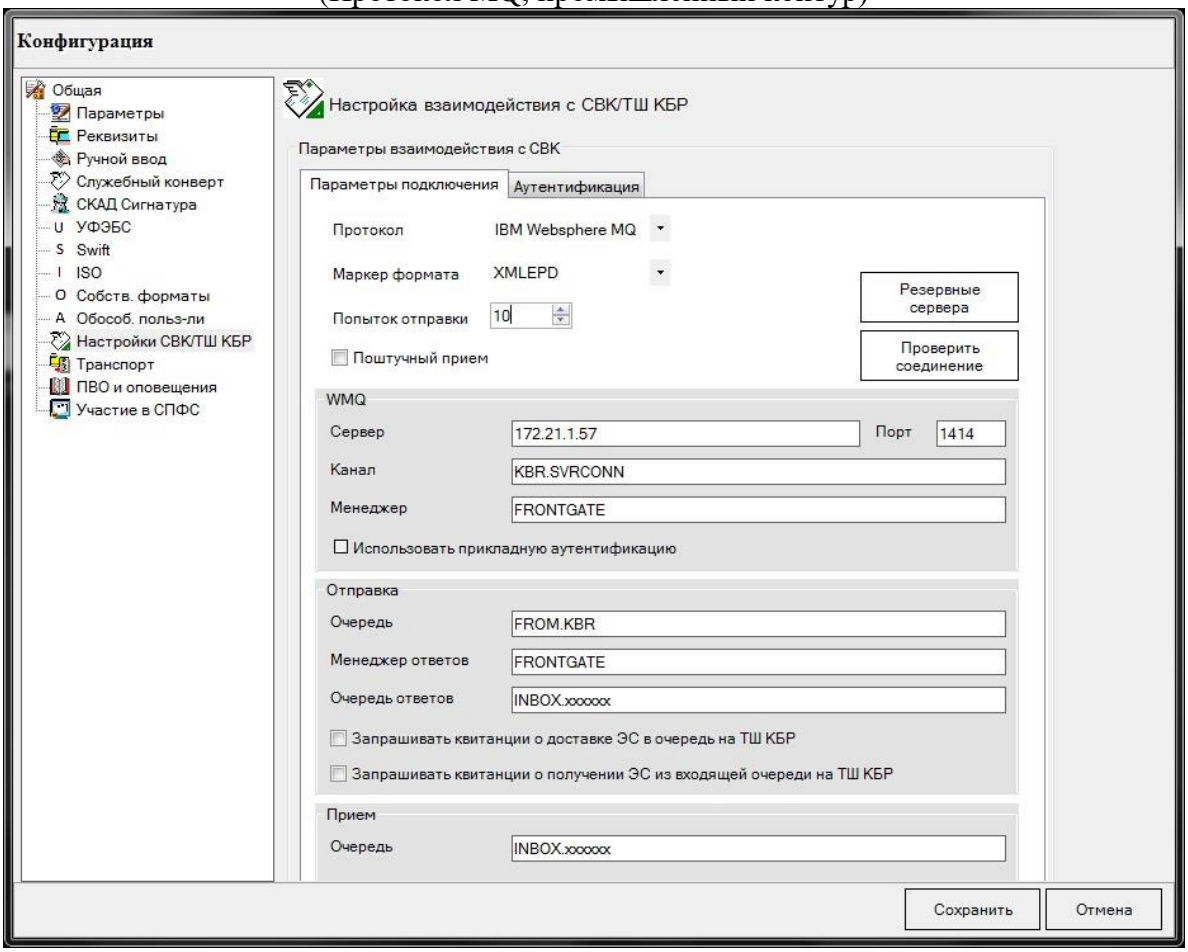


Рис 4б. Настройки взаимодействия с СВК / ТШ КБР для ПК АРМ КБР- СПФС
(Протокол MQ, промышленный контур)

Также необходимо указать резервные IP-адреса сервера:

172.21.1.58:1414

172.21.1.59:1414

172.21.1.60:1414

***Резервные сервера*–** по кнопке открывается окно, в котором нужно задать список IP адресов ТШ КБР, на которые будет перенаправляться соединение в случае отсутствия подключения к основному серверу.