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 1.2 от 07.06.2024)

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 VPNсоединения) 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 России к 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

1	Общие сведения по подключению к КС ТШ КБР	5
2 2.1	Установка СКЗИ «DiSec-W» Подготовительные работы	
2.2	Установка СКЗИ «Disec-W»	8
2.3	Активация СКЗИ «Disec-W»	12
3 3.1	Настройка первого подключения СКЗИ «Disec-W» к узлам ТШ КБР Подготовительные работы	12 12
3.2	Настройка первого подключения к ТШ КБР	13
3.3	Загрузка цепочки сертификатов	16
3	3.3.1 Загрузка закрытого ключа Клиента	16
3	3.3.2 Загрузка личного сертификата Клиента	18
3	3.3.3 Загрузка сертификата корневого УЦ	18
3	3.3.4 Загрузка САС корневого УЦ	19
3	3.3.5 Загрузка сертификата подчиненного УЦ	21
3	3.3.6 Загрузка САС подчиненного УЦ	23
3.4	Настройка автоматического обновления САС	24
3.5	Проверка настроек	29
4	Настройка последующих подключений к узлам ТШ КБР	29
5	Запуск СКЗИ «DiSec-W»	33
6 6.1	Диагностика работы СКЗИ «DiSec-W» Лог файлы СКЗИ «Disec-W»	34 36
6.2	Доступность узлов ТШ КБР	
6.3	Доступность сервисов ТШ КБР	
6.4	Ошибка обновления CRL	
6.5	Направление данных в техническую поддержку	

Сокращение	Расшифровка сокращения
APM	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
CAC	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»

Обозначения и сокращения

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 передает Клиенту СКЗИ «DiSec-W»¹, распространяемое Банком России 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 САС (далее – ключеваяинформация).

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»

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

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-TC». Банк России не оказывает технической поддержки по настройке и эксплуатации таких программно- аппаратных комплексов

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 протоколоввзаимодействия

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 САС, 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 ТСР-портов сервисов ТШ КБР, предоставляемых после построения криптографического туннеля, приведены в Таблице 3.

сервис централизованного распространения САС

аолица 5 – помера тел -портов сервисов тші КВГ					
Номер ТСР-порта	Сервис ТШ КБР				
7777	сервис передачи ЭС по протоколу НТТР				
8888	сервис передачи ЭС по протоколу НТТР				
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)				

Таблица 3 – Номера ТСР-портов сервисов ТШ КБР

9099

2 Установка СКЗИ «DiSec-W»

2.1 Подготовительные работы

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

- a) 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 <u>https://aka.ms/vs/17/release/vc_redist.x86.exe</u>

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

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 указать соответствующие IP-адреса узлов КС ТШ КБР промышленной среды.

Если между оператором связи и APM, 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 APM под своими учетными записями, но с общим закрытым ключом на одном ОМНИ, необходимо выполнить полную установку и настройку СКЗИ «Disec-W» под УЗ Администратора APM 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».

	🕁 Установка — DioNIS(R) Security 7.0 — 🗆 🗙
	Информация Пожалуйста, прочитайте следующую важную информацию перед тем, как продолжить.
	Когда вы будете готовы продолжить установку, нажмите «Далее».
	Энимание! Если на этом компьютере уже установлена программа DiSec, то перед установкой новой версии необходимо удалить предыдущую.
	процедура удаления описана в документации. Программное обеспечение DiSec может конфликтовать со средствами обеспечения безопасности операционной системы, контролирующими сетевую активность (файерволами).
	Рекомендуется удалить или отключить все другие средства обеспечения сетевой безопасности перед установкой DiSec.
	Далее Отмена
Нажать «Далее».	
	🖆 Установка — DioNIS(R) Security 7.0 — 🗆 🗙
	Выбор папки установки В какую папку вы хотите установить DioNIS Security?

нажмите «далее», чтою нажмите «Обзор».	ы продолжить. Если вы хоти	пе выорать другую папку
C:\Program Files\Factor-T	S\DioNIS Security	Обзор

Нажать «Установить».

ё готово к установке			
Программа установки готова компьютер.	начать установку Dic	NIS Security на ваш	(
Нажмите «Установить», что просмотреть или изменить ог	бы продолжить, или « пции установки.	Назад», если вы хот	гите
Папка установки: C:\Program Files\Factor-T	S\DioNIS Security		^
Папка в меню «Пуск»: DioNIS Security			
			>

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.



После перезагрузки на рабочем столе необходимо найти ярлык и кликнуть по нему левой кнопкой мыши. Будет выведено окно активации:

	тортс
Регистрация продукта д С: (SATA SSD) Название	иля выбранного носителя: ~ ? е продукта:
DiSec 1 Номер РС4С6-7186F-70 Ключ ре	 v.7 FULL лиценаии: C3C4-0285F-32318 кистрации:
Зарегистрировать	Запросить ключ
Разрегистрировать	Выход

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 <u>helpdeskmci@cbr.ru</u> 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».

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

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;
- список аннулированных сертификатов корневого УЦ; г)
- сертификат подчиненного УЦ; <u>д</u>)
- е) список аннулированных сертификатов подчиненного УЦ.

ВНИМАНИЕ! В СКЗИ «DiSec-W» существует ограничение при загрузке сертификатов и САС, 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 САС необходимо использовать следующий формат имени файла – CN=ROOTsvc-CA-test.cer; CLN=cln-9805001500.cer

Пля лальнейшей работы СКЗИ «Disec-W» необхолимо, чтобы в ПЭВМ с <u>установленным СКЗИ «Disec-W» был полключен ОМНИ. солержаший закрытый ключ</u> Клиента и цепочку сертификатов.

3.2 Настройка первого подключения к ТШ КБР

ВНИМАНИЕ!

Клиентам Банка России, использующим КС ТШ КБР для взаимодействия в промышленной среде, чьи сертификаты выпущены до 10.06.2024 (на серии ИАС 09), необходимо использовать подключения к ТШ КБР исключительно через узлы «CD-TUZ02» и «CD-TUZ04» КС ТШ КБР, другие узлы при этом не задействуются и должны быть отключены в настройках СКЗИ DiSec-W.

Клиентам Банка России, использующим КС ТШ КБР для взаимодействия в промышленной среде, чьи сертификаты выпущены начиная с 10.06.2024 (на серии ИАС 10), необходимо использовать подключения к ТШ КБР исключительно через узлы «CD-TUZ01» и «CD-TUZ03» КС ТШ КБР, другие узлы при этом не задействуются и должны быть отключены в настройках СКЗИ DiSec-W.

На рабочем столе необходимо найти ярлык мыши.



и кликнуть по нему левой кнопкой

Справа внизу экрана появится значок

14

правой кнопкой мыши вызвать контекстное меню.



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

аметры Обслуживание	
	Версия 7.0
Авто-запуск приложения D/Sec при входе пользователя	
Подключения	
Журнал событий	
Количество файлов журнала 3 Размер файла журнала 10	0000 кБайт
Основной файл журмала	
C:\Program Files\Factor-TS\DioNIS Security\Logs\DiSec.log	
C:\Program Files\Factor-TS\DioNIS Security\DiSec.chk	
С. Улодат Rev Factor TS-DoNIS Security/DSec dHk Провержа сертикикатов подключеной Влочить Провержи кахдине [7] диней	
C-Program Files Vactor TS: DoNIS Security D.Sec chk	

Нажать на кнопку «Подключения» для дальнейшей настройки программы.

10300000	Авто-Коннект	Тип туннеля	IP-agpec(FQDN	Аутентификация	Целевые объек	
						Deeps:
						BHHD
						Экспорт
						Инпорт
						Авто Коннект
						++ 8K/1.
						Balaca
						BCE
Добавить	Изненить	Удалить	Дубль			Очистить
Паранетры А	ато-Коннекта					
	полыток	Число циклов:		ю очереди		

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

aspanite	Авто-Коннект	Тип туннеля	IP-адрес(FQDN	Аутентифия	кация Целевые обт	Beepx
						Вниз
	Выбор осн	овных параметров	в подключения	?	×	Экспорт
	Режин под	аключения:				Импорт
	• дин	АМИЧЕСКИЙ (ІКЕ)	С СТАТИЧЕСК	кий		Авто Коннект
						++ ВКЛ.
						Выкл.
	ОК			OTH	ена	Buffoatta
	L					BCE
0.6.mm			1			
дооавить	Изменить	удалить	Дуоль			Очистить
Паранетры /	вто-Коннекта				-	
		literan unergan		о очерели		

В окне «Реквизиты подключения» выполняются следующие настройки.

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

Реквизиты подключения (CD-TUZ01)	?	×
Общие Параметры Безопасность Задачи		
Тип подключения		
Динамический туннель IKEv1		
Название подключения:		
CD-TUZ01		
Адрес (IP) Сервера VPN:		
172.21.5.26	IPv4	
, Пелевые объекты (доступные ресурсы):		
	~	
	~	
	эктов	
Работа с сетевыми пакетами		
Устанавливать ГГС при туннелировании		
Пооверка входящих ракетов		
Включить защиту от Replay атак		
	_	
Размер ANTI-Replay 512 Макс. Ошибок 20 в SYSLOG		
Макс. Ошибок 100	отные	11
ОК	Отмен	ia

Вкладка «Параметры» – проверить следующие параметры:

Общие Па	раметры Безопасн	юсть Задач	и		
	Γ	IKEv1			
По	итики IKE:		Политики	ESP:	
Создат	Правка		Создать	Правка	1
Интегра	ия в защищенную (еть (MODE_C	FG)		
🔽 3ar	ірос IP-адреса				
0	DOC DNS-CEDBEDOB				
1 34	рос DNS-серверов				
) 3a	прос DNS-серверов				
	рос DNS-серверов	пь жизнеспос	обности туннела	1	
	ірос DNS-серверов Контро	ль жизнеспосо	обности туннеля		
) 3a	рос DNS-серверов Контро Допо	ль жизнеспосо	обности туннеля араметры IKE	·	
j Ja	рос DNS-серверов Контро Допо	ль жизнеспосо	обности туннеля араметры IKE		
) Ja	рос DNS-серверов Контро Допо	ль жизнеспосо	обности туннеля араметры IKE		
<u> </u>	рос DNS-серверов Контро Допо	ль жизнеспосо	обности туннеля аранетры IKE		
1 3a	рос DNS-серверов Контро Допо	ль жизнеспосо лнительные п Стандар	обности туннеля араметры IKE тные		
<u> </u>	рос DNS-серверов Контро Допо	ль жизнеспосо лнительные п Стандар	обности туннеля араметры IKE тные		

Политики IKE	?	×	Политики ESP	? ×	Контроль жизнеспособности тунн ? 🛛 🗙
Параметры алгоритма 28147-89: d-Gost28147-89-CryptoPro-Z-ParamSet	2	•	Режин инкапсуляции трафика: <mark>Туйныслыный</mark>	_	Активный
Режим PFS: Включён	-	•	Преобразование ESP: Крипто-набор: 4М-IMIT	•	Таймаут ожидания ответа (сек): 30
Параметры алгоритма выработки сессионного ключа: id-tc26-gost-3410-12-512-paramSetB +id-tc26-gost3411-12-512		-	Параметры алгоритна выработки сессионного ключа (только 🟹 Как в IKE	для PFS):	Интервал посылки запроса (сек); 10
Период смены ключей Ike(ceк): 2400			Период смены ключей ESP (сек): 2400		Макс. число ошибок 3
			Допустиное количество искаженных пакетов: 100000		
Стандартные			Стандартные		Стандартные
ОК	Отмен	а	ок	Отмена	ОКОтмена

3.3 Загрузка цепочки сертификатов

3.3.1 Загрузка закрытого ключа Клиента Вкладка «Безопасность»:

щие Параметры	Безопасность	Задачи	1			
Настройка PKI для	локального по	пьзовате	ля:			
Настроить		[Ин	циализиро	вать	
Субъект локально	го сертификат	9				_
Аздатель локально	ого сертификат	a (X509)				
					/	
					~	1
) sanpocy		<u> </u>	
Настройка РКІ для Выбрать серті оппонен:	оппонента:) sanpocy	·		
Настройка РКІ для Выбрать серті оппонен Субъект сертифи	оппонента:	ra) sanpocy	, 		
Настройка РКІ для Выбрать серті оппонен Субъект сертифи	оппонента; — фикат а	ra) sanpocy		<u>^</u>	
Настройка РКІ для Выбрать серти оппонен Субъект сертифи	оппонента:	ra) sanpocy	·		
Настройка РКІ для Выбрать серті оппонен Субъект сертифи Издатель сертиф	оппонента:	ra (X500)) sanpocy	·	× · · ·	
Настройка РКІ для Выбрать серті оппонен Субъект сертифи Издатель сертиф	оппонента:	ra ra (X500)) sanpocy	· 		
Настройка РКІ для Выбрать серт оппонен Субъект сертифи Издатель сертиф	оппонента;	ra ra (X500)) sanpocy			
Настройка РКІ для Выбрать серти оппонен Субъект сертифи Издатель сертиф	оппонента;	га га (X500) кента) sanpocy			

Выбрать «Настроить».

16



17

Сообщение "Ошибка получения криптоконтекста. Невозможно получить параметры РКІ 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».

Настройка PKI пользователя	?	×
Общие CRL UPDATE OCSP		
Сертификат пользователя:		
		_
<		>
Установить личный	сертификат	
Работа с хранилищами сертификатов		
🗖 Защитить Хранилище сертификатов корневых УЦ имитовстав	кой	
Предупреждать об окончании срока действия сертификата 3	дней	
Сохранить	Отме	на)

Выбрать «Установить личный сертификат».

Первым этапом будет предложено выбрать ОМНИ, на котором находится закрытый ключ. Если ОМНИ является USB-flash:

Директория	Объект	Формат	Информация	Сер.номер/Имя	
		[DIR]	F:\TEST\		
-:\TEST\	CLN-45999999999	9.p15 P15	F:\TEST\		
C					>

Если ОМНИ является Rutoken:

Folder	Object	Format	Info	Serial/Name	
P11_RuToken:\D\ E·\	899add12.p15	P15	Aktiv Rutoken	3cde8127	/Rutoken ECP <no< th=""></no<>

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

кнопку «Выбрать».

УЦ:

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:

Вниман	ne	\times
Â	В текущей директории НАЙДЕН файл сертификата F:\TEST\CLN-459999999999.cer Установить? Нажмите 'Нет' для продолжения выбора	
	аНет	

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

_
· · · ·

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».

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

3.3.4 Загрузка САС корневого УЦ

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



Убедиться, что предлагаемый к загрузке САС 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».



Настройка РКІ пользователя	?	×
Общие CRL UPDATE OCSP		
Сертификат пользователя:		
X509-Ceptridywat Cyfbeer: ddl@factor-ts.ru, 09.1, 4599999999, CLIENT-FES Идатель: CEPSox-CA-test, CEPS, PKL, region, dry, ru Действителен: C18/10/2022 r. no 19/10/2037 r. Ceptivihiadi nonep: 40601890 1968964 94501240 6348568 HasvaeningCaughenhab: Heissectrice pacupperhoe ic Key Usage: DigitalSignature, NonRepudiation, KeyEnopherment, Data Orme-aros KHA (Thumbornit): AUSTAS C317928 C5953766 2372 Orme-aros KHA (Thumbornit): AUSTAS C317928 C5953766 2374 Authority Key Identifier:	T, 45, KSTS nonusobah Encipherme C27D 6E0D 10923B9	нквк Int, К 6С49
		>
Установить личный	сертифика	л
Работа с хранилищами сертификатов		
🗖 Защитить Хранилище сертификатов корневых УЦ имитовстави	юй	
Предупреждать об окончании срока действия сертификата 3 Сохранить	дней От	мена

В окне «Настройка РКІ 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.

DISEC: ОШИБКА	×
Ошибка получения сертификата пользователя из хранилища	
ОК]

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

Реквизиты подключения (CD-TUZ01)	?	×
Общие Параметры Безопасность Задачи		
Настройка РКІ для локального пользователя:		
Настроить Инициализиров	зать]
Субъект локального сертификата		_
CN=CLN-459999999999, C=RU, L=KSTSHKBR, STREET=45, O=CLIENT-TEST, OU=4599999999, T=09.1, E=ddl@factor-ts.ru		
Издатель локального сертификата (Х509)		
DC=ru, DC=cbr, DC=region, OU=PKI, OU=CEPS, CN=CEPSsvc-C	A-test	
Посылка локального сертификата По запросу	•	
Настройка РКІ для оппонента: Выбрать сертификат оппонента		
Субъект сертификата опппонента		
	$\hat{}$	
Издатель сертификата оппонента (Х500)		
	^	
J Запросить сертификат оппонента	V	
Проверить		
OK	Отме	на

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»

квизиты подключения	(CD-10201)				
Общие Параметры Бе	езопасность 3	адачи			
- Настройка РКІ для ло	кального польз	вателя: -			
Настроить			Инициализ	ировать	
Субъект докадыного	сертификата				
CN=CLN-45999999999 O=CLIENT-TEST, OU=	99, C=RU, L=KS =4599999999, T=	TSHKBR, ST =09.1, E =d	IREET=45, dl@factor-ts	s.ru	Ŷ
, Издатель локального	сертификата ()	(509)			
DC=ru, DC=cbr, DC=	region, OU=PKI,	OU=CEPS,	, CN=CEPSs	vc-CA-tes	t ^
, Посылка локально	го сертификата		0001	-	
— Настройка РКІ для опі Выбрать сертифи оппонента	понента:				
Настройка РКІ для опі Выбрать сертифи оппонента Субъект сертификат	понента:				
Настройка РКІ для опі Выбрать сертифи оппонента Субъект сертификат	понента: кат га опппонента				^
-Настройка РКІ для оп Выбрать сертифи оппонента Субъект сертификат	понента: икат га опппонента				< >
Настройка РКІ для оп Выбрать сертифи оппонента Субъект сертификат Издатель сертифика	понента: икат та опплонента ата оппонента (×500)			< >
Настройка РКІ для оп Выбрать сертифи оппонента Субъект сертификат Издатель сертифика	понента: «кат га опппонента ата оппонента ()	x500)			< > <
Настройка РКІ для оп Выбрать сертифи оппонента Субъект сертификат Издатель сертифика	понента: «кат га опппонента ата оппонента ()	K500)			< >
Настройка РКІ для от Выбрать сертифи оппонента Субъект сертификат Издатель сертифика	понента: «кат га оппонента ата оппонента (фикат оппонента	x500)			< >
Настройка РКІ для оп Выбрать сертифи оппонента Субъект сертификат Издатель сертифика	понента: якат та опплонента ита оппонента () фикат оппонент Прове	x500) га			< > < >

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

Настро	йка PKI пользователя		?	×
Общие	CRL UPDATE OCSP			
Серт	ификат пользователя:			
Key Orri Aut Sub	-Сертификат Субъект: dd@factor-ts.ru, 09; Издатель: CEPSov-CA-test, CE Действителен: c 18/10/2022 г. Серийный номер: 40601890 19; Назначения(расширенные): Не чизаре: DigitaSignature, NonRepuda начаток SHA (Thumbprini): 0.00374A нечаток MD5: 5000A4D103142006 C hority Key Identifier: 0.1890153C545 ject Key Identifier:	1, 459999999, CLIENT-TES 59, PKJ, region, dxr, ru no 19/10/2037 r. 3896F 94501240 634E5568 IvisecTrikop paculipperinde inc bon, KeyEncipherment, Data 5 C3175526 C59537E6 2372 304849A 64579A89 Av98DEC3 1A8D 3A 3DDA IBE6	Г, 45, KSTS пользовані Encipherme C27D 6E0D 0923B9	нквR ие кл nt, К 6С49
<				>
		Установить личный	сертифика	т
	Работа с хранили	щами сертификатов		
□ 3	ащитить Хранилище сертификатов	корневых УЦ имитовставк	ой	
Coxpa	а упреждать об окончании срока де нить	йствия сертификата 3	дней Отг	1ена

Нажать кнопку «Работа с хранилищами сертификатов».

ота с хранилищами се	ртификатов	7	>
Сертификаты Списки от	зыва Корневые УЦ		
Имя	Кем выдан	Срок действия	
CN=CLN-4599999999999 CN=ROOTsvc-CA-test	CN=CEPSsvc-CA-test CN=ROOTsvc-CA-test	18.10.2022 - 19.10.2037 16.03.2022 - 17.06.2039	
062		Экспорт	
доон	Удалито	Jikalopi	
Coversiver: Vestimer	Добавить из файла з	кранилища	
Сохранить хранилище			

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

директория	Объект	Формат	Информация	Сер.номер/Имя		
		[DIR]	F:\TEST\			1
:\TEST\	CEPSsvc-CA-test.cer	CER	F:\TEST\			1
:\TEST\	CLN-4599999999999.cer	CER	F:\TEST\			
:\TEST\	ROOTsvc-CA-test.cer	CER	F:\TEST\			
C					>	

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

Имя	Кем выдан	Срок действия
CN=CLN-459999999999	CN=CEPSsvc-CA-test	18.10.2022 - 19.10.2037
CN=ROOTsvc-CA-test	CN=ROOTsvc-CA-test	16.03.2022 - 17.06.2039
CN=CEPSsvc-CA-test	CN=ROOTsvc-CA-test	16.03.2022 - 17.06.2039
1.0-6	Manager 1	2
Дооавить	удалить	SKCIOPT

3.3.6 Загрузка САС подчинённого УЦ

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

ертификаты Списки отзыва Корневые УЦ		
Кем выдан	Действител	Следующее
IN=ROOTsvc-CA-test	11.04.2022	16.06.2024
Добавить Удалить	Экспорт	

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

Запрос		\times
	В текущей директории НАЙДЕН файл со списком отозванных сертификатов (CRL)	
	F:\TEST\CEPSsvc-CA-test.crl	
	Добавить список в хранилище?	
	Нажмите 'Нет' для продолжения выбора	
	Па Нет	1

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



Следует нажать «Да».

		f 2
сертификаты Списки отзыва Корневые УЦ		
Кем выдан	Действит	ел Следующее
CN=ROOTsvc-CA-test	11.04.202	2 16.06.2024
CN=CEPSsvc-CA-test	11.04.202	2 16.06.2024
Побавить Улавить	Эксполт	1
Добавить Удалить	Экспорт]
Добавить Удалить Соходнить Ходнилине Лобавить	Экспорт]
Добавить Удалить Сохранить Хранилище Добавить и	Экспорт	

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

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

«Сохранить».

3.4 Настройка автоматического обновления САС

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

Настро	йка PKI пользователя	?	×
Общие	CRL UPDATE OCSP		
	I Отключить обновление COC(CRL)		
	ізвлекать URI CDP из сертификатов		
URI (HTTP/FTP/LDAP) точки распределения списка отзыва (CRL):	Справка	10 URI
	<		>
_	Настроить список URI		
~	Выполнить до установки туннеля 🛛 📈 Выполнить после у	становки т	уннеля
	Обновить CRL		
	Принять		
Сохра	ИЛТЬ	От	мена

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

Настройка РКІ пользователя	?	×
Общие CRL UPDATE OCSP		
Отключить обновление COC(CRL)		
Извлекать URI CDP из сертификатов		
URI (HTTP/FTP/LDAP) точки распределения списка отзыва (CRL):	Справка по	URI
<		>
Настроить список URI Выполнить до установки туннеля 🔽 Выполнить после у	становки тун	неля
Обновить CRL		
Принять		
Сохранить	Отм	ена

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	Тестовая	Корневой	http://172.21.5.57:9099/tsh/crl YY .crl
первого объекта		Подчиненный	http://172.21.5.57:9099/xx/crlYY.
			crl

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

где ҮҮ – это номер серии.

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

стройка спи	ıска URI						?	×
Список URI								
Ном П	ро Логи	н Пар	IP-a	Порт	Пап	Имя		
							Вве	px
							BH	ИЗ
Добавит	ть	Из	менить		Уд	алить		
		Очи	стить BCI	=				
ОК							Отг	ена

Нажать кнопку «Добавить».

Настройка URI			?	×
Протокол НТТР IP-адрес		Порт		_
Параметры аутентификации Логин:	Пароль:	зать пароль		
Директория	_	Имя файла		_
		*	0	
			Отме	на

При заполнении полей окна:

- a) в поле «Протокол» необходимо указать «НТТР»;
- 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".

Настройка URI		?	×
Протокол			
IР-адрес 172.21.5.57	Порт 9099		
Параметры аутентификации			1
Логин:	Пароль:		
1	Показать пароль		
Директория tsh	Имя файла crl.crl		
1	1 .		
ОК		Отме	на

Нажать кнопку «ОК».

Нажать кнопку «Добавить».

Настройка URI		?	×
		•	~
Протокол			
IP-адрес	Порт		
Параметры аутентификации			
Логин:	Пароль:		
	🗌 Показать пароль		
Директория	Имя файла		
ОК		Отмен	ia

При заполнении полей окна:

- а) в поле «Протокол» необходимо указать «НТТР»;
- б) в поле «IP-адрес» указать «172.21.5.57»;

2	6	
2	6	

- в) в поле «Директория» указать «45»;
- г) в поле «Имя файла» указать «crlYY.crl», где *YY* номер серии;
- д) в поле "Порт" указать "**9099".**

Настройка URI		?	×
Протокол	Порт 9099		_
, Параметры аутентификации — Логин:	Пароль:		
Директория 45	Имя файла crl.crl		
OK		Отме	на

Нажать «ОК».

По окончании настройки должно иметь следующий вид.

Настро	йка списка l	JRI					?	×
Спис	K URI							
Ho	1 Про	Логин	IP-адрес	Порт	Пап	Имя		
1	HTTP		172.21.5.57	9099	tsh	crl.crl		
2	HTTP		172.21.5.57	9099	45	al.al	Вве	px
							BH	низ
	1060000		Management	1	V			
	цооавить		Изменить			Lavivi B		
			Очистить В	CE				
	_						0	
OK							UTI	пена

Нажать «Ок».

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

еквизиты подключения (CD-TUZ01)	? ×
Общие Параметры Безопасность Задачи	
Настройка РКІ для локального пользователя:	
Настроить Инициализиро	вать
Субъект локального сертификата	
CN=CLN-459999999999, C=RU, L=KSTSHKBR, STREET=45, O=CLIENT-TEST, OU=4599999999, T=09.1, E=ddl@factor-ts.ru	$\hat{}$
Издатель локального сертификата (Х509)	
DC=ru, DC=cbr, DC=region, OU=PKI, OU=CEPS, CN=CEPSsvc-C	A-test
Посылка локального сертификата	
Настройка РКІ для оппонента: Выбрать сертификат оппонента	
Субъект сертификата опппонента	
	$\hat{\mathbf{v}}$
Издатель сертификата оппонента (Х500)	
	<u>^</u>
I П Запросить сертификат оппонента	4
Проверить	
ок	Отмена

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».

ота с хранилищами сертиф	икатов	?	×
ертификаты Списки отзыва	а Корневые УЦ		
Имя	Кем выдан	Срок действия	
CN=CLN-459999999999	CN=CEPSsvc-CA-test	18.10.2022 - 19.10.2037	
CN=ROOTsvc-CA-test	CN=ROOTsvc-CA-test	16.03.2022 - 17.06.2039	
CN=CEPSsvc-CA-test	CN=ROOTsvc-CA-test	16.03.2022 - 17.06.2039	
Выбрать Добавить	Удалить	Экспорт	
Сохранить Хранилище	Добавить из файла >	ранилища	
or I			-

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

• 1-	-	1_	1		
бщие Параметры	Безопасность	Задачи			
Настройка РКІ для	локального пол	њзовател	19:		
Настроить		[Инициализ	ировать	
Субъект локально	го сертификата	•			
CN=CLN-45999999 O=CLIENT-TEST, C	99999, C=RU, L= 0U=45999999999	KSTSHKB , T=09.1,	R, STREET=45, E=ddl@factor-ts	.ru	$\hat{\mathbf{v}}$
, Издатель локальн	ого сертификат	a (X509)			
DC=ru, DC=cbr, D	C=region, OU=P	KI, OU=C	EPS, CN=CEPSsv	c-CA-test	$\hat{}$
Посылка локал	ьного сертифик	ата по	запросу	-	
		,			
Настройка РКІ для Выбрать серт оппонен	оппонента: ификат та				
Настройка РКІ для Выбрать серт оппонен Субъект сертифи	оппонента: ификат та ката опппонент	a			
Настройка РКІ для Выбрать серт оппонен Субъект сертифи	оппонента: ификат та ката опппонент				< >
Настройка РКІ для Выбрать серт оппонен Субъект сертифи Издатель сертиф	оппонента: ификат та ката опплонент иката оппонент	a (X500)			< >
Настройка РКІ для Выбрать серт оппонен Субъект сертифи Издатель сертиф DC=ru, DC=cbr, Г	оппонента: ификат ката опппонент иката оппонент DC=region, OU=I	a (X500) PKI, OU=0	SUBZI, CN=ROOT		< > <
Настройка РКІ для Выбрать серт оппонен Субъект сертифи Издатель сертиф DC=ru, DC=cbr, D CA-test	оппонента: ификат ката оппонент иката оппонент DC=region, OU=1	a (X500) PKI, OU=0	JUBZI, CN=ROOT	ſsvc-	<>
Настройка РКІ для Выбрать серт оппонен Субъект сертифи Издатель сертиф [DC=ru, DC=dr, I CA-test У Запрооть сер	оппонента: ификат та иката оппонент иката оппонент DC=region, OU=1 этификат оппон	а а (X500) РКІ, ОU=0 ента	SUBZI, CN=ROOT		< >

28

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.

DiSec	×
1	Проверка сертификатов Подключения [CD-TUZ01] выполнена УСПЕШНО
	OK

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.

П	одключения					?	\times
	Ресурсы подключений						
	Hassawe CD-TUZ01	Авто-Коннект 0	Тип туннеля Дин. IKEv1	IP-appec(FQDN 172.21.5.26	Аутентификация Ц PKI: CN=DR-45	Вверх Вниз Экспорт Импорт	
	¢				2	++ ВКЛ. Выкл. Выбрать ВСЕ	
	Добавить Изменить	Удалить	Дубль			Очистить	
	Параметры Авто-Коннекта Макс, число полыток одного подключения	Число циклов:	2	По очереди			
		ОК	Пр	ервать			

4 Настройка последующих подключений к узлам ТШ КБР.

Левой кнопкой мыши выделить подключение и нажать «Дубль».

Deutre Internation Internation <t< th=""><th>aspannic</th><th></th><th>ARTO-KONNEKT</th><th>Тип тучнело</th><th>IP-annec/EODN-</th><th>Avrentiebuicaulea</th><th></th></t<>	aspannic		ARTO-KONNEKT	Тип тучнело	IP-annec/EODN-	Avrentiebuicaulea	
ССО-ТИZO1 0 Дин.: IXEV1 172.21.5.26 РИС: СМ=ОR.45 	D-THZ01		ABTO-KOHHEKT		172 21 5 26	PKT: CN-DP-45	Beeny
	JP CD-TUZ01		0	Дин. IKEv1 Дин. IKEv1	172.21.5.26	PKI: CN=DR-45	верх
Внорт Инпорт Авто Коннект ++ ВКЛ. ВыКл. Выбрать ВСЕ							
Экспорт Инпорт Авто Коннект ++ ВКЛ. ВыКЛ. Выбрать ВСЕ							Вниз
 Инпорт 							Remont
Инпорт Авто Коннект ++ ВКЛ. Выкл. Выбрать ВСЕ							DKchopi
Авто Кончект ++ ВКЛ. Выкл. Выбрать ВСЕ							Импорт
Авто Коннект ++ ВКЛ. Выкл. Выбрать ВСЕ							
++ ВКЛ. Выкл. Выбрать ВСЕ							Авто Коннект
Выкл. Выбрать ВСЕ							++ ВКЛ.
Bu6pate BCE							Выкл.
Выбрать ВСЕ							
Выбрать ВСЕ							
BCE							Выбрать
							BCE
							, ,
		1		1	-		
	обавить	Изменить	Удалить	Дубль			Очистить
бавить Изменить Удалить Дубль Очистить							
бавить Изменить Удалить Дубль Очистить							
бавить Удалить Дубль Очистить		о-Коннекта					
бавить Изненить Удалить Дубль Очистить аранетры Авто-Коннекта	Параметры Авт	o reormerero					
бавить Изменить Удалить Дубль Очистить араметры Авто-Коннекта Макс, число польтток	Параметры Авт Макс, число по	пыток	linear interna		De average de la		
>]обавить	Изменить	Удалить	Дубль		2	Выбрать ВСЕ Очистить
	обавить	Изменить	Удалить	Дубль	7		OUNCTINTE
бавить Изменить Ударить Лубль	CCCCC			A)0//0			Очистить
бавить Удалить Дубль Очистить							

Нажать кнопку «И	Ізменить».
------------------	------------

Реквизиты подключения (DUP_CD-TUZ01)	?	×
Общие Параметры Безопасность Задачи		
Тип подключения		
Динамический туннель IKEv1		
Название подключения:		
DUP_CD-TUZ01		
Адрес (IP) Сервера VPN:		
172.21.5.26	🗹 IPv4	
_Целевые объекты (доступные ресурсы):		_
	~	
	\sim	
✓ Запросить IP-подсеть (MODE_CFG) Список об	ъектов	
Работа с сетевыми пакетами		_
Устанавливать TTL при туннелировании 32		
Проверка входящих пакетов		
Размер ANTI-Replay 512 Макс. Ошибок 20	,	
Макс. Ошибок 100 Стан	дартные	1
ОК	Отмен	a

Следует привести к следующему виду:

	ыподолочег	ния (СD-10202)			ſ	
Общие	Параметры	Безопасность	Задачи			
Тиг	п подключени	R				
Дин	амический ту	ннель IKEv1				
Назва	ание подключ	ения:				
CD-	TUZ02					
Адре	с (IP) Сервера	VPN:				
172	.21.5.34				IPv4	
		acer yn die pery	<i>,</i>		^	
					~	
▼ 3	апросить IP-n	одсеть (MODE_C	FG)	Список	: объектов	
✓ 3 Работ	апросить IP-п а с сетевыми і	одсеть (MODE_C пакетами	FG)	Список	объектов	
✓ 3 Работ Устана	апросить IP-п а с сетевыми і авливать TTL і	одсеть (MODE_C пакетами при туннелирова	FG) нии <u>32</u>	Список	собъектов	
Г 3 -Работ Устана -Прове	апросить IP-п а с сетевыми і авливать TTL і рка входящих	одсеть (MODE_C пакетами при туннелирова к пакетов	FG) нии <u>32</u>	Список	с объектов	
Г 3 -Работ Устана Прове Г Вкл	апросить IP-п а с сетевыми і авливать TTL і рка входящих лючить защит	одсеть (MODE_C пакетами при туннелирова к пакетов у от Replay атак	FG) ники 32	Список	собъектов	
Г 3 -Работ Устана Прове Г Вкл Разма	апросить IP-п а с сетевыми і авливать TTL і ірка входящиз пючить защит ер ANTI-Repla	одсеть (MODE_C пакетами при туннелирова к пакетов у от Replay атак у 512	FG) ниии 32 Макс. Ошибок в SYSLOG	Список	20	
Г 3 -Работ Устана Прове Г Вкл Разми Максо	апросить IP-п а с сетевыми и авливать TTL и рка входящих почить защит ер ANTI-Replar с. Ошибок	одсеть (MODE_C пакетами при туннелирова к пакетов у от Replay атак у 512 100	FG) ниии 32 Макс. Ошибок в SYSLOG	Список	20	
Г 3 Работ Устана Прове Г Вкл Разм Макс	апросить IP-п а с сетевыми и авливать TTL и рка входящих почить защит ер ANTI-Replay Ошибок	одсеть (MODE_C пакетами при туннелирова к пакетов у от Replay атак у 512 100	FG) ниии 32 Макс. Ошибок в SYSLOG	Список	20 гандартные	

31

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

Настройка списка URI	-		? ×
Список URI			
Ном Про Логин	Пар ІР-а Порт	Пап Имя	
			Вверх
			Вниз
Добавить	Изменить	Удалить	
	Очистить ВСЕ		
ОК			Отмена

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

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

Для корневого сертификата №1 указываются следующие настройки:

- a) 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 «НТТР»;
- 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:

Ном	Про	Логин	IP-адрес	Порт	Nan	Имя	
1	HTTP		172.21.5.58	9099	tsh	crl.crl	
							Вни
				-1			

Нажать «ОК».

Нажать «Сохранить».

Нажать «ОК».

По окончании настройки должен быть следующий результат:

Тазвание	Авто-Коннект	Тип туннеля	IP-адрес(FQDN	Аутентификация Ц	
D-TUZ01	0	Дин. IKEv1	172.21.5.26	PKI: CN=DR-45	Вверх
CD-TUZ02	0	Дин. ІКЕ 1	172.21.5.34	PKI: CN=DR-45	
CD-TUZ03	0	Дин. ІКЕ 1	172.21.5.42	PKI: CN=DR-45	
D-TUZ04	0	Дин. IКЕ∨1	172.21.5.50	PKI: CN=DR-45	Вниз
					Экспорт
					Импорт
					++ вкл.
					Выкл.
					Выбрать
					BCE
				>	
Добавить Изменить	Удалить	Дубль			Очистить
Deserves Area Konstan					
Паранетры Авточконнекта					
Макс. число попыток одного подключения	Число циклов	: 2	🗌 По очереди		

ВНИМАНИ Е! 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.

ŧ

Подключиться	
Отключиться	>
Состояние	
Настройка	
Проверить сертификаты	
Журналы	
Диагностика	
Протокол сети	
Справка	
О программе	
Выход	

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

Подключиться	? ×
Список ресурсов подключения	Начать
Прервать цикл	Число 1 попыток 1 Число 1 щиклов
Выводить окно диагностических сообщений	По очереди

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

	Начать
CD-TUZ01(VBI) CD-TUZ02(VBI) CD-TUZ03(VBI) CD-TUZ03(VBI) CD-TUZ04(VBI)	Число 10 попыток 2 Число 2
🗌 Выводить окно диагностических сообщений	циклов По очереди

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

Подключиться	? ×
Список ресурсов подключения СD-TUZ01,CD-TUZ02,CD-TUZ03,CD-TUZ04 СD-TUZ01 СD-TUZ01 СD-TUZ02 СD-TUZ03 СD-TUZ04 СD-TUZ04	Начать Число 100 попыток 2 Число 2
Выводить окно диагностических сообщений	🗌 По очереди

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.

🗑 "Annocrina Dise	
Файл Поиск	
24-04-2022 10:11:00.010: [[CD-TUZ01]]: Докалыка проферка серцицикаль пользобањила былоленна целению 24-04-2022 10:11:00.010: [[CD-TUZ01]]: Докалыка проферка серцицикаль пользобањила былоленна целению 24-04-2022 10:43:02,755:	^
Unnetens 1/2/21.5.4b (1Pv4) Tun sponses 100-	
24-64-2022 18 49 02 980. [[CD-TUZ01]]: Tymena. 1922 168 57. 552 → 172. 21. 5. 26 (MTU-1500) 254-2622 18 49 02 980. [[CD-TUZ01]] 254-2622 19 (92. 931. [[CD-TUZ01]]) 70 modema: 172. 21. 5. 34 (IPv4) Tun aguesar, IJun.	l
24-04-2022 19:49:02.958: [[CD-TUZ02]]: Tymens.n. 192_168:57.152 → 172.21.5.34 (MTU-1500) 24-04-2022 19:49:02.558: [[CD-TUZ02]]: []: 24-04-2022 19:49:02.558: [[CD-TUZ02]]: 25-04-2021 20:1000 []: 25-04-2021 20:1000 []: 0000000000 []: 10000000000 []: 100000000000 []: 100000000000 []: 100000000000 []: 100000000000 []: 100000000000 []: 1000000000000000000000000000000000000	l
24-04-2022 18:49:02.999: [[CD-TUZ01]]: Tpumenas. 192_168 57.152 → 172.21.5.42 (MTU-1500) 26-04-2022 18:49:00.0095: [[CD-TUZ013]]: Gueso.neuwo CRL u Epodepna cepnu4unanco 26-04-2022 18:102-22.21.21.21.21.21.21.21.21.21.21.21.21.2	l
2-6-6-2022 10 49 03.006 [[CD-TUZ01]] Directs: 123,2168 27,152 - 172,21,5.50 (MTU-1500) 2-6-6-2022 10 49 03,056 [[CD-TUZ01]] Directs: 1050pepts cemputanses 2-6-6-2022 10 49 03,520 [[CD-TUZ01]] Directs: 1050pepts cemputanses 2-6-6-2022 10 49 03,597 [[CD-TUZ01]] Directs: 107001 [[Massasses] (MFACIDE TSHCK_BootSubordinateGA) Onnovemens (Magamens: CM-FACTOE TSHCK/_BootCA) 2-6-6-2022 10 49 03,997 [[CD-TUZ01]] Directs: 107001 [[Massasses] (MFACIDE TSHCK_BootSubordinateGA) Onnovemens (Magamens: CM-FACTOE TSHCK/_BootCA) 2-6-6-2022 10 49 03,097 [[CD-TUZ01]] Directs: 107001 [[Massasses] (MFACIDE TSHCK_BootSubordinateGA) Onnovemens (Magamens: CM-FACTOE TSHCK/_BootCA) 2-6-6-2022 10 49 04 03 098 [[CD-TUZ01]] Directs: 107001 [[Massasses] (MFACIDE TSHCK_BootSubordinateGA) Onnovemens (Magamens: CM-FACTOE TSHCK/_BootCA) 2-6-6-2022 10 49 04 04 098 [[CD-TUZ01]] Directs: 00000 [[Massasses] (MFACIDE TSHCK_BootSubordinateGA) Onnovemens (Magamens: CM-FACTOE TSHCK/_BootCA) 2-6-6-2022 10 49 04 04 098 [[CD-TUZ01]] Direct companying and monocodamens grammo 2-6-6-2022 10 49 04 04 098 [[CD-TUZ01]] Direct companying and monocodamens grammo 2-6-6-2022 10 49 04 04 098 [[CD-TUZ01]] Direct companying and monocodamens grammo 2-6-6-2022 10 49 04 04 098 [[CD-TUZ01]] Direct companying and monocodamens grammo 2-6-6-202 10 49 04 04 098 [[CD-TUZ01]] Direct companying and monocodamens grammo 2-6-6-202 10 49 04 04 098 [[CD-TUZ01]] Direct companying and monocodamens grammo 2-6-6-202 10 49 04 04 098 [[CD-TUZ01]] Direct companying and monocodamens grammo 2-6-6-202 10 49 04 04 098 [[CD-TUZ01]] Direct companying and monocodamens grammo 2-6-6-202 10 49 04 04 098 [[CD-TUZ01]] Direct companying and monocodamens grammo 2-6-6-202 10 49 04 05 05 29 [[CD-TUZ01]] Direct companying and monocodamens grammo 2-6-6-202 10 49 04 05 05 29 [[CD-TUZ01]] Direct companying and monocodamens grammo 2-6-6-202 10 49 05 05 29 [[CD-TUZ01]] Direct companying and monocodamens grammo 2-6-6-202 10 49 05 05 29 [[CD-TUZ01]] Direct companying and monocodamens grammo 2-	•

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:

34

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 САС (навести на сертификат курсор мыши и нажать левую кнопку мыши) и нажать на кнопку «Удалить», аналогично выполнить для всех САС.

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.

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 САС.

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 APM 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 САС.

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 САС 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 САС 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 САС 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:

- 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.

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: <u>http://172.21.5.57:7777/in</u> Сервер получения: <u>http://172.21.5.57:7777/get</u>

🖳 Настройки точки обмена - kbr	and the state			X
Контроль	Настро	ойки обмена с CBK/TШ КБР		
Шлюз	Параметры подключения	Аутентификация		Â
СКАД Сигнатура	Протокол НТТР	•		
Служебный конверт	Маркер формата ХМLЕРД	•		
СВК/ТШ КБР	🖌 Останавливать передачу после	2 🚔 циклов	Резервные сервера	
Оповещения	Попыток отправки в цикле	2	Проверить соединение	
	Поштучный прием			E
Отменить	НПР Адрес отправки http://172.2	1.5.57:7777/in		
Применить	Адрес приема http://172.2	1.5.57:7777/get		
	Таймаут (с) 30 💌			
				Ŧ

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

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

Также необходимо указать резервные значения ІР-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.xxxxx (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.xxxxx (уточняется через Единую службу поддержки пользователей при начале работы по MQ)

Настройки точки обмена - f701	-		
		Настройки обмена с СВК/ТШ КБР	
Контроль			
Шлюз	Параметры подключ	ения Аутентификация	
СКАД Сигнатура	Протокол	IBM Websphere MQ	
Служебный конверт	Маркер формата	XMLEPD	
СВК/ТШ КБР	Останавливать перед	ачу после 1 👘 циклов	Резервные сервера
Оповещения	Попыток отправки в цик	ле 10 👘	Проверить соединение
	Поштучный прием		
Отменить	WMQ		
	Сервер	172.21.5.57	Порт 1414
Применить	Канал	KBR.SVRCONN	
	Менеджер	FRONTGATE	
	П Использовать прикла	адную аутентификацию	
	Отправка		
	Очередь	FROM.KBR	
	Менеджер ответов	FRONTGATE	
	Очередь ответов	INBOX.xxxxxxx	
	📃 Запрашивать квитани	ции о доставке ЭС в очередь на ТШ КБР	
	🔲 Запрашивать квитани	ции о получении ЭС из входящей очереди на ТШ КБР	
	Прием		
	Очередь	INBOX.xxxxxxx	

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

Конфигурация				
У Общая У Параметры С Реквизиты Учной ввод	Настройка взаимо, Параметры взаимодейст	действия с СВК/ТШ КБР вия с СВК		
 Служебный конверт СКАД Сигнатура УФЭБС S Swift I ISO Собств. форматы А Обособ. польз-ли Настройки СВК/ТШ КБР Транспорт ПВО и оповещения Участие в СПФС 	Параметры подключени Протокол Маркер формата Попыток отправки Поштучный прием WMQ Сервер Канал Менеджер Использовать прии	я Аутентификация IBM Websphere MQ ▼ XMLEPD ▼ 10 ▼ 10 ▼ 172.21.5.57 KBR.SVRCONN FRONTGATE стадную аутентификацию	Резервные сервера Проверить соединение Порт 1414	
	Отправка		1	
	Менеджер ответов Очередь ответов Запрашивать квит.	ГПОМ.ЛВП FRONTGATE INBOX.xxxxxxx анции о доставке ЭС в очередь на ТШ КБР анции о получении ЭС из входящей очеред	и на ТШ КБР	
	Прием Очередь	INBOX.xxxxxxx		
			Сохранить	Отмена

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: <u>http://172.21.1.57:7777/in</u> Сервер получения: <u>http://172.21.1.57:7777/get</u>

🖳 Настройки точки обмена - kbr	- the Fre	-			X
Контроль		Настройки о	обмена с СВК/ТШ КБР		
Шлюз	Параметры подклк	рчения А	утентификация		Â
СКАД Сигнатура	Протокол	HTTP	•		
Служебный конверт	Маркер формата	XMLEPD	•		
СВК/ТШ КБР	🖌 Останавливать пере	едачу после 2	🛓 циклов	Резервные сервера	
Оповещения	Попыток отправки в ци	кле 2	×	Проверить соединение	
	🔲 Поштучный прием				E
Отменить	нпр Адрес отправки	http://172.21.1.57:	7777/in		
Применить	Адрес приема	http://172.21.1.57:	7777/get		
	Таймаут (с)	30 ≑			
					Ŧ
				ALCED II	

Рис За. Настройки обмена СВК / ТШ КБР для ПК АРМ КБР- Н (Протокол НТТР, промышленный контур)

Конфигурация					
Общая Реквизиты Реквизиты Реквизиты Реквизиты Ручной ввод Служебный конверт СКАД Сигнатура U УФЭБС S Swift I ISO O Co6ств. форматы A Обособ. польз-ли Настройки СВК/ТШ КБР Транспорт ПВО и оповещения РУчастие в СПФС	 Настройка взаимоде Параметры взаимодействи Параметры подключения Протокол Н Маркер формата Х Попыток отправки 2 Поштучный прием НТТР Адрес отправки Адрес приема Таймаут (с) 	йствия с CBK/TI я с CBK Аутентификация TTP MLEPD	Ш КБР	Резервные сервера Проверить Эсединение	
				Сохранить	Отмена

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.xxxxx (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.xxxxx (уточняется через Единую службу поддержки пользователей при начале работы по MQ)

Настройки точки обмена - f701	- heles - E-mail	in the second	
Контроль		Настройки обмена с СВК/ТШ КБР	
Шлюз	Параметры подклю	мения Аутентификация	
СКАД Сигнатура	Протокол	IBM Websphere MQ	
Служебный конверт	Маркер формата	XMLEPD -	
СВК/ТШ КБР	🗌 Останавливать пере	дачу после 1 👘 циклов	Резервные сервера
Оповещения	Попыток отправки в ци	кле 10 🚖	Проверить соединение
	Поштучный прием WMQ		
Отменить	Сервер	172.21.1.57	Порт 1414
Применить	Канал	KBR.SVRCONN	
	Менеджер	FRONTGATE	
		iaan je og rennemaane	
	Очередь	FROM.KBR	
	Менеджер ответов	FRONTGATE	
	Очередь ответов	INBOX.xxxxxxx	
	 Запрашивать квитан Запрашивать квитан 	нции о доставке ЭС в очередь на ТШ КБР чими о получении ЭС из вхолящей очереди на ТШ КБР	
	Прием		
	Очередь	INBOX.xxxxxxx	

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

Параметры Рексизиты Рексизиты Сиди Сигнатура U УФЭСС S Switt I ISO O Coforts. форматы A Oбособ. польз-ли Hacтройки CBXTШ КБР Параметры взаимодействия с CBK Параметры водинодействия с CBK Параметры подключения <u>Аутентификация</u> Протокол IBM Websphere MQ • S Switt I ISO O Coforts. форматы A Oбособ. польз-ли Hacтройки CBXTШ КБР Польток отправки Польток отправки 10 Польток отправки 10	🔏 Общая	EV)			
Параметры взаимодействия с СВК Служебный конверт С Служебный конверт С Служебный конверт С САД Сигнатура U Y035C S Swit 1 ISO O Собств. форматы A Обсооб. польз-ли Ж Настройки СВК/ТШ КБР Польток отправки 10	🕎 Параметры	Настройка взаимо	действия с СВК/ТШ КБР		
Служебный конверт СКАД Сигнатура U УФЭБС S Switt I ISO O Coбств. форматы A Обсосб. польз-ли Taatenopr Taatenopr Taatenopr Taatenopr Taatenopr Vaactive в СПФС Vaactive в СПФС	— 🚛 Реквизиты — 🚳 Ручной ввод	Параметры взаимодейст	вия с СВК		
Канал КВR SVRCONN Менеджер FRONTGATE Использовать прикладную аутентификацию Отправка Очередь FROM КВR Менеджер ответов FRONTGATE Очередь ответов INBOX.xxxxxx Запрашивать квитанции о доставке ЭС в очередь на ТШ КБР Эапрашивать квитанции о получении ЭС из входящей очереди на ТШ КБР Прием	 Служебный конверт СКАД Сигнатура УФЭБС S Swift I ISO О Собств. форматы А Обособ. польз-ли Настройки СВК/ТШ КБР Транспорт ПВО и оповещения Участие в СПФС 	Параметры подключени Протокол Маркер формата Попыток отправки Поштучный прием WMQ Сервер	IR Ayтентификация IBM Websphere MQ ▼ XMLEPD ▼ 10 172.21.1.57	Резервные сервера Проверить соединение Порт 1414	
Менеджер FRONTGATE Использовать прикладную аутентификацию Отправка Очередь FROM.KBR Менеджер ответов FRONTGATE Очередь ответов FRONTGATE Очередь ответов INBOX.xxxxxx Запрашивать квитанции о доставке ЭС в очередь на ТШ КБР Запрашивать квитанции о получении ЭС из входящей очереди на ТШ КБР Прием Очередь		Канал		, [,	
Менеджер FRONTGATE Использовать прикладную аутентификацию Отправка Очередь FROM.KBR Менеджер ответов FRONTGATE Очередь ответов FRONTGATE Очередь ответов INBOX.xxxxxxx Запрашивать квитанции о доставке ЭС в очередь на ТШ КБР Запрашивать квитанции о получении ЭС из входящей очереди на ТШ КБР Прием Очередь Прием		M			
Очередь FROM.KBR Очередь FROM.KBR Менеджер ответов FRONTGATE Очередь ответов INBOX.xxxxxx Запрашивать квитанции о доставке ЭС в очередь на ТШ КБР Запрашивать квитанции о получении ЭС из входящей очереди на ТШ КБР Прием		Менеджер	FRONTGATE		
Отправка Очередь FROM.KBR Менеджер ответов FRONTGATE Очередь ответов INBOX.xxxxxx Запрашивать квитанции о доставке ЭС в очередь на ТШ КБР Запрашивать квитанции о получении ЭС из входящей очереди на ТШ КБР Прием		Ц использовать при	кладную аутентификацию		
Очередь FROM.KBR Менеджер ответов FRONTGATE Очередь ответов INBOX.xxxxxxxx Папрашивать квитанции о доставке ЭС в очередь на ТШ КБР Запрашивать квитанции о получении ЭС из входящей очереди на ТШ КБР Прием Очередь		Отправка			
Менеджер ответов FRONTGATE Очередь ответов INBOX.xxxxxxx Запрашивать квитанции о доставке ЭС в очередь на ТШ КБР Запрашивать квитанции о получении ЭС из входящей очереди на ТШ КБР Прием		Очередь	FROM.KBR		
Очередь ответов INBOX.xxxxxx Запрашивать квитанции о доставке ЭС в очередь на ТШ КБР Запрашивать квитанции о получении ЭС из входящей очереди на ТШ КБР Прием		Менеджер ответов	FRONTGATE		
 Запрашивать квитанции о доставке ЭС в очередь на ТШ КБР Запрашивать квитанции о получении ЭС из входящей очереди на ТШ КБР Прием 		Очередь ответов	INBOX.xxxxxxx		
Прием		 Запрашивать квита Запрашивать квита 	анции о доставке ЭС в очередь на ТШ КБР анции о получении ЭС из входящей очере	р ади на ТШ КБР	
		Прием			
INDOX.XXXXX		Очередь	INBOX.xxxxxxx]	

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.