Настройка защищенного удаленного подключения по протоколу IPSec (ГОСТ)

Для создания защищенных каналов связи в режиме шифрования/дешифрования в Dionis-NX должен быть инициализирован ДСЧ и создан КД.

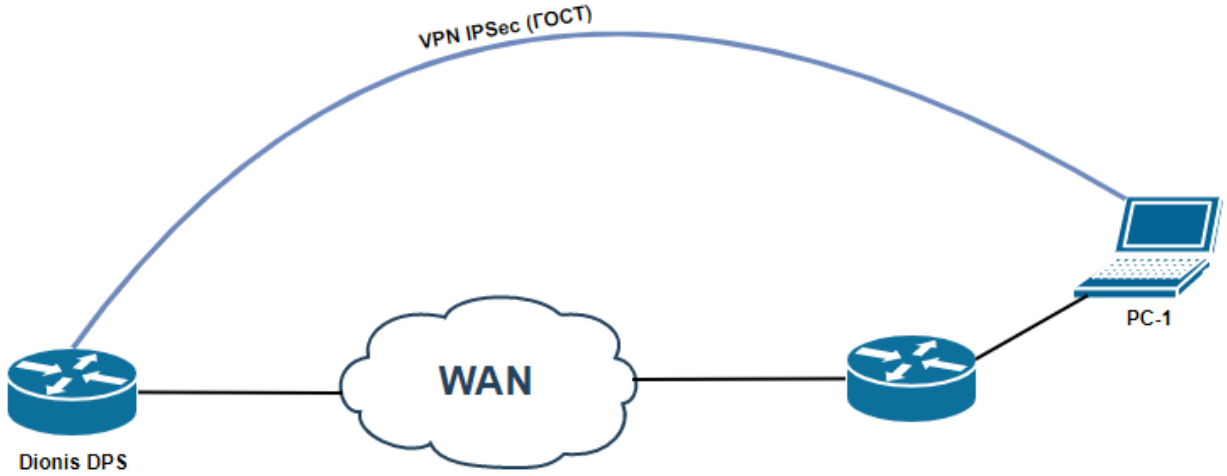

Рис. 1 Схема подключения

Согласно сценарию PC-1 находится за NAT

PC-1 подключается к Dionis DPS с помощью клиентского ПО Disec

Настройка Dionis DPS

Предварительная настройка сетевых интерфейсов

(config)# interface ethernet 0

(config-if-ethernet0)# ip address 83.220.32.68/24

(config-if-ethernet0)# enable

Для работы каналов связи с ассиметричными ключами шифрования необходимо импортировать в систему закрытый ключ, сертификат узла и корневой сертификат. Предположим, что ключ и сертификаты доставлены на внешнем флэш накопителе и находятся в его корне. /u1-256.p15 - закрытый ключ /root.cer – корневой сертификат /u1-256.cer – сертификат узла Dionis DPS /u2-256.cer – сертификат узла PC-1

 # crypto pki import key from flash0:/u1-256.p15

//загрузка контейнера с закрытым ключом

 # crypto pki import root ca cert from flash0:/root.cer

//загрузка корневого сертификата

 # crypto pki import cert from flash0:/u1-256.cer

//загрузка сертификата узла

Также необходимо загрузить сертификат удаленного пользователя:

 # crypto pki import cert from flash0:/u2-256.cer

И список удаленных сертификатов:

 # crypto pki import crl from flash0:/root.crl

Перейдем к настройке соединения:

(config)# crypto ike conn t1

(config-ike-conn-t1)# auth pubkey

(config-ike-conn-t1)# auto listen

(config-ike-conn-t1)# keying tries 1

(config-ike-conn-t1)# local cert u1-256.cer

//Указываем сертификат узла

(config-ike-conn-t1)# local ip 83.220.32.68/24

//Указываем белый адрес туннеля к которому будет подключаться удаленный пользователь

(config-ike-conn-t1)# local subnet from pool

(config-ike-conn-t1)# modeconfig dns 192.168.53.254 8.8.8.8

//Указываем какие DNS нужно назначить подключенному удаленному пользователю

(config-ike-conn-t1)# modeconfig mode pull

(config-ike-conn-t1)# no rekey

(config-ike-conn-t1)# pfs mode force

(config-ike-conn-t1)# ph1 transforms

(config-ike-conn-t1-ph1)# no strict

(config-ike-conn-t1)# ph2 transforms

(config-ike-conn-t1-ph2)# no strict

(config-ike-conn-t1)# remote id *

(config-ike-conn-t1)# remote ip *

(config-ike-conn-t1)# remote source ip mypool

(config-ike-conn-t1)# send cert ifasked

Перейдем к настройке адресов:

(config)# crypto ike pool mypool

(cfg-ike-pool-mypool)# pool 10.10.1.0/24

//Указываем список виртуальных адресов, который будет назначаться удаленному пользователю

(cfg-ike-pool-mypool)# local subnet 192.168.0.0/16

//Указываем локальную сеть к которой необходимо предоставить доступ удаленному пользователю

(config)# crypto ike config

(config-ike)# auth-log all

(config-ike)# crl cache

(config-ike)# debug control

(config-ike)# nat traversal

(config)# crypto ike enable

//запуск сервиса ike

На это настройка Dionis DPS закончилась.

Настройка ПО Disec на PC-1

Открываем программу Disec и выбираем вкладку «Подключения», и нажимаем на кнопку «Добавить»:

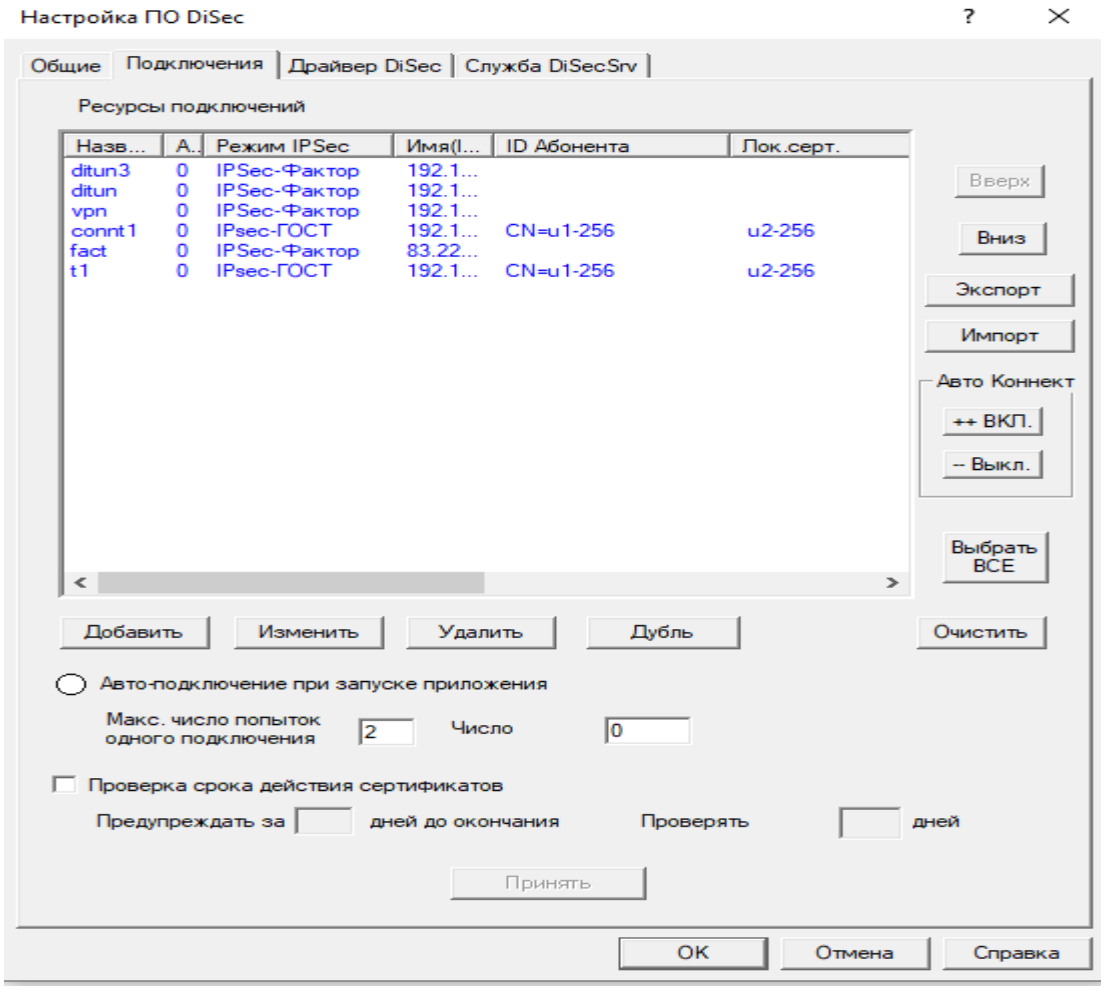

Рис.2 Добавление подключения

После этого откроется окно Общих настроек подключения

В строчке «Название подключения» необходимо ввести произвольное название соединения

В строчке «Адрес (IP) сервера VPN:» необходимо ввести адрес к которому будет подключаться удаленный клиент (нужно указывать адрес, который прописывался в local ip в настройках crypto ike conn tl)

Режим соединения необходимо выбрать IPSec-ГОСТ

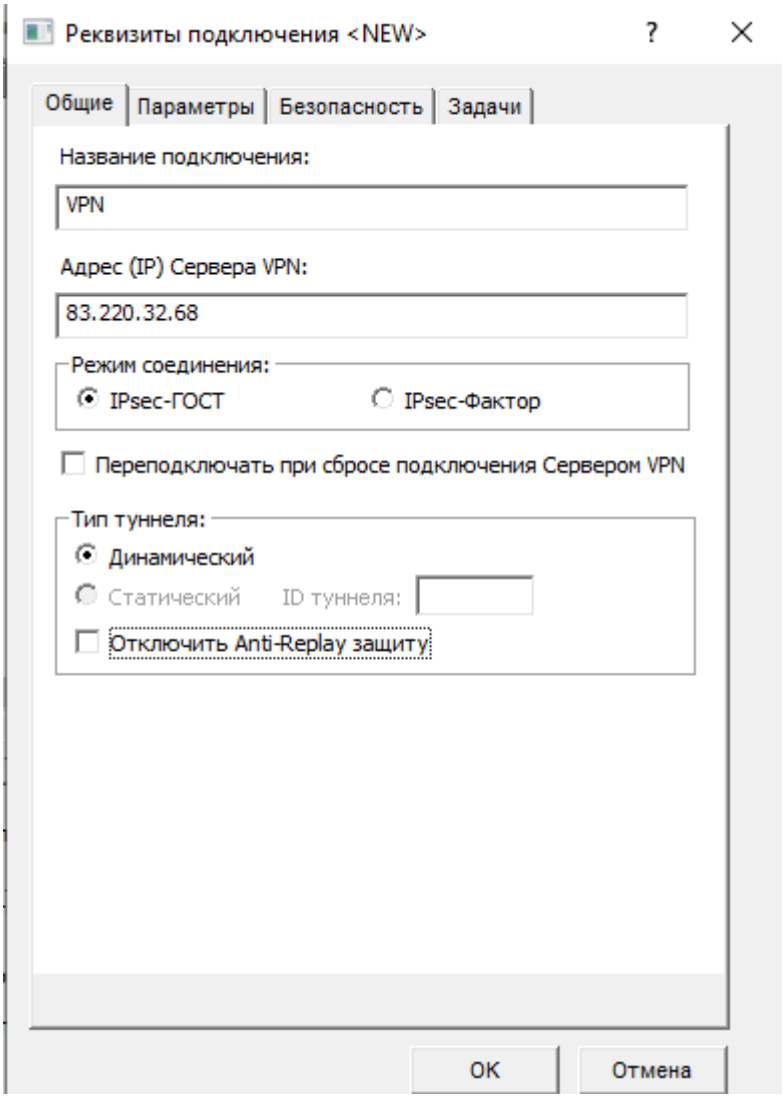

Рис. 3 Общие настройки

Далее необходимо перейти на следующую вкладку «Параметры»

В которой необходимо поставить галочку рядом с пунктом «Запросить IP-подсеть (MODE_CFG)»

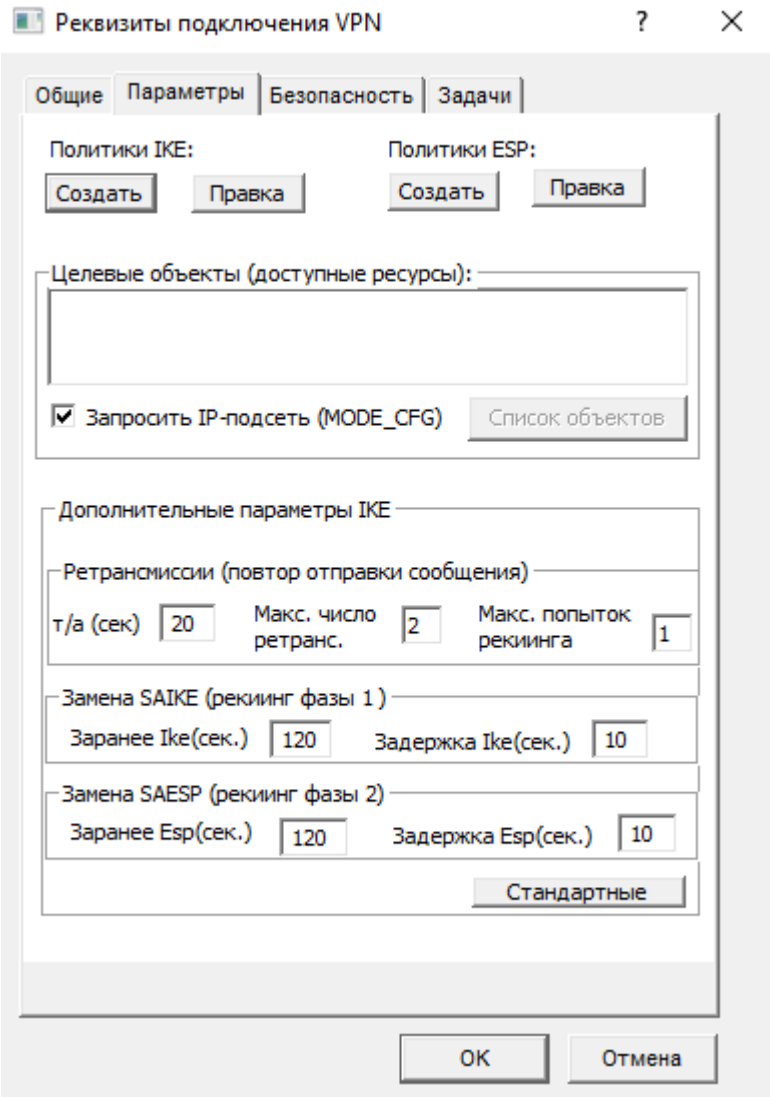

Рис. 4 Настройка параметров

Далее под строчкой «Политики IKE:» необходимо нажать «Правка»

И в столбце «Проверка жизнеспособности туннеля:» указать «Активный»

В «Действие при обнаружении нежизнеспособности» выбрать «Инициировать заново»

И нажать «ОК»

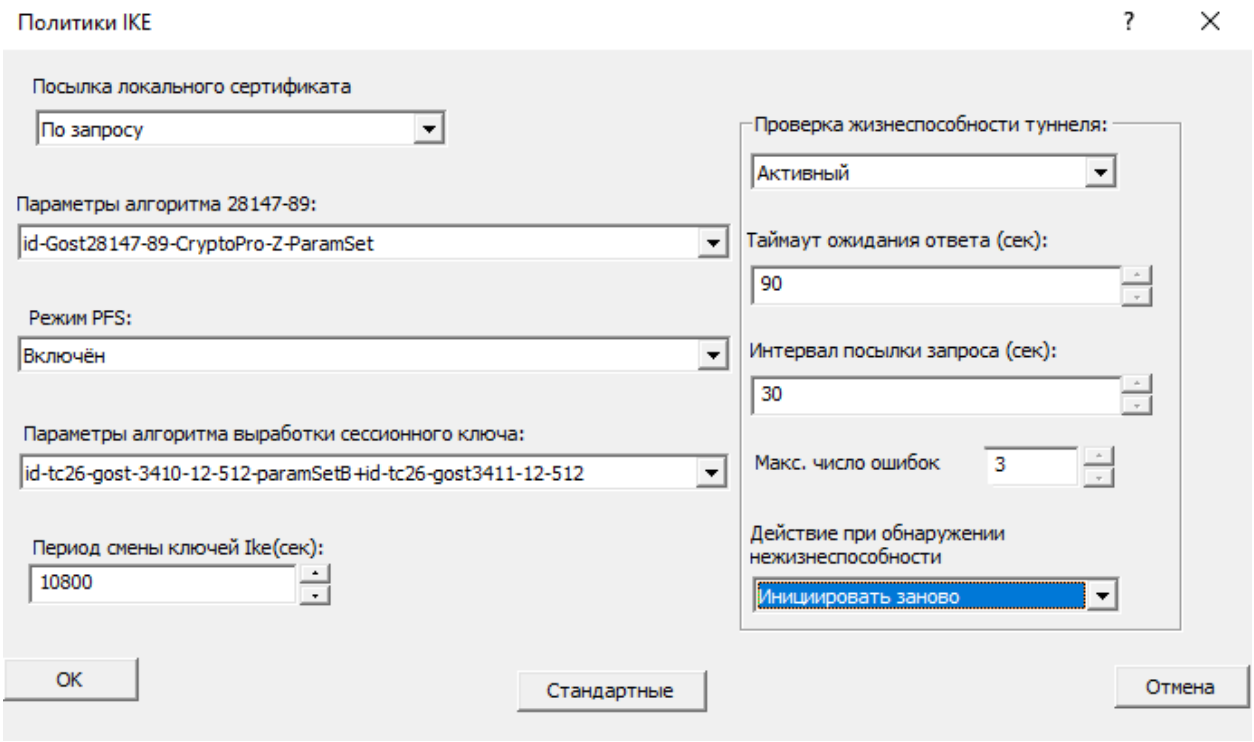

Рис. 5 Политики IKE

Дальше необходимо нажать на кнопку «Правка» под строчкой «Политик ESP», поставит галочку рядом с пунктом Запрос IP-адреса в защищенной сети сети (MODECONFIG) и нажать «ОК».

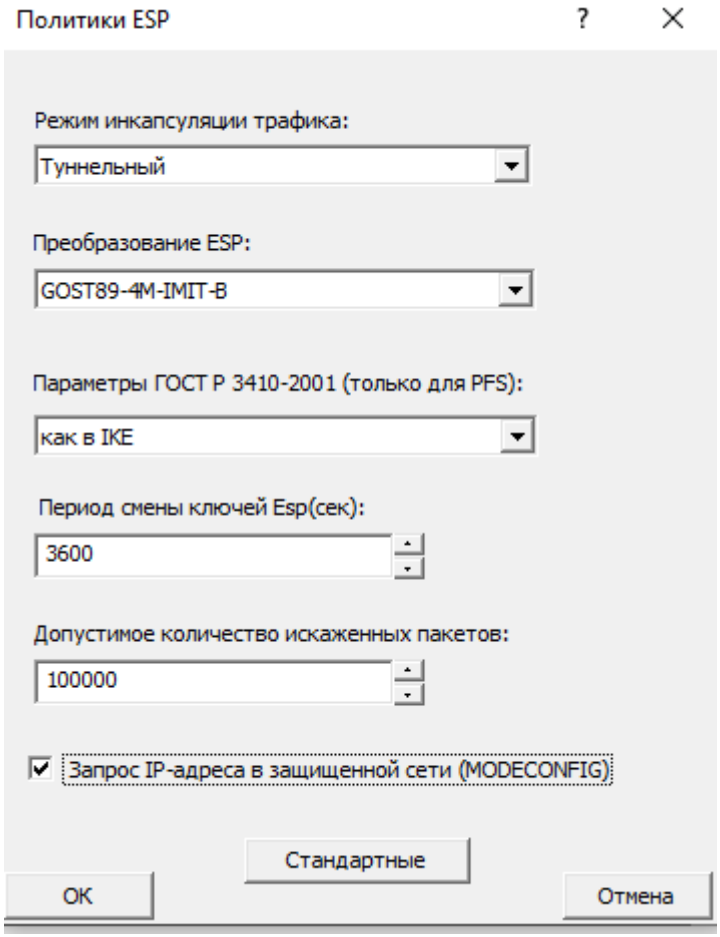

Рис. 6 Политики ESP

Далее переходим во вкладку «Безопасность» и в Настройках криптосистемы нажимаем «Настроить»

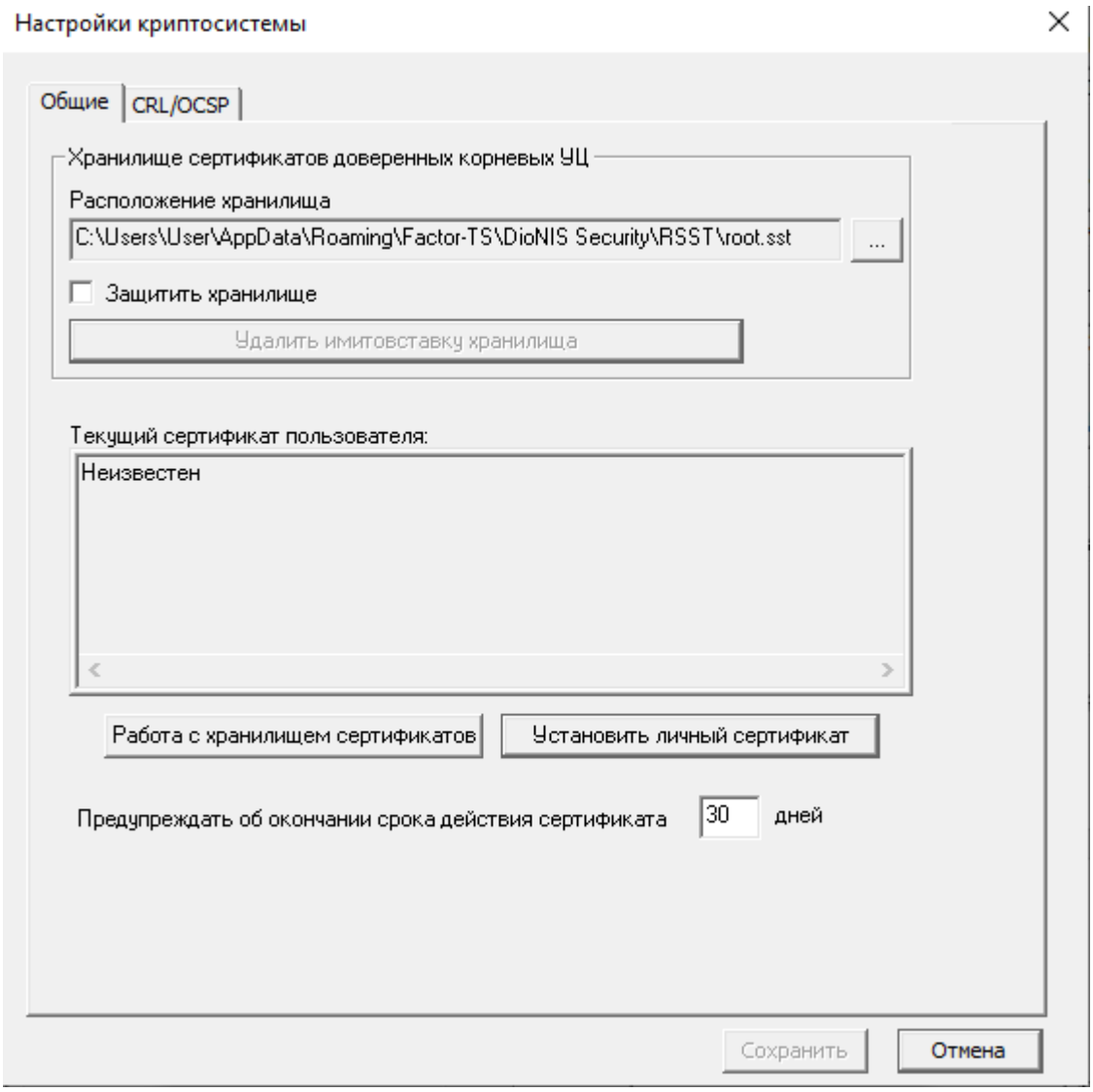

Рис. 7 Настройки криптосистемы

В графе «Текущий сертификат пользователя» необходимо нажать «Установить личный сертификат» и выбрать с носителя ключ и сертификат, который будет использоваться данным удаленным пользователем, в нашем случае это u2-256.p15 – ключевой контейнер и u2-256.cer – сертификат

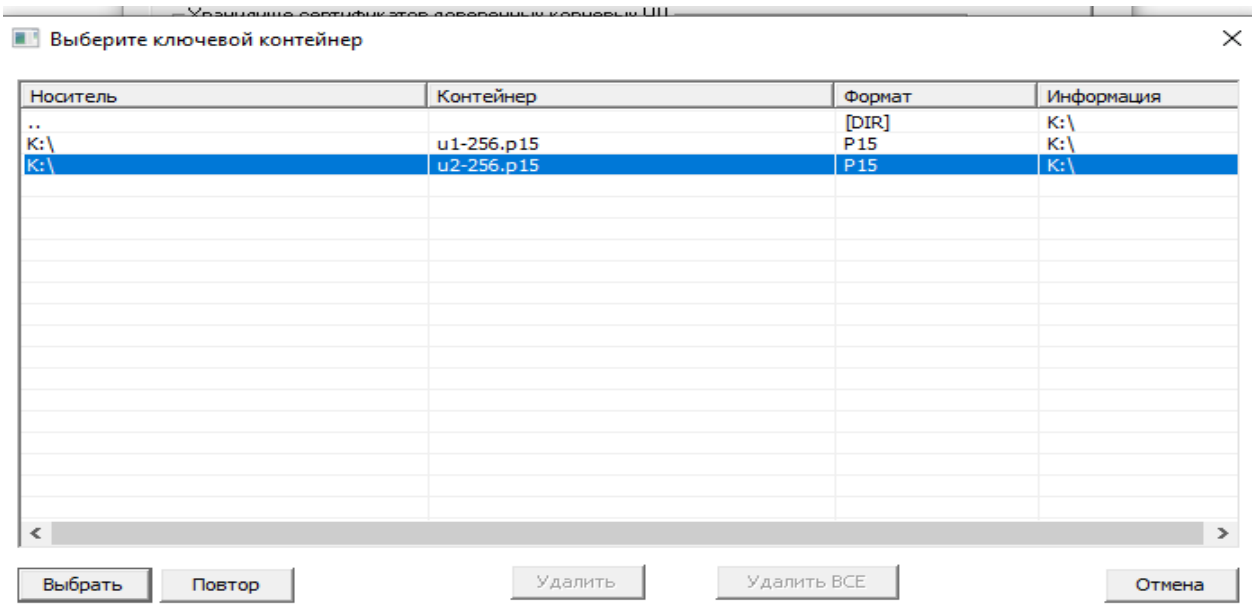

Рис. 8 Выбор ключевого контейнера

После добавления ключевого контейнера система подсказывает что необходимо добавить сертификат:

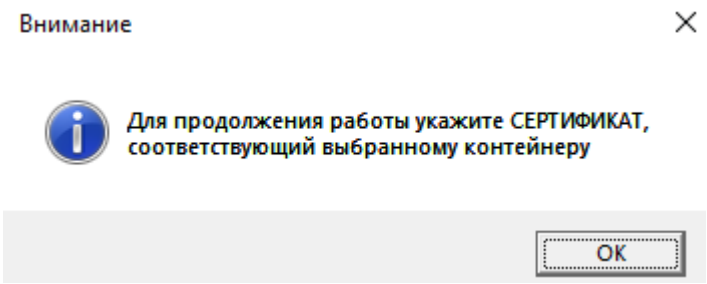

Рис. 9

После нажатия кнопки «ОК» система будет предлагать установить сертификаты найденные на съемном носителе

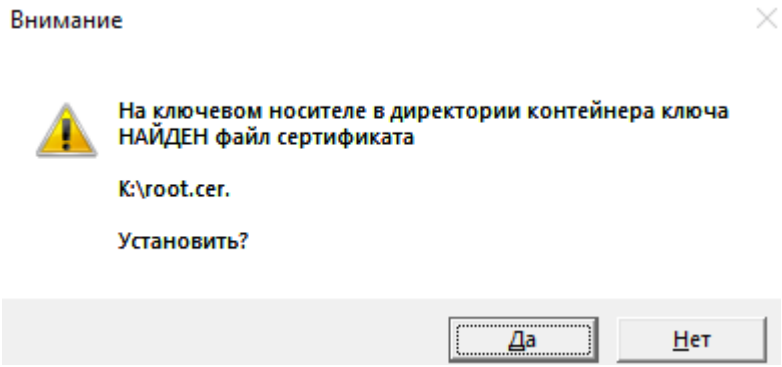

Рис. 10 предложение установки сертификата

На рис. 10 необходимо нажать «Нет» т.к. система предлагает установить корневой сертификат, а в данном случае необходим сертификат удаленного пользователя – u2-256.cer , необходимо нажимать «Нет» пока система перебором не укажет необходимый сертификат

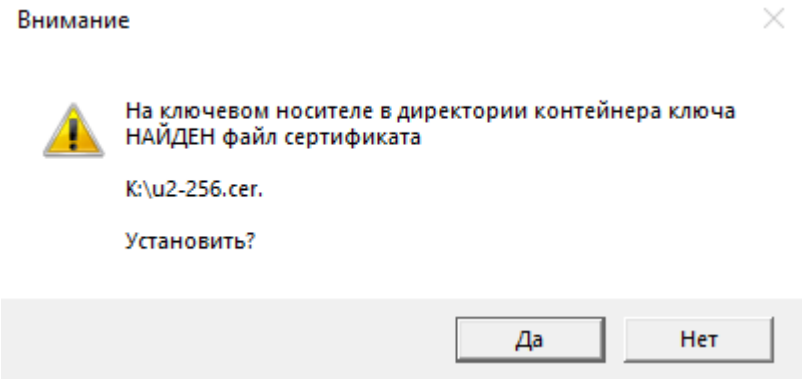

Рис. 11 Предложение установки сертификата удаленного пользователя

Когда появится сообщение о том что найден необходимый сертификат нажимаем «Да»

После этого откроется окно в котором добавляем указанный сертификат в ранее указанное хранилище ключа:

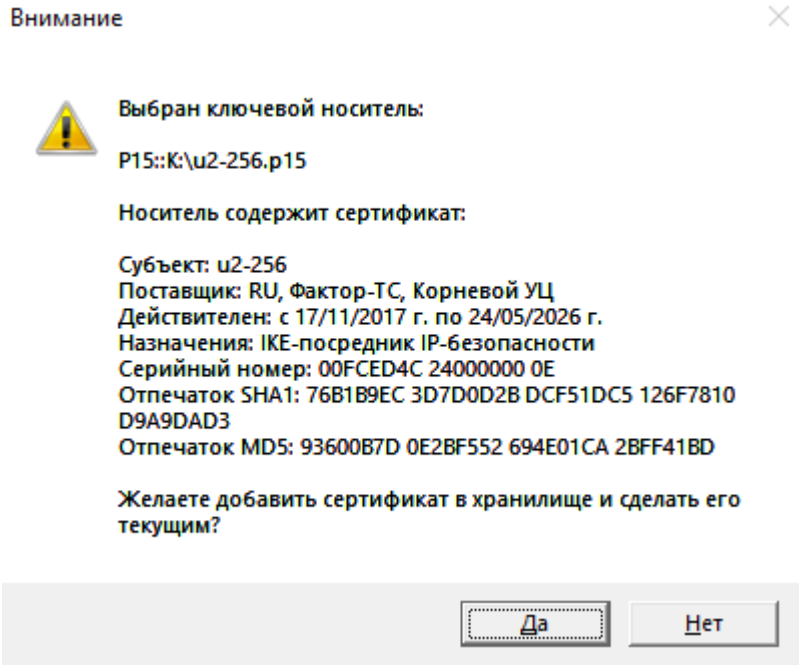

Рис. 12 Добавление сертификата в хранилище

На рис. 12 нажимаем «Да», если все сделано корректно то увидите следующее сообщение:

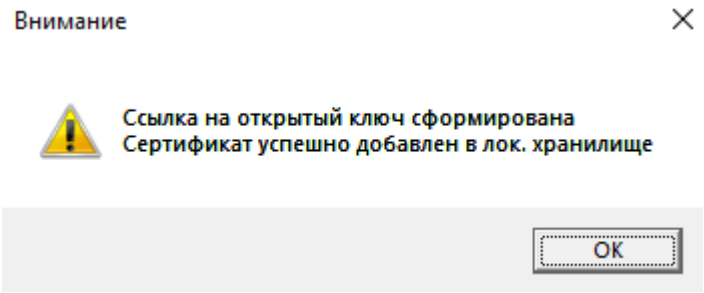

Рис. 13 Информационное окно

После нажатия клавиши «ОК» на рис. 13 система предложит установить корневой сертификат:

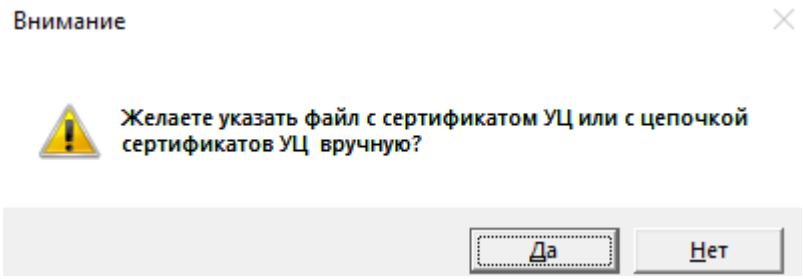

Рис. 14 предложение указать корневой сертификат

После нажатия кнопки «Да» выведется окно съемного носителя с сертификатами в котором необходимо указать корневой сертификат, в данном случае это файл с названием root.cer

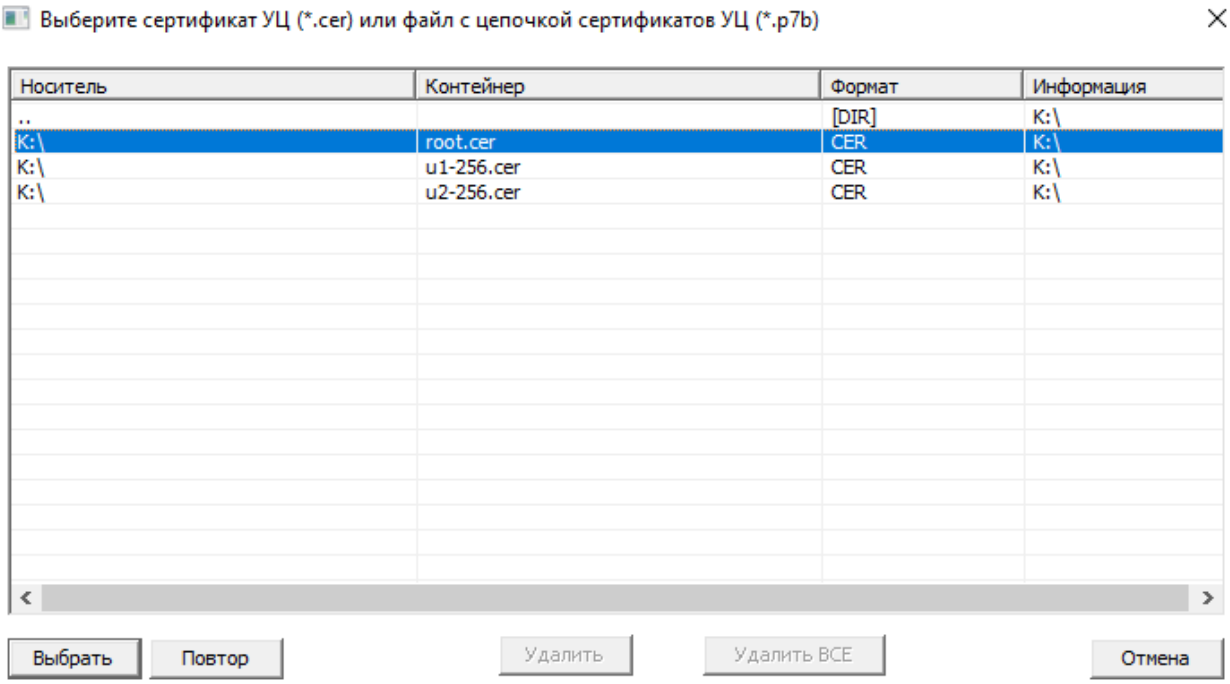

Рис. 15 Выбор корневого сертификата

После выбора на Рис. 15 корневого сертификата появится предложение Заменить предыдущий (если есть) и добавить выбранный в хранилище сертификатов

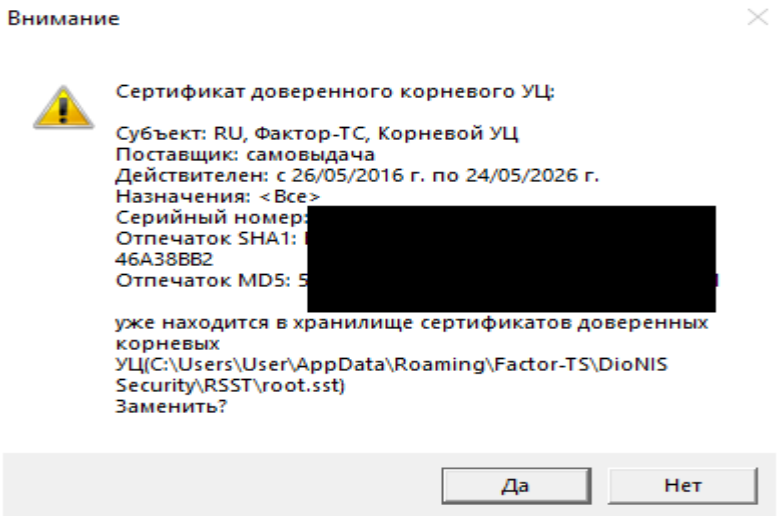

Рис. 16 Добавление корневого сертификата в хранилище сертификатов

Далее система увидит на носителе файл со списком отозванных сертификатов и предложит добавить его в хранилище, необходимо нажать «Да»

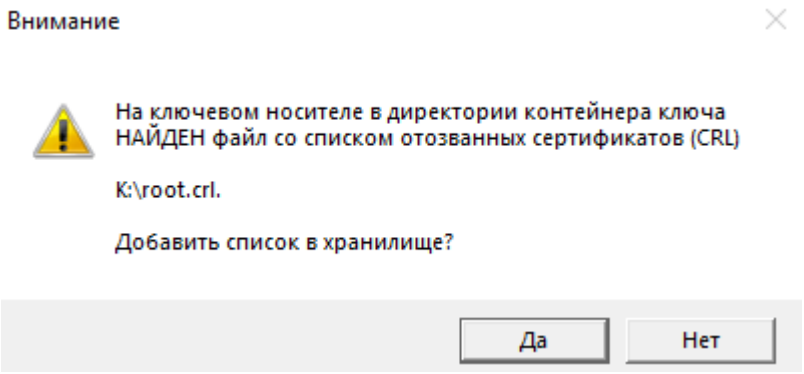

Рис. 17 Добавление списка отозванных сертификатов в хранилище

Если все было сделано корректно, то система выведет следующее окно:

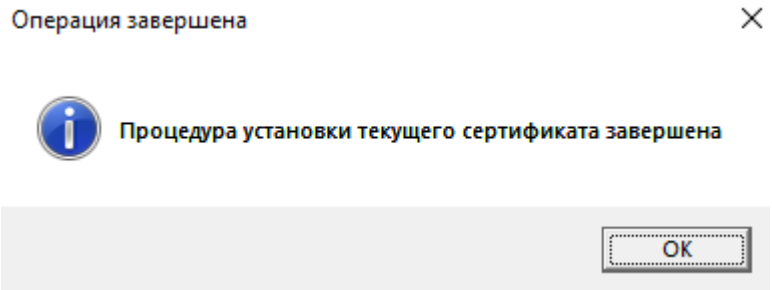

Рис. 18 Информационное окно о корректности установки текущего сертификата

После этого в окне «Настройки криптосистемы» Нажимаем кнопку «Сохранить»

Далее во вкладке «Безопасность», в Главе «Настройки запроса сертификата сервера VPN:» Выбираем «Не запрашивать сертификат сервера VPN» и нажимаем на кнопку «Выбрать сертификат сервера VPN…»

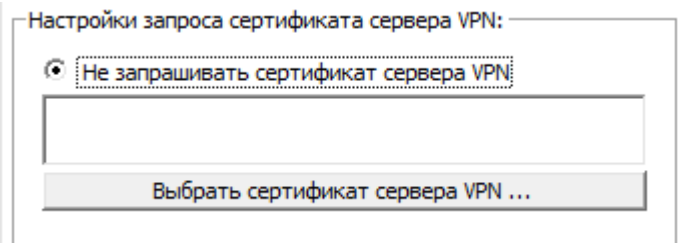

Рис. 19

После нажатия кнопки выбора сертификата сервера VPN системой будет предложено установить сертификат, в данном случае необходим сертификат с названием u1-256.cer

Система будет предлагать установить сертификаты которые найдет, если будет выбор сертификата не совпадающий с необходимым нужно нажать «Больше вариантов» в котором будет возможность Выбрать необходимый сертификат (см. рис. 20-21)

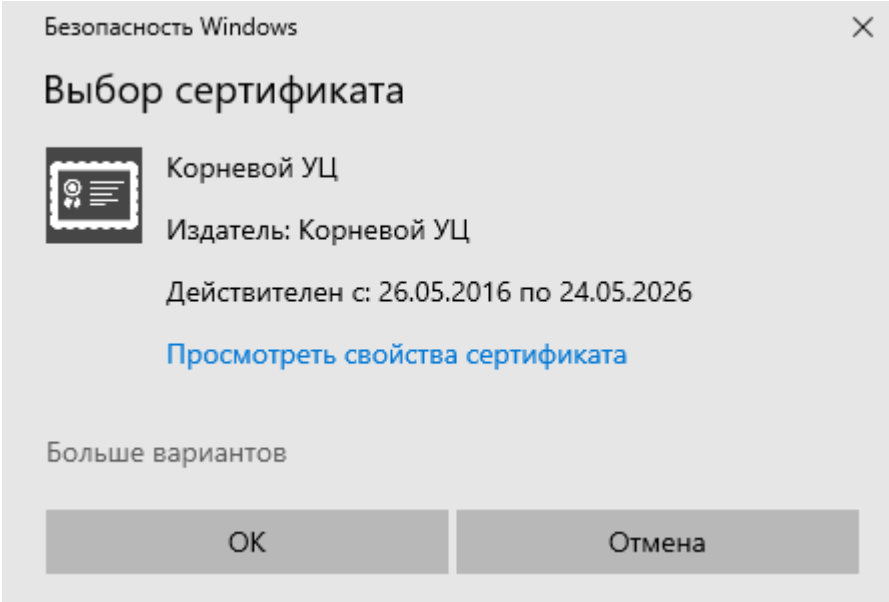

Рис. 20

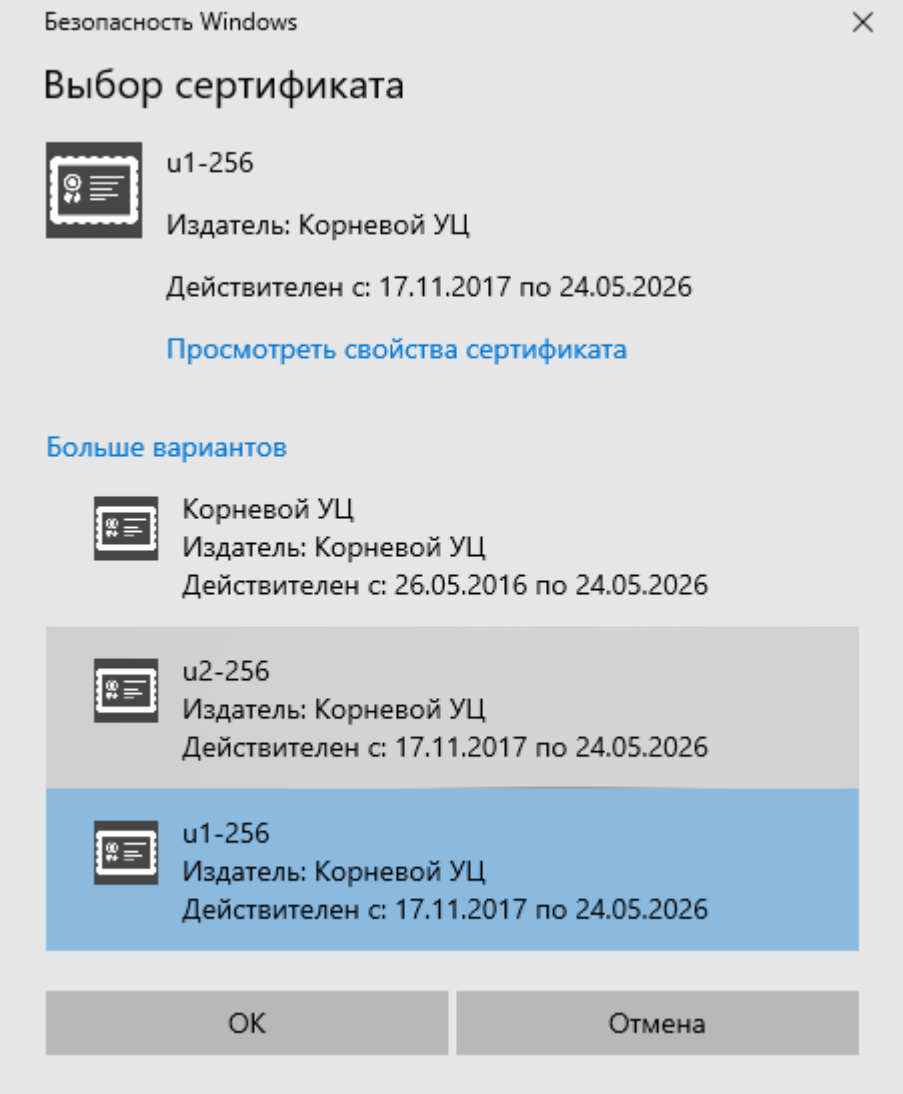

Рис. 21

После выбора необходимого сертификата нужно нажать «ОК» и вкладка «Безопасность» должно выглядеть следующим образом:

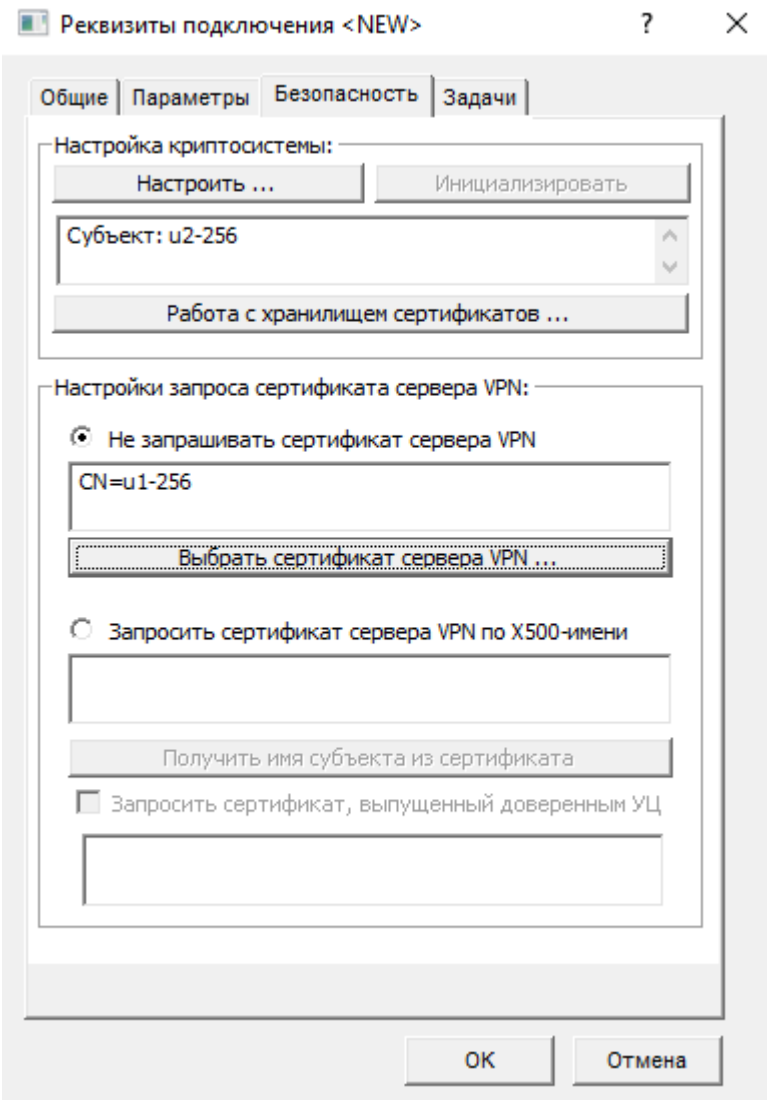

Рис. 22 Вкладка "Безопасность" после добавления сертификатов

После этого необходимо нажать внизу кнопку «ОК», вернемся в окно Настройки ПО Disec на вкладку «Подключения» в которой необходимо нажать кнопку «Принять» и после клавишу «ОК»

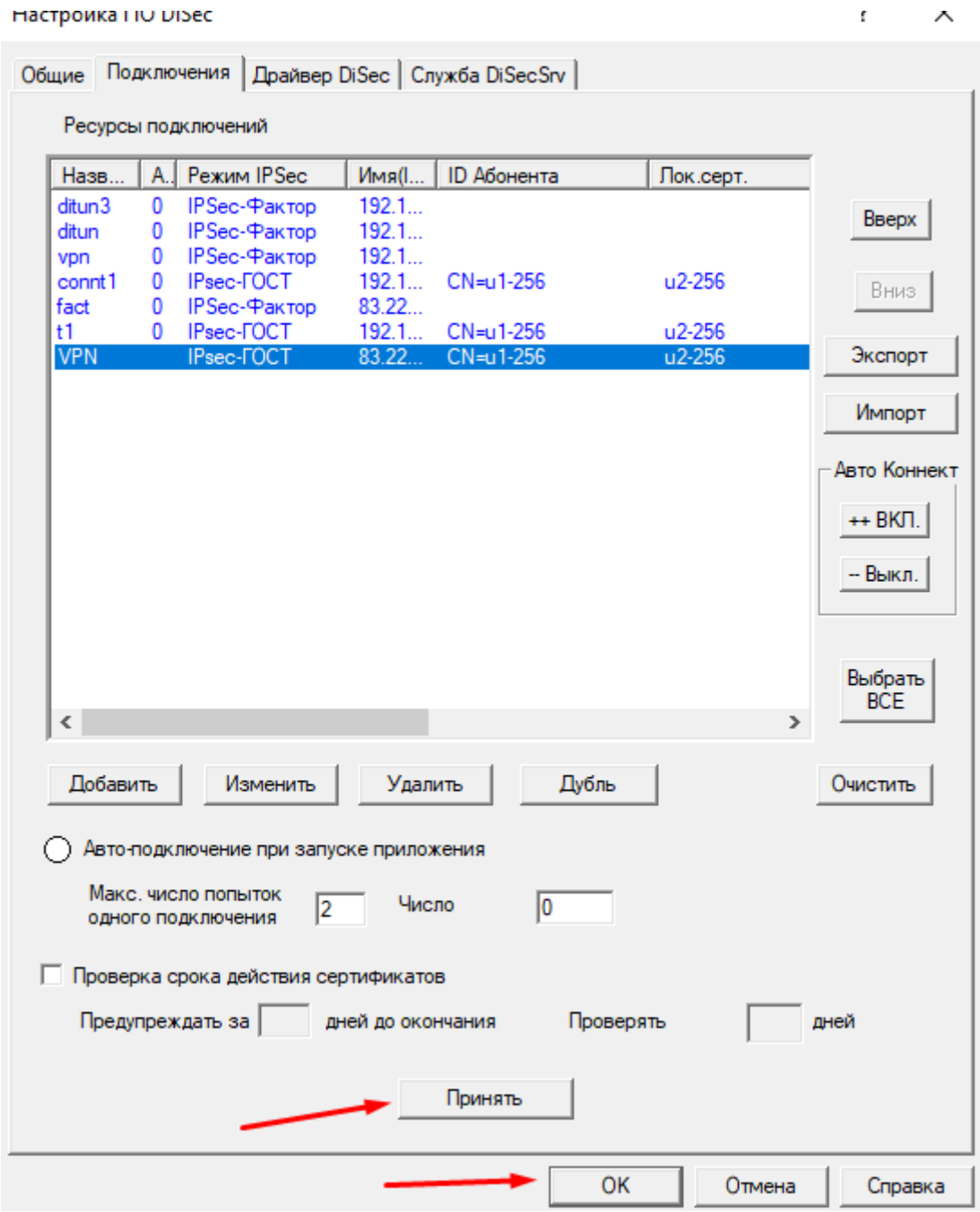

Рис. 23

На этом настройка ПО Disec закончена.