ООО «С-Терра СиЭсПи»
124498, г. Москва, Зеленоград, Георгиевский проспект,
дом 5, помещение I, комната 33
Телефон/Факс: +7 (499) 940 9061
Эл.почта: information@s-terra.com
Сайт: http://www.s-terra.com

Программный комплекс С-Терра Клиент. Версия 4.1

Руководство администратора

Приложение А

РЛКЕ.00009-02 90 03

16.02.2016

Содержание

1. Протоколирование событий 4
1.1 Настройка Syslog-клиента 4
1.1.1 Настройка в GUI 4
1.1.2 Настройка при использовании командной строки 4
1.2 Получение лога в ОС Windows 4
1.3 Утилиты log_mgr show и log_mgr set 5
1.4 Специальные лог-файлы 5
1.5 Журналы Windows 7
2. Список протоколируемых событий 8
2.1 Список ошибок протокола ISAKMP 52
2.1.1 Список выполняемых действий по протоколу ISAKMP 54
2.1.2 Список причин инициации IKE сессии 60
2.2 Ошибки криптографической подсистемы 61
3. Мониторинг 62
3.1 Выдача статистики 62
3.2 Трап-сообщения 75
4. Получение сертификата пользователя 78
4.1 Установка СКЗИ «КриптоПро CSP» 78
4.2 Настройка СКЗИ «КриптоПро CSP» 79
4.2.1 Настройка локального ключевого считывателя 79
4.2.2 Подключение внешних ключевых считывателей 79
4.2.3 Настройка внешнего ключевого считывателя и носителя информации 79
4.2.4 Инсталляция ключевого считывателя Реестр в «КриптоПро CSP» 80
4.2.5 Инсталляция внешнего считывателя и ключевого носителя информации в «КриптоПро CSP» 85
4.2.6 Настройка ДСЧ 87
4.3 Установка и настройка Удостоверяющего Центра. Создание СА сертификата 90
4.4 Создание сертификата пользователя с использованием СКЗИ «КриптоПро CSP 105
4.4.1 Создание ключевой пары и формирование запроса на сертификат пользователя 105
4.4.2 Экспортирование сертификата пользователя в файл 116

4.5 Создание сертификата пользователя с использованием криптобиблиотеки, разработанной компанией «С-Терра СиЭсПи» 122

4.6 Особенности генерации ключевой пары для режима защиты КС2, если для ССДЗ не поддерживается функциональность ДСЧ 127

5. Настройка нескольких сетевых интерфейсов 129

6. Работа «С-Терра Клиент» с продуктами третьих производителей 130

6.1 Работа с Брандмауэром Windows (ОС Windows 7) 130

6.2 Работа с антивирусом Outpost 132

1. Протоколирование событий

В Продукте протоколирование событий происходит по протоколу Syslog. Получатель лога может быть только один. При невозможности использовать Syslog и дополнительно сохранить некоторые сообщения, производится запись в специальные log-файлы или в журналы Windows раздел «Система».

1.1 Настройка Syslog-клиента

Настройка Syslog-клиента производится администратором при подготовке инсталляционного пакета пользователя. Администратор определяет IP-адрес хоста, на который будут посылаться сообщения о событиях, уровень важности сообщений, источник сообщений.

Все настройки syslog-клиента записываются в файл ***syslog.ini*** каталога продукта, который вручную не редактируется.

1.1.1 Настройка в GUI

В GUI административного пакета настройка syslog-клиента производится во вкладке **Settings**.

Подробнее см. «Руководство администатора», раздел «Графический интерфейс (GUI). Вкладка Settings».

1.1.2 Настройка при использовании командной строки

В утилите make_inst административного пакета для настройки syslog-клиента используются следующие опции:

-t <SYSLOG_server_IP> (`default: 127.0.0.1`) – IP-адрес компьютера, на который будут посылаться сообщения о событиях

-s {emerg|alert|crit|err|warning***|notice|info|debug}*** `(default: notice)` – общий уровень для всех протоколируемых событий

-y <log_facility> `(default: log_local7)` – источник сообщений.

-a /l `C:\Client\install_log_file.txt` – протоколирование событий при инсталляции S-Terra Client в указанный файл.

Подробнее см. «Руководство администатора», раздел «Утилита make_inst».

1.2 Получение лога в ОС Windows

Для получения лога в ОС Windows можно использовать Продукт Kiwi Syslog Daemon (http://www.kiwisyslog.com), Tri Action Syslog Daemon и др.

1.3 Утилиты log_mgr show и log_mgr set

С целью фильтрации протоколируемых сообщений тем или иным образом устанавливается общий протоколируемый уровень важности LogLevel (или уровень важности по умолчанию). Также, каждое событие имеет свой фиксированный уровень важности Severity, указанный в файле `C:\Program Files\S-Terra Client\s_log.ini` (Таблица 3). Событие, которому соответствует фиксированный уровень важности X, протоколируется только в том случае, если при его совершении общий уровень важности LogLevel не выше данного фиксированного уровня X.

События можно объединять в группы и назначать новый групповой уровень протоколирования.

В состав продукта S-Terra Client входит утилиты:

- `log_mgr show`, которая позволяет просматривать настройки syslog-клиента и общий уровень лога для всех сообщений.
- `log_mgr set`, которая предназначена для изменения настройки уровня протоколирования всех событий, не включенных в группы, уровня протоколирования группы событий, настройки syslog-клиента, задания группы событий и др.

Эти утилиты описаны в «Руководстве пользователя», в разделе «Специализированные команды».

1.4 Специальные лог-файлы

В специальные лог-файлы, указанные в таблице, производится дополнительно протоколирование некоторых нештатных ситуаций работы Продукта. В эти файлы записывается информация, которая может помочь решить возникшую проблему.

Таблица 1

Имя файла	Путь к файлу	Содержание файла
cspvpn_verify_err.log	Каталог установки продукта (по умолчанию – S-Terra Client)	Ошибки утилиты cspvpn_verify для проверки целостности неизменяемых и исполняемых файлов.
cp.log	Каталог **%TMP%** где %TMP% - переменная среды пользователя	Сообщения криптоподсистемы уровня приложений
failh.log	Каталог **%TMP%** где %TMP% - переменная среды пользователя	Аварийные события, не связанные с работой vpnsvc и lsp_show
error.log	Каталог **%TMP%\lsp_mgr** где %TMP% – переменная среды пользователя	Аварийные события, связанные с работой утилиты lsp_mgr
error.log	Каталог **%TMP%\vpnsvc** где %TMP% – системная переменная (по умолчанию **TMP=C:\WINDOWS\TEMP**)	Аварийные события, связанные с работой vpnsvc

error.log	Каталог **%TMP%\vpnlogsvc** где %TMP% – системная переменная (по умолчанию **TMP=C:\WINDOWS\TEMP**)	Аварийные события, связанные с работой vpnlogsvc
SetupAPI.log	**%Windir%**	Сообщения инсталлятора ОС Windows XP
SetupAPI.app.log SetupAPI.dev.log	**%Windir%\Inf**	Сообщения инсталлятора ОС Windows Vista, ОС Windows 7
Имя и путь к файлу указываются администратором в дополнительных параметрах запуска WinInstaller: во вкладке Settings в GUI в опции –a утилиты make_inst.		Сообщения инсталлятора ОС Windows

Например,

1. при неудачном старте vpn-демона (vpnsvc или vpnlogsvc) в файл error.log записывается сообщение следующего вида:

   ```
   initialization of module '%{1}s' failed with code %{2}x
   ```

   где

   `'%{1}s'` – имя модуля при инициализации которого произошла ошибка

   `'%{2}s'` – код ошибки при инициализации модуля

   Пример

   ```
   1313076721 initialization of module "hashes checker" failed with code 0xff
   ```

   Модуль `hashes checker` появляется при проверке целостности неизменяемых файлов продукта при использовании утилиты `cspvpn_verify`

2. при форсированном завершении работы сервиса vpnsvc в файл error.log записывается последнее осмысленное сообщение вида:

   ```
   vpnsvc: forceServiceFini
   ```

3. при форсированном завершении работы сервиса vpnlogsvc в его файл error.log записывается последнее осмысленное сообщение вида:

   ```
   vpnlogsvc: forceServiceFini
   ```

4. при нарушении контроля целостности ini-файла или базы данных выдается сообщение вида:

   ```
   '%{1}s' Error: the integrity check of the '%{2}s' failed
   ```

   или

   ```
   '%{1}s' FatalError: the integrity check of the '%{2}s' failed
   ```

   где

   `'%{1}s'` – имя модуля (“s_filestore” или “s_ini”), обнаружившего нарушение

   `'%{2}s'` – указание на проблемный файл

   ключ `Error` означает, что из данного модуля будут выданы дополнительные сообщения, и последним будет сообщение о форсированном завершении сервиса

   ключ `FatalError` означает, что это последнее осмысленное сообщение данного модуля (vpnsvc или vpnlogsvc).

Пример файла "%WINDIR%\temp\vpnsvc\error.log" (записан из сервиса vpnsvc):

```
1305822135 s_filestore Error: the integrity check of the body-
file "./db/lsps\00000002" of the DSC-file "00000002.dsc" failed

1305822135 vpnsvc: forceServiceFini
```

1.5 Журналы Windows

Для ОС Windows Vista и более новых версий ОС Windows в журнал «Система» протоколируются сообщения от источника st_ipsm. Список возможных сообщений приведен в Таблица 2.

Таблица 2

Driver loaded	Драйвер-перехватчик st_ipsm.sys загружен
Driver unloaded	Драйвер-перехватчик st_ipsm.sys выгружен
Filter attach to adapter %2 failed	Не удалось присоединится к сетевому интерфейсу <имя сетевого интерфейса>
NdisFRegisterFilterDriver failed	Не удалось зарегистрировать драйвер-перехватчик. Загрузка драйвера невозможна
FilterRegisterDevice failed	Не удалось зарегестрировать виртуальное устройство. Загрузка драйвера невозможна
Can't get MTU of adapter %2. Using 1500	Не удалось определить MTU сетевого интерфейса <имя сетевого интерфейса>

2. Список протоколируемых событий

Строка протоколируемого события формируется из соответствующего описания сообщения, задаваемого во внешнем текстовом файле s_log.ini, который располагается в каталоге продукта (по умолчанию – C:\Program Files\S-Terra Client). Каждому протоколируемому событию присвоен фиксированный идентификатор (***MSG ID***), текстовое представление, уровень важности сообщения, шаблон сообщения.

Уровни важности (Severity) протоколируемых событий соответствуют уровням Severity для протокола Syslog: EMERG, ALERT, CRIT, ERR, WARNING, NOTICE, INFO, DEBUG.

Список протоколируемых событий и сообщений по ним представлен в Таблица 3. Ведется также протоколирование ошибок криптографической подсистемы, представленных в Таблица 7. Эти ошибки доводятся до сведения пользователя также через Syslog, используя источник сообщений (Facility) `kern`.

Таблица 3

MSG ID	Текстовое представление	Раздел	Уровень	Шаблон сообщения	Описание события
03090001	MSG_ID_PRODUCT_START	<MAIN_APPLICATION>	NOTICE	Service started, version %{1}s	Старт сервиса
03090002	MSG_ID_PRODUCT_STOP	<MAIN_APPLICATION>	NOTICE	Service stopped	Остановка сервиса
03090003	MSG_ID_LOG_SUSPEND_SYSTEM	<MAIN_APPLICATION>	INFO	OS is going to the Suspend or Hibernation mode	Операционная Система переходит в режим сна или гибернации (Suspend or Hibernation)
03090004	MSG_ID_LOG_RESUME_SYSTEM	<MAIN_APPLICATION>	INFO	OS resumed from the Suspend or Hibernation mode %{1}u sec ago	Операционная Система вышла из режима сна или гибернации (Suspend or Hibernation) %(1}s - Время, потраченное сервисом на ожидание восстановления доступности сетевых интерфейсов
03090202	MSG_ID_LOGSRV_SET_SETTINGS_FAIL	<MAIN_APPLICATION>	WARNING	Failed to set VPN log service settings	Неудача изменения параметров установок LOG-сервиса. Возможно, серис не запущен.

03090203	MSG_ID_LOGSRV_START	<MAIN_APPLICATION>	INFO	VPN log service started, version %{1}s	Старт LOG-сервиса
03090204	MSG_ID_LOGSRV_STOP	<MAIN_APPLICATION>	INFO	VPN log service stopped	Остановка LOG-сервиса
005B0001	MSG_ID_EVENT_MGR_PROFILER_QUEUE	Event Manager	INFO	Event Manager profiler: waiting time of task queue is %{1}s sec, queue length is %{2}s tasks	сообщение профайлера менеджера событий сервиса о статистике по очереди событий
005B0002	MSG_ID_EVENT_MGR_PROFILER_TASK	Event Manager	WARNING	Event Manager profiler: task time is %{1}s sec (src=%{2}s dst=%{3}s idx=%{4}s proc=%{5}s)	сообщение профайлера менеджера событий сервиса о чрезмерно долгом времени обработки события
08200001	MSG_ID_ARPM_ERR_WRITE_PARP_FILE	<ARPM>	WARNING	Could not write ProxyARP table in file "%{1}s"	ошибка записи служебного файла протоколирования изменений таблицы Proxy ARP
08200002	MSG_ID_ARPM_ERR_READ_PARP_FILE	<ARPM>	WARNING	Could not read ProxyARP table from file "%{1}s"	ошибка чтения служебного файла протоколирования изменений таблицы Proxy ARP
08200003	MSG_ID_ARPM_IP_ADDED_TO_SYSTEM_PARP	<ARPM>	DEBUG	IP %{1}s%[added to ProxyARP table(s) of "%{10}s";%]%[was not added to ProxyARP table(s) of "%{11}s";%]	Добавление или обновление IP адреса в Proxy ARP таблицы сетевых интерфейсов %(1}s - добавляемый IP адрес %{10}s - список интерфейсов, к которым IP добавлен успешно %{11}s - список интерфейсов, к которым следовало добавить IP, но не удалось

08200004	MSG_ID_ARPM_IP_DELETED_FROM_SYSTEM_PARP	<ARPM>	DEBUG	IP %{1}s%[deleted from ProxyARP table(s) of "%{10}s";%]%[was not deleted from ProxyARP table(s) of "%{11}s";%]	Удаление IP адреса из Proxy ARP таблиц сетевых интерфейсов %(1}s - удаляемый IP адрес %{10}s - список интерфейсов, из которым IP удален успешно %{11}s - список интерфейсов, из которых IP удалить не удалось. Возможно, он был удален ранее
08200005	MSG_ID_ARPM_REFRESH_SYSTEM_PARP	<ARPM>	INFO	In the ProxyARP table(s) of "%{11}s" interface(s) %{2}u IP(s) was(were) not refreshed	Пересоздание Proxy ARP таблиц сетевых интерфейсов. Может происходить при перезагрузке LSP %{11}s - список интерфейсов, к которым следовало добавить IP, но не удалось
00014001	MSG_ID_SNMP_TRAP_RECEIVER_ADD_FAILED	Statistics & SNMP	WARNING	[SNMP] failed to configure SNMP trap receiver %{1}s%[:%{2}u%], community "%{3}s"%[, interface "%{4}s"%]%[, local address %{5}s%]	Не удалось добавить получателя SNMP traps (структура LSP TrapReceiver) %{1} - IP-адрес получателя %{2} - порт получателя %{3} - SNMP trap community %{4} - логическое имя сетевого интерфейса %{5} - локальный IP-адрес
00014002	MSG_ID_SNMP_POLLING_SETUP_LOCAL_ADDR_FAILED	Statistics & SNMP	WARNING	[SNMP] failed to configure SNMP polling agent on address(es) %{1}s%[(port %{2}u)%]	Не удалось настроить прием SNMP-запросов в соответствии со структурой LSP SNMPPollSettings на определенном локальном IP-адресе {1} - локальный IP-адрес {2} - локальный порт

--------	--------	--------	--------	--------	Общие параметры для сообщений: %{8}s IP-адрес партнёра по IKE обмену. %{9}u IP-порт партнёра по IKE обмену. Если не указан, то порт стандартный (500) %{10}s Значение IKE идентификатора для аутентификации партнёра. %{15}u Порог ограничения ресурса %{20}s Причина возникновения события %{32}s Идентификатор сессии IKE обмена. Формат - "<n:m>", где n - номер защищающего ISAKMP соединения, m - номер обмена, защищаемого данным ISAKMP соединением %{40}u Номер ISAKMP соединения
00101011	MSG_ID_LP_ISAKMP_PROPOSALS_SEND	LP	DEBUG	%[%{32}s %]Sending ISAKMP proposals:	Партнёру отсылаются наборы криптопараметров устанавливаемого ISAKMP соединения
00101012	MSG_ID_LP_ISAKMP_PROPOSALS_RECV	LP	DEBUG	%[%{32}s %]Received ISAKMP proposals:	От партнёра получены наборы криптопараметров устанавливаемого ISAKMP соединения
00101013	MSG_ID_LP_ISAKMP_TRANSFORM	LP	DEBUG	%[%{32}s %] Transform #%{1}u: %{2}s	Описание варианта криптопараметров устанавливаемого ISAKMP соединения
00101021	MSG_ID_LP_IPSEC_PROPOSALS_SEND	LP	DEBUG	%[%{32}s %]Sending IPSec proposals:	Партнёру отсылаются наборы криптопараметров устанавливаемого IPSec соединения
00101022	MSG_ID_LP_IPSEC_PROPOSALS_RECV	LP	DEBUG	%[%{32}s %]Received IPSec proposals:	От партнёра получены варианты наборов криптопараметров для устанавливаемого IPSec соединения
00101023	MSG_ID_LP_IPSEC_PROPOSAL	LP	DEBUG	%[%{32}s %] Proposal #%{1}u:	Описание варианта набора криптопараметров устанавливаемого IPSec соединения

00101024	MSG_ID_LP_IPSEC_PROTO	LP	DEBUG	%[%{32}s %] Protocol %{1}s:	Описание вариантов криптопараметров для указанного протокола
00101025	MSG_ID_LP_IPSEC_TRANSFORM	LP	DEBUG	%[%{32}s %] Transform #%{1}u: %{2}s	Описание варианта криптопараметров устанавливаемого IPSec соединения
00101031	MSG_ID_LP_CHECK_PROPOSAL	LP	DEBUG	%[%{32}s %]Checking %[Proposal #%{1}u, Protocol %{2}s, %]Transform #%{3}u for Rule "%{4}s", %[Proposal #%{5}u, Protocol %{6}s, %]Transform #%{7}u: %{8}s %{9}s	Проверка каждого из присланных вариантов наборов криптопараметров на соответствие локальному IKE/IPSec правилу. %{1}u номер присланного варианта набора криптопараметров (для IPSec) %{2}s протокол присланного набора криптопараметров (для IPSec) - ESP либо AH %{3}u номер присланного варианта криптопараметров %{4}s имя локального IKE/IPSec правила %{5}u номер локального варианта набора криптопараметров (для IPSec) %{6}s протокол локального набора криптопараметров (для IPSec) - ESP либо AH %{7}u номер локального варианта криптопараметров %{8}s %{9}s результат проверки
00101032	MSG_ID_LP_CHECK_PROPOSAL_SHORT	LP	DEBUG	%[%{32}s %]Checking proposal #%{1}u for Rule "%{4}s", Proposal #%{5}u: %{8}s %{9}s	Проверка набора криптопараметров на соответствие локальному IPSec правилу. %{1}u номер присланного варианта набора криптопараметров %{4}s имя локального IKE правила %{5}u номер локального варианта набора криптопараметров %{8}s %{9}s результат проверки
00101034	MSG_ID_LP_IKE_RULE_NOT_FOUND	LP	INFO	%[%{32}s %]Unable to choose authentication rule	Невозможно подобрать IKE правило для аутентификации партнёра

00101035	MSG_ID_LP_CHOOSE_IKE_RULE_BY_IP	LP	INFO	%[%{32}s %]Unable to find IKE rule by remote id. Using IP-address as partner's id.	Для присланного ID первой фазы IKE не найдено подходящего IKE правила. В качестве идентификатора будет использован IP-адрес партнёра.
00101036	MSG_ID_LP_USE_PRESHARED_KEY	LP	DEBUG	%[%{32}s %]Using preshared key "%{1}s"	Выбран предопределённый ключ для аутентификации %{1}s идентификатор ключа
00101037	MSG_ID_LP_KEY_ABSENT	LP	WARNING	%[%{32}s %]Preshared key "%{1}s" not found, peer %{8}s%[:%{9}u%]%[, id "%{10}s"%]	Не найден предопределённый ключ для аутентификации %{1}u идентификатор ключа
00101038	MSG_ID_LP_IP_DOESNT_MATCH	LP	INFO	%[%{32}s %]IKERule "%{1}s": IP address is not in %{2}s list, peer %{8}s%[:%{9}u%]%[, id "%{10}s"%]	IKE правило не подходит из-за того, что IP адрес отсутствует в списке разрешенных (IKEPeerIPFilter или IKELocalIPFilter) %{1}s имя локального IKE правила %{2}s IKEPeerIPFilter или IKELocalIPFilter
00100101	MSG_ID_LP_IKECFGIF_ASSIGNED_IP	LP	INFO	%[%{32}s %]Address %{1}s assigned to IKECFG network interface, peer %{8}s%[:%{9}u%]%[, id "%{10}s"%]	Активирован ikecfg-интерфейс с адресом %{1}
00100105	MSG_ID_LP_IKECFGIF_DNS_ADDR_SET	LP	INFO	%[%{32}s %]DNS address(es) %{1}s configured on IKECFG network interface, peer %{8}s%[:%{9}u%]%[, id "%{10}s"%]	Адрес или адреса DNS-серверов получены от партнера и добавлены в системный список. %{1}s - список адресов

00100106	MSG_ID_LP_IKECFGIF_DNS_ADDR_ERROR	LP	WARNING	%[%{32}s %]Failed to configure DNS address(es) %{1}s on IKECFG network interface, peer %{8}s%[:%{9}u%]%[, id "%{10}s"%]	Ошибка при добавлении адресов DNS-серверов в системный список %{1}s - список адресов
00100107	MSG_ID_LP_IKECFGIF_DNS_SUFFIXES_SET	LP	INFO	%[%{32}s %]DNS suffix(es) %{1}s added to the system, peer %{8}s%[:%{9}u%]%[, id "%{10}s"%]	DNS-суффиксы получены от партнера и добавлены в системный список %{1}s - список суффиксов
00100108	MSG_ID_LP_IKECFGIF_DNS_SUFFIXES_ERROR	LP	WARNING	%[%{32}s %]Failed to add DNS suffix(es) %{1}s to the system, peer %{8}s%[:%{9}u%]%[, id "%{10}s"%]	Ошибка при добавлении DNS-суффиксов в системный список %{1}s - список суффиксов
00100102	MSG_ID_LP_IKECFGIF_BAD_IP	LP	WARNING	%[%{32}s %]IKECFG address %{1}s can't be used in current network configuration. Attempting to get another address. Peer %{8}s%[:%{9}u%]%[, id "%{10}s"%]	Присланный по IKECFG IP-адрес конфликтует с существующими в системе адресами или правилами роутинга. %{1}s - полученный адрес
00100103	MSG_ID_LP_IKECFGIF_BAD_PH2ID	LP	ERR	%[%{32}s %]Incorrect IKE traffic request %{1}s for IKECFG interface. Subnet expected. Peer %{8}s%[:%{9}u%]%[, id "%{10}s"%]	Присланный во второй фазе IKE ID (селектор SA) не подходит для IKECFG-интерфейса, т.к. содержит протоколы или не является описанем подсети. %{1}s - присланный ID
00100104	MSG_ID_LP_IKECFGIF_RULE_NOT_PERSISTENT	LP	ERR	%[%{32}s %]IKECFG is not supported for non persistent connection, IKERule "%{1}s", peer %{8}s%[:%{9}u%]%[, id "%{10}s"%]	Работа IKECFG по IPsecAction запрещена т.к. он не имеет флага PersistentConnection. %{1}s - имя IKERule, присоединенного к IPsecAction без флага PersistentConnection

00100111	MSG_ID_LP_VIF_NO_PHY	LP	WARNING	[CFG] no physical interface found for NetworkInterface "%{1}s" pattern "%{2}s"	При загрузке конфигурации не найдено ни одного сетевого интерфейса, соответствующего описанию NetworkInterface. %{1}s - LogicalName этого NetworkInterface %{2}s - шаблон имени, найденный по LogicalName
00100201	MSG_ID_IKECFGIF_SETUP_FAILED	LP	CRIT	[IKECFGIF] can't setup IKECFG interface: see failh log	Ошибка при конфигурации виртуального интерфейса IKECFG. Подробности описаны в файле %TEMP%/vpnsvc/error.log, который необходимо передать разработчикам.
00100202	MSG_ID_IKECFGIF_DIFFERENT_IP	LP	WARNING	[IKECFGIF] changing address of IKECFG interface from %{1}s to %{2}s	Возникла необходимость смены адреса, отключения или изменения состояния IKECFG-интерфейса. Вероятно, изменилась конфигурация IKE-партнера, или адрес IKECFG был занят кем-то другим. Производится перезагрузка конфигурации. %{1} - старый адрес %{2} - новый адрес
00100203	MSG_ID_IKECFGIF_ADD_ROUTE_FAILED	LP	WARNING	[IKECFGIF] can't setup IKECFG interface: can't create route %{1}s/%{2}s via %{3}s: %{4}s	Ошибка создания маршрута в системной таблице роутинга при конфигурации IKECFG-интерфейса {1} - подсеть назначения {2} - маска подсети {3} - gateway {4} - расшифровка ошибки
00100205	MSG_ID_LP_IKECFG_REFUSED_BY_SERVER	LP	WARNING	%[%{32}s %]IKECFG address request rejected by server, peer %{8}s%[:%{9}u%]%[, id "%{10}s"%]	На запрос адреса по IKECFG IKE партнер ответил отказом.

00100206	MSG_ID_LP_IKECFG_RADIUS_IGNORED	LP	NOTICE	%[%{32}s %]Framed IP address from RADIUS server will be ignored. Using local IKECFG data instead. Peer %{8}s%[:%{9}u%]%[, id "%{10}s"%]	Присланный RADIUS-сервером Framed IP address для партнёра не будет использован, так как в LSP задано использование локального IKECFG пула.
00100207	MSG_ID_IKECFGIF_WIN_ENABLE_ROUTER_FAILED	LP	WARNING	[IKECFGIF] can't enable packet forwarding	Не удалось включить пересылку пакетов между сетевыми интерфейсами. Возможно, данная функциональность заблокирована антивирусными приложениями.
00100112	MSG_ID_LP_CONFIGURATION_LOADED	LP	NOTICE	[CFG] %{2}s configuration loaded via %{1}s%[, title "%{4}s"%]	Конфигурация успешно загружена. %{1} - источник конфигурации (cs_console, command line, token и т.п.) %{2} - тип конфигурации (driver default, DHCP only, user-defined) %{4} - название из конфигруации (GlobalParameters.Title)
00100113	MSG_ID_LP_CONFIGURATION_PARTIALLY_LOADED	LP	WARNING	[CFG] %{2}s configuration loaded via %{1}s%[, title "%{4}s"%], %{6}u potential problem(s) found%[: %{5}s%]	Конфигурация успешно загружена, но есть предупреждения, которые направлены в лог. %{1} - источник конфигурации (cs_console, command line, token и т.п.) %{2} - тип конфигурации (driver default, DHCP only, user-defined) %{4} - название из конфигруации (GlobalParameters.Title) %{5} - текст предупреждения %{6} - количество предупреждений
00100114	MSG_ID_LP_CONFIGURATION_LOAD_FAILURE	LP	ERR	[CFG] error in configuration from "%{1}s": %{3}s	Ошибка разбора конфигруации %{1} - источник конфигурации (cs_console, command line, token и т.п.) %{3} - описание ошибки

00100115	MSG_ID_LP_CONNECTION_REQUEST	LP	INFO	[IPSEC] connection request #%{1}u, packet %{2}s,%[Filter "%{3}s", %]IPsecAction "%{4}s"	Начало создания IPsec-соединения (обработка bundle request). %{1} - номер запроса %{2} - селектор пакета из запроса %{3} - имя Filter %{4} - имя IPsecAction
00100116	MSG_ID_LP_CONNECTION_REQUEST_INI_FAILED	LP	ERR	[IPSEC] connection request #%{1}u failed,%[Filter "%{2}s", %]packet %{3}s: %{4}s	Ошибка на начальной стадии создания IPsec-соединения (обработка bundle request). %{1} - номер запроса %{2} - селектор пакета из запроса %{3} - описание ошибки
00100117	MSG_ID_LP_CONFIGURATION_SAVE_FAILED	LP	CRIT	[CFG] can't save configuration in db: error "%{1}d"	Ошибка сохранения конфигурации в базе данных продукта. %{1} - код ошибки, который можно передать в службу поддержки для расшифровки
00100119	MSG_ID_LP_HOST_CONNECTED	LP	NOTICE	%[%{32}s %]IPSec connection %{1}u established, traffic selector %{2}s, peer %{8}s%[:%{9}u%], id "%{10}s"%[, Filter %{3}s%], IPsecAction %{4}s, IKERule %{5}s	Создано IPsec-соединения (IKE Quick Mode завершилась успешно). %{1} - номер созданного IPsec-соединения %{2} - IKE traffic request/phase 2id/селектор IPsec SA %{3} - название фильтра %{4} - имя IPsec-правила %{5} - имя IKE-правила

0010011A	MSG_ID_LP_CONNECTION_REQUEST_FAILURE	LP	ERR	%[%{32}s %]IPSec connection request #%{6}u failed%[: %{1}s%]%[: %{2}s%]. Peer %{8}s%[:%{9}u%]%[, id "%{10}s"%]%[, Filter %{3}s%]%[, IPsecAction %{4}s%]%[, IKERule %{5}s%]	Попытка создания IPsec SA закончилась неудачей. %{1} - стадия ike, где обнаружена ошибка %{2} - причина ошибки %{3} - название фильтра %{4} - имя IPsec-правила %{5} - имя IKE-правила %{6} - порядковый номер запроса на создание IPsec-соединения
0010011B	MSG_ID_LP_CONNECTION_REKEYING_FAILURE	LP	WARNING	%[%{32}s %]Re-keying of IPSec connection %{6}u failed%[: %{1}s%]%[: %{2}s%]. Peer %{8}s%[:%{9}u%]%[, id "%{10}s"%]%[, Filter %{3}s%]%[, IPsecAction %{4}s%]%[, IKERule %{5}s%]	Попытка пересоздания IPsec SA закончилась неудачей. %{1} - стадия ike, где обнаружена ошибка %{2} - причина ошибки %{3} - название фильтра %{4} - имя IPsec-правила %{5} - имя IKE-правила %{6} - номер IPsec-соединения, которое пытались обновить
0010011C	MSG_ID_LP_INCOMING_CONNECTION_FAILURE	LP	ERR	%[%{32}s %]Incoming connection failed%[: %{1}s%]%[: %{2}s%]. Peer %{8}s%[:%{9}u%]%[, id "%{10}s"%]%[, Filter %{3}s%]%[, IPsecAction %{4}s%]%[, IKERule %{5}s%]	Обмен IKE, где мы выступаем в качестве респондера, закончился неудачей. %{1} - стадия ike, где обнаружена ошибка %{2} - причина ошибки %{3} - название фильтра %{4} - имя IPsec-правила %{5} - имя IKE-правила
0010011D	MSG_ID_LP_CONNECTION_CLOSED	LP	NOTICE	IPSec connection %{1}u closed: %{3}u bytes sent, %{4}u received: %{2}s%[, matched by license number %{5}u%]	IPsec SA удалены. %{1} - идентификатор IPsec-соединения %{2} - причина удаления SA %{3} - байтов отправлено %{4} - байтов принято

0010011E	MSG_ID_LP_STALE_CONNECTION_BY_LICENSE	LP	WARNING	%[%{32}s %]Stale IPSec connection %{1}u detected with peer %{18}s%[:%{19}u%], id "%{20}s", license number: %{2}s: while processing initial contact from peer %{8}s%[:%{9}u%], id "%{10}s"	По уникальному номеру лицензии партнёра обнаружен старое, неиспользуемое IPSec соединение %{1} - идентификатор старого IPsec-соединения %{2} - номер лицензии партнёра. %{18} - IP-адрес партнёра по IKE обмену для старого соединения. %{19} - IP-порт партнёра по IKE обмену для старого соединения. Если не указан, то порт стандартный (500) %{20} - Значение IKE идентификатора для аутентификации партнёра для старого соединения.
00100124	MSG_ID_LP_LICENSE_CHECKED	LP	INFO	Product license info: product code %{1}s, license number %{2}u	Проверка лицензии прошла успешно %{1} - тип продукта в лицензии %{2} - номер лицензии
00100125	MSG_ID_LP_NO_LICENSE	LP	ALERT	Product license info: no license	Файл лицензии отсутствует или в нем неправильные данные. Продукт будет работать с ограничениями до ввода лицензии и рестарта.
00100129	MSG_ID_LP_SNMP_TRAP_RECV_NO_IP	LP	WARNING	[SNMP] failed to configure SNMP trap destination %{1}s: no IP address found for network interface "%{2}s"	Не удалость найти адрес для сетевого интерфейса, который указан в качестве источника SNMP trap %{1} - адрес получателя SNMP trap %{2} - логическое имя сетевого интерфейса

0010012C	MSG_ID_LP_ID_CONFLICT	LP	WARNING	%[%{32}s %]Traffic request overlaps with other IPsec SA created for peer %{1}s:%{2}d, conflicting address range: %{5}s, peer %{8}s%[:%{9}u%]%[, id "%{10}s"%]	Селектор создаваемого SA пересекается с селектором ранее созданного SA для одного фильтра. Это признак несогласованности конфигураций парнера, может привести к удалению IPsec-пакетов при обработке из-за несоответствия политике безопасности. Данное сообщение является предупреждением о возможных проблемах и не прерывает процесс создания SA. %{1} - IP адрес партнера, создавшего SA, с которым конфликтует вновь создаваемый %{2} - порт этого партнера
00100130	MSG_ID_LP_SAME_AUTH_METHOD_SPEC	LP	WARNING	[CFG] IKERule "%{2}s", line %{3}d: %{1}s has multiple authentication methods with the same type, only first of them will be used.	Предупреждение возникает, если при загрузке конфигурации обнаружено, что в IKERule присутствует несколько методов аутентификации одного типа. Респондер будет использовать только первый вариант из двух однотипных методов. %{1} - список, где встречен повтор (AggrModeAuthMethod/MainModeAuthMethod) %{2} - имя ike-правила %{3} - номер строки, где это правило описано
00100138	MSG_ID_LP_AGENT_INI_CP_CONTEXTS_PER_SA_INVALID	LP	WARNING	DefaultCryptoContextsPerIPSecSA in "agent.ini" is not valid (should be 1..128), %{1}d will be used instead.	При чтении ini-файла обнаружено неправильное значение для DefaultCryptoContextsPerIPSecSA будет использовано значение по-умолчанию. %{1} - значение по-умолчанию

00100139	MSG_ID_LP_AM_USE_ONE_GROUP	LP	WARNING	[CFG] IKERule "%{2}s", line %{3}d: in Aggressive Mode initiator will use %{1}d only.	Предупреждение возникает, если при загрузке конфигурации обнаружено, что в IKERule затребован aggressive-режим для инициатора, но присутствуют трансформы с различными GroupID. Инициатором будет использоваться только указанный GroupID. %{1} - группа, которая будет использована инициатором %{2} - имя ike-правила %{3} - номер строки, где это правило описано
0010013D	MSG_ID_LP_OLD_SA_DIE_BEFORE_NEW	LP	WARNING	%[%{32}s %]Old IPSec SA had been killed before new IPSec SA was created during rekeying. Please report this to the product support. Peer %{8}s%[:%{9}u%]%[, id "%{10}s"%]	SA, для которого проводился rekeying был удален до загрузки вновь созданного SA. Просьба сообщить в службу поддержки о подобном поведении.
0010013E	MSG_ID_LP_DEL_ROUTE_FAILED	LP	WARNING	[ROUTE] can't delete route %{1}s/%{2}d via %{3}s: %{4}s	Ошибка удаления маршрута, описанного в LSP. %{1} - подсеть назначения %{2} - маска подсети %{3} - gateway или имя интерфейса %{4} - пояснение ошибки
0010013F	MSG_ID_LP_ADD_ROUTE_FAILED	LP	WARNING	[ROUTE] can't add route %{1}s/%{2}d via %{3}s: %{4}s	Ошибка добавления маршрута, описанного в LSP. %{1} - подсеть назначения %{2} - маска подсети %{3} - gateway или имя интерфейса %{4} - пояснение ошибки

00100140	MSG_ID_LP_IPSEC_HI_TTL_TRAFFIC	LP	WARNING	%[%{32}s %]SA traffic limit (%{1}d) exceeds limitations imposed by the cryptograghic algorithm, peer %{8}s%[:%{9}u%], id "%{10}s"	В созданном IPsec SA ограничение по трафику не соответствует допустимому ограничению для используемого криптографического алгоритма. %{1} - ограничение, которое будет использовано в созданном IPsec SA (0 - без ограничений)
00100151	MSG_ID_AUDIT_LOAD_NEW_LSP	LP	INFO	[CFG] new LSP (%{1}s line(s)) successfully loaded by "%{2}s" user via %{3}s%["%{6}s"%] process%[%{4}s using unrecognized connection%]%[using %{5}s remote connection%]	Конфигурация успешно загружена по инициативе пользователя посредством утилиты (cs_console, lsp_mgr). Предваряет построчную выдачу загруженной LSP по MSG_ID_AUDIT_SHOW_NEW_LSP. %{1} - количество строк в загруженной LSP. %{2} - имя пользователя, инициировавшего загрузку %{3} - PID процесса локальной утилиты, выполнившей запрос на загрузку LSP %{4} - вспомогательный аргумент %{5} - детали remote-connection ("Daemon(<IPs><ports>)") %{6} - имя утилиты, инициировавшей загрузку
00100152	MSG_ID_AUDIT_SHOW_NEW_LSP	LP	INFO	[CFG] new LSP, line %{1}u/%{2}u: %{3}s	Последовательно выдаются "as is" нумерованные строки загруженной LSP сразу после выдачи сообщения MSG_ID_AUDIT_LOAD_NEW_LSP %{1} - номер выдаваемой строки LSP %{2} - всего строк в LSP %{3} - строка LSP

08500001	MSG_ID_RRI_NOT_CREATED	RRI	WARNING	[RRI] %{1}s, route not created: destination %{2}s, traffic selector %{10}s%[..%{11}s%]%[:%{12}d%] - >%{13}s%[..%{14}d%]%[:%{15}d%]%[proto %{16}s%]	Ошибка формирования маршрута RRI. То есть проблема обнаружена до попытки добавить маршрут в системную таблицу. %{1} - пояснение ошибки %{2} - туннельный адрес %{10}-%{16} - селектор SA
08500002	MSG_ID_RRI_DEL_ROUTE_FAILED	RRI	WARNING	[RRI] can't delete route %{1}s/%{2}d via %{3}s: %{4}s	Ошибка удаления маршрута, созданного RRI. %{1} - подсеть назначения %{2} - маска подсети %{3} - gateway %{4} - пояснение ошибки
08500003	MSG_ID_RRI_ADD_ROUTE_FAILED	RRI	WARNING	[RRI] can't add route %{1}s/%{2}d via %{3}s: %{4}s	Ошибка добавления маршрута RRI. %{1} - подсеть назначения %{2} - маска подсети %{3} - gateway %{4} - пояснение ошибки
08500004	MSG_ID_RRI_UPDATED	RRI	INFO	[RRI] updated route to %{1}s/%{2}d: new gw %{3}s, old gw %{4}s	Обнавлен маршрут RRI. %{1} - подсеть назначения %{2} - маска подсети %{3} - новый gateway %{4} - предыдущий gateway
08500005	MSG_ID_RRI_CREATED	RRI	INFO	[RRI] created route %{1}s/%{2}d via %{3}s for destination %{4}s, traffic selector %{10}s%[..%{11}s%]%[:%{12}d%] - >%{13}s%[..%{14}d%]%[:%{15}d%]%[proto %{16}s%]	Создан маршрут RRI. %{1} - подсеть назначения %{2} - маска подсети %{3} - gateway %{4} - туннельный адрес %{10}-%{16} - селектор SA

08500006	MSG_ID_RRI_REMOVED	RRI	INFO	[RRI] removed route %{1}s/%{2}d via %{3}s for destination %{4}s	Удален маршрут RRI. %{1} - подсеть назначения %{2} - маска подсети %{3} - gateway %{4} - туннельный адрес
10002001	MSG_ID_IKE_IKECFG_ASSIGNED	IKE	INFO	%[%{32}s %]IKECFG address %{1}s assigned to peer %{8}s%[:%{9}u%], id "%{10}s", %{2}s%[, dns server(s): %{11}s%[%{12}s%]%[%{13}s%]%[%{14}s%]%[%{15}s(...)%]%]%[, domain suffix(es): %{21}s%[%{22}s%]%[%{23}s%]%[%{24}s%]%[%{25}s(...)%]%]	Партнёру выдан внутренний адрес из IKECFG пула %{1} - выданный адрес %{2} - статус проксирования ARP-запросов: proxy ARP enabled - проксирование включено для всех интерфейсов с подсетями, включающими выданный адрес; partial proxy ARP - проксирование включено не для всех интерфейсов с подсетями, включающими выданный адрес; no proxy ARP - ARP-запросы не проксируются.
10002003	MSG_ID_IKE_IKECFG_REFUSED_BY_CLIENT	IKE	INFO	%[%{32}s %]IKECFG address rejected by partner. Assigning another address. Peer %{8}s%[:%{9}u%], id "%{10}s"	Партнёр отказался от ранее выданного адреса из IKECFG пула. Делается попытка выдать партёру другой адрес.
10002004	MSG_ID_IKE_IKECFG_POOL_CONFLICT	IKE	INFO	%[%{32}s %]IKECFG address %{1}s is already bound to another partner. Clearing old IKECFG data to resolve address conflict. Peer %{8}s%[:%{9}u%]%[, id "%{10}s"%]	Выдаваемый партнёру внутренний адрес из IKECFG пула уже занят другим партнёром со сходными параметрами. Соединения со старым партнёром будут уничтожены.

00102005	MSG_ID_IKE_IKECFG_ADDRESS_ASSIGNMENT_FAILED	LP	INFO	%[%{32}s %]Cannot assign IKECFG address%[%{1}s%] to partner%[: %{2}s%], peer %{8}s%[:%{9}u%], id "%{10}s"	Ошибка при попытке выдачи внутреннего адреса партнёру. %{1}s - выбранный IKECFG адрес для партнёра (если есть) %{2}s - возможные причины: pool is not configured - пул не задан; pool is over - пул исчерпан; proxy ARP failed - ошибка задания проксирования ARP-запросов
10002006	MSG_ID_IKE_IKECFG_ADDRESS_INCOMPATIBLE	IKE	INFO	%[%{32}s %]IKECFG address %{1}s was previously bound to current partner. Clearing old IKECFG data to assign new address. Peer %{8}s%[:%{9}u%]%[, id "%{10}s"%]	Ранее выданный партнёру внутренний адрес из IKECFG пула несовместим с текущей политикой безопасности, либо партнёр запросил другой IKECFG адрес. Имеющиеся соединения со старым партнёром будут уничтожены.
--------	--------	--------	--------	--------	Общие параметры для сообщений: %{8}s IP-адрес партнёра по IKE обмену. %{9}u IP-порт партнёра по IKE обмену. Если не указан, то порт стандартный (500) %{10}s Значение IKE идентификатора для аутентификации партнёра. %{15}u Порог ограничения ресурса %{20}s Причина возникновения события %{32}s Идентификатор сессии IKE обмена. Формат - "<n:m>", где n - номер защищающего ISAKMP соединения, m - номер обмена, защищаемого данным ISAKMP соединением %{40}u Номер ISAKMP соединения

10000001	MSG_ID_IKE_START_SESSION	IKE	DEBUG	%{32}s Start IKE session, Request: %{1}s, type %{2}s, peer %{8}s%[:%{9}u%]%[, sessionId %{4}s.%{5}s%]	Начат новый IKE обмен. %{1}s Причина, вызвавшая обмен %{2}s Тип обмена (Exchange Type по RFC2408) %{4}s Идентификатор обмена (Initiator Cookie по RFC2408) %{5}s Идентификатор обмена (Message ID по RFC2408)
10000002	MSG_ID_IKE_END_SESSION	IKE	DEBUG	%[%{32}s %]Session completed	IKE обмен завершён
10000003	MSG_ID_IKE_PARTNER_AGENT_INFO	IKE	DEBUG	%[%{32}s %]Partner's VPN Agent info: product:%{1}s%[, build:%{2}s.%{3}s.%{4}s%]%[, OS:%{5}s%]%[, CPU:%{6}s%]%[, features:%{7}s%]%[, product code:%{101}s%]%[, license number:%{103}s%]	Партнёр прислал информацию об используемом CSP VPN Агенте %{1}s Наименование продукта %{2}s Старший номер версии продукта %{3}s Младший номер версии продукта %{4}s Номер сборки продукта %{5}s Операционная система, для которой собран продукт %{6}s Платформа, для которой собран продукт %{7}s Дополнительные опции, включённые в сборку (если имеются) %{101}s Код продукта, указанный в лицензии %{103}s Номер лицензии
10000005	MSG_ID_IKE_SA_CREATED	IKE	INFO	%[%{32}s %]ISAKMP connection %{40}u created, peer %{8}s%[:%{9}u%]%[, id "%{10}s"%]	Создано ISAKMP соединение

10000006	MSG_ID_IKE_SA_CLOSED	IKE	INFO	ISAKMP connection %{40}u closed, peer %{8}s%[:%{9}u%]%[, id "%{10}s"%]%>INFO[, bytes sent/received: %{3}u/%{4}u, exchanges passed: %{5}u%]%[, Reason: %{20}s%]%[, matched by license number %{1}u%]	Уничтожено ISAKMP соединение
10000007	MSG_ID_IKE_ID_RECEIVED_FROM	IKE	DEBUG	%[%{32}s %]Receive identity "%{1}s", peer %{8}s%[:%{9}u%]	Партнёр прислал свою идентификационную информацию
10000008	MSG_ID_IKE_ID_SENT_TO	IKE	DEBUG	%[%{32}s %]Send identity "%{1}s", peer %{8}s%[:%{9}u%]%[, id "%{10}s"%]	Партнёру отослана локальная идентификационная информация
10000009	MSG_ID_IKE_FLOAT_PARTNER	IKE	DEBUG	%[%{32}s %]Float partner to %{8}s%[:%{9}u%]	Изменение сетевых параметров партнёра
1000000A	MSG_ID_IKE_PH2_ID_SEND	IKE	DEBUG	%[%{32}s %]Send traffic request: %{1}s->%{2}s	Партнёру отосланы параметры защищаемого трафика создаваемого IPSec соединения
1000000B	MSG_ID_IKE_PH2_ID_RECV	IKE	DEBUG	%[%{32}s %]Receive traffic request: %{1}s->%{2}s	Партнёр прислал параметры защищаемого трафика создаваемого IPSec соединения
1000000C	MSG_ID_IKE_INITIATE_SESSIONS_LIMIT	IKE	WARNING	[ISAKMP] Exchange pended. Limit of %{15}u initiated sessions achieved. Request: %{1}s, peer %{8}s%[:%{9}u%]	IKE обмен отложен из-за ограниченности ресурсов. %{1}s Причина, вызвавшая отложенный обмен
1000000E	MSG_ID_IKE_ACCESS_RESTRICTED	IKE	INFO	[ISAKMP] Peer %{8}s%[:%{9}u%] has limit of %{15}u responding IKE-sessions. New session requests were rejected %{3}u times	IKE обмен отменён из-за ограничения активности для указанного партнёра. %{3}u Количество отменённых обменов, инициированных партнёром, с момента предыдущего вывода данного сообщения

1000000F	MSG_ID_IKE_ACCESS_DENIED	IKE	WARNING	[ISAKMP] Access denied for peer %{8}s%[:%{9}u%]. %{3}u IKE-packet(s) dropped	IKE трафик от указанного партнёра полностью игнорируется. %{3}u Количество сброшенных IKE пакетов от указанного партнёра с момента предыдущего вывода данного сообщения
10000011	MSG_ID_IKE_NO_PEER_CERT	IKE	INFO	%[%{32}s %]Searching peer certificate failed, Reason: not found, peer %{8}s%[:%{9}u%]%[, id "%{10}s"%]	Сертификат партёра не найден
10000012	MSG_ID_IKE_PEER_CERT_INVALID	IKE	INFO	%[%{32}s %]Searching peer certificate failed. Reason: %{20}s.%{1}s, peer %{8}s%[:%{9}u%]%[, id "%{10}s"%]	Сертификат партёра не пригоден для использования %{1}s Описание сертификата
10000013	MSG_ID_IKE_PEER_CERT_FOUND	IKE	INFO	%[%{32}s %]Using peer certificate:%{1}s, peer %{8}s%[:%{9}u%]%[, id "%{10}s"%]	Использование сертификата партнёра для проверки подписи %{1}s Описание сертификата
10000014	MSG_ID_IKE_NO_LOCAL_CERT	IKE	WARNING	%[%{32}s %]Searching local certificate failed, Reason: not found, peer %{8}s%[:%{9}u%]%[, id "%{10}s"%]	Не найден локальный сертификат для создания подписи
10000015	MSG_ID_IKE_LOCAL_CERT_INVALID	IKE	WARNING	%[%{32}s %]Searching local certificate failed. Reason: %{20}s.%{1}s, peer %{8}s%[:%{9}u%]%[, id "%{10}s"%]	Локальный сертификат не пригоден для использования %{1}s Описание сертификата
10000016	MSG_ID_IKE_LOCAL_CERT_FOUND	IKE	DEBUG	%[%{32}s %]Using local certificate:%{1}s, peer %{8}s%[:%{9}u%]%[, id "%{10}s"%]	Использование локального сертификата для создания подписи %{1}s Описание сертификата

10000018	MSG_ID_IKE_EXCHANGE_FAILED	IKE	DEBUG	%[%{32}s %]IKE session stopped%[at %{1}s%]%<DEBUG[, type %{2}s, peer %{8}s%[:%{9}u%]%[, sessionId %{4}s.%{5}s%]%]%[, Reason: %{20}s%]	Неуспешное завершение IKE обмена %{1}s Список (стек) операций, при выполнении которых произошла ошибка. %{2}s Тип обмена (Exchange Type по RFC2408) %{4}s Идентификатор обмена (Initiator Cookie по RFC2408) %{5}s Идентификатор обмена (Message ID по RFC2408)
10000019	MSG_ID_IKE_DELETION_SEND	IKE	INFO	%[%{32}s %]Sending deletion for%[ISAKMP connection %{40}n%]%[IPSec connection %{2}u -%]%[%{3}s%>INFO[, spi:%{4}s%]%]	Отсылка партнёру сообщения об удалении соединения. %{40}s Номер удаляемого ISAKMP соединения. %{2}u Номер удаляемого IPSec соединения. %{3}u Сетевой протокол IPSec соединения. %{4}s Идентификатор spi удаляемого IPSec соединения.
1000001A	MSG_ID_IKE_DELETION_RECV	IKE	INFO	%[%{32}s %]Received deletion for%[ISAKMP connection %{40}n%]%[IPSec connection %{2}u -%]%[%{3}s%>INFO[, spi:%{4}s%]%]	Получено сообщение об удалении соединения партнёром. %{40}s Номер удаляемого ISAKMP соединения. %{2}u Номер удаляемого IPSec соединения. %{3}u Сетевой протокол удаляемого IPSec соединения. %{4}s Идентификатор spi удаляемого IPSec соединения.

1000001B	MSG_ID_IKE_NOTIFICATION_SEND	IKE	DEBUG	%[%{32}s %]Sending notification [%{1}s]%[for %{33}s%]%[for ISAKMP connection %{40}s%]%[, LifeTime:%{4}u%]%[, LifeTraffic:%{5}u%]	Отсылка партнёру информационного сообщения. %{1}u Тип информационного сообщения (Notification) по RFC2407, RFC2408. %{4}u Новое значение ограничения жизни соединения в секундах (для нотификации RESPONDER-LIFETIME). %{5}u Новое значение ограничения жизни соединения в килобайтах (для нотификации RESPONDER-LIFETIME). %{33}s Идентификатор адресуемой сессии IKE обмена. %{40}s Номер адресуемого ISAKMP соединения.
1000001C	MSG_ID_IKE_NOTIFICATION_RECV	IKE	DEBUG	%[%{32}s %]Received notification [%{1}s]%[for %{33}s%]%[for ISAKMP connection %{40}s%]%[: %{3}s%]%[, LifeTime:%{4}u%]%[, LifeTraffic:%{5}u%]	Получено информационное сообщение. %{1}u Тип информационного сообщения (Notification) по RFC2407, RFC2408. %{3}s Реакция на полученное сообщение. %{4}u Новое значение ограничения жизни соединения в секундах (для нотификации RESPONDER-LIFETIME). %{5}u Новое значение ограничения жизни соединения в килобайтах (для нотификации RESPONDER-LIFETIME). %{33}s Идентификатор адресуемой сессии IKE обмена. %{40}s Номер адресуемого ISAKMP соединения.

1000001D	MSG_ID_IKE_UNPROTECTED_NOTIFICATION_RECV	IKE	DEBUG	%[%{32}s %]Received unprotected notification [%{1}s]%[for %{33}s%]%[for ISAKMP connection %{40}s%]: Ignore	Получено незащищённое (недоверяемое) информационное сообщение. %{1}u Тип информационного сообщения (Notification) по RFC2407, RFC2408. %{33}s Идентификатор адресуемой сессии IKE обмена. %{40}s Номер адресуемого ISAKMP соединения.
1000001E	MSG_ID_IKE_SA_DEACTIVATED	IKE	DEBUG	%[%{32}s %]ISAKMP connection %{40}u deactivated%[, Reason: %{20}s%]%[, matched by license number %{1}u%]	ISAKMP соединение закрыто для использования в новых IKE-обменах. Некоторое время соединение может быть использовано для защиты ранее созданных и информационных обменов.
10000020	MSG_ID_IKE_REDUCE_LIFE_TIME	IKE	INFO	%[%{32}s %]Reducing life time%[for ISAKMP connection %{40}s%] to %{1}u seconds	Изменено ограничение жизни устанавливаемого соединения по времени. %{1}u Новое значение ограничения жизни соединения в секундах.
10000021	MSG_ID_IKE_REDUCE_LIFE_TRAFFIC	IKE	INFO	%[%{32}s %]Reducing life traffic%[for ISAKMP connection %{40}s%] to %{1}u kilobytes	Изменено ограничение жизни устанавливаемого соединения по трафику. %{1}u Новое значение ограничения жизни соединения в килобайтах.
10000050	MSG_ID_IKE_RESPOND_PH1_REJECT	IKE	WARNING	[ISAKMP] Limit of %{1}u responding Phase-1 sessions is achieved. Starting to reject new sessions.	Достигнуто ограничение по общему количеству выполняемых IKE обменов в роли респондера. Все новые обмены певой фазы, предлагаемые партнёрами, будут отвергаться до момента снижения нагрузки (см. MSG_ID_IKE_RESPOND_PH1_ACCEPT). %{1}u Достигнутый порог огранчения.

10000051	MSG_ID_IKE_RESPOND_PH1_ACCEPT	IKE	WARNING	[ISAKMP] %{1}u packets for new Phase-1 sessions were dropped. Starting to accept new sessions.	Возобновление проведения новых IKE обменов певой фазы, предлагаемых партнёрами. (см. MSG_ID_IKE_RESPOND_PH1_REJECT) %{1}u Количество отвергнутых пакетов новых обменов первой фазы за время действия ограничения.
10000070	MSG_ID_IKE_WRONG_PADDING	IKE	DEBUG	%[%{32}s %]Wrong padding in partner's encrypted packet	Партнёр прислал зашифрованный пакет с неправильным форматом padding'a.
10000071	MSG_ID_IKE_SEND_PACKET_FAILED	IKE	DEBUG	%[%{32}s %]Unable to send IKE packet%[to %{8}s%[:%{9}u%]%]	Произошла ошибка при отсылке IKE-пакета. Пакет может быть послан позднее при ретрансмиссии.
10000101	MSG_ID_IKE_NAT_REMOTE_DETECTED	IKE	DEBUG	%[%{32}s %]NAT detected on remote side	Обнаружено NAT-устройство на стороне партнёра
10000102	MSG_ID_IKE_NAT_LOCAL_DETECTED	IKE	DEBUG	%[%{32}s %]NAT detected on local side	Обнаружено NAT-устройство на локальной стороне
10000103	MSG_ID_IKE_NAT_T_WRONG_PORT	IKE	DEBUG	%[%{32}s %]Packet to incompatible port received while using NAT-Traversal	При использовании NAT-Traversal от партнёра получен IKE пакет на UDP порт 500
10000104	MSG_ID_IKE_NAT_T_UNABLE_USE_PORT	IKE	ERR	%[%{32}s %]Unable to use port 4500 for NAT-Traversal, peer: %{8}s%[:%{9}u%]%[, id: "%{10}s"%]	Невозможно задействовать NAT-Traversal так как не был открыт сокет на UDP порт 4500

10000201	MSG_ID_IKE_STALE_CONNECTION_BY_LICENSE	IKE	WARNING	%[%{32}s %]Stale ISAKMP connection %{40}u detected with peer %{18}s%[:%{19}u%], id "%{20}s", license number %{2}u: while processing initial contact from peer %{8}s%[:%{9}u%], id "%{10}s"	По уникальному номеру лицензии партнёра обнаружен старое, неиспользуемое ISAKMP соединение %{2}u Номер лицензии партнёра. %{18}s IP-адрес партнёра по IKE обмену для старого соединения. %{19}u IP-порт партнёра по IKE обмену для старого соединения. Если не указан, то порт стандартный (500) %{20}s Значение IKE идентификатора для аутентификации партнёра для старого соединения.
10000202	MSG_ID_IKE_LOCAL_LICENSE_DUPLICATION_DETECTED	IKE	DEBUG	%[%{32}s %]Duplicate of local license detected	Партнёр использует ту же лицензию, что и на локальном устройстве
10008001	MSG_ID_IKE_UDP_SOCKET_FAILED	IKE	WARNING	[ISAKMP] Failed to open UDP socket for %{8}s:%{9}u. Please send this message to support.	Ошибка открытия сокета для поддержки протокола ISAKMP Начиная с Windows Vista может изредка возникать после выхода Windows из режима Гибернации (Hibernation) или Сна (Suspend). В этом случае следует перезагрузить LSP для восстановления работоспособности Агента.
10000401	MSG_ID_IKE_RADIUS_REQUEST_USER	IKE	DEBUG	%[%{32}s %]RADIUS: Sending request to Access Server for user "%{1}s", peer: %{8}s%[:%{9}u%]%[, id: "%{10}s"%]	Отсылка запроса на аутентификацию Access серверу для указанного username
10000410	MSG_ID_IKE_RADIUS_ACCESS_GRANTED	IKE	DEBUG	%[%{32}s %]RADIUS: Access granted.%[Additional attributes received: %{1}s.%] Peer: %{8}s%[:%{9}u%]%[, id: "%{10}s"%]	От Access сервера получено разрешение на создание соединения с партнёром %{1} - Присланные дополнительные атрибуты. Формируются из сообщения MSG_ID_IKE_RADIUS_IKECFG_DATA

10000411	MSG_ID_IKE_RADIUS_IKECFG_DATA	IKE	DEBUG	Framed-IP-Address:%{1}s%[, cisco-av-pair:"dns-servers=%{10}s%[%{11}s%]"%]%[, cisco-av-pair:"default-domain=%{20}s%[%{21}s%]"%]%[: (%{3}s)%]	Дополнительные атрибуты, присланные RADIUS-сервером, формируемые для сообщения MSG_ID_IKE_RADIUS_ACCESS_GRANTED (Не является самостоятельным сообщением) %{1},%{10},%{11},%{20},%{21} - значения соответствующих атрибутов %{3} - дальнейшие действия по использованию атрибутов: sending received attributes to peer as IKECFG data - значения будут переданы партнёру в качестве IKECFG параметров ignored due to intersection with local AddressPool - значения будут игнорированы, так как присланный ip-адрес попадает в пул, который контролирует локальный IKECFG сервер ignored: IKERule has IKECFGPool, using local IKECFG data instead - значения будут игнорированы, так как в сработавшем IKE-правиле задействована выдача IKECFG параметров из локального пула

10000420	MSG_ID_IKE_RADIUS_ACCESS_FAILED	IKE	DEBUG	%[%{32}s %]RADIUS: %{1}s. Peer: %{8}s%[:%{9}u%]%[, id: "%{10}s"%]	Неуспешное завершение запроса к RADIUS-серверу %{1} - Причина отказа: Access Server timeout - нет отклика от RADIUS-сервера Access Server is not authenticated - неуспешная аутентификация RADIUS-сервера (неверное значение secret) Rejected by Access Server - RADIUS-сервер отказал в доступе партнёру (неверная пара user-password) Request to Access Server failed - прочие ошибки
00880001	MSG_ID_RADIUS_LOAD_SETTINGS	RADIUS Client	WARNING	[RADIUS] AAA Settings are not properly activated: %{1}s	Не удалось настроить клиент RADIUS (структура LSP AAASettings).
00880002	MSG_ID_RADIUS_NO_KEY	RADIUS Client	WARNING	[RADIUS] Can't retrieve key "%{1}s" from DB	Не удалось обнаружить ключ в базе данных продукта
007F0001	MSG_ID_IKECFGSRV_DUMMY_OBJECT	IKECFG Server	WARNING	[IKECFGSRV] There is no pool in new configuration for remaining address %{1}s, peer: %{8}s%[:%{9}u%]%[, id: "%{10}s"%]	В загружаемой новой LSP отсутствуют IKECFG пулы, которые соответствуют сохранённым ранее выданным IKECFG адресам. IKECFG адрес продолжает удерживаться, хотя он не соответствует ни одному из пулов в новой LSP. Примечание: Данное сообщение может не выводиться при логировании на внешний syslog сервер.
00324001	MSG_ID_LDAP_REQ_NOT_FOUND	LDAP	INFO	%[%{32}s %]LDAP request result: NOT FOUND. Query: "%{1}s".	Результат LDAP запроса – объекты не найдены {1} - LDAP запрос (URL) {32} - идентификатор сессии IKE обмена

00324101	MSG_ID_LDAP_CREATE_REQ_FAILED	LDAP	WARNING	%[%{32}s %]Failed to create LDAP request. Query: "%{1}s".	Не удалось сформировать корректный LDAP запрос. {1} - LDAP запрос (URL) Здесь и далее: данный запрос может отличаться от URL, указанного в сообщении о формировании LDAP-запроса (случай "CRL by URL"), если исходный URL не содержал адреса LDAP-сервера. {32} - идентификатор сессии IKE обмена
00324102	MSG_ID_LDAP_PARSE_FAILED	LDAP	WARNING	%[%{32}s %]Failed to parse LDAP message. Query: "%{1}s".	Ошибка разбора сообщения от LDAP сервера. {1} - LDAP запрос (URL) {32} - идентификатор сессии IKE обмена
00324103	MSG_ID_LDAP_REQ_FAILED_TIMEOUT	LDAP	WARNING	%[%{32}s %]LDAP request cancelled by timeout. Query: "%{1}s".	LDAP запрос завершен по таймауту. {1} - LDAP запрос (URL) {32} - идентификатор сессии IKE обмена
00324104	MSG_ID_LDAP_REQ_FAILED_NOT_RESPOND	LDAP	WARNING	%[%{32}s %]LDAP server is not responding. Query: "%{1}s".	LDAP сервер не отвечает. {1} - LDAP запрос (URL) {32} - идентификатор сессии IKE обмена
00324105	MSG_ID_LDAP_REQ_FAILED_CANCELED	LDAP	DEBUG	%[%{32}s %]LDAP request cancelled.	LDAP запрос отменен (например при остановке сервиса vpnsvc) {32} - идентификатор сессии IKE обмена
00324106	MSG_ID_LDAP_REQ_FAILED_CONNECTION_CLOSED	LDAP	DEBUG	%[%{32}s %]LDAP connection was closed by LSP unload.	Соединение LDAP было закрыто при выгрузке LSP. {32} - идентификатор сессии IKE обмена
003241FF	MSG_ID_LDAP_REQ_FAILED_UNKNOWN	LDAP	DEBUG	%[%{32}s %]LDAP internal error.	Внутренняя ошибка модуля LDAP. {32} - идентификатор сессии IKE обмена

00325001	MSG_ID_LDAP_REQ_SUCCESS	LDAP	INFO	%[%{32}s %]LDAP request result: %{2}u object(s) found. Query: "%{1}s".	Результат LDAP запроса - найдено {2} объектов {1} - LDAP запрос (URL) {32} - идентификатор сессии IKE обмена
00327001	MSG_ID_LDAP_REQ_START	LDAP	DEBUG	%[%{32}s %]LDAP request: "%{1}s".	Сформирован LDAP запрос {1} где {1} – запрос в одном из следующих видов: "CRL by DN: <Printable_DN>" – запрос CRL производится по DN. "Certificate by DN: <Printable_DN>" – запрос сертификата производится в виде DN. "CRL by URL: <url>" – запрос CRL по URL (берется из CDP). {32} - идентификатор сессии IKE обмена
00327002	MSG_ID_LDAP_REQ_IGNORED	LDAP	DEBUG	%[%{32}s %]LDAP request ignored: there is no LDAP server available.	LDAP запрос "{1}" проигнорирован: не задан LDAP сервер {32} - идентификатор сессии IKE обмена
00723001	MSG_ID_CSCONF_CONV_END_FAIL	Cisco-like console & converter	ERR	LSP converter finished with errors	LSP конвертор завершил работу с ошибками
00723003	MSG_ID_CSCONF_PARSE_CERT	Cisco-like console & converter	ERR	Certificate for CA "%{1}s", parse error	Ошибка разбора сертификата для CA {1}
00723004	MSG_ID_CSCONF_NOCA_CERT	Cisco-like console & converter	ERR	Wrong certificate type for CA "%{1}s", must be CA certificate	Неверный тип сертификата для CA {1}
00723005	MSG_ID_CSCONF_CERT_EXIST	Cisco-like console & converter	ERR	CA certificate "%{1}s" already exists in the trustpoint "%{2}s". Certificate addition ignored.	CA сертификат {1} уже присутствует в trustpoint {2}. Добавление сертификата проигнорировано

00723006	MSG_ID_CSCONF_POOL_INTERSECT	Cisco-like console & converter	ERR	Current pool entry has intersection with others, no entry will be added	Текущий пул адресов имеют пересечения с другими пулами. Запись не будет добавлена.
00723007	MSG_ID_CSCONF_NON_CSCONS_SAVE_FAIL	Cisco-like console & converter	ERR	Could not save previous user-defined LSP in file "%{1}s"	Не удалось сохранить предыдущую пользовательскую LSP в файл "{1}"
00724001	MSG_ID_CSCONF_CMD_REMOVED_AUTO	Cisco-like console & converter	WARNING	Command "%{1}s" removed from configuration automatically	Команда "{1}" автоматически удалена из конфигурации.
00724002	MSG_ID_CSCONF_REMOVE_CERT	Cisco-like console & converter	WARNING	Removing CA Trustpoint "%{1}s", no certificate found	При старте cs_console из конфигурации автоматически был удален сертификат, отсутствующий в базе локальных настроек. Образовался пустой trustpoint, который также был автоматически удален.
00724003	MSG_ID_CSCONF_REMOVE_KEY	Cisco-like console & converter	WARNING	Removing KEY "%{1}s", no key found in agent	При старте cs_console из конфигурации автоматически был удален preshared key, отсутствующий в базе локальных настроек.
00724004	MSG_ID_CSCONF_USER_AUTOMATICALLY_REUSED	Cisco-like console & converter	WARNING	User(s) %{1}s were automatically added to configuration. Zero privilege level was assigned to them.	При старте cs_console обнаружены пользователи системы, отсутствующие в конфигурации, но для которых в качестве shell выставлена cs_console. Данные пользователи автоматически добавлены в конфигурацию с нулевым уровнем привилегий.
00725001	MSG_ID_CSCONS_START	Cisco-like console & converter	NOTICE	Cisco-like console started by user "%{1}s"	cs_console запущена пользователем "{1}".
00725002	MSG_ID_CSCONS_EXIT	Cisco-like console & converter	NOTICE	Cisco-like console exited (user "%{1}s")	Пользователь "{1}" вышел из cs_console.

00725003	MSG_ID_CSCONF_USER_CREATED	Cisco-like console & converter	NOTICE	User "%{1}s" created	Успешно создан пользователь операционной системы "{1}". Может выдаваться как при ручном вводе команды, так и при старте cs_console (в случае, если в конфигурации присутствует пользователь, отсутствующий в системе).
00725004	MSG_ID_CSCONF_USER_REMOVED	Cisco-like console & converter	NOTICE	User "%{1}s" removed	Пользователь операционной системы "{1}" успешно удален. Может выдаваться при ручном вводе команды no username ...
00725005	MSG_ID_CSCONF_USER_PWD_CHANGED	Cisco-like console & converter	NOTICE	User "%{1}s" password changed	Пароль пользователя операционной системы {1} успешно сменен. Может выдаваться как при ручном вводе команды (только для уже существующего пользователя), так и при старте cs_console (в случае, если пароль пользователя в конфигурации не совпадает с паролем пользователя в системе).
00725006	MSG_ID_CSCONF_USER_PRIVL_CHANGED	Cisco-like console & converter	NOTICE	User "%{1}s" privilege changed to %{2}d	Привилегия пользователя операционной системы {1} изменена на новое значение {2}. Может выдаваться при ручном вводе команды username (только для уже существующего пользователя). Одна команда username... может порождать сразу два сообщения: о смене пароля и о смене привилегии.
00725007	MSG_ID_CSCONF_USER_EXEC_ENTERED	Cisco-like console & converter	NOTICE	User "%{1}s" has entered into the privileged EXEC mode	Пользователь вошел в привилегированный режим (по команде enable). Выдается только при ручном вводе команды enable.

00725008	MSG_ID_CSCONF_NON_CSCONS_LSP	Cisco-like console & converter	NOTICE	Previous user-defined LSP saved in file "%{1}s"	Предыдущая пользовательская LSP сохранена в файле "{1}"
00725009	MSG_ID_CSCONF_POLICY_NON_SYNC	Cisco-like console & converter	INFO	Non-synchronized policy detected. Policy type: %{1}s	Обнаружена несинхронизированная политика. Тип политики: <type> где <type> один из: DDP DHCP Only User-defined (Source: Command-line utility)
0072500A	MSG_ID_CSCONF_PRESHARED_KEYS_OR_CERTS_CHANGED	Cisco-like console & converter	INFO	Certificates or preshared keys were changed. Conversion required	Сертификаты или preshared keys изменились. Требуется конвертирование
0072500B	MSG_ID_CSCONF_START	Cisco-like console & converter	NOTICE	Command interpreter started	Старт интерпретатора команд
0072500C	MSG_ID_CSCONF_USER_SHELL_CHANGED	Cisco-like console & converter	NOTICE	User "%{1}s" shell changed to /opt/VPNagent/bin/cs_console	Shell пользователя операционной системы {1} успешно сменен. Может выдаваться при старте cs_console (в случае, если пользователь присутствует в конфигурации и в системе, но в системе в качестве shell прописано другое приложение).
00726001	MSG_ID_CSCONF_CONV_BEGIN	Cisco-like console & converter	INFO	Starting LSP converter	Запуск LSP конвертора
00726002	MSG_ID_CSCONF_CONV_END_OK	Cisco-like console & converter	INFO	LSP converter finished successfully	LSP конвертор отработал без ошибок
00727001	MSG_ID_CSCONF_CMD_START	Cisco-like console & converter	DEBUG	Start interpreting command: "%{1}s"	Начало обработки команды {1} интерпретатором

00727002	MSG_ID_CSCONF_CMD_END_OK	Cisco-like console & converter	DEBUG	Command "%{1}s" processed with status OK	Обработка команды "{1}" завершена успешно
00727003	MSG_ID_CSCONF_CMD_END_FAIL	Cisco-like console & converter	DEBUG	Command "%{1}s" processed with status FAIL	Команда "{1}" обработана с ошибкой
00733001	MSG_ID_CSCONV_INTERFACE_EMPTY_ACL	Cisco-like console & converter	ERR	Interface "%{1}s" references to the empty access list "%{2}s".	Интерфейс "{1}" ссылается на пустой ACL "{2}"
00733002	MSG_ID_CSCONV_NO_ACTIVE_POOL	Cisco-like console & converter	ERR	Address pool "%{1}s" not found.	Не найден пул адресов "{1}".
00733003	MSG_ID_CSCONV_CLASS_MAP_EMPTY_ACL	Cisco-like console & converter	ERR	Class map "%{1}s" (from policy map "%{2}s") references to the empty or absent access list "%{3}s".	Class map "{1}" (из policy map "{2}") ссылается на пустой или отсутствующий ACL "{3}"
00733101	MSG_ID_CSCONV_NO_ISAKMP_POLICY	Cisco-like console & converter	ERR	Could not convert crypto map "%{1}s". Reason: There is no isakmp policy.	Невозможно сконвертировать crypto map "{1}". Причина: Отсутствует isakmp policy.
00733102	MSG_ID_CSCONV_WRONG_AUTH	Cisco-like console & converter	ERR	Could not convert crypto map "%{1}s". Reason: There is no CA or appropriate preshared key. Also isakmp policy can have wrong type (rsa-sig or pre-share).	Невозможно сконвертировать crypto map "{1}". Причина: Отсутствует CA или подходящий Preshared Key, либо isakmp policy неправильного типа (rsa-sig или pre-share).
00733103	MSG_ID_CSCONV_NO_PEER	Cisco-like console & converter	ERR	Could not convert crypto map "%{1}s". Reason: There is no peer.	Невозможно сконвертировать crypto map "{1}". Причина: Отсутствует peer.

00733104	MSG_ID_CSCONV_NO_TRANSFORM_SET	Cisco-like console & converter	ERR	Could not convert crypto map "%{1}s". Reason: There are no transform sets.	Невозможно сконвертировать crypto map "{1}". Причина: Отсутствуют transform sets.
00733105	MSG_ID_CSCONV_INCOMPLETE_CRYPTO_MAP	Cisco-like console & converter	ERR	Could not convert %{1}s. Reason: It is incomplete.	Невозможно сконвертировать crypto map или dynamic crypto map template: Причина: Crypto map неполная (в случае crypto map: не хватает crypto ACL или peer; в случае crypto map или dynamic crypto map template: ссылка на пустой crypto ACL). %{1}s - один из двух вариантов: crypto map "<name> <seq-num>" или dynamic crypto map template "<name> <seq-num>"
00733106	MSG_ID_CSCONV_CRYPTO_MAP_EMPTY_ACL	Cisco-like console & converter	ERR	Could not convert crypto map "%{1}s". Reason: Reference to the empty access list "%{2}s" for a clear-text packets filtration.	Невозможно сконвертировать crypto map "{1}". Причина: Ссылка на пустой ACL "{2}" для Clear-Text фильтрации (внутри защищенного туннеля).
00733107	MSG_ID_CSCONV_CRYPTO_MAP_IKECFG_MISMATCH	Cisco-like console & converter	ERR	Could not convert %{1}s. Reason: %{2}s references to the same pool ("%{3}s") but the additional parameters to send to client are different.	Невозможно сконвертировать crypto map "{1}". Причина: crypto map (или dynamic crypto map template) "{2}" ссылается на тот же самый пул ("{3}"), но дополнительные параметры, отсылаемые клиенту, различаются.
00733108	MSG_ID_CSCONV_CRYPTO_MAP_PH1_MODE_MISMATCH	Cisco-like console & converter	ERR	Could not convert crypto map "%{1}s". Reason: conflicting Phase 1 modes (main and aggressive) for different peers. Check the "crypto isakmp peer" commands.	Невозможно сконвертировать crypto map "{1}". Причина: конфликтующие режимы первой фазы (main mode и aggressive mode) для разных peer-ов. Проверьте команды "crypto isakmp peer".

00733109	MSG_ID_CSCONV_CRYPTO_MAP_ACL_WITH_TIME_RANGE	Cisco-like console & converter	ERR	Could not convert %{1}s. Reason: access list "%{2}s" references time range.	Невозможно сконвертировать crypto map "{1}". Причина: ACL "{2}" ссылается на time range.
0073310A	MSG_ID_CSCONV_CRYPTO_MAP_NO_CLIENT_USERNAME	Cisco-like console & converter	ERR	Could not convert %{1}s. Reason: AAA client authentication list has been referenced without username source ("set client username...").	Невозможно сконвертировать crypto map "{1}". Причина: Пристуствует ссылка на список AAA аутентификации, но отсутствует источник имени пользователя ("set client username...").
0073310B	MSG_ID_CSCONV_CRYPTO_MAP_NO_AUTH_LIST_REF	Cisco-like console & converter	ERR	Could not convert %{1}s. Reason: AAA client authentication username source has been set without authentication list reference ("set client authentication list...").	Невозможно сконвертировать crypto map "{1}". Причина: задан источник имени пользователя, но отсутствует список AAA аутентификации ("set client authentication list...")
0073310C	MSG_ID_CSCONV_CRYPTO_MAP_UNKNOWN_AUTH_LIST	Cisco-like console & converter	ERR	Could not convert %{1}s. Reason: Reference to unknown AAA client authentication list.	Невозможно сконвертировать crypto map "{1}". Причина: Ссылка на неизвестный список AAA аутентификации.
007331FF	MSG_ID_CSCONV_CRYPTO_MAP_NOT_CONVERTED	Cisco-like console & converter	ERR	Could not convert crypto map "%{1}s". Reason: Unknown	Невозможно сконвертировать crypto map "{1}" по неизвестной причине.
00733A01	MSG_ID_CSCONV_LSP_LOAD_FAILED	Cisco-like console & converter	ERR	LSP load failed%[: %{1}s%].%[Erroneous LSP saved in file "%{2}s".%]	Не удалось прогрузить сформированную LSP. Расшифровка ошибки: {1} Ошибочная LSP сохранена в файле "{2}".
00733A02	MSG_ID_CSCONV_LSP_LOAD_FAILED_VPNSVC_NOT_RUNNING	Cisco-like console & converter	ERR	LSP load failed: vpnsvc daemon is not running.	Не удалось прогрузить сформированную LSP. Невозможно установить связь с сервисом vpnsvc.

00733A03	MSG_ID_CSCONV_NO_TIME_RANGE	Cisco-like console & converter	ERR	Access list "%{1}s" references absent time range "%{2}s".	ACL "{1}" ссылается на отсутствующий time range "{2}"
00733A04	MSG_ID_CSCONV_AUTH_LIST_RADIUS_WITHOUT_SERVER	Cisco-like console & converter	ERR	AAA authentication list has been set without RADIUS server.	Задан список AAA аутентификации, но не задан адрес RADIUS сервера
00733A05	MSG_ID_CSCONV_RADIUS_SERVER_WITHOUT_KEY	Cisco-like console & converter	ERR	RADIUS server has been set without shared secret.	Задан RADIUS сервер, но не задан пароль доступа к нему
00733FFF	MSG_ID_CSCONV_FAILED	Cisco-like console & converter	ERR	LSP conversion failed	Неизвестная ошибка конвертирования LSP.
00734001	MSG_ID_CSCONV_LDAP_IGNORED	Cisco-like console & converter	WARNING	LDAP url "%{1}s" ignored. IP address and port allowed only.	Введенный LDAP url {1} проигнорирован, поскольку допускаются только IP-адрес и порт.
00734002	MSG_ID_CSCONV_SOME_PEERS_IGNORED	Cisco-like console & converter	WARNING	Crypto map "%{1}s" contains several peers. Peer(s) "%{2}s" ignored due to authentication information mismatch.	В crypto map-е {1} прописаны несколько peer-ов. Peer(s) {2} проигнорированы из-за того, что для них не совпадает аутентификационная информация.
00734003	MSG_ID_CSCONV_SEVERAL_IPSEC_ACTIONS	Cisco-like console & converter	WARNING	Crypto map "%{1}s" contains several peers with different preshared keys. This is not recommended.	Crypto map "{1}" содержит несколько peers с разными preshared keys. Это нерекомендуемая ситуация.
00734004	MSG_ID_CSCONV_MIXED_MODE_TUNNEL	Cisco-like console & converter	WARNING	Crypto map(s) "%{1}s" contain transform sets with different encapsulation modes. Tunnel mode is used.	Crypto map(-ы) {1} содержат transform set-ы, в которых заданы разные encapsulation режимы. Используется туннельный режим.

00734005	MSG_ID_CSCONV_MIXED_MODE_TRANSPORT	Cisco-like console & converter	WARNING	Crypto map(s) "%{1}s" contain transform sets with different encapsulation modes. Transport mode is used.	Crypto map(-ы) {1} содержат transform set-ы, в которых заданы разные encapsulation режимы. Используется транспортный режим.
00734006	MSG_ID_CSCONV_STATIC_AFTER_DYNAMIC	Cisco-like console & converter	WARNING	Crypto map set(s) "%{1}s" contain static crypto map(s) with priorities lower than dynamic.	Crypto map set(s) "{1}" содержат статические crypto map(s) с приоритетом ниже, чем у динамических.
00734101	MSG_ID_CSCONV_LSP_LOAD_WITH_ONE_WARNING	Cisco-like console & converter	WARNING	LSP successfully loaded with warning: %{1}s.	Сформированная LSP загружена с одним предупреждением. {1} - текст предупреждения
00734102	MSG_ID_CSCONV_LSP_LOAD_WITH_WARNINGS	Cisco-like console & converter	WARNING	LSP successfully loaded, %{1}u potential problems were reported to syslog.	Сформированная LSP загружена с двумя и более предупреждениями. {1} - количество выданных предупреждений (если было выдано два и больше)
00735001	MSG_ID_CSCONV_START	Cisco-like console & converter	NOTICE	LSP conversion started	Начат процесс конвертирования
00735002	MSG_ID_CSCONV_STOP	Cisco-like console & converter	NOTICE	LSP conversion complete%[. Warnings: %{1}u%]	Процесс конвертирования завершен успешно. Опционально: выдано {1} предупреждений.
00793001	MSG_ID_INCORRECT_CPUUSAGE	Statistics & SNMP	WARNING	SNMP polling of CPU usage is unavailable. SNMP variables cpmCPUTotal* will be invalid.	Невозможно получать информацию о загрузке CPU для SNMP. Переменные SNMP cpmCPUTotal* будут иметь неверное значение.
00793002	MSG_ID_USE_INTERCALARY_INSTANEOUS_CPUUSAGE	Statistics & SNMP	INFO	The system clock changed. SNMP cpmCPUTotal* statistics may be incorrect for a while.	Время на часах OS изменено. Статистика о загрузке CPU для SNMP может быть некорректна какое-то время.

00200001	MSG_ID_LOCAL_CERTIFICATE_ADDED	Certificates	NOTICE	New local certificate added%[Subject="%{1}s"%]%[Issuer="%{2}s"%]%[SN="%{3}s"%]	Добавление локального сертификата в базу данных
00200002	MSG_ID_CA_CERTIFICATE_ADDED	Certificates	NOTICE	New certificate authority added%[Subject="%{1}s"%]%[Issuer="%{2}s"%]%[SN="%{3}s"%]	Добавление Сертифицирующего Центра в базу данных
00200003	MSG_ID_CERTIFICATE_DISABLED	Certificates	WARNING	Certificate disabled%[Subject="%{1}s"%]%[Issuer="%{2}s"%]%[SN="%{3}s"%]	Удаление локального сертификата, либо Сертифицирующего Центра из базы данных
00200004	MSG_ID_LOG_PRIV_KEY_INACCESSIBLE	Certificates	CRIT	Local certificate '%{1}s' is invalid: private key %[at container%{3}s %]'%{4}s' is inaccessible	Приватный ключ локального сертификата недоступен Где: %{1}s – значение поля Subject локального сертификата «at container» – если ключ не был задан явно %{4}s – путь к ключу, если он был задан явно, иначе имя контейнера
00200005	MSG_ID_LOG_PRIV_CONT_INACCESSIBLE	Certificates	CRIT	Local certificate '%{1}s' is invalid: container '%{4}s' is inaccessible	Контейнер ключа локального сертификата недоступен Где: %{1}s – значение поля Subject локального сертификата %{4}s – имя контейнера
00200006	MSG_ID_LOG_PRIV_KEY_INCONSISTENCY	Certificates	CRIT	Local certificate '%{1}s' is invalid: private key %[at container%{3}s %]'%{4}s' is inconsistent with the certificate	Приватный ключ не соответствует локальному сертификату. Это возможно только после установки OCI Где параметры - см.описание MSG_ID_LOG_PRIV_KEY_INACCESSIBLE

006F0001	MSG_ID_LOG_X509_CONV_UNSUP_ENCODING	Certificates	CRIT	Unsupported "%{1}s" iconv encoding	В файле x509conv.ini указана неподдерживаемая кодировка
006F0002	MSG_ID_LOG_X509_CONV_UNSUP_ENCODING_USE_DEFAULT	Certificates	WARNING	Unsupported encoding "%{1}s" has been specified in x509conv.ini, "%{2}s" will be used	В файле x509conv.ini указана неподдерживаемая кодировка %{1}, будет использоваться умолчательная %{2}
006F0003	MSG_ID_LOG_X509_CONV_UNEXP_INI_FIELD	Certificates	WARNING	Unexpected parameter "%{1}s" has been specified in x509conv.ini, ignored	В файле x509conv.ini указан неизвестный параметр
006F0004	MSG_ID_LOG_X509_CONV_INCOMP_ENCODING_ATTR	Certificates	WARNING	Certificate with subject "%{1}s" has incompatible attribute value encoding. Probably, the connection won't be established. Please, configure x509conv.ini according to actual attribute encoding.	Ошибка при перекодировке полей Issuer или Subject сертификата в UTF-8
00650001	MSG_ID_USER_LOGIN	<MAIN_APPLICATION>	NOTICE	User logged in	Доступ Пользователя к Агенту
00650002	MSG_ID_USER_LOGOUT	<MAIN_APPLICATION>	NOTICE	User logged out	Отключение доступа Пользователя к Агенту
00650003	MSG_ID_USER_LOGIN_FAILED	<MAIN_APPLICATION>	ERR	User%["%{1}s"%] login failed	Неудача доступа Пользователя к Агенту
00290001	MSG_ID_ON_IPSM_LOG_MID_FW_TCP_STATS_TRAIL	Firewall	INFO	Session closed: initiator %{8}s%[:%{9}u%] sent %{3}U bytes -- responder(%{18}s%[:%{19}u%]) sent -> %{13}U bytes	Сообщение инициируется когда закрывается соединение. Сообщает, сколько байт было послано и принято. Где %{8} – ip адрес источника %{3} – кол-во байт посланных инициатором %{18} – ip адрес принимающей стороны %{13} – кол-во байт посланных принимающей стороной

00290002	MSG_ID_ON_IPSM_LOG_MID_FW_TCP_HCONN_ALERT	Firewall	WARNING	getting aggresive, count(%{1}u/%{2}u), current 1-minute rate: %{3}u	Появление такого сообщения в логе может свидетельствовать о начале DOS атаки. где, %{1} – кол-во полуоткрытых соединений %{2} – кол-во новых соединений %{3} – кол-во новых соединений за минуту
00290003	MSG_ID_ON_IPSM_LOG_MID_FW_TCP_HCONN_ALERT_OFF	Firewall	WARNING	calming down, count (%{1}u/%{2}u), 1-minute rate %{3}u	Появление такого сообщения может свидетельствовать об окончании DOS атаки где параметры - см.описание MSG_ID_ON_IPSM_LOG_MID_FW_TCP_HCONN_ALERT
00290004	MSG_ID_ON_IPSM_LOG_MID_FW_FTP_PORT_PRIV_PORT	Firewall	WARNING	Privileged port %{9}u, used in PORT command -- FTP client %{8}s FTP server %{18}s	FTP клиент пытается выполнить команду PORT на привилегированном порту (<1024) где, %{9} – номер порта %{8} – ip FTP клиента %{18} – ip FTP сервера
00290005	MSG_ID_ON_IPSM_LOG_MID_FW_FTP_PASV_PRIV_PORT	Firewall	WARNING	Privileged port %{9}u, used in PASV response command -- FTP client %{8}s FTP server %{18}s	FTP сервер пытается выполнить ответ на PASV команду на привилегированном порту. где параметры - см.описание MSG_ID_ON_IPSM_LOG_MID_FW_FTP_PORT_PRIV_PORT
00290006	MSG_ID_ON_IPSM_LOG_MID_FW_FTP_PORT_NOTAUTH	Firewall	WARNING	Command issued before the session is authenticated -- FTP client %{8}s (client side)	Попытка выполнить FTP команду до окончании аутентификации со стороны FTP клиента где %{8} – ip FTP клиента
00290007	MSG_ID_ON_IPSM_LOG_MID_FW_FTP_PASV_NOTAUTH	Firewall	WARNING	Command issued before the session is authenticated -- FTP client %{8}s (server side)	Попытка выполнить FTP команду до окончании аутентификации со стороны FTP сервера где %{8} – ip FTP клиента

00290008	MSG_ID_ON_IPSM_LOG_OTHERS	Firewall	DEBUG	no format string: message id %{1}u	Нет формата строки: сообщение номер…
00290009	MSG_ID_KLOGLIB_INIT_NO_MEMORY	Firewall	DEBUG	Can't create statistic states(no memory)	Недостаточно памяти для создания объектов статистики
0029000A	MSG_ID_KLOGLIB_INIT_CANT_ATTACH	Firewall	DEBUG	unable to attach as listener	Невозможно присоединится к драйверу “klogview” в режиме слушателя
0029000B	MSG_ID_KLOGLIB_INIT_CANT_SET_FILTER	Firewall	DEBUG	unable to set event filter	Невозможно установить фильтр сообщений из ядра
0029000C	MSG_ID_KLOGLIB_INIT_MISSED_ALERT_PACKETS	Firewall	WARNING	access-list logging missed %{1}u alert packets	Оповещение о количестве пропущенных тревожных сообщений, превысивших допустимую частоту их обновления
0029000D	MSG_ID_KLOGLIB_INIT_MISSED_PACKETS	Firewall	WARNING	access-list logging rate-limited or missed %{1}u packets	Оповещение о количестве пропущенных сообщений из IPSEC драйвера, превысивших допустимую частоту их обновления.
0029000E	MSG_ID_KLOGLIB_INIT_PRINT_SUMMARY	Firewall	INFO	list %{1}s %{2}s %[%{3}s %]%[%{13}u %]%{8}s(%{4}u) -> %{18}s(%{14}u), %{5}U packet(s)	Статистика по соединению за интервал времени где: %{1} – название access list, если задано в LSP %{2} - статус, %{3}/%(13} - выдается или имя протокола или его номер %{8} - ip адрес источника, %{18} – ip адрес приемника, %{5} - количество пакетов
08530001	MSG_ID_WATCHDOG_VPNSVC_CRASHED	Installer for Unix	WARNING	IPsec daemon (vpnsvc) crashed (see /tmp/vpnsvc/error.log for details)	Оповещение watchdog: IPsec демон (vpnsvc) аварийно завершился

08530002	MSG_ID_WATCHDOG_VPNSVC_RUNNING_AGAIN	Installer for Unix	NOTICE	IPsec daemon (vpnsvc) is running	Оповещение watchdog: IPsec демон (vpnsvc) запущен
08530003	MSG_ID_WATCHDOG_VPNSVC_RUN_ERROR	Installer for Unix	ERR	Error restarting IPsec daemon (vpnsvc)	Оповещение watchdog: перезапуск IPsec демона (vpnsvc) не удался
08530004	MSG_ID_WATCHDOG_VPNSVCLOG_CRASHED	Installer for Unix	WARNING	VPN log daemon (vpnlogsvc) crashed (see /tmp/vpnlogsvc/error.log for details)	Оповещение watchdog: демон логирования (vpnlogsvc) аварийно завершился
08530005	MSG_ID_WATCHDOG_VPNSVCLOG_RUNNING_AGAIN	Installer for Unix	NOTICE	VPN log daemon (vpnlogsvc) is running	Оповещение watchdog: демон логирования (vpnlogsvc) запущен
08530006	MSG_ID_WATCHDOG_VPNSVCLOG_RUN_ERROR	Installer for Unix	ERR	Error restarting VPN log daemon (vpnlogsvc)	Оповещение watchdog: перезапуск демона логирования (vpnlogsvc) не удался
08530007	MSG_ID_VPNSVC_RUN_ERROR	Installer for Unix	ERR	Starting IPsec daemon failed. See /tmp/vpnsvc/error.log for details.	Оповещение скрипта запуска: запуск IPsec демона (vpnsvc) не удался
08530008	MSG_ID_VPNSVCLOG_RUN_ERROR	Installer for Unix	ERR	Starting VPN log daemon failed. See /tmp/vpnlogsvc/error.log for details.	Оповещение скрипта запуска: запуск демона логирования (vpnlogsvc) не удался
08530009	MSG_ID_WATCHDOG_VPNSVC_STOPPED	Installer for Unix	NOTICE	IPsec daemon (vpnsvc) stopped	Оповещение watchdog: IPsec демон (vpnsvc) остановлен
0853000A	MSG_ID_WATCHDOG_VPNSVCLOG_STOPPED	Installer for Unix	NOTICE	VPN log daemon (vpnlogsvc) stopped	Оповещение watchdog: демон логирования (vpnlogsvc) остановлен

00020001	MSG_ID_LOG_SET_DEFAULT_LOGLEVEL	Log	INFO	Default log level is %{1}s	Нефильтруемое сообщение об установке умолчательного уровня логирования сообщений. Выдается при каждом его изменении и в начале сессии VPN Сервиса. Где: %{1} – значение установленного log level - {emerg | alert | crit | err | warning | notice | info | debug}
00020002	MSG_ID_LOG_SET_SYSLOG_SETTINGS	Log	INFO	Syslog settings are: %{1}s, %{2}s, %{3}s	Нефильтруемое сообщение об установках syslog. Выдается при каждом их изменении и в начале сессии VPN Сервиса. Где: %{1} – разрешение отсылки сообщений - {enable | disable}; %{2} – IP адрес syslog сервера %{3} – параметр facility, указываемый при передаче сообщений syslog серверу
00020003	MSG_ID_LOG_SET_PARTICULAR_LOGLEVELS	Log	INFO	Some particular log levels are set	Нефильтруемое сообщение об установке частных уровней логирования некоторым сообщениям. Выдается при каждом их изменениях и в начале сессии VPN Сервиса.
00020004	MSG_ID_LOG_SAVE_PARTICULAR_LOGLEVELS	Log	INFO	Current particular log levels are permanently saved	Нефильтруемое сообщение о сохранении всех текущих частных уровней логирования сообщений для использования в следующих сессиях VPN Сервиса. Выдается при каждом таком сохранении.
00020005	MSG_ID_LOG_RESET_PARTICULAR_LOGLEVELS	Log	INFO	All particular log levels are reset	Нефильтруемое сообщение о сбросе частных уровней логирования всем сообщениям. Выдается при каждом таком сбросе.

2.1 Список ошибок протокола ISAKMP

(указываются в сообщениях в поле «Reason:» %{20}s в Таблица 3)

Таблица 4

	Описание ошибки	Запись об ошибке в строке сообщения
1	От партнера пришло сообщение неверного типа вместо ожидаемого сообщения CONNECTED (свидетельствующего о готовности IPSec-соединения на стороне партнера)	Unexpected Notification type: need CONNECTED
2	Получен компонент IKE-пакета типа 130, соответствующий компоненту для обнаружения устройства NAT, что не соответствует протоколу обмена для данного этапа	Unexpected payload found (payload type - 130, possibly NAT Discovery)
3	От партнера пришла команда дополнительного конфигурирования ISAKMP-соединения (XAuth, IKE-CFG, и т.п.), не соответствующая протоколу обмена для данного этапа	Unexpected configuration message type
4	От партнера пришли параметры дополнительного конфигурирования ISAKMP-соединения (XAuth, IKE-CFG, и т.п.), не соответствующие текущей политике безопасности	Bad Config proposal
5	Потеряны внутренние данные от предыдущего пакета	Previous packet missed
6	Потеряны данные формируемого пакета	OUT packet missed
7	Потерян SA-компонент предыдущего пакета	Missing SA payload
8	Невозможно выбрать сценарий IKE-обмена для выбранного типа аутентификации	Unknown IKE-scenario for chosen Authentification method
9	Не найден один из необходимых компонентов пакета	Can’t find proposal
10	Партнер вернул неправильную идентификационную информацию ответчика IKE-обмена при создании IPSec-соединения	Bad IDcr returned
11	Потеряны данные входящего пакета	IN packet missed
12	Партнер вернул неправильную идентификационную информацию инициатора IKE-обмена при создании IPSec-соединения	Bad IDci returned
13	Сессия дополнительного конфигурирования ISAKMP-соединения (XAuth, IKE-CFG, и т.п.) была прервана встречным запросом – другой сессией дополнительного конфигурирования XAuth	Replaced with new XAuth request
14	Сессия Quick Mode остановлена для перезапуска с новыми параметрами запроса после дополнительного конфигурирования защищающего ISAKMP-соединения.	Restart session
15	Невозможность продолжить IKE-обмен после выполнения асинхронного запроса. (Возможно, за время выполнения запроса произошло событие, вызвавшее прекращение обмена)	Can't Complete Async Task
16	Невозможно создать информационный IKE-обмен	Can't create new Informational Exchange
17	Невозможно создать IKE-обмен 2-й фазы	Can't create new Phase-II

	Описание ошибки	Запись об ошибке в строке сообщения
18	Невозможно создать IKE-обмен 1-й фазы	Can't create new Exchange
19	Невозможно создать IKE-обмен 2-й фазы из-за незавершенности обмена 1-й фазы	Request to create Phase-II without completed Phase-I
20	IKE-обмен не начат по причине чрезмерной активности недоверяемого партнёра	Access denied
21	Фактический размер IKE-пакета не соответствует указанному в его заголовке	Invalid packet (size mismatch)
22	Партнер прислал IKE-пакет с неправильной структурой, либо пакет не удалось правильно расшифровать	Invalid packet (invalid structure)
23	Некорректный компонент IKE-пакета	Invalid packet (invalid payload)
24	Зашифрованность (либо незашифрованность) присланного пакета не соответствует IKE-сценарию, либо ошибка в процессе дешифрования IKE-пакета	Unable to decode packet
25	Внутренняя (системная) ошибка	Internal error
26	Переполнение памяти	Out of memory
27	IKE-пакет распознан как перепосылка для ранее созданного IKE-обмена	Retransmission detected
28	Присланный IKE-пакет не распознан, либо не актуален для существующего обмена	Wrong IKE packet received
29	Присланный IKE-пакет не актуален для существующего обмена	IKE packet dropped
30	Присланный IKE-пакет является перепосылкой для только что созданного IKE-обмена	Repeat for the first packet in exch
31	Для присланного IKE-пакета сценарий не поддерживается	Unable to determine IKE scenario
32	Запрет на создание нового IKE-обмена в процессе смены политики безопасности	Process blocked by Local Policy
33	Незавершённый асинхронный запрос	Asynchronous request was started...
34	Ошибка при шифровании IKE-пакета	CP coding error
35	Ошибка установки таймера для сервиса перепосылок IKE-пакетов	Unable to set Timer

2.1.1 Список выполняемых действий по протоколу ISAKMP

(указываются в сообщениях в поле «Stopped at: %{1}s» в Таблица 3)

Таблица 5

	Описание действия	Информация в строке сообщения
1	Шифрование сформированного IKE-пакета перед отправкой партнеру	[Coding packet]
2	Расшифрование IKE-пакета, присланного партнером	[Decoding packet]
3	Проверка предложений, на которые согласился партнер	[Check replied SA]
4	Проверка сертификата, присланного партнером	[Check for Remote Certificate]
5	Запрос локального сертификата	[Check for Local Certificate]
6	Проверка идентификационной информации, присланной партнером	[Check incom IDs]
7	Использование в качестве идентификационной информации партнера его IP-адреса	[Check IDs as IP-addresses]
8	Проверка используемого алгоритма хэширования	[Check for Hash method]
9	Синтаксический разбор пакета, присланного партнером на отдельные компоненты (payloads)	[Make payload set for received packet]
10	Проверка всех компонентов присланного пакета	[Check received payloads]
11	Проверка формируемого пакета на наличие компонентов перед отправкой партнеру. Используется только при создании пакетов Informational обменов чтобы удостовериться, что информация не была отправлена с другим пакетом.	[Check for added payloads]
12	Вычисление подписи	[Calculate Signature]
13	Выбор правила IKE согласно текущей конфигурации по идентификационной информации партнера	[Choose Rule for Partner’s identity]
14	Создание ключевых пар текущей IKE-сессии	[Generate Keys]
15	Формирование ключевого материала	[Generate SKEYIDs]
16	Выбор политики безопасности согласно текущей конфигурации на основании предложений от партнера	[Compare policy]
17	Формирование SPI	[Set SPI]
18	Проверка и принятие параметров устанавливаемого соединения, на которые согласился партнер	[Accept Transform]
19	Вычисление хэша для обнаружения устройства NAT	[Calculate NAT Discovery payload]

	Описание действия	Информация в строке сообщения
20	Вычисление общего ключа	[Calculate Shared Key]
21	Вычисление инициализационного вектора	[Calculate InitVector]
22	Определение метода аутентификации	[Detect Authentification Method]
23	Запрос локального сертификата для метода аутентификации с использованием сертификатов	[Get Local Certificates]
24	Проверка метода аутентификации, предложенного партнером, на соответствие текущей политике безопасности	[Check Authentification Method]
25	Выбор метода аутентификации	[Choose Authentification Method]
26	Проверка выбранной комбинации параметров устанавливаемого соединения	[Get Proposal]
27	Задание выбранного алгоритма шифрации для устанавливаемого соединения	[Get Algorithm]
28	Запрос возможных параметров устанавливаемого соединения согласно текущей конфигурации для их согласования с партнером	[Get Local Policy]
29	Проверка на наличие в предложении партнера параметра, устанавливающего MODP-группу	[Get DH group for QM]
30	Выбор используемой идентификационной информации для отправки партнеру	[Get ID from Local Policy]
31	Выбор используемой идентификационной информации для отправки партнеру при создании ISAKMP-соединения в качестве инициатора	[Get IDii from Local Policy
32	Выбор используемой идентификационной информации для отправки партнеру при создании ISAKMP-соединения в качестве ответчика	[Get IDir from Local Policy]
33	Выбор используемой идентификационной информации для отправки партнеру при создании IPSec-соединения в качестве инициатора IKE-обмена	[Get IDci from Local Policy]
34	Выбор используемой идентификационной информации для отправки партнеру при создании IPSec-соединения в качестве ответчика IKE-обмена	[Get IDcr from Local Policy]
35	Инициализация ключевой информации для формирования IPSec-соединения	[Initialize Encryption Container for QM
36	Формирование готового IPSec-соединения	[Create contexts
37	Распознавание метода дополнительного конфигурирования ISAKMP-соединения (XAuth, IKE-CFG, и т.п.)	[Determine IKE configuration method]
38	Распознавание команды дополнительного конфигурирования ISAKMP-соединения (XAuth, IKECFG, и т.п.)	[Determine Config message type]

	Описание действия	Информация в строке сообщения
39	Распаковка параметров присланного запроса на дополнительную аутентификацию (XAuth) и формирование соответствующего графического пользовательского диалога	[Analyse attributes and fill user dialog fields]
40	Запуск графического пользовательского диалога дополнительной аутентификации (XAuth).	[Start dialog for user extended authentication]
41	Проверка наличия компонента IKE-пакета	[Check payload %s[1]]
42	Проверка структуры компонента IKE-пакета	[Analyse payload structure %s[2]]
43	Формирование компонента IKE-пакета	[Form payload %s[3]]
44	Заполнение блока данных указанного компонента IKE-пакета	[Fill payload %s[4]]
45	Проверка содержимого компонента IKE-пакета	[Check %s[5]]
46	Вычисление хэша – содержимого указанного компонента	[Calculate %s[6]]
47	Выполнение сценария инициации информационного обмена IKE согласно RFC 2409	[Informational Exchange, Initiator, Packet 1]
48	Выполнение сценария обработки пакета информационного обмена IKE согласно RFC 2409	[Informational Exchange, Responder, Packet 1]
49	Выполнение шага сценария формирования 1-го пакета IKE Main Mode согласно RFC 2409	[Main Mode, Initiator, Packet 1]
50	Выполнение шага сценария обработки 1-го пакета IKE Main Mode согласно RFC 2409 и формирование ответного пакета	[Main Mode, Responder, Packets 1,2]
51	Выполнение шага сценария начала обработки 2-го пакета IKE Main Mode согласно RFC 2409	[Main Mode, Initiator, Packets 2,3]
52	Выполнение шага сценария продолжения обработки 2-го пакета IKE Main Mode для аутентификации на общих ключах согласно RFC 2409 и формирование ответного пакета	[Main Mode, Initiator, Packets 2,3, Pre-Shared Key]
53	Выполнение шага сценария продолжения обработки 2-го пакета IKE Main Mode для аутентификации на сертификатах согласно RFC 2409 и формирование ответного пакета	[Main Mode, Initiator, Packets 2,3, Signature]

[1] Название компонента (payload type) – согласно разделам 3.4 – 3.16 RFC 2408

[2] Название компонента (payload type) – согласно разделам 3.4 – 3.16 RFC 2408

[3] Название компонента (payload type) – согласно разделам 3.4 – 3.16 RFC 2408

[4] Название компонента (payload type) – согласно разделам 3.4 – 3.16 RFC 2408

[5] Название компонента (payload type) – согласно разделам 3.4 – 3.16 RFC 2408

[6] Название компонента (payload type) – согласно разделам 3.4 – 3.16 RFC 2408

	Описание действия	Информация в строке сообщения
54	Выполнение шага сценария обработки 3-го пакета IKE Main Mode для аутентификации на общих ключах согласно RFC 2409 и формирование ответного пакета	[Main Mode, Responder, Packets 3,4, Pre-Shared Key]
55	Выполнение шага сценария обработки 3-го пакета IKE Main Mode для аутентификации на сертификатах согласно RFC 2409 и формирование ответного пакета	[Main Mode, Responder, Packets 3,4, Signature]
56	Выполнение шага сценария обработки 4-го пакета IKE Main Mode для аутентификации на общих ключах согласно RFC 2409 и формирование ответного пакета	[Main Mode, Initiator, Packets 4,5, Pre-Shared Key]
57	Выполнение шага сценария обработки 4-го пакета IKE Main Mode для аутентификации на сертификатах согласно RFC 2409 и формирование ответного пакета	[Main Mode, Initiator, Packets 4,5, Signature]
58	Выполнение шага сценария обработки 5-го пакета IKE Main Mode для аутентификации на общих ключах согласно RFC 2409 и формирование ответного пакета	[Main Mode, Responder, Packets 5,6, Pre-Shared Key]
59	Выполнение шага сценария обработки 5-го пакета IKE Main Mode для аутентификации на сертификатах согласно RFC 2409 и формирование ответного пакета	[Main Mode, Responder, Packets 5,6, Signature]
60	Выполнение шага сценария обработки 6-го пакета IKE Main Mode для аутентификации на общих ключах согласно RFC 2409	[Main Mode, Initiator, Packet 6, Pre-Shared Key]
61	Выполнение шага сценария обработки 6-го пакета IKE Main Mode для аутентификации на сертификатах согласно RFC 2409	[Main Mode, Initiator, Packet 6, Signature]
62	Выполнение шага сценария начала формирования 1-го пакета IKE Aggressive Mode Mode согласно RFC 2409	[Aggressive Mode, Initiator, Packet 1]
63	Выполнение шага сценария продолжения формирования 1-го пакета IKE Aggressive Mode для аутентификации на общих ключах согласно RFC 2409	[Aggressive Mode, Initiator, Packet 1, Pre-Shared Key]
64	Выполнение шага сценария продолжения формирования 1-го пакета IKE Aggressive Mode для аутентиф икации на сертификатах согласно RFC 2409	[Aggressive Mode, Initiator, Packet 1, Signature]
65	Выполнение шага сценария начала обработки 2-го пакета IKE Aggressive Mode согласно RFC 2409	[Aggressive Mode, Responder, Packets 1,2]
66	Выполнение шага сценария продолжения обработки 1-го пакета IKE Aggressive Mode для аутентификации на общих ключах согласно RFC 2409 и формирование ответного пакета	[Aggressive Mode, Responder, Packets 1,2, Pre-Shared Key]
67	Выполнение шага сценария продолжения обработки 1-го пакета IKE Aggressive Mode для аутентификации на сертификатах согласно RFC 2409 и формирование ответного пакета	[Aggressive Mode, Responder, Packets 1,2, Signature]
68	Выполнение шага сценария обработки 2-го пакета IKE Aggressive Mode для аутентификации на общих ключах согласно RFC 2409 и формирование ответного пакета	[Aggressive Mode, Initiator, Packets 2,3, Pre-Shared Key]
69	Выполнение шага сценария обработки 2-го пакета IKE Aggressive Mode для аутентификации на сертификатах согласно RFC 2409 и формирование ответного пакета	[Aggressive Mode, Initiator, Packets 2,3, Signature]

	Описание действия	Информация в строке сообщения
70	Выполнение шага сценария обработки 3-го пакета IKE Aggressive Mode для аутентификации на общих ключах согласно RFC 2409	[Aggressive Mode, Responder, Packet 3, Pre-Shared Key]
71	Выполнение шага сценария обработки 3-го пакета IKE Aggressive Mode для аутентификации на сертификатах согласно RFC 2409	[Aggressive Mode, Responder, Packet 3, Signature]
72	Выполнение шага сценария формирования 1-го пакета IKE New Group Mode согласно RFC 2409	[New Group Mode, Initiator, Packet 1]
73	Выполнение шага сценария обработки 1-го пакета IKE New Group Mode согласно RFC 2409 и формирование ответного пакета	[New Group Mode, Responder, Packets 1,2]
74	Выполнение шага сценария обработки 2-го пакета IKE New Group Mode согласно RFC 2409	[New Group Mode, Initiator, Packet 2]
75	Выполнение шага сценария формирования 1-го пакета служебного обмена IKE	[Transaction Exchange, Initiator, Packet 1]
76	Выполнение шага сценария обработки 1-го пакета служебного обмена IKE и формирование ответного пакета	[Transaction Exchange, Responder, Packets 1,2]
77	Выполнение шага сценария обработки 2-го пакета служебного обмена IKE	[Transaction Exchange, Initiator, Packet 2]
78	Выполнение шага сценария формирования 1-го пакета IKE Quick Mode согласно RFC 2409	[Quick Mode, Initiator, Packet 1]
79	Выполнение шага сценария обработки 1-го пакета IKE Quick Mode согласно RFC 2409 и формирование ответного пакета	[Quick Mode, Responder, Packets 1,2]
80	Выполнение шага сценария обработки 2-го пакета IKE Quick Mode согласно RFC 2409 и формирование ответного пакета	[Quick Mode, Initiator, Packets 2,3]
81	Выполнение шага сценария обработки 3-го пакета IKE Quick Mode согласно RFC 2409 и формирование ответного пакета (при поддержке партнером Commit Bit)	[Quick Mode, Responder, Packet 3,(4)]
82	Выполнение шага сценария обработки 4-го пакета IKE Quick Mode (при поддержке партнером Commit Bit)	[Quick Mode, Initiator, Packet 4]
83	Вычисление ключевого материала	[Make SKEYID]
84	Проведение PFS - создание отдельной ключевой пары для IPSec соединения	[Make PFS]
85	Выбор ISAKMP либо IPSec правила	[Choose Rule]
86	Проверка присланного атрибута – компонента пакета IKE	[Check Attr]
87	Проверка присланного сертификата – компонента пакета IKE	[Check Cert]
88	Проверка присланного хэша – компонента пакета IKE	[Check HASH]
89	Проверка присланного идентификатора – компонента пакета IKE	[Check ID]

	Описание действия	Информация в строке сообщения
90	Проверка присланного ключа – компонента пакета IKE	[Check KE]
91	Проверка присланного NAT-детектора – компонента пакета IKE	[Check NAT-D]
92	Проверка присланного NAT Original Address – компонента пакета IKE	[Check NAT-OA]
93	Проверка присланного Nonce – компонента пакета IKE	[Check Nonce]
94	Проверка присланного сообщения – компонента пакета IKE	[Check Notif]
95	Проверка присланного запроса на сертификат – компонента пакета IKE	[Check REQ]
96	Проверка присланных предложений на создание соединения – компонента пакета IKE	[Check SA]
97	Проверка присланной подписи – компонента пакета IKE	[Check SIG]
98	Проверка вендор-идентификатора – компонента пакета IKE	[Check VID]
99	Формирование атрибута – компонента пакета IKE	[Form Attr]
100	Формирование сертификата – компонента пакета IKE	[Form Cert]
101	Формирование хэша – компонента пакета IKE	[Form HASH]
102	Формирование идентификатора – компонента пакета IKE	[Form ID]
103	Формирование ключа – компонента пакета IKE	[Form KE]
104	Формирование NAT-детектора – компонента пакета IKE	[Form NAT-D]
105	Формирование NAT Original Address – компонента пакета IKE	[Form NAT-OA]
106	Формирование Nonce – компонента пакета IKE	[Form Nonce]
107	Формирование запроса на сертификат – компонента пакета IKE	[Form CertReq]
108	Формирование подписи – компонента пакета IKE	[Form SIG]
109	Формирование вендор-идентификатора – компонента пакета IKE	[Form VendorID]
110	Проверка на наличие устройства NAT	[NAT existence check]

2.1.2 Список причин инициации IKE сессии

(указываются в сообщениях IKE в поле «Request: %{1}s» в Таблица 3)

Таблица 6

	Причина инициации	Шаблон, используемый в сообщениях	Параметр
1	IKE-обмен в роли респондера	Inbound ISAKMP packet	
2	Запрос на создание IPsec соединения	Create IPSec #%{1}u	%{1}u – номер инициации IPSec-соединения
3	Пересоздание устаревшего IPsec соединения	IPSec %{1}u re-establishing	%{1}u – номер пересоздаваемого IPsec соединения
4	Удаление IPsec соединения	IPSec %{1}u deletion	%{1}u – номер удаляемого IPsec соединения
5	Пересоздание устаревшего ISAKMP соединения	ISAKMP %{1}s re-establishing	%{1}s – идентификатор пересоздаваемого ISAKMP соединения
6	Конфигурирование ISAKMP соединения (проведение IKECFG, XAuth)	ISAKMP %{1}s configure	%{1}s – идентификатор конфигурируемого ISAKMP соединения
7	Информирование партнёра по IKE-обмену (коррекция ISAKMP соединения, прекращение IKE-обмена)	ISAKMP notification	
8	Удаление ISAKMP соединения	ISAKMP %{1}s deletion	%{1}s – идентификатор удаляемого ISAKMP соединения
9	Удаление соединения по запросу пользователя[7]	User request	

[7] Посредством использования команды sa_mgr clear <…>

2.2 Ошибки криптографической подсистемы

Список сообщений об ошибках криптографической подсистемы, работающей в ядре ОС, приведен в таблице.

Таблица 7

	Текст шаблона сообщения	Рекомендуемые пользователю действия, краткое описание
1	CP_Conf_K2U_PushPluginConf: Plugin is not properly loaded	Если есть проблемы с загрузкой LSP или прохождением трафика, обратитесь в службу поддержки.
2	CP_ReOpen: bad check handle	Если есть проблемы с прохождением трафика, переустановить IPsec соединение, обратитесь в службу поддержки.
3	CP_Transform: bad handle 0x%x	Если есть проблемы с прохождением трафика, переустановить IPsec соединение, обратитесь в службу поддержки.
4	Skipping unused algorithm [%s]	Не ошибка, можно игнорировать.
5	forced close: 0x%x,0x%x	В результате падения приложения были автоматически уничтожены созданные им криптоконтексты. Если есть проблемы с прохождением трафика, переустановить IPsec соединение, обратитесь в службу поддержки.
6	drvcsp:_info()=OK	Не ошибка, можно игнорировать.
7	drvcsp: loglevel=0x1, logformat=0x39	Не ошибка, можно игнорировать.
8	drvcsp: serial= <...>	Не ошибка, можно игнорировать.

3. Мониторинг

Мониторинг S-Terra Client осуществляется по протоколу обмена SNMPv1 или SNMPv2c.

SNMP-менеджер имеет возможность запрашивать содержимое базы данных агента.

SNMP-агент может посылать SNMP-менеджеру сообщение о возникшем прерывании в виде трап-сообщения. Список этих сообщений приведен в разделе «Trap-сообщения».

База данных MIB, которую поддерживает SNMP-агент, описана в разделе «Выдача статистики».

Настройка SNMP-агента производится администратором при подготовке инсталляционного пакета пользователя:

- В GUI административного пакета настройка SNMP производится во вкладке **LSP**, в окне Advanced LSP Settings, в разделе SNMP settings.
- В конфигурационном файле задание настроек SNMP-агента осуществляется:
  - структурой `SNMPPollSettings` – для выдачи статистики SNMP-менеджеру. В этой структуре указывается IP-адрес и порт, на который можно получать запросы от SNMP-менеджера, строку, играющую роль пароля при аутентификации сообщений, размещение SNMP-агента и контактное лицо.
  - структурами `SNMPTrapSettings` и `TrapReceiver` – для посылки трап-сообщений. В этих структурах указывается IP-адрес и порт, на который отсылаются сообщения SNMP-менеджеру, идентификатор и IP-адрес отправителя трап-сообщения, версия SNMP, в которой создаются трап-сообщения.

В качестве SNMP-менеджера могут быть использована бесплатная утилита NET-SNMP (http://www.net-snmp.org/), которая является простейшим SNMP-менеджером. При работе с SNMP-агентом нужно указывать версию SNMP –v 1 или – v 2c.

3.1 Выдача статистики

SNMP-менеджер инициирует запрос на значения одной или нескольких переменных, который посылает SNMP-агенту. SNMP-агент, отвечая на запрос, возвращает значения одной или нескольких переменных.

База данных MIB, поддерживаемая SNMP-агентом, разделена на группы. В приведенной ниже таблице перечислены переменные из стандартной группы `system`, глобальной статистики IKE и IPsec, которые могут быть запрошены SNMP-менеджером.

Примечание 1: при принудительном перезапуске сервиса IKE-статистика сбрасывается и начинает считаться со старта Агента. IPsec-статистика считается со старта компьютера и при принудительном перезапуске сервиса не сбрасывается.

Примечание 2: в IKE-статистике при подсчете трафика учитывается только количество байт в ISAKMP-пакете. У Cisco же в IKE-статистике учитываются данные из IP-заголовка, UDP-заголовка и Ethernet-заголовка пакета.

Таблица 8

Название переменной	OID (идентификатор объекта)	Тип переменной	Значение переменной	MIB
Статистика по стандартной группе System и специфичным константным значениям				
sysDescr	1.3.6.1.2.1.1.1.0	DisplayString	Текстовое описание сетевого объекта. Строка вида "S-Terra Client 4.1.<build>"	RFC1213-MIB
sysObjectID	1.3.6.1.2.1.1.2.0	OID	Идентификатор фирмы-производителя (внутри поддерева 1.3.6.1.4.1): 1.3.6.1.4.1.9.1.576(cisco2811XM из CISCO-PRODUCTS-MIB)	RFC1213-MIB
sysUpTime	1.3.6.1.2.1.1.3.0	TimeTicks	The time (in hundredths of a second) since the network management portion of the system was last re-initialized. Время в сотых долях секунды с момента последней загрузки системы	RFC1213-MIB
sysContact	1.3.6.1.2.1.1.4.0	DisplayString	Имя контактной персоны и способ контакта	RFC1213-MIB
sysName	1.3.6.1.2.1.1.5.0	DisplayString	Полное имя домена <hostname>.<domain-name>	RFC1213-MIB
sysLocation	1.3.6.1.2.1.1.6.0	DisplayString	Физическое местоположение агента	RFC1213-MIB
sysServices	1.3.6.1.2.1.1.7.0	int32	Значение, которое характеризует сервисы, предоставляемые узлом. Это значение есть сумма номеров уровней модели OSI в зависимости от того, какие сервисы поддерживаются: 0x01 (физический), 0x02 (канальный), 0x04 (сетевой), 0x08 (точка-точка), 0x40 (прикладной). Например, если поддерживается IP уровень (маршрутизация) и транспортный уровень (точка-точка), то значение sysServices есть сумма 4 и 8. 78 (c2611XM)	RFC1213-MIB
chassisType	1.3.6.1.4.1.9.3.6.1.0	int32	413 (c2811XM)	OLD-CISCO-CHASSIS-MIB
cipSecMibLevel	1.3.6.1.4.1.9.9.171.1.1.1.0	int32	The level of the IPsec MIB 1	CISCO-IPSEC-FLOW-MONITOR-MIB

Название переменной	OID (идентификатор объекта)	Тип переменной	Значение переменной	MIB
snmpSetSerialNo	1.3.6.1.6.3.1.1.6.1.0	int32	<An advisory lock used to allow several cooperating SNMPv2 entities, all acting in a manager role, to coordinate their use of the SNMPv2 set operation. Используется как значение, которое ограничивает сверху Cisco-specific значения. Фактически является неформальным обозначением конца MIB-а. Служит для предотвращения возможных коллизий при отработке GET-NEXT операций. 0	SNMPv2-MIB
ciscoImageString	1.3.6.1.4.1.9.9.25.1.1.1.2.<i>	DisplayString	<The string of this entry.> (описание таблицы – <A table provides content information describing the executing IOS image.>). Выдаются данные для агента: 1: "CW_BEGIN$-csp-vpn$" 2: "CW_IMAGE$C2800NM$" 3: "CW_FAMILY$C2800 NM $" 4: "CW_FEATURE$IP|FIREWALL|PLUS|3DES|VPN|SSH|IPSEC$" 5: "CW_VERSION$12.4(13a)$" 6: "CW_MEDIA$RAM$" 7: "CW_SYSDESCR$S-Terra {Gate\|Server\|Client} <major>.<minor>.<build>, Emulation of: Cisco IOS Software, 2800 Software (C2800NM-ADVIPSERVICESK9-M), Version 12.4(13a), RELEASE SOFTWARE (fc1)$"" 8: "CW_MAGIC$$" 9: "CW_END$-csp-vpn$"	CISCO-IMAGE-MIB
dot1dBaseBridgeAddress	1.3.6.1.2.1.17.1.1.0	MacAddress	Используется при взаимодействии с устройствами Cisco. 00 00 00 00 00 00	BRIDGE-MIB
dot1dBaseNumPorts	1.3.6.1.2.1.17.1.2.0	int32	The number of ports controlled by this bridging entity. Используется при взаимодействии с устройствами Cisco. 0	BRIDGE-MIB

Название переменной	OID (идентификатор объекта)	Тип переменной	Значение переменной	MIB
dot1dBaseType	1.3.6.1.2.1.17.1.3.0	int32 { unknown (1) , transparent-only (2) , sourceroute-only (3) , srt (4) }	Используется при взаимодействии с устройствами Cisco. srt (4)	BRIDGE-MIB
Глобальная IKE-статистика				
cikeGlobalActiveTunnels	1.3.6.1.4.1.9.9.171.1.2.1.1.0	uint32	<The number of currently active IPsec Phase-1 IKE Tunnels> Все существующие на данный момент активные ISAKMP SA.	CISCO-IPSEC-FLOW-MONITOR-MIB
cikeGlobalPreviousTunnels	1.3.6.1.4.1.9.9.171.1.2.1.2.0	uint32	<The total number of previously active IPsec Phase-1 IKE Tunnels> Количество ISAKMP SA с момента старта Агента, которые были созданы, но уже не являются активными, либо удалены.	CISCO-IPSEC-FLOW-MONITOR-MIB
cikeGlobalInOctets	1.3.6.1.4.1.9.9.171.1.2.1.3.0	uint32	<The total number of octets received by all currently and previously active IPsec Phase-1 IKE Tunnels> Количество байт, принятых в течение всех IKE-сессий с момента старта Агента	CISCO-IPSEC-FLOW-MONITOR-MIB
cikeGlobalInPkts	1.3.6.1.4.1.9.9.171.1.2.1.4.0	uint32	<The total number of packets received by all currently and previously active IPsec Phase-1 IKE Tunnels> Количество ISAKMP-пакетов, принятых в течение всех IKE-сессий с момента старта Агента	CISCO-IPSEC-FLOW-MONITOR-MIB
cikeGlobalInDropPkts	1.3.6.1.4.1.9.9.171.1.2.1.5.0	uint32	<The total number of packets which were dropped during receive processing by all currently and previously active IPsec Phase-1 IKE Tunnels> Количество ISAKMP-пакетов, отвергнутых в течение всех IKE-сессий с момента старта Агента	CISCO-IPSEC-FLOW-MONITOR-MIB
cikeGlobalInP2Exchgs	1.3.6.1.4.1.9.9.171.1.2.1.7.0	uint32	<The total number of IPsec Phase-2 exchanges received by all currently and previously active IPsec Phase-1 IKE Tunnels> Количество успешных Quick Modes в качестве респондера.	CISCO-IPSEC-FLOW-MONITOR-MIB

Название переменной	OID (идентификатор объекта)	Тип переменной	Значение переменной	MIB
cikeGlobalInP2ExchgInvalids	1.3.6.1.4.1.9.9.171.1.2.1.8.0	uint32	<The total number of IPsec Phase-2 exchanges which were received and found to be invalid by all currently and previously active IPsec Phase-1 IKE Tunnels> Общее количество IKE-сессий по созданию IPsec соединений, инициированных партнёрами, не состоявшихся по причине ошибки обмена.	CISCO-IPSEC-FLOW-MONITOR-MIB
cikeGlobalInP2ExchgRejects	1.3.6.1.4.1.9.9.171.1.2.1.9.0	uint32	<The total number of IPsec Phase-2 exchanges which were received and rejected by all currently and previously active IPsec Phase-1 IKE Tunnels> Общее количество IKE-сессий по созданию IPsec соединений, инициированных партнёрами, которые не состоялись по причине рассогласования политик безопасности.	CISCO-IPSEC-FLOW-MONITOR-MIB
cikeGlobalOutOctets	1.3.6.1.4.1.9.9.171.1.2.1.11.0	uint32	<The total number of octets sent by all currently and previously active and IPsec Phase-1 IKE Tunnels> Количество байт, высланных в течение всех IKE-сессий с момента старта Агента	CISCO-IPSEC-FLOW-MONITOR-MIB
cikeGlobalOutPkts	1.3.6.1.4.1.9.9.171.1.2.1.12.0	uint32	<The total number of packets sent by all currently and previously active and IPsec Phase-1 Tunnels> Количество ISAKMP-пакетов, высланных в течение всех IKE-сессий с момента старта Агента	CISCO-IPSEC-FLOW-MONITOR-MIB
cikeGlobalOutDropPkts	1.3.6.1.4.1.9.9.171.1.2.1.13.0	uint32	<The total number of packets which were dropped during send processing by all currently and previously active IPsec Phase-1 IKE Tunnels> Количество ISAKMP-пакетов в течение всех IKE-сессий с момента старта Агента, которые были готовы к отсылке, но по каким-то причинам не были отосланы	CISCO-IPSEC-FLOW-MONITOR-MIB
cikeGlobalOutP2Exchgs	1.3.6.1.4.1.9.9.171.1.2.1.15.0	uint32	<The total number of IPsec Phase-2 exchanges which were sent by all currently and previously active IPsec Phase-1 IKE Tunnels> Количество успешных Quick Modes в качестве инициатора.	CISCO-IPSEC-FLOW-MONITOR-MIB

Название переменной	OID (идентификатор объекта)	Тип переменной	Значение переменной	MIB
cikeGlobalOutP2ExchgInvalids	1.3.6.1.4.1.9.9.171.1.2.1.16.0	uint32	<The total number of IPsec Phase-2 exchanges which were sent and found to be invalid by all currently and previously active IPsec Phase-1 Tunnels> Общее количество инициированных IKE-сессий по созданию IPsec соединений, не состоявшихся по причине ошибки обмена.	CISCO-IPSEC-FLOW-MONITOR-MIB
cikeGlobalOutP2ExchgRejects	1.3.6.1.4.1.9.9.171.1.2.1.17.0	uint32	<The total number of IPsec Phase-2 exchanges which were sent and rejected by all currently and previously active IPsec Phase-1 IKE Tunnels> Общее количество инициированных IKE-сессий по созданию IPsec соединений, не состоявшихся по причине рассогласования политик безопасности.	CISCO-IPSEC-FLOW-MONITOR-MIB
cikeGlobalInitTunnels	1.3.6.1.4.1.9.9.171.1.2.1.19.0	uint32	<The total number of IPsec Phase-1 IKE Tunnels which were locally initiated> Количество созданных ISAKMP SA в качестве инициатора (т.е. по инициативе локальной стороны).	CISCO-IPSEC-FLOW-MONITOR-MIB
cikeGlobalInitTunnelFails	1.3.6.1.4.1.9.9.171.1.2.1.20.0	uint32	<The total number of IPsec Phase-1 IKE Tunnels which were locally initiated and failed to activate> Количество инициированных сессий по созданию ISAKMP SA, завершившихся неудачей	CISCO-IPSEC-FLOW-MONITOR-MIB
cikeGlobalRespTunnelFails	1.3.6.1.4.1.9.9.171.1.2.1.21.0	uint32	<The total number of IPsec Phase-1 IKE Tunnels which were remotely initiated and failed to activate> Количество сессий по созданию ISAKMP SA, инициированных партнёрами, которые завершились неудачей	CISCO-IPSEC-FLOW-MONITOR-MIB
cikeGlobalAuthFails	1.3.6.1.4.1.9.9.171.1.2.1.23.0	uint32	<The total number of authentications which ended in failure by all current and previous IPsec Phase-1 IKE Tunnels> Количество неудачных сессий по созданию ISAKMP SA, в которых не прошла аутентификация	CISCO-IPSEC-FLOW-MONITOR-MIB
cikeGlobalDecryptFails	1.3.6.1.4.1.9.9.171.1.2.1.24.0	uint32	<The total number of decryptions which ended in failure by all current and previous IPsec Phase-1 IKE Tunnels> Общее количество IKE-сессий, не состоявшихся по причине ошибки расшифрования пакета.	CISCO-IPSEC-FLOW-MONITOR-MIB

Название переменной	OID (идентификатор объекта)	Тип переменной	Значение переменной	MIB
cikeGlobalHashValidFails	1.3.6.1.4.1.9.9.171.1.2.1.25.0	uint32	<The total number of hash validations which ended in failure by all current and previous IPsec Phase-1 IKE Tunnels> Количество неудачных операций по проверке значения хэш-функции во всех IKE сессиях	CISCO-IPSEC-FLOW-MONITOR-MIB
cikeGlobalNoSaFails	1.3.6.1.4.1.9.9.171.1.2.1.26.0	uint32	<The total number of non-existent Security Association in failures which occurred during processing of all current and previous IPsec Phase-1 IKE Tunnels> Общее количество IKE-сессий, не состоявшихся по причине отсутствия ISAKMP соединения.	CISCO-IPSEC-FLOW-MONITOR-MIB
Глобальная IPsec-статистика				
cipSecGlobalActiveTunnels	1.3.6.1.4.1.9.9.171.1.3.1.1.0	uint32	<The total number of currently active IPsec Phase-2 Tunnels> Количество существующих на данный момент IPsec соединений. Период обновления всех переменных этого раздела (**Глобальная IPsec-статистика)** – 1 секунда. Поэтому, после изменения значения переменной в течение 1 секунды на компьютере может выдаваться устаревшее значение.	CISCO-IPSEC-FLOW-MONITOR-MIB
cipSecGlobalPreviousTunnels	1.3.6.1.4.1.9.9.171.1.3.1.2.0	uint32	<The total number of previously active IPsec Phase-2 Tunnels> Количество IPsec SA с момента старта Агента, которые были созданы, но уже не являются активными, либо удалены.	CISCO-IPSEC-FLOW-MONITOR-MIB
cipSecGlobalInOctets	1.3.6.1.4.1.9.9.171.1.3.1.3.0	uint32	<The total number of octets received by all current and previous IPsec Phase-2 Tunnels. This value is accumulated BEFORE determining whether or not the packet should be decompressed. See also cipSecGlobalInOctWraps for the number of times this counter has wrapped> Количество байт, принятых под защитой всех IPsec SA с момента старта Агента	CISCO-IPSEC-FLOW-MONITOR-MIB
cipSecGlobalInOctWraps	1.3.6.1.4.1.9.9.171.1.3.1.5.0	uint32	<The number of times the global octets received counter (cipSecGlobalInOctets) has wrapped> Количество переполнений счетчика cipSecGlobalInOctets.	CISCO-IPSEC-FLOW-MONITOR-MIB

Название переменной	OID (идентификатор объекта)	Тип переменной	Значение переменной	MIB
cipSecGlobalInPkts	1.3.6.1.4.1.9.9.171.1.3.1.9.0	uint32	<The total number of packets received by all current and previous IPsec Phase-2 Tunnels> Количество пакетов, принятых под защитой всех IPsec SA с момента старта Агента	CISCO-IPSEC-FLOW-MONITOR-MIB
cipSecGlobalInDrops	1.3.6.1.4.1.9.9.171.1.3.1.10.0	uint32	<The total number of packets dropped during receive processing by all current and previous IPsec Phase-2 Tunnels. This count does NOT include packets dropped due to Anti-Replay processing> Общее количество всех входящих пакетов, отвергнутых локальным устройством, при задействовании IPsec соединения (Кроме проигнорированных по Anti-Replay).	CISCO-IPSEC-FLOW-MONITOR-MIB
cipSecGlobalInReplayDrops	1.3.6.1.4.1.9.9.171.1.3.1.11.0	uint32	<The total number of packets dropped during receive processing due to Anti-Replay processing by all current and previous IPsec Phase-2 Tunnels> Общее количество всех входящих пакетов, отвергнутых локальным устройством посредством механизма Anti-Replay, при задействовании IPsec соединения.	CISCO-IPSEC-FLOW-MONITOR-MIB
cipSecGlobalInAuthFails	1.3.6.1.4.1.9.9.171.1.3.1.13.0	uint32	<The total number of inbound authentication's which ended in failure by all current and previous IPsec Phase-2 Tunnels> Общее количество всех неудачных входящих аутентификаций по IPsec соединениям.	CISCO-IPSEC-FLOW-MONITOR-MIB
cipSecGlobalInDecrypts	1.3.6.1.4.1.9.9.171.1.3.1.14.0	uint32	<The total number of inbound decryption's performed by all current and previous IPsec Phase-2 Tunnels> То же самое значение, что и cipSecGlobalInPkts. Общее количество входящих пакетов, которые были расшифрованы всеми IPsec соединениями.	CISCO-IPSEC-FLOW-MONITOR-MIB
cipSecGlobalInDecryptFails	1.3.6.1.4.1.9.9.171.1.3.1.15.0	uint32	<The total number of inbound decryption's which ended in failure by all current and previous IPsec Phase-2 Tunnels> Общее количество входящих пакетов, которые были неудачно расшифрованы IPsec соединениями.	CISCO-IPSEC-FLOW-MONITOR-MIB

Название переменной	OID (идентификатор объекта)	Тип переменной	Значение переменной	MIB
cipSecGlobalOutOctets	1.3.6.1.4.1.9.9.171.1.3.1.16.0	uint32	<The total number of octets sent by all current and pre-vious IPsec Phase-2 Tunnels. This value is accumulated AFTER determining whether or not the packet should be compressed. See also cipSecGlobalOutOctWraps for the number of times this counter has wrapped> Количество байт, отосланных под защитой всех IPsec SA с момента старта Агента	CISCO-IPSEC-FLOW-MONITOR-MIB
cipSecGlobalOutOctWraps	1.3.6.1.4.1.9.9.171.1.3.1.18.0	uint32	<The number of times the global octets sent counter (cipSecGlobalOutOctets) has wrapped> Количество переполнений счетчика cipSecGlobalOutOctets.	CISCO-IPSEC-FLOW-MONITOR-MIB
cipSecGlobalOutPkts	1.3.6.1.4.1.9.9.171.1.3.1.22.0	uint32	<The total number of packets sent by all current and previous IPsec Phase-2 Tunnels> Количество пакетов, отосланных под защитой всех IPsec SA с момента старта Агента	CISCO-IPSEC-FLOW-MONITOR-MIB
cipSecGlobalOutDrops	1.3.6.1.4.1.9.9.171.1.3.1.23.0	uint32	<The total number of packets dropped during send processing by all current and previous IPsec Phase-2 Tunnels> Общее количество всех исходящих пакетов, отвергнутых локальным устройством, при задействовании IPsec соединения.	CISCO-IPSEC-FLOW-MONITOR-MIB
cipSecGlobalOutAuthFails	1.3.6.1.4.1.9.9.171.1.3.1.25.0	uint32	<The total number of outbound authentication's which ended in failure by all current and previous IPsec Phase-2 Tunnels> Общее количество всех неудачных исходящих аутентификаций по IPsec соединениям.	CISCO-IPSEC-FLOW-MONITOR-MIB
cipSecGlobalOutEncrypts	1.3.6.1.4.1.9.9.171.1.3.1.26.0	uint32	<The total number of outbound encryption's performed by all current and previous IPsec Phase-2 Tunnels> Тоже самое значение, что и cipSecGlobalOutPkts. Общее количество исходящих пакетов, которые были зашифрованы всеми IPsec соединениями.	CISCO-IPSEC-FLOW-MONITOR-MIB
cipSecGlobalOutEncryptFails	1.3.6.1.4.1.9.9.171.1.3.1.27.0	uint32	<The total number of outbound encryption's which ended in failure by all current and previous IPsec Phase-2 Tunnels> Общее количество исходящих пакетов, которые были неудачно зашифрованы IPsec соединениями.	CISCO-IPSEC-FLOW-MONITOR-MIB

Название переменной	OID (идентификатор объекта)	Тип переменной	Значение переменной	MIB
cipSecGlobalNoSaFails	1.3.6.1.4.1.9.9.171.1.3.1.29.0	uint32	<The total number of non-existent Security Association in failures which occurred during processing of all current and previous IPsec Phase-2 Tunnels> Общее количество обменов, не состоявшихся по причине отсутствия IPsec соединения.	CISCO-IPSEC-FLOW-MONITOR-MIB
Статистика по сетевым интерфейсам				
ifPhysAddress	1.3.6.1.2.1.2.2.1.6.<ifIndex>	Octet string	<The interface's address at the protocol layer immediately `below' the network layer in the protocol stack. For interfaces which do not have such an address (e.g., a serial line), this object should contain an octet string of zero length.> MAC-адрес данного интерфейса. Индекс для данного значения берется из ipAdEntIfIndex.<ip>	RFC1213-MIB
ifIndex	1.3.6.1.2.1.2.2.1.1.<ifIndex>	int32	<A unique value for each interface. Its value ranges between 1 and the value of ifNumber. The value for each interface must remain constant at least from one re-initialization of the entity's network management system to the next re-initialization> ifIndex – индекс интерфейса, значение лежит в диапазоне от 1 до ifNumber (ifNumber - число сетевых интерфейсов)	RFC1213-MIB
ipAdEntAddr	1.3.6.1.2.1.4.20.1.1.<ip>	IpAddress	<The IP address to which this entry's addressing information pertains.> Собственно сам <ip> (совпадает с индексом значения)	IP-MIB
ipAdEntNetMask	1.3.6.1.2.1.4.20.1.3.<ip>	IpAddress	<The subnet mask associated with the IP address of this entry. The value of the mask is an IP address with all the network bits set to 1 and all the hosts bits set to 0.> Маска адреса.	IP-MIB

Название переменной	OID (идентификатор объекта)	Тип переменной	Значение переменной	MIB
ipAdEntIfIndex	1.3.6.1.2.1.4.20.1.2.<ip>	int32	<The index value which uniquely identifies the interface to which this entry is applicable. The interface identified by a particular value of this index is the same interface as identified by the same value of RFC 1573's ifIndex.> Индексом переменной является IP-адрес устройства. Значением – индекс интерфейса (в таблице ifTable), который содержит данный адрес. Период обновления всех переменных этого раздела (**Статистика по сетевым интерфейсам)** – 5 секунд. Поэтому, после изменения значения переменной в течение 5 секунд на компьютере может выдаваться устаревшее значение.	IP-MIB
CPU (загрузка процессора), Memory – статистика				
cpmCPUTotal5sec	1.3.6.1.4.1.9.9.109.1.1.1.1.3.1	uint32 (1..100)	<The overall CPU busy percentage in the last 5 second period. This object obsoletes the busyPer object from the OLD-CISCO-SYSTEM-MIB. This object is deprecated by cpmCPUTotal5secRev which has the changed range of value (0..100).> Загрузка процессора за последние 5 секунд (в процентах).	CISCO-PROCESS-MIB
cpmCPUTotal5secRev	1.3.6.1.4.1.9.9.109.1.1.1.1.6.1	uint32 (0..100)	<The overall CPU busy percentage in the last 5 second period. This object deprecates the object cpmCPUTotal5sec and increases the value range to (0..100). This object is deprecated by cpmCPUTotalMonInterval> Загрузка процессора за последние 5 секунд. Отличается от cpmCPUTotal5sec допустимыми пределами.	CISCO-PROCESS-MIB
cpmCPUTotal1min	1.3.6.1.4.1.9.9.109.1.1.1.1.4.1	uint32 (1..100)	<The overall CPU busy percentage in the last 1 minute period. This object obsoletes the avgBusy1 object from the OLD-CISCO-SYSTEM-MIB. This object is deprecated by cpmCPUTotal1minRev which has the changed range of value (0..100).> Загрузка процессора за последнюю минуту. Отличается от cpmCPUTotal1minRev допустимыми пределами.	CISCO-PROCESS-MIB

Название переменной	OID (идентификатор объекта)	Тип переменной	Значение переменной	MIB
cpmCPUTotal1minRev	1.3.6.1.4.1.9.9.109.1.1.1.1.7.1	uint32 (0..100)	<The overall CPU busy percentage in the last 1 minute period. This object deprecates the object cpmCPUTotal1min and increases the value range to (0..100).> Загрузка процессора за последнюю минуту. Отличается от cpmCPUTotal1min допустимыми пределами.	CISCO-PROCESS-MIB
cpmCPUTotal5min	1.3.6.1.4.1.9.9.109.1.1.1.1.5.1	uint32 (1..100)	<The overall CPU busy percentage in the last 5 minute period. This object deprecates the avgBusy5 object from the OLD-CISCO-SYSTEM-MIB. This object is deprecated by cpmCPUTotal5minRev which has the changed range of value (0..100).> Средняя загрузка процессора за последние 5 минут (в процентах).	CISCO-PROCESS-MIB
cpmCPUTotal5minRev	1.3.6.1.4.1.9.9.109.1.1.1.1.8.1	uint32 (0..100)	<The overall CPU busy percentage in the last 5 minute period. This object deprecates the object cpmCPUTotal5min and increases the value range to (0..100).> Загрузка процессора за последние 5 минут. Отличается от cpmCPUTotal5min допустимыми пределами.	CISCO-PROCESS-MIB
busyPer	1.3.6.1.4.1.9.2.1.56.0	int32 (0..100)	<CPU busy percentage in the last 5 second period. Not the last 5 realtime seconds but the last 5 second period in the scheduler.> Загрузка процессора за последние 5 секунд. Аналогично cpmCPUTotal5secRev, за исключением типа переменной. Примечание: данное поведение отличается от Cisco IOS – там указанные значения могут различаться. Значение, выдаваемое агентом, зависит от ОС и немного отличается по смыслу от обоих значений Cisco IOS.	OLD-CISCO-CPU-MIB
ciscoMemoryPoolUsed	1.3.6.1.4.1.9.9.48.1.1.1.5.1	uint32	<Indicates the number of bytes from the memory pool that are currently in use by applications on the managed device.> Рассматривается как таблица из одного элемента (с индексом 1), которая задает общее количество используемой физической памяти.	CISCO-MEMORY-POOL-MIB

Название переменной	OID (идентификатор объекта)	Тип переменной	Значение переменной	MIB
ciscoMemoryPoolFree	1.3.6.1.4.1.9.9.48.1.1.1.6.1	uint32	<Indicates the number of bytes from the memory pool that are currently unused on the managed device. Note that the sum of ciscoMemoryPoolUsed and ciscoMemoryPoolFree is the total amount of memory in the pool> Общее количество свободной физической памяти.	CISCO-MEMORY-POOL-MIB

3.2 Трап-сообщения

SNMP-агент посылает трап-сообщения о возникших событиях SNMP-менеджеру.

В приведенной ниже таблице перечислены реализованные трапы и переменные, которые высылаются SNMP-менеджеру, и описание трапа.

Таблица 9

Название трапа	SNMPv1 Enterprise and Specific Type; SNMPv2 OID	Список переменных	Значение переменной	MIB
cikeSysFailure	1.3.6.1.4.1.9.9.171.2 3 1.3.6.1.4.1.9.9.171.2.0.3	cikePeerLocalAddr – адрес local peer cikePeerRemoteAddr – адрес remote peer Оба значения – табличные.	<This notification is generated when the processing for an IPsec Phase-1 IKE Tunnel experiences an internal or system capacity error.> Сигнализация о внутренней ошибке или исчерпании ресурсов при обработке IKE.	CISCO-IPSEC-FLOW-MONITOR-MIB
cikeCertCrlFailure	1.3.6.1.4.1.9.9.171.2 4 1.3.6.1.4.1.9.9.171.2.0.4	cikePeerLocalAddr cikePeerRemoteAddr	<This notification is generated when the processing for an IPsec Phase-1 IKE Tunnel experiences a Certificate or a Certificate Revoke List (CRL) related error.> Ошибка, связанная с сертификатами или CRL.	CISCO-IPSEC-FLOW-MONITOR-MIB
cikeProtocolFailure	1.3.6.1.4.1.9.9.171.2 5 1.3.6.1.4.1.9.9.171.2.0.5	cikePeerLocalAddr cikePeerRemoteAddr	<This notification is generated when the processing for an IPsec Phase-1 IKE Tunnel experiences a protocol related error.> Ошибка, связанная с обработкой протокола IKE: • Authentication error (в ситуациях, не попадающих под cikeCertCrlFailure) • BlackLog	CISCO-IPSEC-FLOW-MONITOR-MIB
cikeNoSa	1.3.6.1.4.1.9.9.171.2 6 1.3.6.1.4.1.9.9.171.2.0.6	cikePeerLocalAddr cikePeerRemoteAddr	<This notification is generated when the processing for an IPsec Phase-1 IKE Tunnel experiences a non-existent security association error.> Приход IKE-пакетов на несуществующий SA (Invalid cookie).	CISCO-IPSEC-FLOW-MONITOR-MIB

Название трапа	SNMPv1 Enterprise and Specific Type; SNMPv2 OID	Список переменных	Значение переменной	MIB
cipSecSetUpFailure	1.3.6.1.4.1.9.9.171.2 10 1.3.6.1.4.1.9.9.171.2.0.10	cikePeerLocalAddr cikePeerRemoteAddr	<This notification is generated when the setup for an IPsec Phase-2 Tunnel fails.> По тем или иным причинам не удалось создать IPsec SA (при существующем IKE SA). Примечание: этот трап отсылается только при появлении ошибки во время проведения IKE-сессии и тем партнером, на котором случилась ошибка. Если создание соединения прекращено по другим причинам – остановка сервиса, перезагрузка LSP, delete payload, получение нотификации о том, что партнер по своей инициативе прекратил создание соединения, timeout и др., то локальное устройство трап не отсылает. В этом состоит отличие нашего агента от IOS, где трапы отсылаются с обоих партнеров при любой неуспешной сессии по созданию IPsec соединения.	CISCO-IPSEC-FLOW-MONITOR-MIB
cipSecTunnelStart	1.3.6.1.4.1.9.9.171.2 7 1.3.6.1.4.1.9.9.171.2.0.7	cipSecTunLifeTime cipSecTunLifeSize Табличные значения.	<This notification is generated when an IPsec Phase-2 Tunnel becomes active.> Успешное создание туннеля.	CISCO-IPSEC-FLOW-MONITOR-MIB
cipSecTunnelStop	1.3.6.1.4.1.9.9.171.2 8 1.3.6.1.4.1.9.9.171.2.0.8	cipSecTunActiveTime Табличное значение	<This notification is generated when an IPsec Phase-2 Tunnel becomes inactive.> Уничтожение созданного туннеля (по разным причинам).	CISCO-IPSEC-FLOW-MONITOR-MIB
cipsTooManySAs	1.3.6.1.4.1.9.10.62.2 7 1.3.6.1.4.1.9.10.62.2.0.7	cipsMaxSAs – максимальное количество IPsec SAs. Если не существует предела – 0.	<This trap is generated when a new SA is attempted to be setup while the number of currently active SAs equals the maximum configurable. The variables are: cipsMaxSAs> Отказ от создания SA по причине достигнутого максимального количества SA, указанного в лицензии. В переменной прописывается максимальное количество SA из лицензии.	CISCO-IPSEC-MIB

Название трапа	SNMPv1 Enterprise and Specific Type; SNMPv2 OID	Список переменных	Значение переменной	MIB
ciscoConfigManEvent	1.3.6.1.4.1.9.9.43.2 1 1.3.6.1.4.1.9.9.43.2.0.1	ccmHistoryEventCommandSource = { commandLine(1), snmp(2) } ccmHistoryEventConfigSource = { erase(1), commandSource(2), running(3), startup(4), local(5), networkTftp(6), networkRcp(7) } ccmHistoryEventConfigDestination = { erase(1), commandSource(2), running(3), startup(4), local(5), networkTftp(6), networkRcp(7) } Табличные значения. Индекс – целое число, начинающееся с единицы. Инкрементируется при каждой посылке трапа данного типа.	<Notification of a configuration management event as recorded in ccmHistoryEventTable.> Всегда ccmHistoryEventCommandSource=1 Несколько вариантов: 1 При вызове lsp_mgr show или cs_console show run: ccmHistoryEventConfigSource=2 ccmHistoryEventConfigDestination=2 Примечание: аналогично реакции Cisco на команду show run 2 При успешной прогрузке LSP: ccmHistoryEventConfigSource=2 ccmHistoryEventConfigDestination=3 Примечание: аналогично реакции Cisco на команду configure terminal. Для стартовой загрузки LSP надо задать ccmHistoryEventConfigSource = 4 3 При отгрузке LSP (по разным причинам): ccmHistoryEventConfigSource=1 ccmHistoryEventConfigDestination=3	CISCO-CONFIG-MAN-MIB

4. Получение сертификата пользователя

Независимо от используемой криптобиблиотеки, формирование ключей электронной подписи можно выполнить как с применением ПО «КриптоПро УЦ» (централизованно), так и с использованием сертифицированного СКЗИ «КриптоПро CSP», создав свой Удостоверяющий центр при помощи Microsoft Certification Authority.

Примечание: если в С-Терра Клиент используется криптографическая библиотека компании «С-Терра СиЭсПи, то при централизованном получении ключевой пары и локального сертификата, полученный контейнер необходимо конвертировать в соответствующий формат утилитой cpkey_conv, которая описана в «Руководстве пользователя» в разделе «Специализированные команды».

Далее в данном документе будет рассмотрен вариант получения сертификата пользователя с использованием своего Удостоверяющего центра.

Действия по созданию сертификата пользователя зависят от того, какую криптобиблиотеку использует С-Терра Клиент:

- если использует СКЗИ «КриптоПро CSP», то генерация ключевой пары, запрос и получение сертификата выполняется непосредственно на самом Удостоверяющем центре;
- при использовании криптобиблиотеки «С-Терра СиЭсПи», генерация ключевой пары и запроса на сертификат выполняется при помощи утилиты cont_mgr. Затем, подготовленный запрос на сертификат отправляется в Удостоверяющий центр, созданный с использованием СКЗИ «КриптоПро CSP» и Microsoft Certification Authority.

Независимо от используемой криптобиблиотеки, для создания своего Удостоверяющего центра Вам потребуется отдельный компьютер с установленными СКЗИ «КриптоПро CSP» и например, ОС Windows Server 2008 R2. Далее настройте КриптоПро CSP и УЦ. Затем в зависимости от криптобиблиотеки перейдите соответствующие разделы для создания сертификата пользователя.

Далее описаны:

- настройка СКЗИ «КриптоПро CSP»;
- установка и настройка Удостоверяющего центра;
- создание сертификата пользователя с использованием СКЗИ «КриптоПро CSP»;
- создание сертификата пользователя с использованием криптобиблиотеки «С-Терра».

4.1 Установка СКЗИ «КриптоПро CSP»

При выполнении процедуры инсталляции СКЗИ «КриптоПро CSP» выберите:

вид установки – ***Выборочная***

компоненты программы, которые необходимо установить – ***Криптопровайдер уровня ядра ОС.***

4.2 Настройка СКЗИ «КриптоПро CSP»

Если в Продукте S-Terra Client аутентификация пользователя осуществляется с использованием сертификатов, необходимо провести некоторые настройки в СКЗИ «КриптоПро CSP».

Для хранения секретного ключа сертификата пользователя используется контейнер, который может быть защищен паролем. Контейнер размещается:

- либо на внешнем ключевом носителе, который должен находиться только у пользователя,
- либо на локальном ключевом носителе (Реестре) на компьютере пользователя.

СКЗИ «КриптоПро CSP» умеет считывать секретный ключ из контейнера на внешнем ключевом носителе и на локальном ключевом носителе.

Также настраивается и ДСЧ – выбирается биологический или аппаратный ДСЧ, описан в разделе «Настройка ДСЧ».

При использовании криптобиблиотеки «С-Терра СиЭсПи» инсталлируйте только ключевой считыватель Реестр, описанный в разделе «Инсталляция ключевого считывателя Реестр в «КриптоПро CSP», и настройте ДСЧ. Затем перейдите к созданию УЦ.

4.2.1 Настройка локального ключевого считывателя

Если контейнер надо разместить в Реестре, то инсталлируйте считыватель Реестр, если он не был зарегистрирован во время инсталляции СКЗИ. Инсталляция считывателя описана в разделе «Инсталляция ключевого считывателя Реестр в «КриптоПро CSP».

4.2.2 Подключение внешних ключевых считывателей

Если контейнер будет сохранен на внешнем ключевом носителе, то сначала подключите внешний ключевой считыватель к компьютеру, следуя прилагаемой инструкции (Но, eToken до установки драйверов подключать не следует).

Установите все необходимые файлы и драйвера для работы внешнего считывателя. Например, для работы с электронными ключами eToken PRO, eToken NG-OTP, eToken NG-FLASH, eToken PRO 72K(Java) набор драйверов и утилит "eToken PKI Client 5.1 SP1 для Microsoft Windows" можно взять с web-страницы http://www.aladdin-rd.ru/support/download/177/.

Далее перейдите к настройке внешнего считывателя.

4.2.3 Настройка внешнего ключевого считывателя и носителя информации

В состав дистрибутива СКЗИ «КриптоПро CSP» входят драйвера, обеспечивающие взаимодействие внешних ключевых считывателей с «КриптоПро CSP».

После установки «КриптоПро CSP» сразу же инсталлированы все считыватели смарт-карт и все съемные диски, если была выполнена их регистрация при инсталляции СКЗИ. В противном случае, выполните инсталляцию считывателя, описанную в разделе «Инсталляция внешнего ключевого считывателя в «КриптоПро CSP». Для токена надо выбрать один из считывателей. После установки «КриптоПро CSP» инсталляция внешних носителей уже выполнена.

4.2.4 Инсталляция ключевого считывателя Реестр в «КриптоПро CSP»

Для инсталляции локального ключевого считывателя Реестр выполните следующие действия:

Шаг 1: запустите КриптоПро CSP: `Пуск – Настройка – Панель управления – КриптоПро CSP`

Шаг 2: в ОС Windows 7 (и более поздних ОС Windows) в появившемся окне КриптоПро CSP во вкладке `Общие` выберите предложение «`Запустить с правами администратора`» (Рисунок 1).

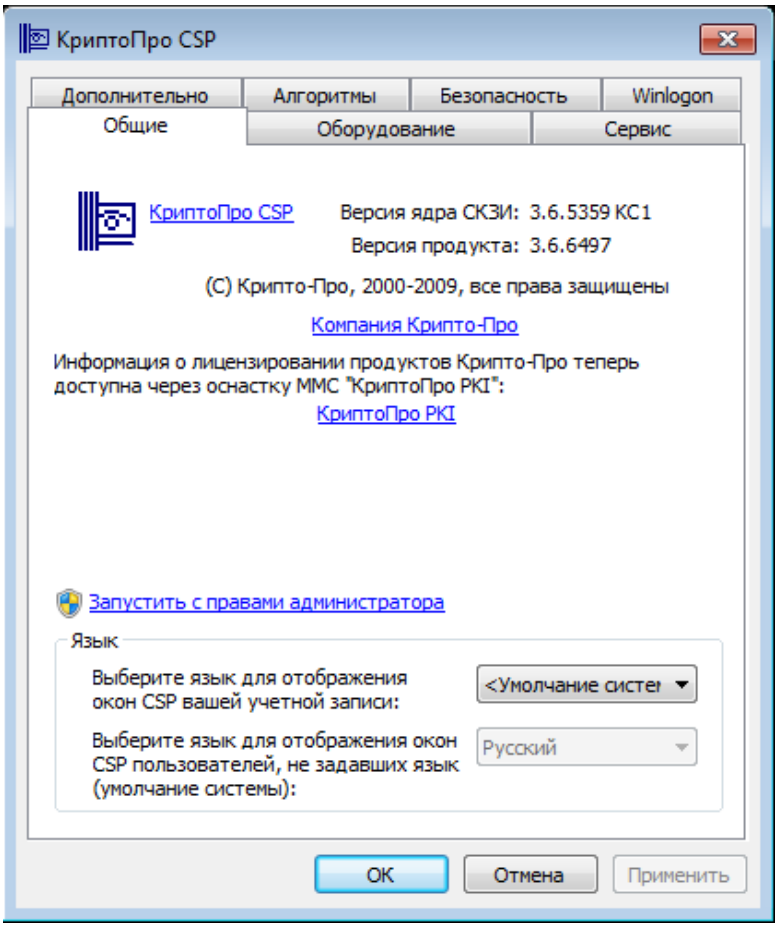

Рисунок 1

Шаг 3: войдите во вкладку `Оборудование` и нажмите кнопку `Настроить считыватели...`:

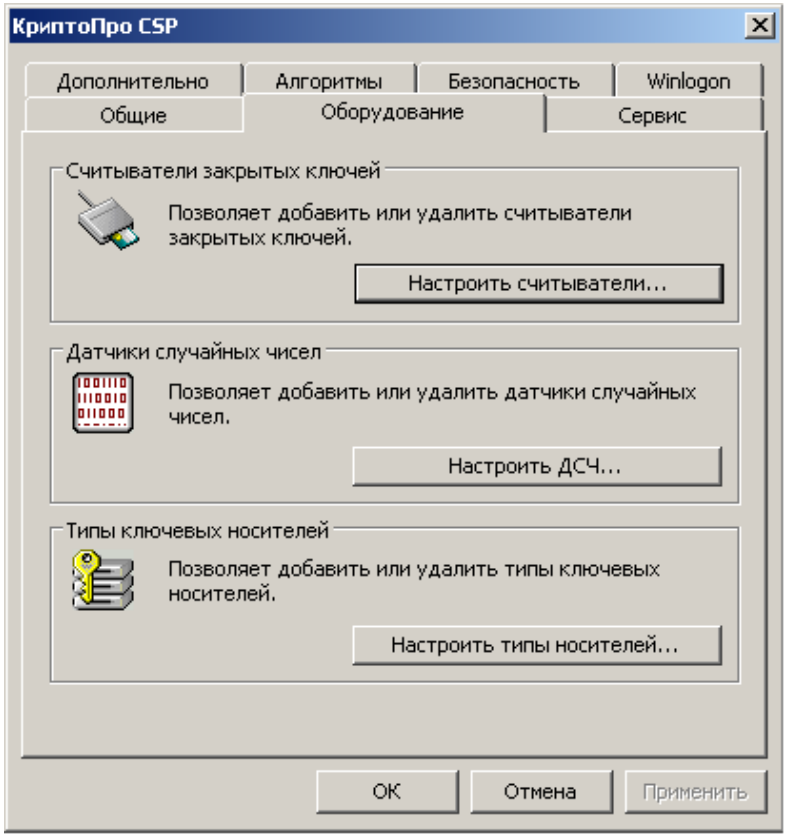

Рисунок 2

Шаг 4: нажмите кнопку `Добавить...`, чтобы установить новый ключевой считыватель:

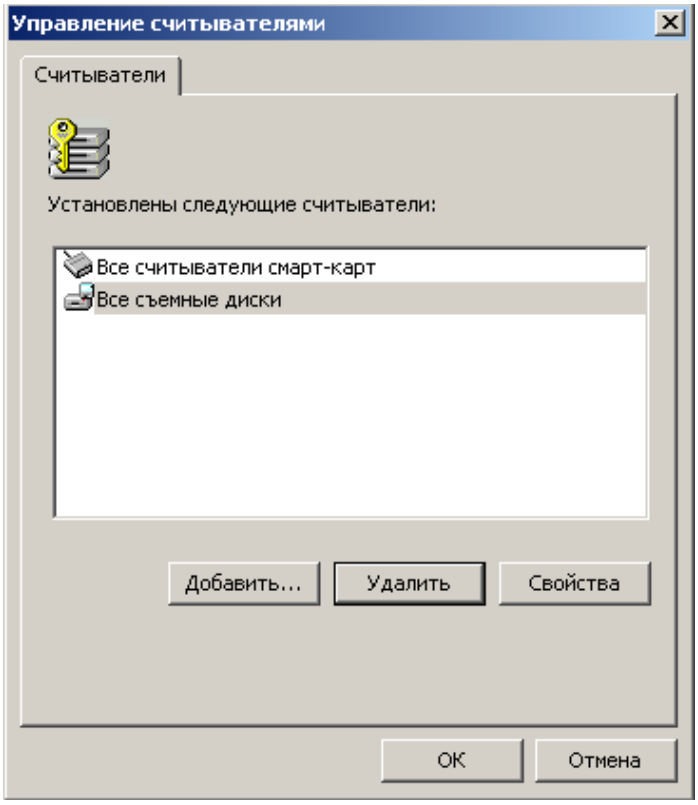

Рисунок 3

Шаг 5: в окне визарда нажмите кнопку `Далее`:

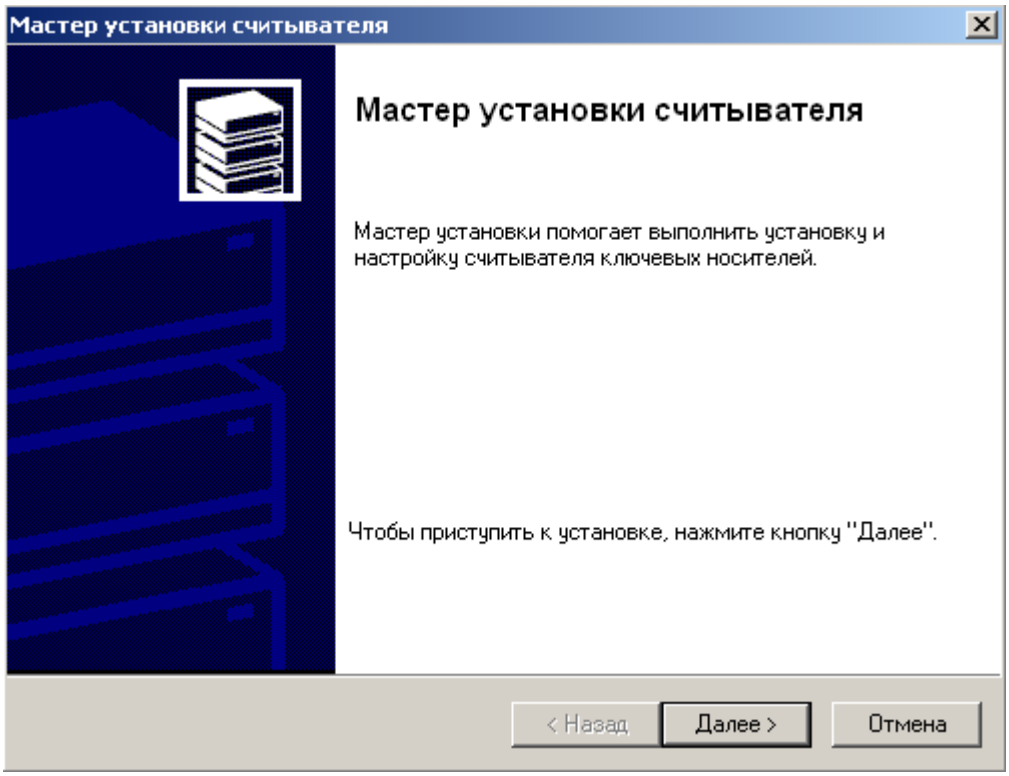

Рисунок 4

Шаг 6: из представленного списка выберите считыватель `Реестр` и нажмите кнопку `Далее`:

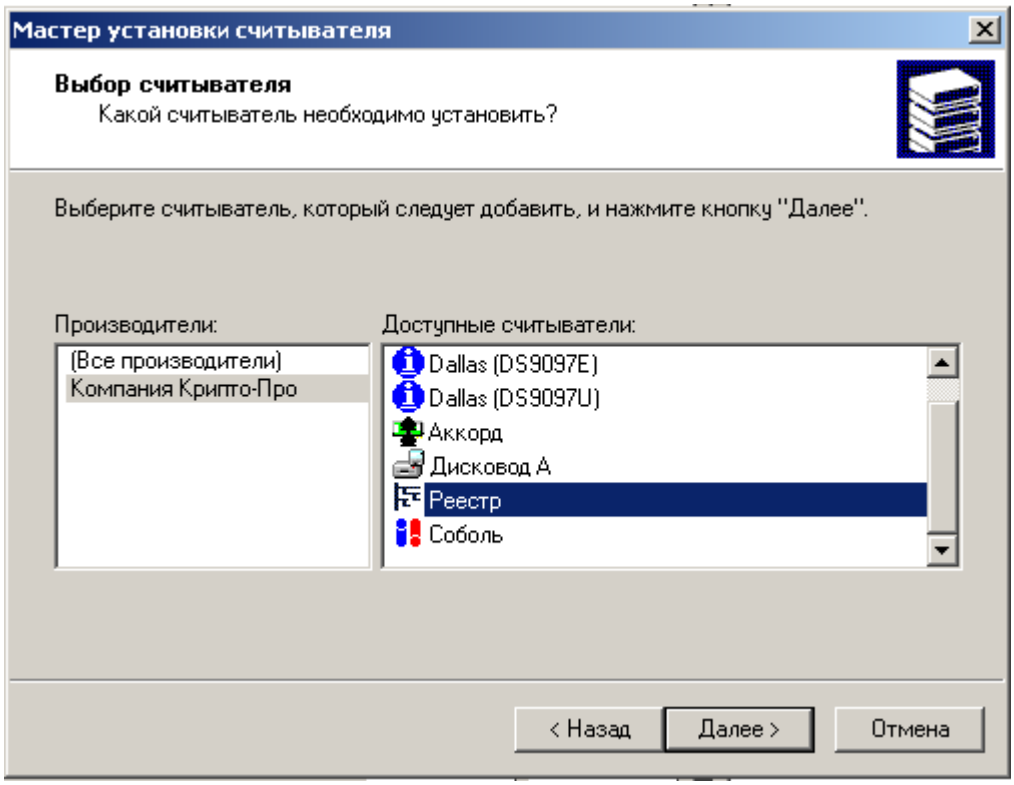

Рисунок 5

Шаг 7: считывателю `Реестр` можно присвоить имя и нажать кнопку `Далее`:

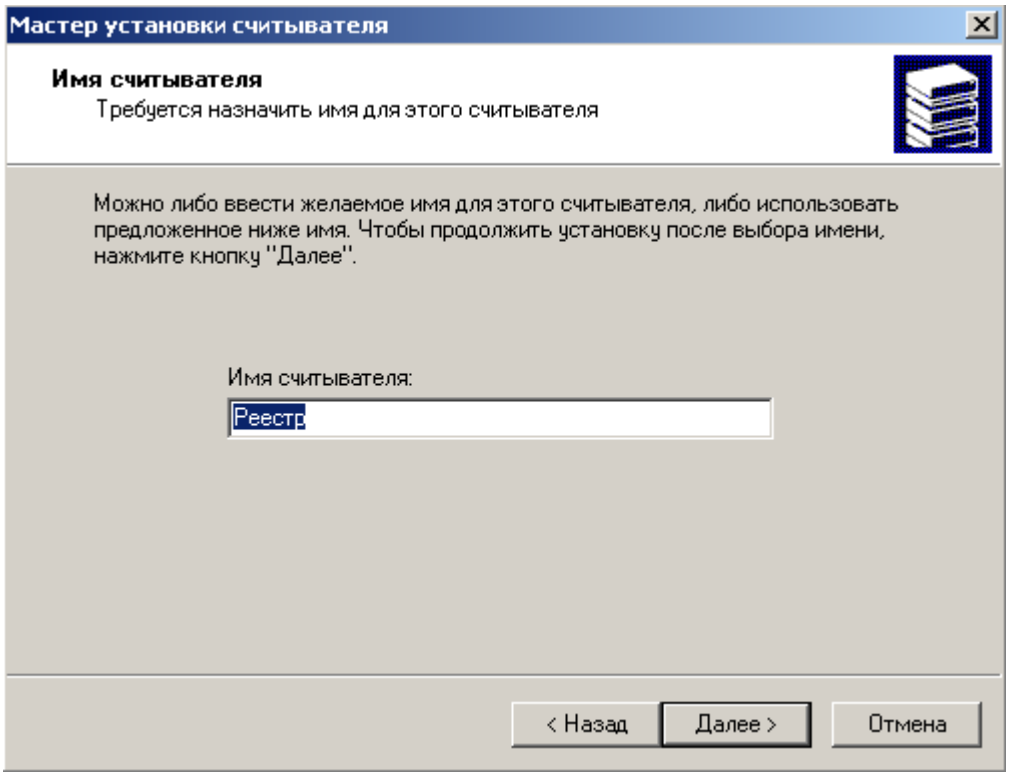

Рисунок 6

Шаг 8: инсталляция считывателя `Реестр` завершена, нажмите `Готово`:

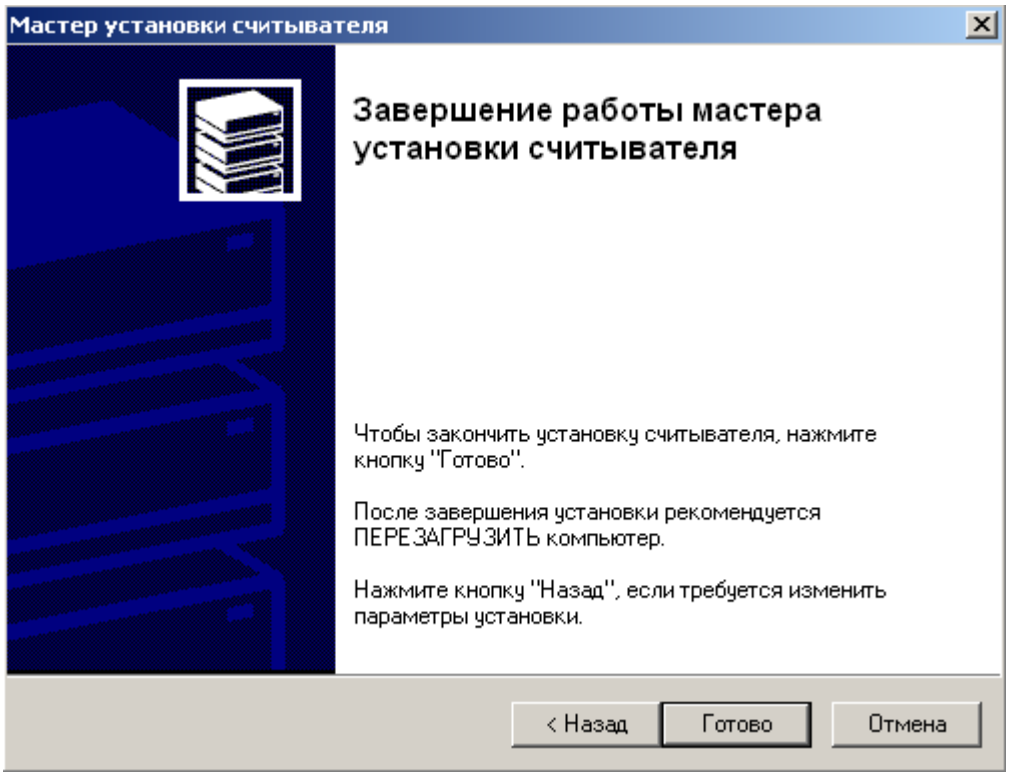

Рисунок 7

Шаг 9: считыватель `Реестр` добавлен в список инсталлированных считывателей, нажмите `OK`:

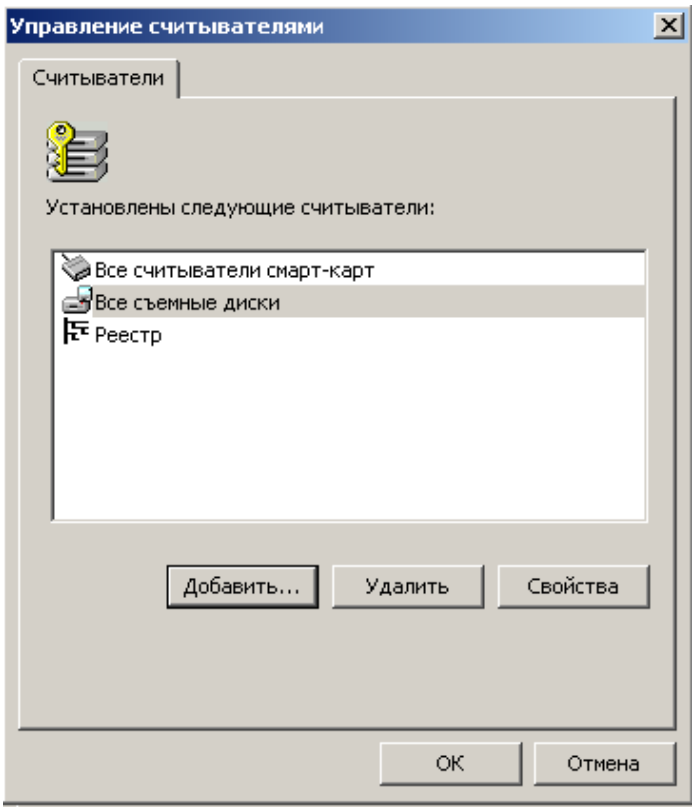

Рисунок 8

Шаг 10: перезагрузите компьютер.

4.2.5 Инсталляция внешнего считывателя и ключевого носителя информации в «КриптоПро CSP»

Инсталляция внешних считывателей выполняется так же как и для Реестра «Инсталляция ключевого считывателя Реестр в «КриптоПро CSP».

Во вкладке `Оборудование` нажмите кнопку `Настроить считыватели` (Рисунок 9) и выберите нужный считыватель. Далее следуйте описанию предыдущего раздела.

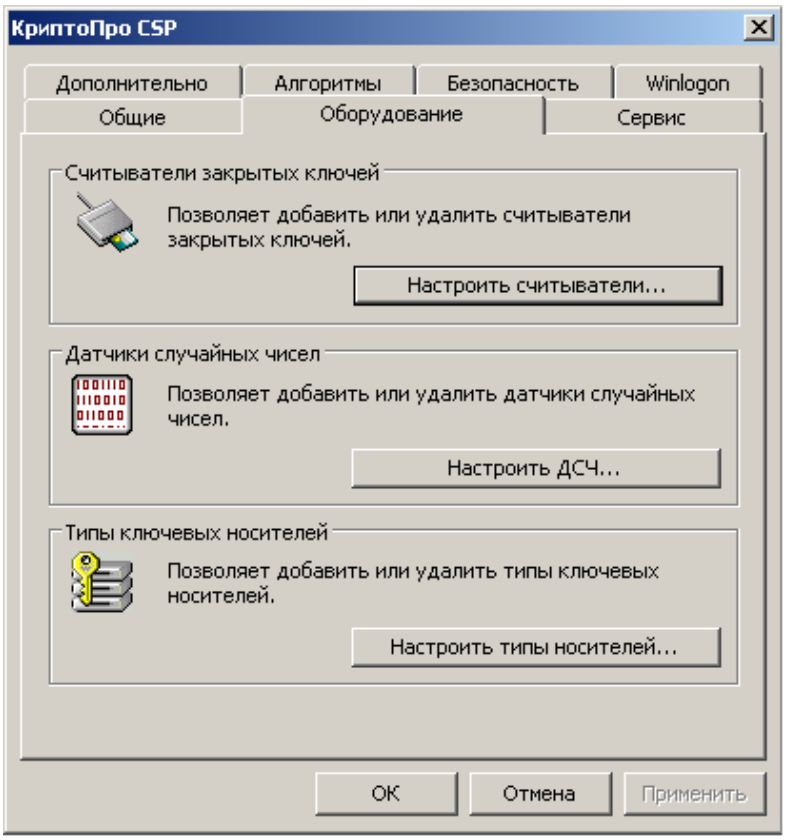

Рисунок 9

Для токена надо выбрать один из считывателей (Рисунок 10).

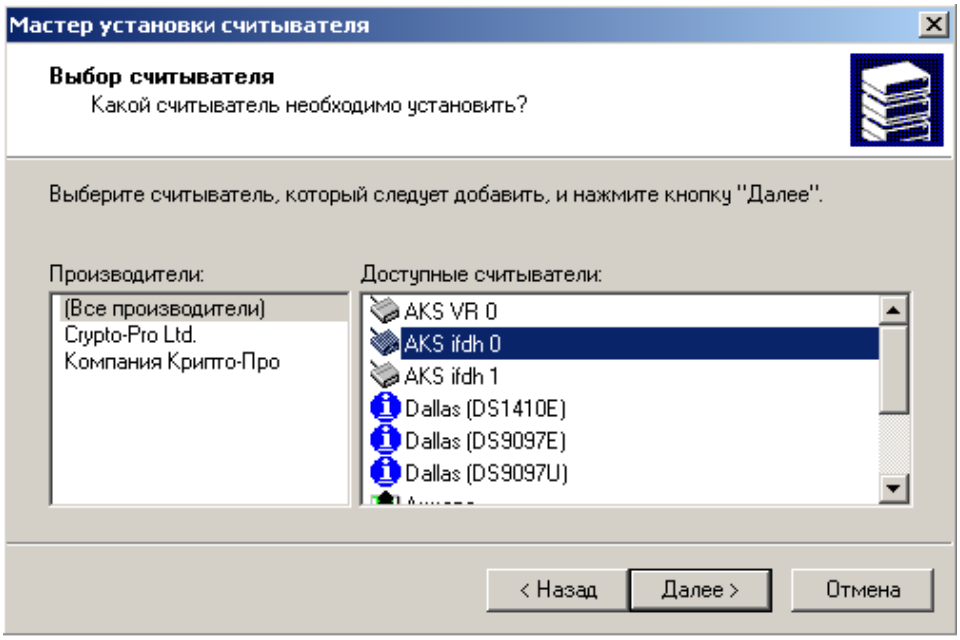

Рисунок 10

Все установленные ключевые носители можно посмотреть в открывшемся окне при нажатии на кнопку `Настроить типы носителей` (Рисунок 9).

Для добавления отсутствующего носителя нажмите кнопку `Добавить...` (Рисунок 11).

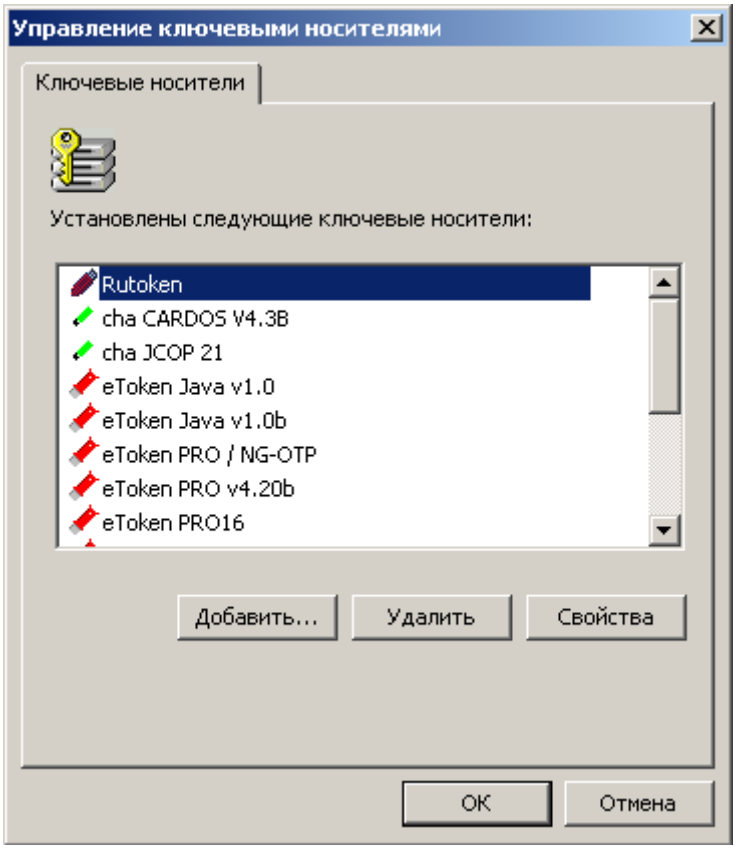

Рисунок 11

Далее следуйте указаниям Мастера установки ключевого носителя. По завершению инсталляции настройка внешнего ключевого носителя и считывателя полностью выполнена.

4.2.6 Настройка ДСЧ

В режиме защиты КС1 ПК от НСД используется биологический ДСЧ. В режиме защиты КС2 – используется ПАК «Соболь» или «Аккорд-АМДЗ».

Шаг 1: во вкладке `Оборудование` нажмите кнопку `Настроить ДСЧ...`: (Рисунок 12).

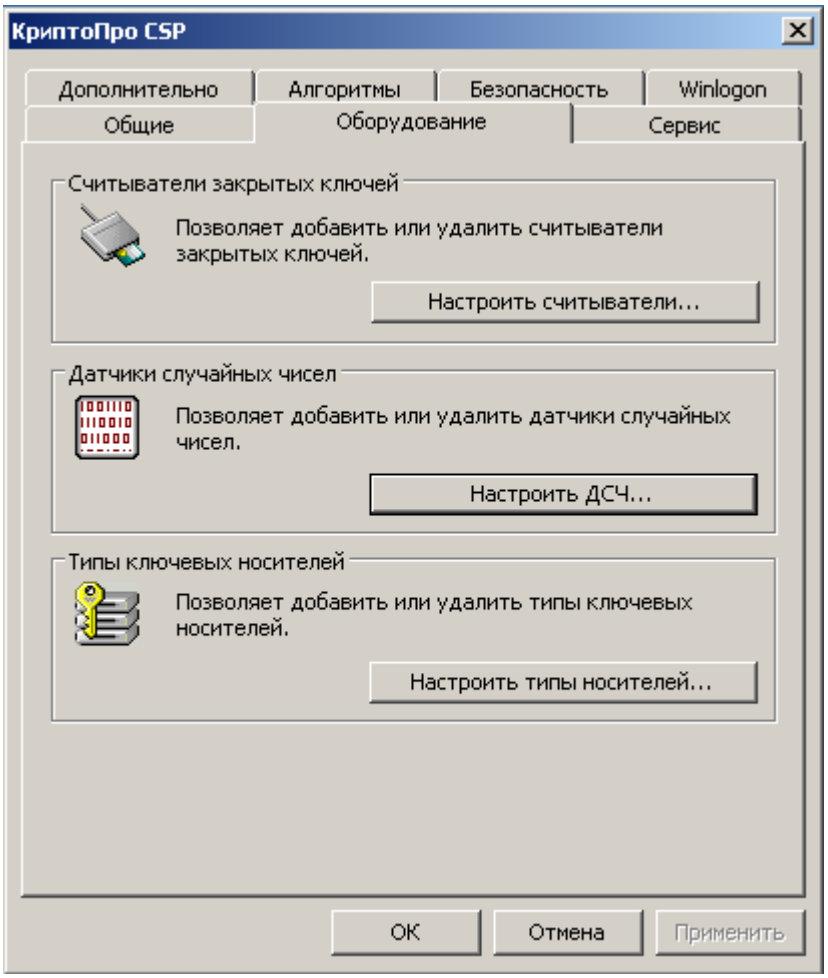

Рисунок 12

Шаг 2: если используется режим защиты КС1, то в открывшемся окне должен быть установлен только «Биологический ДСЧ» (Рисунок 13). Нажмите кнопку `OK`.

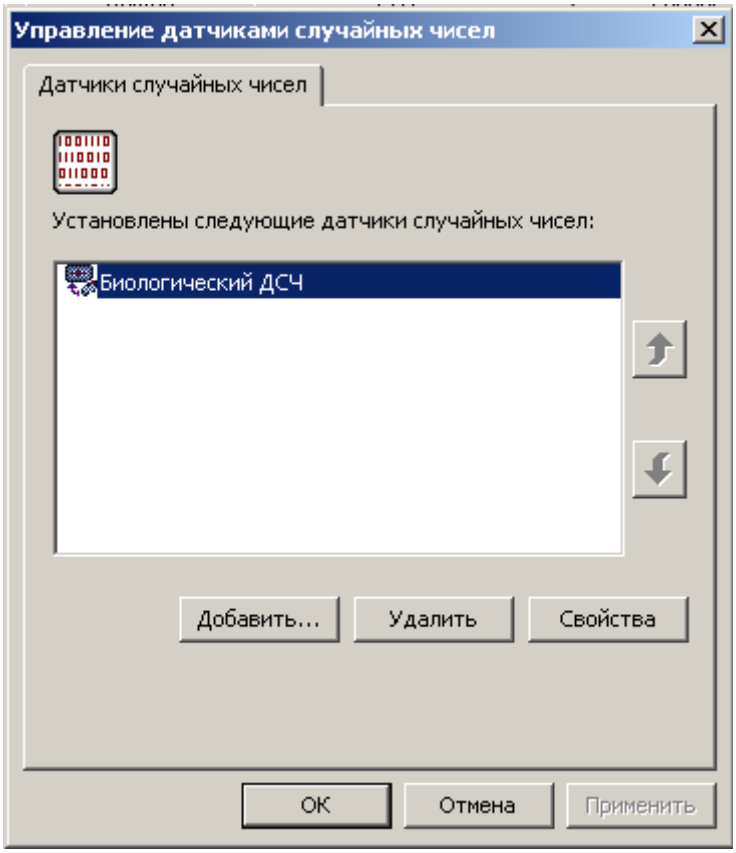

Рисунок 13

Шаг 3: для режима защиты КС2 добавьте аппаратный ДСЧ, нажав кнопку `Добавить`…(Рисунок 13).

Шаг 4: открывается Мастер установки ДСЧ, нажмите кнопку `Далее`.

Шаг 5: в окне выбора ДСЧ выберите ДСЧ и нажмите `Далее`

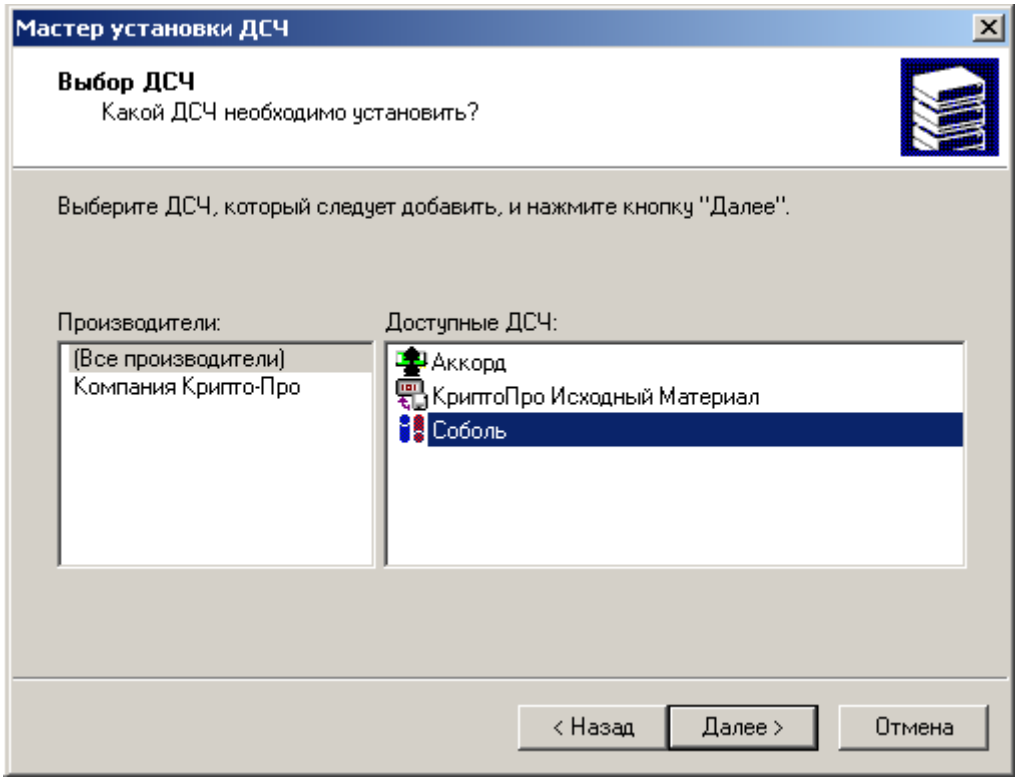

Рисунок 14

Шаг 6: **у**становленный аппаратный ДСЧ переместите в верхнюю строчку, Биологический ДСЧ можно удалить или оставить, нажмите кнопку `OK`.

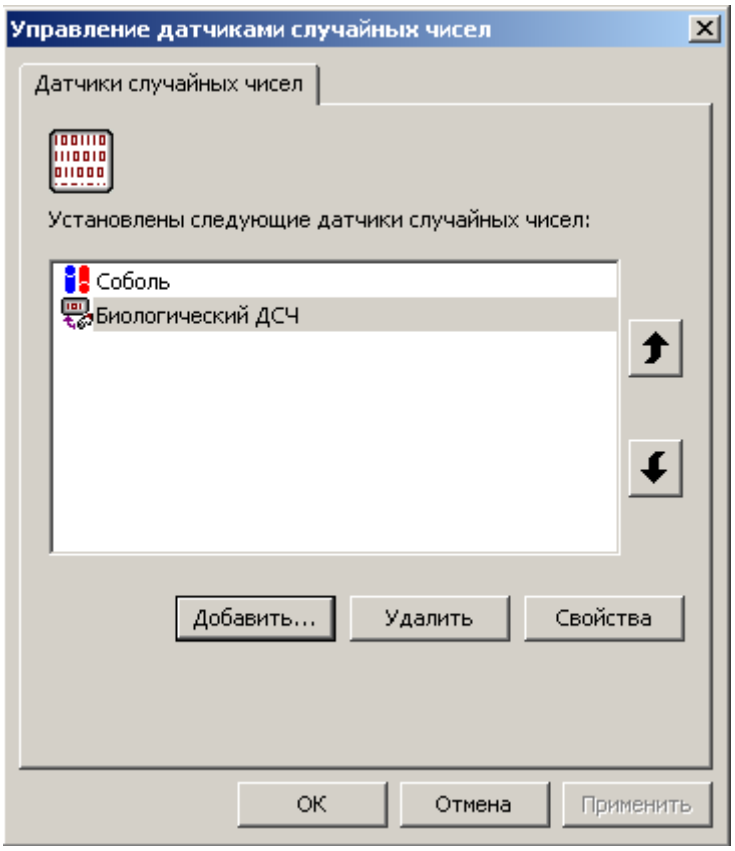

Рисунок 15

4.3 Установка и настройка Удостоверяющего Центра. Создание CA сертификата

Перед созданием ключевой пары и запроса на сертификат пользователя опишем как создать Удостоверяющий Центр (центр сертификации – CA) средствами MS, который будет издавать сертификат пользователю.

На отдельном компьютере установите ОС Windows Server 2008 R2 и СКЗИ «КриптоПро CSP».

Запустите «КриптоПро CSP» и инсталлируйте ключевой считыватель Реестр для хранения контейнера с секретным ключом CA сертификата, как описано в разделе «Инсталляция ключевого считывателя Реестр в «КриптоПро CSP».

Для инсталляции Удостоверяющего Центра Microsoft Certification Authority запустите `Server Manager` (`Start-Administrative Tools-Server Manager`) и войдите в раздел `Roles`. Выберите `Add Roles` и инсталлируйте `Web Server (IIS)`.

Затем, выполните инсталляцию `Active Directory Certificate Services` (Рисунок 16), которую опишем подробнее.

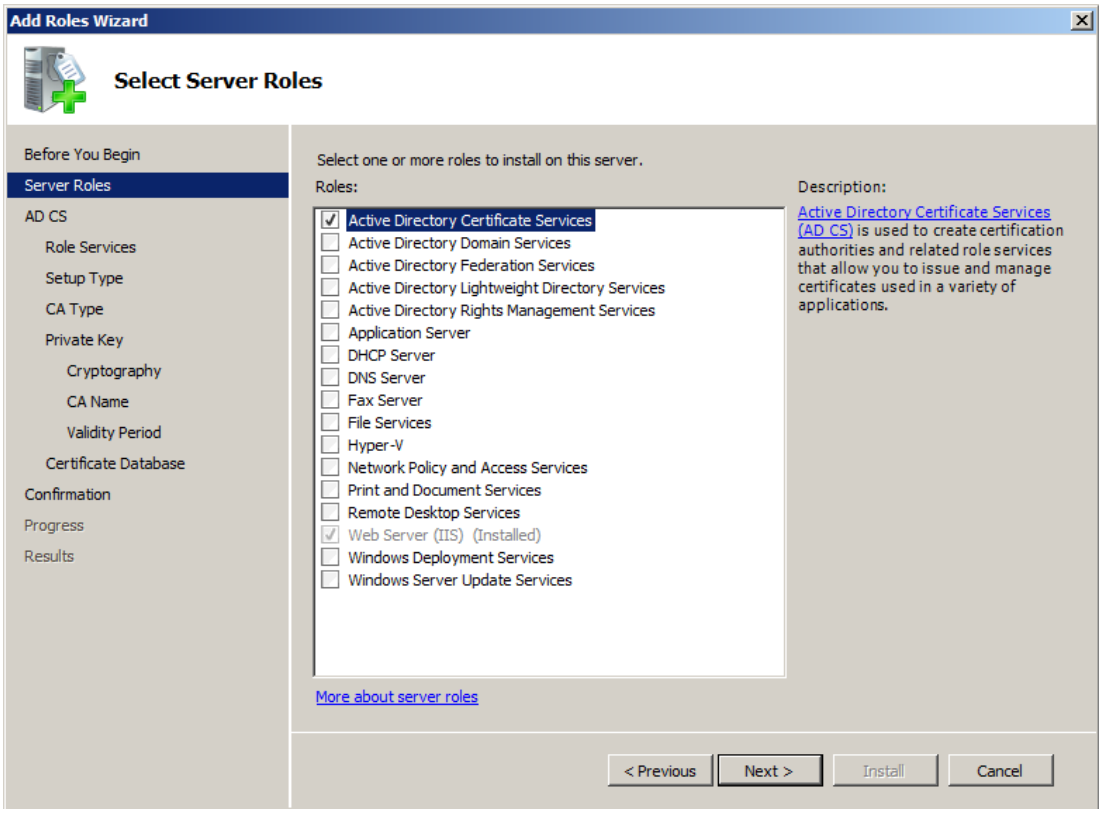

Рисунок 16

Шаг 1: установите флажки `Certification Authority` и `Certification Authority Web Enrollment` и нажмите `Next`.

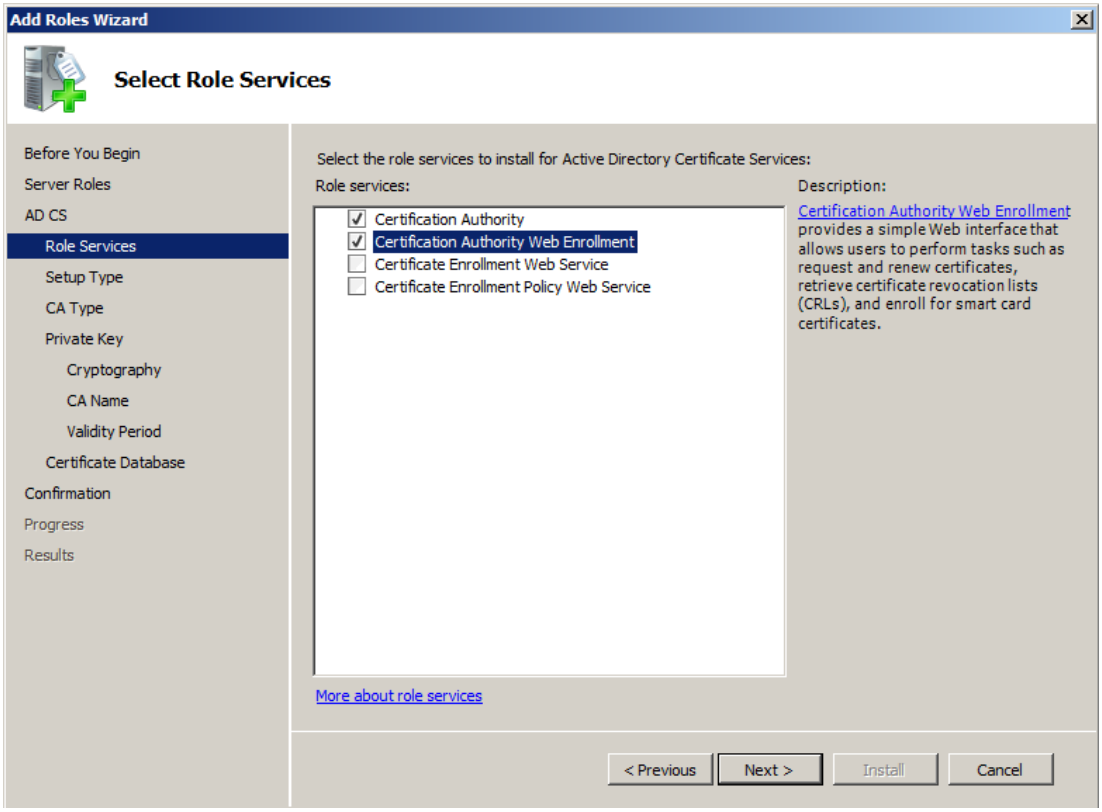

Рисунок 17

Шаг 2: переключатель должен стоять в положении `Standalone`, нажмите `Next`.

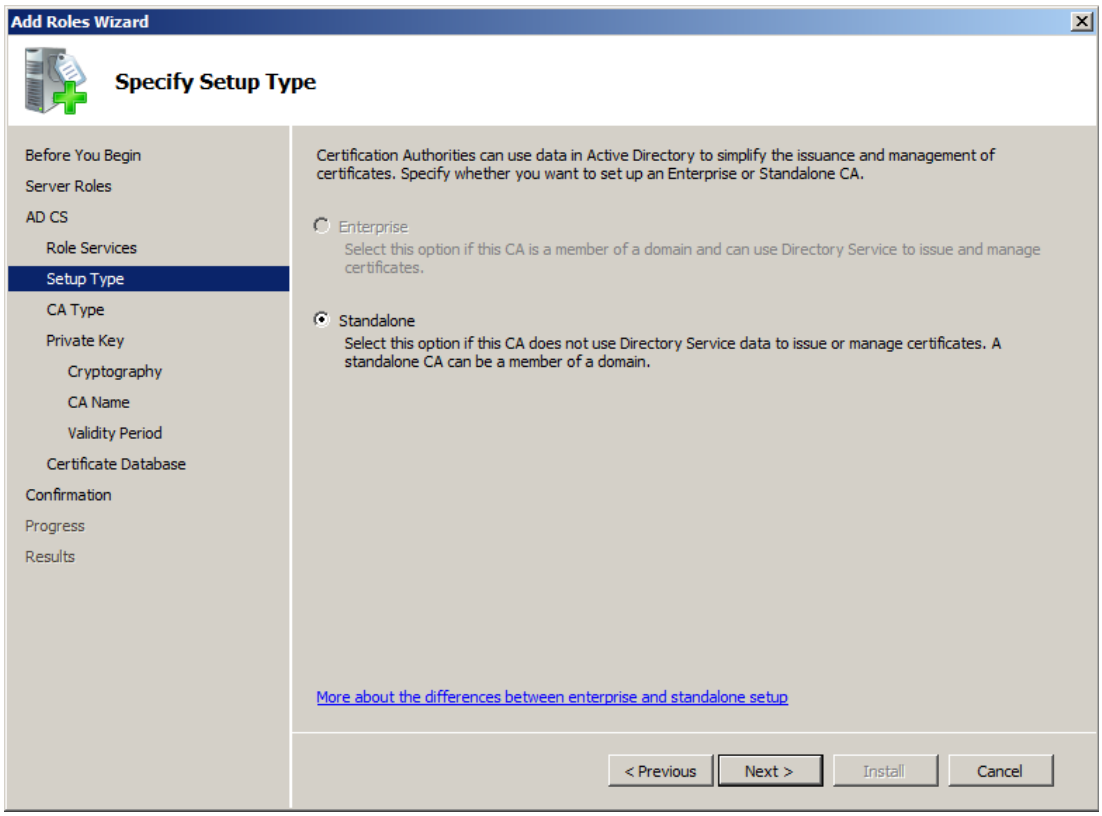

Рисунок 18

Шаг 3: поставьте переключатель в положение `Roote CA` и нажмите `Next`.

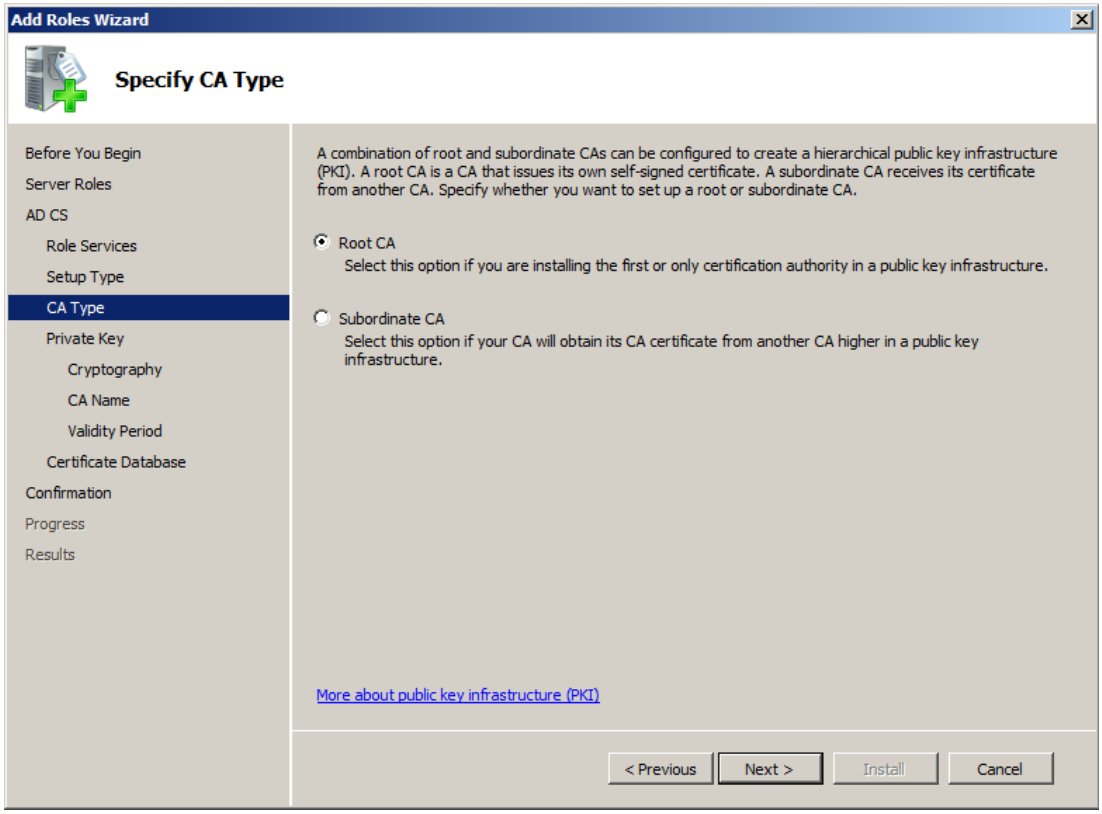

Рисунок 19

Шаг 4: поставьте переключатель в положение `Create a new private key`.

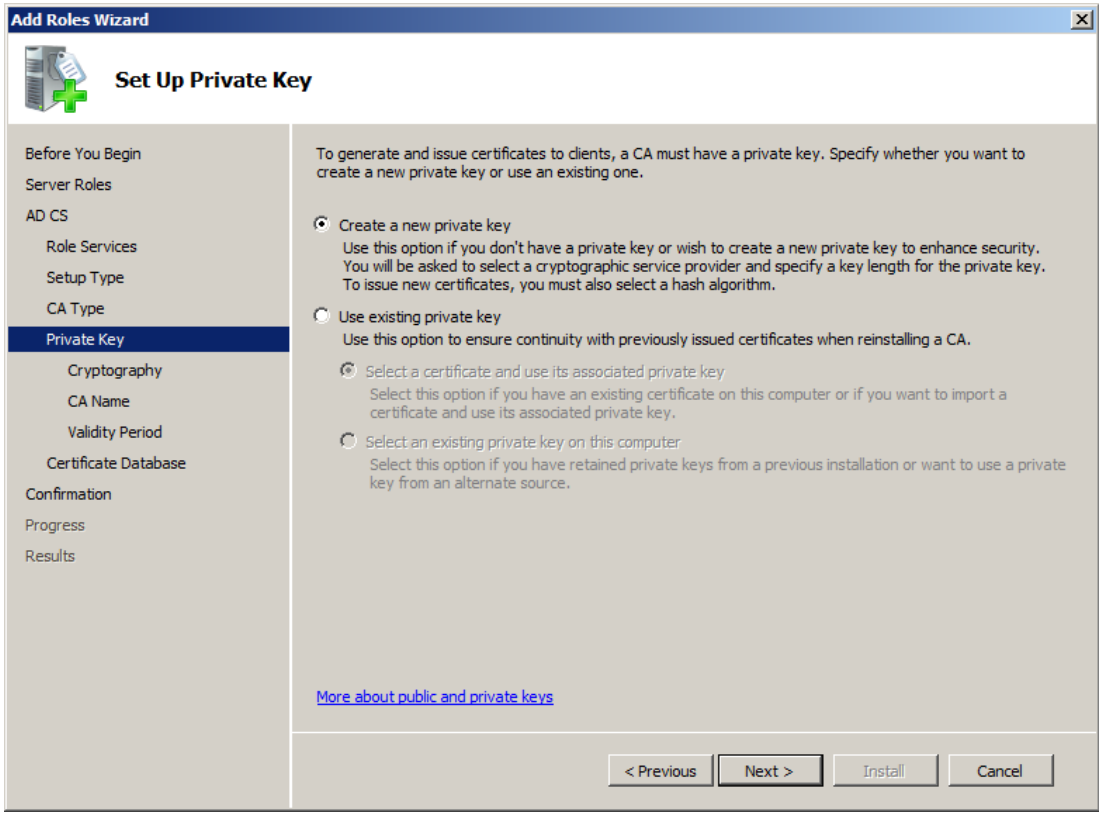

Рисунок 20

Шаг 5: выберите криптопровайдера `Crypto-Pro GOST R 34.10-2001 Cryptographic Service Provider` и установите флажок `Allow administrator interaction when the private key is accessed by the CA`, нажмите `Next`.

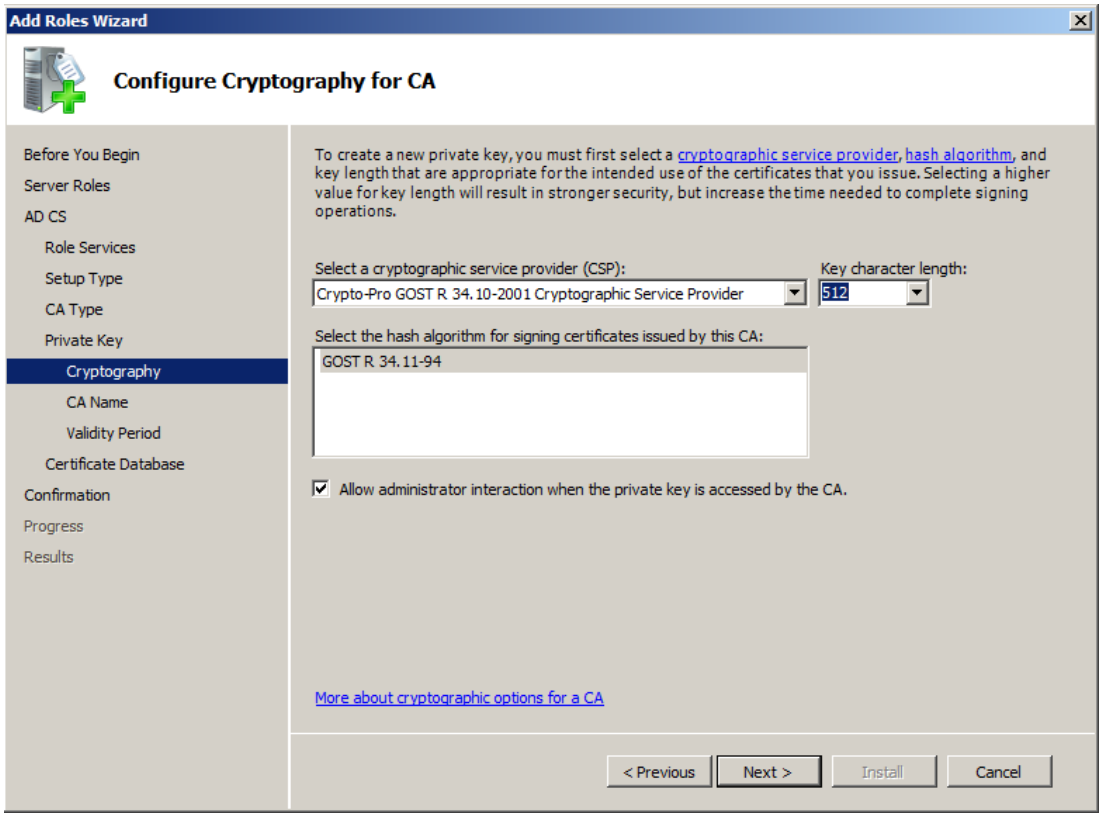

Рисунок 21

Шаг 6: заполните поля для CA сертификата и нажмите `Next`.

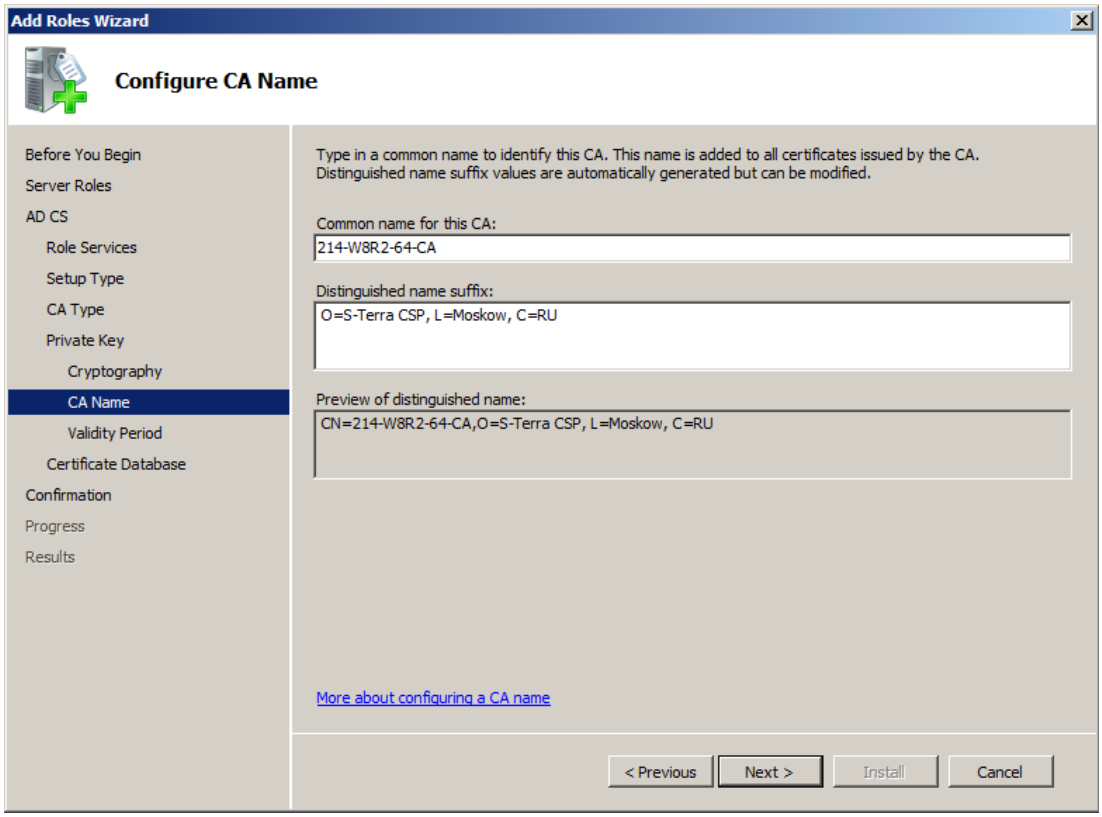

Рисунок 22

Шаг 7: укажите период действия для сертификата.

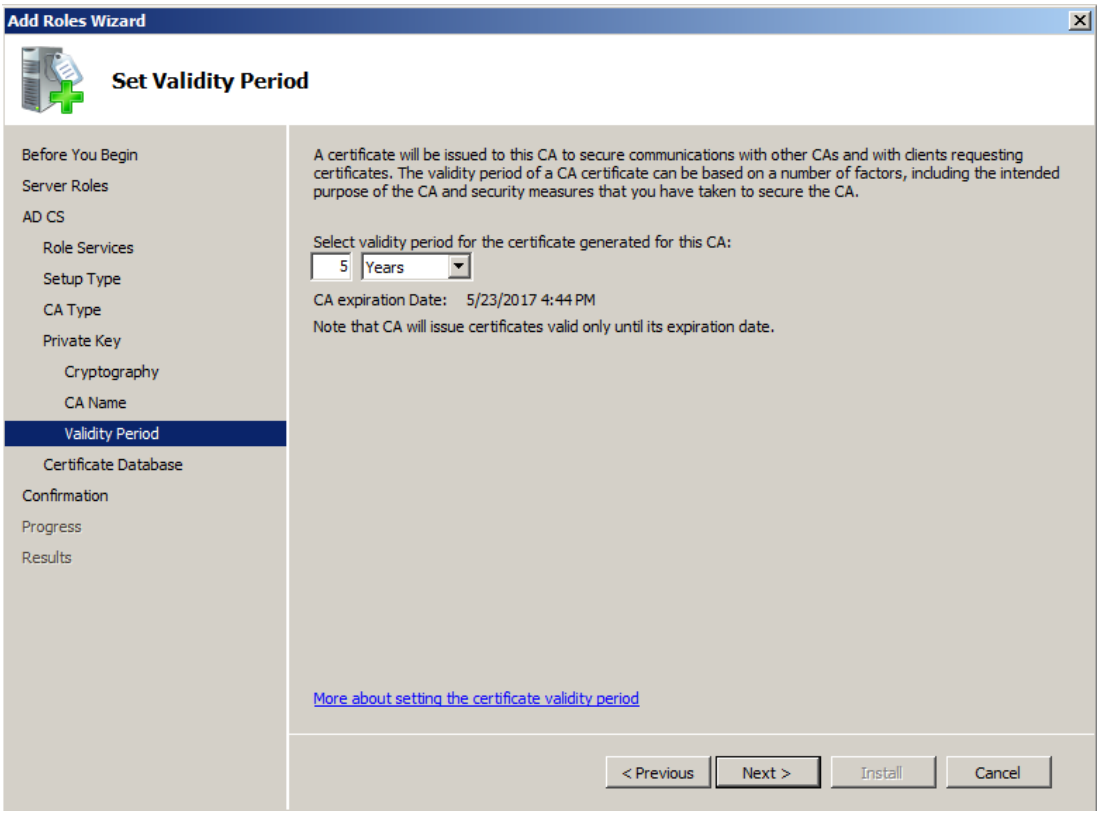

Рисунок 23

Шаг 8: в окне с указанием о размещении хранилища оставьте значения по умолчанию и нажмите `Next`.

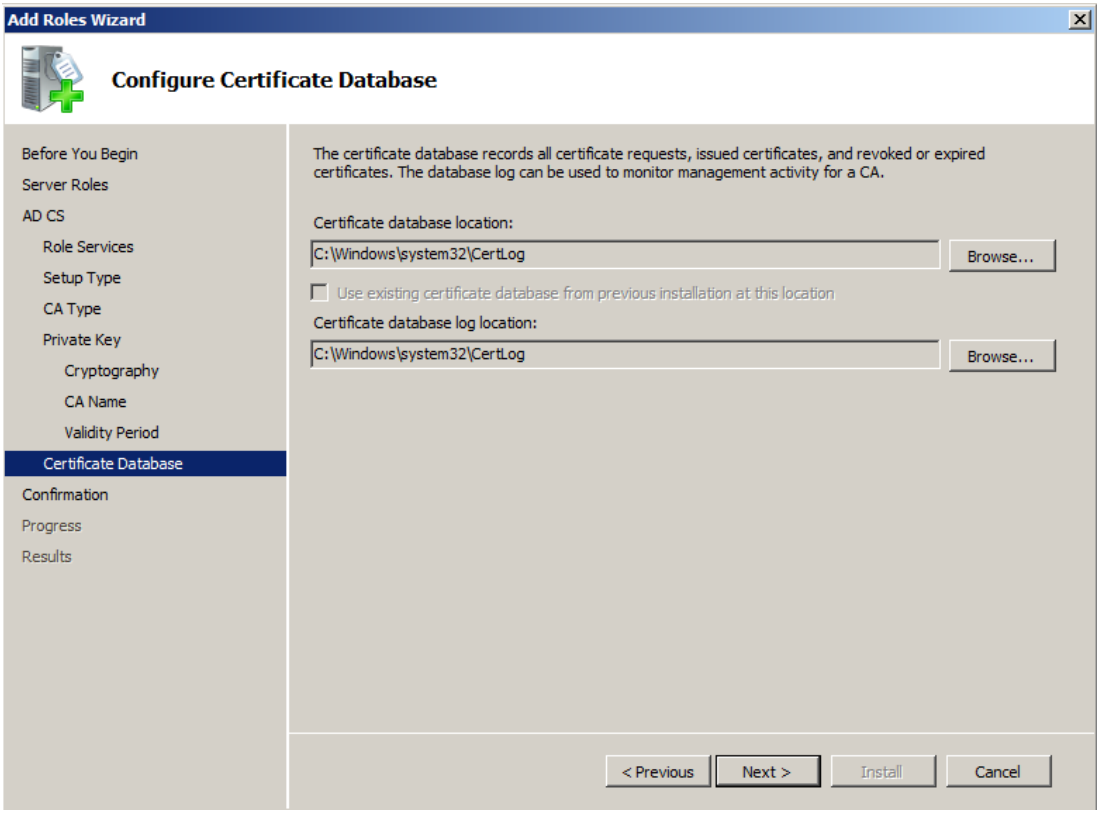

Рисунок 24

Шаг 9: нажмите `Install`.

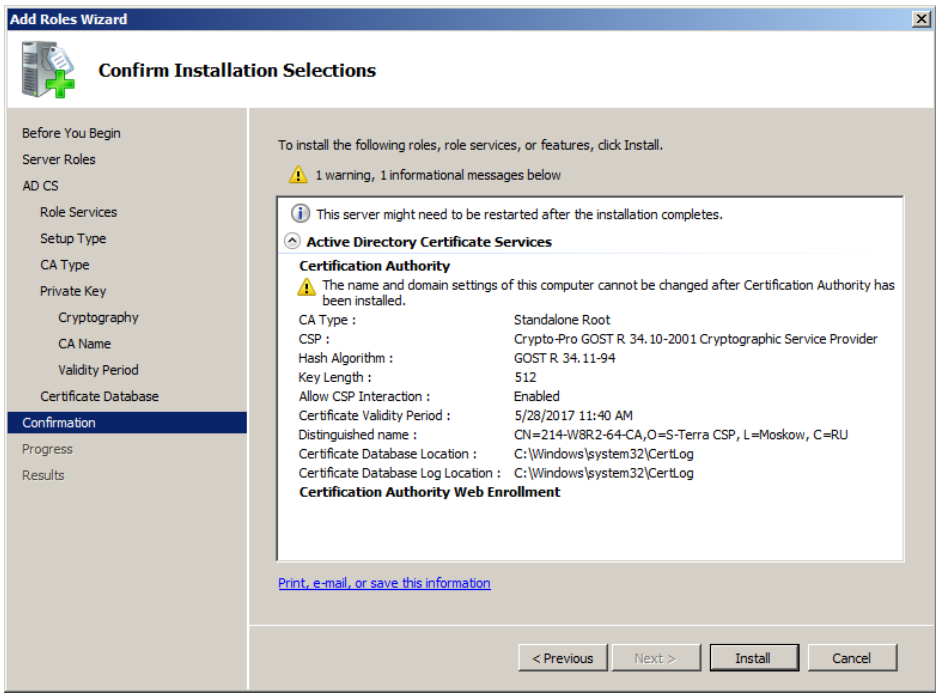

Рисунок 25

Шаг 10: выберите ключевой носитель `Registry`, куда будет записан контейнер с секретным ключом для CA сертификата.

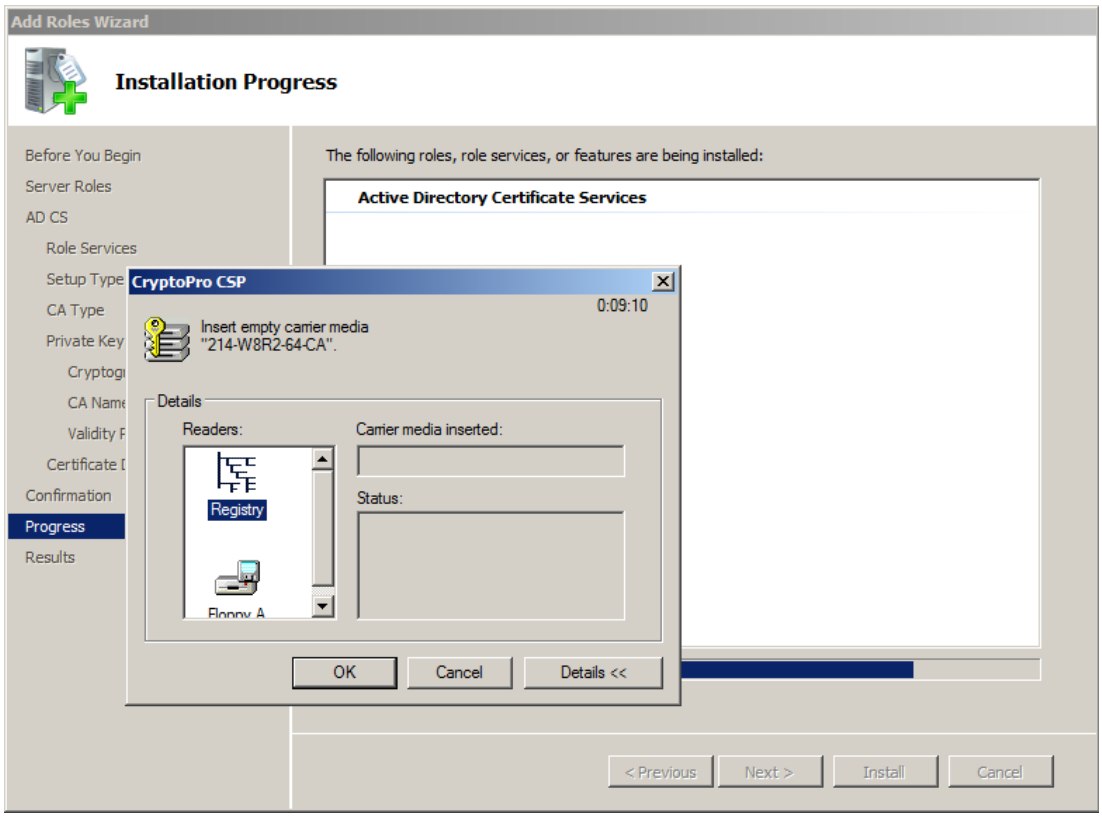

Рисунок 26

Шаг 11: подвигайте мышкой или понажимайте клавиши, пока происходит создание ключевой пары.

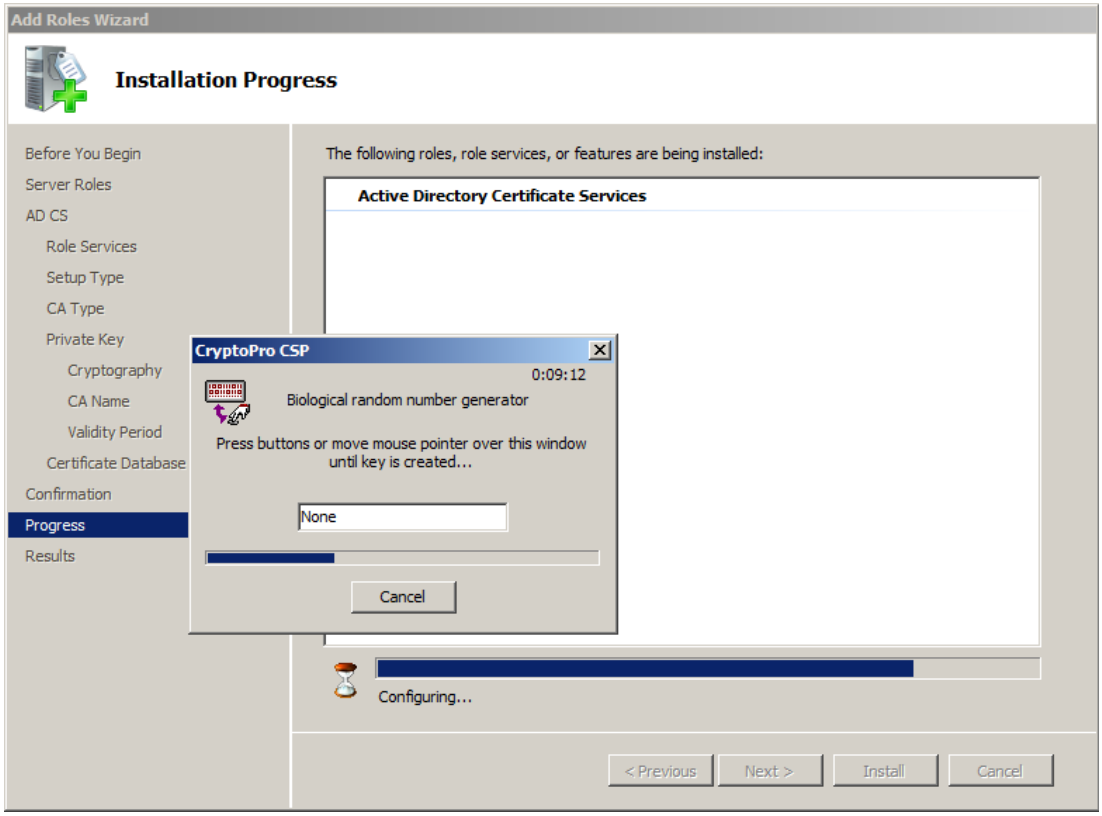

Рисунок 27

Шаг 12: задайте пароль к созданному контейнеру.

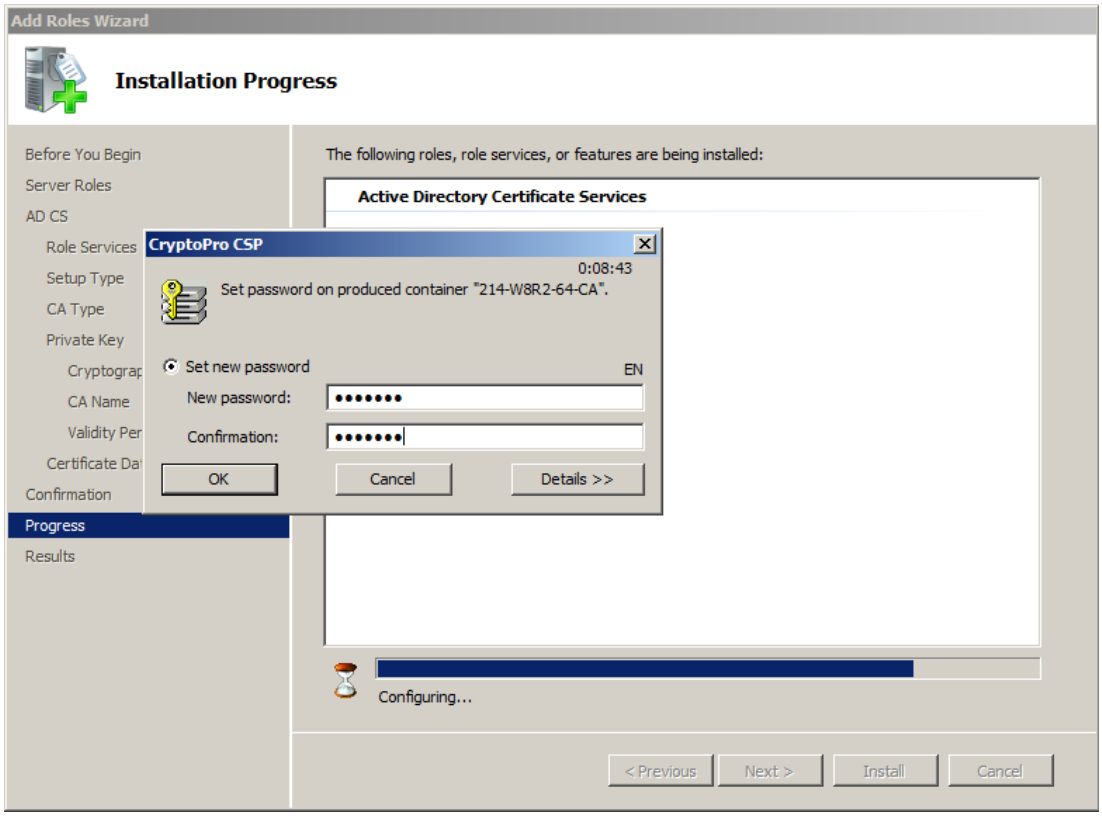

Рисунок 28

Шаг 13: укажите пароль к созданному контейнеру.

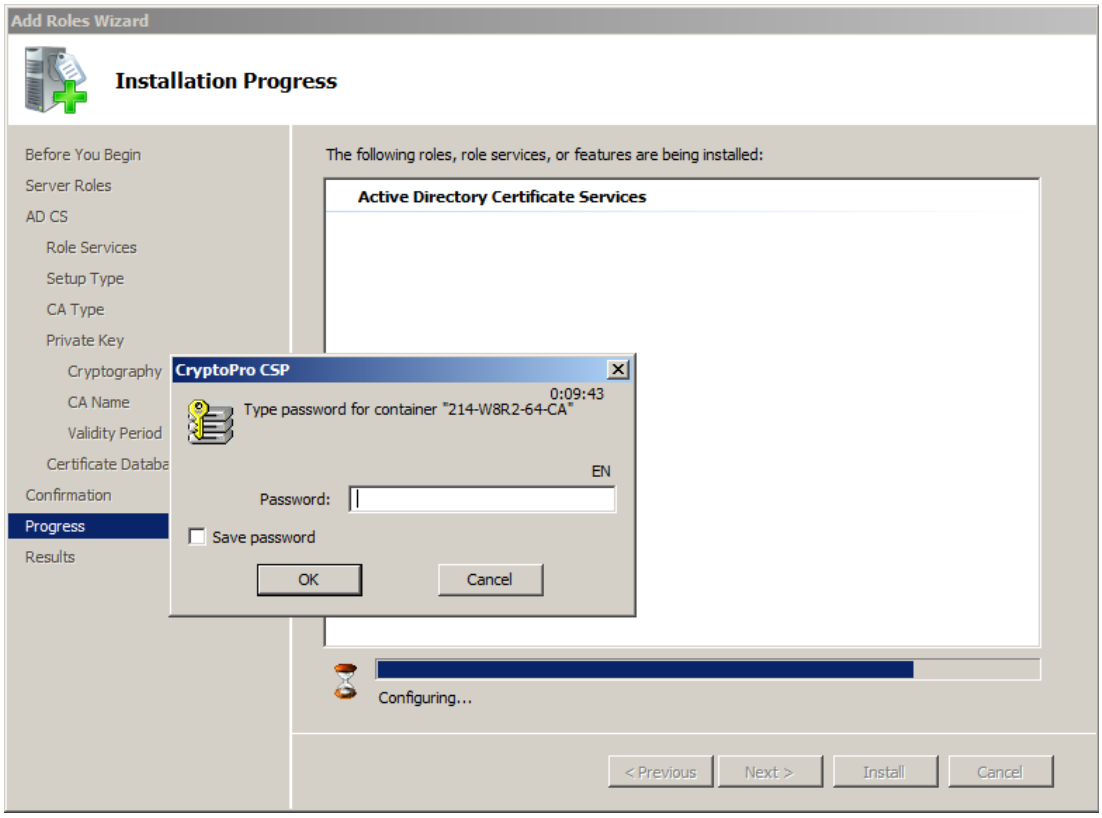

Рисунок 29

Шаг 14: инсталляция Удостоверяющего Центра завершена, нажмите `Close`.

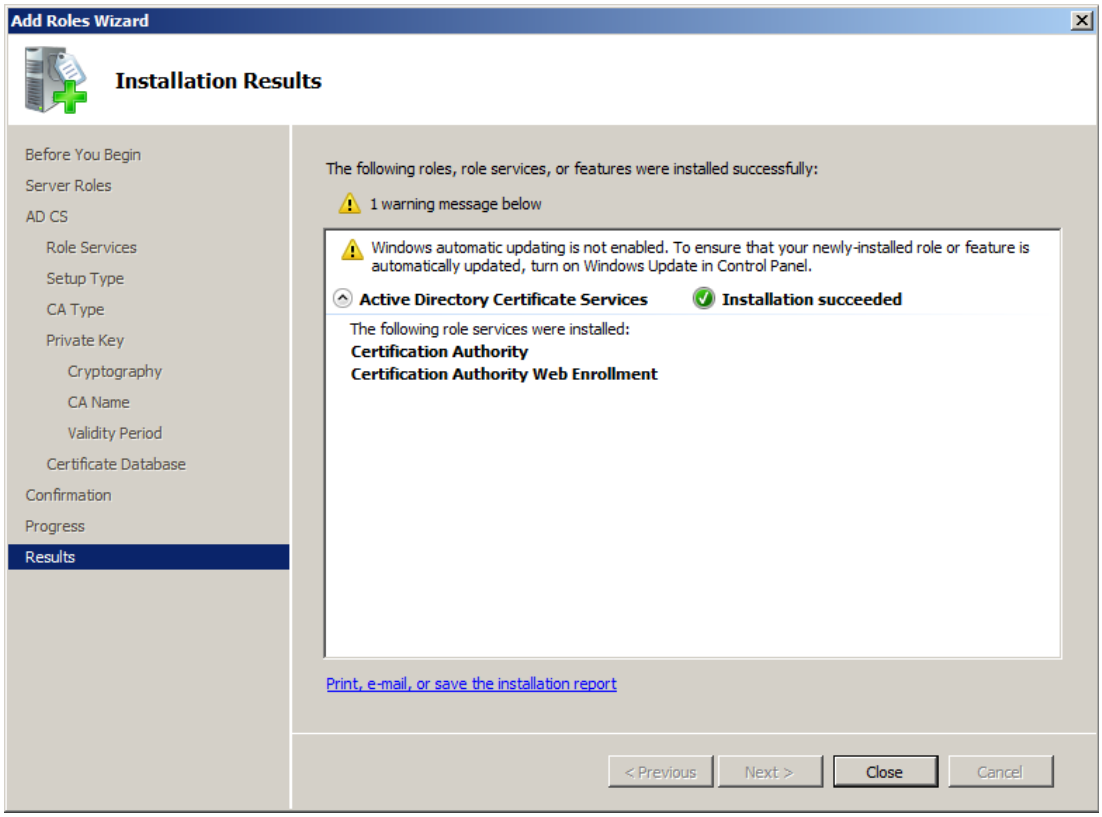

Рисунок 30

Шаг 15: для автоматического создания подписываемых сертификатов по запросу проведите некоторые настройки Удостоверяющего Центра. Вызовите `Certificate Authority (Start- Administrative Tools-Certification Authority)`, выделите центр CA и нажмите `Properties`. В окне `Properties` войдите во вкладку `Policy Module` (Рисунок 31) и нажмите кнопку `Properties...`

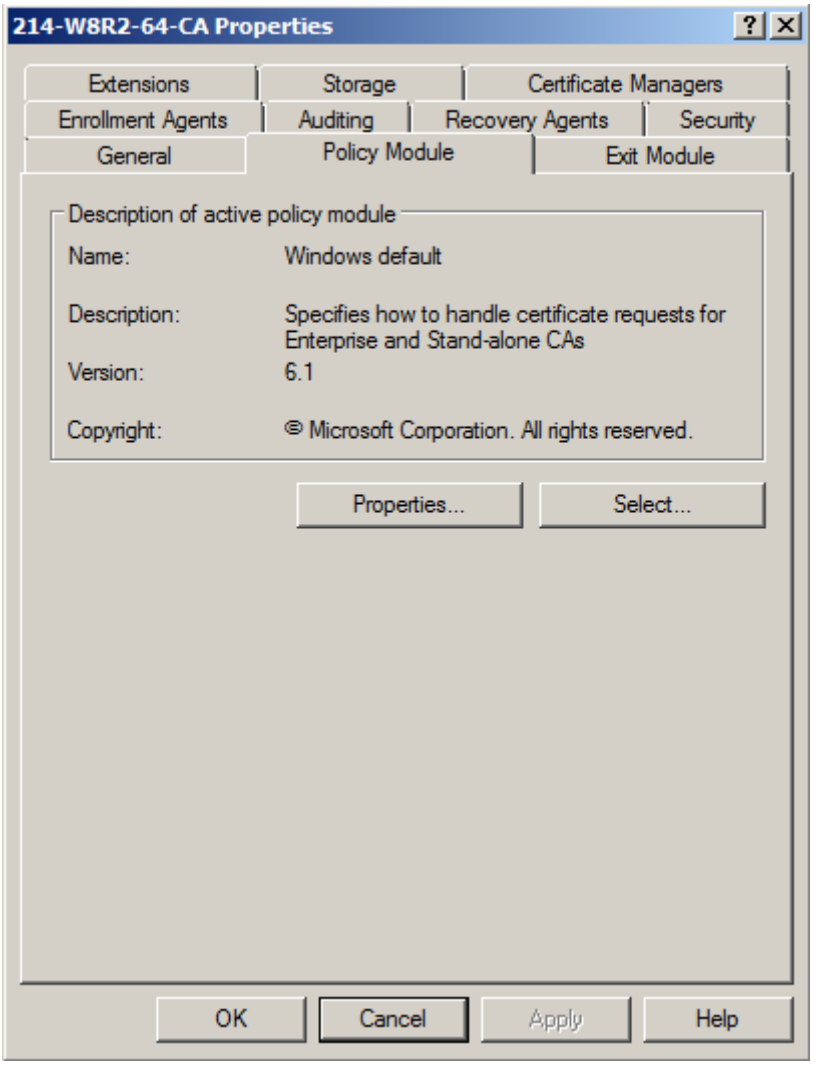

Рисунок 31

Шаг 16: в появившемся окне `Properties` установите переключатель в положение `Follow the settings…` (автоматически издавать сертификат по запросу) (Рисунок 32) и нажмите `OK`.

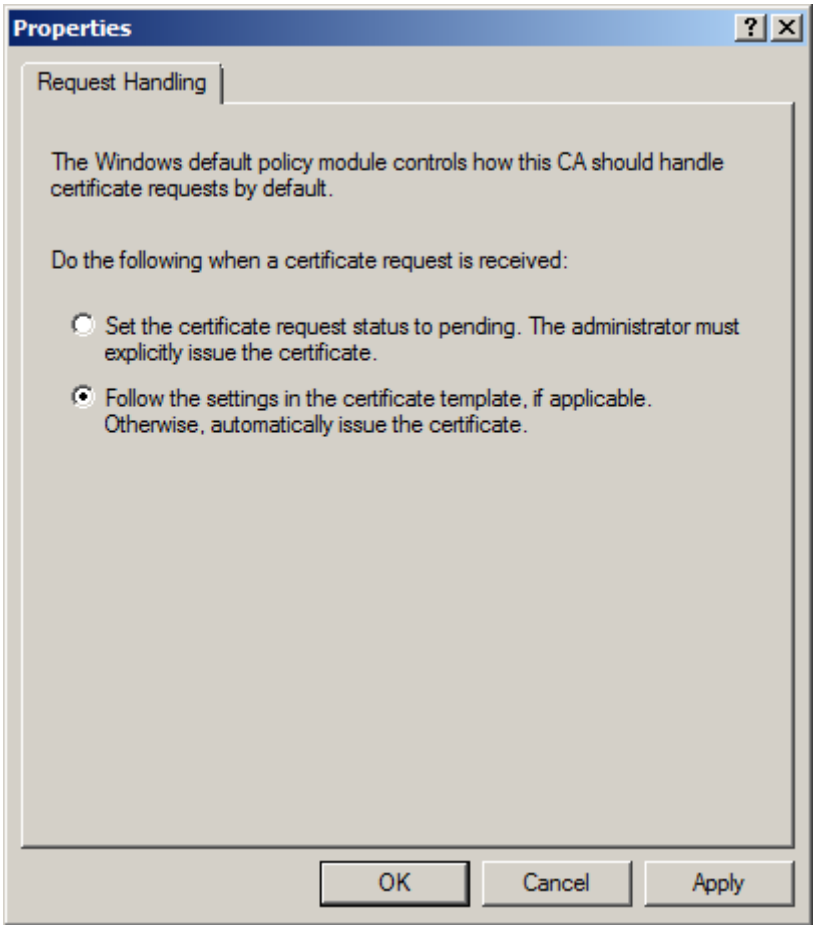

Рисунок 32

Шаг 17: в окне `Windows default` выдается предупреждение о необходимости перезапуска сертификатного сервиса:

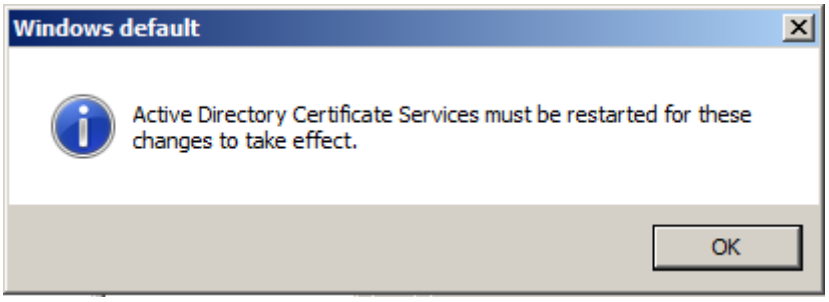

Рисунок 33

Шаг 18: в окне `Certificate Authority` выберите предложение меню `Action`, в выпадающем меню предложение `All Tasks`, а в следующем выпадающем меню – предложение `Stop Service`. После остановки сервиса выберите предложение `Start Service`.

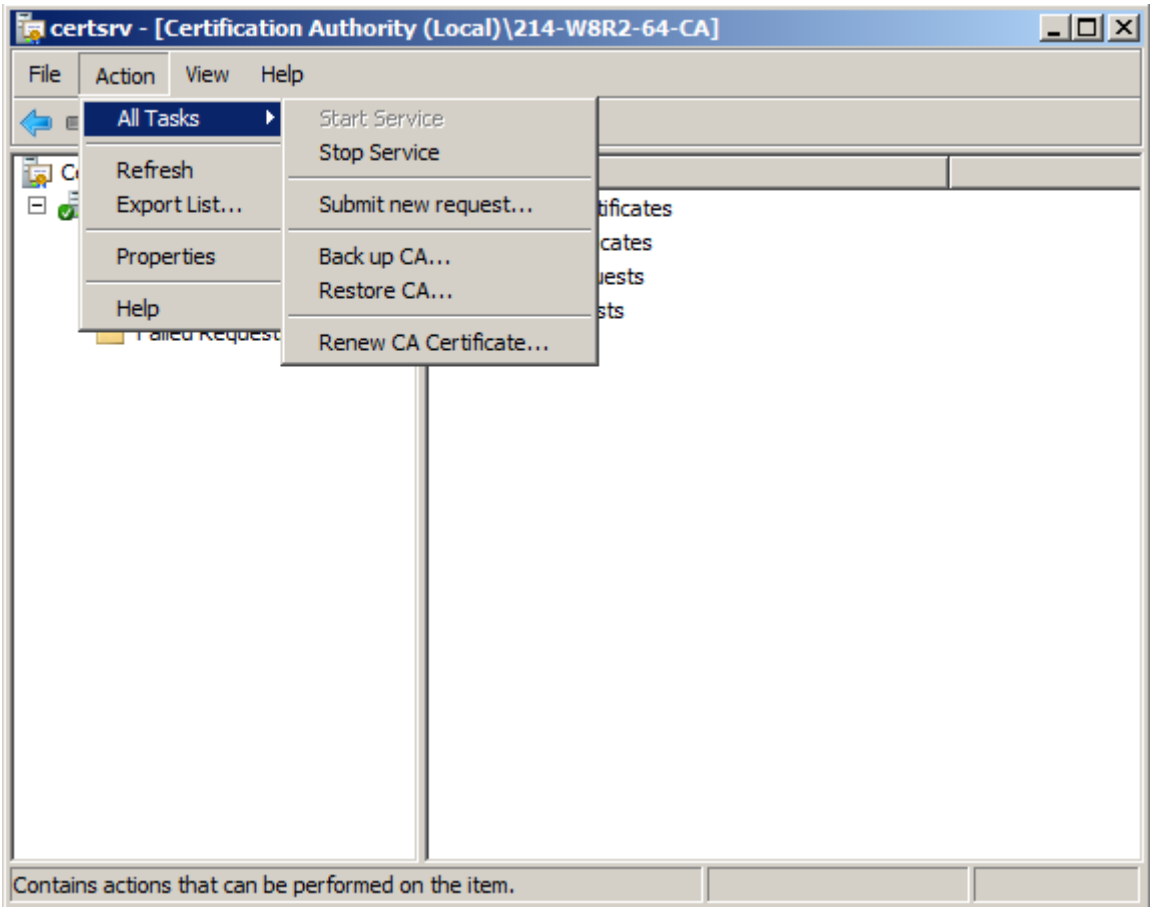

Рисунок 34

На этом создание Удостоверяющего Центра и его CA сертификата закончено.

Примечание:

Для возможности дальнейшего выбора криптопровайдера “КриптоПро CSP” в окне создания запроса на сертификат, выполните следующее:

в файле `System32\certsrv\certsgcl.inc` измените значение константы `ConstnMaxProvType` с 25 на 99. В стандартном скрипте перечислено только 25 типов криптопровайдера.

4.3.1.1.1 Экспортирование CA сертификата в файл

Шаг 1: для экспортирования CA сертификата в файл, войдите сначала в Certificate Authority (Start- Administrative Tools-Certification Authority), выделите центр CA и нажмите Properties:

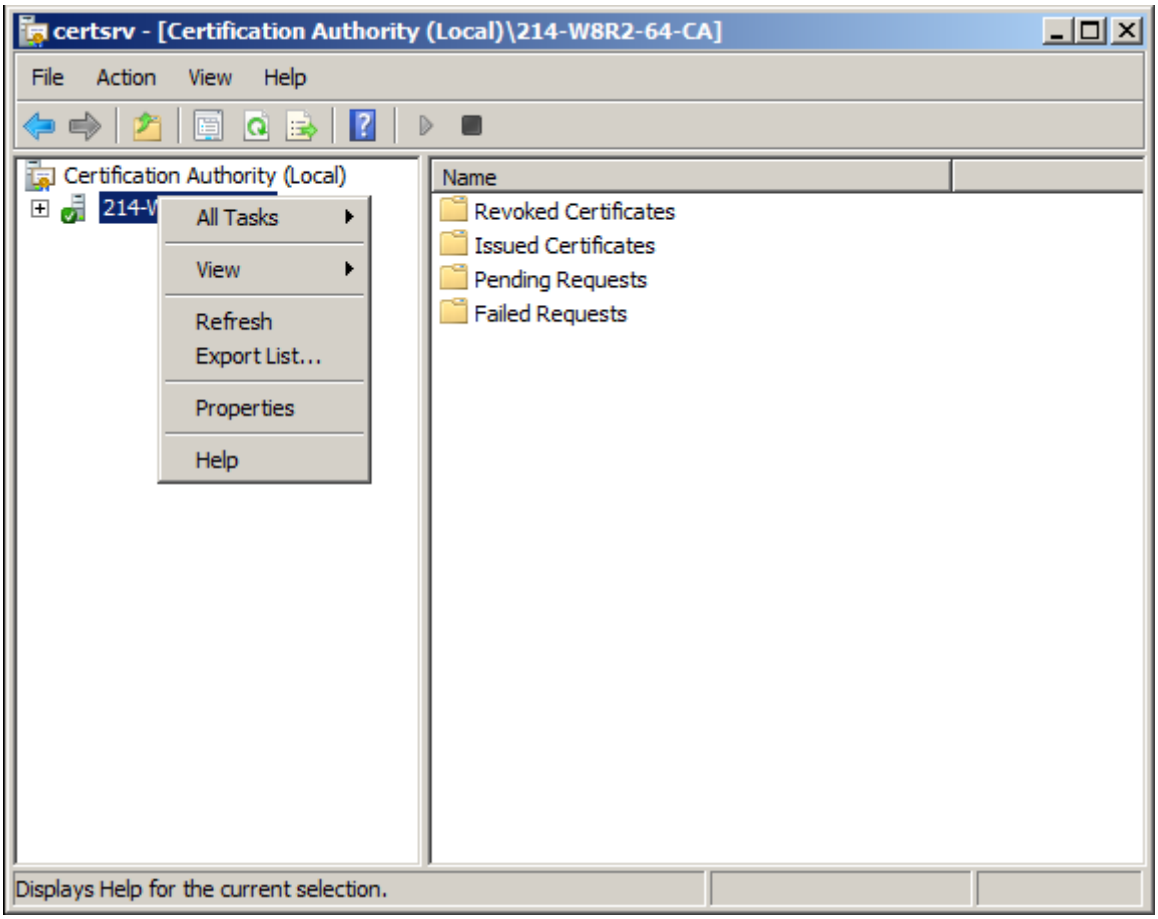

Рисунок 35

Шаг 2: далее во вкладке General нажмите кнопку View Certificate. В появившемся окне Certificate выберите вкладку Details, в выпадающем меню Show выберите предложение All, чтобы увидеть все поля сертификата. Нажмите кнопку Copy to File.

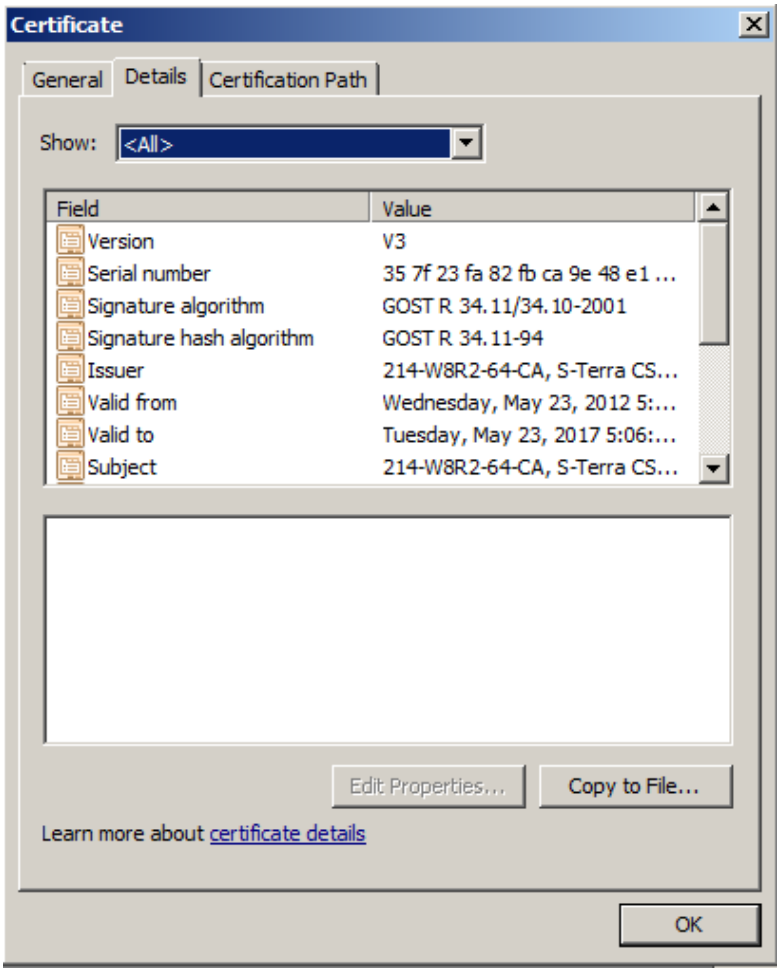

Рисунок 36

Шаг 3: в окне визарда экспортирования сертификата нажмите `Next`.

Рисунок 37

Шаг 4: далее в окне визарда `Certificate Export` выберите формат, в котором должен быть экспортирован сертификат.

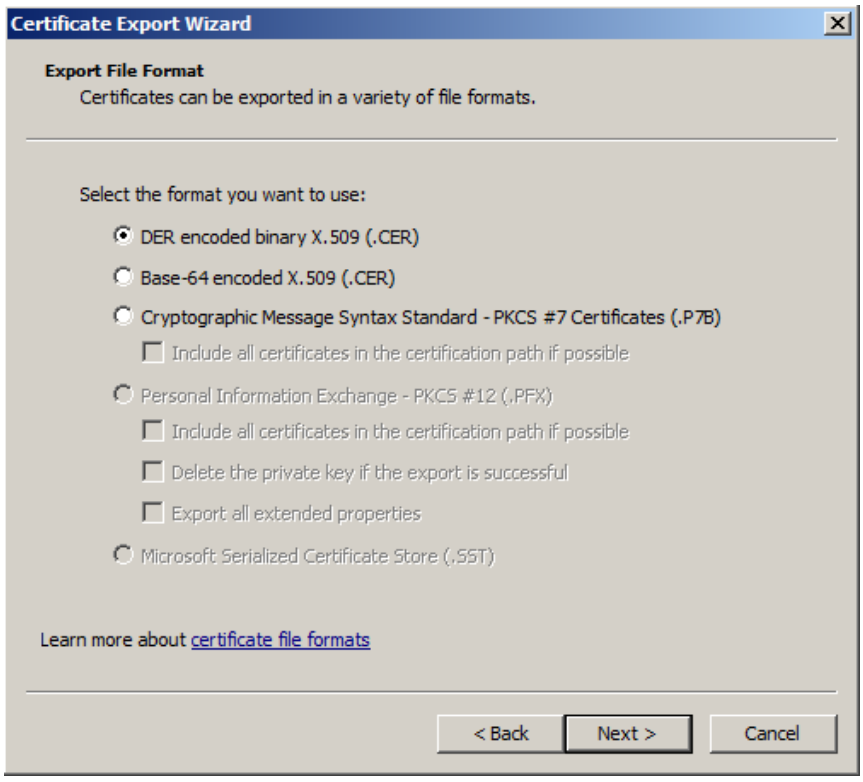

Рисунок 38

Шаг 5: укажите имя файла, в который будет экспортирован сертификат.

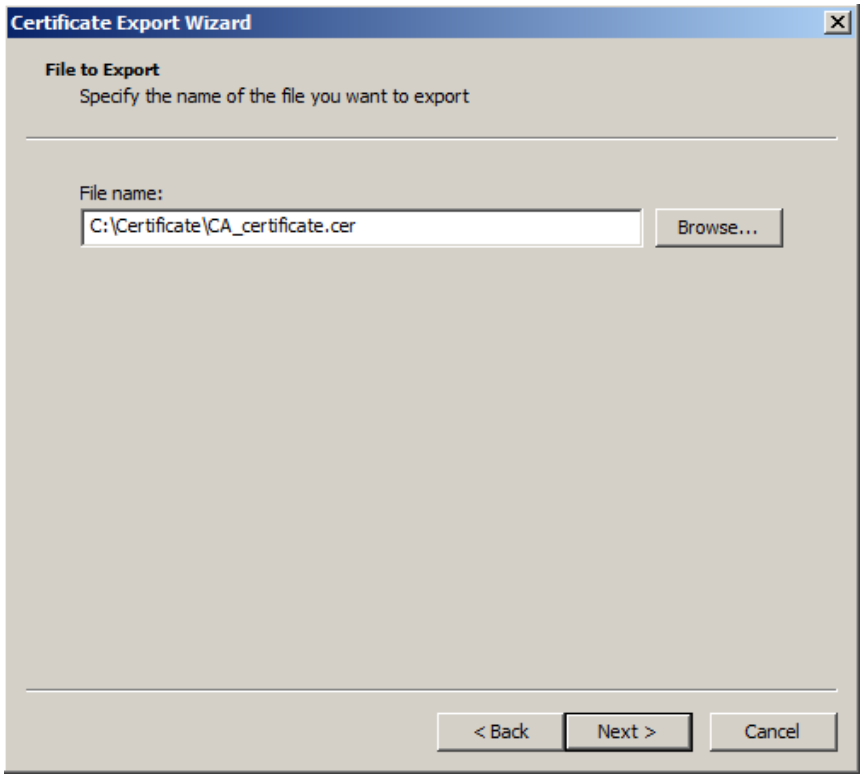

Рисунок 39

Шаг 6: экспортирование СА сертификата в файл завершено, нажмите `Finish`

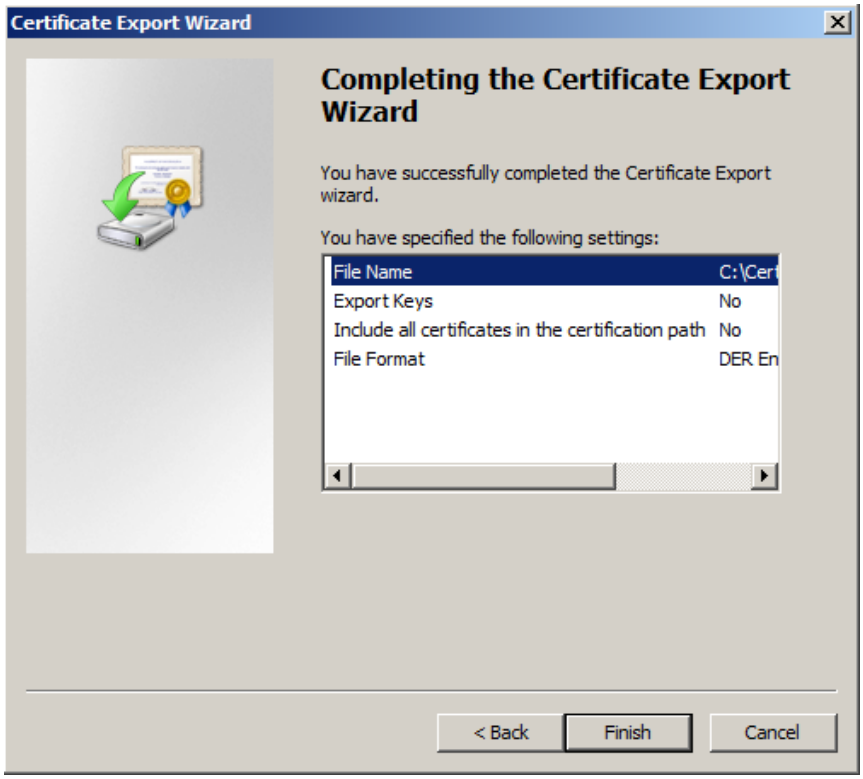

Рисунок 40

При использовании криптобиблиотеки «С-Терра СиЭсПи» далее перейдите в раздел «Создание сертификата пользователя с использованием криптобиблиотеки, разработанной компанией «С-Терра СиЭсПи».

4.4 Создание сертификата пользователя с использованием СКЗИ «КриптоПро CSP

4.4.1 Создание ключевой пары и формирование запроса на сертификат пользователя

Опишем этот процесс на отдельном компьютере пользователя.

Шаг 1: установите программный Продукт СКЗИ «КриптоПро CSP»..

Шаг 2: инсталлируйте ключевой носитель, на котором будет размещен контейнер с секретным ключом пользователя, используя СКЗИ "КриптоПро CSP

Шаг 3: запустите Microsoft Internet Explorer. В поле Address укажите адрес сервера Удостоверяющего Центра и запустите утилиту `certsrv` (Certificate Service), например, `http://10.0.6.214/certsrv/`.

Полагаем, что на сервере уже установлен Продукт СКЗИ «КриптоПро CSP».

Шаг 4: в появившемся окне высвечивается имя удостоверяющего центра – в нашем случае 214-W8R2-64-CA. Для формирования запроса на создание сертификата пользователя выберите предложение "`Request a certificate`" (Рисунок 41):

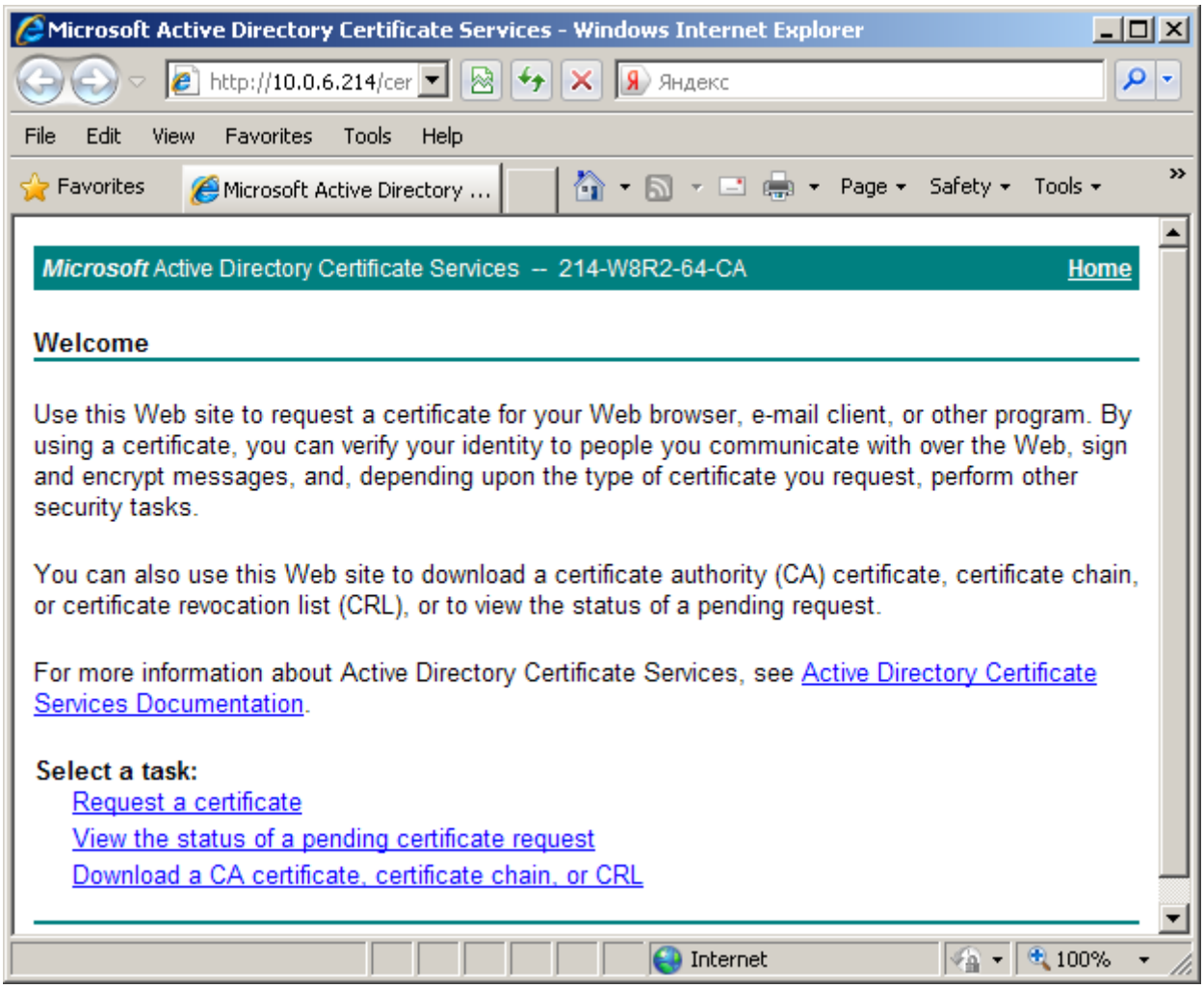

Рисунок 41

Шаг 5: выберите расширенный запрос на сертификат – предложение "`advanced certificate request`" (Рисунок 42):

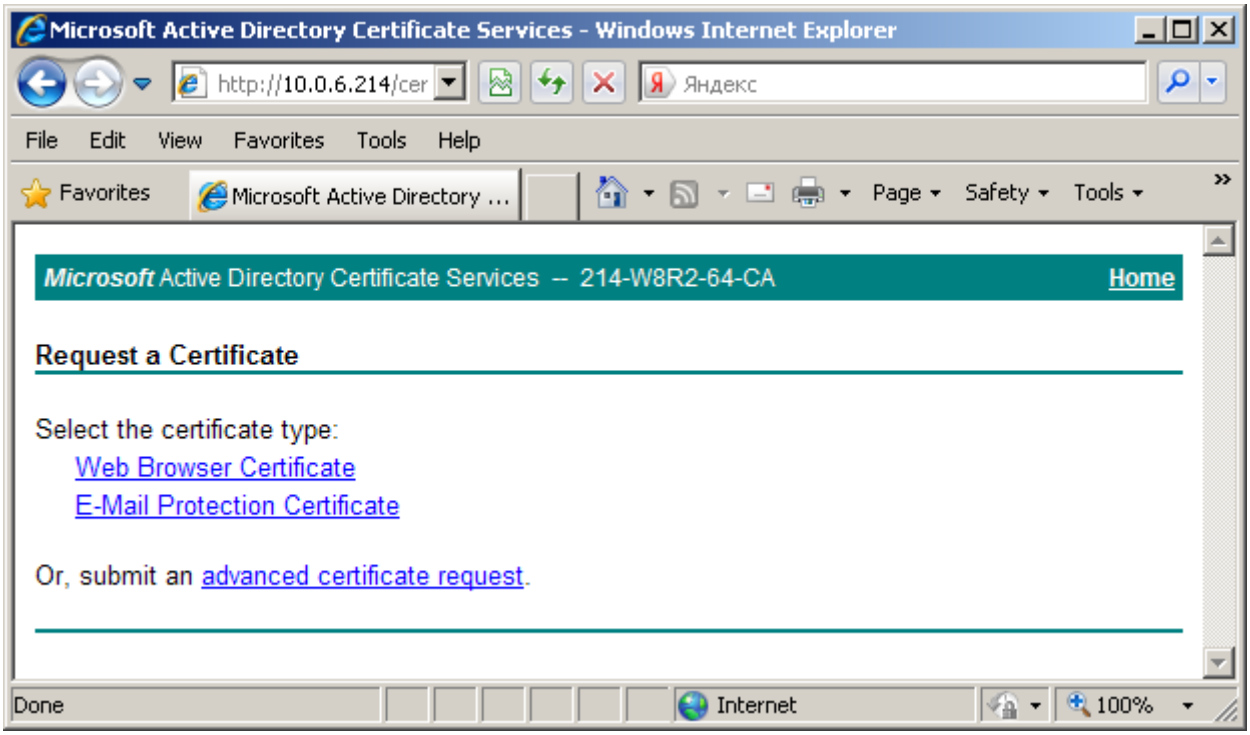

Рисунок 42

Шаг 6: для получения формы для формирования запроса на сертификат выберите предложение "`Create and submit a request to this CA`" (Рисунок 43):

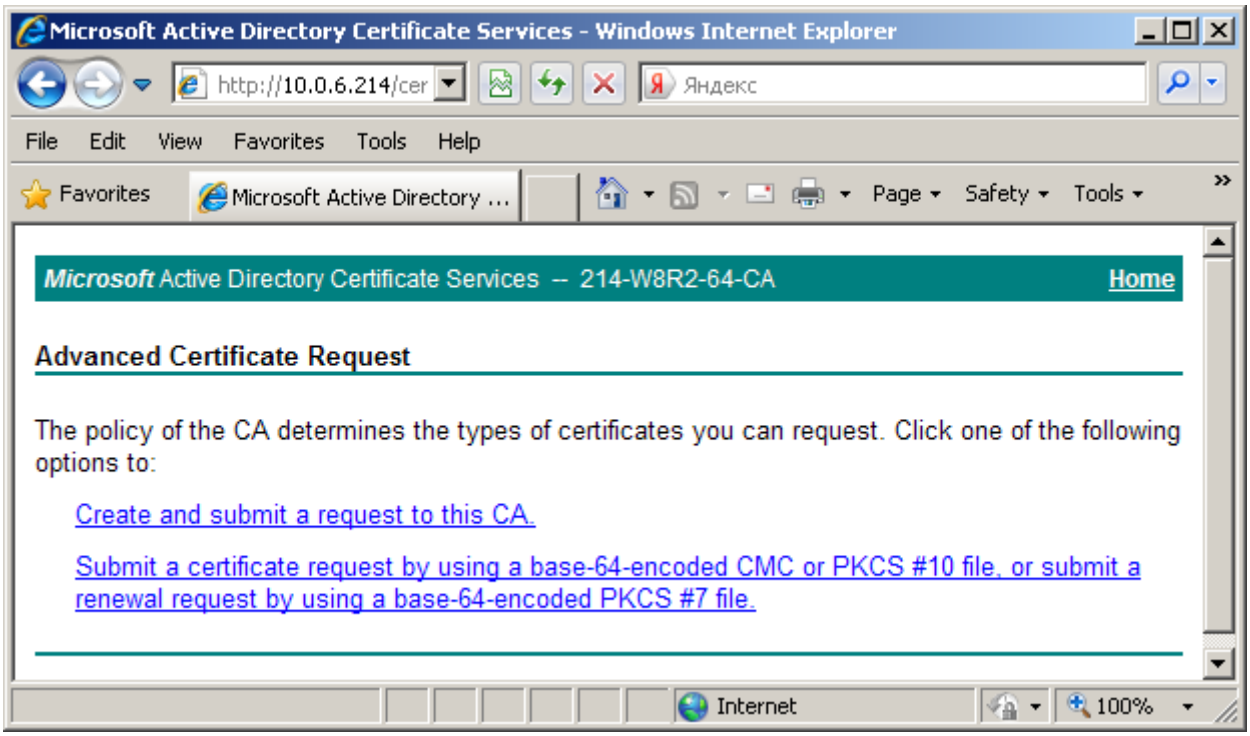

Рисунок 43

Шаг 7: заполните форму расширенного запроса, показанную ниже (Рисунок 44). Дадим некоторые пояснения для ее заполнения:

- в разделе **Identifying Information** (Информация о Владельце Сертификата) внесите данные о владельце сертификата. Во всех полях этого раздела разрешается использовать не только латинские, но и русские буквы, кроме поля Country/Region, оно всегда содержит значение RU.
- в разделе **Type of Certificate Needed** (Тип требуемого сертификата) из выпадающего списка выберите предложение Client Authentication Certificate
- в разделе **Key Options** (Опции ключей) задаются параметры создаваемой ключевой пары и размещение секретного ключа. Рекомендуется выбрать следующие опции:
  - поставьте переключатель в положение `Create new key set` (Создать установки для нового секретного ключа)
  - `CSP` (Тип Криптопровайдера) – из выпадающего списка выберите Crypto-Pro GOST R 34.10-2001 Cryptographic Service Provider
  - `Key Usage` (Использование ключей) – выбор типа ключа – Signature (для подписи), Exchange (для обмена), Both (для подписи и обмена) – поставьте переключатель в положение Both
  - `Key Size` (Размер ключа) – при выборе алгоритма GOST R 34.10-2001 длина ключа всегда 512
  - поставьте переключатель в положение `User specified key container name`, чтобы задать имя контейнера с секретным ключом
  - в поле `Container name` (Имя контейнера) введите имя контейнера, в котором будет размещен секретный ключ без указания ключевого носителя, выбрать ключевой носитель будет предложено далее. В имени контейнера разрешается использовать латинские буквы и цифры
  - `Mark keys as exportable` – поставьте флажок, чтобы можно было скопировать контейнер с секретным ключом с одного ключевого носителя на другой, а также во время создания инсталляционного файла провести проверку соответствия сертификата пользователя и секретного ключа
- в разделе **Additional Options** (Дополнительные опции):
  - `Hash Algorithm` – выбрать GOST R34.11-94
  - далее установок никаких делать не нужно.

По этому образцу заполните форму запроса и нажмите кнопку `Submit` (послать запрос):

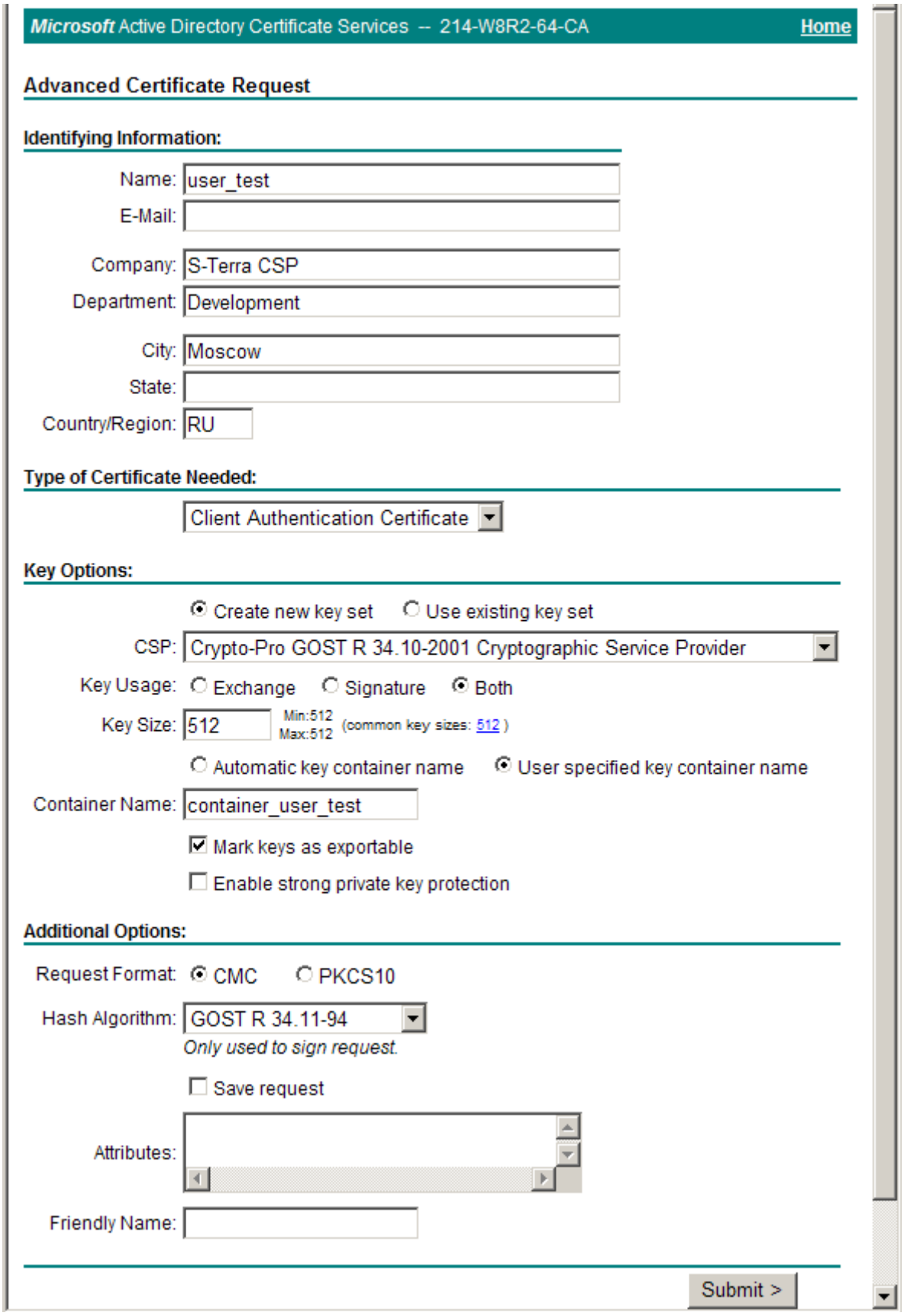

Рисунок 44

Шаг 8: появляется предупреждение (Рисунок 45), нажмите кнопку `Yes`, чтобы продолжить:

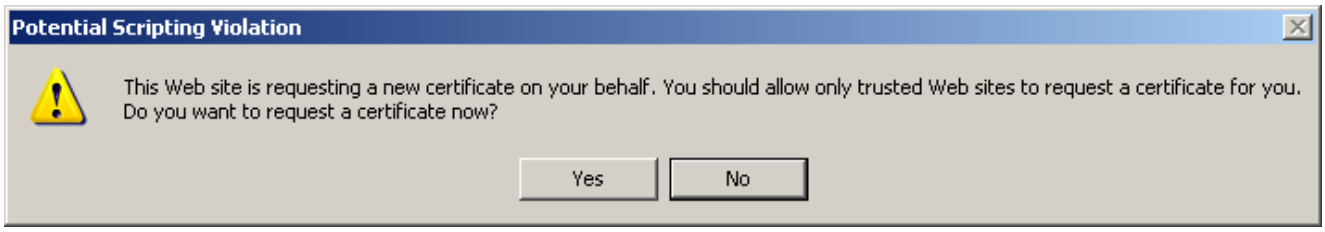

Рисунок 45

Шаг 9: выберите ключевой носитель, в котором будет размещен контейнер с секретным ключом, например, Реестр, и нажмите `OK`. В целях безопасности контейнер с секретным ключом лучше размещать на внешнем носителе (eToken), который будет храниться только у пользователя.

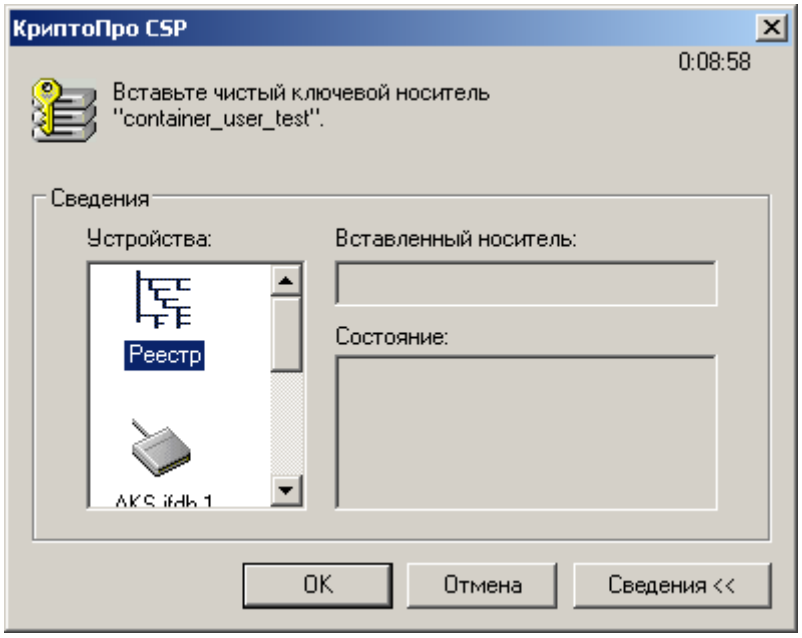

Рисунок 46

Шаг 10: для создания ключевой пары в режиме КС1 появляется окно для биологической инициализации ДСЧ – нажмите любые клавиши или подвигайте мышкой: В режиме КС2 такое окно не появляется.

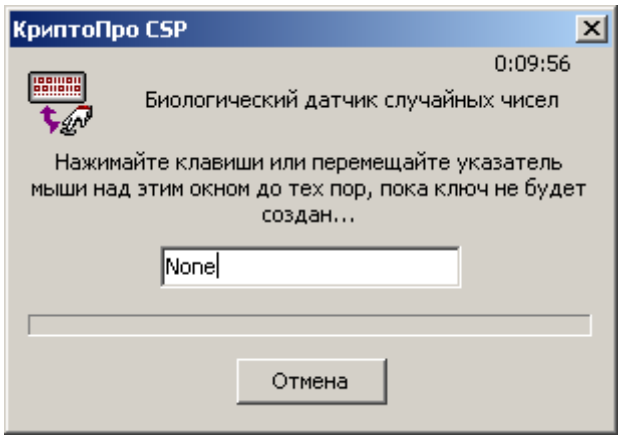

Рисунок 47

Шаг 11: задайте пароль на контейнер с секретным ключом и нажмите OK:

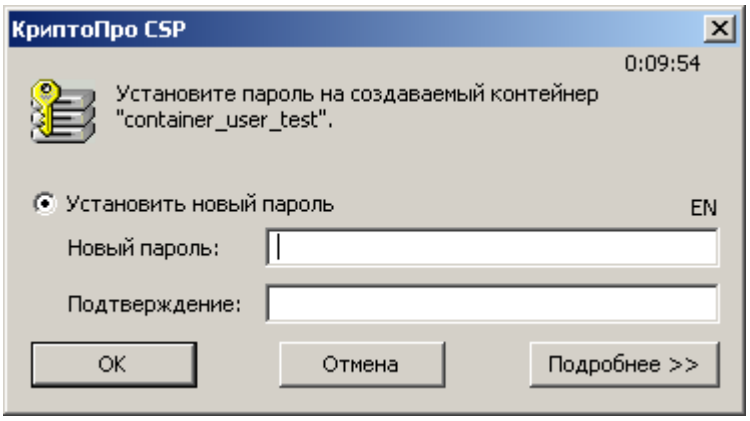

Рисунок 48

Таким образом, ключевая пара – открытый и секретный ключи созданы. Секретный ключ размещен в контейнере в ключевом носителе Реестр на компьютере пользователя и защищен паролем. А на основе открытого ключа Удостоверяющий Центр создаст сертификат пользователя.

Шаг 12: Удостоверяющий Центр сразу издал сертификат пользователя и прислал об этом уведомление (Рисунок 49). Выберите предложение “Install this certificate”, чтобы получить сертификат пользователя из Удостоверяющего Центра и разместить его в контейнере с секретным ключом, в нашем примере – в Реестре.

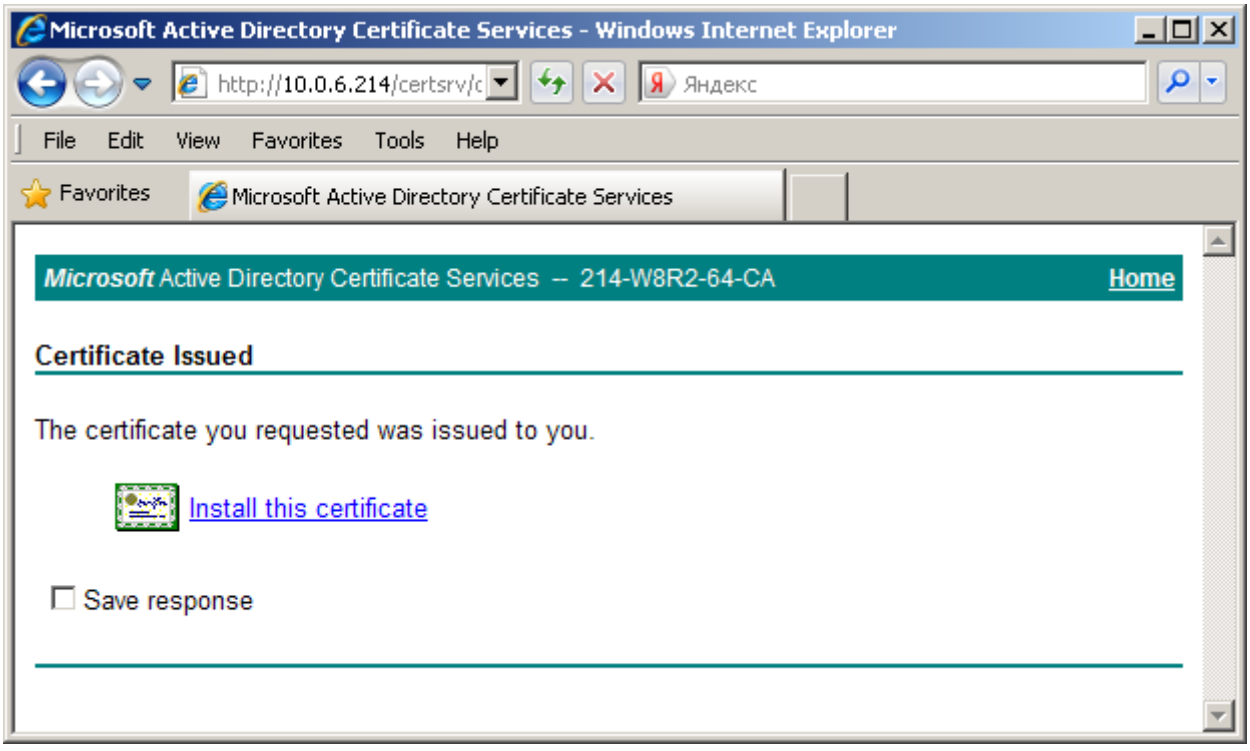

Рисунок 49

Шаг 13: появляется предупреждение (Рисунок 50), нажмите кнопку `Yes`, чтобы продолжить:

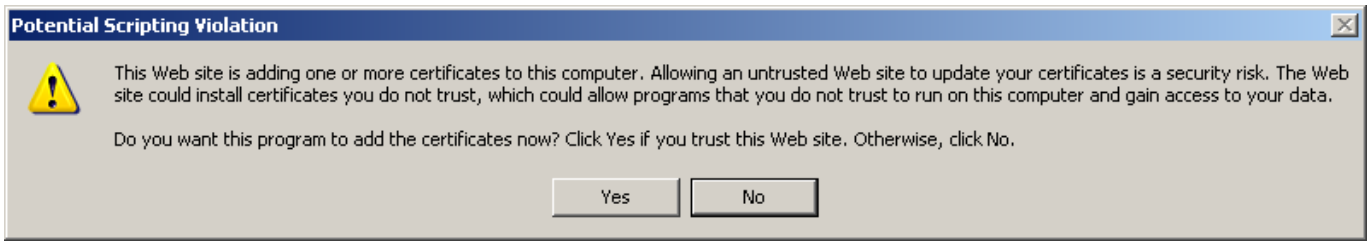

Рисунок 50

Шаг 14: еще раз введите пароль на контейнер с секретным ключом и нажмите `OK` (Рисунок 51):

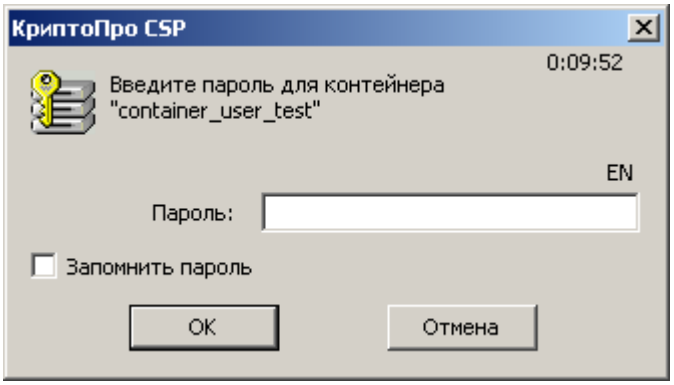

Рисунок 51

Выдается сообщение, что сертификат пользователя успешно размещен в контейнере с секретным ключом (Рисунок 52).

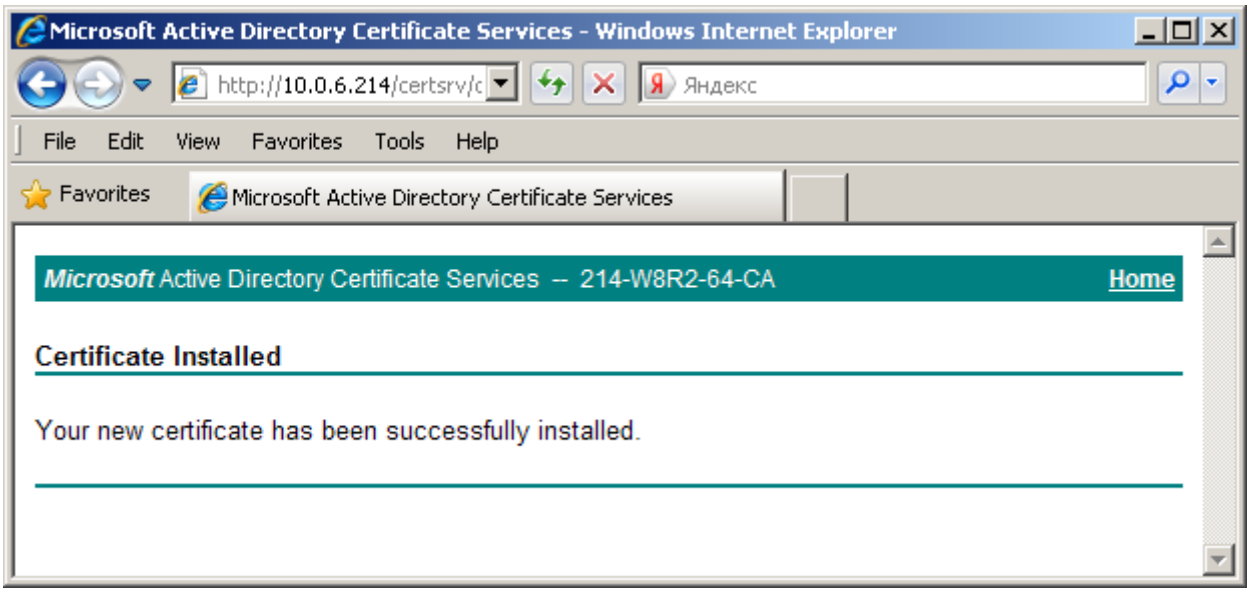

Рисунок 52

Сертификат пользователя можно получить из Удостоверяющего Центра и другими путями, но описанный здесь наиболее удобен.

В контексте безопасности компьютера, пользователь не может запрашивать сертификат компьютера через интернет с использованием обозревателя Internet Explorer. Поэтому, чтобы получить контейнер с сертификатом для компьютера, необходимо скопировать контейнер с локальным сертификатом, который был получен из Удостоверяющего центра в контейнер компьютера. Эти действия выполняются при помощи продукта «КриптоПро CSP» и описаны в следующем разделе.

4.4.1.1 Копирование контейнера

Для копирования контейнера с локальным сертификатом пользователя в контейнер компьютера выполните следующие действия:

Шаг 1: запустите продукт «КриптоПро CSP».

Шаг 2: войдите во вкладку Сервис и нажмите кнопку Скопировать контейнер…

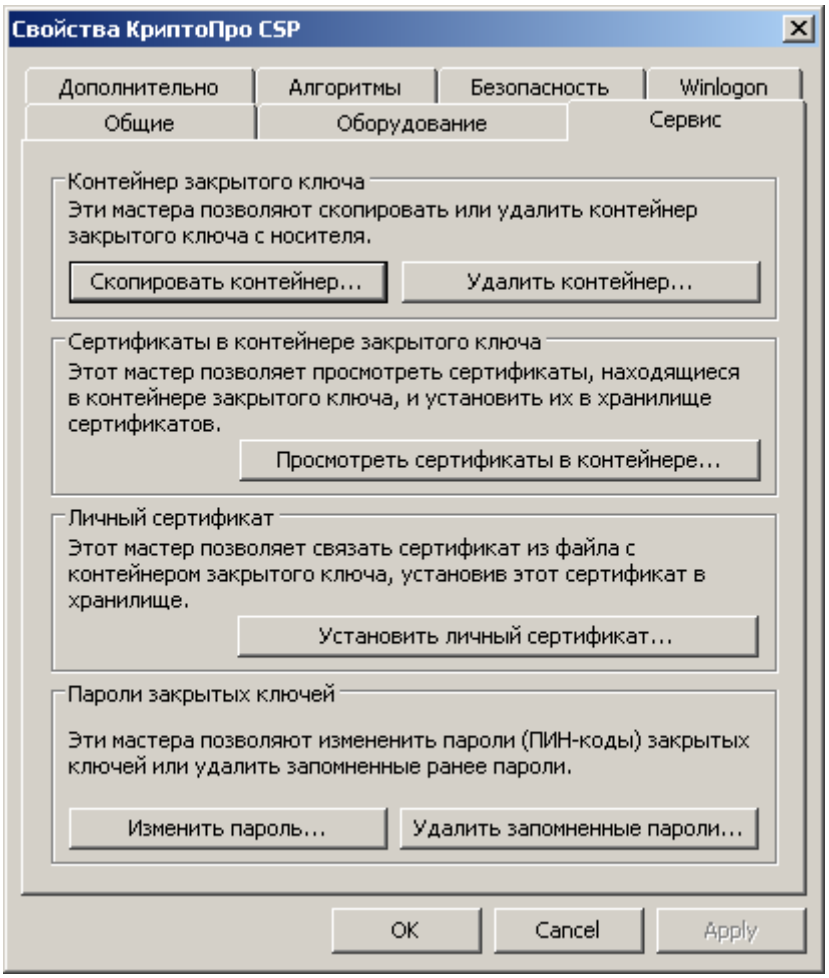

Рисунок 53

Шаг 3: в следующем окне для указания контейнера поставьте переключатель в положение `ключевой контейнер Пользователя` и нажмите кнопку `Обзор…`

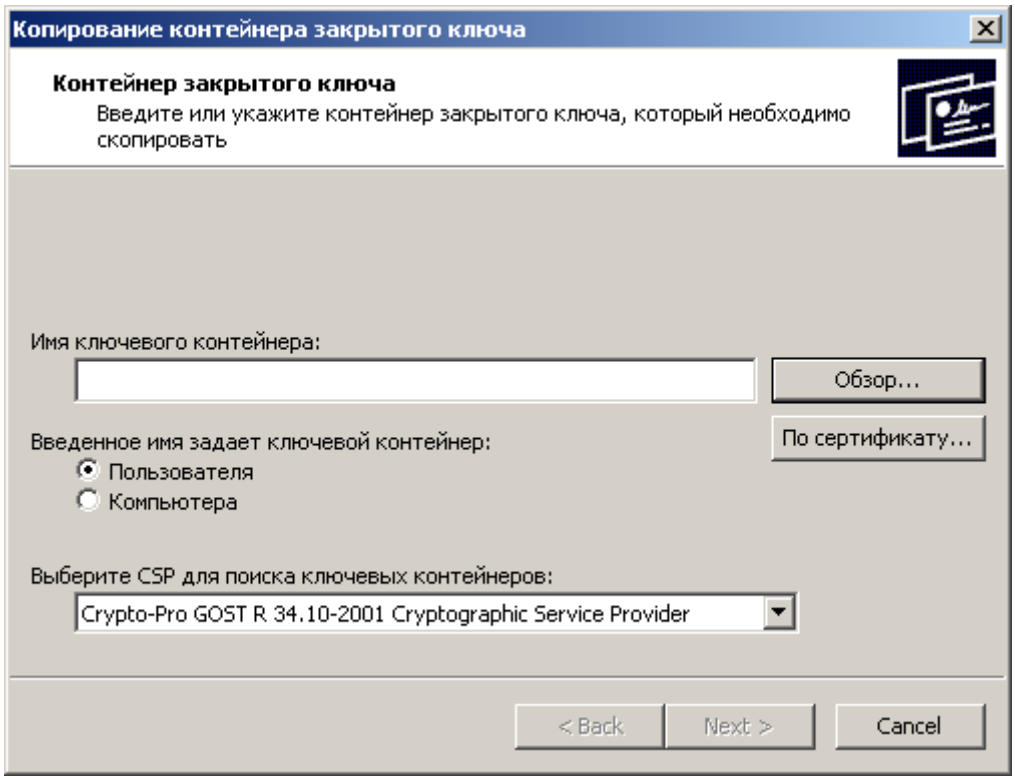

Рисунок 54

Шаг 4: поставьте переключатель в положение `Уникальные имена` и выберите контейнер с локальным сертификатом, который был получен из Удостоверяющего центра.

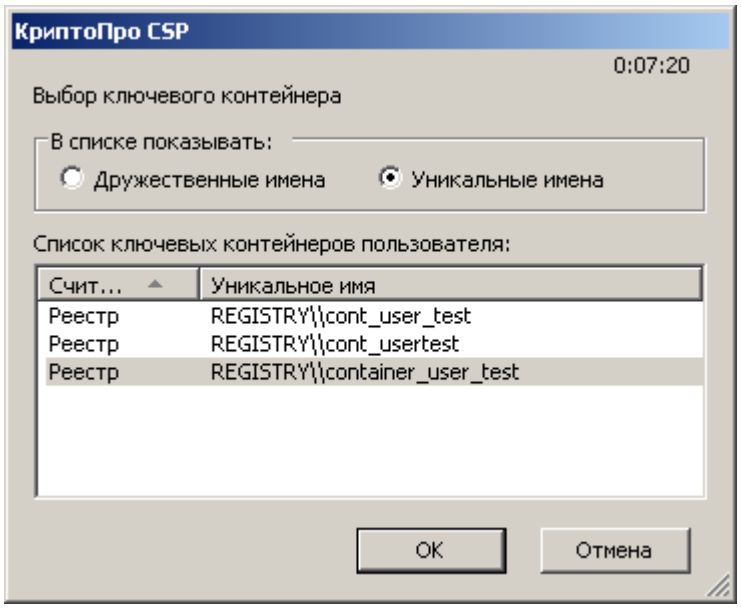

Рисунок 55

Шаг 5: поставьте переключатель в положение `ключевой контейнер Пользователя` и нажмите `Next`.

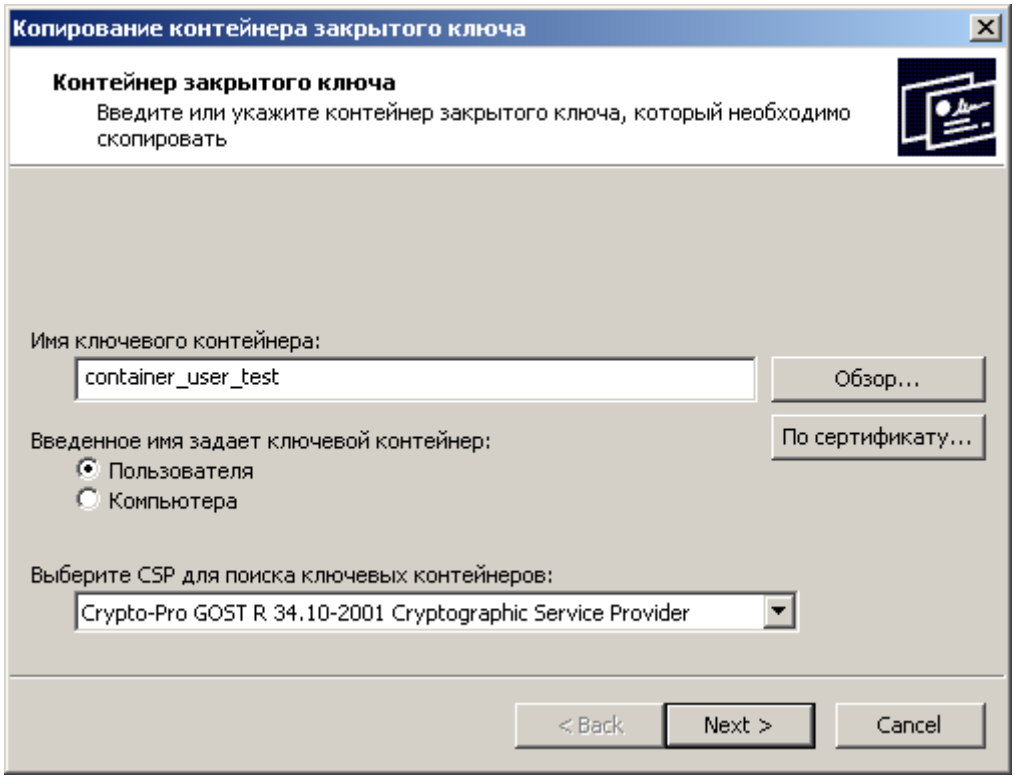

Рисунок 56

Шаг 6: задайте имя ключевого контейнера, на который будет выполняться копирование, поставьте переключатель в положение `Ключевой контейнер Компьютера` и нажмите кнопку `Finish`.

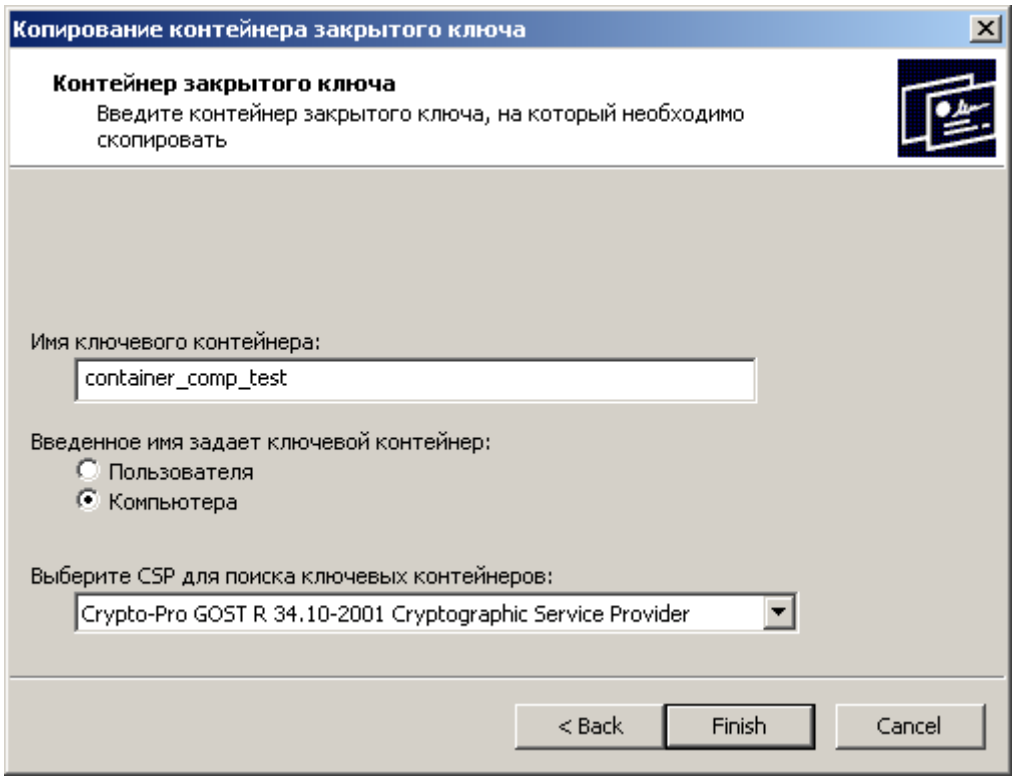

Рисунок 57

Шаг 7: выберите ключевой носитель, например Реестр, для размещения контейнера с секретным ключом и нажмите OK.

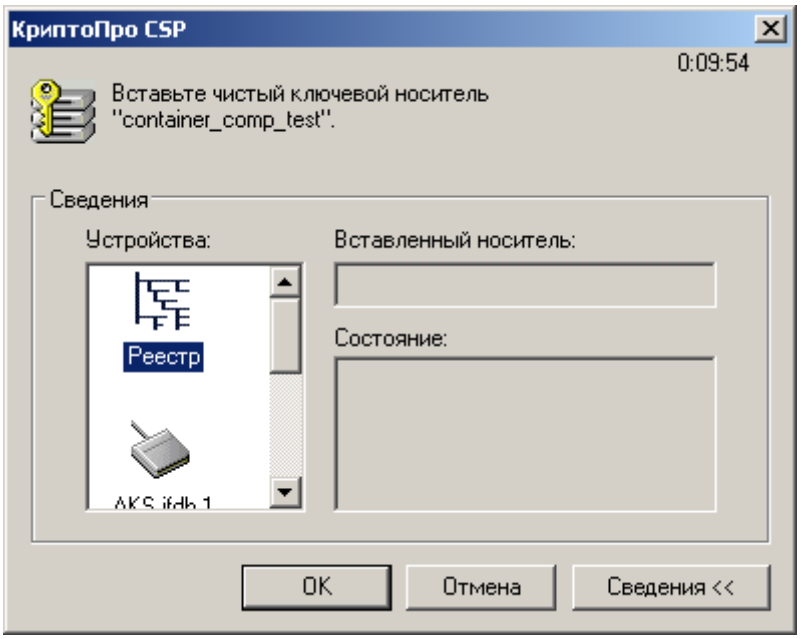

Рисунок 58

Шаг 8: установите пароль на создаваемый контейнер и нажмите OK.

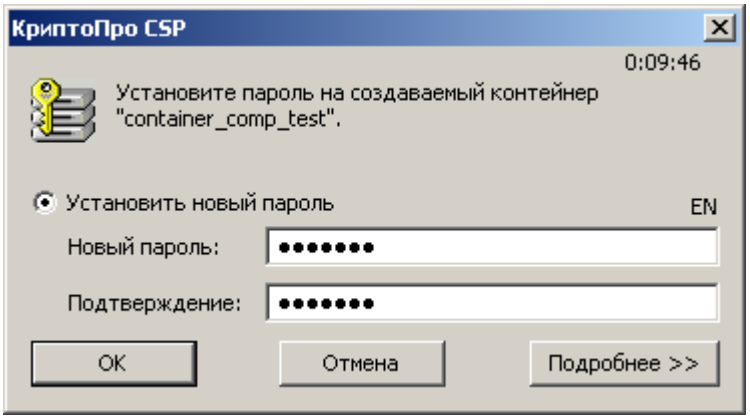

Рисунок 59

Для регистрации локального сертификата на шлюзе безопасности необходимо экспортировать локальный сертификат из контейнера в файл, поэтому перейдите к следующему разделу.

4.4.2 Экспортирование сертификата пользователя в файл

На компьютере пользователя в ключевом носителе Реестр находится контейнер, который содержит сертификат пользователя и секретный ключ этого сертификата. Для экспортирования сертификата в файл выполните следующие действия:

Шаг 1: запустите продукт «КриптоПро CSP» – `Пуск – Настройка – Панель управления – КриптоПро CSP`

Шаг 2: войдите во вкладку Сервис (Рисунок 60) и нажмите кнопку `Просмотреть сертификаты в контейнере…`

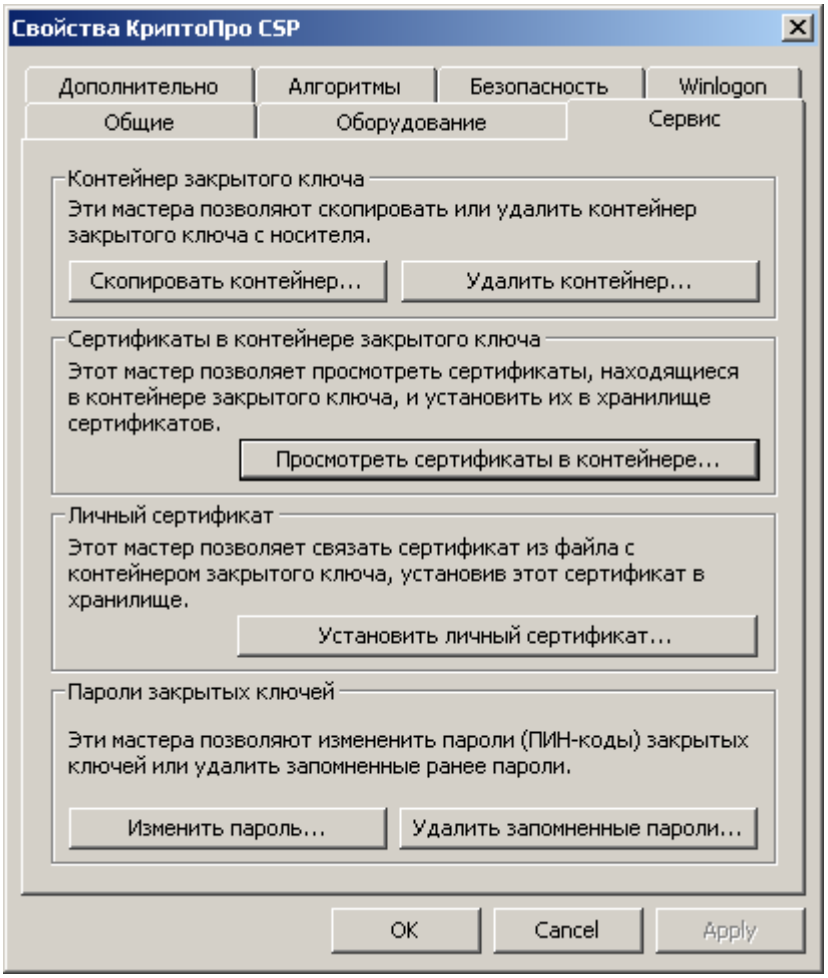

Рисунок 60

Шаг 3: для указания контейнера поставьте переключатель в положение `Компьютера` и нажмите кнопку `Обзор`…

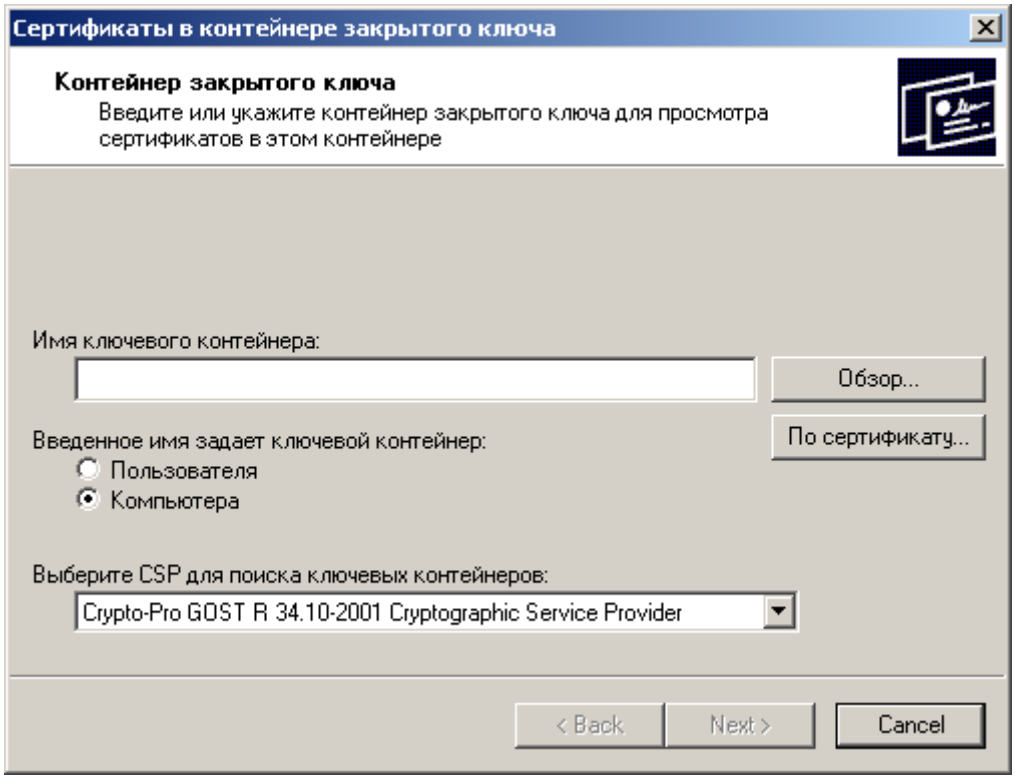

Рисунок 61

Шаг 4: в окне со списком контейнеров, размещенных в Реестре, поставьте переключатель в положение `Уникальные имена` и выберите контейнер, в котором лежит секретный ключ и сертификат пользователя. Нажмите кнопку `OK`:

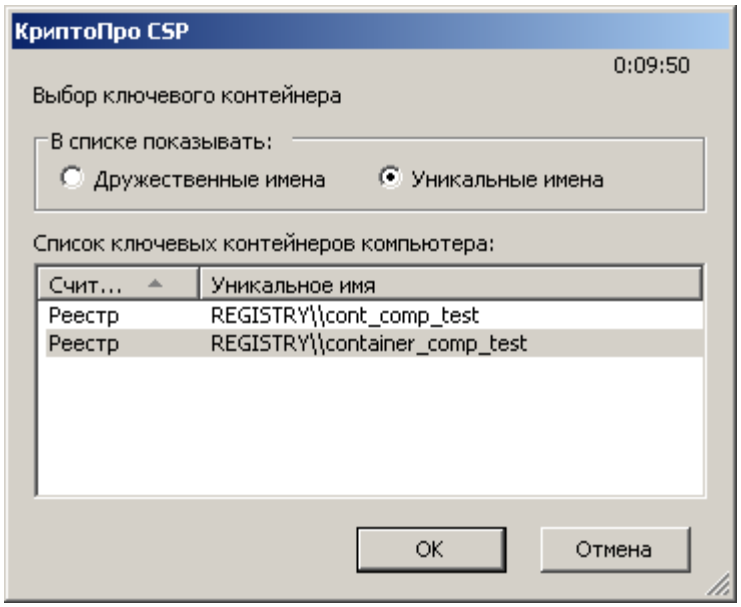

Рисунок 62

Шаг 5: выбор контейнера произведен, нажмите кнопку `Next`:

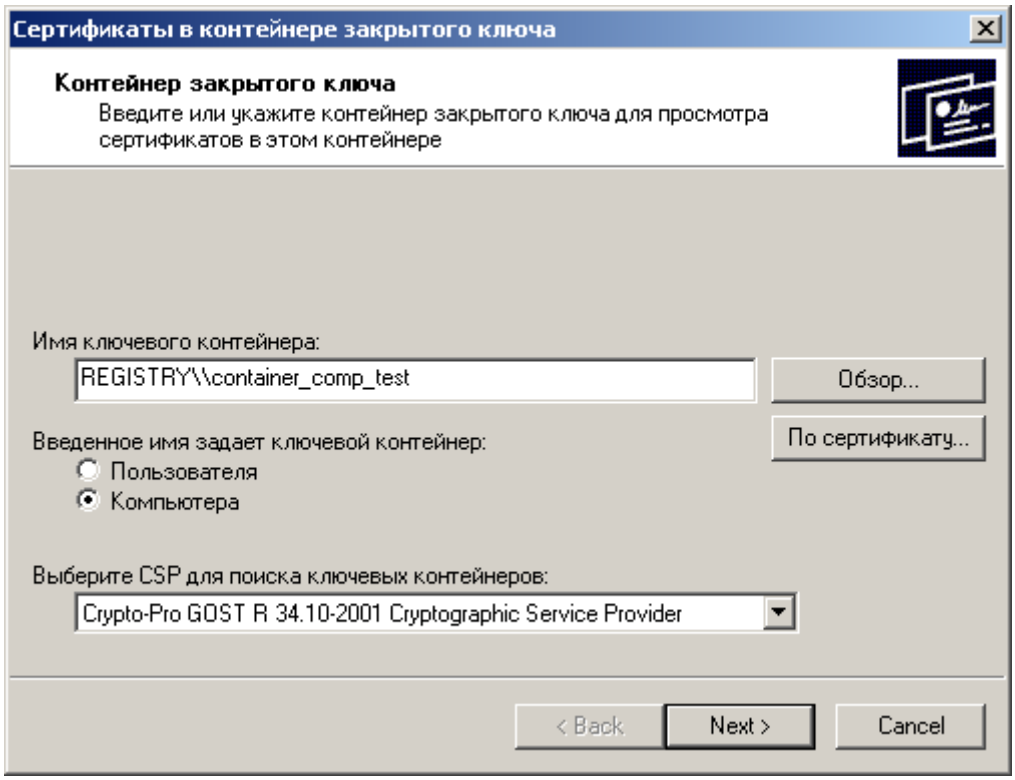

Рисунок 63

Шаг 6: следующее окно показывает поля сертификата пользователя, нажмите кнопку `Свойства`:

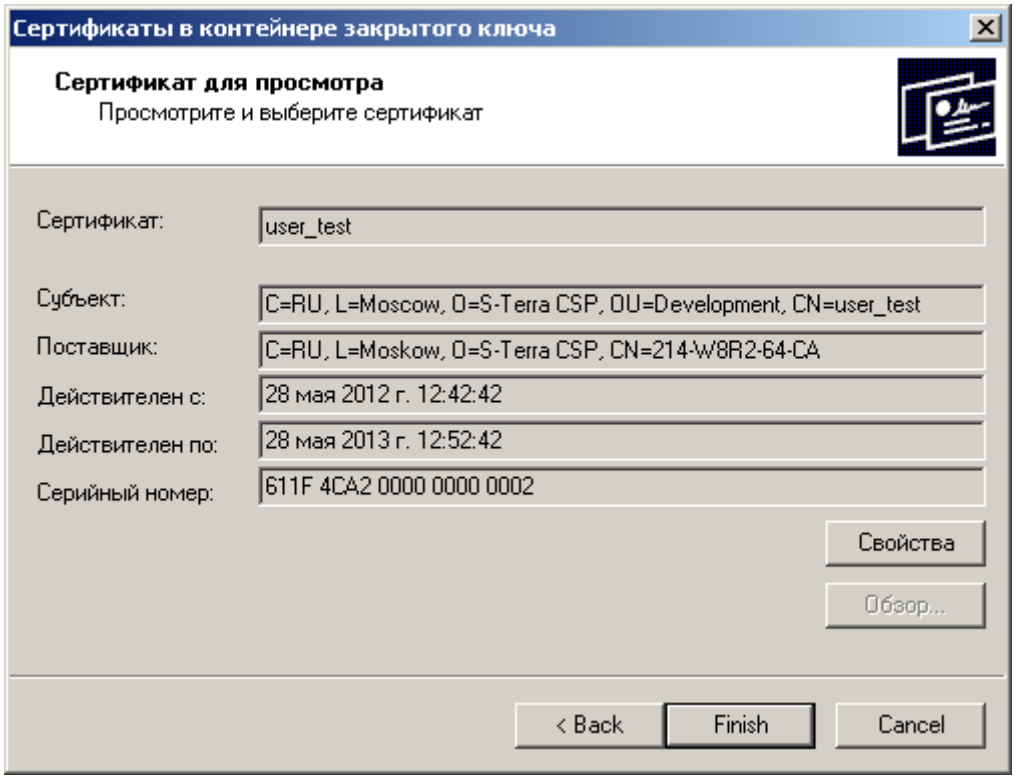

Рисунок 64

Шаг 7: выберите вкладку Detail и нажмите кнопку `Copy to File…`

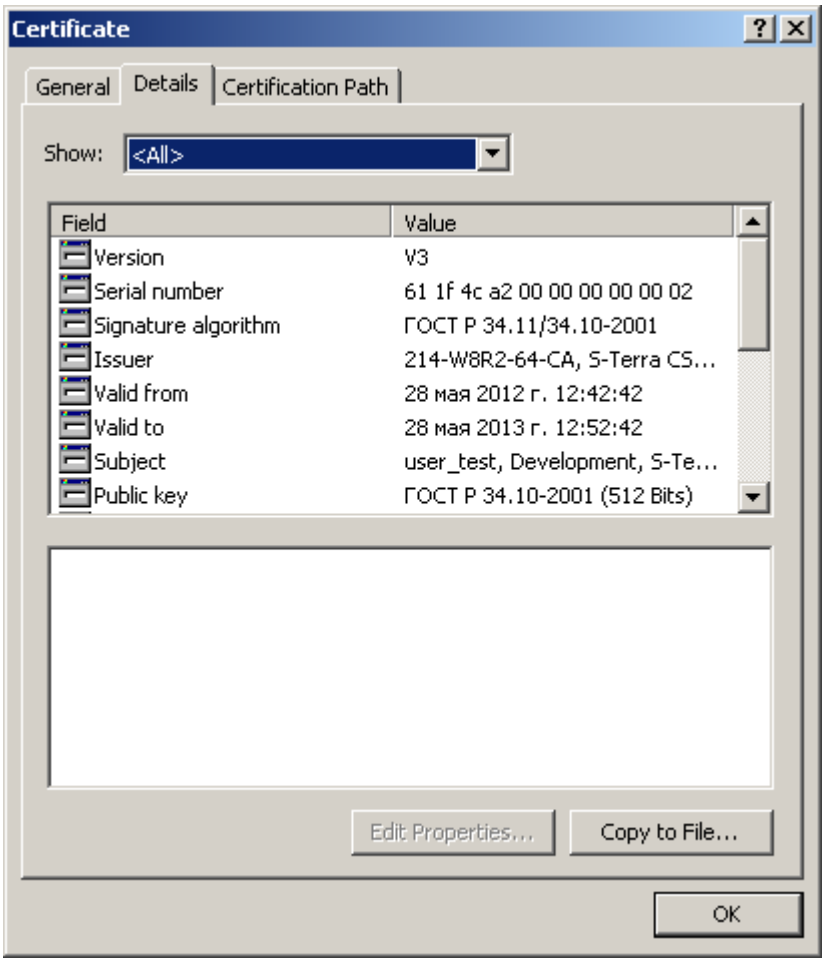

Рисунок 65

Шаг 8: в окне визарда нажмите кнопку `Next`:

Рисунок 66

Шаг 9: установите переключатель во второе положение, чтобы экспортировать в файл только сертификат без секретного ключа и нажмите `Next`:

Рисунок 67

Шаг 10: выберите формат файла сертификата – `DER encoded binary X.509 (.CER)` и нажмите `Next`:

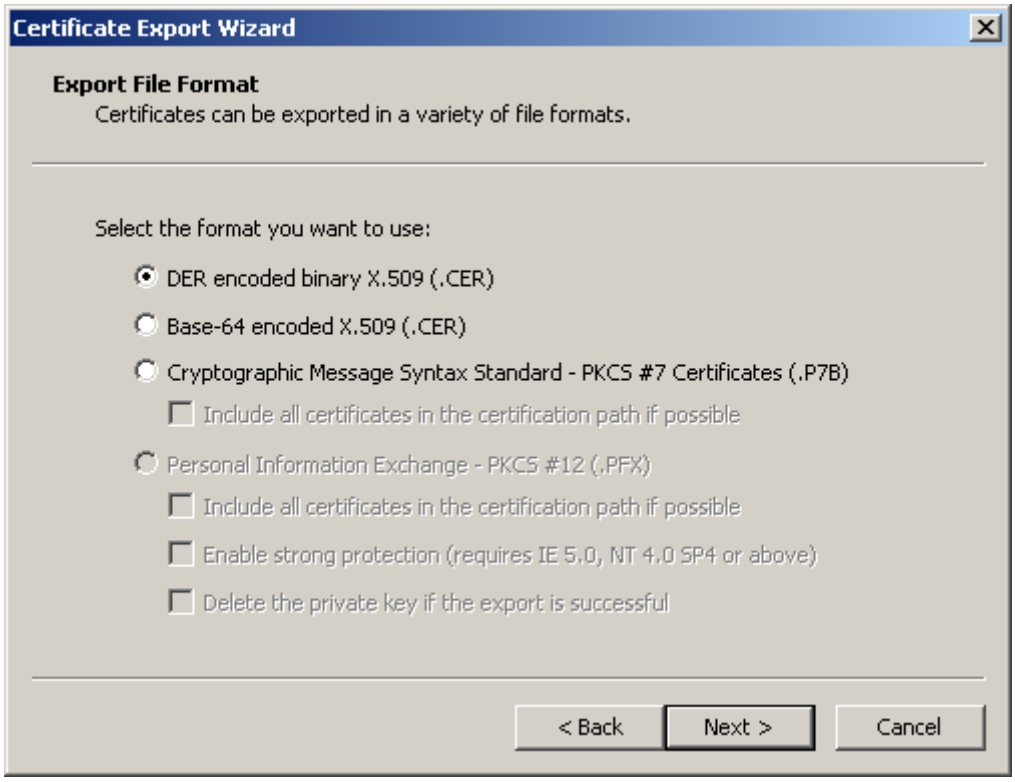

Рисунок 68

Шаг 11: укажите имя файла, в который экспортируется сертификат, и нажмите `Next`:

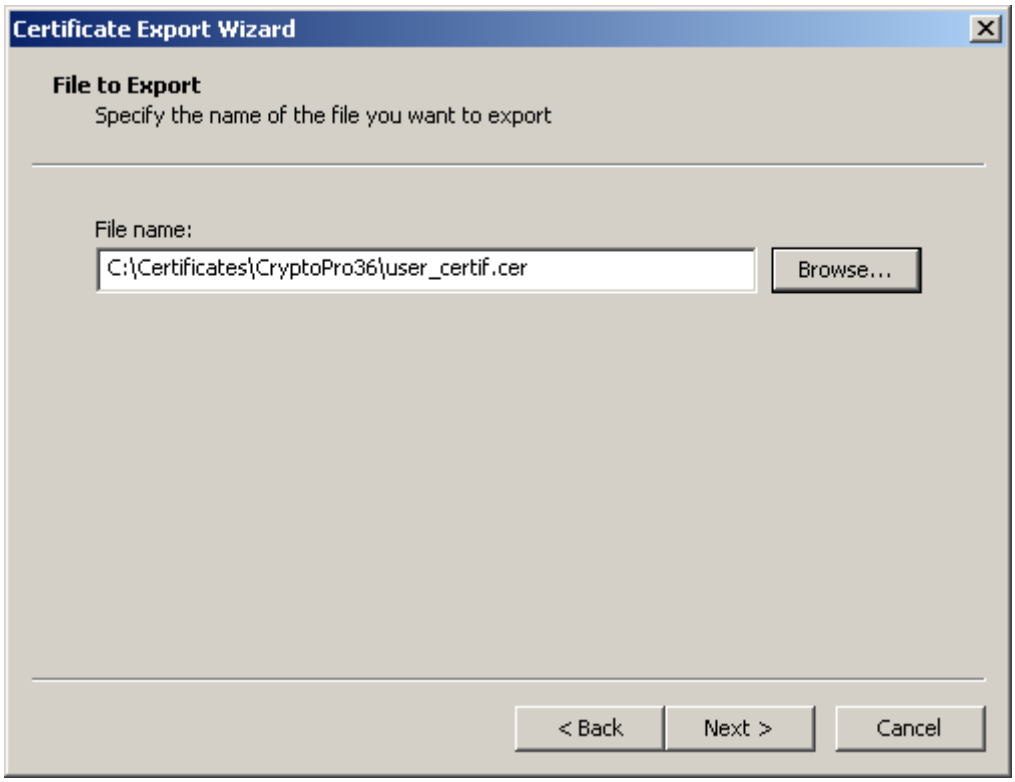

Рисунок 69

Шаг 12: экспортирование сертификата пользователя в файл закончено, нажмите `Finish`.

Рисунок 70

На этом создание сертификата пользователя и CA сертификата закончено, они оба экспортированы в файлы.

4.5 Создание сертификата пользователя с использованием криптобиблиотеки, разработанной компанией «С-Терра СиЭсПи»

Создать контейнер с ключевой парой и запрос на сертификат можно при помощи утилиты `cont_mgr`, расположенной в каталоге `C:\Program Files\S-Terra Client AdminTool st` и предназначенной для работы с контейнерами. Утилита подробно описана в «Руководстве пользователя» в разделе «Специализированные команды».

В качестве Удостоверяющего Центра воспользуемся тем, который описан в разделе «Установка и настройка Удостоверяющего Центра. Создание СА сертификата», и создан с использованием СКЗИ «КриптоПро CSP» и Microsoft Certification Authority.

Шаг 1: Создадим контейнер с ключевой парой, используя утилиту `cont_mgr`. В приведенном ниже примере создается контейнер с именем `ContName1` , общий для всех пользователей и задается PIN к контейнеру:

```
C:\Program Files\S-Terra Client AdminTool st>cont_mgr create -
cont ContName1 -PIN 1234
```

Шаг 2: Затем, используя ту же утилиту, подготовим запрос на сертификат в формате PEM, задав Distinguished Name `"C=ru,CN=user1,O=S-Terra"`, указав имя и PIN ранее созданного контейнера, и сохранив запрос в файл `file_req`:

```
C:\Program Files\S-Terra Client AdminTool st>cont_mgr request -o
file_req -n "C=ru,CN=user1,O=S-Terra" -cont ContName1 -PIN 1234
-pem
```

Шаг 3: Запустите браузер. Укажите адрес сервера Удостоверяющего Центра и запустите утилиту `certsrv` (Certificate Service).
В нашем примере `http://10.0.12.205/certsrv/` (Рисунок 71).

Шаг 4: В появившемся окне выберите задачу - `Request a certificate`.

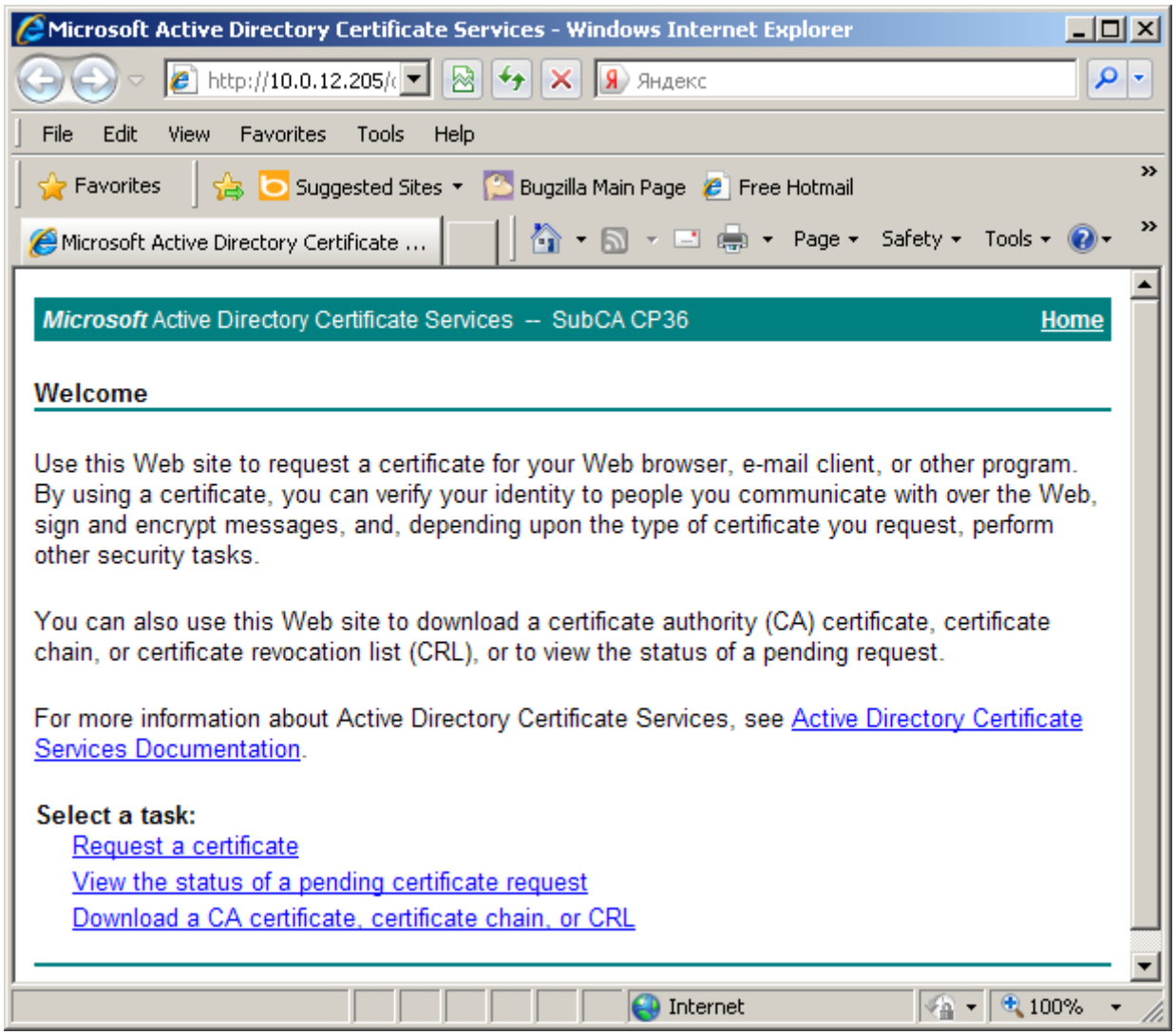

Рисунок 71

Шаг 5: Выберите расширенный запрос на сертификат – предложение `advanced certificate request` (Рисунок 72):

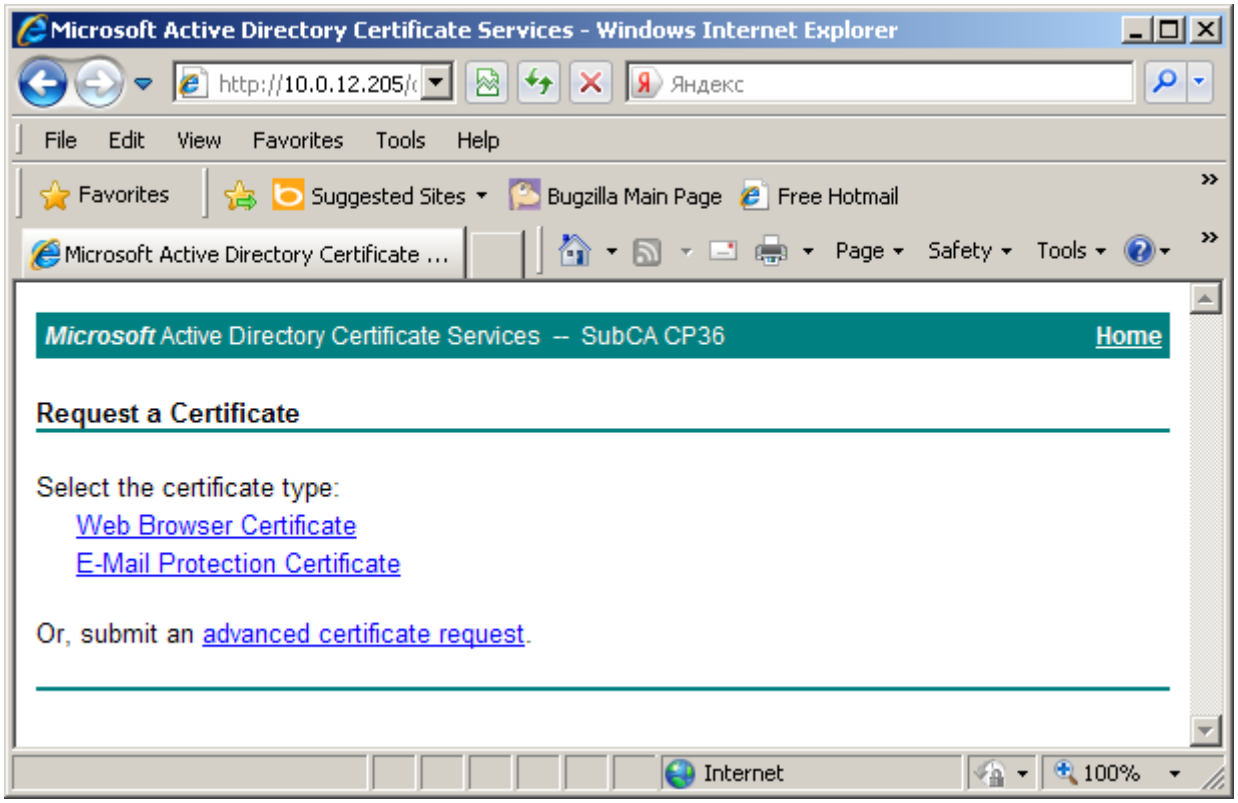

Рисунок 72

Шаг 6: Выберите предложение `Submit a certificate request by using a base 64-encoded CMC or PKCS#10file, or submit a renewal request by using a base 64-encoded PKCS#7 file` (Рисунок 73):

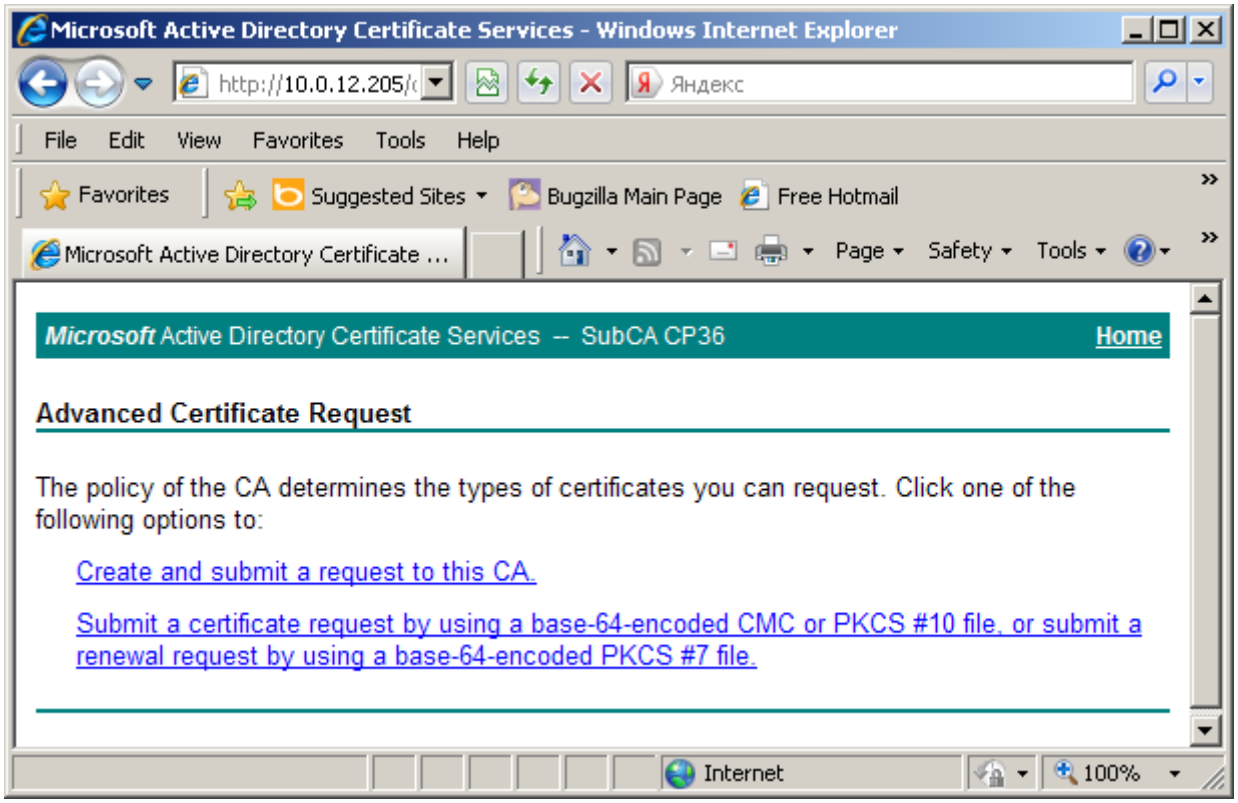

Рисунок 73

Шаг 7: Скопируйте запрос из файла (`file_req`), в котором ранее был сохранен запрос на сертификат, подготовленный с помощью утилиты `cont_mgr` (Рисунок 74) в соответствующее поле и нажмите `Submit`:

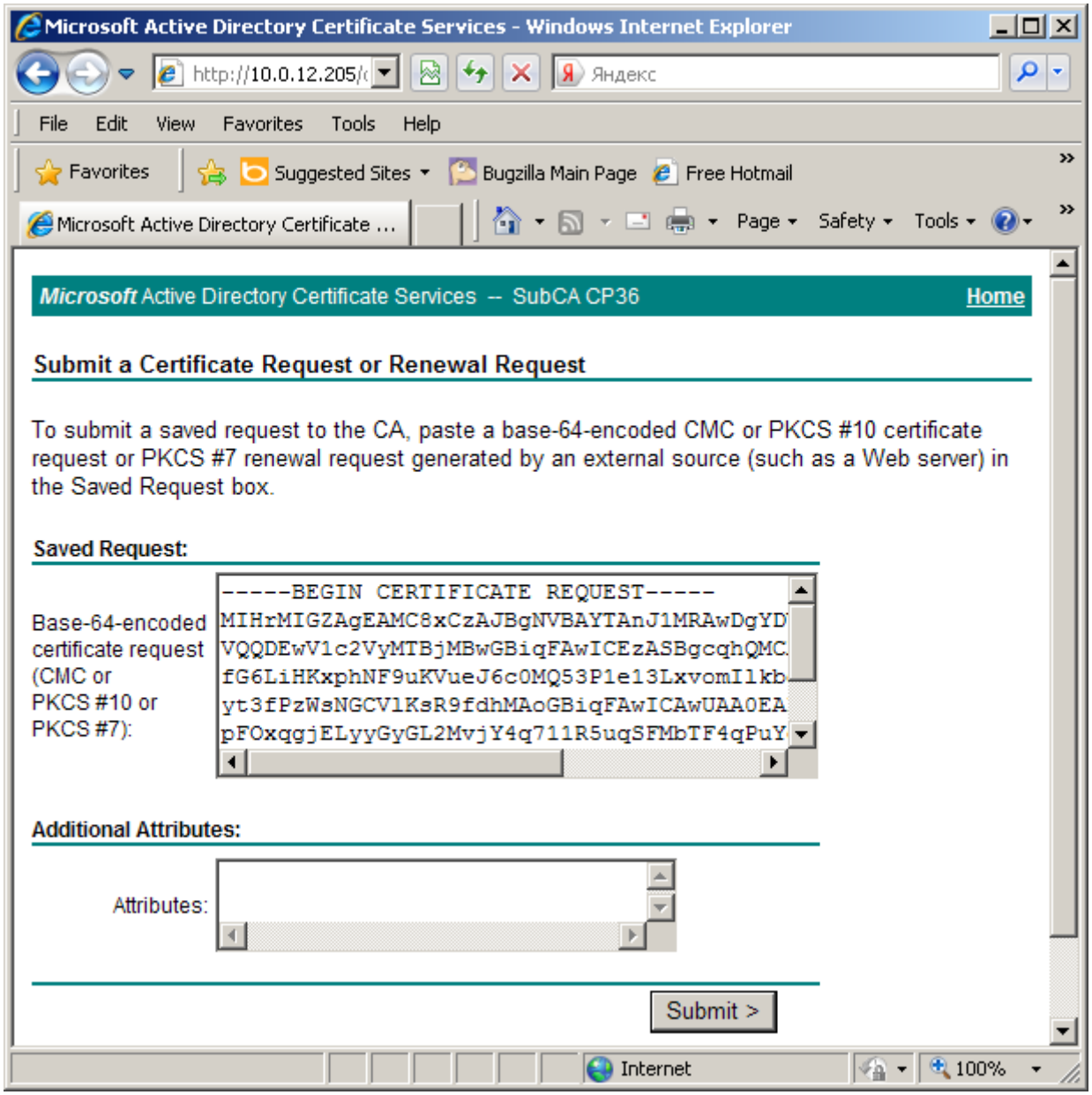

Рисунок 74

Шаг 8: Загрузите и сохраните сертификат (Рисунок 75).

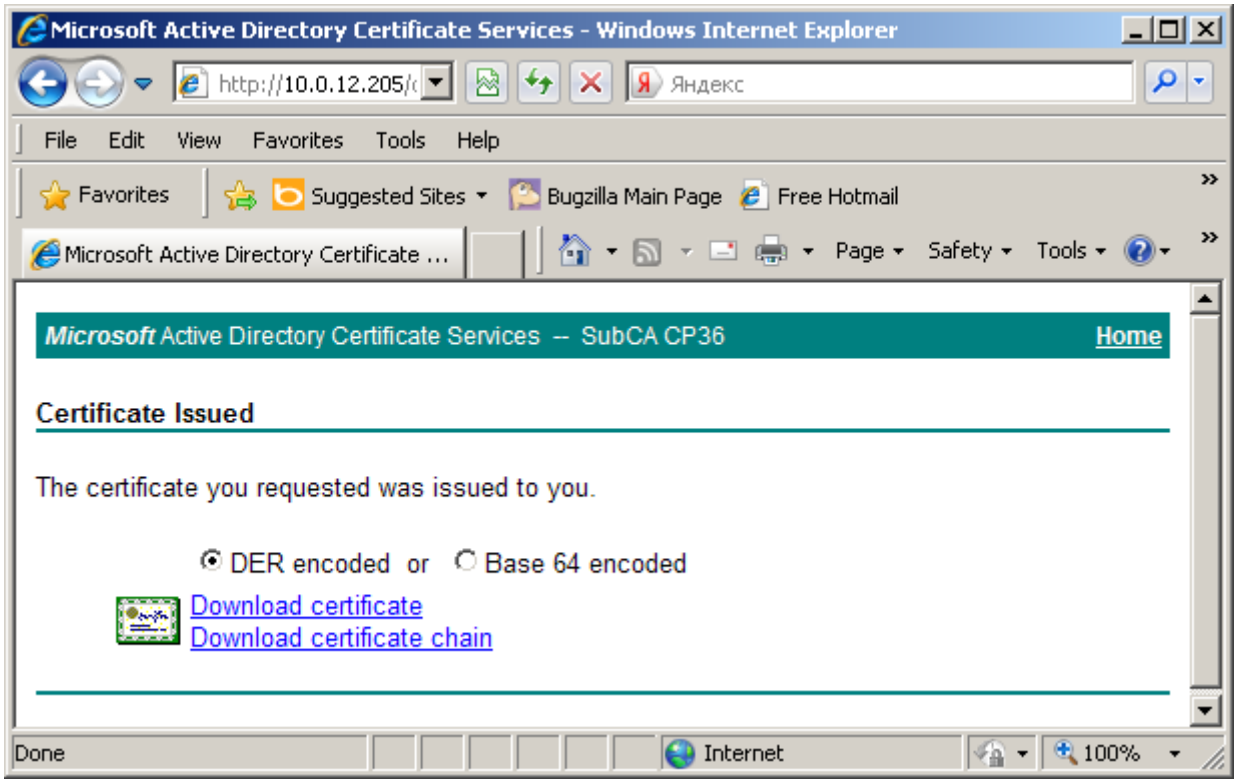

Рисунок 75

4.6 Особенности генерации ключевой пары для режима защиты КС2, если для ССДЗ не поддерживается функциональность ДСЧ

Существуют некоторые особенности генерации ключевой пары и создания запроса на сертификат в случае использования «Программного комплекса С-Терра Клиент» в режиме защиты КС2, т.к. для некоторых ССДЗ не поддерживается функциональность ДСЧ.

Возможны различные варианты, в зависимости того, какая криптографическая библиотека применяется в «С-Терра Клиент»:

- Если используется криптобиблиотека, разработанная компанией «С-Терра СиЭсПи», то при генерации ключевой пары возможно использование биологического ДСЧ.
- Если используется СКЗИ «КриптоПро CSP»:
  - Администратор, на отдельной машине, с установленными СКЗИ «КриптоПро CSP» (класс защиты КС2) и электронным замком «Соболь», изготавливает внешнюю гамму, доставляет ее безопасным способом на «С-Терра Клиент» и затем, при помощи утилиты `cert_mgr`, создает ключевую пару и запрос на сертификат. Подробнее изготовление внешней гаммы описано ниже.

4.6.1.1 Изготовление внешней гаммы

Внешнюю гамму можно применять на «С-Терра Клиент», независимо от используемой криптобиблиотеки.

На отдельной машине должно быть установлено СКЗИ «КриптоПро CSP» (класс защиты КС2) и электронный замок «Соболь».

Для изготовления внешней гаммы в командной строке запустите утилиту `genkpim`, например:

```
genkpim.exe 500 12121111 f:\gamma
```

`500` – необходимое количество случайных отрезков гаммы для записи на носитель,

`12121111` – номер комплекта внешней гаммы (8 символов в 16-ричном коде),

`f:\gamma` – путь на носителе, по которому будет записан файл с внешней гаммой.

В результате выполнения команды создается файл `kis_1`, который записывается на носитель по пути `f:\gamma` дублированием в два каталога: `DB1` и `DB2`.

Далее действия будут различаться в зависимости от используемого СКЗИ:

- В случае использования СКЗИ «КриптоПро CSP 3.6», выполните копирование файлов с внешней гаммой с носителя на «С-Терра Клиент». Название каталога, в который следует скопировать `DB1` и `DB2`, можно посмотреть при помощи «КриптоПро CSP» во вкладке `Оборудование`, нажав кнопку `Настроить ДСЧ`, далее выберите ДСЧ `Создать исходный материал` (если такого ДСЧ нет – добавьте его) и нажмите кнопку `Свойства`, во вкладке `Настройка` показан `Путь к файлам db` (обычно `c:\cpsd`).

  Если используется «КриптоПро CSP 3.9» каталог, в который будут копироваться `DB1` и `DB2` следует создать самостоятельно.

- В случае использования криптобиблиотеки от компании «С-Терра СиЭсПи», выполните копирование одного файла с внешней гаммой с носителя на «С-Терра Клиент», в каталог `C:\Documents and Settings\All Users\s-terra\ext-gamma\`.
  Переименуйте файл с внешней гаммой в `eg_data`.
  В конфигурационном файле `/etc/S-Terra/skzi.conf` пропишите путь до каталога с внешней гаммой:

```
ExtGammaPath=C:\Documents and Settings\All Users\s-terra\ext-gamma\
```

Надёжно удалите файлы с внешней гаммой с носителя. Перезагрузите «С-Терра Клиент».

Далее, в случае использования СКЗИ «КриптоПро CSP», выполните настройку ДСЧ.

4.6.1.2 Настройка ДСЧ

Для возможности использовать внешнюю гамму, на управляемом устройстве запустите «КриптоПро CSP 3.6» (Рисунок 76), во вкладке `Оборудование` нажмите кнопку `Настроить ДСЧ`. В открывшемся окне предложение «`КриптоПро Исходный Материал`» переместите в верхнюю строку, как первый датчик случайных чисел и нажмите кнопку `OK`.

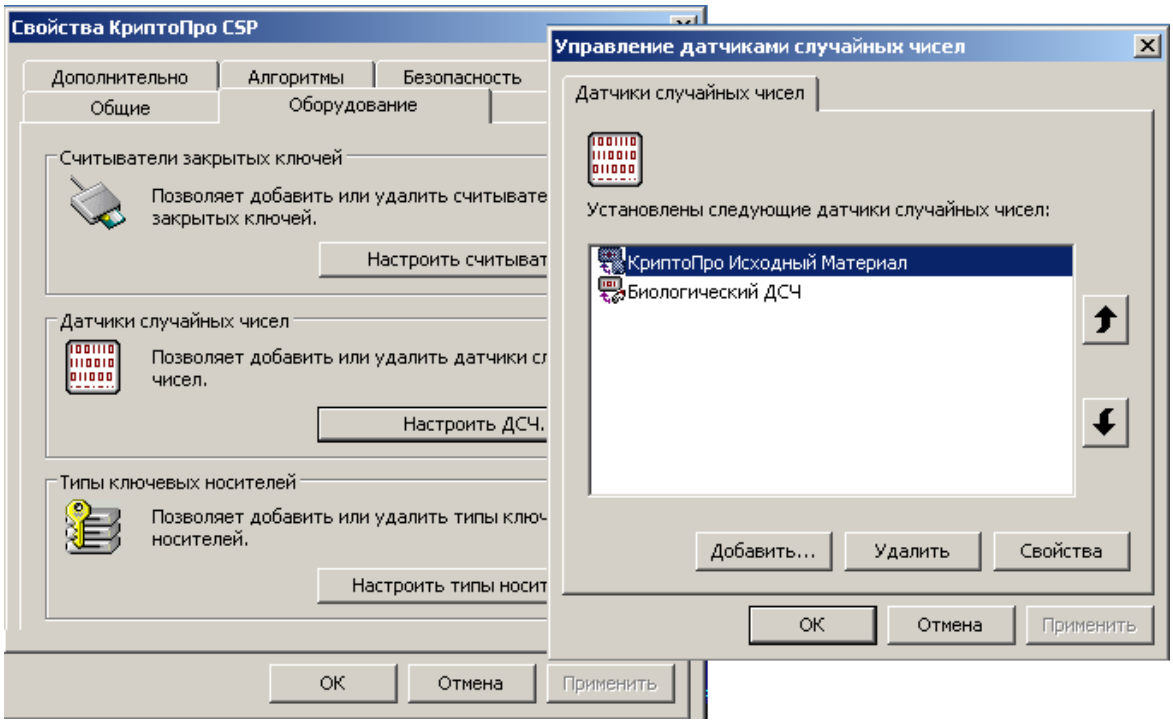

Рисунок 76

В случае использования «КриптоПро CSP 3.9» надо будет указать `Путь к папкам db`, куда была скопирована внешняя гамма.

5. Настройка нескольких сетевых интерфейсов

При необходимости создать разную политику безопасности для сетевых интерфейсов необходимо отредактировать файл `ifaliases.cf`, расположенный в каталоге Продукта. Синтаксис файла соответствует синтаксису LSP (см. описание конфигурационного файла в «Руководстве администратора». Файл содержит структуры типа "interface" с двумя обязательными полями – "pattern" и "name". Каждое поле должно иметь одно строковое значение.

Изначально файл `ifaliases.cf` содержит лишь одну строку – `interface (name="default" pattern="*")`. Чтобы иметь возможность задействовать различные интерфейсы при создании политики безопасности, нужно внести описание этих интерфейсов в файл в соответствии с форматом:

`interface (name="имя интерфейса" pattern="шаблон для имени интерфейса в ОС")`

`pattern` указывается как `<prefix>{<GUID>}`, где `<prefix>` – буквенное обозначения типа интерфейса, `GUID` – шестнадцатеричный иденитификатор интерфейса.

Возможные префиксы:

`eth` – ethernet

`wan` – интерфейс NDISWAN (dial-up и т.д.)

`ike` – виртуальный интерфейс для ikecfg.

При задании `pattern` допускается указание любых символов кроме `\0`, а также специальные символы:

',' – этим символом разделяются альтернативы,

'`*`' – при сравнении имен вместо `*` допускается подстановка любой последовательности символов.

Чтобы использовать специальные символы в имени как обычные, им нужно добавлять префикс '\' (сам символ \ записывается как `\\`).

После редактирования, необходимо пересчитать хэш-сумму измененного файла, запустив утилиту integr_mgr calc (см. «Руководство пользователя», раздел «Специализированные команды»): `integr_mgr calc -f ifaliases.cf`. Затем надо перезапустить службу S-Terra VPN Service.

6. Работа «С-Терра Клиент» с продуктами третьих производителей

6.1 Работа с Брандмауэром Windows (ОС Windows 7)

При работе продукта S-Terra Client под управлением ОС Windows 7 могут появляться проблемы, связанные с пропусканием исходящих и входящих пакетов.

Как выяснили, это связано с настройкой Брандмауэр Windows на устройстве.

Если Брандмауэр Windows выключен – проблем с пропусканием пакетов нет.

Если Брандмауэр Windows включен – он автоматически определяет типы сетей, к которым подключены интерфейсы, – «Домашние сети», «Рабочие (частные) сети» и «Общественные сети» (Рисунок 77).

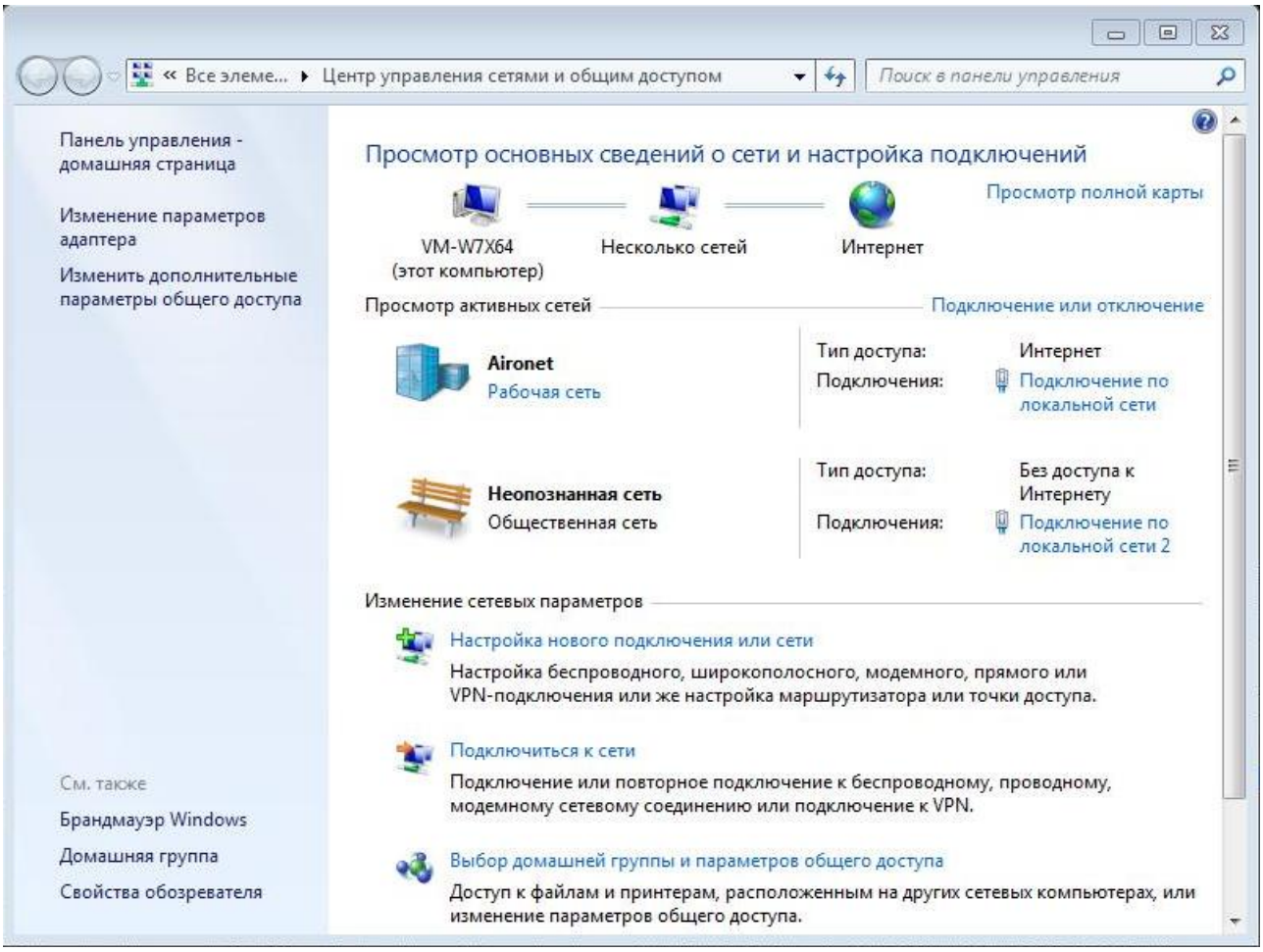

Рисунок 77

Для «Домашних сетей» и «Рабочих (частных) сетей» применяются предопределенные правила, которые пользователь не может увидеть и не может изменить. А для «Общественных сетей» имеется возможность изменять настройки брандмауэра и создавать новые правила. Изменять настройки можно по-разному, например, в окне Брандмауэр Windows выберите предложение «Дополнительные параметры» (Рисунок 78).

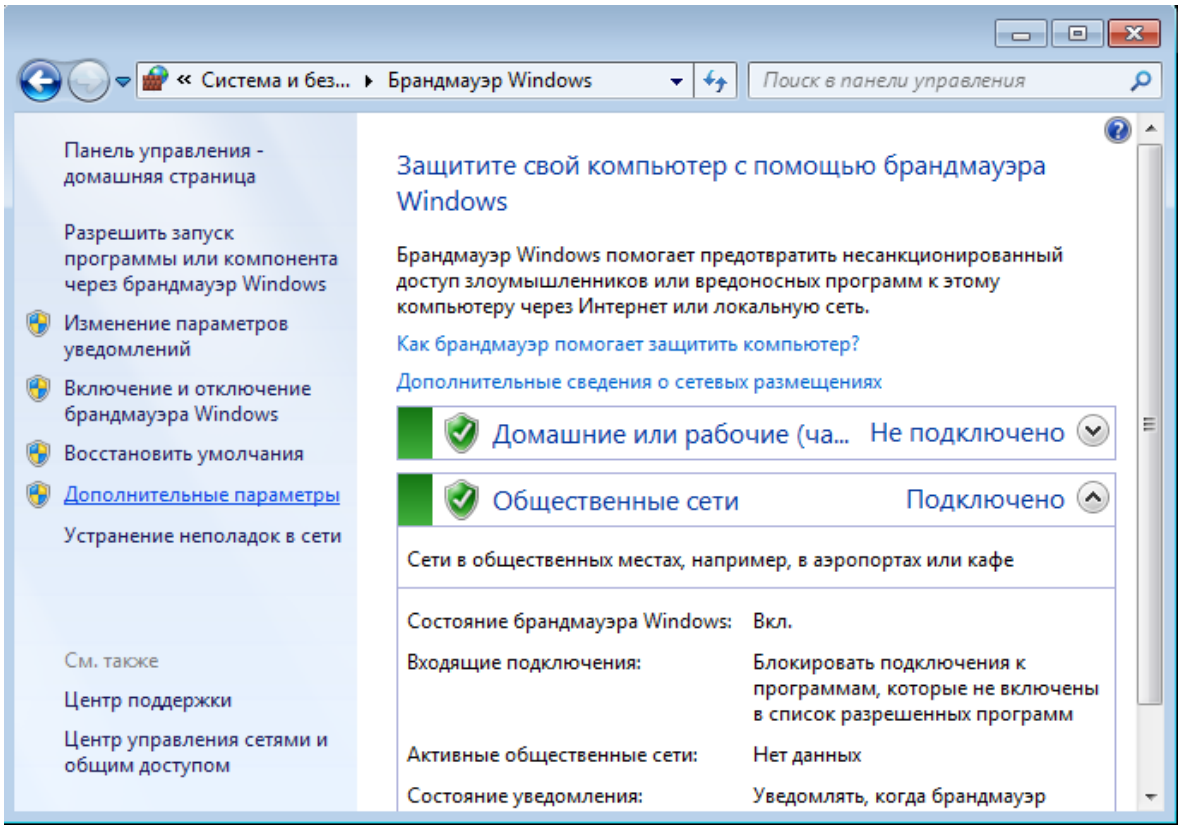

Рисунок 78

В появившемся окне (Рисунок 79) в разделах Правила для входящих и исходящих подключений создайте правила для прохождения нужного трафика.

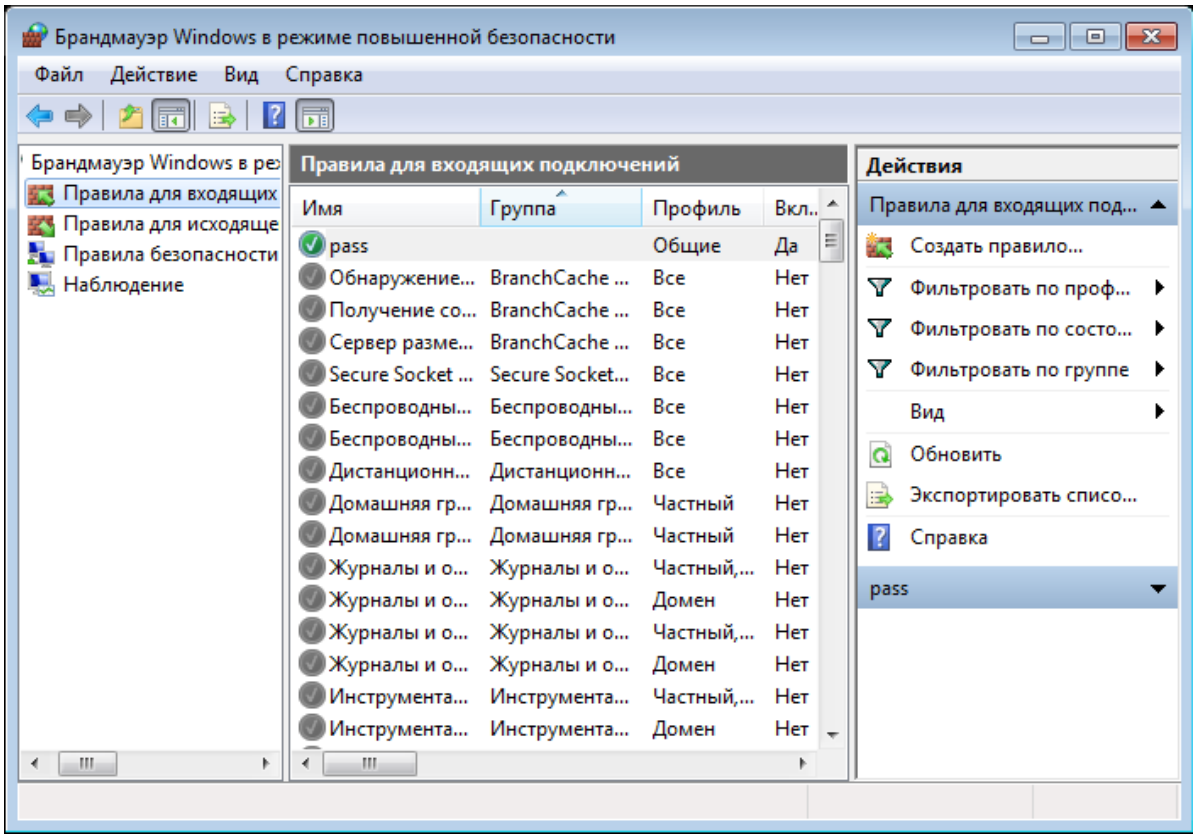

Рисунок 79

6.2 Работа с антивирусом Outpost

При работе S-Terra Client под управлением ОС Windows Vista, Windows 7 (x32), Windows 8(x32), на которых установлен антивирус Outpost, возможны проблемы с созданием соединений, использующих ikcfg-адреса. При этом в syslog появляются сообщения "`[IKECFGIF] can't enable packet forwarding`".

В этом случае необходимо выполнить следующие действия:

1. В реестре, в разделе HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Services\Tcpip\Parameters для IPEnableRouter установить значение 1.
2. Перезагрузить ОС.

