ЗАО «С-Терра СиЭсПи»
124460, г. Москва, Зеленоград, проезд 4806, д.6, этаж 4-й
Телефон: +7 (499) 940 9061
Факс: +7 (499) 940 9061
Эл.почта: information@s-terra.com
Сайт: http://www.s-terra.com

Программный комплекс “Клиент безопасности CSP VPN Client. Версия 3.1”

Руководство пользователя

РЛКЕ.00004-01 90 05

16.12.2013

Содержание

Лицензионное Соглашение

о праве пользования программным комплексом «Клиент безопасности CSP VPN Client» производства ЗАО «С-Терра СиЭсПи»

Настоящее Лицензионное Соглашение определяет условия использования законно приобретенного программного комплекса «Клиент безопасности CSP VPN Client» (далее – Изделия) Конечным Пользователем (физическим или юридическим лицом, указанным в Лицензии на использование Продукта, являющейся неотъемлемой частью настоящего Лицензионного Соглашения). Предметом настоящего Лицензионного Соглашения является возмездная передача Конечному Пользователю неисключительных непередаваемых прав пользования Изделием.

Под Изделием понимается комплекс материальных объектов (программных средств, носителей информации, кода программных Продуктов, документации в печатной и электронной формах), включенных в Спецификацию Комплекта Изделия.

Изделие может использоваться только в качестве персонального Агента защиты (устанавливаться на персональный компьютер пользователя) и не предназначено для использования в других целях. Использование Изделия в прочих системах и/или в иных целях является нарушением настоящего Лицензионного Соглашения.

Изделие может включать компоненты (программные средства, информационные носители и прочее) от третьих поставщиков. Конечный Пользователь получает права на использование этих компонент на основе Лицензий и Лицензионных Соглашений этих поставщиков, которые являются в совокупности неотъемлемой частью настоящего Лицензионного Соглашения.

Изделие в полном комплекте передается Конечному Пользователю на условиях настоящего Лицензионного Соглашения.

Изделие и его компоненты являются интеллектуальной собственностью Производителя и, при наличии третьих поставщиков, интеллектуальной собственностью третьих поставщиков и защищаются законодательством Российской Федерации об авторском и имущественном праве на объекты интеллектуальной собственности.

Установка Изделия после предъявления Конечному Пользователю текста Лицензионного Соглашения рассматривается как согласие Конечного Пользователя с условиями Лицензионного Соглашения и вступление его в законную силу, после чего настоящее Лицензионное Соглашение в соответствии со ст. 433 ГК РФ имеет силу договора между Конечным Пользователем и Производителем Изделия (ЗАО «С-Терра СиЭсПи»).

При наличии компонент третьих поставщиков Производитель является законным и полномочным представителем третьих поставщиков, если обратное не оговорено в Лицензионных Соглашениях третьих поставщиков или в других документах, регламентирующих отношения между Конечным Пользователем и третьими поставщиками.

Все компоненты третьих поставщиков объединяются в программный Продукт (комплекс) в процессе установки Изделия. Конечный Пользователь имеет право на копирование, установку и эксплуатацию всех компонент третьих поставщиков, поставленных в составе Изделия только в составе работ, связанных с эксплуатацией Изделия. Копирование, распространение, установка и эксплуатация отдельных компонент являются нарушением настоящего Лицензионного Соглашения и авторских прав как Производителя, так и третьих поставщиков (если обратное не оговорено в Лицензиях и Лицензионных Соглашениях третьих поставщиков).

Конечный Пользователь может устанавливать и использовать в рамках настоящего Лицензионного Соглашения только один экземпляр Изделия и не имеет права устанавливать и использовать большее количество экземпляров Изделия.

Конечный Пользователь не имеет права распространять Изделие в формах предоставления доступа третьим лицам к воспроизведению или к воспроизведенным в любой форме компонентам Изделия путем продажи, проката, сдачи внаем, предоставления взаймы или иными другими способами отчуждения.

Конечный Пользователь не имеет права дисассемблировать, декомпилировать (преобразовывать бинарный код в исходный текст) программы и другие компоненты Изделия, вносить какие-либо изменения в бинарный код программ и совершать относительно Изделия другие действия, нарушающие Российские и международные нормы по авторскому праву и использованию программных средств.

Настоящее Лицензионное Соглашение вступает в силу с момента установки Изделия и действует на протяжении всего срока использования Изделия.

Неисполнение требований настоящего Лицензионного Соглашения является нарушением Закона Российской Федерации "О правовой охране программ для электронных вычислительных машин и баз данных" и преследуется по закону.

Настоящее Лицензионное Соглашение предоставляет Конечному Пользователю Ограниченные гарантии, состоящие в том, что

1. В случае, если в ходе эксплуатации Изделия Конечным Пользователем или любым третьим лицом будет обнаружена Критичная Проблема, Производитель Изделия (ЗАО «С-Терра СиЭсПи») обеспечивает:

а) информирование доступными способами Конечного Пользователя о существовании Критичной Проблемы и о способах ее устранения

б) бесплатное предоставление обновлений программного обеспечения Производителя Изделия, в которых устранены Критичные Проблемы.

Примечание 1. Гарантийное обязательство 1 базируется на следующем определении: Критичная Проблема заключается в том, что Изделие, вследствие ошибки в программном обеспечении, не выполняет основные функции безопасности, а именно шифрование трафика и контроль доступа, что приводит к нарушению безопасности сети Конечного Пользователя.

Примечание 2. Обновления программного обеспечения в соответствии с гарантийным обязательством п.1б предоставляются по запросу Конечного Пользователя и по мере разработки обновлений.

2. Если Конечный Пользователь обнаружит в течение 90 (девяноста) дней со дня поставки Изделия дефекты в составе информационных носителей или некомплектность Изделия, то информационные носители будут заменены, а комплектность Изделия восстановлена. По истечении 90 дней претензии Конечного Пользователя по некомплектности изделия и/или дефектам носителей информации рассматриваться не будут.

Настоящее Лицензионное Соглашение не содержит никаких гарантий по поставке, функциональности и соответствию Изделия любым техническим требованиям, стандартам и условиям. Эти вопросы относятся к области лицензирования деятельности поставщика, сертификации Изделия и его компонент в установленном порядке, договоров о поставке, техническом сопровождении и технической поддержке и регламентируются в рамках отдельных документов.

Настоящее Лицензионное Соглашение (в рамках законодательства Российской Федерации и если противное не оговорено в виде отдельного дополнительного соглашения с Конечным Пользователем) не регламентирует вопросы технических, организационных и прочих возможных проблем, связанных с эксплуатацией Изделия и возможных материальных, финансовых и прочих потерь Конечного Пользователя в результате эксплуатации Изделия.

Срок действия настоящего Лицензионного Соглашения распространяется на весь период эксплуатации Изделия Конечным Пользователем. Действие настоящего Лицензионного Соглашения может быть прекращено по решению Конечного Пользователя. В этом случае Конечный Пользователь должен уничтожить все информационные носители, содержащие код и прочие информационные компоненты Изделия, включая информацию на внутренних носителях Изделия. Прекращение действия Лицензионного Соглашения по инициативе Конечного Пользователя является односторонней добровольной акцией Конечного Пользователя и не является предметом для взаиморасчетов и других хозяйственных операций.

Программный Продукт Системная Библиотека GNU libc является свободно распространяемым Продуктом и используется в составе Изделия без каких либо модификаций в соответствии с лицензией "The GNU General Public License" (http://www.gnu.org/licenses/licenses.html).

MS-DOS, Windows, Windows 98/NT/2000/XP/Vista/7 являются торговыми марками компании Microsoft Corporation в США и в других странах.

Sun Solaris и Java являются торговыми марками компании Sun Microsystems, Inc в США и в других странах.

Cisco, Cisco PIX Firewall, Cisco IOS Router, CiscoWorks, CiscoWorks VPN/Security Management Solution, CiscoWorks Management Center for VPN Routers, CiscoWorks Management Center for PIX Firewall являются торговыми марками компании Cisco Systems в США и в других странах.

Изделие включает в себя программное обеспечение, написанное Эриком Янгом (Eric Young. eay@cryptsoft.com)

Другие названия компаний и Продуктов, упомянутые в настоящем Лицензионном Соглашении и в составе информационных источников Изделия могут являться зарегистрированными торговыми марками соответствующих им компаний. Упоминание наименований, Продуктов, торговых марок третьих организаций исключительно неформально и не является ни поддержкой, рекомендацией либо рекламой. ЗАО «С-Терра СиЭсПи» не несет какой-либо ответственности в отношении работоспособности и использования этих Продуктов.

Напечатано в Российской Федерации

Закрытое Акционерное Общество «С-Терра СиЭсПи»

124460, г. Москва, Зеленоград, проезд 4806, д.6, этаж 4-й

Телефон: +7 (499) 940 9061

Факс: +7 (499) 940 9061

Эл.почта: *information@s-terra.com*

http://www.s-terra.com

1. Назначение и функции Продукта

Программный комплекс «Клиент безопасности CSP VPN Client. Версия 3.1», функционирующий на аппаратных платформах в архитектуре Intel x86 под управлением операционных систем Microsoft Windows XP (в том числе Embedded), Microsoft Windows Vista и Microsoft Windows 7 устанавливается на компьютер и функционирует в интересах одного пользователя.

Программный комплекс (далее Продукт CSP VPN Client, Продукт, CSP VPN Client) предназначен для создания защищенных соединений между клиентом VPN и другими взаимодействующими с ним доверенными шлюзами VPN и клиентами VPN, а также может выполнять роль межсетевого экрана.

Продукт CSP VPN Client выполняет следующие функции:

- защиту трафика на уровне аутентификации/шифрования сетевых пакетов по протоколам IPsec AH и/или IPsec ESP
- пакетную фильтрацию трафика с использованием информации в полях заголовков сетевого, транспортного и прикладного уровней
- аутентификацию пользователя и аутентификацию узла сети
- событийное протоколирование
- реализацию заданной дисциплины взаимодействия (аутентификацию и/или защиту трафика) для каждого защищенного соединения, доступ в заданном защищенном режиме только для зарегистрированных, в том числе и для мобильных партнеров по взаимодействию
- регулируемую стойкость защиты трафика.

CSP VPN Client осуществляет защиту трафика протоколов семейства TCP/IP в рамках международных стандартов IKE/IPsec:

- Security Architecture for the Internet Protocol – RFC2401
- IP Authentication Header (AH) – RFC2402
- IP Encapsulating Security Payload (ESP) – RFC2406
- Internet Security Association and Key Management Protocol (ISAKMP) – RFC2408
- The Internet Key Exchange (IKE) – RFC2409
- The Internet IP Security Domain of Interpretation for ISAKMP (DOI) – RFC2407.

Продукт CSP VPN Client использует в качестве внешней криптографической библиотеки средство криптографической защиты информации (СКЗИ) "КриптоПро CSP 3.6", разработанное компанией "Крипто-Про".

СКЗИ "КриптоПро CSP" реализует российские криптографические алгоритмы:

- ГОСТ 28147-89 – шифрование/расшифрование данных
- ГОСТ Р 34.11-94 – алгоритм хэширования
- ГОСТ Р 34.10-2001 – формирование и проверка электронно-цифровой подписи (ЭЦП)
- VKO ГОСТ Р 34.10-2001 – поддержка схемы открытого распределения ключей Диффи-Хеллмана в соответствии с RFC 4357

- генерацию случайных чисел.

CSP VPN Client является продуктом для корпоративного использования в том смысле, что политику безопасности и настройки режимов этого Продукта осуществляет системный администратор или администратор безопасности предприятия.

Продукт CSP VPN Client для всех интерфейсов задает одинаковую политику безопасности.

2. Требования на базовые платформы и совместимость

Продукт CSP VPN Client выпущен для следующих базовых платформ:

- MS Windows 7 (32-bit) Russian Edition
- MS Windows Vista (32-bit) Business SP2 Russian Edition
- MS Windows XP Professional SP3 Russian Edition (в том числе Embedded).

Продукт совместим с криптографической библиотекой "КриптоПро CSP 3.6", разработанной компанией "Крипто-Про".

В части реализации протоколов IPsec/IKE и их расширений Продукт совместим с Cisco IOS v.12.4.

В части удаленного мониторинга и сбора статистики управления Продукт совместим с CiscoWorks Monitoring Center for Performance 2.0.2, входящим в состав CiscoWorks VMS 2.3.

Продукт совместим с eToken PRO32k, eToken PRO64k, eToken NG-FLASH, eToken NG-OTP, eToken PRO (Java) производства компании Aladdin.

3. Атрибуты аутентификации

Технология IPsec обеспечивает аутентификацию, шифрование и целостность данных на уровне передаваемых IP пакетов.

Для реализации этих функций технологии IPsec необходима дополнительная информация, которая поставляется протоколом IKE: ключевой материал и согласованная политика защиты.

Для аутентификации взаимодействующих сторон протоколу IKE необходима некоторая аутентификационная информация.

Такой аутентификационной информацией может быть:

- предустановленный (разделяемый) ключ (Preshared Key)
- сертификат стандарта X.509.

Имеются некоторые ограничения при работе с расширениями сертификата (Extensions), которые помечены как критичные. В таблице приведен список расширений сертификата, которые будут распознаваться и обрабатываться Продуктом, если у них установлен признак критичности TRUE. Если в сертификате будут присутствовать другие расширения, не указанные в таблице и заданные как критичные, то такой сертификат не может быть использован. Если же расширение отсутствует в таблице, но является некритичным, то оно игнорируется, и сертификат используется.

Name	OID value
Subject Key Identifier	2.5.29.14
Key Usage	2.5.29.15
Subject Alternative Name	2.5.29.17
Issuer Alternative Name	2.5.29.18
Basic Constraints	2.5.29.19
Name Constraints	2.5.29.30
CRL Distribution Points	2.5.29.31
Authority Key Identifier	2.5.29.35

Описания значений и полный список Certificate Extensions можно посмотреть в документе RFC 5280 (http://tools.ietf.org/html/rfc5280#section-4.2).

4. Процесс подготовки персонального инсталляционного пакета пользователя

В этой главе описано как администратор безопасности готовит для пользователя инсталляционный пакет и поэтому эта информация для пользователя носит ознакомительный характер.

Продукт CSP VPN Client рассчитан для применения внутри корпоративных сетей. Полагаем, что в таких сетях пользователь не имеет право на изменение политики безопасности корпоративной сети. Поэтому, Продукт CSP VPN Client разработан таким образом, что администратор безопасности корпоративной сети формирует персонализованный инсталляционный пакет для каждого пользователя. При этом он производит настройки для пользователя, которые согласуются с его должностными обязанностями.

Для подготоки инсталляционного пакета пользователя администратору необходимо иметь предустановленные ключи либо сертификаты открытых ключей пользователя и локальную политику безопасности, предписанную для данного пользователя.

При использовании предустановленных (разделяемых) ключей (Preshared Keys) подготовка персонального инсталляционного пакета пользователя осуществляется полностью администратором.

При использовании сертификатов открытых ключей подготовка инсталляционного пакета пользователя осуществляется по одному из двух сценариев.

Секретный ключ пользователя, соответствующий открытому ключу сертификата, находится в контейнере. Контейнер имеет сложную структуру, где кроме секретного ключа содержится служебная информация, необходимая для обеспечения защиты и целостности ключа. Этот контейнер не является каталогом файловой системы. Контейнер может находиться на локальном ключевом носителе (Registry) или на каком-либо внешнем ключевом носителе, например, дискете, электронном ключе eToken и др.

Сценарии отличаются тем, кто создает ключевую пару для локального сертификата пользователя и на каком ключевом носителе размещен контейнер с секретным ключом пользователя, возможна или нет проверка соответствия сертификата пользователя и секретного ключа, копируется или нет контейнер с секретным ключом во время инсталляции на компьютере пользователя.

4.1. Первый сценарий

Все действия по созданию ключевой пары, формированию запроса и созданию сертификата пользователя производятся администратором CA. При этом контейнер с секретным ключом записывают на внешний ключевой носитель, например, дискету или eToken. Инсталляция считывателя описана в разделе "Инсталляция внешнего считывателя и ключевого носителя в “КриптоПро CSP 3.6".

В этом сценарии возможна проверка соответствия сертификата пользователя и секретного ключа во время создания инсталляционного файла, а также копирование контейнера с одного носителя на другой, например, в Реестр во время установки инсталляционного файла на компьютере пользователя.

Действия администратора по этому сценарию следующие:

- администратор безопасности получает от администратора CA локальный сертификат пользователя и корневой сертификат Удостоверяющего Центра (Trusted CA Certificate), экспортированные в файлы. Ему передается и контейнер с секретным ключом на внешнем носителе
- администратор безопасности задает для пользователя локальную политику безопасности, локальные настройки, определяет проводить или нет проверку на соответствие сертификата и секретного ключа, копировать или нет контейнер, и создает инсталляционный файл для пользователя
- подготовленный инсталляционный файл содержит исполняемый код Продукта CSP VPN Client, персональные настройки, локальную политику безопасности, локальный сертификат со ссылкой местоположения контейнера с секретным ключом пользователя и CA сертификат. Администратор безопасности передает пользователю подготовленный инсталляционный пакет, состоящий из инсталляционного файла, и контейнера с секретным ключом пользователя на внешнем ключевом носителе, например, eToken. Контейнер должен быть передан пользователю по заслуживающему доверия каналу связи.

Пользователь, получив инсталляционный пакет, производит установку Продукта CSP VPN Client на своем компьютере.

4.2. Второй сценарий

Создание ключевой пары и формирование запроса на локальный сертификат пользователя производятся администратором безопасности или пользователем на компьютере пользователя. При этом контейнер с секретным ключом размещаются на жестком диске компьютера пользователя. В этом сценарии невозможна проверка соответствия сертификата пользователя и секретного ключа, копирование контейнера из Реестра в этом случае не производится.

Действия администратора по этому сценарию следующие:

- администратор безопасности или пользователь на компьютере пользователя создает ключевую пару и формирует запрос на локальный сертификата пользователя. Созданный запрос посылается на сервер Удостоверяющего Центра сертификатов. При этом контейнер с секретным ключом пользователя размещается на локальном ключевом носителе (Реестре) на компьютере пользователя. Подробно этот пункт описан в разделе "Генерация ключевой пары и формирование запроса на создание сертификата пользователя"
- администратор CA на сервере Удостоверяющего Центра по полученному запросу создает локальный сертификат пользователя и экспортирует его в файл. Корневой сертификат Удостоверяющего Центра (Trusted CA Certificate) также экспортируется в файл. Администратор безопасности получает оба эти сертификата от администратора CA
- администратор безопасности на своем рабочем месте задает для пользователя локальную политику безопасности, локальные настройки и создает инсталляционный файл для пользователя
- подготовленный инсталляционный файл содержит исполняемый код Продукта CSP VPN Client, персональные настройки, локальную политику безопасности, локальный сертификат со ссылкой местоположения контейнера с секретным ключом пользователя и CA сертификат. Администратор безопасности передает пользователю подготовленный инсталляционный пакет, состоящий из одного инсталляционного файла.

Пользователь, получив инсталляционный пакет, производит установку Продукта CSP VPN Client на своем компьютере.

5. Создание ключевой пары и формирование запроса на создание сертификата пользователя

Для создания ключевой пары и формирования запроса на создание сертификата пользователя можно использовать средства Microsoft Windows. Опишем этот процесс на компьютере пользователя.

Шаг 1: установите программный Продукт СКЗИ "КриптоПро CSP 3.6". Установка этого Продукта описана в разделе "Установка СКЗИ "КриптоПро CSP 3.6".

Шаг 2: инсталлируйте ключевой носитель, на котором будет размещен контейнер с секретным ключом пользователя, например, Реестр, используя СКЗИ "КриптоПро CSP 3.6". Эта инсталляция описана в разделе "Инсталляция ключевого считывателя Реестр в "КриптоПро CSP 3.6".

Шаг 3: запустите Microsoft Internet Explorer. В поле Address укажите адрес сервера Удостоверяющего Центра и запустите утилиту `certsrv` (Certificate Service), например, `http://10.0.232.7/certsrv/`.

Полагаем, что на сервере уже установлен Продукт СКЗИ "КриптоПро CSP 3.6".

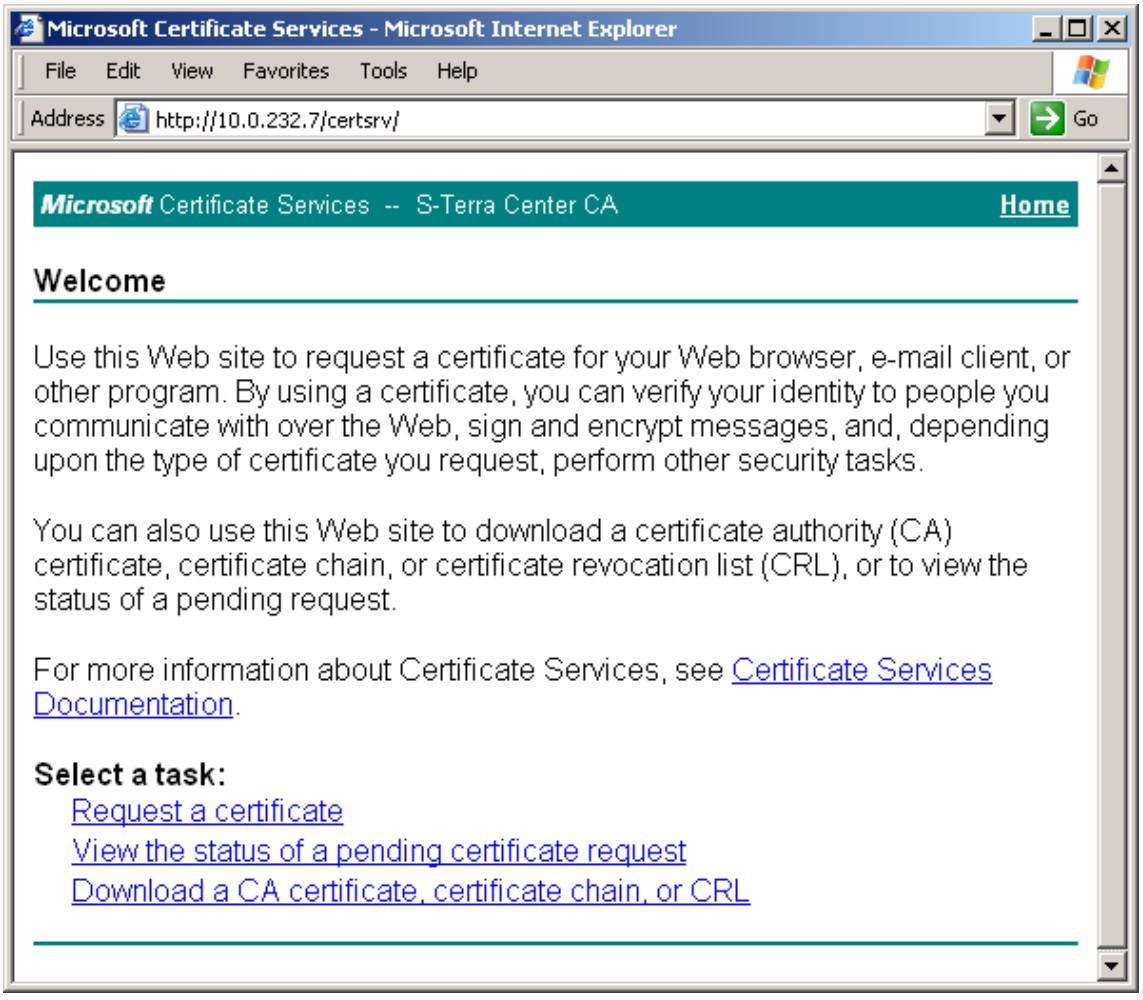

Рисунок 1

Шаг 4: в появившемся окне высвечивается имя Удостоверяющего Центра – в нашем случае S-Terra Center CA. Для формирования запроса на создание сертификата пользователя выберите предложение ”Request a certificate” (Рисунок 1).

Шаг 5: выберите расширенный запрос на сертификат – предложение “advanced certificate request” (Рисунок 2):

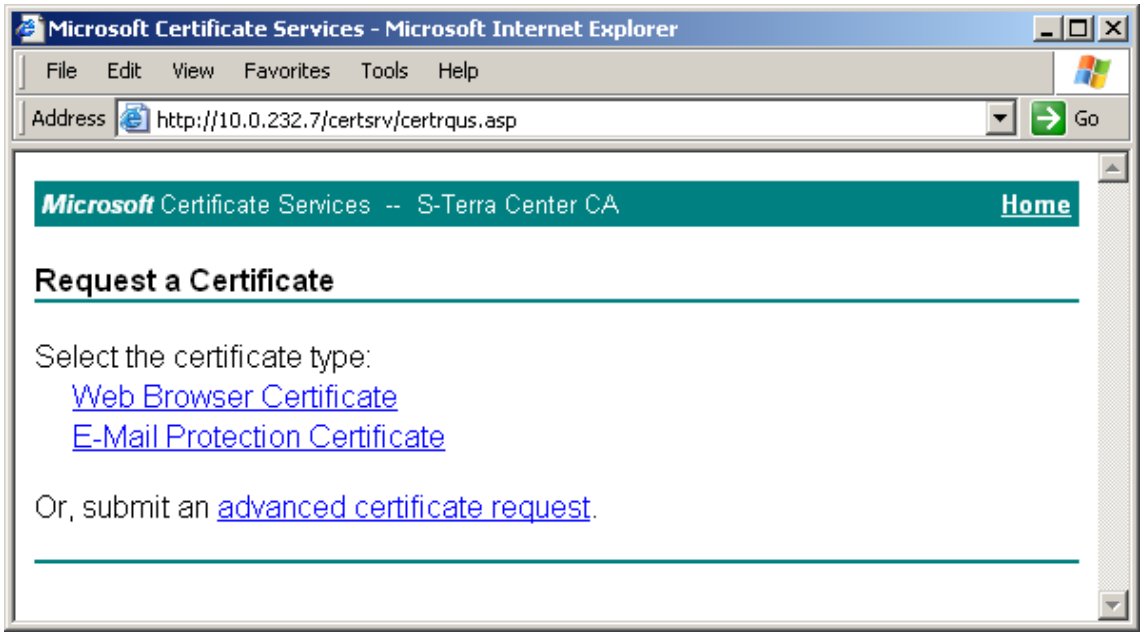

Рисунок 2

Шаг 6: для получения формы для формирования запроса на сертификат выберите предложение “Create and submit a request to this CA” (Рисунок 3):

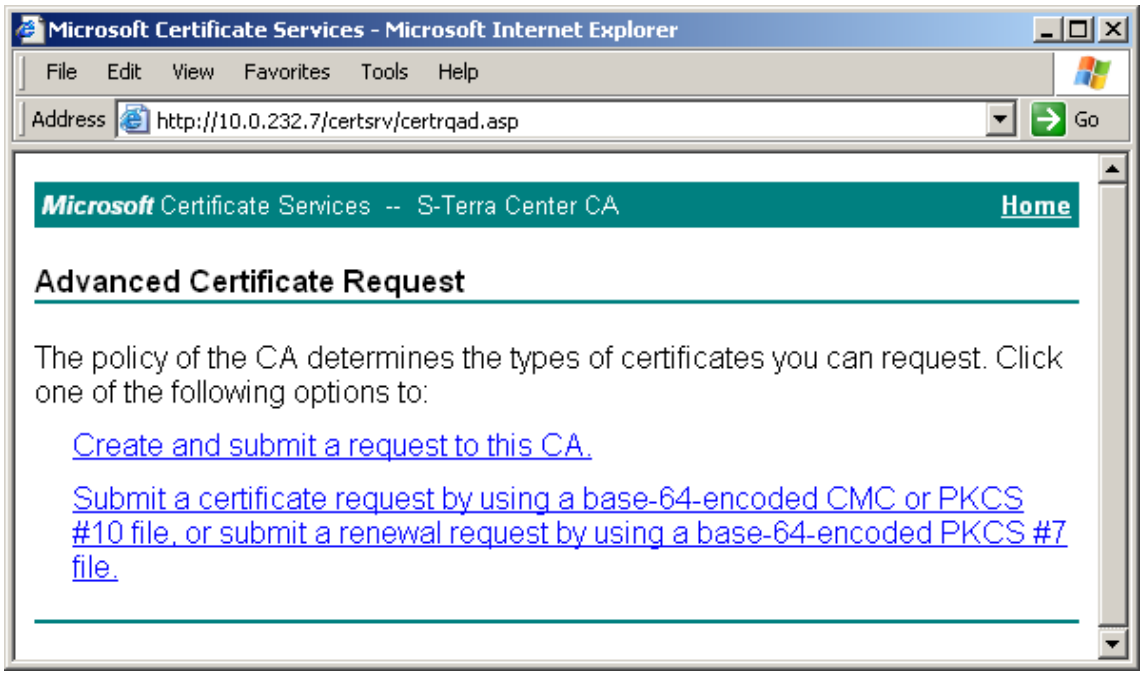

Рисунок 3

Шаг 7: заполните форму расширенного запроса, показанную ниже (Рисунок 4). 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. Примечание: если при создании запроса на сертификат при заполнении полей сертификата используются русские буквы, необходимо, чтобы они были введены в формате UTF-8
- 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 KC1 CSP
  - 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
    - Export keys to file – этот флажок выставляется, если нужно экспортировать ключи в файл. Мы этот флажок не выставляем, так как секретный ключ размещаем в контейнере
  - Enable strong private key protection – этот флажок не выставляем
  - Store certificate in the local computer certificate store (Использовать локальное хранилище)- всегда выставляйте этот флажок
- 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):

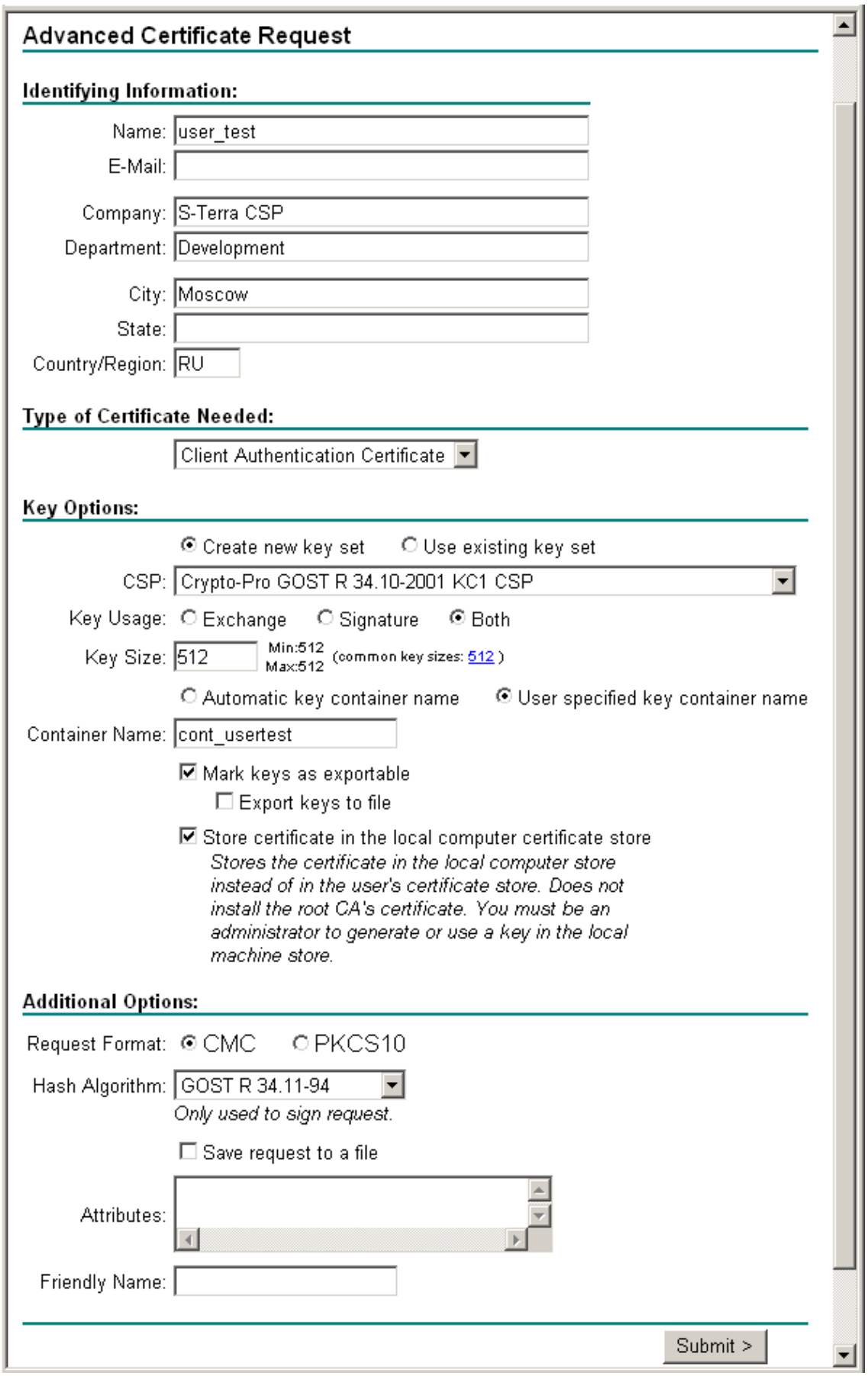

Рисунок 4

Шаг 8: появляется предупреждение (Рисунок 5), нажмите кнопку Yes, чтобы продолжить:

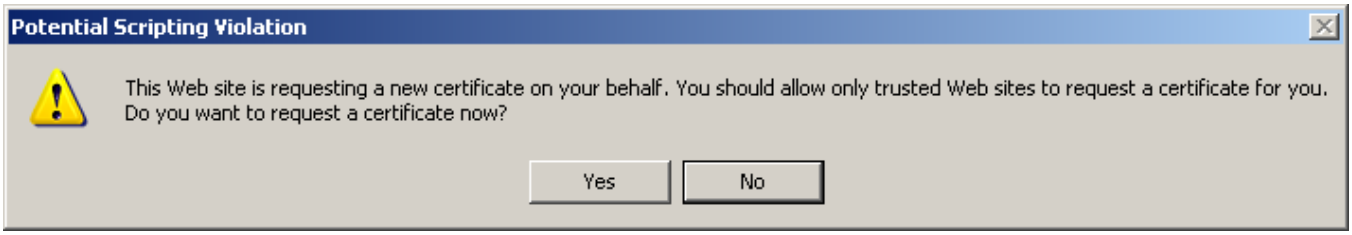

Рисунок 5

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

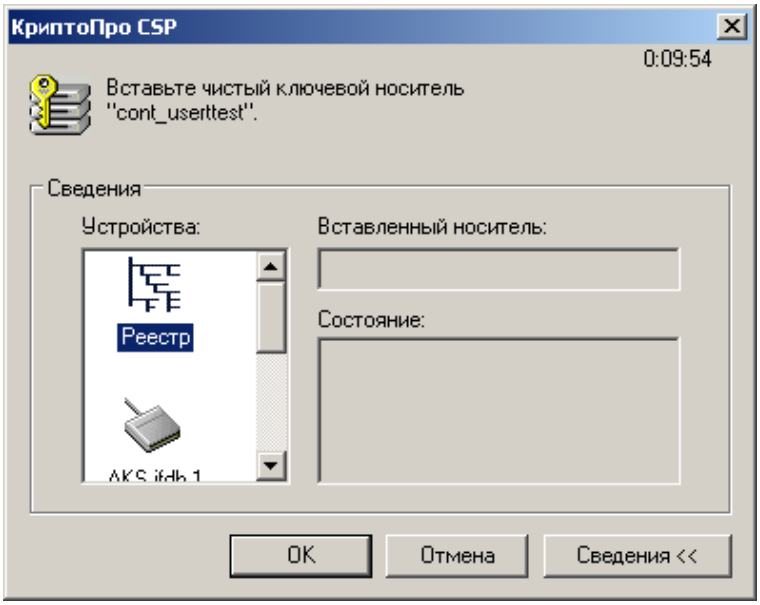

Рисунок 6

Шаг 10: для генерации ключевой пары датчик случайных чисел просит нажать любую клавишу или подвигать мышкой:

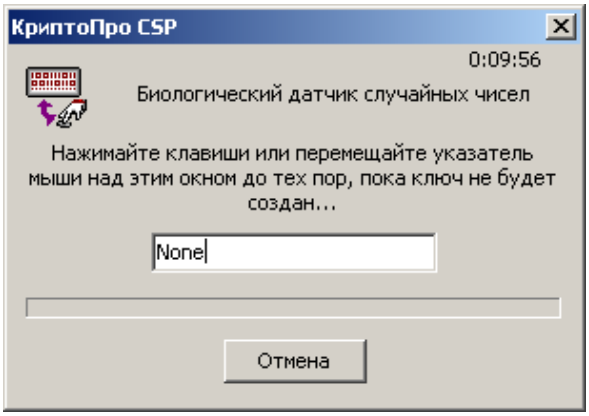

Рисунок 7

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

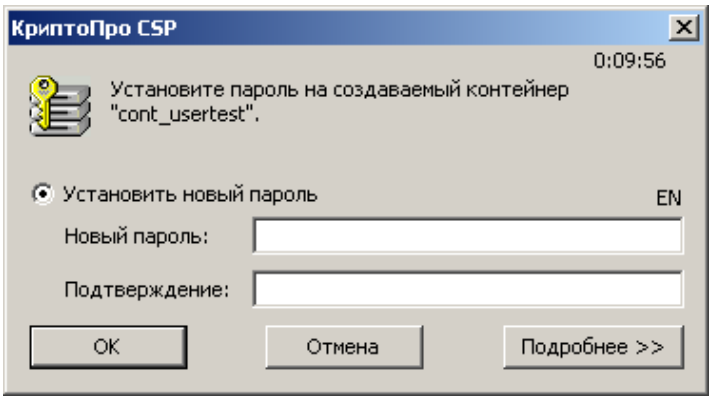

Рисунок 8

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.

Удостоверяющий Центр сразу создал сертификат пользователя и прислал об этом уведомление. При выборе предложения `Install this certificate` сертификат пользователя будет получен из Удостоверяющего Центра и размещен в контейнере с секретным ключом, в нашем примере - в Registry.

Шаг 12: Удостоверяющий Центр сразу издал сертификат пользователя и прислал об этом уведомление (Рисунок 9). Выберите предложение “Install this certificate”, чтобы получить сертификат пользователя из Удостоверяющего Центра и разместить его в контейнере с секретным ключом.

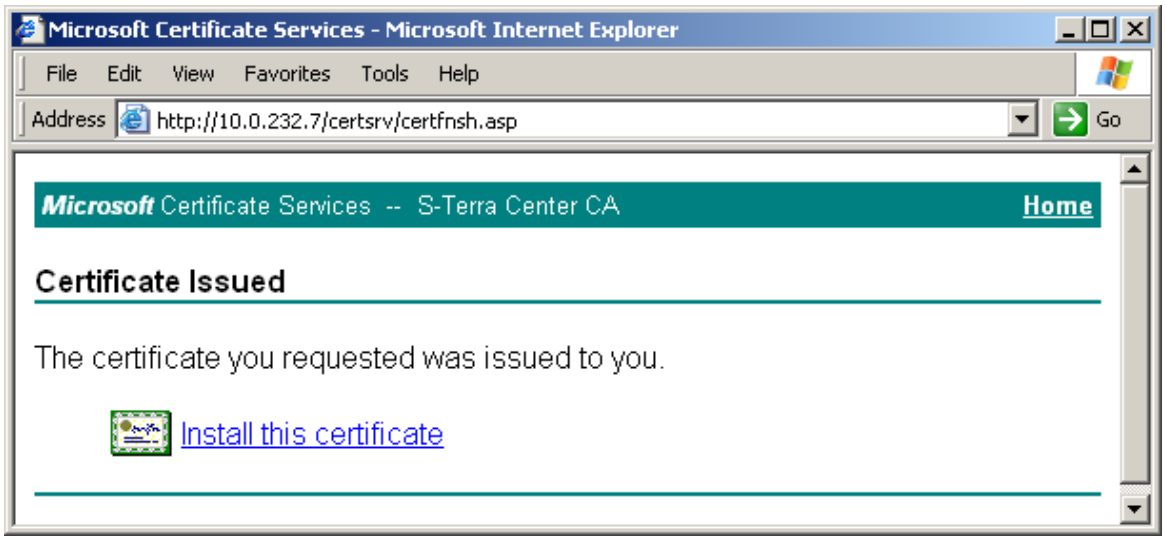

Рисунок 9

Шаг 13: появляется предупреждение (Рисунок 10), нажмите кнопку Yes, чтобы продолжить:

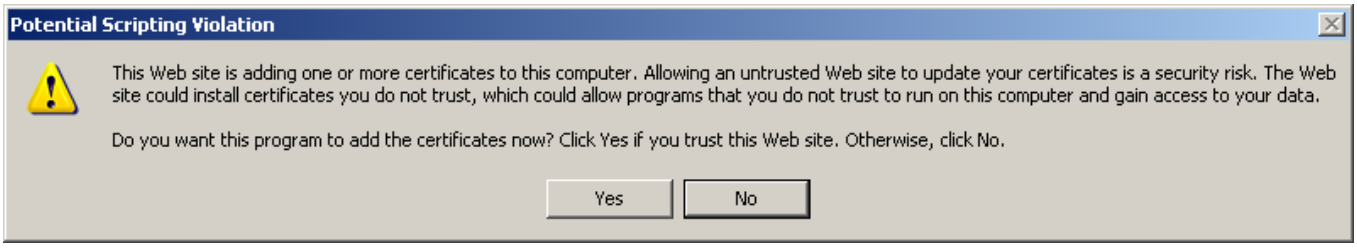

Рисунок 10

Шаг 14: еще раз введите пароль на контейнер с секретным ключом и нажмите ОК (Рисунок 11):

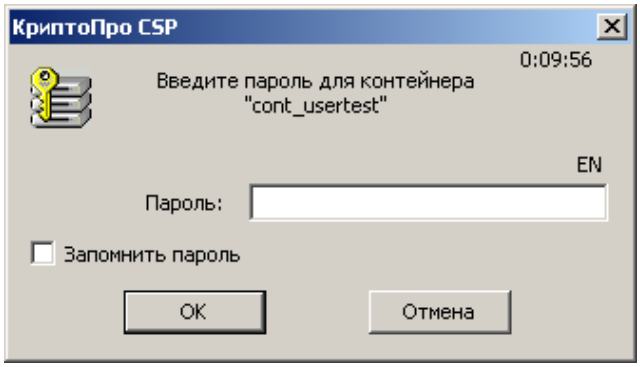

Рисунок 11

Выдается сообщение, что сертификат пользователя успешно размещен в контейнере с секретным ключом (Рисунок 12).

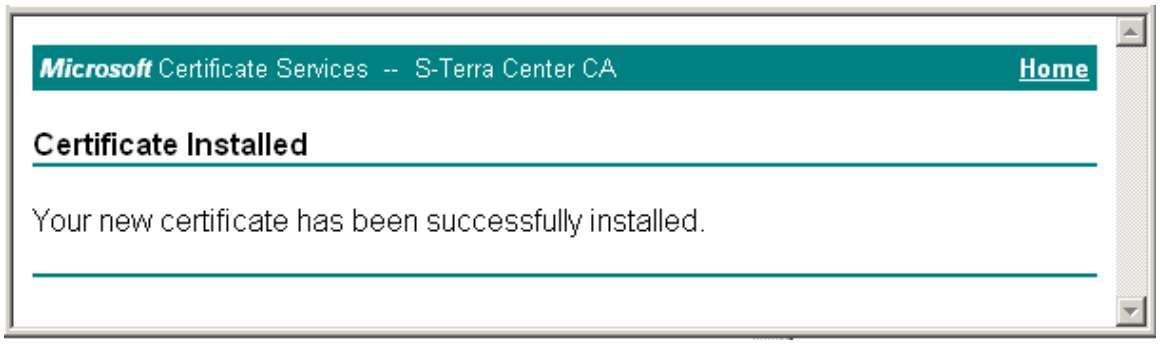

Рисунок 12

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

Для создания инсталляционного файла пользователя требуется экспортировать сертификат пользователя из контейнера в файл, поэтому перейдите к следующему разделу.

5.1. 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 3.6" – Пуск – Настройка – Панель управления – КриптоПро CSP

Шаг 2: войдите во вкладку Сервис и нажмите кнопку Просмотреть сертификаты в контейнере…

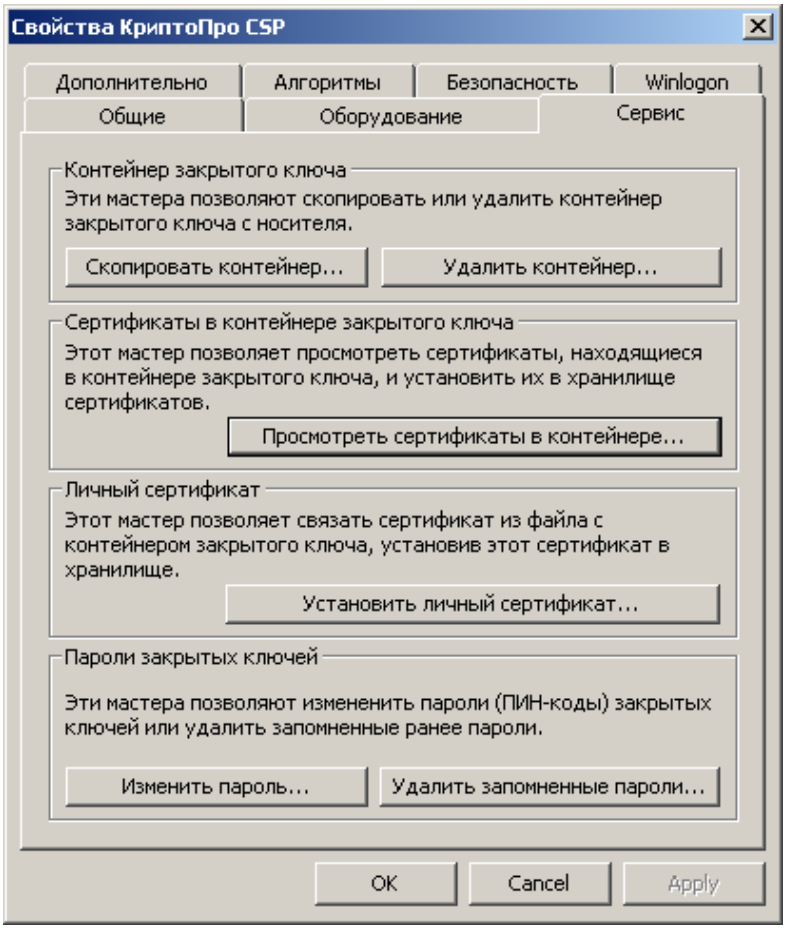

Рисунок 13

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

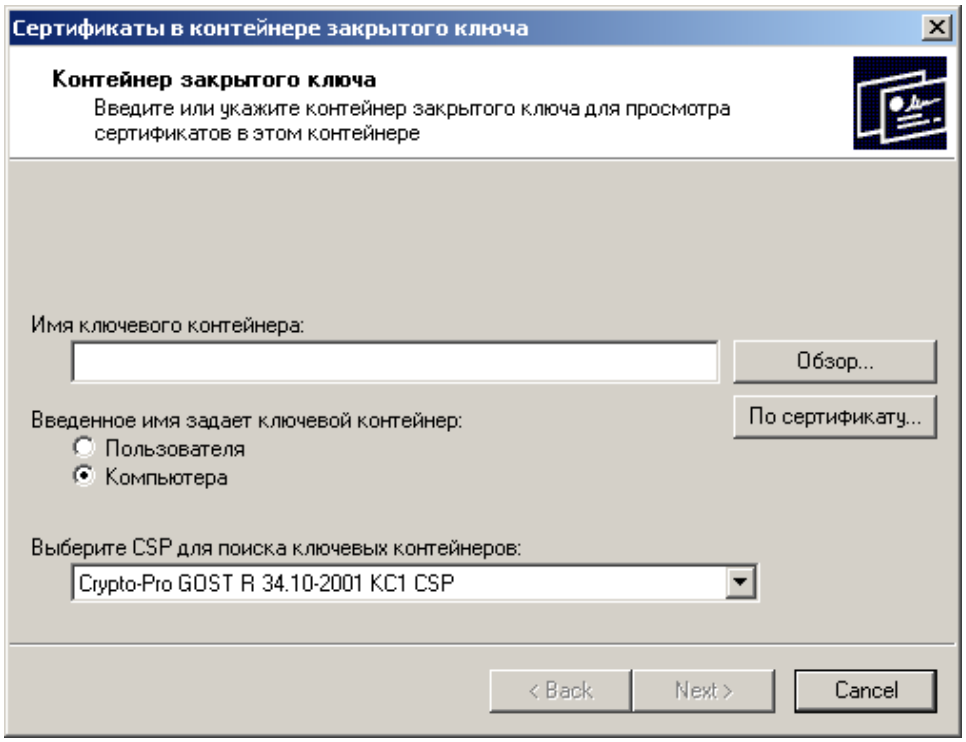

Рисунок 14

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 (Рисунок 15). Нажмите кнопку ОК:

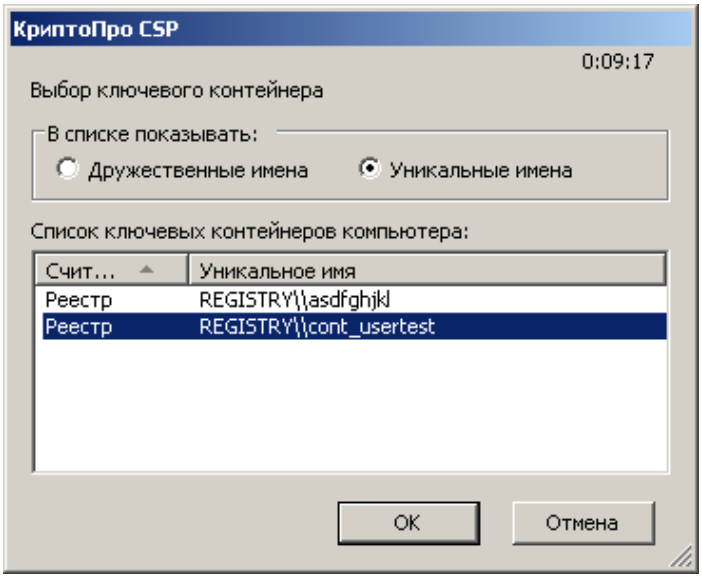

Рисунок 15

Шаг 5: выбор контейнера произведен, нажмите кнопку Next:

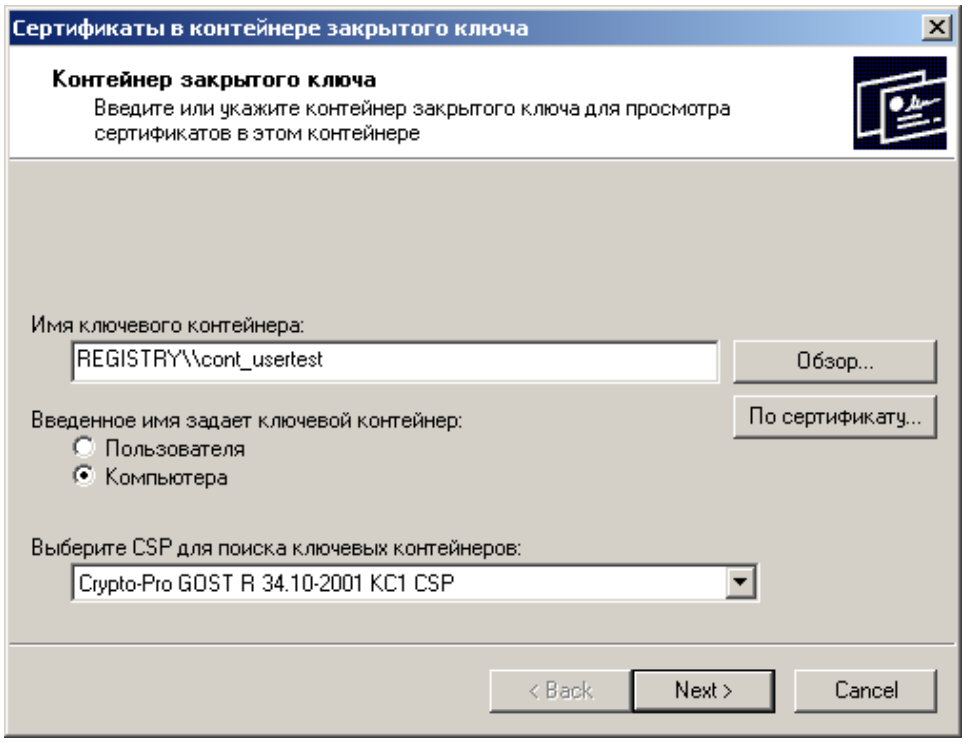

Рисунок 16

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

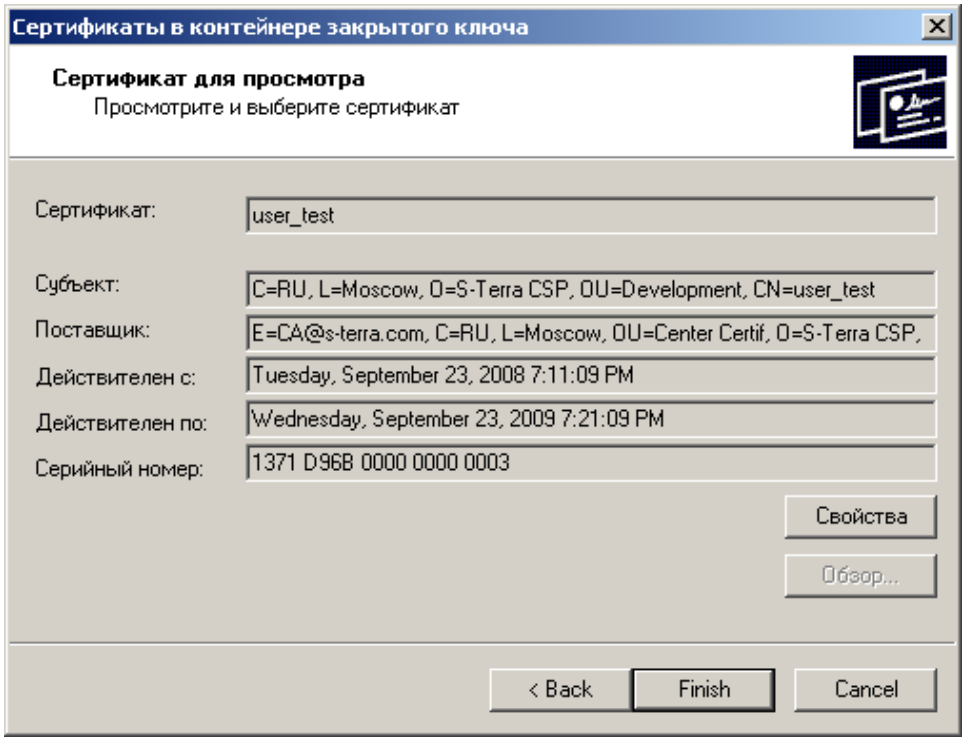

Рисунок 17

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

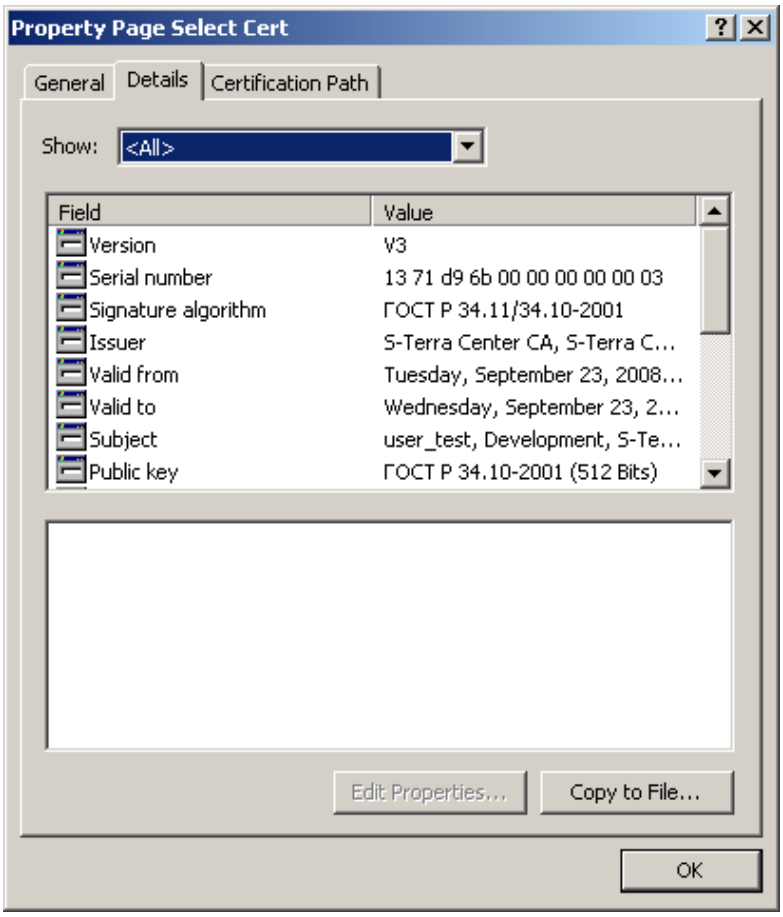

Рисунок 18

Шаг 8: в окне визарда нажмите кнопку Next:

Рисунок 19

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

Рисунок 20

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

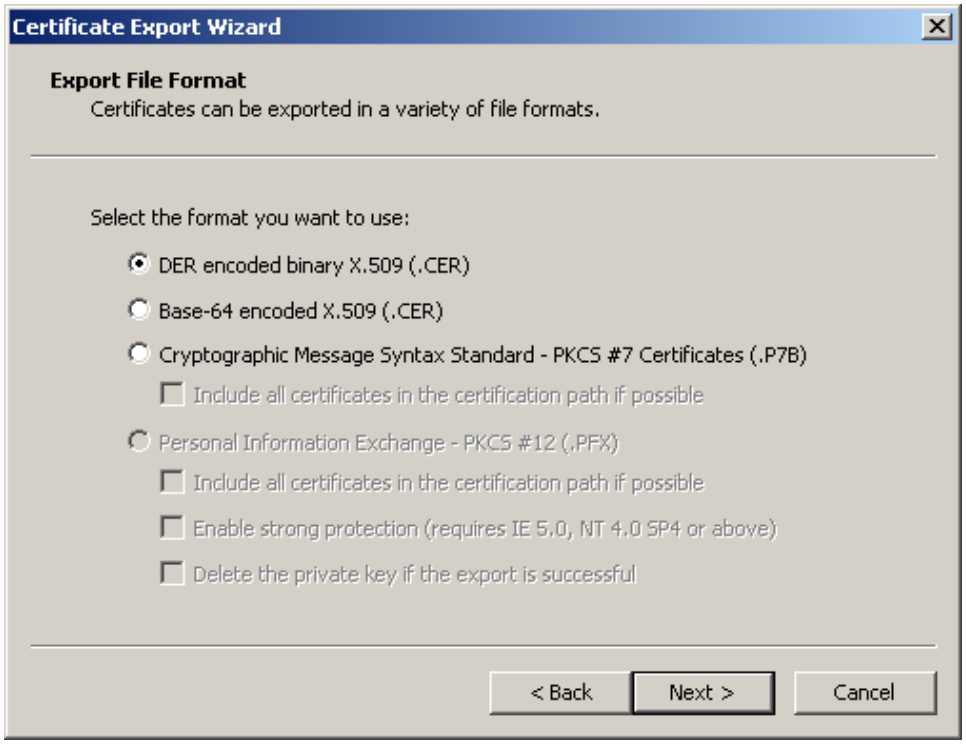

Рисунок 21

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

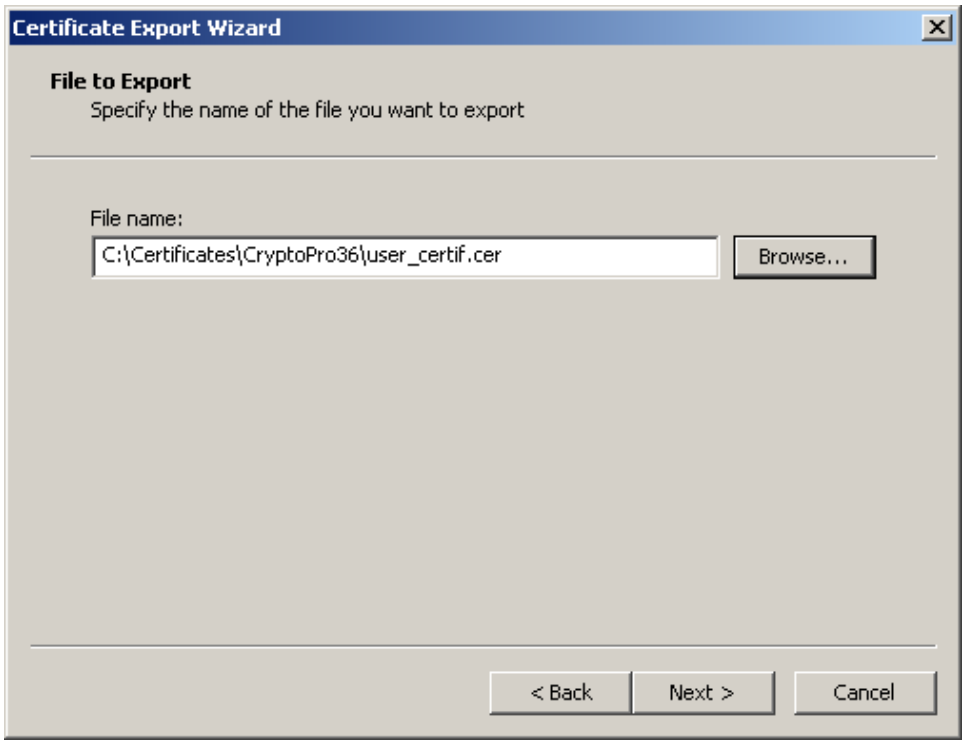

Рисунок 22

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

Рисунок 23

Экспортированный в файл сертификат пользователя будет использоваться администратором для создания инсталляционного файла.

6. Подготовка к инсталляции CSP VPN Client

Продукт CSP VPN Client работает под управлением операционных систем:

- MS Windows 7 (32-bit) Russian Edition
- MS Windows Vista (32-bit) Business SP2 Russian Edition
- MS Windows XP Professional SP3 Russian Edition (в том числе Embedded).

Перед установкой Продукта CSP VPN Client на компьютере пользователя выполните следующие действия:

1. установите программный Продукт СКЗИ "КриптоПро CSP 3.6", если он еще не установлен. Установка описана в разделе "Установка СКЗИ "КриптоПро CSP 3.6"
2. инсталлируйте ключевой считыватель Реестр для временного контейнера, создаваемого в процессе инсталляции CSP VPN Client, в который будет записано начальное значение ДСЧ. Такая инсталляция описана в разделе "Инсталляция ключевого считывателя Реестр в "КриптоПро CSP 3.6".
   Если аутентификация партнеров осуществляется с использованием сертификатов, то временный контейнер для ДСЧ может быть размещен на том же носителе, что и контейнер с секретным ключом, в этом случае перейдите к выполнению следующего действия
3. если аутентификация сторон осуществляется с использованием сертификатов и контейнер с секретным ключом сертификата находится не на дискете, а на другом внешнем ключевом носителе, то сначала подключите считыватель этого носителя, как описано в разделе "Подключение внешних ключевых считывателей". Затем инсталлируйте считыватель и ключевой носитель. Такая инсталляция изложена в разделе "Инсталляция внешнего считывателя и ключевого носителя в "КриптоПро CSP 3.6". Если же контейнер с секретным ключом находится в Реестре, то этот носитель ключевой информации уже инсталлирован
4. В ОС Windows XP Embedded имеются некоторые особенности в подготовке ОС, которые следует учесть перед инсталляцией CSP VPN Client, описанные в разделе «Подготовка ОС Windows XP Embedded к инсталляции CSP VPN Client».
5. В ОС Windows 7 x32 перед инсталляцией CSP VPN Client переведите службу «Модули ключей IPsec для обмена ключами в Интернете и протокола IP с проверкой подлинности» (внутреннее название – IKEEXT) в состояние «Отключен» (Панель управления-Система и безопасность-Администрирование-Службы).

6.1. Подготовка ОС Windows XP Embedded к инсталляции

Предполагается, что используется некоторый типичный вариант установки Windows XP Embedded для формирования работоспособной клиентской среды, в которой запускаются и работают большинство программ для Windows XP. В этом варианте обязательно должны присутствовать сетевые компоненты, Windows Installer, GUI и т.п.

Далее в таблице перечислены необходимые компоненты ОС, которые могут отсутствовать в типичном варианте установки Windows XP Embedded. Желательно, чтобы данные компоненты были добавлены при сборке образа ОС.

Таблица 1

Необходимый компонент	DLL для обходного решения
Performance Data Helper	pdh.dll, odbcbcp.dll
Quality of Service Traffic Control	traffic.dll

Если данные компоненты не были добавлены, то после инсталляции CSP VPN Client используйте DLL для обходного решения. Данные DLL возьмите из той же версии ОС XP Embedded либо из стандартной ОС Windows XP Professional (каталог `C:\WINDOWS\System32`) и скопируйте указанные DLL в каталог Продукта.

> Выполните копирование вручную после того, как инсталлятор создаст каталог Продукта. Это желательно сделать до запуска сервиса vpnsvc. Если файлы не будут скопированы до попытки старта сервиса, будет выдано сообщение об ошибке 1920 (`"Service 'CSP VPN Service' (vpnsvc) failed to start. Verify that you have sufficient privileges to start system services."`). Скопируйте требуемые DLL и нажмите кнопку Retry.
>
> **Внимание!** Перед копированием убедитесь, что указанные файлы действительно отсутствуют в каталоге `C:WINDOWS\System32`.

В некоторых системах во время инсталляции могут появляться сообщения о нехватке свободного места на диске, несмотря на то, что на системном диске свободного места достаточно. Эта ситуация может быть вызвана тем, что каталог %TEMP% (%TMP%) указывает на маленький RAM-диск.

Для обхода этой проблемы:

- создайте временный каталог на системном диске (например, `C:\TEMP`)
- переопределите переменные окружения TEMP и TMP, указав в них полный путь к данному каталогу:
  - нажмите правой кнопкой на "`My Computer`", далее `Properties -> Advanced -> Environment Variables`; в разделе "`User variables for Administrator`" поменяйте значения TEMP и TMP.

После завершения инсталляции верните данные переменные в исходное значение, а также удалите временный каталог.

Для массовых установок можно написать скрипт или или BAT-файл, выполняющий вышеперечисленные действия.

7. Инсталляция CSP VPN Client

Установка Продукта осуществляется запуском инсталляционного файла, подготовленного и переданного администратором безопасности пользователю.

Инсталляция должна производиться пользователем, имеющим права администратора.

Если контейнер с секретным ключом пользователя находится на дискете, то дискета должна быть вставлена в дисковод.

После запуска файла для установки CSP VPN Client инсталляция происходит в одном из 3 режимов, который был выбран администратором при подготовке инсталляционного файла:

- **режим basic** – основной режим, неинтерактивная установка с запросом на инсталляцию, вариант по умолчанию
- **режим normal** - интерактивная установка
- **режим silent** - неинтерактивная установка без запросов.

Если при подготовке инсталляционного файла администратор включил копирование контейнера с секретным ключом с внешнего ключевого носителя в другой контейнер, например, в Реестр, то копирование произойдет в процессе установки CSP VPN Client. Подробное описание копирования размещено в разделе "Копирование контейнера при инсталляции".

Все протоколируемые события при инсталляции CSP VPN Client будут записываться в файл, который задал администратор при создании инсталляционного пакета пользователя.

При возникновении ошибок во время инсталляции или работы Продукта устраните их и попытайтесь повторно провести инсталляцию Продукта. При появлении сбоев во время работы Продукта перезагрузите компьютер, но если перезагрузка не устраняет проблему – обратитесь в службу поддержки по адресу mailto:support@s-terra.com.

При инсталляции CSP VPN Client происходит отключение стандартного сервиса, связанного с IPsec и IKE и перевод его в состояние Manual. В Windows XP – это Служба IPSEC, внутреннее название которой PolicyAgent. В Windows Vista/Windows 7 – это Служба «Модули ключей IPsec для обмена ключами в Интернете и протокола IP с проверкой подлинности» (внутреннее название – IKEEXT).

В Windows Vista/Windows 7 производится настройка штатного FireWall сервиса (Брандмауэр Windows). При установке CSP VPN Client в Windows FireWall добавляется новое правило:

- правило для входящих подключений
- имя – CSP VPN Service – UDP allowed (predefined)
- правило включено
- действие – разрешить подключение
- протокол – UDP (все порты)
- программа – полный путь к установленному файлу vpnsvc.exe
- службы – применятьтолько к службам
- профили – все профили
- остальные параметры - по умолчанию.

Эти настройки можно посмотреть следующим образом: Панель управления – Администрирование – Брандмауэр Windows в режиме повышенной безопасности – Правила для входящих подключений.

7.1. Режим basic

В ОС **Windows Vista/Windows 7** при установке CSP VPN Client выдается окно (Рисунок 24). Необходимо разрешить запуск инсталлятора – выберите предложение Разрешить.

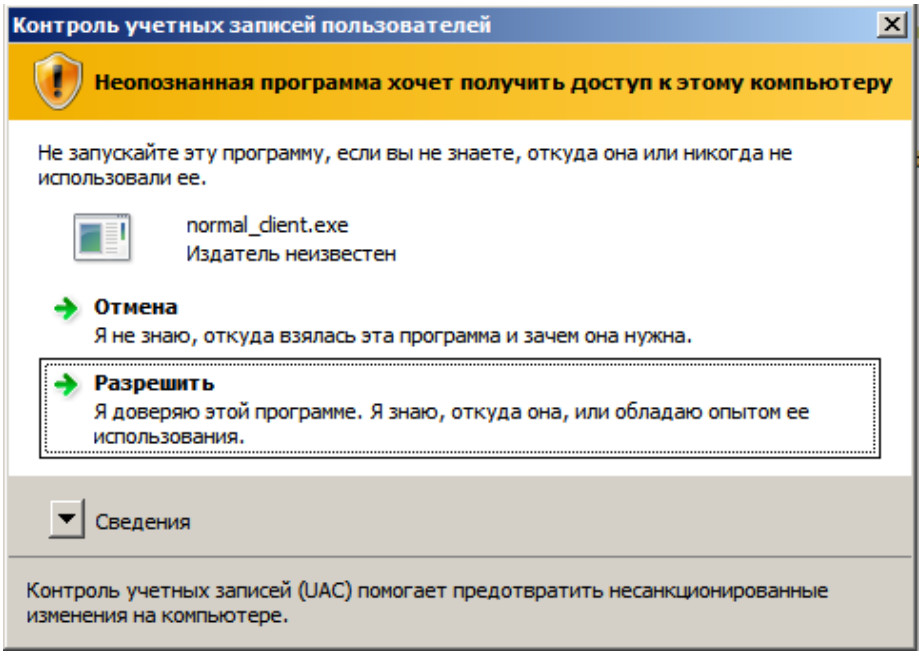

Рисунок 24

Затем выдается запрос на инсталляцию CSP VPN Client (в ОС Windows XP это окно появляется первым):

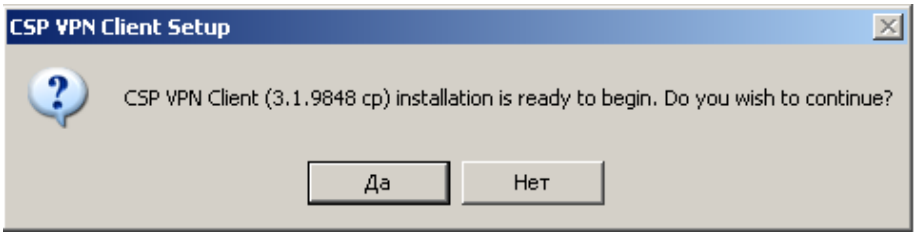

Рисунок 25

После нажатия кнопки Да происходит установка Продукта:

Рисунок 26

Появляется окно с индикатором процесса инсталляции:

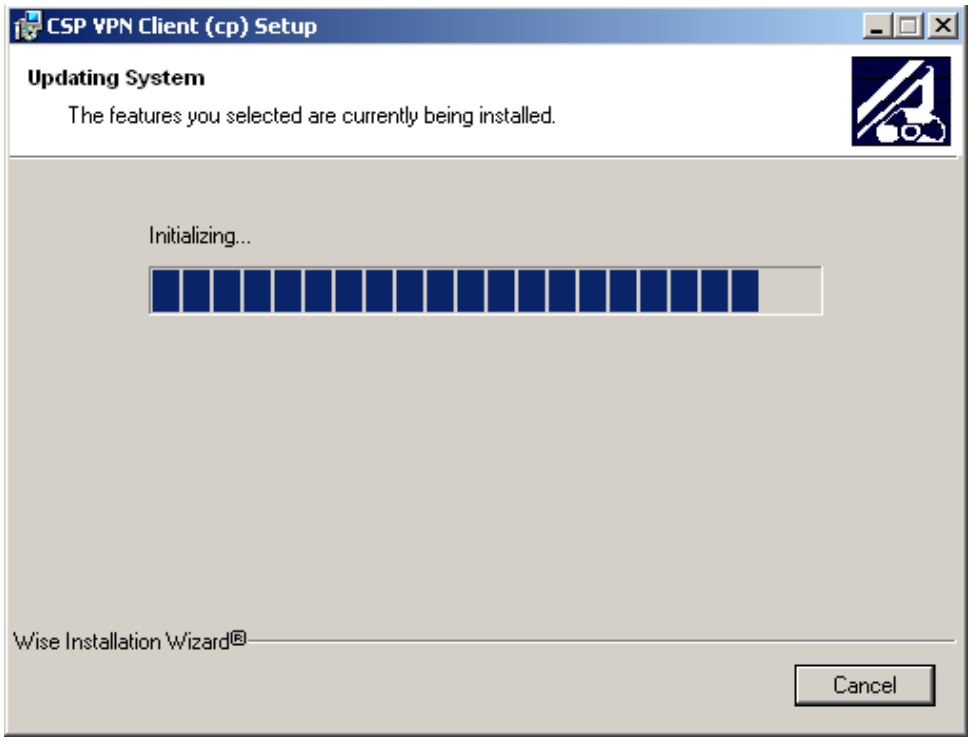

Рисунок 27

Создается контейнер, в который будет записано начальное значение ДСЧ. Если ключевой считыватель Реестр уже инсталлирован, то в него и будет записан контейнер. Если Реестр не инсталлирован, то появится окно с предложением выбрать ключевой носитель:

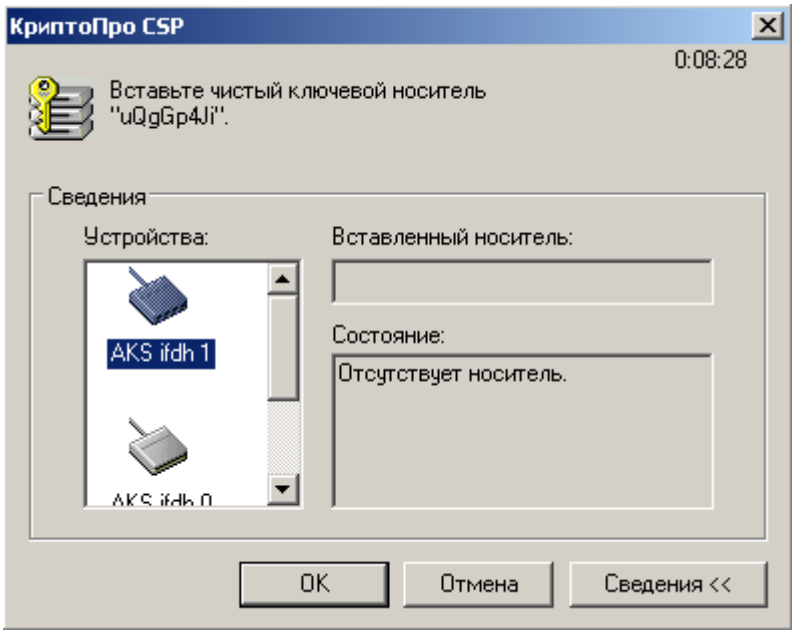

Рисунок 28

Предлагается «биологическая» инициализация ДСЧ – понажимайте клавиши или перемещайте указатель мыши:

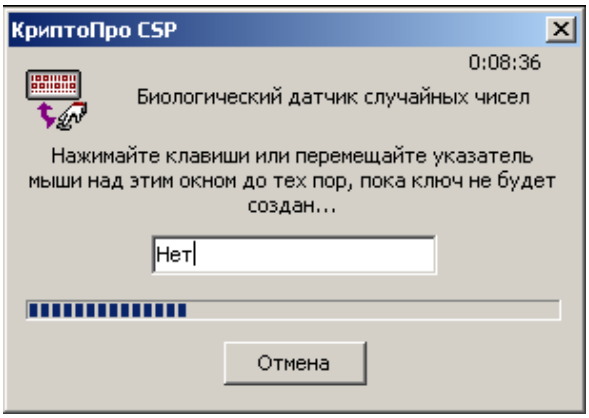

Рисунок 29

При инсталляции в ОС **Windows Vista/Windows 7** появляется окно (Рисунок 30) с запросом на установку драйверов. Выберите предложение – Все равно установить этот драйвер.

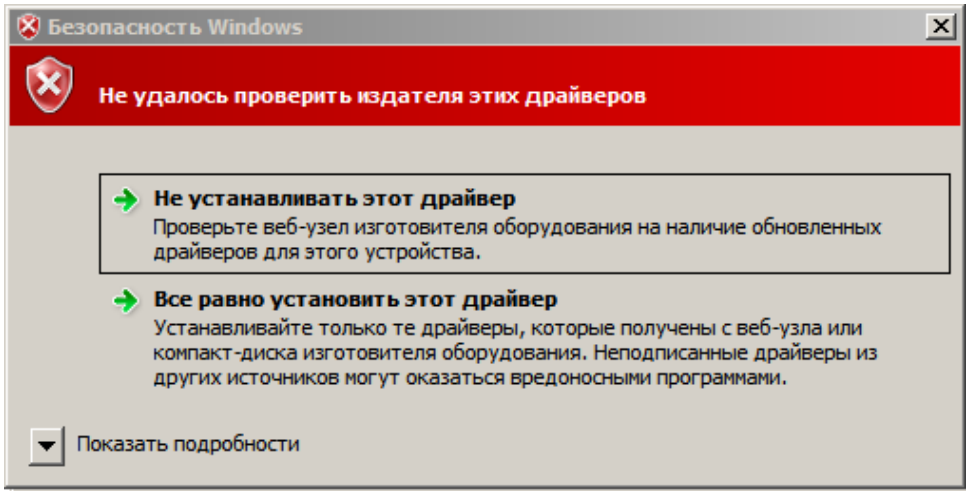

Рисунок 30

При инсталляции в ОС **Windows XP** и если реакция системы Windows на установку неподписанных драйверов установлена в положение `Предупреждать` (`Пуск – Настройка – Панель управления - Система – Свойства системы- Оборудование – Подписывание драйверов – Предупреждать`), то возможно появление окна (Рисунок 31) для подтверждения установки VPN Filter на интерфейс. Таких окон может появиться несколько. Для продолжения процесса инсталляции нажмите кнопку `Все равно продолжить` в каждом из этих окон:

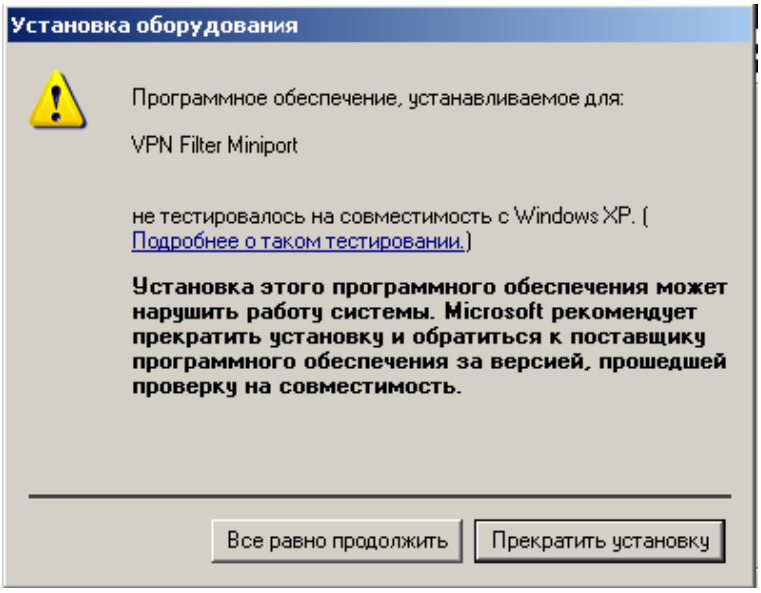

Рисунок 31

Для отключения возможности появления такого окна, установите реакцию системы Windows на установку неподписанных драйверов в положение `Пропускать (Пуск – Настройка – Панель управления - Система – Свойства системы- Оборудование – Подписывание драйверов – Пропускать)`.

При инсталляции в ОС **Windows XP Embedded**, при установке драйверов не показывается предупреждение об установке неподписанных драйверов (вне зависимости от соответствующей системной настройки).

При попытке установки драйвера vpndrvr, система может не найти файлы vpndrvr.sys, netvpn_m.inf, которые изначально располагаются в директории Продукта, и выдать окно с запросом на указание пути к одному из этих файлов:

```
The file '<имя_файла>' on VPN Filter Disk is needed.
Type the path where the file is located, and then click OK.
Copy files from:...
```

Укажите директорию Продукта по кнопке `Browse...`

По окончании установки CSP VPN Client выдается окно (Рисунок 50) с предупреждением о необходимости перезагрузки операционной системы.

Примечание: если при инсталляции будет обнаружена база локальных настроек, оставшаяся от предыдущей установки продукта, то по умолчанию происходит обновление базы локальных настроек кроме тех, которые отсутствуют при новой инсталляции. В некоторых ситуациях это может привести к неработоспособности или некорректной работе продукта.

7.2. Режим normal

В ОС **Windows Vista/Windows 7** при установке CSP VPN Client выдается окно (Рисунок 24). Необходимо разрешить запуск инсталлятора – выберите предложение Разрешить.

Этот режим является диалоговым режимом. Открывается стартовое окно визарда с приглашением к инсталляции:

Рисунок 32

После нажатия кнопки Next будет открыто окно визарда с текстом Лицензионного Соглашения. После установки переключателя в положение "`I accept the license agreement`" будет доступна кнопка `Next`:

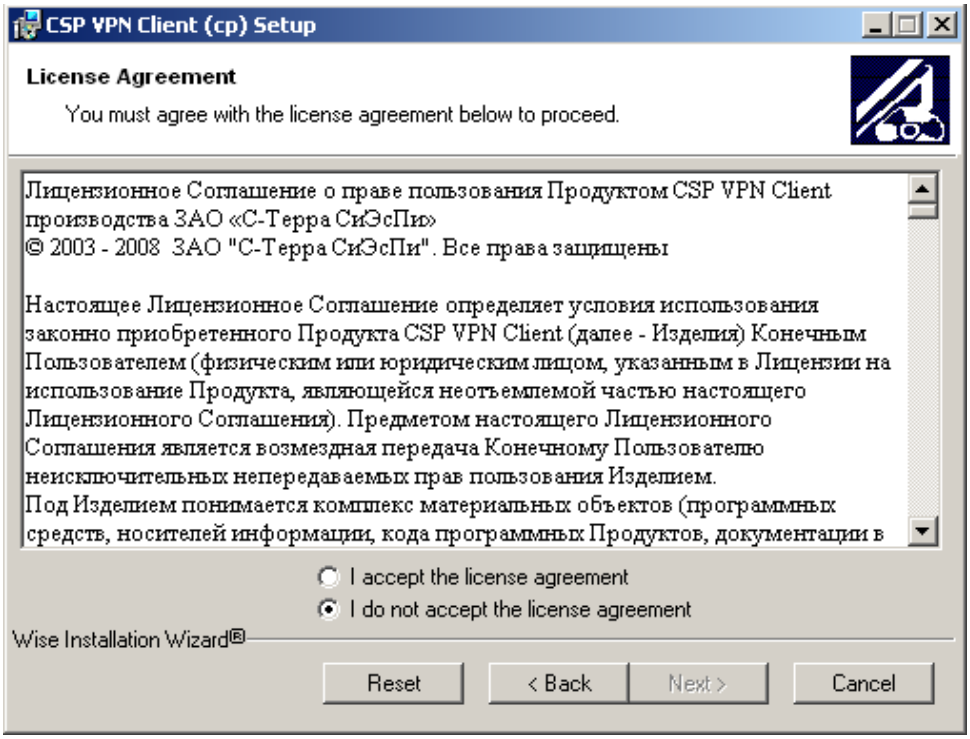

Рисунок 33

Для указания папки, в которую будет установлен Продукт, нажать кнопку `Browse` и сделать выбор:

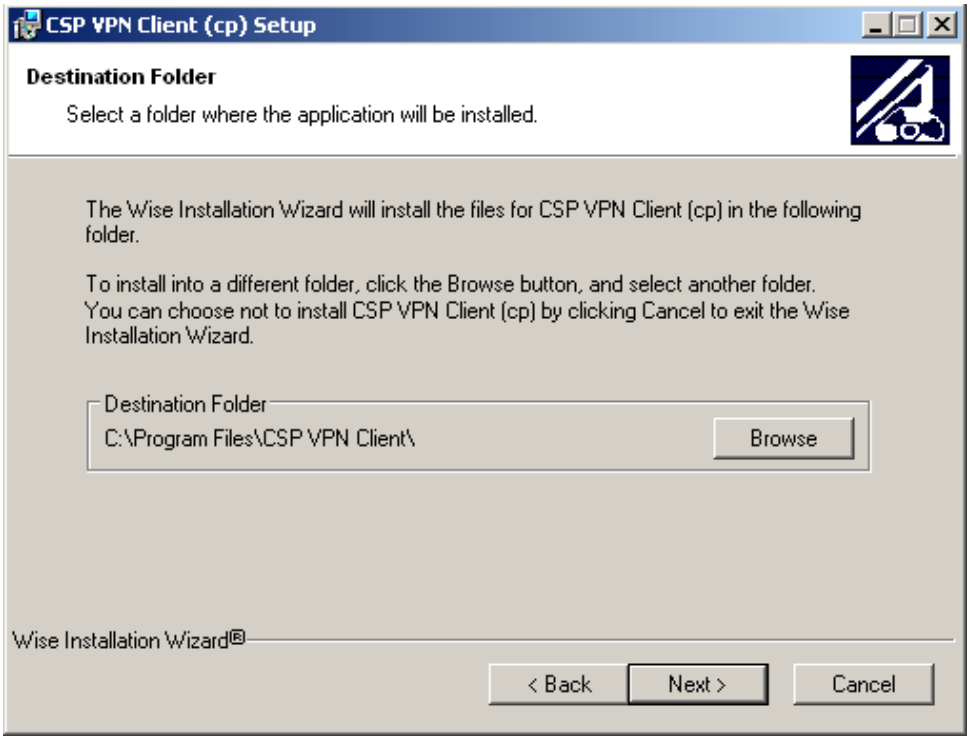

Рисунок 34

Если при создании инсталляционного файла регистрационные данные Лицензии на Продукт CSP VPN Client не были включены в инсталляционный файл, то появится окно для ввода данных Лицензии на Продукт:

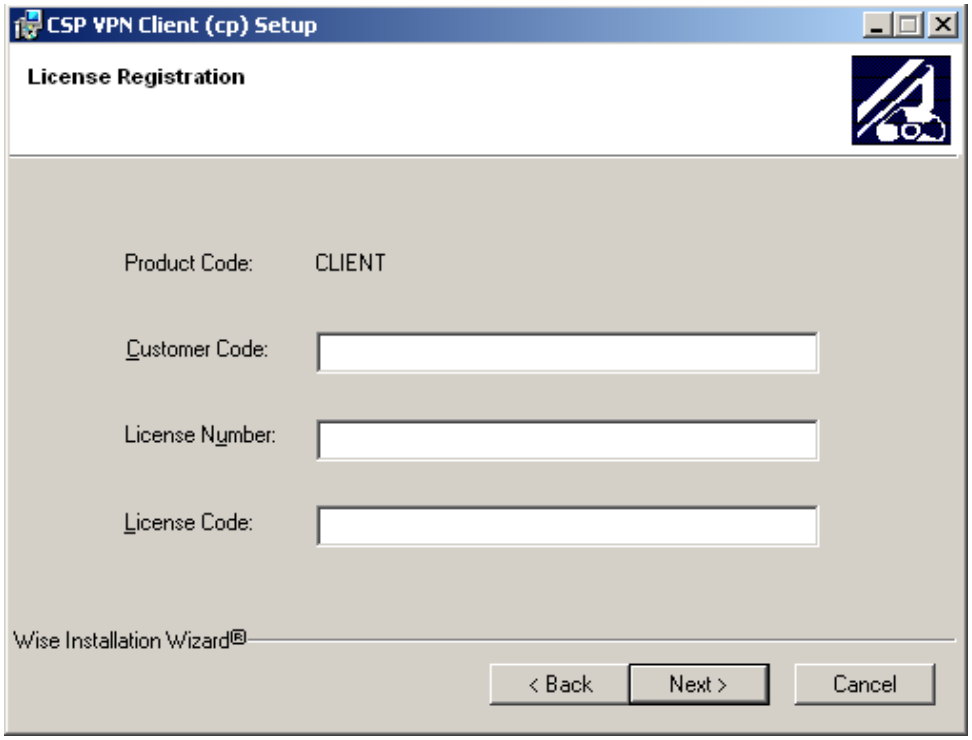

Рисунок 35

Стандартное окно визарда сообщает о готовности к инсталляции. Для начала инсталляции нажать Next:

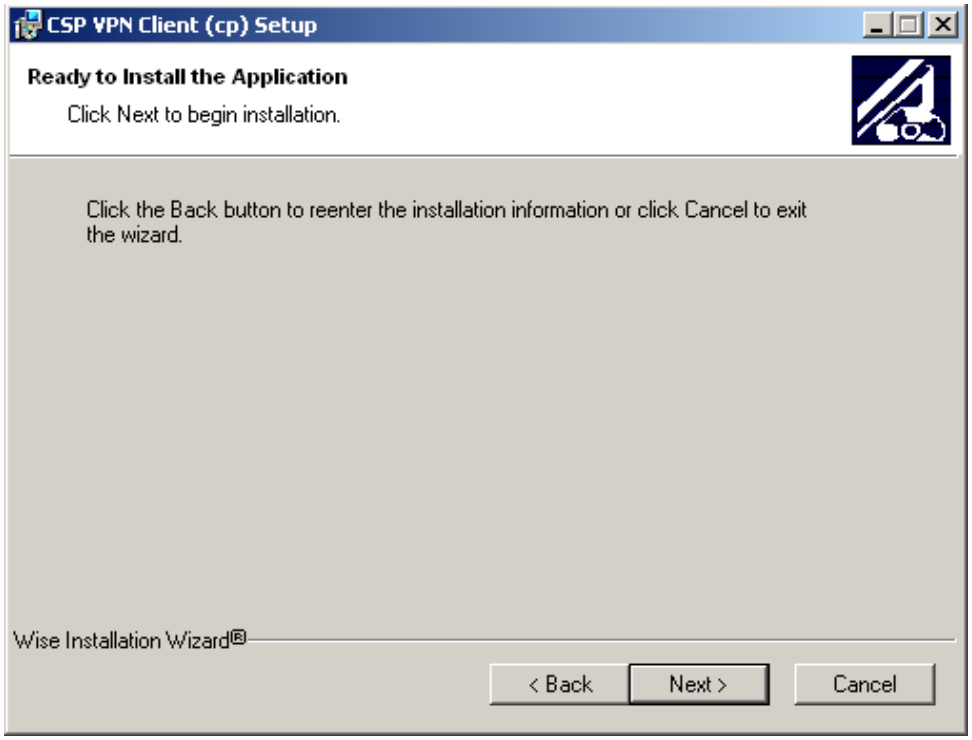

Рисунок 36

Далее появляется окно с индикатором процесса инсталляции:

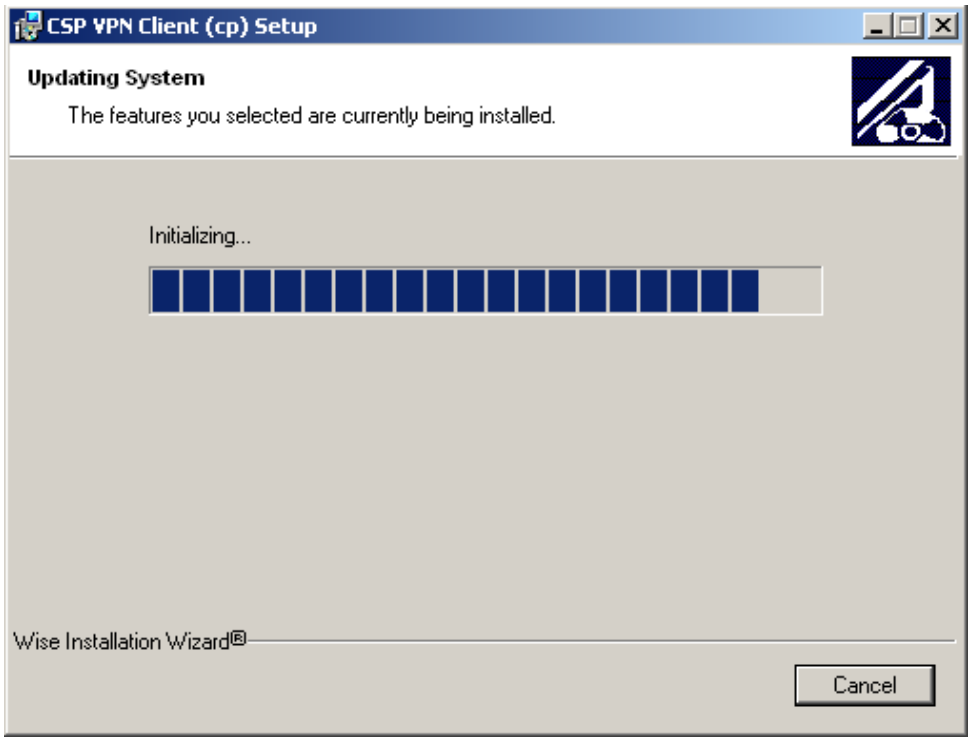

Рисунок 37

Создается контейнер, в который будет записано начальное значение ДСЧ. Если ключевой считыватель Реестр уже инсталлирован, то в него и будет записан контейнер. Если Реестр не инсталлирован, то появится окно с предложением выбрать ключевой носитель (Рисунок 38):

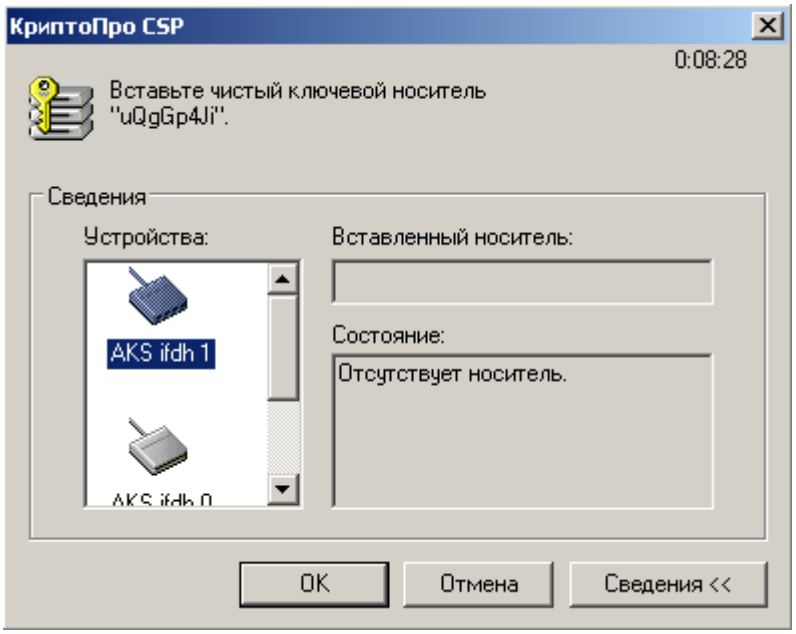

Рисунок 38

Предлагается «биологическая» инициализация ДСЧ – понажимайте клавиши или перемещайте указатель мыши:

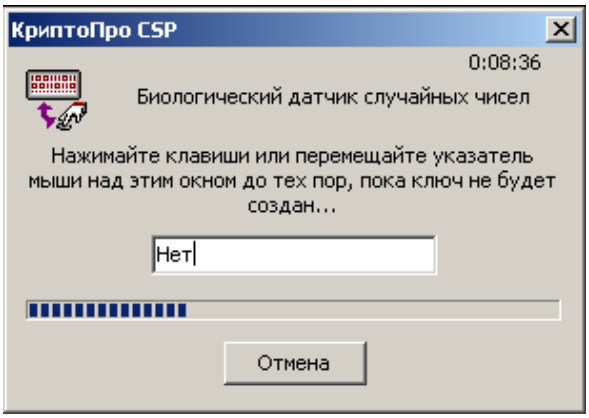

Рисунок 39

Дальнейшее поведение инсталлятора зависит от ОС и установленной пользователем опции `Подписывание драйверов`, описанной в разделе "Режим basic".

После завершения процедуры инсталляции нажать Finish:

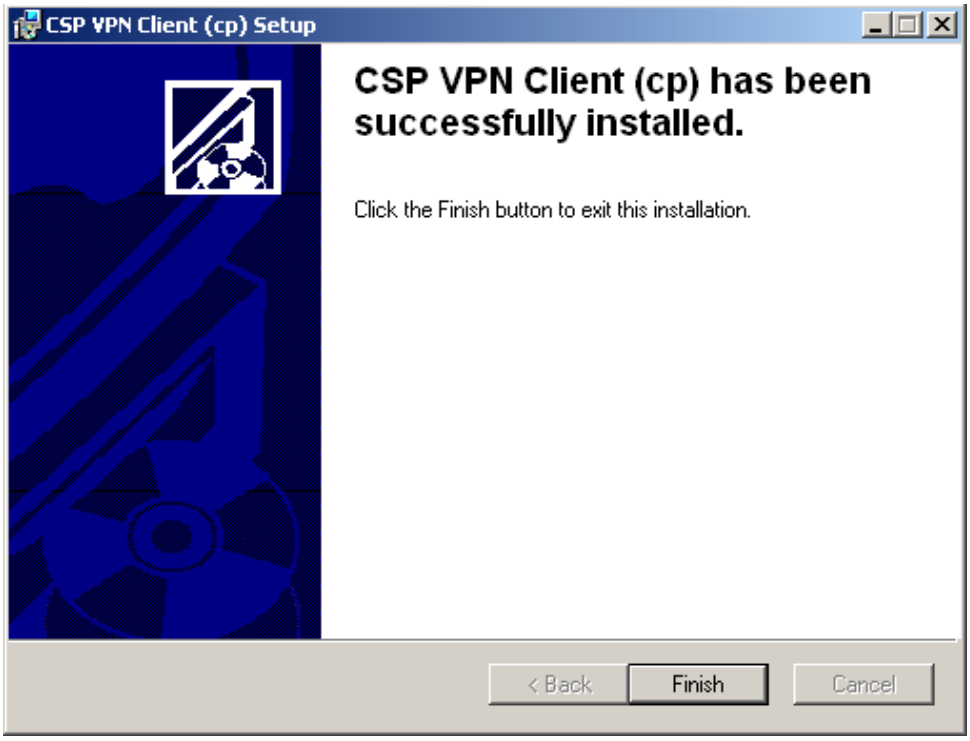

Рисунок 40

По окончании установки CSP VPN Client выдается окно (Рисунок 50) с предупреждением о необходимости перезагрузки операционной системы.

7.3. Режим silent

В ОС **Windows Vista/Windows 7** при установке CSP VPN Client выдается окно (Рисунок 24). Необходимо разрешить запуск инсталлятора – выберите предложение Разрешить.

В режиме silent происходит установка CSP VPN Client без запросов, но могут появляться либо системные диалоговые окна, либо некоторые интерактивные компоненты, относящиеся к криптоподсистеме.

Рисунок 41

Создается контейнер, в который будет записано начальное значение ДСЧ. Если ключевой считыватель Реестр уже инсталлирован, то в него и будет записан контейнер. Если Реестр не инсталлирован, то появится окно с предложением выбрать ключевой носитель (Рисунок 42):

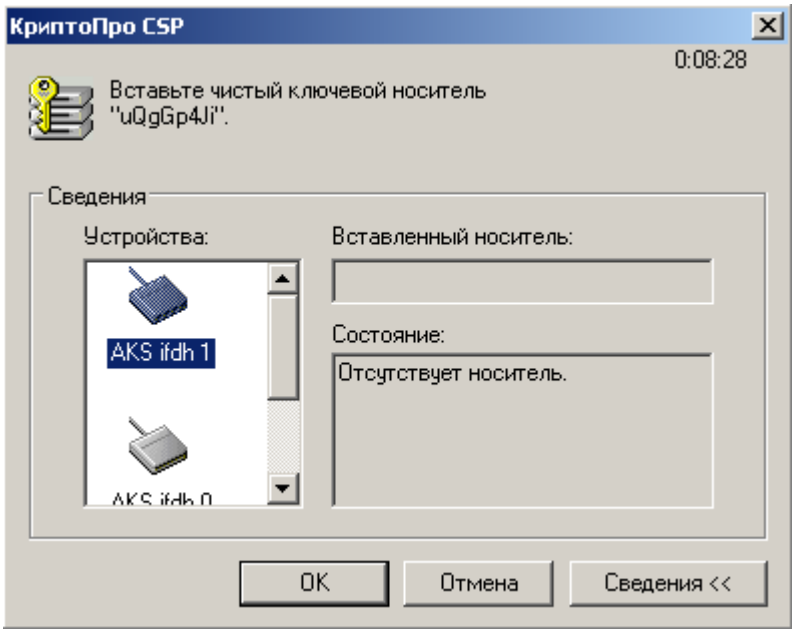

Рисунок 42

Предлагается «биологическая» инициализация ДСЧ – понажимайте клавиши или перемещайте указатель мыши:

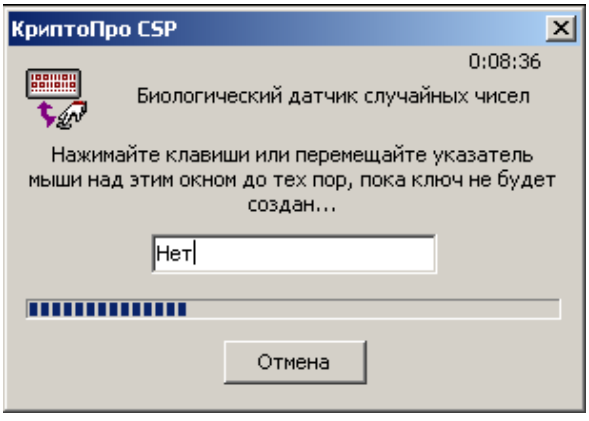

Рисунок 43

Дальнейшее поведение инсталлятора зависит от ОС и установленной пользователем опции `Подписывание драйверов`, описанной в разделе "Режим basic".

По окончании установки CSP VPN Client происходит перезагрузка операционной системы без предупреждений.

В случае возникновения ошибок и прерывания инсталляции никакие сообщения на экран не выводятся. Эти сообщения можно посмотреть программой ОС Windows «Просмотр событий» или, если при подготовке инсталляционного пакета Администратором была указана опция протоколирования событий при инсталляции в файл, то сообщения можно посмотреть в заданном файле.

Примечание: если при инсталляции будет обнаружена база локальных настроек, оставшаяся от предыдущей установки продукта, то по умолчанию происходит обновление базы локальных настроек кроме тех, которые отсутствуют при новой инсталляции. В некоторых ситуациях это может привести к неработоспособности или некорректной работе продукта.

7.4. Копирование контейнера при инсталляции

Если при подготовке инсталляционного файла с использованием сертификатов было задано копирование контейнера, то такое копирование контейнера с секретным ключом будет происходить при инсталляции CSP VPN Client.

В случае, если контейнер, в который происходит копирование уже существует, то выдается окно следующего вида:

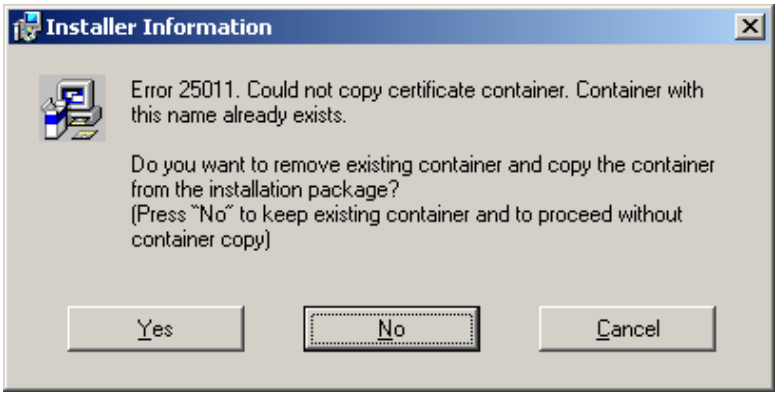

Рисунок 44

Если нажать `Yes`, то существующий контейнер будет удален и процедура копирования будет продолжена.

Если нажать `No`, существующий контейнер останется, а процедура копирования будет отменена.

Если нажать `Cancel`, то инсталляция клиента будет прервана.

Опишем последовательность действий при копировании контейнера с внешнего ключевого носителя, например, дискеты, в Реестр так, как она выглядит для пользователя.

При копировании в первом окне предлагается установить внешний ключевой носитель в устройство считывания, с которого будет производиться копирование контейнера, например, дискету. Это окно не появляется, если ключевой носитель уже установлен (например, дискета находится в дисководе):

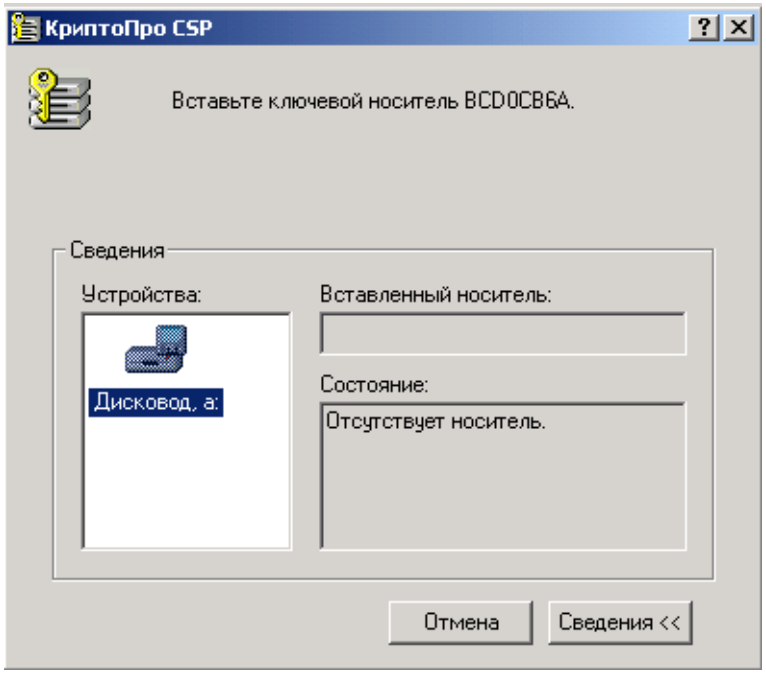

Рисунок 45

Отображается работа утилиты копирования в текстовом окне:

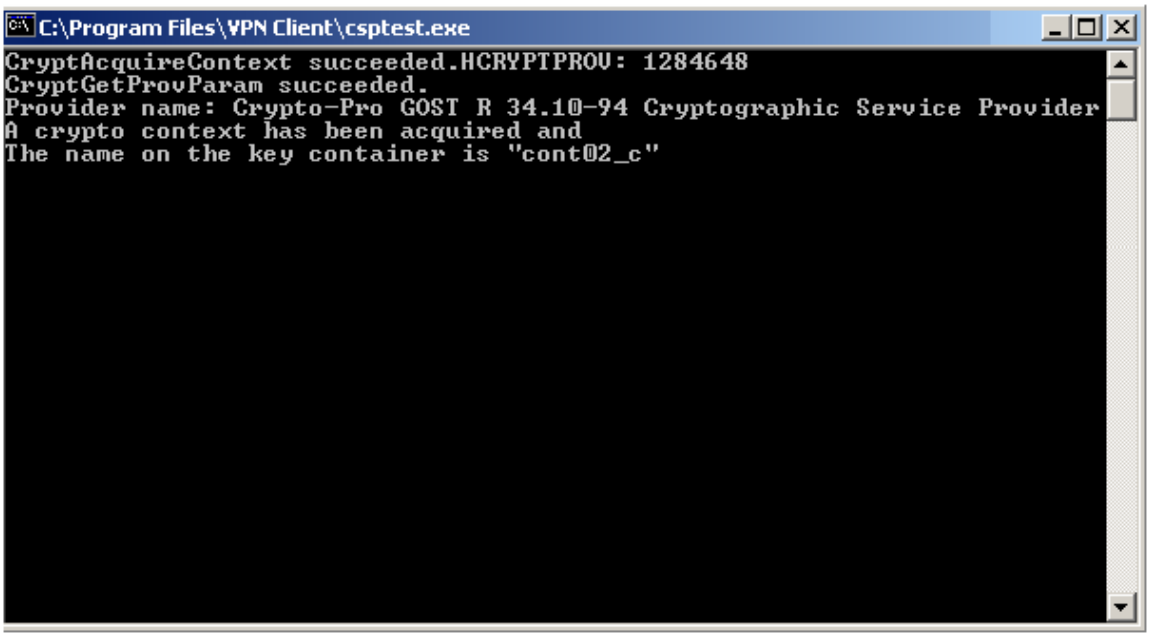

Рисунок 46

Если исходный контейнер защищен паролем, а при подготовке инсталляционного файла он не был задан, то появляется окно для ввода пароля:

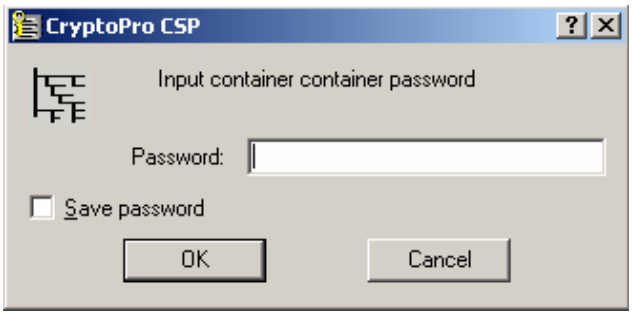

Рисунок 47

В окне с запросом пароля для нового контейнера надо ввести пароль, который обязательно должен совпадать с указанным паролем при подготовке инсталляционного файла. Если используется пустой пароль - достаточно нажать OK:

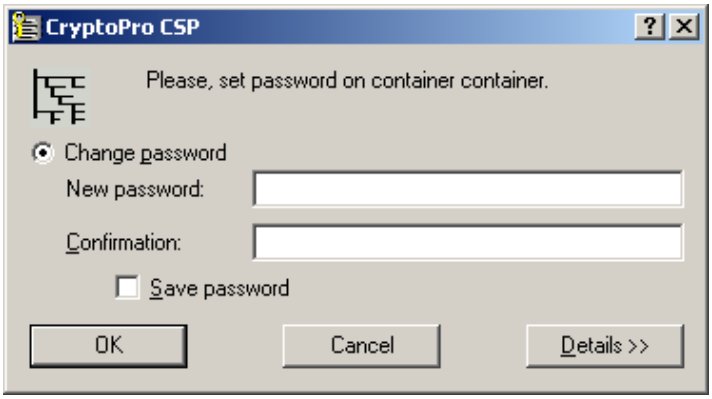

Рисунок 48

Если при копировании контейнера возникли ошибки, то в текстовом окне появляется сообщение об ошибке и предложение нажать на Enter:

Рисунок 49

Инсталляция после этого завершится с сообщением об ошибке: "`Copy certificate container failed. Installation aborted.`"

Если копирование прошло без ошибок, текстовое окно просто закрывается. Инсталляция Продукта продолжается.

Примечание: если инсталляции происходит в режиме `silent`, и на компьютере пользователя уже существует контейнер с указанным именем, в который происходит копирование, то инсталляция прерывается без выдачи на экран каких-либо запросов пользователю.

7.5. Перезагрузка операционной системы

После установки CSP VPN Client в режимах `basic` и `normal` открывается окно, сообщающее о необходимости перезагрузки операционной системы:

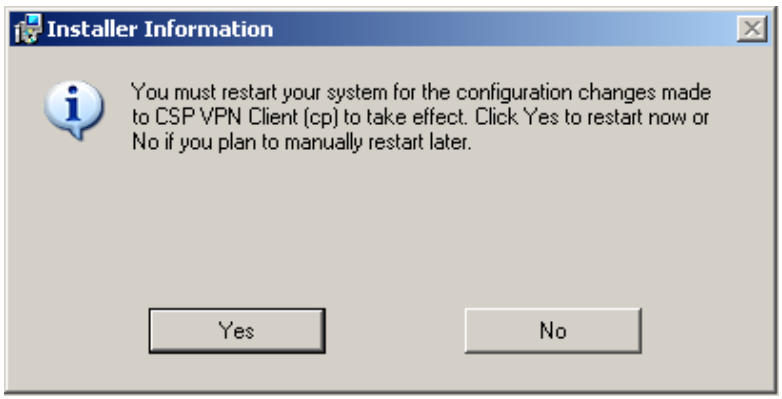

Рисунок 50

После нажатия кнопки `Yes` происходит перезагрузка операционной системы, а нажатие кнопки `No` закрывает окно без перезагрузки.

7.6. Сообщения об ошибках

Ниже приведены тексты сообщений об ошибках, которые могут возникать при инсталляции CSP VPN Client.

Таблица 2

	Текст сообщения	Примечание
25001	License check failed.	Неправильная лицензия
25002	CryptoPro must be installed before the product installation.	Перед установкой Продукта должно быть установлено CryptoPro
25006	RNG initialization failed. {Reason: <reason>.} Installation aborted, где <reason> может быть одной из следующих: Random initialization tool returned an error You must have Administrator privileges Random initialization tool not found Random initialization tool can't run: system error Random value initialization failed В отдельных случаях Reason может отсутствовать	Не удалось создать RNG контейнер. {Причина: <reason>} Инсталляция прервана, где причина может быть одной из следующих: Утилита для инициализации ДСЧ вернула ошибку Вы должны иметь администраторские привилегии Утилита для инициализации ДСЧ не найдена Не удалось запустить утилиту для инициализации ДСЧ: системная ошибка Инициализация ДСЧ провалилась

	Текст сообщения	Примечание
25009	Copy certificate container failed. {Reason: <reason>.} Installation aborted. Source container path: <src>. Destination container path: <dst>.	Не удалось скопировать сертификатный контейнер. {Причина: <reason>} Инсталляция прервана. Путь к исходному контейнеру: <src>. Путь к новому контейнеру: <dst>.
25011	Could not copy certificate container. Container with this name already exists. Do you want to remove existing container and copy the container from the installation package? (Press “No” to keep existing container and to proceed without container copy)	Нельзя скопировать сертификатный контейнер, поскольку контейнер с таким именем уже есть. Хотите ли вы удалить существующий контейнер и скопировать контейнер из инсталляционного пакета? (Нажмите “No” для того, чтобы сохранить существующий контейнер и продолжить без копирования)
25016	Version {<Version> } of CryptoPro CSP is not supported. CryptoPro CSP version 3.6 must be installed before the product installation	Версия <Version> продукта КриптоПро CSP не поддерживается. Должно быть установлено КриптоПро CSP версии 3.6 до инсталляции продукта. Примечания: <Version> в сообщении может отсутствовать, если ее не удалось определить Для версии 3.6 с build меньше, чем 5402, к <Version> добавляется приписка “(beta)” К <Version> добавляется приписка “(unrecognized)”, если по каким-либо причинам не удалось определить build КриптоПро CSP.
25017	Product "<Product_name version>" was detected. You should uninstall it first before the installation.	Был обнаружен Продукт "<Product_name version>". Вам необходимо сначала деинсталлировать его.
	You must have Administrator privileges	Вам необходимы администраторские привилегии
	This product needs Windows 2000 or higher	Для Продукта необходима Windows 2000 или выше
25019	The "<dll_path>" was wrongly marked as the previous GINA DLL. The system GINA DLL will be used instead.	**[Windows XP]** Файл <dll_path> был ошибочно помечен, как предыдущая GINA DLL. Будет использована системная GINA DLL.
25020	The previous GINA DLL "<dll_path>" was not found. The system GINA DLL will be used instead.	**[Windows XP]** Предыдущая GINA DLL <dll_path> не найдена. Будет использована системная GINA DLL.
25021	Driver "<driver_name>" installation failed. Product installation aborted.	Не удалось установить драйвер <driver_name>. Инсталляция продукта прервана.

	Текст сообщения	Примечание
25022	Product "<Product_name version>" was advertised. You should uninstall it first before the installation.	Для продукта <Product_name version> была выполнена операция объявления пользователям (advertisement). Вы должны деинсталлировать его до инсталляции.
25023	There is no CryptoPro CSP driver library installed on the system. You should install it first before the installation. Product installation aborted.	Не установлена драйверная библиотека КриптоПро CSP. Вы должны инсталлировать ее до инсталляции продукта. Инсталляция продукта прервана.
25025	Windows Firewall setup failed.	**[Windows Vista]** Не удалось настроить Windows Firewall.
25026	You must have administrator privileges.	Вам необходимы администраторские привилегии.
25032	Version {<Version> } of CryptoPro CSP is higher than the supported one. It could be incompatible with the product. Do you want to continue the installation?	Версия КриптоПро CSP больше, чем поддерживаемая. Она может быть несовместима с продуктом. Продолжить инсталляцию?

8. Регистрация пользователя

При подготовке инсталляционного пакета возможно было установить интерактивный или неинтерактивный режим логина пользователя в Продукт.

ОС Windows XP

В ОС Windows XP после перезагрузки ОС при интерактивном режиме появляется окно логина (Рисунок 55) в Продукт (см. раздел “Интерактивный режим логина в Продукт”). Это окно появляется только после инициализации VPN сервиса (см. раздел “Время инициализации VPN сервиса”).

Окно логина в ОС Windows XP появляется только после регистрации пользователя в Продукте или отказе от нее.

При неинтерактивном режиме логина в Продукт или переключении на него см. раздел “Неинтерактивный режим логина в Продукт”.

ОС Windows Vista/Windows 7

В ОС Windows Vista/Windows 7 после перезагрузки ОС при интерактивном режиме логина на экран выводятся иконки для выбора пользователя, иконка, отображающая текущий статус Продукта CSP VPN Client и окно логина в Продукт (Рисунок 51).

В ОС Windows Vista/Windows 7 процессы входа в ОС и логина в Продукт независимы друг от друга. Можно сначала зарегистрироваться в Продукте, а потом войти в ОС или наоборот.

Рисунок 51

В окне выбора пользователя (Рисунок 51) иконка, отображающая текущий статус Продукта, может быть смещена в нужном направлении, если ее положение неудобно (см. раздел “Изменение положения иконки текущего статуса Продукта”).

В ОС Windows Vista/Windows 7 окно логина в Продукт автоматически появляется в интерактивном режиме, когда необходимо выбрать пользователя для входа в ОС:

- после загрузки системы
- при выходе пользователя из системы
- при смене пользователя.

При неинтерактивном режиме логина в Продукт или переключении на него см. раздел “Неинтерактивный режим логина в Продукт”.

Окно логина в Продукт (Рисунок 55) будет выводиться только при запущенном VPN сервисе. Если к моменту вывода окна ОС Windows еще не запустила VPN сервис, то Продукт будет ждать 30 секунд (время по умолчанию). Если VPN сервис не будет запущен и через 30 секунд, то появится сообщение с предложением повторить процесс логина (Рисунок 52). Чтобы данное окно не появлялось – увеличьте время инициализации сервиса (см. раздел “Время инициализации VPN сервиса”).

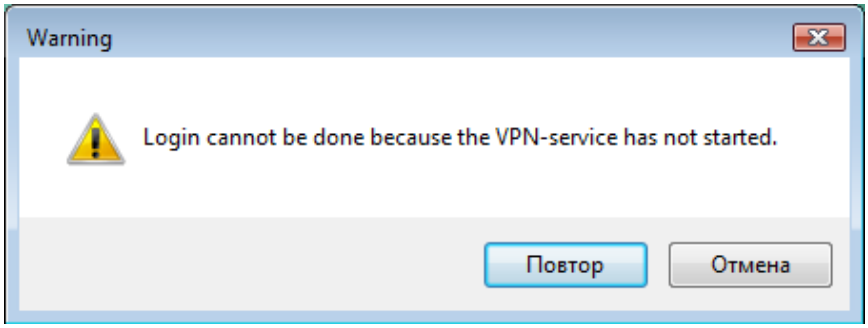

Рисунок 52

После успешной регистрации пользователя в Продукте иконка статуса Продукта изменит свой вид (Рисунок 53) (см. главу “Отображение текущего статуса Продукта”):

Рисунок 53

После входа пользователя в ОС иконка статуса Продукта будет размещена в панели задач.

Если отказаться от логина пользователя в Продукт, то потом зарегистрироваться в Продукте можно:

- нажав на иконку статуса Продукта в окне выбора пользователя, и в выпадающем меню выбрать предложение Login (Рисунок 54)
- либо после входа в ОС, нажав на иконку статуса Продукта в панели задач (см. раздел “Login/Logout”).

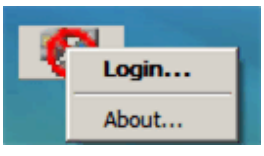

Рисунок 54

8.1. Интерактивный режим логина в Продукт

При интерактивном режиме логина в Продукт после перезагрузки операционной системы открывается окно для ввода и изменения пароля пользователя. По умолчанию пароль является пустым.

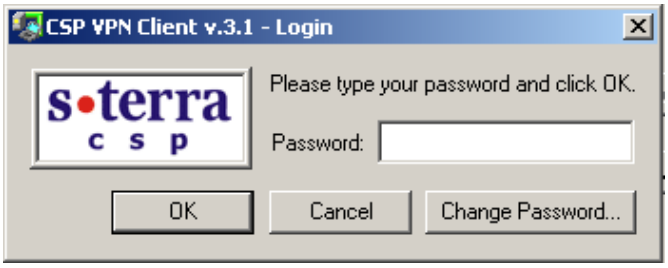

Рисунок 55

При нажатии на кнопку Change Password откроется окно, в котором можно изменить пароль пользователя:

Рисунок 56

Для смены пароля необходимо ввести старый пароль и новый с подтверждением правильности нового пароля. Если старый пароль вводится трижды неправильно, то каждая последующая попытка ввода пароля будет прерываться паузой на полминуты.

При успешной аутентификации пользователя в Продукт загружается локальная политика безопасности, заданная для данного пользователя администратором и находящаяся в базе Продукта.

Специальная политика безопасности `Log-off policy`, которая задается администратором при подготовке инсталляционного пакета, и служит для безопасности работы пользователя, при которой клиент не может создавать защищенных соединений, загружается автоматически в следующих случаях:

- до тех пор, пока пользователь не ввел свой пароль
- при вводе неверного пароля три раза
- при отказе от регистрации (login), если нажать кнопку Cancel
- при выходе пользователя из системы
- при смене пользователя.

Политика `Log-off policy` - агент работает по одному из двух правил:

- правило `Drop All` – удалять любой трафик, приходящий на компьютер пользователя

- правило `Default Driver Policy (DDP)` – политика драйвера по умолчанию, может принимать одно из двух значений:
  - правило `Passall` – пропускать все пакеты. Значение по умолчанию
  - правило `PassDHCP` – пропускать пакеты только по протоколу DHCP. Трафик DHCP пропускается для настройки TCP/IP стека по протоколу DHCP.

Политика Default Driver Policy (DDP), которая задается администратором, загружается в следующих случаях:

- при ошибочной загрузке конфигурации – до старта VPN сервиса
- при остановке VPN сервиса.

8.2. Неинтерактивный режим логина в Продукт

При неинтерактивном режиме логина в Продукт автоматически производится попытка логина с пустым паролем (в качестве пароля используется пустая строка) и при успешном логине окно с запросом пароля (Рисунок 55) не появляется. При неуспешном логине - Продукт ведет себя как при интерактивном логине - будет выдано окно запроса пароля (Рисунок 55).

При установленном Продукте CSP VPN Client можно изменить интерактивный режим логина на неинтерактивный. Включение неинтерактивного режима осуществляется установкой значения, отличного от 0, переменной в реестре NonInteractiveLogin:

`HKEY_LOCL_MACHINE\SOFTWARE\VPN Agent\NonInteractiveLogin.`

При значении 0 будет включен интерактивный режим (значение по умолчанию).

8.3. Время инициализации VPN сервиса

В ОС Windows можно задать время инициализации VPN сервиса в реестре при помощи переменной `MaxServiceStartTimeout`:

`HKEY_LOCL_MACHINE\SOFTWARE\VPN Agent\MaxServiceStartTimeout`

Эта переменная задает время в секундах ожидания запуска VPN сервиса. Если эта переменная не задана, то принимается значение по умолчанию, равное 30 секундам. Максимальное значение, которое можно задать – 600 секунд. При задании большего значения – устанавливается значение в 600 секунд.

При старте vpn-сервиса выполняется стартовый контроль целостности установленного Продукта CSP VPN Client, описанный в разделе «Стартовый и регламентный контроль целостности продукта».

8.4. Неинтерактивный режим логина в ОС

При интерактивном/неинтерактивном режиме логина в CSP VPN Client для автоматического входа пользователя в ОС Windows (не появляется окно Log On to Windows) выполните настройки, описанные для ОС Windows XP по адресу:

http://support.microsoft.com/?kbid=315231

Опишем здесь настройки трех переменных в Редакторе реестра:

- нажмите Пуск – Выполнить, введите `regedit`, нажмите `OK`
- в реестре войдите в ключ

`HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\WindowsNT\CurrentVersion\Winlogon`

- после двойного клика на переменной `DefaultUserName` в открывшемся окне в поле Значение введите имя пользователя и нажмите ОК
- двойным кликом на переменной `DefaultPassword` откройте окно и в поле Значение введите пароль пользователя, если эта переменная отсутствует, то создайте ее:
  - в окне Редактор реестра войдите в меню `Правка`, выберите предложение `Создать – Строковый параметр`
  - напечатайте имя переменной - `DefaultPassword` и нажмите Enter
  - двойным кликом на этой переменной откройте окно и в поле `Значение` введите пароль
- двойной клик на переменной `AutoAdminLogon` откроет окно, в котором в поле `Значение` введите 1 и нажмите `OK`. Если переменная `AutoAdminLogon` отсутствует, то создайте ее:
  - в окне Редактор реестра войдите в меню `Правка`, выберите предложение Создать `– Строковый параметр`
  - напечатайте имя переменной - `AutoAdminLogon` и нажмите Enter
  - двойным кликом на этой переменной откройте окно и в поле `Значение` введите 1 и нажмите `OK`
- Выйдите из Редактора реестра `– Выход`
- Нажмите `Пуск – Перезагрузка – OK.`

После этого вход пользователя в ОС будет осуществляться автоматически.

Замечание

Время загрузки ОС Windows XP с продуктом CSP VPN Client зависит от нескольких факторов, в том числе:

- аппаратной платформы (CPU, объема памяти, диска)
- количества и качества установленного программного обеспечения
- степени фрагментации жесткого диска
- количества накопленного "информационного мусора" в реестре.

Установленный на компьютер CSP VPN Client позволяет создавать защищенное соединение до логина пользователя в ОС Windows XP, но для этого пользователь должен пройти дополнительную аутентификацию (окно регистрации в продукт) перед логином в ОС.

Сервис аутентификации дожидается запуска всех пользовательских сервисов и запуска CSP VPN Client. Для давно эксплуатирующийся системы, где установлено много приложений, время загрузки сервисов значительно возрастает. На компьютерах с небольшим объемом памяти процесс загрузки сервисов еще увеличивается, поскольку системе не хватает памяти и она начинает выгружать только что загруженные приложения в swap файл на диск.

Ожидание появления дополнительного окна аутентификации может расцениваться пользователем как запуск конкретного приложения CSP VPN Client, а не запуск всех приложений ОС. Пользователю кажется, что загрузка ОС становится значительно дольше, хотя объективные замеры с секундомером доказывают обратное.

Чтобы избежать описанной выше ситуации рекомендуется выполнить некоторые действия:

- удалить неиспользуемые приложения, запускающиеся в процессе загрузки Windows
- выполнить чистку и дефрагментацию реестра
- выполнить дефрагментацию жесткого диска.

9. Стартовый и регламентный контроль целостности Продукта

В состав CSP VPN Client входит файл `.hashes`, который устанавливается в каталог Продукта (по умолчанию - “Program Files\CSP VPN Client”).

Файл `.hashes` содержит строки вида (между хэш-суммой и именем файла один пробел):

```
<hash> <encoded_file_path>
```

где

`<hash>` – эталонное значение хэш-суммы для данного файла

`<encoded_file_path>` - полный путь к проверяемому файлу

При старте сервиса vpnsvc автоматически запускается утилита `cspvpn_verify` для проверки целостности установленного Продукта. При успешной проверке никакого сообщения на экран не выдается, а в файл `cspvpn_verify_err.log`, расположенный в каталоге Продукта, передается сообщение: `Verification SUCCESS: <n> files verified`.

При обнаружении ошибки работа утилиты прерывается и выдается сообщение об ошибке в файл `cspvpn_verify_err.log`.

Регламентный контроль целостности CSP VPN Client осуществляется во время работы Продукта запуском вручную утилиты `cspvpn_verify` из каталога установленного Продукта.

При успешной проверке и при обнаружении ошибки реакция будет такой же как и при стартовом контроле.

Возможные сообщения об ошибках

Таблица 3

	Сообщение об ошибке	Описание проблемы	Код возврата	Продолжение работы утилиты
1	Integrity verification tool not found	Отсутствует продукт, используемый непосредственно для подсчета контрольных сумм.	1	
2	Integrity verification list “<file_.hashes_full_path >” not found	Отсутствует файл .hashes.	2	
3	Integrity verification list “<file_.hashes_full_path >” is corrupted	Проблемы с чтением файла .hashes (например, ошибочный синтаксис файла).	3	

4	Integrity verification tool call failed on file “<product_file_full_path> ”	Запуск cpverify по каким-либо причинам не произошел (какая-то системная ошибка; например, нехватка ресурсов, проблемы с правами доступа и т.п.) или вернул неожиданный код возврата (прерывание по сигналу, необработанный exception и т.п.).	4	+
5	File “<product_file_full_path> ” is corrupted	Один или больше файлов продукта повреждены (хэш-сумма не соответствует эталонной; также возможны и другие ситуации – например, отсутствующий файл – cpverify их не различает).	5	+

где

<file_.hashes_full_path> – полный путь к файлу .hashes

<product_file_full_path> – полный путь к файлу Продукта, на котором произошла ошибка.

При обнаружении ошибки по окончании работы утилиты выдается сообщение: Verification FAILED. Затем проверяется сервис vpnsvc и если он работает, то выполняется его аварийное прерывание.

Если обнаруживается несколько разнородных ошибок, то код возврата утилиты формируется по первому сообщению об ошибке.

При устранении ошибки перезапустите сервис vpnsvc:

```
net start vpnsvc.
```


10. Отображение текущего статуса Продукта

Текущий статус Продукта отображает иконка, расположенная в панели задач.

Если пользователь не аутентифицировался, то иконка имеет вид:

Рисунок 57

Пользователь аутентифицировался, но Продукт не имеет ни одного защищенного соединения – иконка принимает вид:

Рисунок 58

Когда появляется хотя бы одно защищенное соединение, но трафик по этим соединениям отсутствует, то на иконке изменяется цвет "соединения" с серого на зеленый:

Рисунок 59

Если Продукт имеет хотя бы одно защищенное соединение и обрабатывает трафик по этим соединениям, то на иконке изменяется цвет "монитора" с синего на бирюзовый:

Рисунок 60

При наведение курсора мыши на иконку всплывает информация о количестве "живых" SA (существующих на момент наведения курсора мыши на иконку) и количестве байт обработанного трафика по всем существовавшим и существующим SA с момента загрузки операционной системы.

Рисунок 61

10.1. Изменение положения иконки текущего статуса Продукта

В окне выбора пользователя (Рисунок 51) положение иконки, отображающей текущий статус Продукта, если оно неудобно, можно изменить с помощью переменной в реестре:

```
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Authentication\PLAP Providers\{7026F7B9-3C2E-4b80-A62E-69645BFF1190}\Position
```

Значением переменной `Position` является строка формата:

```
<int_x>,<int_y>
```

где

`int_x` – целое число, задающее смещение иконки по горизонтальной оси, которое может принимать значения:

- 0 - положение иконки задается автоматически с учетом разных параметров
- положит.знач. – положение иконки отсчитывается относительно левой стороны экрана
- отрицат.знач. – положение иконки отсчитывается относительно правой стороны экрана

`int_y` – целое число, задающее смещение иконки по вертикальной оси, которое может принимать значения:

- 0 - положение иконки задается автоматически с учетом разных параметров
- положит.знач. – положение иконки отсчитывается относительно верхней стороны экрана
- отрицат.знач. – положение иконки отсчитывается относительно нижней стороны экрана.

10.2. Login/Logout

При нажатии на иконку правой кнопкой мыши открывается меню следующего вида:

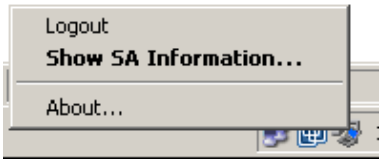

Рисунок 62

В зависимости от состояния системы (аутентифицировался пользователь или нет) будет показано предложение `Login` или `Logout`.

При выборе предложения `Login` появится окно ввода пароля (Рисунок 55) для аутентификации пользователя и изменения пароля.

При выборе предложения `Logout` выполнится следующее:

- будут уничтожены все существующие SA с данным клиентом
- загрузится специальная политика Log-off policy
- предложение `Logout` изменится на `Login`.

10.3. SA Information

При выборе предложения `Show SA Information` – появится окно монитора созданных SA вида:

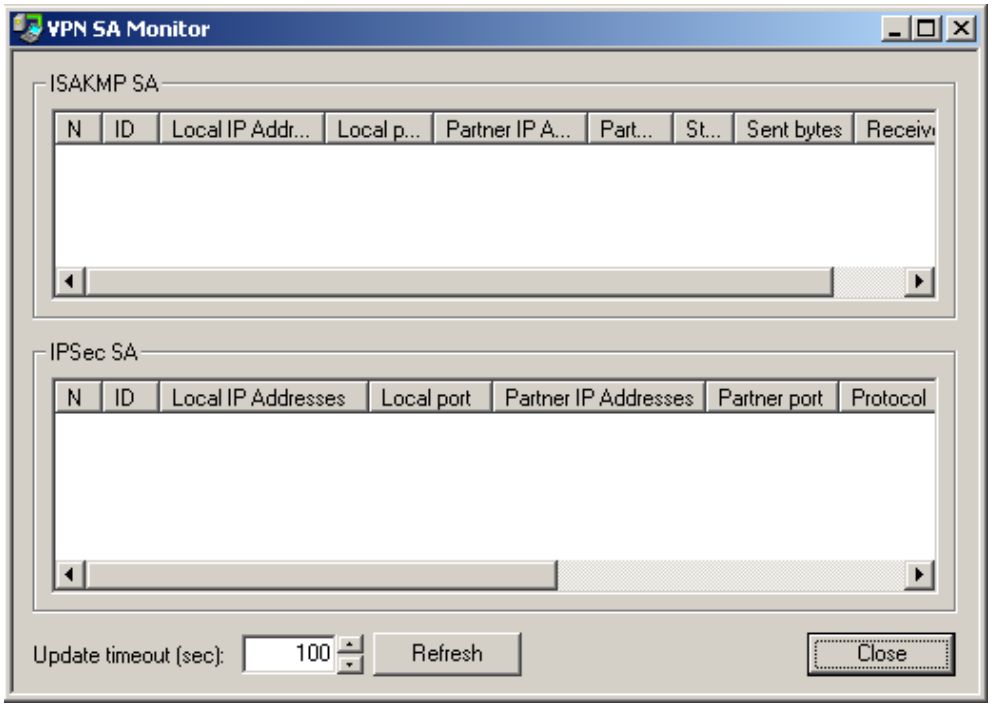

Рисунок 63

где:

`ISAKMP SA` – список ISAKMP SA. Выводятся следующие поля:

- `N` – порядковый номер в таблице
- `ID` – уникальный номер SA
- `Local IP Addresses` – локальные адреса
- `Local port` – локальный IKE порт
- `Partner IP Addresses` – партнерские адреса
- `Partner port` – партнерский IKE порт
- `State` – состояние SA:
  - `incomplete` – недостроенный
  - `ready` – рабочий
  - `configuration` – изменяемый
  - `deletion` – удаляемый
  - `unknown` – неизвестное состояние (не должно выводится)
- `Sent bytes` – количество отосланных байт
- `Received bytes` – количество полученных байт

`IPSec SA` – список IPsec SA с полями:

- `N` – порядковый номер в таблице
- `ID` – уникальный номер SA
- `Local IP Addresses` – локальные адреса
- `Local port` – локальные порты
- `Partner IP Addresses` – партнерские адреса
- `Partner port` – партнерские порты
- `Protocol` – сетевые протоколы
- `Action` – тип действия:
  - `AH`
  - `ESP`
  - `AH+ESP`
- `Type` – тип соединения:
  - `transport` – транспортный режим
  - `tunnel` – туннельный режим
  - `nat-t-transport` - транспортный режим через NAT
  - `nat-t-tunnel` - туннельный режим через NAT
- `Sent bytes` – количество отосланных байт
- `Received bytes` – количество полученных байт

`Update timeout (sec)` – время, через которое будут обновляться данные в таблице о созданных SA. Диапазон значений `1..9999`, начальное значение - `2`.

При выборе предложения `About` в меню выводится информация о версии Продукта:

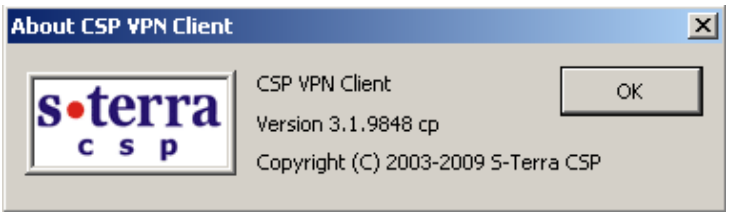

Рисунок 64

11. Деинсталляция CSP VPN Client

Деинсталляция CSP VPN Client производится стандартными средствами операционной системы – вызовом модуля Add/Remove Programs и выбором из списка строки CSP VPN Client.

При деинсталляции CSP VPN Client происходит включение стандартного сервиса, связанного с IPsec и IKE. В Windows XP – это Служба IPSEC, в Windows Vista/Windows 7 – это Служба «Модули ключей IPsec для обмена ключами в Интернете и протокола IP с проверкой подлинности».

В Windows Vista/Windows 7 при деинсталляции CSP VPN Client выдается окно (Рисунок 65). Необходимо разрешить запуск деинсталлятора.

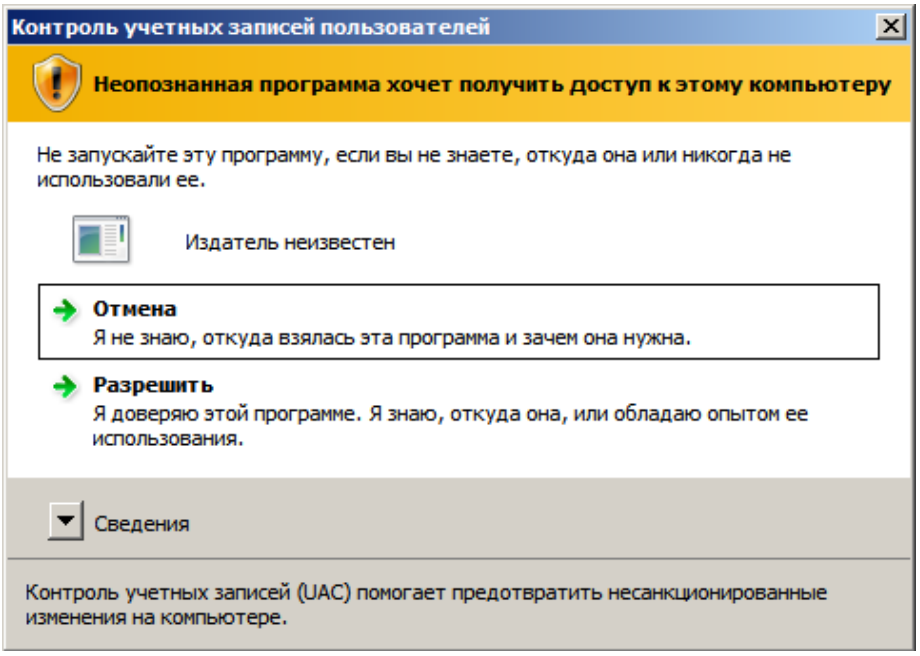

Рисунок 65

12. Восстановление CSP VPN Client

Во внештатных ситуациях – сбой в работе продукта, зависание продукта и др. перезагрузите LSP конфигурацию командой lsp_reload (если это возможно) или перезапустите компьютер. Если функции продукта не восстановились, то переустановите CSP VPN Client.

13. Специализированные команды

Программные утилиты, входящие в состав Продукта CSP VPN Client:

В операционной системе Microsoft® Windows выполнение этих команд можно производить из командной строки.

Для запуска утилиты из командной строки перейдите в папку, в которой находится утилита: `C:\Programs Files\CSP VPN Client.`

Запуск утилит с ключом `-h` вызывает помощь.

13.1. cert_show

Команда `cert_show` предназначена для просмотра сертификатов и списков отозванных сертификатов (CRL), лежащих в файле или базе Продукта.

Синтаксис

```
cert_show [-f C_FILE [-p C_FILE_PWD]] [-i OBJ_INDEX1]…
[-i OBJ_INDEXN] [-expired_remote]
```

`-f C_FILE`	путь к файлу с сертификатами.
`-p C_FILE_PWD`	пароль к файлу с сертификатами. Необязательный параметр. Используется только для доступа к файлам, защищенным паролем.
`-i OBJ_INDEXN`	индекс сертификата в файле или базе Продукта. Если при написании команды указан путь к файлу, то индекс будет задавать номер искомого сертификата в файле. Индекс задается в виде целого десятичного числа. В качестве индекса нельзя указывать 0.
`-expired_remote`	показать все сертификаты партнеров, срок действия которых истек. Сертификаты, не вступившие в силу, не показываются.

Значение по умолчанию значение по умолчанию отсутствует

Рекомендации по использованию

Используйте данную команду для ознакомления со списком сертификатов и CRL, размещенных в файле или базе Продукта. Без указания файла и индекса сертификата будет показан весь нумерованный список сертификатов и CRL, лежащих в базе Продукта.

13.2. cert_import

Команда `cert_import` предназначена для регистрации сертификатов партнеров и промежуточных CA сертификатов в базе Продукта.

Синтаксис

```
cert_import -f C_FILE [-p C_FILE_PWD] [-i OBJ_INDEX1]…
[-i OBJ_INDEXN]
```

`-f C_FILE`	путь к файлу с сертификатами
`-p C_FILE_PWD`	пароль к файлу с сертификатами. Необязательный параметр. Используется только для доступа к файлам, защищенным паролем.
`-i OBJ_INDEXN`	индекс сертификата в файле. При импорте одного сертификата из файла, содержащего один сертификат, данный параметр можно не указывать, он будет равен 1. Индекс задается в виде целого десятичного числа. В качестве индекса нельзя указывать 0.

Значение по умолчанию значение по умолчанию отсутствует.

Рекомендации по использованию

Используйте данную команду для импорта сертификатов партнеров в базу Продукта (сертификат партнера может быть получен и протоколу IKE). При импорте нескольких объектов из одного файла используйте последовательное описание параметров импортируемых объектов.

13.3. cert_check

Команда `cert_check` предназначена для проверки сертификатов, размещенных в базе Продукта.

Синтаксис **`cert_check`** `[-i OBJ_INDEXN]`

`-i OBJ_INDEXN`	индекс сертификата в базе Продукта, который следует проверить. Необязательный параметр.

Значение по умолчанию значение по умолчанию отсутствует

Рекомендации по использованию

Проверяются сертификаты, находящиеся в базе Продукта. Без указания параметра `-i` проверяются все сертификаты из базы Продукта.

Утилита выводит состояние сертификата `"Active"` или `"Inactive"`. В случае, если сертификат имеет состояние `"Inactive"`, то выводится краткое описание причины неактивности:

- `Certificate is invalid` – неверный формат сертификата
- `Certificate is expired` – срок использования сертификата истек
- `Certificate is not valid yet` – время использования сертификата не наступило
- `Certificate is revoked` – сертификат отозван
- `Certificate can not be verified` – сертификат не удается проверить:
  - в базе отсутствует сертификат(ы) для построения цепочки сертификатов с корректным конечным CA сертификатом, которому мы доверяем
  - в базе нет необходимого CRL для проверки одного из сертификатов цепочки, подобная ситуация может возникнуть при включении проверки CRLs (загружена DDP или в загруженной конфигурации явно задано CRLHandlingMode = ENABLE)
- `Private key container is not accessible` – нет доступа к контейнеру с секретным ключом
- `Private key is not accessible` – нет доступа к секретному ключу
- `Private key is not consistent certificate` – секретный ключ не подходит к сертификату
- `It is certificate request` – данный объект является сертификатным запросом.

13.4. client_login

Команда `client_login` запускается автоматически при логине пользователя в систему и представляет собой GUI-приложение (Рисунок 55), в котором нужно ввести пароль для аутентификации пользователя.

Эта команда запускается и при выборе предложения Login в меню (Рисунок 62), которое появляеся на иконке в панели задач при работающем сервисе после того, как было выбрано предложение Logout.

Может быть использована и для изменения пароля пользователя.

Синтаксис **`client_login`**

13.5. client_logout

Команда client_logout предназначена для завершения сессии пользователя. При этом производится загрузка политики Log-off Policy.

Эта команда запускается при выборе предложения Logout в меню (Рисунок 62), которое появляеся на иконке в панели задач при работающем сервисе после того, как было выбрано предложение Login. Возможен запуск команды вручную.

Синтаксис **client_logout**

Пример

Ниже приведен пример запуска вручную команды `client_logout`:

```
client_logout
Logout OK
```


13.6. pwd_change

Команда pwd_change предназначена для изменения пароля пользователя. Эта команда запускается автоматически при нажатии кнопки `Change Password...` в окне логина пользователя (Рисунок 55) и вызовом окна `Change Password` (Рисунок 55) для ввода старого и нового пароля. Эту команду можно запускать и вручную.

Синтаксис **pwd_change** [old_user_PWD new_user_PWD]

old_user_PWD	старый пароль
new_user_PWD	новый пароль

Если не задать старый и новый пароль, то в интерактивном режиме они будут запрошены. При вводе символов их печать на консоль не производится. Новый пароль будет запрошен дважды во избежание ошибки.

Пример

Ниже приведен пример изменения пароля пользователя:

```
pwd_change "old_pwd" "new_pwd"
New password is set successfully
```

```
pwd_change
Enter old password:
Enter new password:
Re-enter new password:
New password is set successfully
```


13.7. key_show

Команда `key_show` предназначена для просмотра предопределенных ключей, зарегистрированных в Продукте.

Синтаксис **`key_show`**

Данная команда не имеет аргументов и ключей.

Значение по умолчанию Значение по умолчанию отсутствует.

Рекомендации по использованию

Используйте данную команду для ознакомления со списком предопределенных ключей, хранящихся в базе Продукта.

При выполнении этой команды будут выводиться следующие данные:

- количество предопределенных ключей
- для каждого ключа:
  - имя ключа
  - тело ключа в печатном виде. Если тело ключа содержит непечатные символы, то при выводе в печатном виде они заменяются на `'.'` (символ точка).
  - тело ключа в hex-представлении.

Пример:

```
Found #1 keys.
----Key----
Name   :        key1
Content         testkey1..
Content (hex):  746573746B6579310D0A
```

13.8. lsp_show

Команда `lsp_show` предназначена для просмотра локальной политики безопасности пользователя (LSP).

Синтаксис **`lsp_show`**

Данная команда не имеет аргументов и ключей.

Значение по умолчанию Значение по умолчанию отсутствует.

Рекомендации по использованию

Если загружена конфигурация пользователя, то по данной команде она будет выведена.

При просмотре конфигурацию можно сохранить в файле, например `current_lsp.txt`, командой:

```
lsp_show > current_lsp.txt
```


13.9. lsp_reload

Команда `lsp_reload` предназначена для перезагрузки LSP конфигурации.

Синтаксис **`lsp_reload`**

Значение по умолчанию Значение по умолчанию отсутствует.

Рекомендации по использованию

Используйте команду `lsp_reload` в следующих случаях:

- если произошли какие-то изменения в сертификатах, изменения у партнера, у шлюза безопасности и др.
- для устранения всех установленных соединений с партнерами
- во внештатных ситуациях – зависание Продукта и др.

Пример

Ниже приведен пример загрузки LSP конфигурации из базы Продукта:

```
lsp_reload
LSP is reloaded successfully.
```


13.10. log_show

Команда `log_show` предназначена для просмотра настройки уровня протоколирования событий.

Синтаксис **`log_show`**

Данная команда не имеет аргументов и ключей.

Значение по умолчанию Значение по умолчанию отсутствует.

Рекомендации по использованию

Данная команда выводит текущий уровень протоколирования событий:

```
Log severity level: (3) err
```


13.11. dp_show

Команда `dp_show` предназначена для просмотра установленных настроек политики `Default Driver Policy`.

`Default Driver Policy` – политика безопасности, загружаемая при старте Продукта до загрузки конфигурации пользователя, или же при отгрузке пользовательской конфигурации. Возможные значения:

- `passall` - пропускать весь трафик
- `passdhcp` - пропускать только DHCP пакеты.

Синтаксис **`dp_show`**

Данная команда не имеет аргументов и ключей.

Значение по умолчанию Значение по умолчанию отсутствует.

Рекомендациипо использованию

Данная команда выводит установленное значение политики DDP, например:

```
Default Driver Policy : passall
```

13.12. sa_show

Команда `sa_show` предназначена для просмотра информации обо всех IPsec SA, ISAKMP SA и их состоянии и о количестве IKE обменов.

Синтаксис

sa_show [-isakmp|-ipsec] [-i CONN1_ID] [-i CONNn_ID] [-detail]

-isakmp	выводится информацию об ISAKMP соединениях
-ipsec	выводится информацию об IPsec соединениях
-i CONNn_ID	выводится информация о соединении с указанным идентификатором
-detail	выводится детальная информация о соединениях

Команда `sa_show` позволяет просмотреть действующие в данный момент `IPsec SA`.

Значение по умолчанию Значение по умолчанию отсутствует.

Рекомендации по использованию

sa_show

В данной команде без указания опции `-detail` выводится краткая информация обо всех соединениях, например:

```
ISAKMP sessions: 0 initiated, 0 responded

ISAKMP connections:
Num Conn-id (Remote Addr,Port)-(Local Addr,Port) State Sent Rcvd
1 2 (10.0.10.16,500)-(10.0.10.99,500) active 1560 656
2 3 (10.0.10.18,500)-(10.0.10.99,500) active 1560 656


IPsec connections:
Num Conn-id (Remote Addr,Port)-(Local Addr,Port) Protocol Action
Type Sent Rcvd
1 6 (192.168.15.16,*)-(10.0.10.99,*) * AH+ESP tunn 600 1120
2 8 (192.168.15.18,*)-(10.0.10.99,*) * ESP tunn 1600 3140
```

В выводе присутствует следующая информация:

- `ISAKMP sessions` – количество незавершенных IKE-обменов:
  - `ni initiated` - в качестве инициатора
  - `nr responded` – в качестве ответчика.
- `ISAKMP connections` – информация обо всех ISAKMP SA и для каждого соединения:
  - `Num` – порядковый номер ISAKMP соединения
  - `Conn-id` – уникальный идентификатор ISAKMP соединения
  - `Remote Addr,Port` – адрес и порт партнера, если порт любой - *

- `Local Addr,Port` – локальный адрес и порт, если порт любой - *
- `State` - состояние SA:
  - `incomplete` – недостроенное соединение
  - `active` – активное соединение
  - `configuration` – для данного SA проводится дополнительная настройка `(IKECFG, XAuth, etc.)`
  - `deleted` – SA не используется, подготовлен к удалению
  - `unknown` – статус соединения неизвестен
- `Sent` - количество переданной информации (в байтах)
- `Rcvd` - количество принятой информации (в байтах)

- `IPsec connections` – информация обо всех IPsec SA и для каждого соединения:
  - `Num` – порядковый номер IPsec соединения
  - `Conn-id` – уникальный идентификатор IPsec соединения
  - `Remote Addr,Port` – адрес и порт партнера, если порт любой - *
  - `Local Addr,Port` – локальный адрес и порт, если порт любой - *
  - `Protocol` – сетевой протокол, если протокол любой - *
  - `Action` – действие – {`AH+ESP|AH|ESP`}
  - Type – тип:
    - `tunn` - туннельный режим
    - `trans` - транспортный режим
    - `nat-t-tunn` - туннельный режим через NAT
    - `nat-t-trans` - транспортный режим через NAT
  - `Sent` - количество переданной информации (в байтах)
  - `Rcvd` - количество принятой информации (в байтах)

sa_show –ipsec –i 8

Данная команда выводит информацию о соединении с заданными свойствами.

IPsec connections:

```
Num Conn-id (Remote Addr,Port)-(Local Addr,Port) Protocol Action
Type Sent Rcvd
1 8 (192.168.15.18,*)-(10.0.10.99,*) * ESP tunn 1600 3140
```

sa_show -detail

Команда с опцией `detail` выводит полную информацию обо всех соединениях.

```
ISAKMP sessions: 0 initiated, 0 responded

ISAKMP connection id: 2
    cookies: 613E427395946DFE.DE99B25554306A75
    local  peer (addr/port): 10.0.10.99/500
    remote peer (addr/port): 10.0.10.16/500

    local identity (IPV4_ADDR): 10.0.10.99
```

```
    remote identity (IPV4_ADDR): 10.0.10.16
    IKERule name: ike_rule_without_ikecfg
    auth: preshared key
    mode: main

    sa:
     transform: gost2814789cp-cbc gostr341194cp
     Oakley group: 5
     sa limits: key lifetime (qm/k/sec): -/200/28800
     sa timing: remaining key lifetime (qm/k/sec): -/198/26622
     status: active


IPsec connection id: 6
    local  ident (addr/prot/port): 10.0.10.99/0/0
    remote ident (addr/prot/port): 192.168.15.16/0/0

    #pkts sent/rcvd: 32/6777
    #send/recv errors: 2/0

    local crypto endpt.: 10.0.10.99, remote crypto endpt.:
10.0.10.16
    connection status: {initiated locally, }

    remote identity (IPV4_ADDR): 10.0.10.16
    IPsecAction name: IPsec_action_01
    FilteringRule name: filter rule 00 00
    PFS: none

    inbound esp sa:
     spi: 0x94857A70(2491775600)
      transform: esp-gost2814789cp-cbc esp-gostr341194cp-hmac
      in use settings ={Tunnel, }
      sa limits: key lifetime (k/sec): 4608000/3600
      sa timing: remaining key lifetime (k/sec): 4607998/1426

    inbound ah sa:
     spi: 0x6CD88232(1826128434)
      transform: ah-gostr341194cp-hmac
      in use settings ={Tunnel, }
      sa limiting: key lifetime (k/sec): 4608000/3600
      sa timing: remaining key lifetime (k/sec): 4607999/1426

    outbound esp sa:
     spi: 0xF40CDEE0(4094484192)
      transform: esp-gost2814789cp-cbc esp-gostr341194cp-hmac
      in use settings ={Tunnel, }
      sa limits: key lifetime (k/sec): 4608000/3600
      sa timing: remaining key lifetime (k/sec): 4607999/1426

    outbound ah sa:
     spi: 0xFBE599CD(4226128333)
      transform: ah-gostr341194cp-hmac
      in use settings ={Tunnel, }
      sa limiting: key lifetime (k/sec): 4608000/3600
      sa timing: remaining key lifetime (k/sec): 4607998/1426
```

В выводе присутствует следующая информация:

- `ISAKMP sessions` – количество незавершенных IKE-обменов:
  - `ni initiated` - в качестве инициатора
  - `nr responded` – в качестве ответчика.

- `ISAKMP connection` – в выводе будет присутствовать:
  - поле `IKECFG address`, если был получен IKECFG адрес:

```
ISAKMP connection id: 1
    cookies: F86F80B571D2240F.A0455C78E9DE66C
    local  peer (addr/port): 10.0.10.193/500
    remote peer (addr/port): 10.0.10.178/500
    IKECFG address: 192.168.15.193
```

  - поле `Status` может принимать следующие значения:
    - `incomplete` – недостроенное соединение
    - `active` – активное соединение
    - `configuration` – для данного SA проводится дополнительная настройка `(IKECFG, XAuth, etc.)`
    - `deleted` – SA не используется, подготовлен к удалению
    - `unknown` – статус соединения неизвестен
- `IPsec connection:`
  - поле connection s`tatus` может принимать значения:
    - `initiated locally` - локальный хост выступает инициатором
    - `initiated remotely` - локальный хост выступает ответчиком
    - `rekeyed` – произведено досрочное пересоздание соединения
    - `no rekeying` - досрочное пересоздание соединения в качестве инициатора запрещено
  - поле `in use settings` может принимать значения:
    - `Tunnel` - туннельный режим
    - `Transport` - транспортный режим
    - `Tunnel NAT-T` - туннельный режим через NAT
    - `Transport-NAT-T` - транспортный режим через NAT

13.13. klogview

Утилита `klogview` предназначена для просмотра сообщений, выдаваемых системой протоколирования IPsec-драйвера.

Синтаксис **`klogview`** `[-ltT] [-p ts_precision][-m event_mask] [-f event_mask]`

`-l` ожидать сообщения из ядра и выводить их по мере поступления. Эта опция принимается по-умолчанию, если не задана опция `-m`.

`-t` печатать дату и время вывода сообщения

`-T` печатать относительное время, когда произошло событие. Время выводится в секундах относительно предыдущего события, показанного данным экземпляром утилиты. Например, значение `10.353245 – это 10 секунд и 353245 микросекунд`. Максимальная точность – наносекунды, но реальная погрешность зависит от аппаратной плаформы и операционной системы. Значение, выдаваемое с первым сообщением, отображает абсолютное значение часов, которое используется для вычисления относительного времени. Абсолютное значение - это либо время со старта системы, либо время относительно какой-то даты, принятой в данной системе за точку отсчета.

`-p ts_precision` количество знаков долей секунд, используемых при печати относительного времени события (-T).

`-f event_mask` задать фильтр событий для данного экземпляра утилиты. Возможные события описаны в таблице.

`-m event_mask` задать фильтр событий по-умолчанию. Заданное значение используется, если не указана опция `-f`.

`-h` вывести краткую информацию об использовании утилиты.

В настоящий момент утилита может выводить сообщения, относящиеся к одной или нескольким группам событий. События, по которым выводятся сообщения, сгруппированы следующим образом:

Таблица 4

Группа событий	Код	Описание
drop	2	Уничтожение пакета. Выводится непосредственно перед уничтожением какого-либо пакета. Сообщение содержит краткий текст, поясняющий причину уничтожения и информацию из IP-заголовка пакета. В некоторых случаях IP-заголовок может быть испорчен к моменту вывода сообщения, тогда в сообщении допускаются нулевые или любые другие случайные адреса.
pass	1	Пропуск пакета. Выводится непосредственно перед отсылкой какого-либо пакета. Сообщение содержит краткий текст, поясняющий действия, которые были произведены над пакетом.
sa_minor	8	Некоторые внутренние события, происходящие с IPsec - контекстом. Сообщения содержат номер контекста (ID), который можно увидеть из сообщения о загрузке

Группа событий	Код	Описание
		контекста.
sa_major	4	Взаимодействия между IPsec-драйвером и приложением, касающиеся изменения состояния IPsec-контекстов. Сообщения содержат номер контекста (ID), который можно увидеть из сообщения о загрузке контекста.
sa_trace	16	Сообщения выводятся перед попыткой применения к пакету IPsec-контекста.
sa_errors	32	Ошибки, связанные с неуспешным применением IPsec-контекста к пакету.
filt_trace	64	Выводится имя и индекс правила фильтрации, если такое для пакета найдено.

Нужный набор событий (`event_mask`) можно указать двумя способами:

сложением кодов групп событий (см. в таблице)

Пример:

```
klogview –f 0x43 или klogview –f 67
```

перечислением названий групп событий через запятую, без пробелов между запятой и названием группы

Пример:

```
klogview –f drop,pass,filt_trace
```

Значение по умолчанию Значение по умолчанию отсутствует.

Рекомендации по использованию Используйте данную команду для просмотра сообщений, выдаваемых системой протоколирования.

Сообщения, выводимые утилитой

Сообщения, выводимые утилитой, формируются на основе данных, присылаемых из IPsec-драйвера. Структура большинства сообщений определяется строкой формата[1], получаемой из IPsec-драйвера (см. Примеры сообщений).

Специальные сообщения, выводимые утилитой:

`*** N messages lost ***`	выводится, если утилита не успевает обрабатывать сообщения и N сообщений поретяны.
`no format string`	в сообщении отсутствует строка формата[2].
`<error: .в выводимом сообщении`	несоответствие строки формата параметрам сообщения[3].

Приведем список сообщений, которые выводятся системой протоколирования IPsec-драйвера для разных групп событий.

[1] Строка формата по смыслу и стилю похожа на форматную строку в printf.

[2] Это не является нормальной ситуацией, просьба сообщать разработчикам о подобных проявлениях.

[3] Это не является нормальной ситуацией, просьба сообщать разработчикам о подобных проявлениях.

13.13.1. События группы pass и drop

Сообщения для этой группы выводятся непосредственно перед уничтожением или отправкой пакета.

Формат сообщения (в порядке следования):

- входящий или выходящий пакет
- IP-адрес источника
- порт источника
- IP-адрес получателя
- порт получателя
- номер IP-протокола
- логическое имя интерфейса или код интерфейса, если имя неизвестно
- действие "passed" или "dropped"
- строка, описывающая причину уничтожения или отправки пакета.

По возможности выводится дополнительная информация, например, имя правила фильтрации и идентификатор SA.

Примеры сообщений группы pass

Пакет обработан по правилу фильтрации с действием PASS:

```
in packet 2.3.4.5:12->3.4.3.3:14, proto 6, if eth0, passed:
filter flt_abc: filtered
```

Пакет был обработан по IPsec-правилу:

```
in packet 2.3.4.5:12->3.4.3.3:14, proto 6, if eth0, passed:
filter flt_cba: decapsulated
```

```
out packet 2.3.4.5:12->3.4.3.3:14, proto 6, if eth0, passed:
packet encapsulated
```

Открытый пакет был пропущен по правилу с действием IPsec+PASS:

```
in packet 2.3.4.5:12->3.4.3.3:14, proto 6, if eth0, passed:
filter flt_cba: IPsec rule, but the packet was not
decapsulated
```

Пакет был пропущен в открытом виде по правилу с действием IPsec+PASS:

```
out packet 2.3.4.5:12->3.4.3.3:14, proto 6, if eth0, passed:
filter flt_abc: bundle not found
```

Примеры сообщений группы drop

Сообщения, связанные с некорректными данными заголовков пакета:

IP-заголовок испорчен:

```
in packet 2.3.4.5:12->3.4.3.3:14, proto 6, if eth0, dropped:
corrupted headers
```

TCP/UDP заголовок испорчен:

```
in packet 2.3.4.5:12->3.4.3.3:14, proto 6, if eth0, dropped:
corrupted protocol headers
```


Следующее сообщение аналогично "corrupted protocol headers", выводится после сборки (реассемблирования) IP-пакета:

```
in packet 2.3.4.5:12->3.4.3.3:14, proto 6, if eth0, dropped:
can't update selector
```

Испорченные заголовки после раскрытия IPsec, это может быть также связано с использованием неверного ключа для расшифровки при отсутствии проверки целостности:

```
in packet 2.3.4.5:12->3.4.3.3:14, proto 6, if eth0, dropped:
SA 33: can't prase packet headers after decapsulation
```

Испорчен ESP или AH заголовок:

```
in packet 2.3.4.5:12->3.4.3.3:14, proto 6, if eth0, dropped:
unable to fetch SPI
```

Может выводиться при внутренних ошибках работы клиентской стороны IKEcfg:

```
in packet 2.3.4.5:12->3.4.3.3:14, proto 6, if eth0, dropped:
filter flt_aaa: firewall procedure's result
```

Превышено ограничение по количеству вложений IPsec, раскрываемых на одном хосте (допускается не более 16 вложений):

```
in packet 2.3.4.5:12->3.4.3.3:14, proto 6, if eth0, dropped:
too many nested encapsulations
```

Пакет уничтожен в соответствии с `RefuseTCPPeerInit`, выставленном в правиле фильтрации:

```
in packet 2.3.4.5:12->3.4.3.3:14, proto 6, if eth0, dropped:
filter flt_aaa: incoming TCP connections restricted
```

Сообщения о подпадании пакета под правило с действием `DROP`:

```
in packet 2.3.4.5:12->3.4.3.3:14, proto 6, if eth0, dropped:
filter flt_aaa: packet hit a "DROP" rule
```

```
out packet 2.3.4.5:12->3.4.3.3:14, proto 6, if eth0, dropped:
filter flt_aaa: filtered
```

Пакет был закрыт с помощью IPsec, но подпадает под правило `PASS`:

```
in packet 2.3.4.5:12->3.4.3.3:14, proto 6, if eth0, dropped:
filter flt_aaa: decapsulated packet hit a "PASS" rule
```

Открытый пакет подпадает под правило фильтрации с IPsec-действием:

```
in packet 2.3.4.5:12->3.4.3.3:14, proto 6, if eth0, dropped:
filter flt_aaa: IPsec rule, but the packet was not
decapsulated
```

Правило с действием `IPsec+DROP`, и соответствующий SA bundle не был создан:

```
out packet 2.3.4.5:12->3.4.3.3:14, proto 6, if eth0, dropped:
filter flt_aaa: bundle not found
```

Ошибки IPsec:

```
in packet 2.3.4.5:12->3.4.3.3:14, proto 6, if eth0, dropped:
SA 33: decapsulation error 5: integrity verification failed
```



```
out packet 2.3.4.5:12->3.4.3.3:14, proto 6, if eth0, dropped:
SA 33: encapsulation error 4: sequence number wrapped
```

Возможны следующие ошибки

Код	Название	Описание поблемы
1	replay packet detected	обнаружен повторный пакет
2	call to crypto subsystem failed	ошибка крипто-подсистемы
3	last sequence number	последний номер пакета
4	sequence number wrapped	переполнение счетчика пакетов
5	integrity verification failed	проверка целостности не прошла
6	corrupted protocol headers	испорченный протокольный заголовок
7	corrupted headers after decapsulation	испорченный протокольный заголовок после декапсуляции
8	memory allocation failed	невозможно выделить память
9	IP ttl expired	счетчик IP ttl истек
10	buffer is too small[4]	буфер слишком мал
11	can't parse IP options	невозможно разобрать опции IP
12	padding check failed	ошибка в заполнителе
13	incorrect SA parameters (from pmod_init_sa)[5]	неправильные параметры SA
14	encapsulation mode (tunnel/transport) doesn't match the SA	режим инкапсуляции (туннельный или транспортный) не соответствует SA
15	traffic limit exceeded[6]	превышено ограничение на количество обработанного трафика

Промежуточное состояние при IPsec-rekeying (процесс rekeying (смена ключевого материала) не успел завершиться вовремя):

```
out packet 2.3.4.5:12->3.4.3.3:14, proto 6, if eth0, dropped:
filter flt_aaa: bundle is unusable
```

Ограничение на обработку транзитноготрафика (Server, Client):

```
in packet 2.3.4.5:12->3.4.3.3:14, proto 6, if eth0, dropped:
decapsulated packet is not local (not a security gateway)
```

[4] Это является внутренней ошибкой, просьба сообщать разработчикам.

[5] Это является внутренней ошибкой, просьба сообщать разработчикам.

[6] SA удалится, и потом должна произойти смена ключей.

Ограничение на обработку транзитноготрафика при вложенном IPsec:

```
in packet 2.3.4.5:12->3.4.3.3:14, proto 6, if eth0, dropped:
decapsulated IPsec packet is not local (not a security
gateway)
```

Очередь пакетов, ожидающая создания IPsec SA bundle переполнена:

```
out packet 2.3.4.5:12->3.4.3.3:14, proto 6, if eth0, dropped:
filter flt_aaa: waiting for a bundle: queue overflow
```

Следующее сообщение говорит о слишком большом количестве пакетов на обработку одним SA (более 40). Скорее всего, это означает неоптимальные настройки Продукта с точки зрения производительности. Просьба обращаться к разработчикам:

```
in packet 2.3.4.5:12->3.4.3.3:14, proto 6, if eth0, dropped:
SA 33: queue overflow
```

Внутренние ошибки, о которых просьба сообщать разработчикам:

```
in packet 2.3.4.5:12->3.4.3.3:14, proto 6, if eth0, dropped:
ip data is not 4-byte aligned
```

Другие сообщения:

```
in packet 2.3.4.5:12->3.4.3.3:14, proto 6, if eth0, dropped:
no matching filtering rule
```

```
in packet 2.3.4.5:12->3.4.3.3:14, proto 6, if eth0, dropped:
SA 33: decapsulated packet's IP header doesn't match the SA
```

```
out packet 2.3.4.5:12->3.4.3.3:14, proto 6, if eth0, dropped:
out of memory
```

```
in packet 2.3.4.5:12->3.4.3.3:14, proto 6, if eth0, dropped:
SA not found
```

13.13.2. События группы filt_trace

Сообщения этой группы позволяют определить, какое правило фильтрации используется для обработки пакета. Эти сообщения не содержат информацию о самом пакете. Такую информацию можно получить из контекста сообщения (например, из следующих сообщений группы `pass и drop`).

Пример сообщения:

```
found filtering rule 102(filter_tcp)
```

13.13.3. События группы sa_minor, sa_major

Сообщения этой группы позволяют контролировать процессы создания, уничтожения и замены IPsec-контекстов. Сообщения о загрузке контекстов содержат детальную информацию о параметрах контекста, включая IP-параметры (адреса, порты), SPI, режимы и др.

Если сообщение содержит IP-параметры (selector), то они выводятся в следующем порядке:

- локальный адрес/диапазон адресов
- локальный порт
- удаленный адрес/диапазон адресов
- удаленный порт
- IP- протокол.

Под локальным адресом понимается адрес источника (source) для исходящих пакетов.

Примеры сообщений группы sa_major

Превышено ограничение SA по трафику:

```
SA 55 expired
```

Пора начинать rekeying SA (пройден барьер по трафику):

```
requesting rekeying for SA 33
```

SA нигде не используются и должны быть удалены:

```
requesting to remove SA: 44,45
```

Сообщения о загрузке новых SA:

```
loaded SA: id 12; flags 0x1; ipsec flags: 0x18; selector:
5.4.3.2->2.3.4.5; type: 51; SPI: 0xabababba
```

Следующее сообщение говорит о замене ipsec SA без прерывания обработки трафика:

```
loaded replacement for SA 55: id 12; flags 0x0; ipsec
flags: 0x38; selector: 3.4.5.1->2.3.4.0-2.3.4.255,
proto 17; type: 50; SPI: 0x3b7f44e0
```

Расшифровка type:

```
51 – AH
50 - ESP
```

Расшифровка некоторых[7] битов flags:

0x1 – входящий

Расшифровка битов `ipsec flags`:

```
0x1 – туннельный режим
0x2 – сбрасывать DF-bit
0x4 - устанавливать DF-bit
0x8 – включена защита от replay-атак
0x10 – включена проверка целостности
0x20 – включено шифрование
0x40 – испольуется UDP-encapsulation (NAT traversal)
```

Загрузка связки SA (SA bundle):

[7] Остальные значения флагов не предназначены для интерпретации пользователями.

```
loaded bundle: filter: 298(ipsec_filter); selector:
3.4.5.1:98->3.4.5.2:99, proto 17; SA ids: 4, 5
```

Сообщение о загрузке SA bundle, не содержащее списка SA, означает ошибку создания SA bundle приложением (демоном).

Запрос SA bundle (обычно для его обработки требуется IKE-обмен):

```
bundle request: filter: 59; selector: 5.4.3.2:1->1.2.3.4:5,
proto 17
```

SA заблокирован (превышено ограничение по времени/трафику), ожидается завершение процесса rekeying:

```
disabled SA 33
```

Удаление SA:

```
removed SA 33
```

Удаление ранее заблокированного SA:

```
removed dead SA 33
```

Другие сообщения:

```
application request to enable SA 33 processed
first packet will trigger rekeying of SA 33
```

Сообщения, возникающие при ошибочном/странном[8] поведении Продукта:

```
can't add bundle: filter id 299 not found
can't add bundle: SA id 33 not found
can't add bundle: SA id 33 is unusable
can't load SA: unable to unpack
can't load replacement for SA 33: SA not found
can't load replacement for SA 33: can't unpack
can't load replacement for SA 33: race condition - SA is dead
can't remove SA 33: sa not found
can't disable SA 33: sa not found
can't enable SA 33: sa not found
rekey trigger: can't find SA 33
```

Примеры сообщений группы sa_minor[9]

```
destroyed SA 12
replacing SA 12 with SA 13
can't enable sa 13: it's already enabled
enabled sa 14, but didn't activate it
enabled sa 15
```

[8] Просьба сообщать разработчикам о возникновении одной из перечисленных ошибок.

[9] Сообщения данного раздела предназначены для внутреннего использования. Расшифровка пользователям Продукта не предоставляется.

13.13.4. События группы sa_trace

Сообщения группы `sa_trace` позволяют увидеть факт применения IPsec-контекстов к пакету. Для исходящих пакетов – это инкапсуляция, для входящих – декапсуляция. Сообщения содержат идентификатор SA, который выводится при загрузке SA (должны быть включены сообщения группы `sa_major`). Информация о пакете выводится в том же порядке, что и для сообщений группы `pass и drop`.

Примеры сообщений:

```
decapsulating with SA 10: 1.2.3.4:5->5.4.3.2:1, proto 6, if
iprb0
```

```
encapsulating with SA 10: 5.4.3.2:1->1.2.3.4:5, proto 6, if
iprb0
```

13.13.5. События группы sa_error

Сообщения этой группы выводят дополнительную информацию о специфических ошибках IPsec.

В данный момент есть только одно сообщение – о детектировании replay-атаки. Выводится состояние окна, номер пакета (sequence number).

Пример сообщения:

```
replay packet detected: SA 10 last sequence number 92, window
0x1, packet sequence number 4.
```


13.14. Сообщения об ошибках

Ниже приведены тексты сообщений об ошибках, которые могут возникать при работе с программными утилитами.

Если в тексте полученного сообщения присутствует фраза ” Internal error:”, то обращайтесь в службу поддержки по адресу support@s-terra.com.

Утилита sa_show

Текст сообщения	Описание проблемы
`Internal error. Код ошибки.`	Внутренняя ошибка.
`SA info is not found. Error: ACCESS DENIED.`	Пользователь не аутентифицировался.

Утилита key_show

Текст сообщения	Описание проблемы
`Unable to obtain keys from DB.Error: ACCESS DENIED.`	Не удалось получить Preshared Key из базы.

Утилита lsp_show

Текст сообщения	Описание проблемы
`Failed to retrieve policy from product data base.Error: ACCESS DENIED.` `Other operations are cancelled due to error`	Ошибка при повторной загрузке LSP.

Утилита log_show

Текст сообщения	Описание проблемы
`Failed to get severity level.Error: ACCESS DENIED.`	Ошибка при получении уровня протоколирования событий.

Утилита cert_check

Текст сообщения	Описание проблемы
`Internal error. Unable to obtain certs from DB` `No certificates found.`	Неудачная попытка получить сертификаты из базы продукта.

Утилита dp_show

Текст сообщения	Описание проблемы
`Error %d: VPN demon is not started`	Проблема со стартом демона
`Error %d: Default driver policy is not read from db`	Ошибка при чтении Default Driver Policy из базы продукта
`Error %d: Log-off policy is not read from db`	Ошибка при получении Log-off policy
`<Описания операции>. Error: ACCESS DENIED.`	Пользователь не аутентифицировался.
`Failed to get default driver policy.Error: ACCESS DENIED.`	Ошибка при загрузке DDP.

Утилита pwd_change

Текст сообщения	Описание проблемы
`Error %d: VPN demon is not started`	Проблема со стартом демона
`Error %d: Old password is wrong`	Неверный старый пароль
`Error %d: New password is not set`	Ошибка при установке пароля

Утилита client_logout

Текст сообщения	Описание проблемы
`Error %d: VPN demon is not started`	Проблема со стартом демона
`Error %d: Log-out fail`	Неудачный logout

14. Протоколирование событий

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

14.1. Получение лога в Windows

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

14.2. Список протоколируемых событий

Каждому протоколируемому событию присваивается фиксированный идентификатор (MSG ID) и соответствующий ему уровень важности (Severity) для протокола Syslog:

EMERG, ALERT, CRIT, ERR, WARNING, NOTICE, INFO, DEBUG.

Выдаваемые сообщения и описание событий по этим сообщениям представлены в Таблица 5 – Таблица 9.

Сообщения уровня ERROR

Таблица 5

	Описание события	Уровень важности	Раздел	Шаблоны сообщений
1	Локальный сертификат непригоден	ERR	CERT	Searching local certificate failed. Reason: %s[10]. Subject: %s Issuer: %s SN: %s
2	Секретный ключ локального сертификата недоступен	ERR	CERT	Local certificate '%{1}s' is invalid: private key %{2}s%{3}s'%{4}s' is inaccessible где: %{1}s – значение поля Subject локального сертификата %{2}s – «», если ключ был задан явно, иначе «at container» %{3}s – «», если ключ был задан явно, иначе « » %{4}s – путь к ключу, если он был задан явно, иначе имя контейнера

[10] revoked | expired | not verified

	Описание события	Уровень важности	Раздел	Шаблоны сообщений
3	Контейнер ключа локального сертификата недоступен	ERR	CERT	Local certificate '%{1}s' is invalid: container '%{4}s' is inaccessible где: %{1}s – значение поля Subject локального сертификата %{4}s – путь к ключу, если он был задан явно, иначе имя контейнера
4	Секретный ключ не соответствует локальному сертификату. Это возможно только после установки OCI	ERR	CERT	Local certificate '%{1}s' is invalid: private key %{2}s%{3}s'%{4}s' is inconsistent with the certificate где: %{1}s – значение поля Subject локального сертификата %{2}s – «», если ключ был задан явно, иначе «at container» %{3}s – «», если ключ был задан явно, иначе « » %{4}s – путь к ключу, если он был задан явно, иначе имя контейнера
5	Неуспешная попытка установить соединение в качестве инициатора	ERR	POLICY	Connection request FAILED, Reason: %s[11], ip: %s, protocol: %s[12], IKERule: "%s", IPsecAction: "%s", FilteringRule: “%s”[13], Stopped at: %s[14]
6	Обнаружены некорректные данные в базе данных, связанные с LSP	ERR	POLICY	There is a bad lsp object in product db: '%{1}s', %{1}s – имя некорректного файла описания объекта в базе данных
7	Обнаружена более чем одна активная LSP в базе данных	ERR	POLICY	There are at least two active configurations in product db: '%{1}s' and '%{2}s' %{1}s – имя первого файла описания объекта в базе данных с активной LSP %{2}s – имя второго файла описания объекта в базе данных с активной LSP

[11] Session timeout | Invalid packet | No proposal chosen | Invalid ID | Authentication failed | Process blocked by Local Policy (попытка установить соединение блокируется из-за перезагрузки LSP) | Internal error

[12] ISAKMP либо IPsec

[13] Если на момент вывода сообщения сведения о правилах ISAKMP, IPsec либо о фильтре отсутствуют, то соответствующие сведения не выводятся

[14] Дополнительные сведения об операции, на которой прервался процесс установления соединения

	Описание события	Уровень важности	Раздел	Шаблоны сообщений
8	Ошибка в записи маршрутизации	ERR	SYSTEM	Invalid route to %{1}s%{2}d through %{3}s %{4}s%{5}s%{6}s - %{7}s где: %{1}s%{2}d – destination в виде одиночного IP или подсети %{3}s – gw или interface %{4}s – адрес gateway-я или имя интерфейса %{5}s – “, metric”, если указана метрика в LSP %{6}s – значение метрики %{7}s – описание ошибки: inconsistency, invalid gateway (matches local address)
9	Ошибка при добавлении записи в таблицу маршрутизации	ERR	SYSTEM	Failed to add routing: %{1}s%{2}d through %{3}s %{4}s%{5}s%{6}s - %{7}s где: %{1}s%{2}d – destination в виде одиночного IP или подсети %{3}s – gw или interface %{4}s – адрес gateway-я или имя интерфейса %{5}s – “, metric”, если указана метрика в LSP %{6}s – значение метрики %{7}s – описание ошибки: inconsistency, invalid gateway (matches local address) На уровне ERROR параметр %{7}s может принимать следующие значения: system error, unknown network interface, internal error. На уровне WARNING параметр %{7}s может принимать следующие значения: already exists.

	Описание события	Уровень важности	Раздел	Шаблоны сообщений
10	Ошибка при удалении записи из таблицы маршрутизации	ERR	SYSTEM	Failed to delete routing: %{1}s%{2}d through %{3}s %{4}s%{5}s%{6}s - %{7}s где: %{1}s%{2}d – destination в виде одиночного IP или подсети %{3}s – gw или interface %{4}s – адрес gateway-я или имя интерфейса %{5}s – “, metric”, если указана метрика в LSP %{6}s – значение метрики %{7}s – описание ошибки: inconsistency, invalid gateway (matches local address) На уровне ERROR параметр %{7}s может принимать следующие значения: system error, internal error. На уровне WARNING параметр %{7}s может принимать следующие значения: not found.

Сообщения уровня WARNING

Таблица 6

	Описание события	Уровень важности	Раздел	Шаблоны сообщений
1	В файле x509conv.ini указана неподдерживаемая кодировка	WARNING	CERT	Unsupported encoding "%{1}s" has been specified in x509conv.ini, "%{2}s" will be used %{1}s – неподдерживаемая кодировка %{2}s – кодировка, которая будет использована для соответствующего ASN.1-типа
2	В файле x509conv.ini указан неизвестный параметр	WARNING	CERT	Unexpected parameter "%{1}s" has been specified in x509conv.ini, ignored %{1}s – имя неизвестного параметра
3	Ошибка при перекодировке полей Issuer или Subject сертификата в UTF-8	WARNING	CERT	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. %{1}s – строковое представление поля Subject сертификата

	Описание события	Уровень важности	Раздел	Шаблоны сообщений
4	LDAP запрос {1} закончился неудачей. Причина: {2}	WARNING	LDAP	LDAP request failed. Reason: %{2}s[15]. Query[16]: "%{1}s".
5	Неуспешная попытка установить соединение в качестве ответчика	WARNING	POLICY	Incoming connection request FAILED, Reason: %s[17], ip: %s, protocol: %s[18], IKERule: "%s", IPsecAction: "%s"[19], FilteringRule: "%s"[20], Stopped at: %s[21]
6	Значение параметра DefaultCryptoContextsPerIPSecSA задано неверно	WARNING	POLICY	DefaultCryptoContextsPerIPSecSA in "agent.ini" is not valid (must be from 1 to 128), %{1}d will be used instead. %{1}d – значение, которое будет использовано для параметра DefaultCryptoContextsPerIPSecSA
7	В правиле IKERule задано несколько трансформов с различными группами. Если в качестве инициатора Агент будет использовать Aggressive Mode, то в этом случае будут высылаться только трансформы с такой же группой как у первого трансформа в правиле.	WARNING	POLICY	WARNING: IKERule '%{2}s', line %{3}d: in Aggressive Mode initiator will use %{1}s only. %{1}s – название выбранной группы, по которой будет работать Агент в качестве инициатора в Aggressive Mode. %{2}s – имя IKERule, для которого выведена эта диагностика %{3}d – строка, на которой располагается IKERule.

[15] Create request failed – Не удалось сформировать корректный запрос

Failed to parse message – Ошибка разбора сообщения LDAP

Timeout

LDAP server is not responding – LDAP сервер недоступен

Request canceled – Запрос прерван (например при выгрузке конфигурации)

Unknown – Причина неизвестна

[16] Здесь и далее Query показывается в виде URL. По возможности пишется адрес LDAP-сервера (как правило во всех случаях, кроме “LDAP request ignored…”). Данный Query может отличаться от URL, указанного в сообщении о формировании LDAP-запроса (случай “CRL by URL”), если исходный URL не содержал адреса LDAP-сервера.

[17] Session timeout | Limit of %u responded sessions achieved | Invalid packet | No proposal chosen | No rule chosen | Invalid ID | Authentication failed | Internal error

[18] ISAKMP либо IPsec

[19] Если на момент вывода сообщения правило ISAKMP, либо IPsec не выбрано, то сведения о нём не выводятся

[20] Если на момент вывода сообщения сведения о правилах ISAKMP, IPsec либо о фильтре отсутствуют, то соответствующие сведения не выводятся

[21] Дополнительные сведения об операции, на которой прервался процесс установления соединения

Сообщения уровня NOTICE

Таблица 7

	Описание события	Уровень важности	Раздел	Шаблоны сообщений
1	Результат LDAP запроса {1} – объекты не найдены	NOTICE	LDAP	LDAP request result: NOT FOUND. Query: "%{1}s".
2	Результат LDAP запроса {1} – найдено {2} объектов	NOTICE	LDAP	LDAP request result: %{2}s object(s) found. Query: "%{1}s".
3	Присвоен IP-адрес из удалённого IKE-CFG пула	NOTICE	POLICY	VPN ip-address %s obtained, Partner: %s:%d[22]
4	Партнёру присвоен IP-адрес из IKE-CFG пула	NOTICE	POLICY	VPN ip-address %s assigned to external host Partner: %s:%d[23]
5	Превышено ограничение на количество инициированных IKE-сессий. Инициированная сессия отложена до завершения любой активной инициированной IKE-сессии.	NOTICE	POLICY	[ISAKMP]: Exchange pended. Limit of %u initiated sessions achieved. Partner: %s:%d[24]
6	Превышено ограничение на количество IKE-сессий, инициированных партнерами. Запрос от партнера игнорируется, новая сессия не создается.	NOTICE	POLICY	[ISAKMP]: Exchange cancelled. Limit of %u responded sessions achieved. Partner: %s:%d[25]
7	Старт сервиса	NOTICE	SYSTEM	Service started, version %s
8	Остановка сервиса	NOTICE	SYSTEM	Service stopped
9	Доступ Пользователя к Агенту	NOTICE	SYSTEM	User logged in
10	Отключение доступа Пользователя к Агенту	NOTICE	SYSTEM	User logged out

[22] ip:port

[23] ip:port

[24] ip:port. Порт партнёра может указываться нулевым в случаях, когда он ещё не определен. Это возможно, поскольку ISAKMP обмен на момент вывода сообщения ещё не начат, а другие источники фактической информации о партнёре могут быть недоступны. Порт партнера в таких случаях определяется после возобновления ISAKMP обмена.

[25] ip:port

Сообщения уровня INFO

Таблица 8

	Описание события	Уровень важности	Раздел	Шаблоны сообщений
1	Установлено соединение	INFO	POLICY	Connection established, %u.%u.%u.%u[-%u.%u.%u.%u][:%u]<->%u.%u.%u.%u[-%u.%u.%u.%u][:%u][, proto %u], FilteringRule: “%s”, IPsecAction: “%s” где: квадратные скобки обозначают, что данная часть сообщения может отсутствовать первый аргумент вида “%u.%u.%u.%u[-%u.%u.%u.%u][:%u]” – IP-адрес или диапазон IP-адресов и порт, которые защищаются Агентом второй аргумент вида “%u.%u.%u.%u[-%u.%u.%u.%u][:%u]” –IP-адрес или диапазон IP-адресов и порт, которые защищаются партнером [, proto %u] – защищаемый протокол FilteringRule: “%s” – фильтр, на который загружена созданная цепочка IPsec SA-ев IPsecAction: “%s” – правило IPsecAction по которому создалось соединение
2	Получен ISAKMP-пакет от партнера, с которым запрещен IKE-трафик[26]	INFO	POLICY	Inbound IKE packet dropped, Reason: Access denied, Partner: %s:%d[27]

[26] Партнер (идентифицируется по паре ip:port) может быть помещен в «черный список», если с ним нет ни одного ISAKMP соединения, и за определенный промежуток времени он неуспешно пытался установить ISAKMP соединение достаточно большое количество раз. При получении нового IKE-пакета от такого партнера любая обработка IKE-пакетов игнорируется, поэтому невозможно определить намерение партнера: это может быть новая попытка установления ISAKMP соединения, продолжение старых попыток, информационное сообщение, либо просто пакет неправильного формата. Обмен с таким партнером разрешается спустя установленный промежуток времени, либо при инициировании соединения со стороны локального устройства.

[27] ip:port

	Описание события	Уровень важности	Раздел	Шаблоны сообщений
3	Закрытие соединения	INFO	POLICY	Connection closed, %u.%u.%u.%u[-%u.%u.%u.%u][:%u]<->%u.%u.%u.%u[-%u.%u.%u.%u][:%u][, proto %u], bytes sent/received: %d / %d, Reason: %s где: квадратные скобки обозначают, что данная часть сообщения может отсутствовать первый аргумент вида “%u.%u.%u.%u[-%u.%u.%u.%u][:%u]” – IP-адрес или диапазон IP-адресов и порт, которые защищаются Агентом второй аргумент вида “%u.%u.%u.%u[-%u.%u.%u.%u][:%u]” –IP-адрес или диапазон IP-адресов и порт, которые защищаются партнером [, proto %u] – защищаемый протокол bytes sent/received: %d / %d – количество байт, который были отосланы и приняты под защитой этого соединения Reason: %s – причина удаления соединения, возможны следующие варианты: Loading new configuration – соединение уничтожено по причине загрузки новой конфигурации Delete payload received – от партнера пришел запрос на удаление этого соединения Time expired – истек лимит действия соединения по времени Traffic expired – истек лимит действия соединения по трафику Dead peer detected – партнер признан «мертвым» Initial contact – соединение удалено при получении нотификации INITIAL-CONTACT Cannot start DPD (no ISAKMP SA) – нет возможности инициировать DPD, партнер признается «мертвым» и соединение с ним удаляется Replaced with new one – соединение удаляется в связи с тем, что построено новое SA bundle destroyed – возникает в случае использования вложенного IPsec, когда удаляется одна из цепочек IPsec SAs, что приводит к уничтожению всей связки цепочек.

	Описание события	Уровень важности	Раздел	Шаблоны сообщений
4	IPsec-соединение не установилось из-за превышения количества, разрешенного лицензией	INFO	POLICY	Unable to establish connection: resources exceeded
5	Информация о лицензии Продукта	INFO	SYSTEM	Product licence: product code: %s, customer code: %s, license number: %n, license code: %s

Сообщения уровня DEBUG

Таблица 9

	Описание события	Уровень важности	Раздел	Шаблоны сообщений
1	Не найден сертификат партнёра	DEBUG	CERT	Searching peer certificate failed. Reason: not found. Search template: %s
2	Найден непригодный сертификат партнёра	DEBUG	CERT	Searching peer certificate failed. Reason: %s[28]. Subject: %s Issuer: %s SN: %s
3	Выбран сертификат партнёра	DEBUG	CERT	Use peer certificate: Subject: %s Issuer: %s SN: %s
4	Сформирован LDAP запрос {1}	DEBUG	LDAP	LDAP request: "%{1}s[29]". Где %{1}s – 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).
5	LDAP запрос {1} проигнорирован: не задан LDAP сервер	DEBUG	LDAP	LDAP request ignored: there is no LDAP server available. Query: "%{1}s".

[28] revoked | expired | not verified

[29] Во всех сообщениях LDAP запрос описывается в виде URL. В настоящее время если используются IP-адрес и порт, заданные в LSP, они в URL не указываются.

	Описание события	Уровень важности	Раздел	Шаблоны сообщений
6	Запрос на создание соединения	DEBUG	POLICY	Connection request, packet: %u.%u.%u.%u[:%u]-> %u.%u.%u.%u[:%u][, proto %u], FilteringRule: “%s” где: квадратные скобки обозначают, что данная часть сообщения может отсутствовать первый аргумент вида “%u.%u.%u.%u[:%u]” – IP-адрес источника и порт, если он указан в пакете второй аргумент вида “%u.%u.%u.%u[:%u]” - IP-адрес приемника и порт, если он указан в пакете [,proto %u] – номер протокола, если указан в пакете, иначе не пишется FilteringRule “%s” – название фильтра, под который попал пакет
7	Ошибка инициирования создания соединения	DEBUG	POLICY	Failed to initiate connection request processing, packet: %u.%u.%u.%u[:%u]->%u.%u.%u.%u[:%u][, proto %u] где: квадратные скобки обозначают, что данная часть сообщения может отсутствовать первый аргумент вида “%u.%u.%u.%u[:%u]” – IP-адрес источника и порт, если он указан в пакете второй аргумент вида “%u.%u.%u.%u[:%u]” - IP-адрес приемника и порт, если он указан в пакете [,proto %u] – номер протокола, если указан в пакете, иначе не пишется
8	Создание ISAKMP SA	DEBUG	POLICY	ISAKMP connection [%u] established, Partner: %s:%d[30], Identity: %s, IKERule: “%s”
9	Удаление ISAKMP SA	DEBUG	POLICY	ISAKMP connection [%u] closed, Partner: %s:%d[31], Identity: %s, bytes sent/received: %d / %d, Exchanges passed: %d
10	Обнаружение устройства NAT	DEBUG	POLICY	NAT detected on ...[32] side, Partner: %s:%d[33]

[30] ip:port

[31] ip:port

[32] local | remote

[33] ip:port

	Описание события	Уровень важности	Раздел	Шаблоны сообщений
11	Proposals высланы партнёру	DEBUG	POLICY	(Phase I):[34] Sending IKE proposals. Rule “%s”: Auth: %s Transform #1: Hash: %s, Cipher: %s, Group: %s, Life Time: %s, Life Traffic: % Transform #2: .. (Phase II):[35] Sending IPsec proposals. Rule “%s”: Encapsulation mode: %s, Group: %s Proposal #1: Protocol AH: Transform #1: Integrity: %s, Life Time: %s, Life Traffic: %s Transform #2: ..... Protocol ESP: Transform #1: Integrity: %s, Cipher: %s, Life Time: %s, Life Traffic: %s Transform #2: Proposal #2:
12	Партнёр прислал набор proposals	DEBUG	POLICY	(Phase I):[36] IKE proposals received. Transform #1: Auth: %s, Hash: %s, Cipher: %s, Group: %s, Life Time: %s, Life Traffic: % Transform #2: (Phase II):[37] IPsec proposals received. Encapsulation mode: %s, Group: %s Proposal #1: Protocol AH: Transform #1: Integrity: %s, Life Time: %s, Life Traffic: %s Transform #2 Protocol ESP: Transform #1: Integrity: %s, Cipher: %s, Life Time: %s, Life Traffic: %s Transform #2: Proposal #2
13	Проверка proposal для правила	DEBUG	POLICY	Check proposal #%u, Protocol %s[38], Transform #%u for Rule “%s”. Result: %s[39], attribute: %s[40]

[34] Если отдельные структуры, либо атрибуты отсутствуют, то они не протоколируются

[35] Если отдельные структуры, либо атрибуты отсутствуют, то они не протоколируются

[36] Если отдельные структуры, либо атрибуты отсутствуют, то они не протоколируются

[37] Если отдельные структуры, либо атрибуты отсутствуют, то они не протоколируются

	Описание события	Уровень важности	Раздел	Шаблоны сообщений
14	Выбран proposal	DEBUG	POLICY	(Phase I): [41] ISAKMP proposal selected. Auth: %s, Hash: %s, Cipher: %s, Group: %s, Life Time: %s, Life Traffic: %s (Phase II):[42] IPsec proposal selected. Mode: %s[43], Group: %s, AH Integrity: %s, ESP Integrity: %s, Cipher: %s, Life Time: %s, Life Traffic: %s
15	Выбран Preshared ключ	DEBUG	POLICY	Using preshared key "%{1}s" for partner %{2}s:%{3}d, где: %{1}s – Идентификатор выбранного ключа, указанный в LSP %{2}s:%{3}d - IP-адрес и порт партнера по IKE-обмену
16	Недоступен выбранный Preshared ключ	DEBUG	POLICY	Preshared key "%{1}s" not found, где: %{1}s – Идентификатор выбранного ключа, указанный в LSP
17	Присланный идентификатор партнера по IKE-обмену не подошел ни под одно правило ISAKMP. Предпринимается попытка идентифицировать партнера по его IP-адресу.	DEBUG	POLICY	WARNING: Unable to proceed IKE remote ID for partner %{2}s:%{3}d. Using ip-address from IKE packet instead, где: %{2}s:%{3}d - IP-адрес и порт партнера по IKE-обмену
18	Не удалось подобрать правило аутентификации для данного партнера по IKE-обмену	DEBUG	POLICY	Unable to choose authentication rule for partner %{2}s:%{3}d, где: %{2}s:%{3}d - IP-адрес и порт партнера по IKE-обмену
19	Информация об используемом локальном IKE-Identity	DEBUG	POLICY	[ISAKMP]: Sending identity "%s" to partner <ip:port>
20	Информация об IKE-Identity, присланным партнером	DEBUG	POLICY	[ISAKMP]: Identity "%s" is received from partner <ip:port>

[38] ISAKMP | AH | ESP

[39] Not matched | OK

[40] Authentication method | Hash | Cipher | Oakley group | Integrity | mode – только для не совпавших proposals

[41] Если отдельные структуры, либо атрибуты отсутствуют, то они не протоколируются

[42] Если отдельные структуры, либо атрибуты отсутствуют, то они не протоколируются

[43] Transport | Tunnel

	Описание события	Уровень важности	Раздел	Шаблоны сообщений
21	Информация о сообщении (IKE-Notification), присланным партнером	DEBUG	POLICY	[ISAKMP]: Notification [%s[44]] has been received for Exchange <%u[45]>: %s[46]
22	Инициированный IKE-обмен завершился с ошибкой	DEBUG	POLICY	[ISAKMP]: Connection request FAILED. %s где: %s – дополнительная доступная информация о несостоявшемся обмене: причина аварийного завершения [47] (см. Таблица 10) стек выполняемых операций (см.Таблица 11) сведения о партнере: <ip:port>, IKE-Identity [48]
23	IKE-обмен, инициированный партнером, завершился с ошибкой	DEBUG	POLICY	[ISAKMP]: Incoming connection FAILED. %s где: %s – дополнительная доступная информация о несостоявшемся обмене: причина аварийного завершения [49] (см.Таблица 10) стек выполняемых операций (см.Таблица 11) сведения о партнере: <ip:port>, IKE-Identity[50]

[44] Согласно списку п. 3.14.1 в RFC 2408 и п. 4.6.3 в RFC 2407.

[45] Номер-идентификатор IKE-обмена.

[46] Реакция Агента на присланное сообщение: Ignore | Ignore unprotected Notification | Cancel target connection | Correct TTL for target connection | Start IPsec traffic | Target connection is already disabled | Peer is alive | Wrong sequence: Ignore | Peer is interested in my liveness: send acknowledgement | Clear all old connections

[47] Если к моменту завершения партнерам удалось договориться о применении метода аутентификации на Preshared-ключах, и в списке операций присутствует «*Unable to decode packet*», то, наряду с ошибкой собственно расшифрования, либо IKE-пакета, неправильно сформированного партнером, причиной отказа в соединении может быть применение неправильного ключа.

[48] *IKE Identity* указывается только в случаях, когда в пределах данного IKE-обмена такая информация доступна.

[49] Если к моменту завершения партнерам удалось договориться о применении метода аутентификации на Preshared-ключах, и в списке операций присутствует «Unable to decode packet», то, наряду с ошибкой собственно расшифрования, либо IKE-пакета, неправильно сформированного партнером, причиной отказа в соединении может быть применение неправильного ключа.

[50] *IKE Identity* указывается только в случаях, когда в пределах данного IKE-обмена такая информация доступна.

	Описание события	Уровень важности	Раздел	Шаблоны сообщений
24	Пересечение соединений по адресам от разных партнеров на одном фильтре	DEBUG	POLICY	Connection to %{1}s:%{2}d conflicts with connection to %{3}s:%{4}d, conflicting address range: %{5}s %{1}s:%{2}d – IP-адрес и порт партнера, который блокирует соединение к партнеру %{3}s:%{4}d в адресном пространстве %{5}s

14.2.1. Список ошибок протокола ISAKMP

(см. пункты 22 и 23 Таблица 9)

Таблица 10

	Описание ошибки	Запись об ошибке в строке сообщения
1	Не удалось сформировать подпись	Unable to Form Signature
2	От партнера пришло сообщение неверного типа вместо ожидаемого сообщения CONNECTED (свидетельствующего о готовности IPsec-соединения на стороне партнера)	Unexpected Notification type: need CONNECTED
3	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)
4	От партнера пришла команда дополнительной настройки ISAKMP-соединения (XAuth, IKE-CFG, и т.п.), не соответствующая протоколу обмена для данного этапа	Unexpected configuration message type
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 обнаружен локальный сертификат	Local Certificate is not present
10	Не обнаружен сертификат партнера	Remote Certificate is not present
11	Не найден сертификат	Certificate not found
12	Нет доступа к публичному ключу сертификата	Cert Public Key is inaccessible
13	Не найден один из необходимых компонентов пакета	Can't find proposal
14	Потеряны данные с ключевой информацией	Encryption container missed

	Описание ошибки	Запись об ошибке в строке сообщения
15	Партнер вернул неправильную идентификационную информацию ответчика IKE-обмена при создании IPsec-соединения	Bad IDcr returned
16	Потеряны данные входящего пакета	IN packet missed
17	Партнер вернул неправильную идентификационную информацию инициатора IKE-обмена при создании IPsec-соединения	Bad IDci returned
18	Партнер прислал IKE-пакет с неправильной структурой, либо пакет не удалось правильно расшифровать.	Invalid packet (invalid structure).

14.2.2. Список выполняемых действий по протоколу ISAKMP

(см. пункты 22 и 23 Таблица 9)

Таблица 11

	Описание дествия	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	Формирование подписи	Encrypt 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

	Описание дествия	Информация в строке сообщения
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
20	Вычисление общего ключа	Calculate Shared Key
21	Вычисление инициализационного вектора	Calculate InitVector
22	Определение метода аутентификации	Detect Authentification Method
23	Проверка локального сертификата для метода аутентификации с использованием сертификатов	Authentification uses Certificates: Check for 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

	Описание дествия	Информация в строке сообщения
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 дополнительной настройки ISAKMP-соединения (XAuth, IKE-CFG, и т.п.)	Determine IKE configuration method
38	Распознавание команды дополнительной настройки ISAKMP-соединения (XAuth, IKE-CFG, и т.п.)	Determine ike-cfg message type
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[51]
42	Проверка структуры компонента IKE-пакета	Analyse payload structure %s[52]

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

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

	Описание дествия	Информация в строке сообщения
43	Формирование компонента IKE-пакета	Form payload %s[53]
44	Заполнение блока данных указанного компонента IKE-пакета	Fill payload %s[54]
45	Проверка содержимого компонента IKE-пакета	Check %s[55]
46	Вычисление хэша – содержимого указанного компонента	Calculate %s[56]
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]
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]

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

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

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

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

	Описание дествия	Информация в строке сообщения
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 аутентификации 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]

	Описание дествия	Информация в строке сообщения
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]
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]

	Описание дествия	Информация в строке сообщения
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	Выбор ISAKMP либо IPsec правила	[Choose Rule]
85	Проверка присланного атрибута – компонента пакета IKE	[Check Attr]
86	Проверка присланного сертификата – компонента пакета IKE	[Check Cert]
87	Проверка присланного хэша – компонента пакета IKE	[Check HASH]
88	Проверка присланного идентификатора – компонента пакета IKE	[Check ID]
89	Проверка присланного ключа – компонента пакета IKE	[Check KE]
90	Проверка присланного NAT-детектора – компонента пакета IKE	[Check NAT-D]
91	Проверка присланного NAT Original Address – компонента пакета IKE	[Check NAT-OA]
92	Проверка присланного Nonce – компонента пакета IKE	[Check Nonce]

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

14.3. Ошибки криптографической подсистемы

Список сообщений об ошибках криптографической подсистемы, работающей в ядре ОС, при которых пользователю рекомендуется выполнить какие-либо действия, приведен в Таблица 12. При всех остальных сообщениях – обращайтесь в службу поддержки - support@s-terra.com.

Таблица 12

	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, обратиться в службу поддержки.
2	CP_ReOpen: bad check handle	Если есть проблемы с прохождением трафика, переустановить IPsec соединение, обратиться в службу поддержки.
3	CP_Transform: bad handle 0x%x	Если есть проблемы с прохождением трафика, переустановить IPsec соединение, обратиться в службу поддержки.
4	CPCCreateProvider failed with return code 0x%.8X!	Удалить файл лицензии крипто-провайдера и ввести ее заново. В случае повторения ошибки - обратиться в службу поддержки.
5	%s: Can't get function addresses from CSP	Удалить файл лицензии крипто-провайдера и ввести ее заново. В случае повторения ошибки - обратиться в службу поддержки.
6	CP_Open: can't find alg %s	Удалить файл лицензии крипто-провайдера и ввести ее заново. В случае повторения ошибки - обратиться в службу поддержки.
7	Skipping unused algorithm [%s]	Не ошибка, можно игнорировать.
8	forced close: %u contexts	Не ошибка, можно игнорировать.
9	drvcsp:_info()=OK	Не ошибка, можно игнорировать.
10	drvcsp: loglevel=0x1, logformat=0x39	Не ошибка, можно игнорировать.
11	drvcsp: serial= <...>	Не ошибка, можно игнорировать.

15. Мониторинг

Мониторинг CSP VPN Client осуществляется по протоколу обмена SNMPv1 или SNMPv2c.

Настройка SNMP-агента произведена администратором при подготовке инсталляционного пакета для пользователя.

SNMP-менеджер имеет возможность только запрашивать содержимое базы данных агента. 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. Другие типы сообщений между менеджером и агентом не поддерживаются.

В качестве SNMP-менеджера могут быть использованы:

- программный Продукт CiscoWorks VPN Monitor, который входит в состав комплекта CiscoWorks VMS 2.2.
- 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.

15.1. Выдача статистики

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 13

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 "CSP VPN Gate 3.1.<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): 1.3.6.1.4.1.9.1.467(cisco2611XM из CISCO-PRODUCTS-MIB)	RFC1213-MIB

Название переменной	OID (идентификатор объекта)	Тип переменной	Значение переменной	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 зависимоти 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	335 (c2611XM)	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
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

Название переменной	OID (идентификатор объекта)	Тип переменной	Значение переменной	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$C2600-CSP-VPN$" 3: "CW_FAMILY$C2600$" 4: "CW_FEATURE$IP\|FIREWALL 2 PLUS 3DES$" 5: "CW_VERSION$12.2(13)T5, $" 6: "CW_MEDIA$RAM$" 7: "CW_SYSDESCR$CSP VPN {Gate|Server|Client} <major>.<minor>.<build>$"" 8: "CW_MAGIC$$" 9: "CW_END$-csp-vpn$"	CISCO-IMAGE-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

Название переменной	OID (идентификатор объекта)	Тип переменной	Значение переменной	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
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

Название переменной	OID (идентификатор объекта)	Тип переменной	Значение переменной	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
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

Название переменной	OID (идентификатор объекта)	Тип переменной	Значение переменной	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
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.	CISCO-IPSEC-FLOW-MONITOR-MIB

Название переменной	OID (идентификатор объекта)	Тип переменной	Значение переменной	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
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

Название переменной	OID (идентификатор объекта)	Тип переменной	Значение переменной	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.	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
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

Название переменной	OID (идентификатор объекта)	Тип переменной	Значение переменной	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
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

Название переменной	OID (идентификатор объекта)	Тип переменной	Значение переменной	MIB
Interfaces-статистика				
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, находится в диапазоне между 1 и ifNumber (ifNumber – число сетевых интерфейсов)	RFC1213-MIB
IP - статистика				
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
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.	IP-MIB

Название переменной	OID (идентификатор объекта)	Тип переменной	Значение переменной	MIB
CPU, 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.	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
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

Название переменной	OID (идентификатор объекта)	Тип переменной	Значение переменной	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
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
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

15.2. Трап-сообщения

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

Для этого в конфигурационном файле администратор задает IP-адрес и порт, на который отсылаются сообщения SNMP-менеджеру, идентификатор и IP-адрес отправителя трап-сообщения, версию SNMP, в которой создаются трап-сообщения.

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

Таблица 14

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	1.3.6.1.4.1.9.9.171.7 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	1.3.6.1.4.1.9.9.171.8 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 загрузке 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

16. Приложение

16.1. Установка СКЗИ "КриптоПро CSP 3.6"

При выполнении процедуры инсталляции СКЗИ "КриптоПро CSP 3.6" выбирайте:

вид установки – Выборочная

компоненты, которые необходимо установить:

- Криптопровайдер уровня ядра ОС
- Совместимость с КриптоПро CSP 3.0.

16.2. Настройка СКЗИ "КриптоПро CSP"

В случае использования в Продукте CSP VPN Client аутентификации пользователей на основе 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 (Реестр) на компьютере пользователя.

СКЗИ "КриптоПро CSP" умеет считывать секретный ключ из контейнера как на внешнем ключевом носителе так и на локальном ключевом носителе.

Локальный ключевой носитель

Если контейнер с секретным ключом сертификата пользователя надо разместить в Реестре, то его нужно инсталлировать как считыватель. Такая инсталляция описана в Приложении в разделе “Инсталляция ключевого считывателя Реестр в "КриптоПро CSP 3.6".

Внешний ключевой считыватель и носитель информации

Если контейнер будет расположен на внешнем ключевом носителе, то сначала нужно подключить к компьютеру считыватель ключевой информации, а затем инсталлировать его. Подключение внешних считывателей ключевой информации, например eToken и др., описано в Приложении в разделе "Подключение внешних ключевых считывателей".

После установки "КриптоПро CSP 3.6" сразу же инсталлированы - Все считыватели смарт-карт и Все съемные диски, а остальные считыватели нужно инсталлировать. Для eToken и дисковода инсталляция считывателя уже выполнена.

Для некоторых внешних считывателей еще нужно выполнить Инсталляцию носителей. После установки "КриптоПро CSP 3.6" сразу же инсталлированы несколько типов носителей для eToken, остальные носители информации нужно инсталлировать.

Процедура инсталляции внешних считывателей и носителей описана в разделе “Инсталляция внешнего считывателя и ключевого носителя информации в "КриптоПро CSP 3.6".

16.3. Подключение внешних ключевых считывателей

Подключите внешний ключевой считыватель к компьютеру, следуя прилагаемой инструкции (Не следует подключать eToken до установки драйверов).

Установите все необходимые файлы и драйверы для работы внешнего считывателя, прилагаемые к нему.

В состав дистрибутива СКЗИ "КриптоПро CSP 3.6" не входят драйвера, обеспечивающие взаимодействие внешних ключевых считывателей с "КриптоПро CSP 3.6".

Для этого с Web-страницы http://www.cryptopro.ru/cryptopro/products/csp/readers.htm компании Крипто-ПРО загрузите и установите модуль поддержки внешнего считывателя для СКЗИ "КриптоПро CSP".

16.4. Инсталляция ключевого считывателя Реестр в "КриптоПро CSP 3.6"

Для инсталляции локального ключевого считывателя Реестр надо выполнить следующие действия:

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

Шаг 2: в появившемся окне Свойства войдите во вкладку Оборудование и нажмите кнопку Настроить считыватели...:

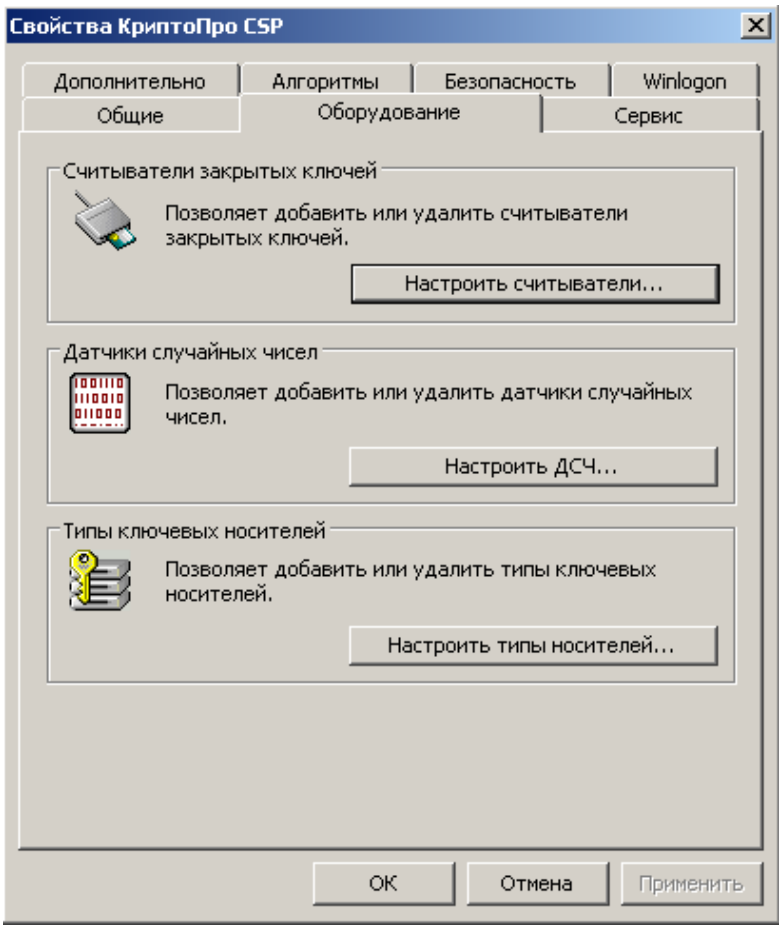

Рисунок 66

Шаг 3: нажмите кнопку Добавить..., чтобы добавить новый ключевой считыватель:

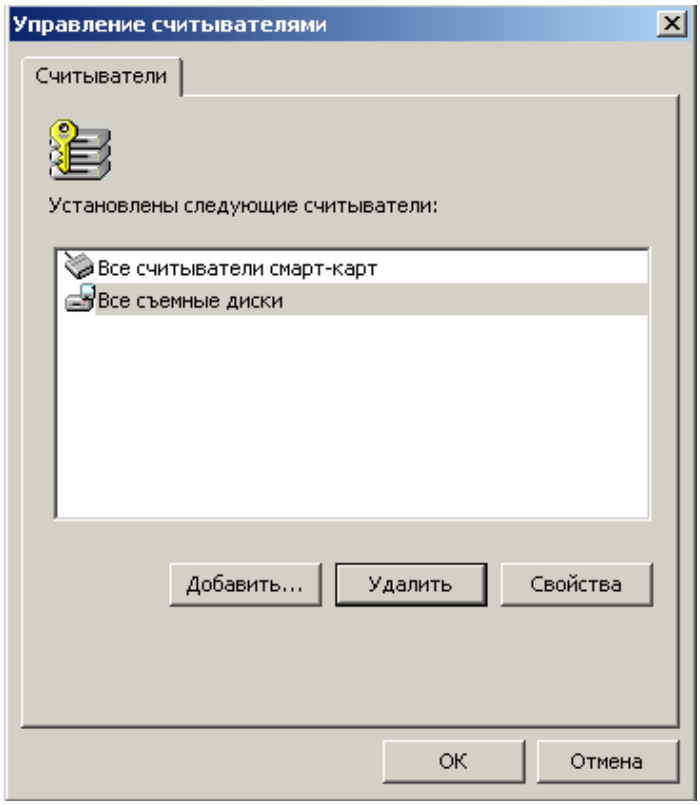

Рисунок 67

Шаг 4: в окне визарда нажмите кнопку Далее:

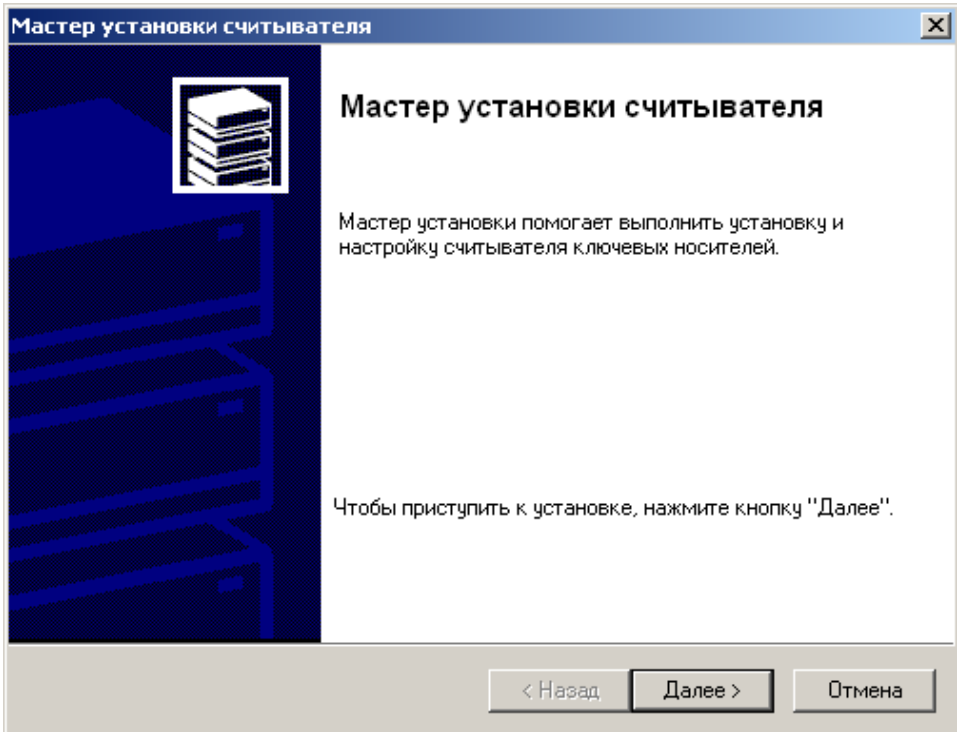

Рисунок 68

Шаг 5: из представленного списка выберите считыватель "Реестр" и нажмите кнопку Далее:

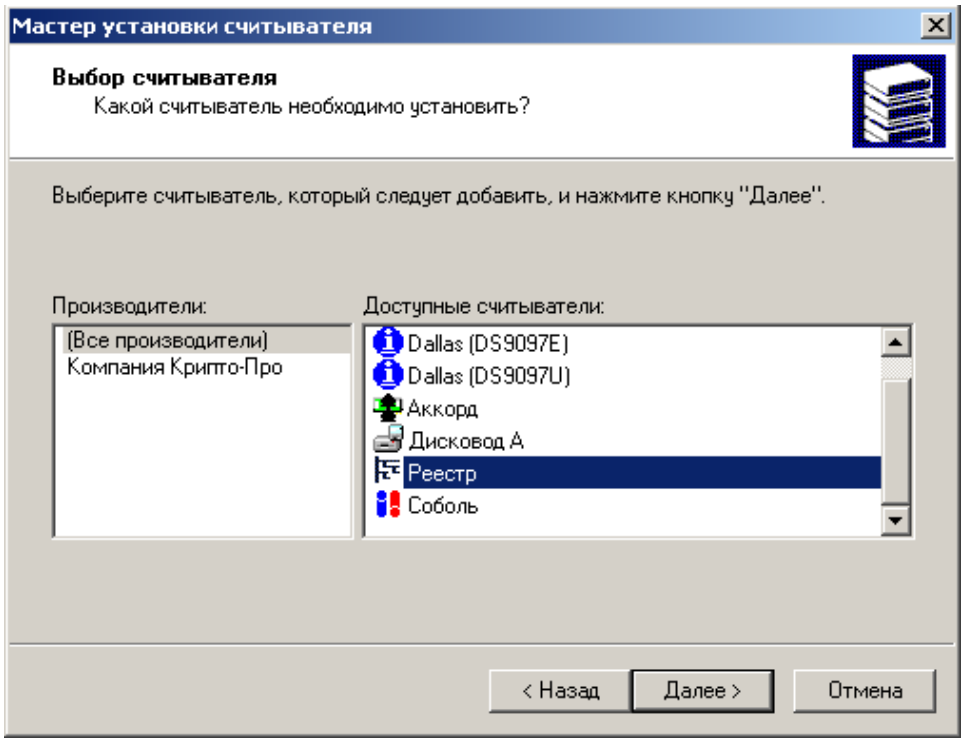

Рисунок 69

Шаг 6: считывателю Реестр можно присвоить имя и нажать кнопку Далее:

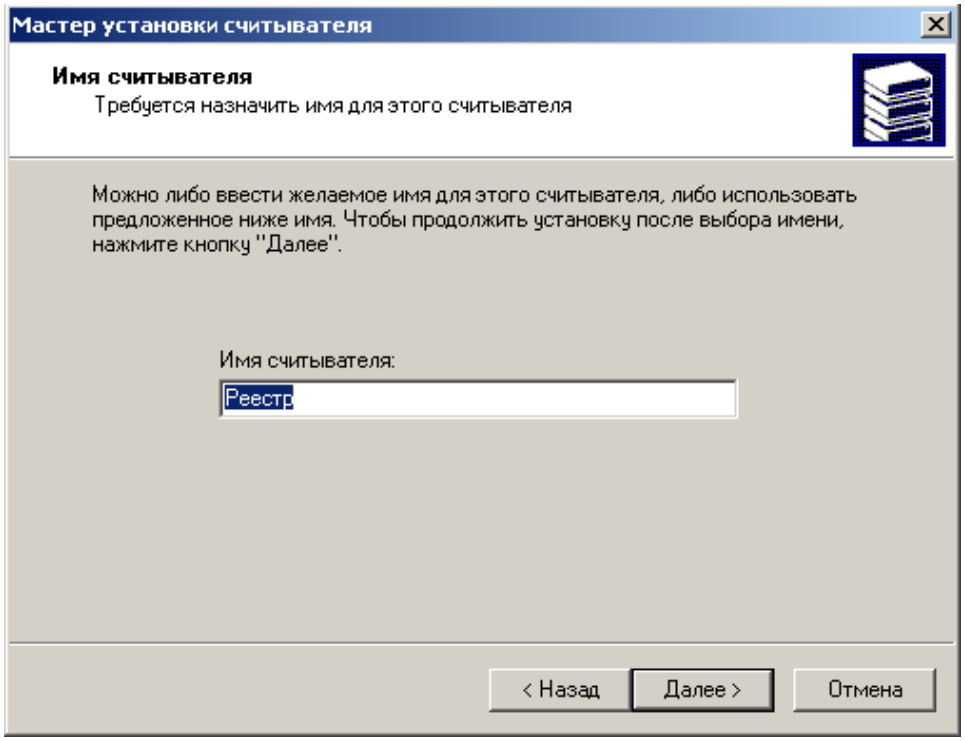

Рисунок 70

Шаг 7: инсталляция считывателя Реестр завершена, нажмите Готово:

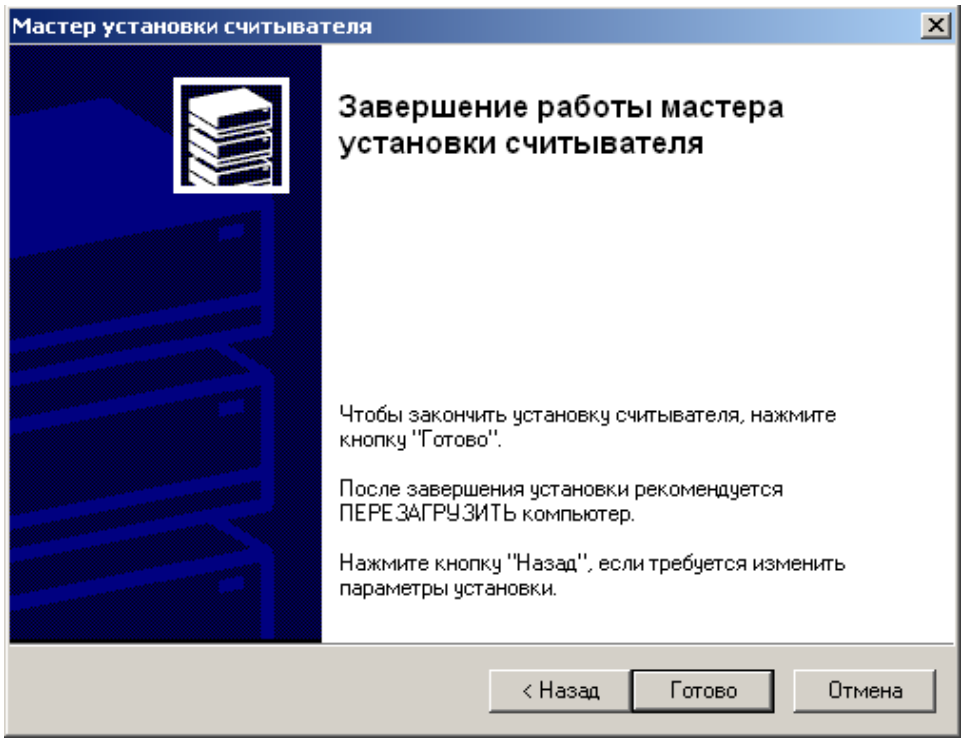

Рисунок 71

Шаг 8: считыватель Реестр добавлен в список инсталлированных считывателей, нажмите ОК:

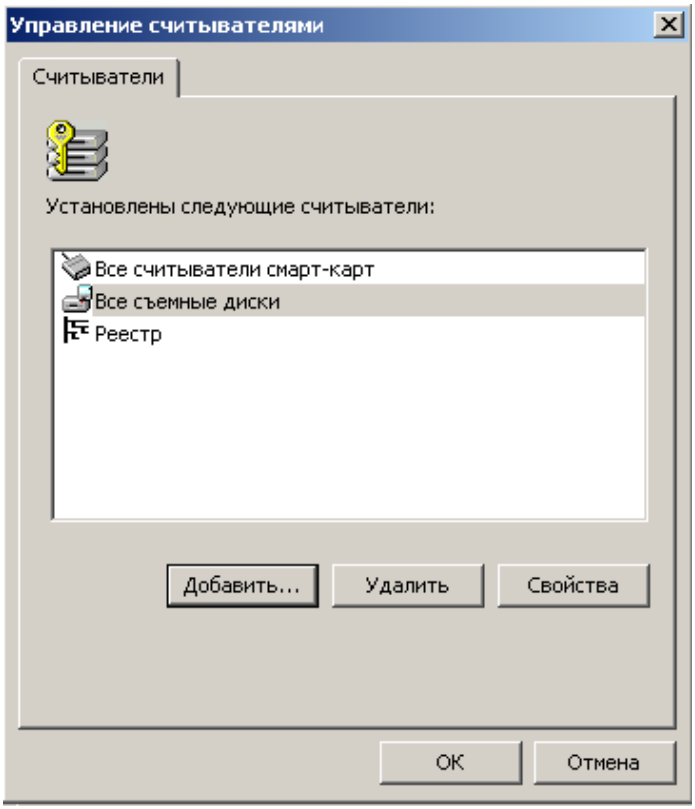

Рисунок 72

Шаг 9: перезагрузите компьютер.

16.5. Инсталляция внешнего считывателя и ключевого носителя информации в "КриптоПро CSP 3.6"

Инсталляция некоторых внешних считывателей уже выполнена. Для остальных внешних считывателей инсталляция выполняется так же как и для Реестра, описанная в разделе "Инсталляция ключевого считывателя Реестр в "КриптоПро CSP 3.6".

Для некоторых считывателей необходимо еще выполнить инсталляцию носителей. Для Rutoken и eTokenPro такая инсталляция уже выполнена.

Шаг 1: Инсталляция других носителей производится при выборе предложения Настроить типы носителей... в окне Свойства КриптоПро CSP во вкладке Оборудование (Рисунок 73).

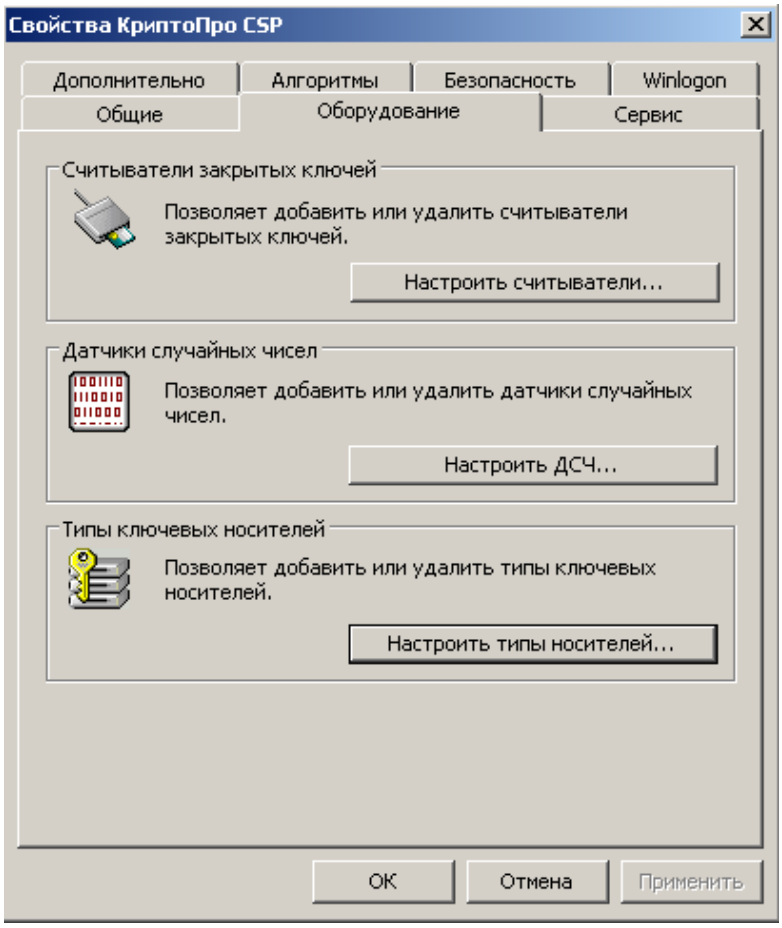

Рисунок 73

Шаг 2: вкладка Ключевые носители показывает инсталлированные ключевые носители. Для добавления носителя нажмите кнопку Добавить...

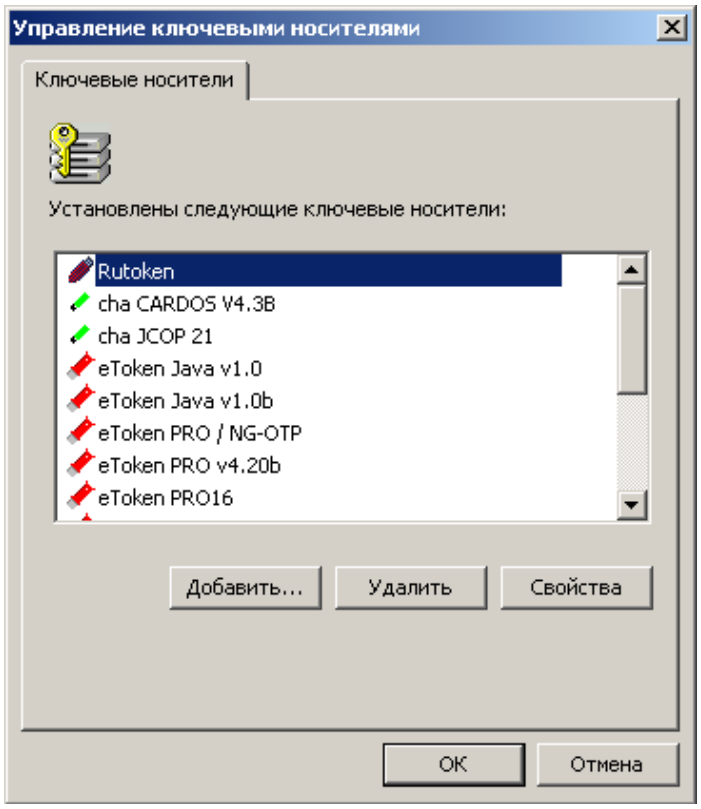

Рисунок 74

Далее следуйте указаниям Мастера установки ключевого носителя.

По завершению инсталляция внешнего ключевого носителя и считывателя полностью выполнена.

