

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



Программный комплекс «Шлюз безопасности CSP VPN Gate. Версия 3.11»

СПДС «ПОСТ»

Руководство администратора

18.05.2015

Содержание

1.	Назначение СПДС «ПОСТ»	3
1.1.	Угрозы в системах удаленного доступа	3
1.2.	Технологии построения доверенного сеанса	4
2.	Комплект поставки	6
3.	Требования к программно-аппаратным средствам	7
4.	Назначение и функции СПДС «ПОСТ»	8
5.	Принцип работы СПДС «ПОСТ»	11
6.	Подготовка СПДС «ПОСТ» к работе	13
6.1.	Подготовка рабочего места администратора	14
6.2.	Установка PIN-кодов	15
6.3.	Создание ключевой пары и запроса на сертификат СПДС «ПОСТ»	16
6.4.	Подготовка данных для инициализации СПДС «ПОСТ»	23
6.5.	Инициализация СПДС «ПОСТ»	24
7.	Работа с СПДС «ПОСТ»	26
7.1.	Режимы работы	28
7.2.	Отображение текущего статуса СПДС «ПОСТ»	29
7.3.	Организация ввода/вывода данных	30
7.4.	Диагностическая информация	31
7.5.	Обновление Продукта	32
7.6.	Завершение работы с СПДС «ПОСТ»	33

1. Назначение СПДС «ПОСТ»

1.1. Угрозы в системах удаленного доступа

Задача организации удаленного доступа пользователей весьма актуальна для государственных и коммерческих организаций, причем потребность в защите доступа растет год от года.

В то же время в системах удаленного доступа риски информационной безопасности, по ряду причин выше, чем в локальных сетях:

- Работая вне контролируемой зоны предприятия, пользователь может отступить от предписанного ему регламента безопасности, в частности – пытаться изменять конфигурацию своего компьютера, в том числе – отключить требуемые корпоративной политикой безопасности механизмы защиты.
- Социальное окружение пользователя вне офиса предприятия может быть более агрессивным. В частности, пользователь может находиться в поле наблюдения злоумышленников. Скрытое наблюдение может иметь цели перехвата информации, атрибутов аутентификации, фишинга. К пользователю в целях мошенничества или промышленного шпионажа могут применяться атаки типа social engineering.
- Временно оставленное без присмотра оборудование пользователя может быть компрометировано или похищено.
- Вычислительная среда рабочего места удаленного пользователя может быть заражена опасным кодом, содержать вирусы, программные закладки, опасное программное обеспечение (spyware, malware).
- Сетевая среда рабочего места пользователя может быть незамкнута, с рабочего места пользователя, наряду с соединением с корпоративной сетью, могут быть установлены опасные посторонние соединения. Это создает возможность для осуществления транзитной атаки на корпоративную сеть через компрометированное рабочее место удаленного пользователя.

Администратор безопасности не может с достоверностью контролировать все перечисленные риски и поэтому удаленный доступ для него всегда представляется не до конца решенной проблемой безопасности. Без контроля над рабочим местом пользователя устранить угрозы или снизить до приемлемого уровня перечисленные выше риски невозможно.

1.2. Технологии построения доверенного сеанса

Однако риски информационной безопасности при удаленном доступе пользователей могут быть существенно снижены в случае применения среды построения доверенного сеанса (СПДС).

Технология СПДС реализуется следующим образом.

Пользователь получает специальный загрузочный носитель, на котором находится целостный эталон среды функционирования (СФ), включающей доверенную операционную систему, комплект средств криптографической защиты информации (СКЗИ) и целевые приложения.

На рабочем месте пользователя производится настройка BIOS, позволяющая производить загрузку рабочего места с внешнего USB-носителя.

После аутентификации пользователя со специального загрузочного носителя загружаются эталонный образец среды функционирования и прикладное программное обеспечение.

Между рабочим местом пользователя и точкой доступа в корпоративную сеть устанавливается защищенное при помощи технологии IPsec соединение. Открытый трафик при этом исключается политикой безопасности VPN-продукта, чем достигается полная изоляция сетевой среды, в которой реализуется доверенный сеанс.

Пользователь получает доступ строго к целевому приложению. Доступ к операционной системе или посторонним приложениям для него исключен, командная консоль операционной системы и посторонние приложения просто изъяты из среды функционирования.

Прикладное программное обеспечение может иметь узко ограниченную функциональность. Например, в веб-браузере может быть исключена возможность доступа к настройкам браузера и строке ввода URL. Это приведет к тому, что пользователь будет осуществлять доступ только к ограниченному составу веб-объектов, на основе встроеной в веб-страницы навигации.

При этом к компьютеру, выступающему в качестве рабочего места пользователя, не предъявляются требования защищенности. Компьютер может быть поражен вирусами и опасным ПО, доступен по сети для хакеров – эталон среды функционирования не будет взаимодействовать с опасными носителями и читать с них данные, VPN-клиент «отключит» все опасные соединения.

Таким образом, применение технологии СПДС дает, в сравнении с традиционными технологиями защиты удаленных и мобильных клиентов, целый ряд преимуществ:

- Обеспечивается целостность программной среды терминала удаленного доступа. Эталонный образец среды функционирования загружается в рабочее место со специального защищенного носителя, исключая запись на него посторонних данных. При всякой инициализации доверенного сеанса производится загрузка эталонного образца СФ. Никакие данные по результатам работы пользователя в течение предыдущих сеансов в СФ не вносятся. Таким образом, в случае изолированного процесса доступа к прикладному ПО Заказчик может отказаться от применения средств защиты от вирусов, опасного ПО, закладок. Это обстоятельство позволяет не только сэкономить средства на антивирусном программном обеспечении, но и существенно облегчить процесс эксплуатации мобильных терминалов, поскольку нет необходимости контролировать их конфигурацию обновлять на них антивирусные базы данных.
- Обеспечивается изоляция вычислительного процесса клиента удаленного доступа в ходе доверенного сеанса: модуль загрузки среды функционирования исключает взаимодействие с «грязной «периферией» и загрузку недоверенного программного обеспечения.

- Строгая аутентификация пользователя при доступе к доверенному сеансу работает по традиционной двухфакторной схеме: пользователь аутентифицируется перед загрузкой СФ при помощи стойкого установленного администратором безопасности пароля (число попыток ввода пароля ограничено), доступ в корпоративную сеть и к серверным ресурсам осуществляется при помощи цифрового сертификата X.509, хранящегося на защищенном носителе. При необходимости эти средства аутентификации могут быть усилены средствами аутентификации в составе целевых приложений.
- Сетевая среда доверенного сеанса полностью изолирована от посторонних воздействий: трафик шифрован на основе криптоалгоритма ГОСТ 28147, обеспечивается целостность передаваемых данных и целостность потока пакетов. Поскольку в защищенную сеть может войти только владелец секретного ключа – контроль доступа в защищенный сегмент сети приобретает криптографическую стойкость, недоступную для некриптографических методов контроля сетевого доступа.

Качество реализации функциональности защиты СПДС подтверждено сертификатами ФСТЭК (как межсетевой экран 3го класса, как СЗИ с оценочным уровнем доверия 3+ (усиленный) по «Общим критериям» ГОСТ Р ИСО.МЭК 15408, по 3му уровню контроля на отсутствие недеklarированных возможностей) и ФСБ России (СКЗИ КС2). Продукт применим для всех задач защиты конфиденциальной информации, не составляющей государственную тайну, в АС до класса 1Г включительно и в ИСПДн до класса К1 включительно.

2. Комплект поставки

Программный комплекс «Шлюз безопасности CSP VPN Gate. Версия 3.11» на специальном загрузочном носителе «СПДС-USB-01» поставляется в следующей комплектации:

- Специальный загрузочный носитель СЗН «СПДС-USB-01» (общий объем 2ГБ или 4ГБ), на котором находится специальное и функциональное программное обеспечение.
- Эталонный диск программного обеспечения.
- Компакт-диск с документацией.
- Копия сертификата соответствия ФСБ России.
- Лицензия на использование программного комплекса CSP VPN Gate версии 3.11.
- Лицензия на использование программного продукта «КриптоПро CSP».

3. Требования к программно-аппаратным средствам

СПДС «ПОСТ» функционирует совместно с ПЭВМ, имеющей следующий минимальный состав технических и программных средств:

- процессор в архитектуре Intel x861 поддерживающий работу устройств по интерфейсу USB стандарта 1.1 и выше;
- свободный USB-порт;
- сетевой интерфейс;
- возможность BIOS ПЭВМ осуществлять загрузку ОС с USB-устройств.

4. Назначение и функции СПДС «ПОСТ»

СПДС «ПОСТ» – это специальный загрузочный носитель «СПДС-USB-01» с установленным СКЗИ CSP VPN Gate 3.11 и функциональным программным обеспечением, который подключается к USB-порту компьютера пользователя и позволяет получить доступ к защищаемым ресурсам, в соответствии с заданной политикой безопасности (Рисунок 1).

Специальный загрузочный носитель «СПДС-USB-01», разработанный ЗАО «С-Терра СиЭсПи» и компанией Promwad, – это USB-устройство с собственным микропроцессором со встроенным специальным программным обеспечением, энергонезависимой флэш-памятью и приемником специального типа, выполненного в виде приемника SIM-карт.

Скорость обмена данными по интерфейсу USB – 480 Мб/сек (соответствует USB 2.0 HighSpeed). Потребляемая мощность – не более 0,3 Вт (сила тока – не более 60 мА при напряжении 5 В). Объем установленной памяти 2 или 4 гигабайта.

Память устройства разделена на области с различными правами доступа:

- В области памяти с доступом на чтение находится ОС и специальное программное обеспечение.
- В области памяти с доступом на чтение и запись находится функциональное программное обеспечение. Доступ на запись предоставляется только после идентификации и аутентификации пользователя (с использованием PIN-кода).

Размер области памяти, доступной пользователю для чтения/записи: 226Мб при объеме установленной памяти 2Гб и 1834Мб при объеме установленной памяти 4Гб.



Рисунок 1

СПДС «ПОСТ» (далее Продукт или Изделие) предназначен для создания удаленного защищенного автоматизированного рабочего места (АРМ) на основе среды построения доверенного сеанса (СПДС).

Среда построения доверенного сеанса обеспечивает:

- целостность программной среды терминала удаленного доступа;
- изоляцию вычислительного процесса клиента удаленного доступа;
- строгую аутентификацию клиента удаленного доступа;
- изоляцию сетевой среды удаленного пользователя;
- защиту потока пакетов от внедрения посторонних данных;
- применение сертифицированных средств криптографической защиты информации и фильтрации трафика;
- контролируемый администратором файловый обмен при помощи выделенного раздела специального загрузочного носителя.

СПДС «ПОСТ» выполняет следующие функции:

- аутентификацию пользователя;
- защиту трафика на уровне аутентификации/шифрования сетевых пакетов по протоколам IPsec;

- пакетную фильтрацию трафика с использованием информации в полях заголовков сетевого, транспортного и прикладного уровней;
- событийное протоколирование и мониторинг;
- 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;
- маскировку адресных пространств защищаемых сетей (туннелирование трафика).

СПДС «ПОСТ» запрещает доступ к жестким дискам, съемным носителям и системам ввода-вывода АРМ пользователя, за исключением:

- видеокарты,
- клавиатуры (USB, PS/2),
- мыши (USB, PS/2).

СПДС «ПОСТ» поддерживает работу со следующими видами сетевых интерфейсов:

- Ethernet,
- LTE.

СПДС «ПОСТ» позволяет использовать следующие варианты задания IP-адреса:

- статический адрес,
- динамический адрес по протоколу DHCP,
- динамический адрес, назначаемый интерфейсу мобильного соединения по протоколам семейства PPP или другим протоколам, применяемым в сетях операторов мобильной связи.

5. Принцип работы СПДС «ПОСТ»

Специальный загрузочный носитель СПДС-USB-01 подключается к USB-порту АРМ пользователя. Предварительно на рабочем месте пользователя необходимо настроить BIOS, чтобы загрузка ОС производилась с USB-устройства. При загрузке со специального загрузочного носителя выполняются следующие действия:

- автоматически запускается модуль доверенной загрузки, который аутентифицирует пользователя и проверяет целостность программного обеспечения;
- происходит загрузка среды функционирования, в которую входят: операционная система, средства криптографической защиты (СКЗИ CSP VPN Gate 3.11) и другие модули;
- запрашивается режим работы – администратора или пользователя и запускается целевое функциональное программное обеспечение:
- в режиме работы администратора комплекс находится в состоянии ожидания защищённого удалённого подключения администратора;
- в режиме работы пользователя, в зависимости от типа изделия, выполняется одно из следующих действий:
 - ◆ устанавливается соединение терминальной программы rdesktop с рабочим столом удаленного ресурса, адрес которого установлен администратором;
 - ◆ устанавливается соединение с заданным веб-сервером, адрес которого установлен администратором.

Схема применения Продукта представлена на рисунке.



Рисунок 2

Специальный загрузочный носитель (*Продукт СПДС*) через USB-порт подключается к АРМ (*Недоверенное рабочее место пользователя*).

Происходит аутентификация пользователя – вводится PIN-код. В случае успешной аутентификации загружается среда функционирования.

Пользователь выбирает режим работы. В зависимости от выбранного режима:

- управление передается администратору или Серверу управления – административный режим;
- пользователь получает доступ к терминальному серверу/веб-серверу – режим работы пользователя.

Причем пользователь получает доступ только к целевому программному обеспечению. Доступ к операционной системе, посторонним приложениям и периферийным устройствам АРМ, за исключением специально разрешенных к использованию исключен, что обеспечивает целостность программной среды терминала удаленного доступа и изоляцию вычислительного процесса клиента удаленного доступа в ходе доверенного сеанса.

Между рабочим местом пользователя и точкой доступа в доверенную сеть (*Шлюз безопасности CSP VPN Gate*) устанавливается защищенное IPsec соединение (*IPsec туннель*), параметры которого определяются администратором.

Аутентификация пользователя при доступе в *Доверенную сеть* осуществляется при помощи ключа подписи ГОСТ Р 34.10-2001, хранящегося на специальном загрузочном носителе под защитой пароля пользователя.

Сетевая среда доверенного сеанса полностью изолирована от посторонних воздействий благодаря строгой аутентификации пользователя, шифрованию трафика с использованием криптографического алгоритма ГОСТ 28147-89 и контролю целостности передаваемых данных.

В случае необходимости выполнить административные действия (изменить параметры защищенного соединения, изменить сетевой профиль или изменить порядок перебора сетевых профилей, поменять сертификат, добавить комплект драйверов, включаемых в среду функционирования СПДС «ПОСТ»), можно применять встроенные в СПДС «ПОСТ» средства или *Сервер управления* (программный продукт «С-Терра КП 4.1»).

Программный продукт «С-Терра КП 4.1» входит в комплект поставки СПДС «ПОСТ».

6. Подготовка СПДС «ПОСТ» к работе

Перед началом работы с Продуктом ознакомьтесь с Правилами пользования.

Подготовка продукта СПДС «ПОСТ» к работе выполняется администратором.

Изначально на специальном загрузочном носителе СЗН «СПДС-USB-01» установлено СКЗИ CSP VPN Gate версии 3.11 и функциональное программное обеспечение.

Опишем кратко действия администратора при использовании Продукта «С-Терра КП 4.1» (более подробное описание приведено в документе [«Программный продукт «С-Терра КП 4.1»](#)). Администратор должен подготовить политику безопасности и создать *Клиента управления* для СПДС «ПОСТ».

Клиент управления – клиентская часть продукта «С-Терра КП 4.1», устанавливается на СПДС «ПОСТ» с инсталлированным продуктом CSP VPN Gate (начиная с версии CSP VPN Gate 3.11, *Клиент управления* входит в состав СКЗИ CSP VPN Gate). *Сервер управления* – Серверная часть продукта «С-Терра КП 4.1», устанавливается на выделенный компьютер.

Администратор:

- устанавливает PIN администратора и PIN пользователя для доступа к специальному загрузочному носителю;
- устанавливает опциональный дополнительный пароль на доступ к разделу СЗН, предназначенному для файлов пользователя;
- создает контейнер с ключевой парой и сертификатом;
- формирует политику безопасности для СПДС;
- задает необходимые настройки (лицензии, сетевые настройки, параметры целевого приложения пользователя).

Подготовленные данные размещаются администратором на специальном загрузочном носителе.

Администратор подключает специальный загрузочный носитель к компьютеру, предварительно настроив BIOS, чтобы загрузка ОС производилась с USB-устройства. Настройка BIOS описана в [«Руководстве пользователя»](#) в разделе «Приложение».

В процессе первой загрузки происходит инициализация СПДС «ПОСТ».

Дальнейшее техническое обслуживание продукта СПДС «ПОСТ» может выполняться дистанционно, по защищенному каналу, с рабочего места администратора CSP VPN Gate с использованием встроенных в СПДС «ПОСТ» средств, либо при помощи *Сервера управления* и *Клиента управления*.

6.1. Подготовка рабочего места администратора

Администратору потребуется компьютер с ОС Windows Server 2003/2008, на котором должны быть установлены:

- «КриптоПро CSP 3.6/3.6R2/3.6R4»,
- Сервер управления (продукт «С-Терра КП»),
- «С-Терра Редактор СПДС» (дистрибутив продукта размещен на сайте компании по адресу <http://s-terra.com/documents/R311/SPDSEditor/SPDSEditor.rar>).

Сервер управления необходимо дополнительно настроить. Установка и настройка *Сервера управления* описаны в документе [«Программный продукт «С-Терра КП 4.1»](#).

После того как будут установлены и настроены все необходимые продукты, в следующих разделах рассмотрим более подробно действия, выполняемые администратором при подготовке СПДС «ПОСТ» к работе.

6.2. Установка PIN-кодов

Используя «С-Терра Редактор СПДС» администратор может поменять PIN пользователя, администратора и транспортный PIN устройства или вернуть всем PIN-кодам устройства их заводские значения.

Изначально заданы следующие значения:

PIN пользователя данных, PIN пользователя, PIN администратора – 12345678,

Транспортный PIN – случайное число.

Меню *Действия* и *PIN-коды* дублируются кнопками на правой панели окна **С-Терра Редактор СПДС** (Рисунок 3). Единственное отличие – если не выделено никакого устройства, то доступно действие – *Закреть все сессии*.

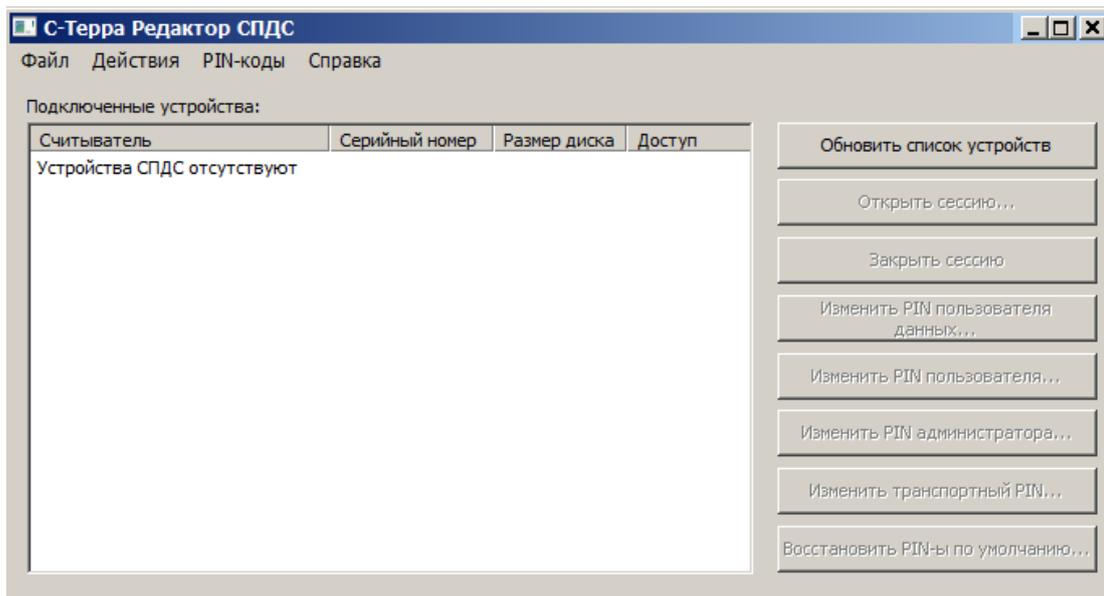


Рисунок 3

Обновить – обновляет список доступных устройств.

Открыть сессию... – открывает раздел выбранного устройства на запись.

Закреть сессию... – закрывает раздел выбранного устройства от записи.

Изменить PIN пользователя данных... – позволяет сменить PIN-код пользователя раздела данных выбранного устройства. Этот PIN-код необходим пользователю для открытия раздела данных на запись.

Изменить PIN пользователя... – позволяет сменить PIN-код пользователя выбранного устройства. Этот PIN-код необходим пользователю для аутентификации при загрузке с устройства или для открытия раздела данных на запись.

Изменить PIN администратора... – позволяет сменить PIN-код администратора выбранного устройства. Этот PIN-код необходим администратору для смены PIN-кодов устройства.

Изменить транспортный PIN... – позволяет сменить транспортный PIN-код выбранного устройства. Этот PIN-код необходим для возможности низкоуровневых операций над устройством.

Восстановить PIN-ы по умолчанию... – возвращает всем PIN-кодам устройства их заводские значения.

6.3. Создание ключевой пары и запроса на сертификат СПДС «ПОСТ»

Администратор подготавливает ключевую пару и сертификат, которые надо поместить на специальный загрузочный носитель. В данном разделе рассмотрим пример создания ключевой пары и запроса на сертификат СПДС «ПОСТ».

Вставьте специальный загрузочный носитель в USB-разъем компьютера администратора и запустите установленный «С-Терра Редактор СПДС». Распознанное устройство появится в окне **Редактора СПДС**. Нажмите кнопку *Открыть сессию*, чтобы открыть доступ не только на чтение, но и на запись (Рисунок 4).

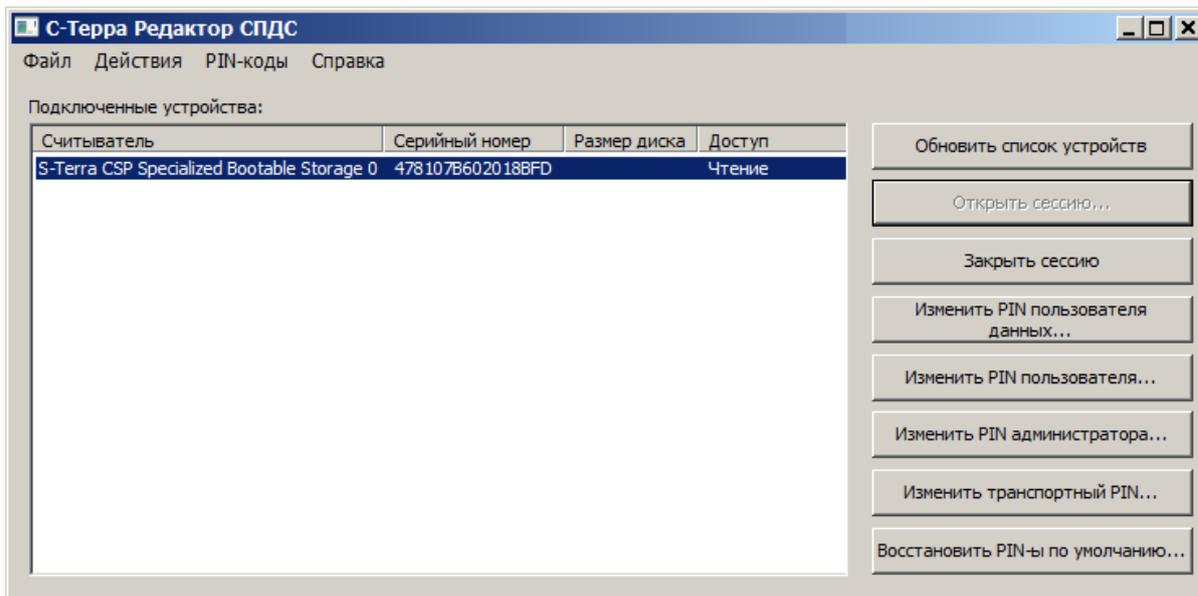


Рисунок 4

В окне **Авторизация** введите PIN пользователя и нажмите **ОК** (Рисунок 5).

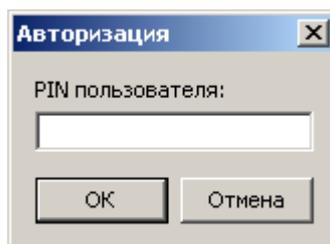


Рисунок 5

Примечание: Если PIN-код введен неправильно, дается еще 4 попытки, после чего специальный загрузочный носитель будет заблокирован. Разблокировать устройство может пользователь, идентифицированный как администратор. Если устройство будет заблокировано, из-за неправильного ввода PIN-кода администратора, то дальнейшее использование СПДС «ПОСТ» будет невозможно.

Далее в СКЗИ «КриптоПро CSP 3.6» инсталлируйте считыватель «*Все считыватели смарт-карт*» (Рисунок 6).

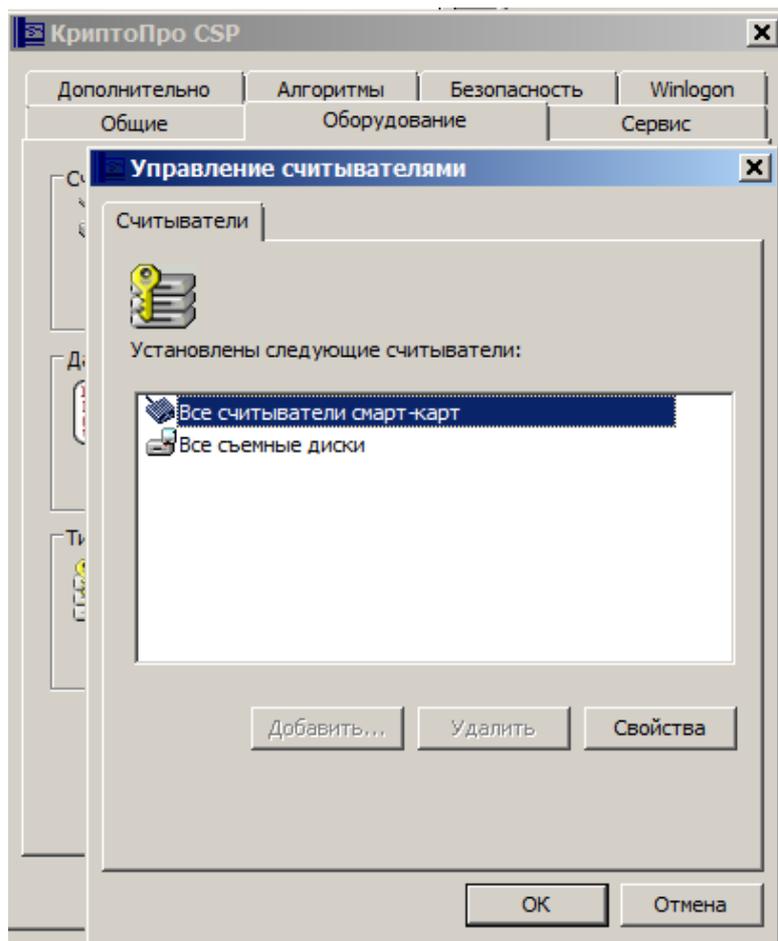


Рисунок 6

Для создания ключевой пары и запроса на локальный сертификат СПДС «ПОСТ» можно использовать средства Microsoft Windows. На рабочем месте администратора запустите Microsoft Internet Explorer. В поле Address укажите IP-адрес сервера Удостоверяющего Центра и запустите утилиту `certsrv` (Certificate Service), например, `http://10.0.232.10/certsrv/` (Рисунок 7).

В появившемся окне высвечивается имя Удостоверяющего Центра – в нашем случае S-Terra CA. Выберите предложение *Request a certificate*.

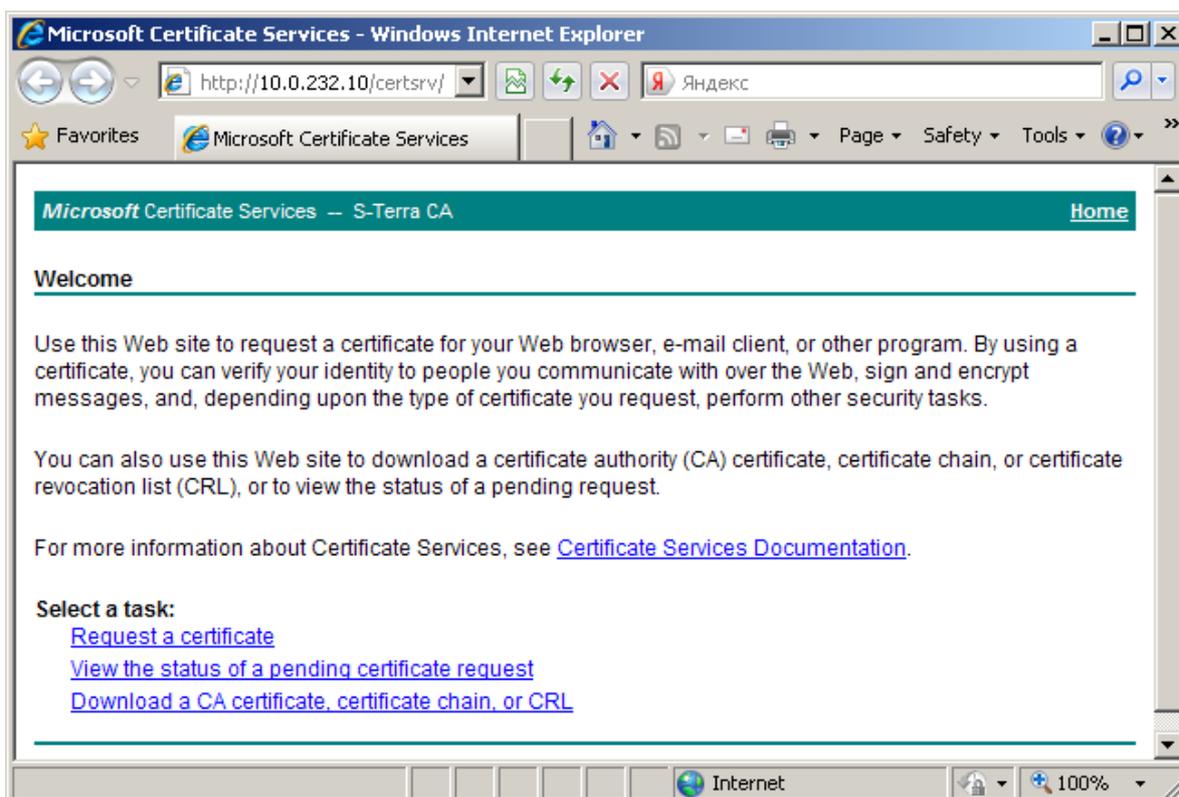


Рисунок 7

Далее выберите форму расширенного запроса – предложение *advanced certificate request* (Рисунок 8).

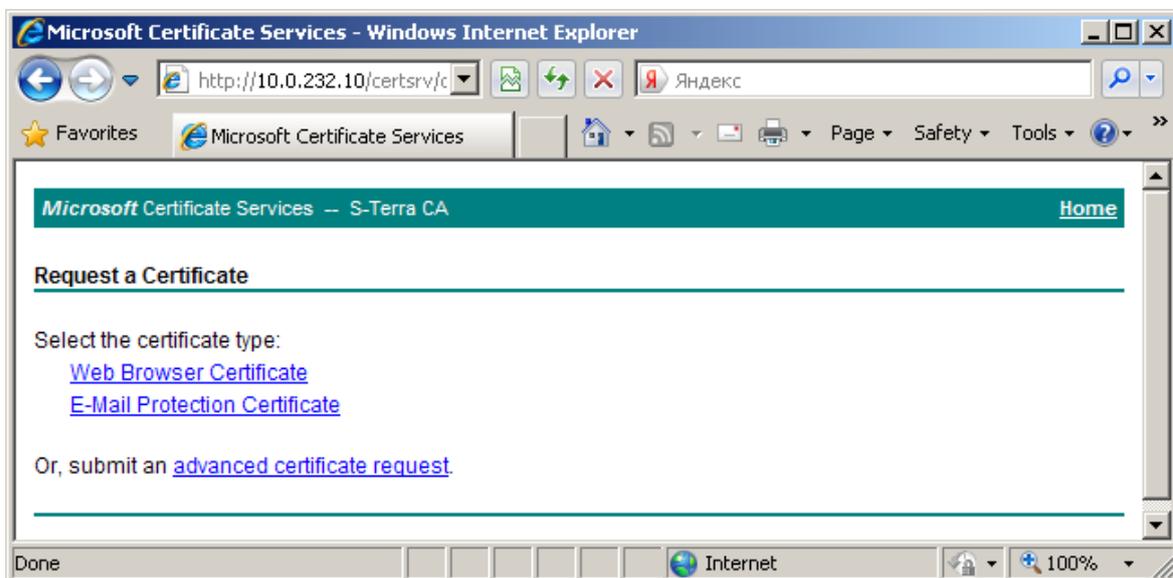


Рисунок 8

Для получения формы выберите предложение *Create and submit a request to this CA* (Рисунок 9).

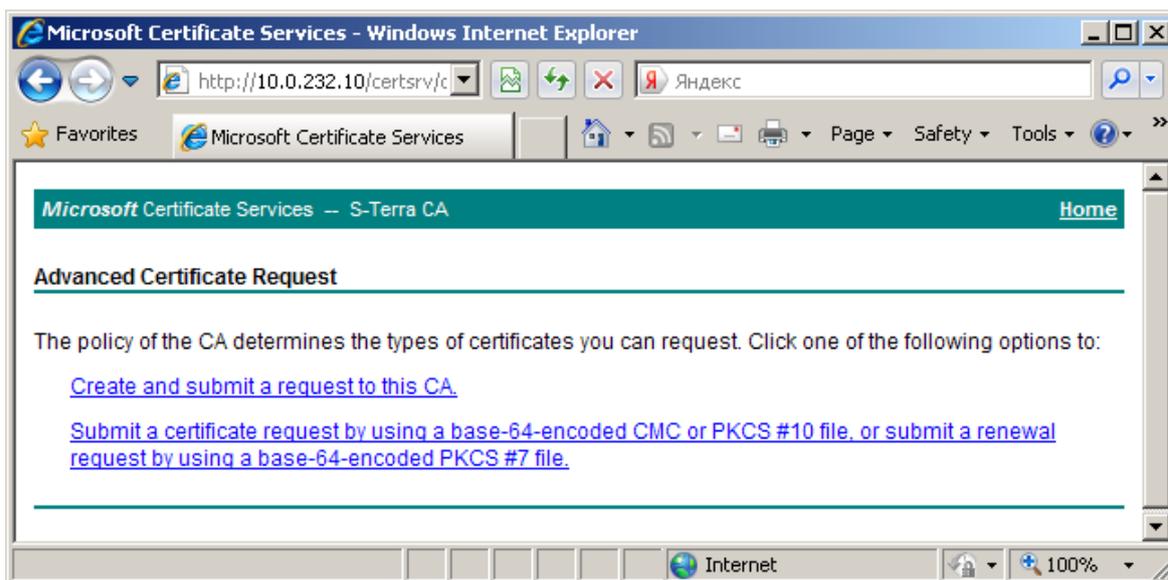


Рисунок 9

Заполните форму расширенного запроса (Рисунок 10). Дадим некоторые пояснения для ее заполнения:

- в разделе **Identifying Information** (Информация о Владельце Сертификата) внесите данные о владельце сертификата. Во всех полях этого раздела разрешается использовать не только латинские, но и русские буквы, кроме поля *Country/Region*, оно всегда содержит значение RU.
- в разделе **Type of Certificate Needed** (Тип требуемого сертификата) из выпадающего списка выберите предложение *IPSec Certificate*
- в разделе **Key Options** (Опции создания ключей) выбираются опции для создания ключевой пары и размещения секретного ключа. Рекомендуется сделать следующий выбор:
 - ◆ поставьте переключатель в положение *Create new key set* (Создать установки для нового секретного ключа)
 - ◆ *CSP* (Тип Криптопровайдера) – из выпадающего списка выберите *Crypto-Pro GOST R 34.10-2001 Cryptographic Service provider*
 - ◆ *Key Usage* (Использование ключей) – для выбора типа ключа поставьте переключатель в положение *Both* (для подписи и обмена)
 - ◆ *Key Size* (Размер ключа) – размер ключа. При выборе алгоритма GOST R 34.10-2001 длина ключа всегда 512
 - ◆ поставьте переключатель в положение *Automatic key container name*, чтобы имя контейнера с секретным ключом задавалось автоматически
 - ◆ *Mark keys as exportable* – поставьте флажок, чтобы можно было скопировать контейнер с секретным ключом
- в разделе **Additional Options** (Дополнительные опции):
 - ◆ *request Format* – CMC
 - ◆ *Hash Algorithm* – выбрать *GOST R 34.11-94*.

По этому образцу заполните форму запроса и нажмите кнопку *Submit*.

Microsoft Certificate Services -- S-Terra Demo CA Home

Advanced Certificate Request

Identifying Information:

Name:

E-Mail:

Company:

Department:

City:

State:

Country/Region:

Type of Certificate Needed:

Key Options:

Create new key set Use existing key set

CSP:

Key Usage: Exchange Signature Both

Key Size: Min:512
Max:512 (common key sizes: [512](#))

Automatic key container name User specified key container name

Mark keys as exportable

Export keys to file

Enable strong private key protection

Store certificate in the local computer certificate store
Stores the certificate in the local computer store instead of in the user's certificate store. Does not install the root CA's certificate. You must be an administrator to generate or use a key in the local machine store.

Additional Options:

Request Format: CMC PKCS10

Hash Algorithm: Only used to sign request.

Save request to a file

Attributes:

Friendly Name:

Рисунок 10

На следующем предупреждении нажмите кнопку Yes.

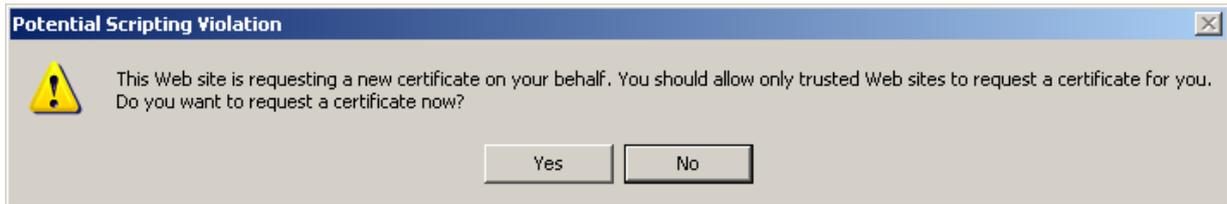


Рисунок 11

В следующем окне укажите ключевой носитель, соответствующий СПДС «ПОСТ», и нажмите ОК (Рисунок 12).

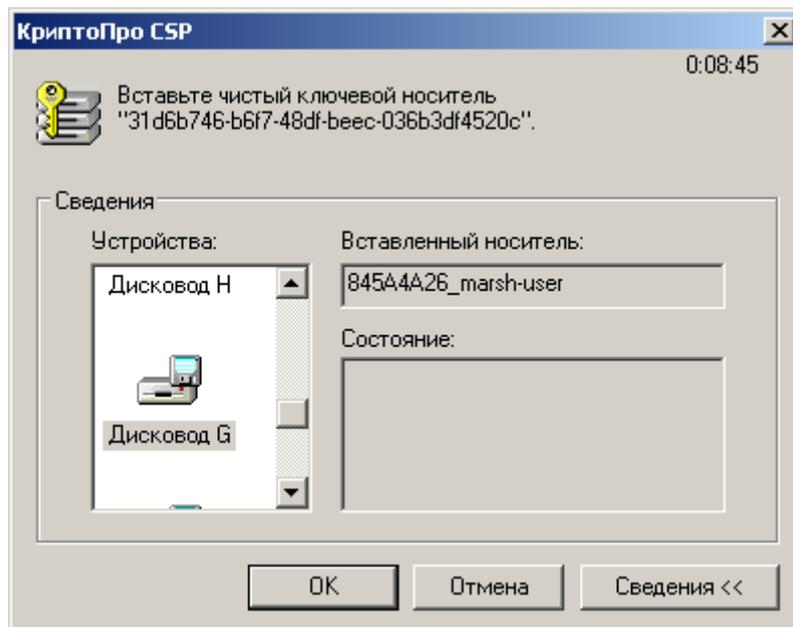


Рисунок 12

Если используется биологический ДСЧ, то нажимайте клавиши или перемещайте указатель мыши, если используется аппаратный генератор ДСЧ, то это окно не появляется (Рисунок 13).

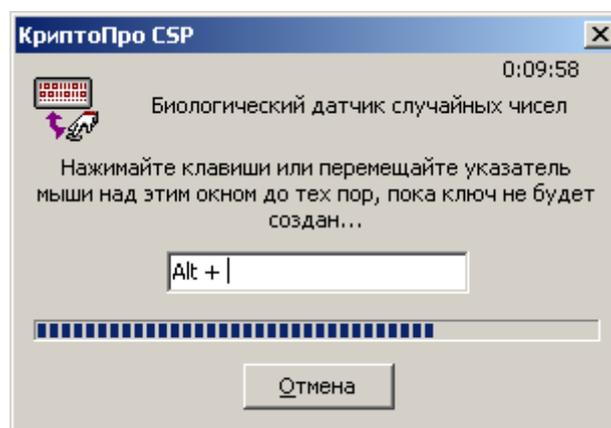


Рисунок 13

В окне запроса пароля поля оставьте пустыми (Рисунок 14).

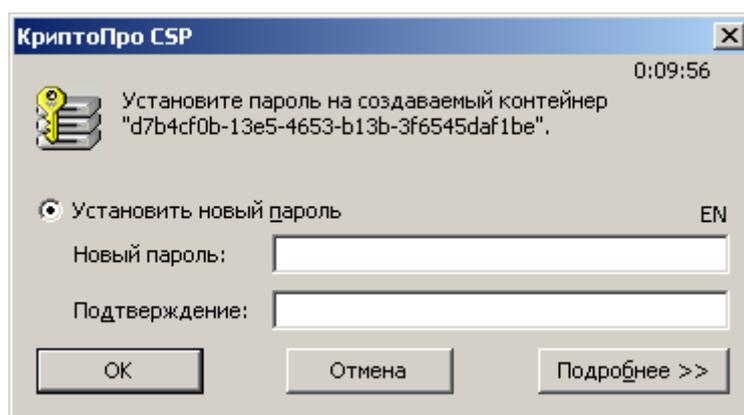


Рисунок 14

Если на Удостоверяющем Центре сертификаты выпускаются автоматически при получении запроса, то появляется окно с предложением установить сертификат (Рисунок 15). В этом случае выберите предложение *Install this certificate*.

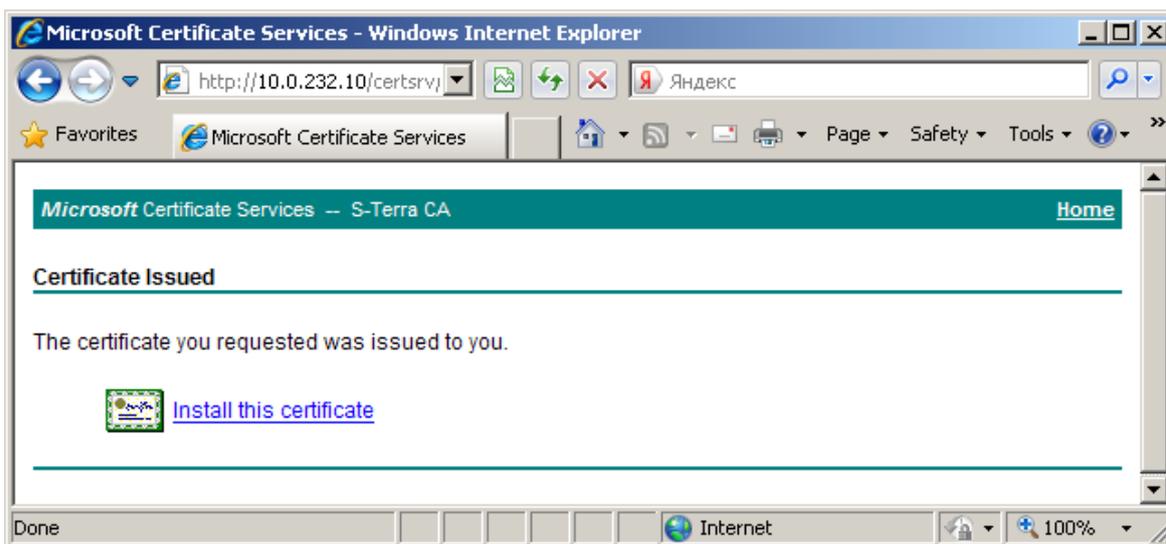


Рисунок 15

В результате сертификат будет записан на специальный загрузочный носитель в тот же контейнер, что и ключевая пара. Экпортируйте локальный сертификат из контейнера в файл, так как он будет необходим на *Сервере управления* при настройке СПДС «ПОСТ».

Дальнейшие действия выполняются администратором на компьютере, с установленным и настроенным *Сервером управления*.

6.4. Подготовка данных для инициализации СПДС «ПОСТ»

Администратор при помощи *Сервера управления* задает политику безопасности и создает *Клиента управления* для СПДС «ПОСТ».

Опишем кратко действия, которые необходимо выполнить администратору (подробное описание дано в документе [«Программный продукт С-Терра КП 4.1»](#)):

- Создайте на *Сервере управления* учетную запись клиента для СПДС «ПОСТ».
- Выполните необходимые настройки (укажите лицензии, сетевые настройки, параметры целевого приложения пользователя) и задайте политику безопасности для СПДС «ПОСТ», обеспечивающую защищенную работу пользователя с целевым функциональным программным обеспечением, а также позволяющую создавать защищенное соединение с *Сервером управления*.
- Сохраните дистрибутив подготовленного *Клиента управления* на специальном загрузочном носителе.
- Подготовьте скрипты для инициализации CSP VPN Gate и инсталляции *Клиента управления* и поместите их на специальный загрузочный носитель.

Затем СПДС «ПОСТ» необходимо инициализировать.

6.5. Инициализация СПДС «ПОСТ»

Процедура выполняется администратором, так как данные инициализации хранятся на специальном загрузочном носителе в незащищенном виде.

1. Подключите специальный загрузочный носитель к USB-порту выключенного компьютера. Включите компьютер и вызовите программу настройки BIOS. Клавиши, позволяющие попасть в программу настройки BIOS, обычно отображаются на экране монитора.
2. Настройте приоритетную загрузку ОС с USB-носителя (настройка BIOS описана в [«Руководстве пользователя»](#) в разделе «Приложение»). Выйдите из программы настройки с сохранением изменений.

Начнется загрузка со специального загрузочного носителя.

3. На экран выводится серийный номер устройства СПДС-USB. Запрашивается PIN пользователя, ввод PIN маскируется знаками «*».

Примечание: Если PIN-код введен неправильно, дается еще 4 попытки, после чего специальный загрузочный носитель будет заблокирован. Перед тем, как устройство будет заблокировано, выдается диагностическая информация. Разблокировать устройство может пользователь, идентифицированный как администратор. Блокировка производится аппаратными средствами. При утрате паролей пользователя и администратора дальнейшее использование СПДС «ПОСТ» будет невозможно.

4. Затем осуществляется проверка целостности файлов.
5. Выполняется инициализация СПДС «ПОСТ» (инициализируется CSP VPN Gate и на специальный загрузочный носитель устанавливается *Клиент управления*).
6. Происходит дальнейшая загрузка и появляется заставка СПДС «ПОСТ» (Рисунок 16).



Рисунок 16

7. Если инициализация прошла успешно, то появится окно (Рисунок 17), с предложением запустить административный режим и убывающим прогресс-баром (по завершению таймаута будет запущен режим пользователя). Нажмите *ОК* для перехода в

административный режим, чтобы проверить возможность скачивания обновлений с *Сервера управления*.

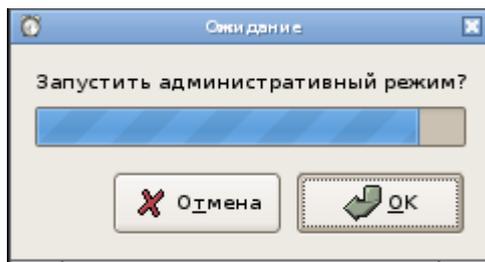


Рисунок 17

СПДС «ПОСТ» должен установить соединение с *Сервером управления* и загрузить с него нулевое обновление. После этого произойдет выключение устройства.

8. Затем необходимо проверить работу СПДС «ПОСТ» в режиме пользователя. Заново включите компьютер и, в появившемся окне (Рисунок 17), нажмите *Отмена*. Пользователь должен получить доступ к целевому программному обеспечению.

В случае успешного функционирования в обоих режимах, СПДС «ПОСТ» готов к дальнейшей эксплуатации пользователем.

7. Работа с СПДС «ПОСТ»

Подключите специальный загрузочный носитель к USB-порту выключенного компьютера (APM). Компьютер должен быть подготовлен к загрузке ОС с USB-устройства. Включите компьютер. Начнет выполняться загрузка со специального загрузочного носителя:

1. Запрашивается PIN пользователя.
2. Выполняется проверка подлинности подключаемых драйверов и функционального программного обеспечения. (Проверка целостности файлов).
3. Из заданных сетевых профилей выбирается первый, приводящий к успешному соединению. Если соединение установить не удалось, то появляется предупреждение о необходимости ручной настройки. Пользователь, если это разрешено может выполнить настройки сетевого соединения.
4. На панели задач появляются иконки (Рисунок 18), нажав на которые можно вызвать программы настройки системы времени и сетевого соединения (Рисунок 19).



Рисунок 18

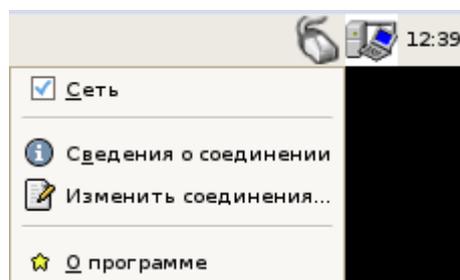
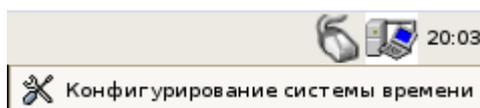


Рисунок 19

Если далее предполагается работать в административном режиме, то рекомендуется выполнить эти настройки до выбора режима работы. Описание настроек приведено в [«Руководстве пользователя»](#) в разделе «Приложение».

Также становятся доступны утилиты, вызываемые из меню рабочей панели (Рисунок 20). Подробное описание утилит приведено в [«Руководстве пользователя»](#) в разделе «Приложение».

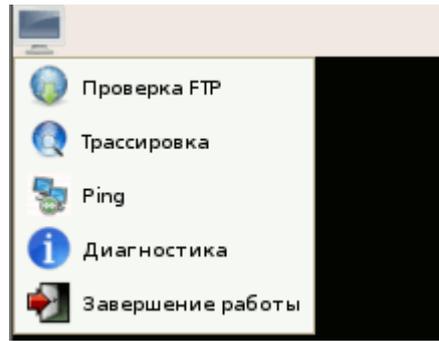


Рисунок 20

5. Предлагается выбрать режим работы (Рисунок 17).
Режим работы выбирается только во время загрузки. Чтобы сменить режим работы, надо закончить работу и перезагрузить компьютер.
6. Запускается функциональное программное обеспечение, соответствующее выбранному режиму работы.

7.1. Режимы работы

Административный режим

Административный режим предназначен для выполнения администратором конфигурационных действий. При этом будет заблокирован доступ пользователя к управлению операционной системой компьютера и средой функционирования СПДС «ПОСТ». Действия администратора по настройке и управлению СПДС «ПОСТ» с помощью *Сервера управления* описаны в документе [«Программный продукт С-Терра КП 4.1»](#).

Режим пользователя

В режиме пользователя выполняется работа с целевым функциональным программным обеспечением. Создается соединение терминальной программы rdesktop с рабочим столом удалённого ресурса, адрес которого был установлен администратором при подготовке СПДС «ПОСТ» к работе, или запускается приложение, дающее пользователю возможность выбора удалённого ресурса, если администратором задан их перечень. В случае если администратор не указал адрес удалённого ресурса или не удалось установить соединение с единственным заданным сервером, то будет запрошен адрес сервера.

7.2. Отображение текущего статуса СПДС «ПОСТ»

Наличие защищенного соединения	
VPN соединение отсутствует	
Установлено соединение VPN	
Наличие сетевого соединения	
Сетевое соединение отсутствует	
Сетевое соединение активно	

7.3. Организация ввода/вывода данных

Организация ввода/вывода данных определяется сценарием использования СПДС «ПОСТ» и политикой безопасности, заданной администратором.

СПДС «ПОСТ» запрещает доступ к жестким дискам, съемным носителям и системам ввода-вывода АРМ пользователя, за исключением:

- видеокарты,
- клавиатуры,
- мыши.

Если СПДС используется для терминального доступа, то пользователь может:

- обмениваться данными между специальным загрузочным носителем и приложениями, работающими на удалённом ресурсе;
- печатать из приложений, работающих на удалённом ресурсе, на локально подключенный принтер HP LaserJet P1606dn (при его наличии), доступный с СПДС «ПОСТ» по USB;
- печатать из приложений, работающих на удалённом ресурсе, на PDF-принтер и сохранять полученный файл на специальном загрузочном носителе.

Настройки сервиса печати выполняются администратором при подготовке СПДС «ПОСТ» к работе и могут быть изменены позднее, в ходе административного сеанса.

7.4. Диагностическая информация

Диагностическая информация собирается для каждого сеанса и записывается на СЗН «СПДС-USB-01 в каталог `disk/diaginfo` в виде архивного файла.

Имя архивного файла содержит идентификатор данного экземпляра СПДС «ПОСТ», дату и время и дополнительный указатель на момент создания файла (*on* – файл создан при загрузке продукта, *off* – при окончании работы, *run* – во время работы продукта).

В архивном файле находятся сведения об аппаратной платформе, на которой выполнялась загрузка СПДС, а также журнал сообщений, формируемый системой протоколирования событий.

Диагностическая информация хранится для пяти последних сессий.

Мониторинг и событийное протоколирование происходит на основе протоколов Syslog и SNMP в составе СКЗИ CSP VPN Gate 3.11.

7.5. Обновление Продукта

Обновление настроек Продукта всегда выполняется администратором.

Обновление настроек возможно как в ручном режиме, с использованием штатных утилит CSP VPN Gate 3.11 и ОС, так и с использованием другого продукта – «С-Терра КП 4.1». Описание создания и применения обновлений с использованием «С-Терра КП 4.1» смотрите в документе [«Программный продукт С-Терра КП 4.1»](#).

7.6. Завершение работы с СПДС «ПОСТ»

Административный режим

В административном режиме завершение работы выполняется автоматически – после применения обновлений компьютер выключается.

В критической ситуации, в случае зависания (обрыва) соединения, чтобы завершить работу с СПДС «ПОСТ» нажмите на иконку в верхней левой части экрана (Рисунок 21) и выберите пункт меню *Завершение работы*.



Рисунок 21

Будет запрошено подтверждение на завершение работы (Рисунок 22).

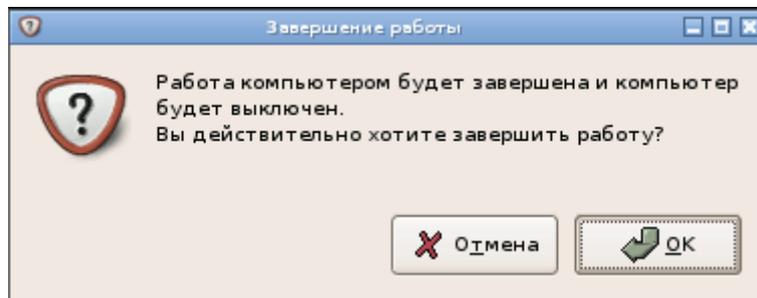


Рисунок 22

Режим пользователя

Завершение работы с СПДС «ПОСТ» в режиме пользователя можно выполнить, нажав на иконку в верхней левой части экрана (Рисунок 21) и выбрав пункт меню *Завершение работы*.

Если в настройках для соединения указан только один RDP-сервер, а не список серверов, то завершение работы автоматически выполняется после закрытия RDP-сессии (*Пуск* → *Завершение сеанса*).

В обоих случаях будет запрошено подтверждение на завершение работы.