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 С-Терра Шлюз. Версия 4.1

С-Терра «Пост»

Руководство пользователя

17.03.2016

Содержание

1. Подготовка АРМ пользователя к работе

С-Терра «Пост» – это специальный загрузочный носитель (СЗН «СПДС-USB-01») с установленным СКЗИ «С-Терра Шлюз. Версия 4.1» и функциональным программным обеспечением.

С-Терра «Пост» предназначен для создания удаленного автоматизированного рабочего места (АРМ) на основе среды построения доверенного сеанса (СПДС).

Пользователь получает от администратора С-Терра «Пост» полностью подготовленный к работе. Администратор предварительно должен установить PIN для доступа к специальному загрузочному носителю, создать и разместить на устройстве сертификат, сформировать политику безопасности, задать сетевые настройки и параметры целевого приложения пользователя.

Далее перейдите к разделу «Работа с С-Терра «Пост».

2. Работа с С-Терра «Пост»

При работе с С-Терра «Пост» 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.

Существует два режима работы с С-Терра «Пост»:

- Административный режим – предоставляет возможность изменить PIN администратора, разблокировать PIN пользователя.
- Режим пользователя – предоставляет доступ к функциональному программному обеспечению.

Административный режим работы выбирается только во время загрузки.

Административный режим подробно описан в «Руководстве администратора». Далее рассмотрим работу с С-Терра «Пост» в режиме пользователя.

2.1. Начало работы

Подключите специальный загрузочный носитель к USB-порту выключенного компьютера (АРМ). Включите компьютер. Начнет выполняться загрузка со специального загрузочного носителя:

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

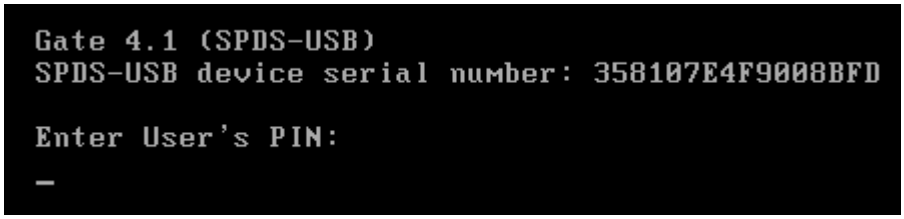

Рисунок 1

Примечание: Если PIN 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 С-Терра «Пост» будет невозможно.

2. После аутентификации пользователя загружается графическая оболочка LXDE (Рисунок 2).

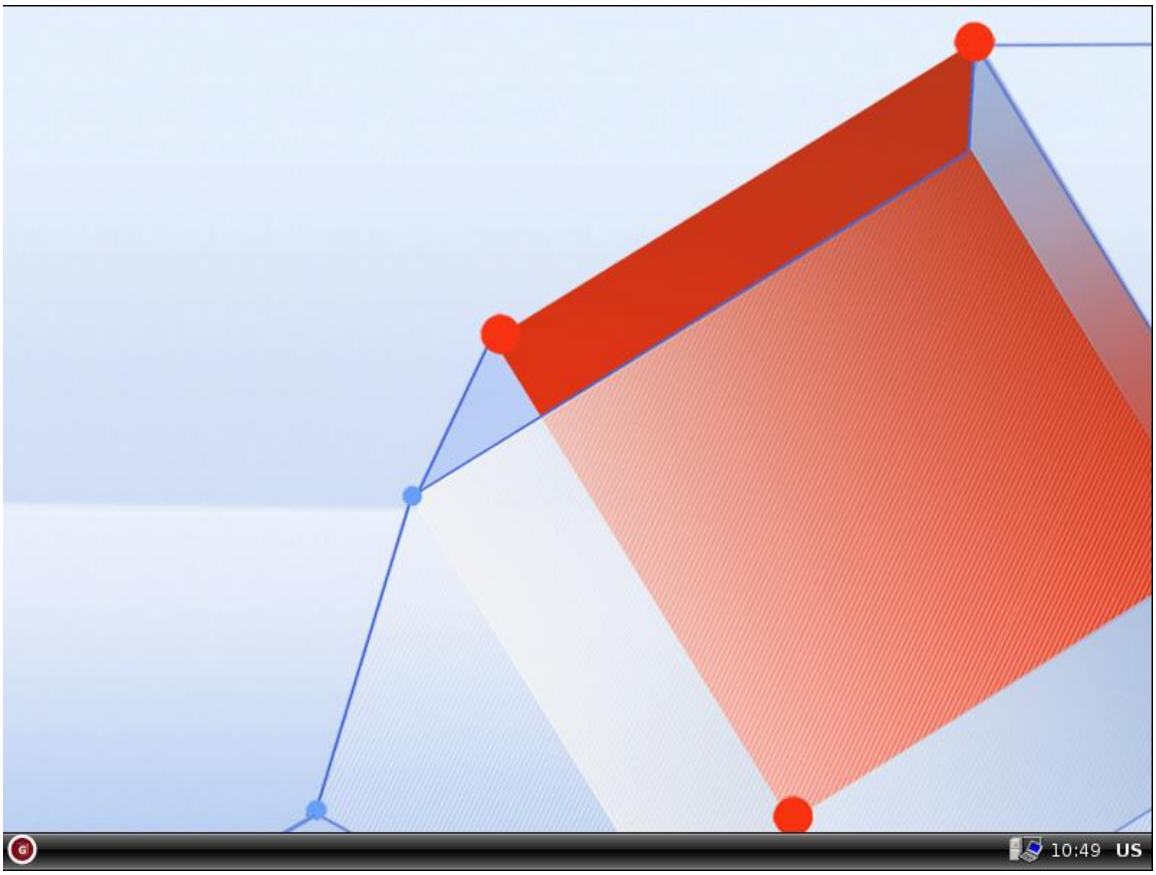

Рисунок 2

3. Если в настройках RDP-сессии, заданных Администратором, указана автозагрузка, то после запуска С-Терра «Пост» на рабочий стол будет выведено окно RDP-сессии (Рисунок 3). Для подтверждения подключения к указанному адресу, нажмите кнопку OK.

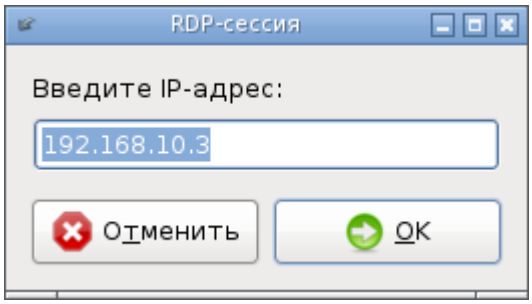

Рисунок 3

4. В случае выключенной автозагрузки запуск RDP-сессии производится из пункта системного меню **Интернет** (Рисунок 4):

   - **Интернет > Удаленный рабочий стол –** при заданных параметрах RDP-сессии от Сервера управления. В открывшемся окне RDP-сессии подтвердите подключение к указанному IP-адресу (Рисунок 3).
   - **Интернет > Удаленный рабочий стол (Без настроек) –** если IP-адрес удаленного рабочего стола требуется ввести вручную (при отсутствии, либо некорректном задании настроек ранее). В открывшемся окне RDP-сессии укажите адрес RDP-сервера (Рисунок 5). Логин и пароль при доступе к RDP-серверу будут запрашиваться непосредственно в RDP-сессии.

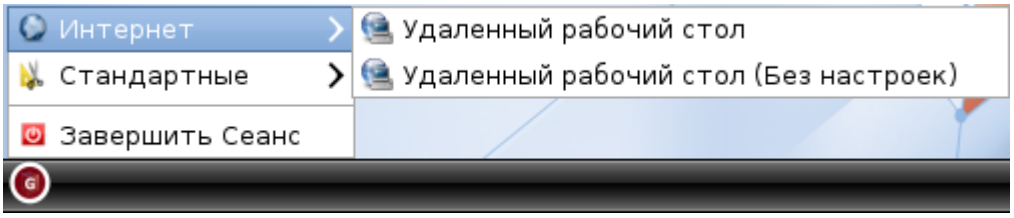

Рисунок 4

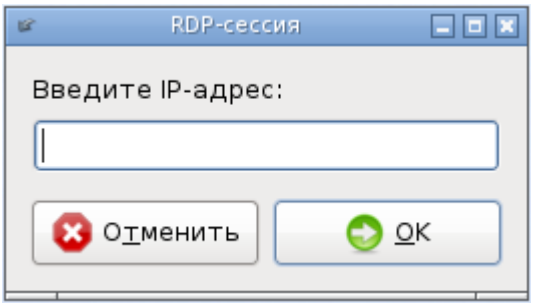

Рисунок 5

2.2. Обновление настроек Продукта

Обновление настроек Продукта, подготовленное администратором, выполняется автоматически с использованием продукта «С-Терра КП 4.1». Клиент управления проверяет наличие доступных для него обновлений и загружает их с Сервера управления. Обновление применяется сразу, перезагрузка устройства не требуется. Во время выполнения обновления VPN-сервис может быть остановлен.

2.3. 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 С-Терра «Пост», дату и время, а также 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 С-Терра «Пост», а также журнал сообщений, формируемый системой протоколирования событий.

Диагностическая информация хранится для пяти последних сессий (Рисунок 6).

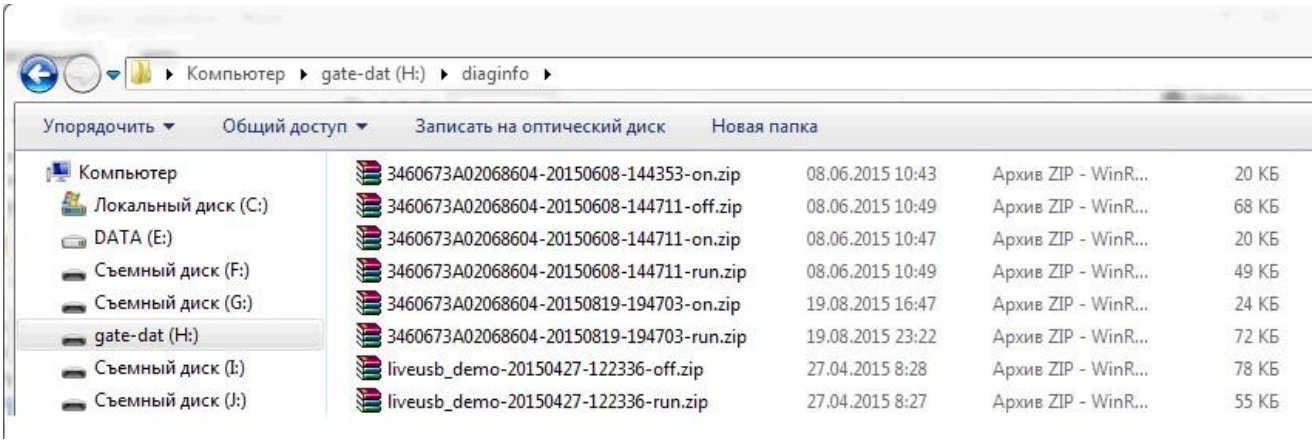

Рисунок 6

2.4. Завершение работы с С-Терра «Пост»

Для завершения работы с С-Терра «Пост» нажмите на иконку в нижней левой части экрана и выберите пункт меню **Завершить сеанс** (Рисунок 7).

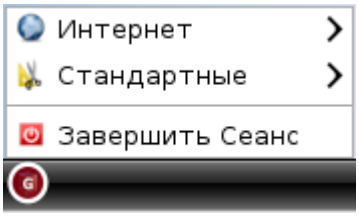

Рисунок 7

Появляется окно с выбором подтверждения выключения С-Терра «Пост» либо отменой действия (Рисунок 8).

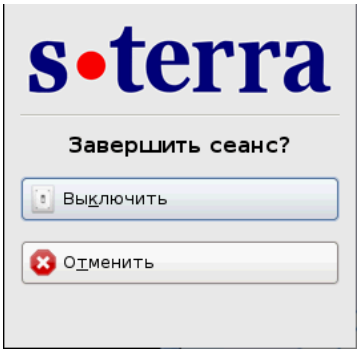

Рисунок 8

3. Диагностические утилиты

Диагностические утилиты вызываются нажатием на иконку в нижней левой части экрана и выбором пункта меню **Стандартные** (Рисунок 9).

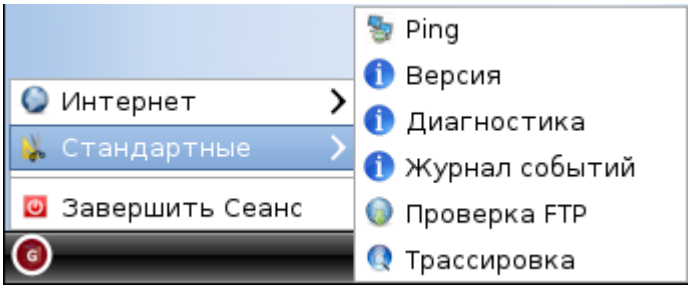

Рисунок 9

Пункты меню: **Проверка FTP**, **Трассировка** и **Ping** вызывают приложения, представляющие собой графическую оболочку для доступа к системным утилитам `wget`, `traceroute` и `ping` соответственно. При вызове вышеуказанных утилит на экране появляется окно, в котором надо ввести IP-адрес диагностируемого сетевого ресурса.

- **Ping** – определяет доступность сетевого устройства (Рисунок 10). Результат работы утилиты отображается в информационном окне (Рисунок 11).

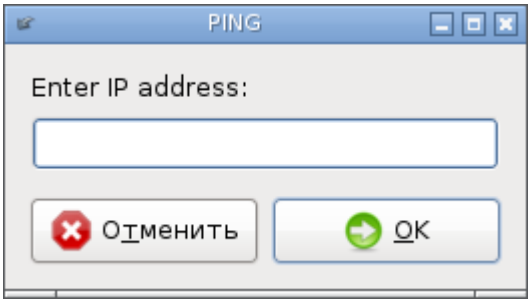

Рисунок 10

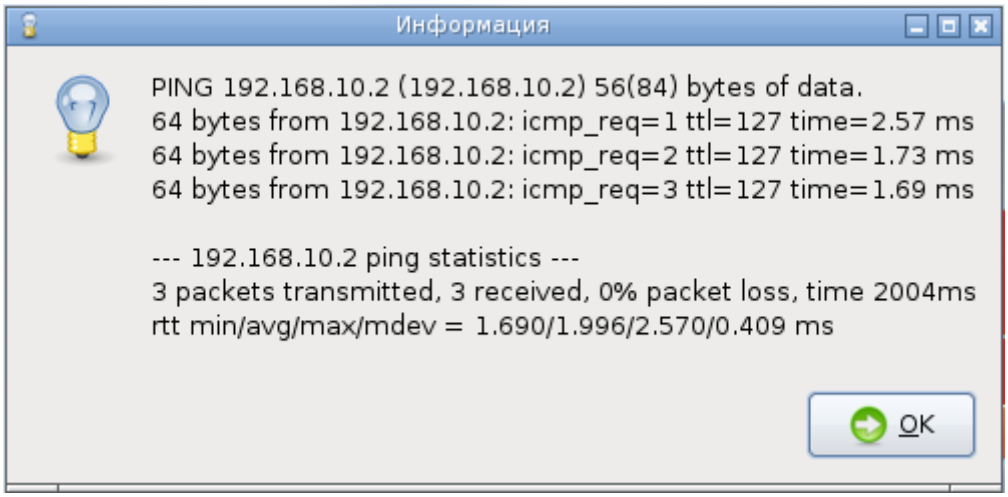

Рисунок 11

- **Проверка FTP** – определяет доступность FTP-сервера (Рисунок 12). Результат работы утилиты отображается в информационном окне (Рисунок 13).

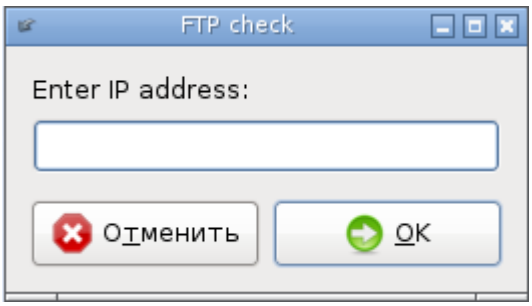

Рисунок 12

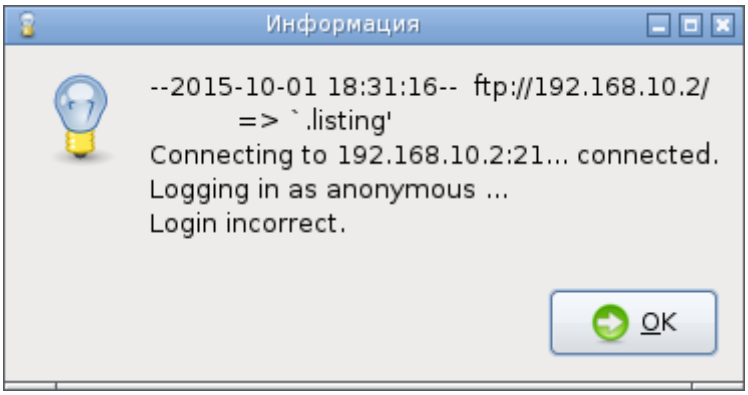

Рисунок 13

- **Трассировка** – выполняется трассировка маршрута до заданного целевого узла (Рисунок 14). Результат работы утилиты отображается в информационном окне (Рисунок 15).

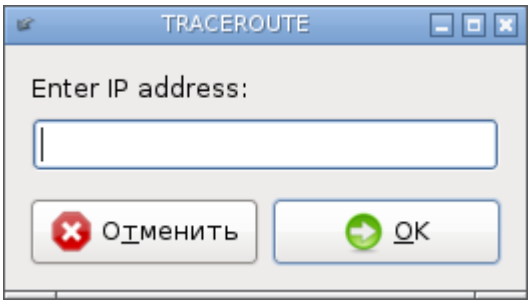

Рисунок 14

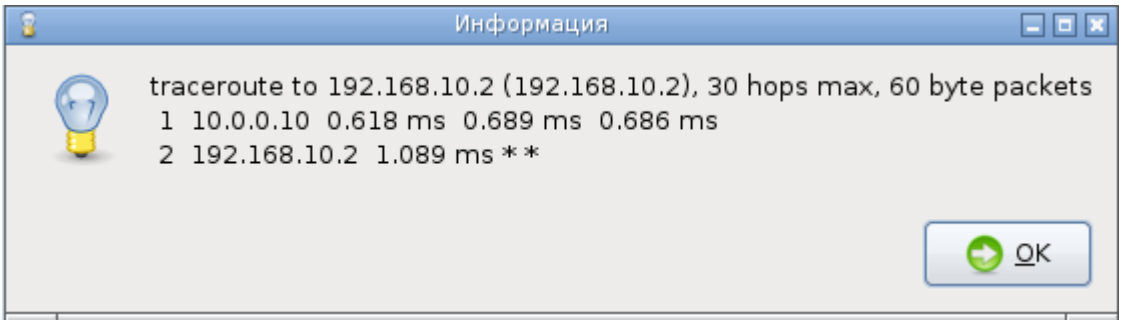

Рисунок 15

Пункт меню **Диагностика** вызывает специализированные информационные команды (Рисунок 16), входящие в состав С-Терра Шлюз и позволяющие получить данные о сертификатах и предопределенных ключах, зарегистрированных в базе Продукта, о параметрах сетевых интерфейсов, созданных защищенных соединениях, лицензии на Продукт, лицензии на продукт КриптоПро CSP.

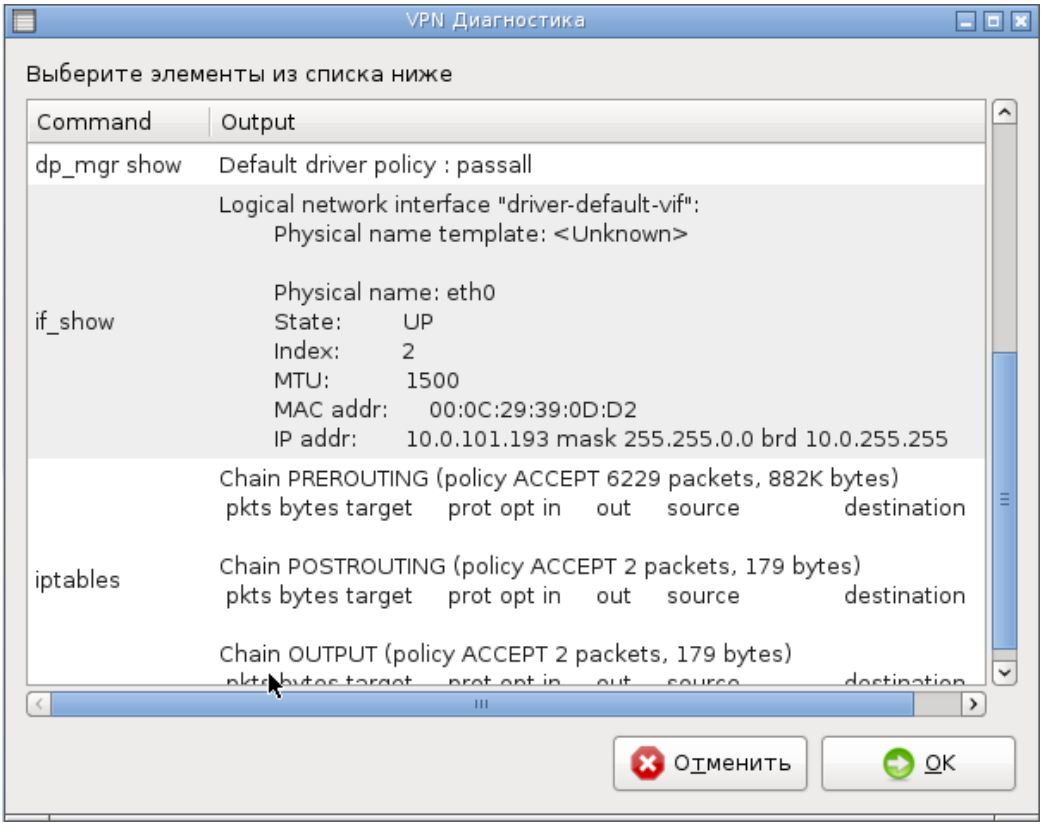

Рисунок 16

Рассмотрим эти команды подробнее:

- `sa_mgr show` выводит информацию обо всех IPsec SA, ISAKMP SA и их состоянии, и о количестве IKE обменов;
- `cert_mgr show` позволяет просмотреть сертификаты и список отозванных сертификатов, размещенных в файле или базе Продукта;
- `cert_mgr check` предназначена для проверки сертификатов, находящихся в базе Продукта;
- `key_mgr show` показывает предопределенные ключи, зарегистрированные в базе Продукта;
- `lic_mgr show` выводит информацию о текущей лицензии на продукт С-Терра Шлюз;
- `cpro lic` выводит информацию о текущей лицензии на продукт КриптоПро CSP;
- `dp_mgr show` предназначена для просмотра установленных настроек политики драйвера по умолчанию;
- `if_show` предназначена для просмотра логических, физических имен и других параметров сетевых интерфейсов;
- `iptables` выводит информацию о правилах iptables, которые задаются администратором в «С-Терра КП 4.1» (настройки EX_SRC_IP и EX_DST_IP_<N>).

Выбор пункта меню **Журнал событий** вызывает окно с вкладками для различных групп протоколируемых событий С-Терра «Пост». В правом нижнем углу каждой вкладки расположены кнопки Обновить и Закрыть, позволяющие обновить информацию о событиях, либо закрыть окно. Рассмотрим подробнее вкладки:

- **cspvpngate.log** - позволяет посмотреть журнал протоколирования событий VPN сервиса (Рисунок 17). Информация, выводимая в этом окне, может быть полезна при первичной диагностике проблем построения защищенного соединения и предназначена, прежде всего, администратору.

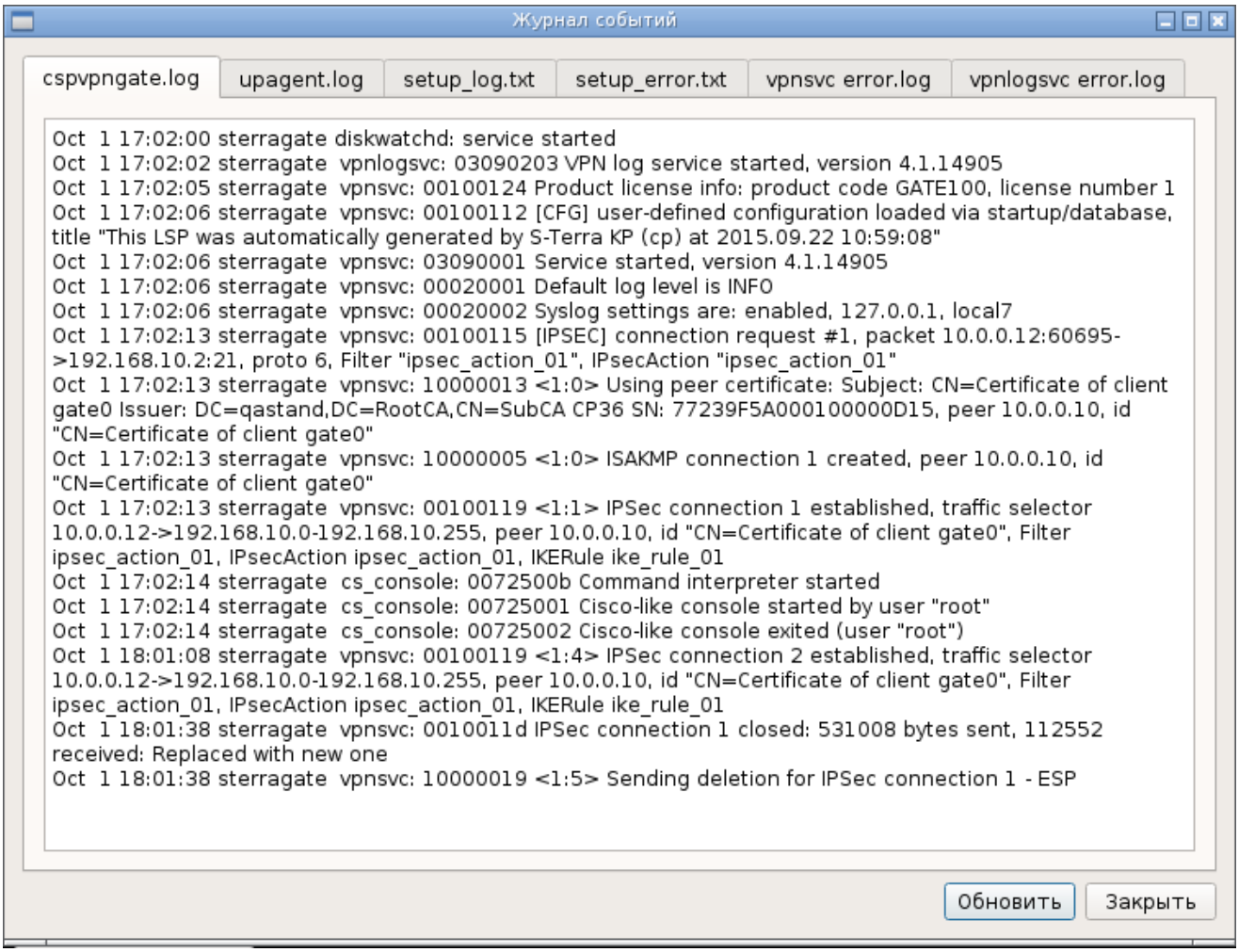

Рисунок 17

- **upagent.log** – позволяет посмотреть журнал протоколирования событий, связанных с обновлением настроек на С-Терра «Пост» (Рисунок 18).

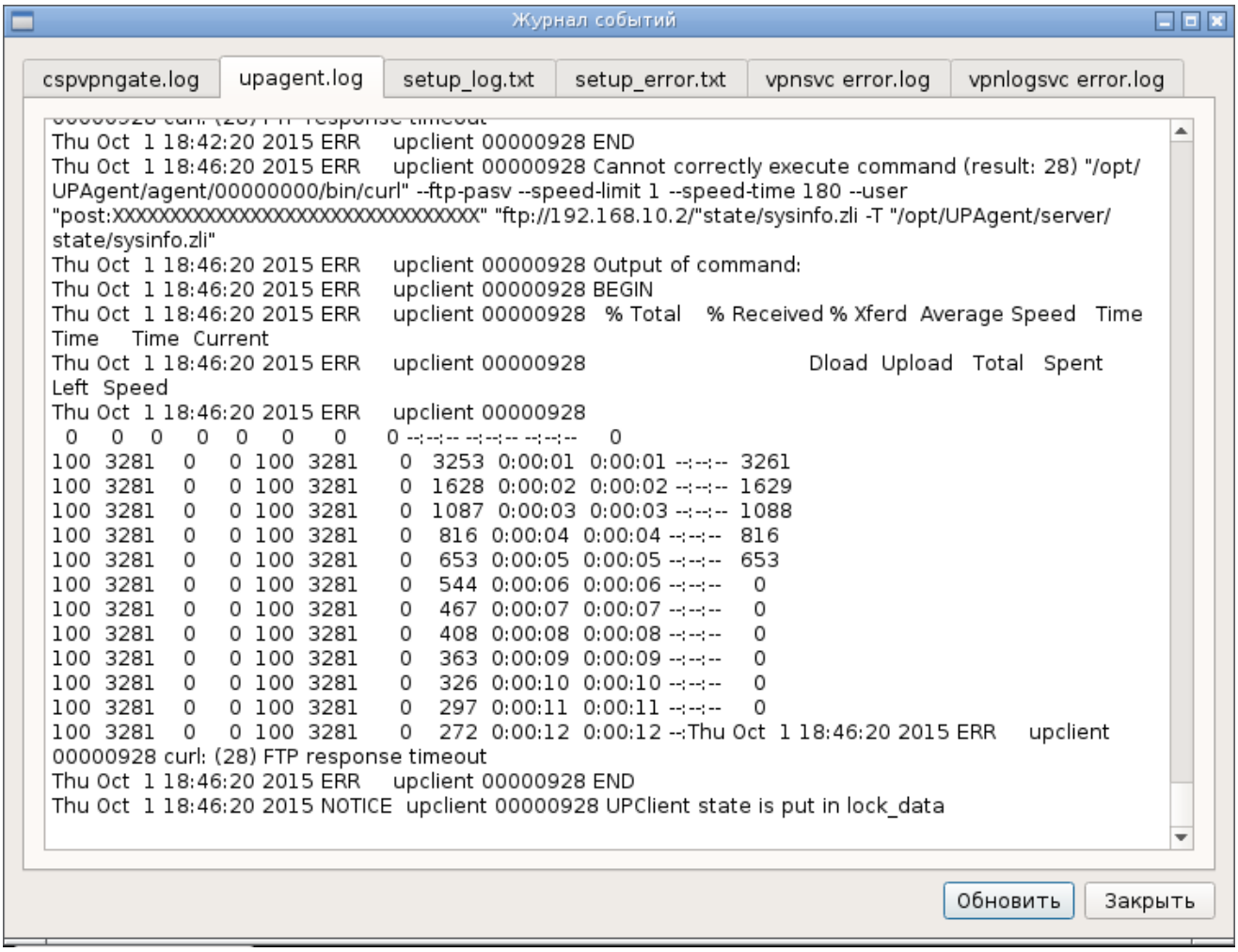

Рисунок 18

- **setup_log.txt** – выводит информацию об успешной инициализации продукта и установке клиента управления (Рисунок 19).

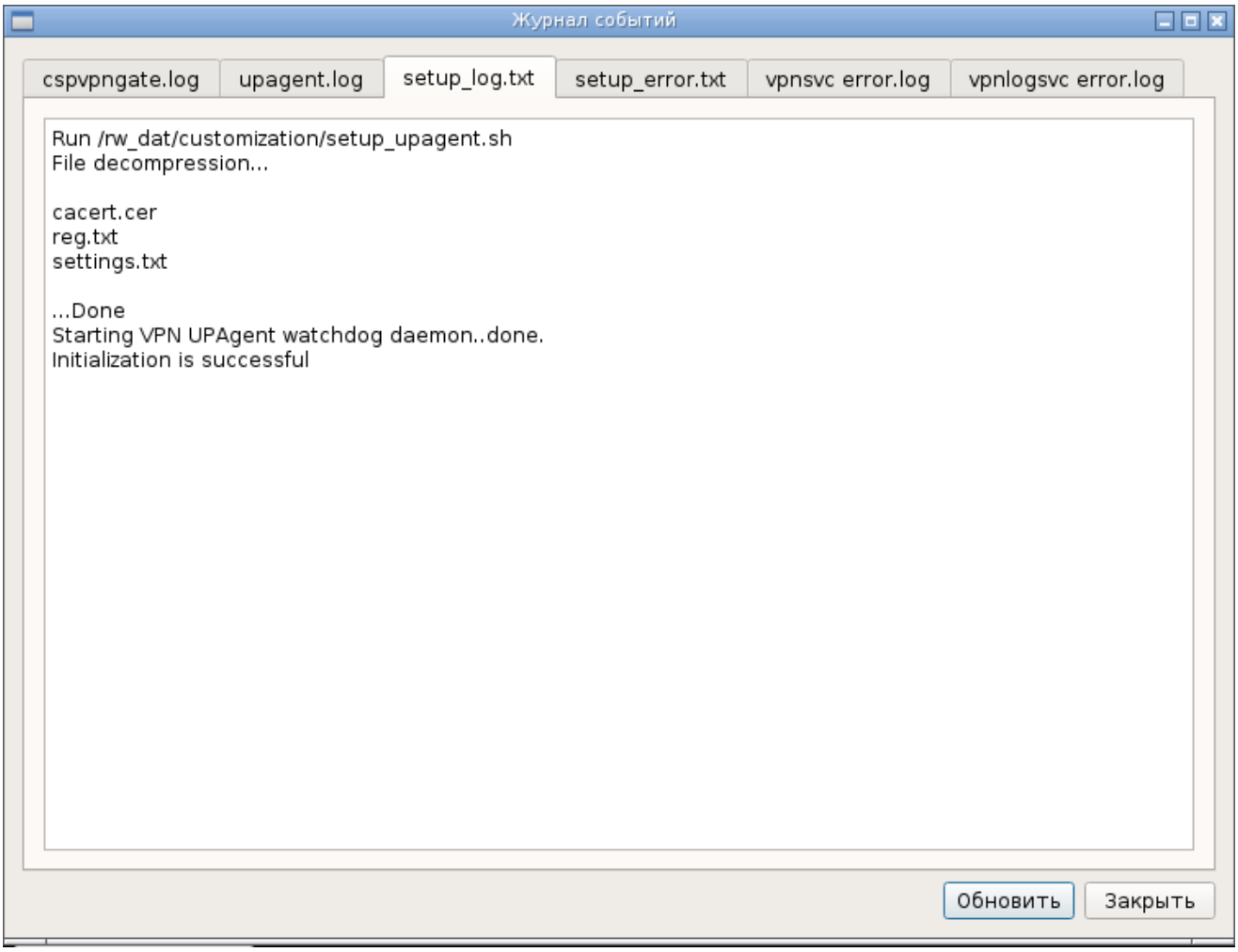

Рисунок 19

- **setup_error.txt** – выводит сообщения об ошибках в случае неуспешной инициализации.
- **vpnsvc error.log** – выводит сообщения об ошибках при неуспешном запуске IPsec демона.
- **vpnlogsvc error.log** – выводит сообщения об ошибках при неуспешном запуске vpnlogsvc.

Пункт меню **Версия** позволяет просмотреть сведения о версии установленного С-Терра Шлюз, операционной системе и краткую информацию о лицензии (Рисунок 20).

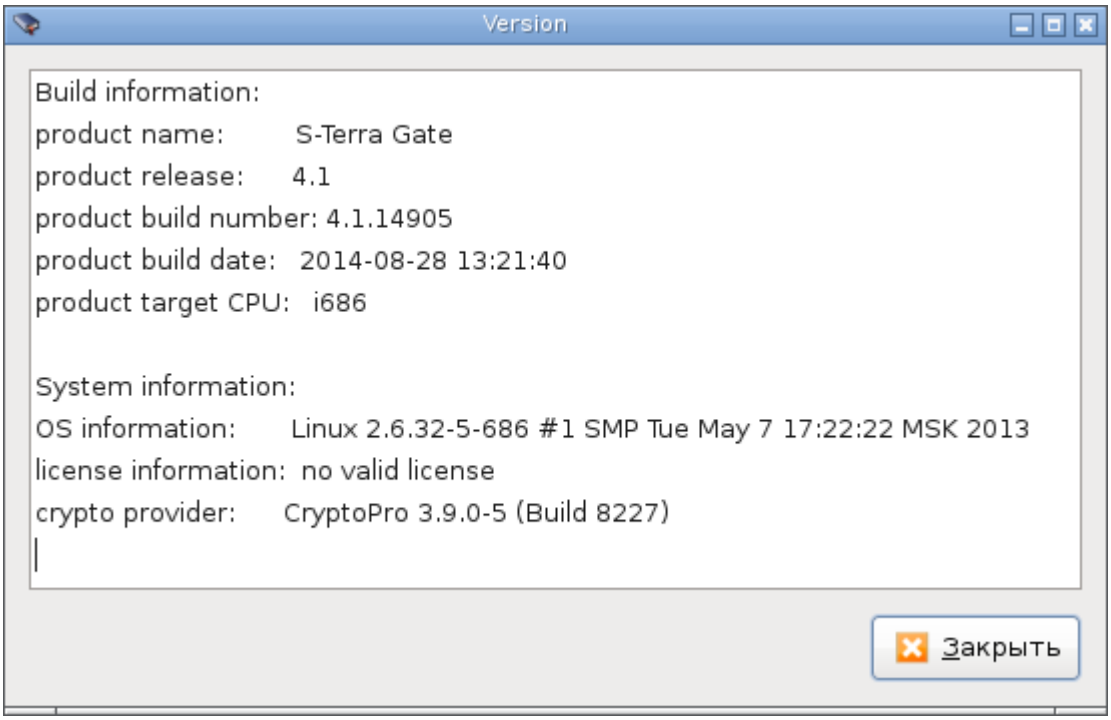

Рисунок 20

3.1. Дополнительная функциональность

Пользователь может посмотреть состояние защищенного соединения, которое отображается иконкой в правом нижнем углу рабочей панели (Таблица 1):

VPN соединение отсутствует	
Установлено соединение VPN	
VPN-сервис остановлен	

Таблица 1

Список доступных «горячих» клавиш приведен в Таблица 2**.**

Win+R	открыть меню запуска программ
Alt+Tab	переключить текущее активное окно на следующее
Alt+Shift+Tab	переключить текущее активное окно на предыдущее
Alt+F4	закрыть окно
Win+D	свернуть\развернуть все окна
Ctrl+Alt+Enter	переключить окно RDP-сессии в режим «На весь экран» и обратно

Таблица 2

4. Приложение

4.1. Процесс загрузки С-Терра «Пост» 4.1

Обратите внимание! Загрузка С-Терра «Пост» 4.1 может занимать до 3 минут. Если загрузка занимает больше времени, убедитесь, что выполнены все рекомендации, представленные выше.

Меню ввода PIN (Рисунок 21).

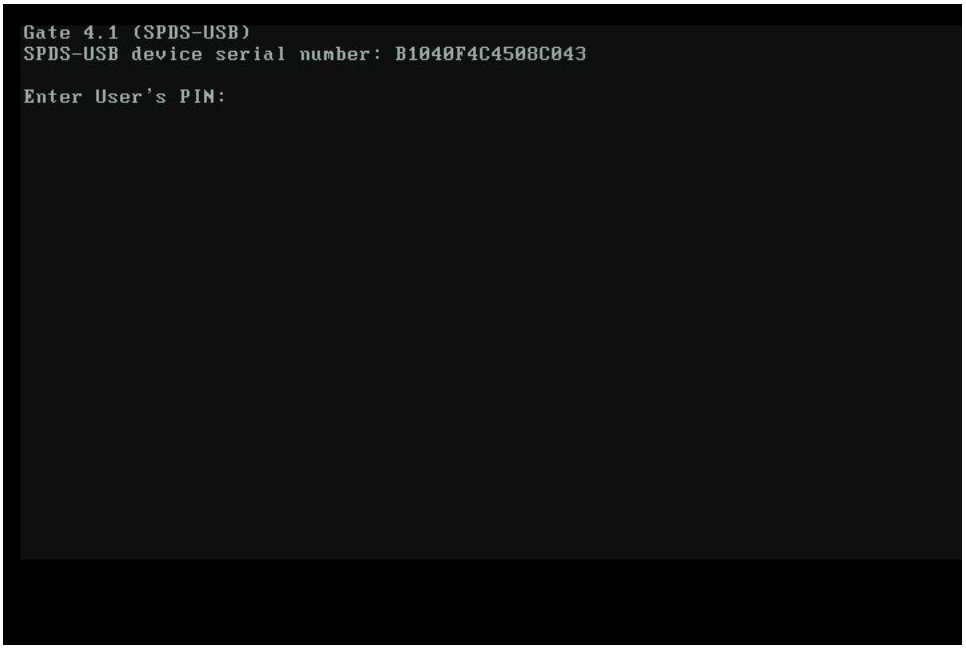

Рисунок 21

Загрузка после ввода PIN (Рисунок 22).

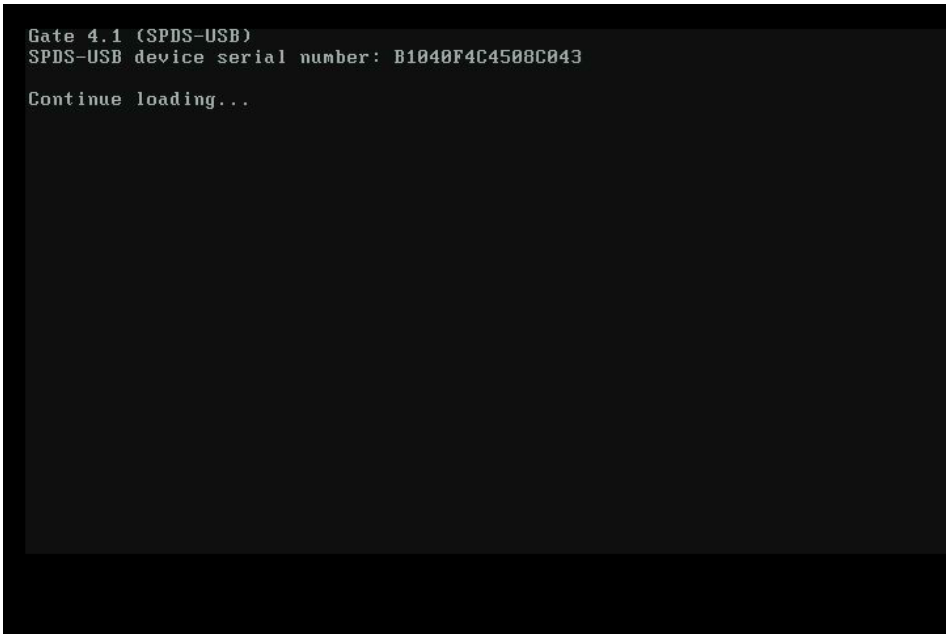

Рисунок 22

Загруженная ОС (Рисунок 23).

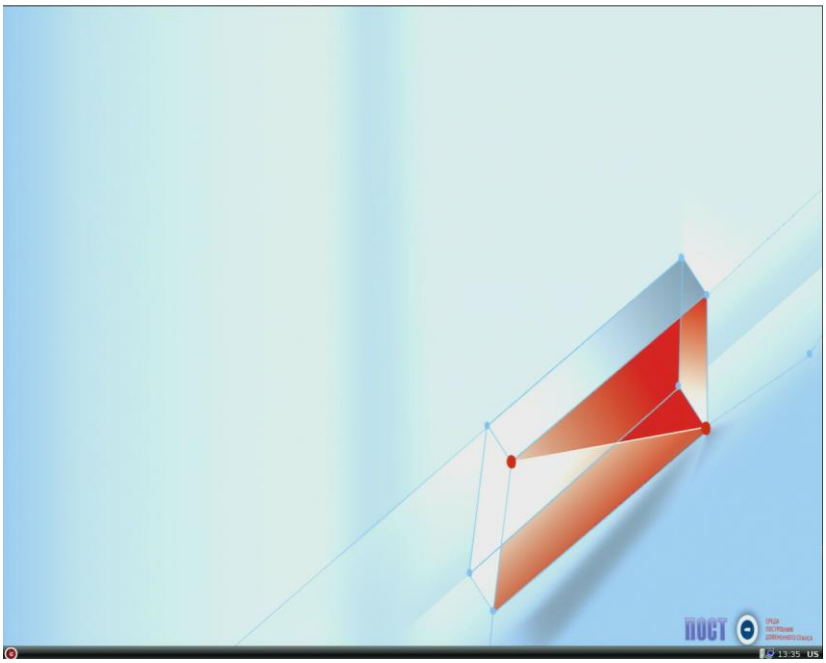

Рисунок 23

