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	3
2.	Работа с С-Терра «Пост»	4
2.1.	Начало работы	4
2.2.	Обновление настроек Продукта	6
2.3.	Диагностическая информация	6
2.4.	Завершение работы с С-Терра «Пост»	7
3.	Диагностические утилиты	8
3.1.	Дополнительная функциональность	15
4.	Приложение	16
4.1.	Процесс загрузки С-Терра «Пост» 4.1	16

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 C-Teppa «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 <u>«Руководстве администратора»</u>. Далее рассмотрим работу с С-Терра «Пост» в режиме пользователя.

2.1. Начало работы

Подключите специальный загрузочный носитель к USB-порту выключенного компьютера (APM). 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

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

12	RDP-сессия	_ 0 🗙
Введ	ите IP-адрес:	
192.	168.10.3	
8	О <u>т</u> менить	<mark>0</mark> ок



- 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.

 Интернет Стандартные 	> >	Удаленный рабочий стол Удаленный рабочий стол (Без настроек)				
📴 Завершить Сеан	нс					
0						
	Рисунок 4					
📽 RDР-сессия 🔲 🖬 🕷						
Введите IP-адрес:						
Отменить						

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.

Упорядочить 🔻 Общий дос	туп 🔻 Записать на оптический диск Новая г	тапка		
🜉 Компьютер	🖀 3460673A02068604-20150608-144353-on.zip	08.06.2015 10:43	Архив ZIP - WinR	20 K
🏭 Локальный диск (С:)	🔚 3460673A02068604-20150608-144711-off.zip	08.06.2015 10:49	Архив ZIP - WinR	68 k
👝 DATA (E:)	🔚 3460673A02068604-20150608-144711-on.zip	08.06.2015 10:47	Архив ZIP - WinR	20 K
👝 Съемный диск (F:)	🔚 3460673A02068604-20150608-144711-run.zip	08.06.2015 10:49	Архив ZIP - WinR	49 k
🚗 Съемный диск (G:)	🔚 3460673A02068604-20150819-194703-on.zip	19.08.2015 16:47	Архив ZIP - WinR	24 H
🕳 gate-dat (H:)	🔚 3460673A02068604-20150819-194703-run.zip	19.08.2015 23:22	Архив ZIP - WinR	72 k
👝 Съемный диск (I:)	🔚 liveusb_demo-20150427-122336-off.zip	27.04.2015 8:28	Архив ZIP - WinR	78 k
👝 Съемный диск (J:)	liveusb demo-20150427-122336-run.zip	27.04.2015 8:27	Архив ZIP - WinR	55 F

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).

s•terra
Завершить сеанс?
Выключить
8 О <u>т</u> менить

Рисунок 8

3. Диагностические утилиты

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

12	PING	_ = ×
Enter	IP address:	
8	О <u>т</u> менить	<u>о</u> к

Рисунок 10

8	Информация 🗖 🗖 🗙
9	PING 192.168.10.2 (192.168.10.2) 56(84) bytes of data. 64 bytes from 192.168.10.2: icmp_req=1 ttl=127 time=2.57 ms 64 bytes from 192.168.10.2: icmp_req=2 ttl=127 time=1.73 ms 64 bytes from 192.168.10.2: icmp_req=3 ttl=127 time=1.69 ms 192.168.10.2 ping statistics 3 packets transmitted, 3 received, 0% packet loss, time 2004ms rtt min/avg/max/mdev = 1.690/1.996/2.570/0.409 ms

Рисунок 11

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

С-Терра «Пост». Руководство пользователя

12	FTP cheo	:k	
Enter	IP address:		
		<u> </u>	
	Отменить		

Рисунок 12



Рисунок 13

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

12	TRACEROU	TE 💶 🖬 🗙
Enter	P address:	
	<u>т</u> менить	<u>o</u> k

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.

С-Терра «Пост». Руководство пользователя

]	VPN Диагностика	
Выберите элем	енты из списка ниже	
Command	Output	^
dp_mgr show	Default driver policy : passall	
	Logical network interface "driver-default-vif": Physical name template: <unknown></unknown>	
if_show	Physical name: eth0 State: UP Index: 2 MTU: 1500 MAC addr: 00:0C:29:39:0D:D2 IP addr: 10.0.101.193 mask 255.255.0.0 brd 10.0.255.255	5
iptables	Chain PREROUTING (policy ACCEPT 6229 packets, 882K bytes) pkts bytes target prot opt in out source destination Chain POSTROUTING (policy ACCEPT 2 packets, 179 bytes) pkts bytes target prot opt in out source destination Chain OUTPUT (policy ACCEPT 2 packets, 179 bytes) pkts bytes target prot opt in out source destination	on E
<		>
	😢 Отменить 💽 📀 О	к

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).

	Жур	нал событий		_ 0 ×
			Y	
cspvpngate.log upagent.log	setup_log.txt	setup_error.txt	vpnsvc error.log	vpnlogsvc error.log
00000020 can. (20) 1 11 respon	Je timeout			
Thu Oct 1 18:42:20 2015 ERR	upclient 000009	28 END		
Thu Oct 1 18:46:20 2015 ERR	upclient 000009	28 Cannot correct	ly execute command	d (result: 28) "/opt/
UPAgent/agent/0000000/bin/c	url"ftp-pasvsp	eed-limit 1speed	-time 180user	IDA an anti (an an an a'
state/svsipfo_zli"	ххххххххх "тtp://	.92.168.10.2/"state	e/sysinfo.zii -1 "/opt/u	DPAgent/server/
Thu Oct 1 18:46:20 2015 EBB	upclient 000009	28 Output of comr	nand:	
Thu Oct 1 18:46:20 2015 ERR	upclient 000009	28 BEGIN		
Thu Oct 1 18:46:20 2015 ERR	upclient 000009	28 % Total % R	eceived % Xferd Ave	erage Speed Time
Time Time Current				
Thu Oct 1 18:46:20 2015 ERR	upclient 000009	28	Dload Upload	Total Spent
Thu Oct 1 19:46:20 2015 EPP	unclient 00000	20		
	0:::::	0		
100 3281 0 0 100 3281	0 3253 0:00:0)1 0:00:01:: 3	3261	
100 3281 0 0 100 3281	0 1628 0:00:0)2 0:00:02::]	L629	
100 3281 0 0 100 3281	0 1087 0:00:0)3 0:00:03::]	1088	
	0 816 0:00:0	4 0:00:04:: 8	316	
	0 53 0:00:0	5 0:00:05:: (0	
100 3281 0 0 100 3281	0 467 0:00:0	7 0:00:07::	õ	
100 3281 0 0 100 3281	0 408 0:00:0	8 0:00:08::	0	
100 3281 0 0 100 3281	0 363 0:00:0	9 0:00:09::	0	
100 3281 0 0 100 3281	0 326 0:00:1	0 0:00:10::	0	
	0 29/ 0:00:1	1 0:00:11:: 2 0:00:12 .Thu 0	0	EBB updiant
00000928 curl: (28) ETP respon	0 272 0:00:1	2 0:00:12: mu 0	CC 1 18:40:20 2015	ERR upclient
Thu Oct 1 18:46:20 2015 ERR	upclient 000009	28 END		
Thu Oct 1 18:46:20 2015 NOTIO	E upclient 00000	928 UPClient state	e is put in lock_data	
			—	-
			ſ	Обновить Закрыть
			L	

Рисунок 18

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

			Жур	нал событий		E		
cs	pvpngate.log	upagent.log	setup_log.txt	setup_error.txt	vpnsvc error.log	vpnlogsvc error.log		
P	Run /rw_dat/customization/setup_upagent.sh File decompression							
c r s	acert.cer eg.txt ettings.txt							
s Ir	.Done tarting VPN UP nitialization is s	Agent watchdog uccessful	daemondone.					
					[Обновить Закры	ть	

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.



\$	Version	
Ruild information:		
product porpor	S Torro Coto	
product name:	S-lerra Gale	
product release:	4.1	
product build numb	er: 4.1.14905	
product build date:	2014-08-28 13:21:40	
product target CPU	i686	
System information	:	
OS information:	Linux 2.6.32-5-686 #1 SMP Tue May 7 17:22:22 MSK 20	13
license information:	no valid license	
crypto provider:	CryptoPro 3.9.0-5 (Build 8227)	
	🔀 <u>З</u> акр	ыть

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	2



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





Рисунок 23