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 администратора

18.03.2016

Содержание

1.	ŀ	Комплект поставки	3
2.	Г	Тодготовка С-Терра «Пост» к работе	4
3.	F	Работа с С-Терра «Пост»	5
	3.1.	Административный режим	5
	3.2.	Пользовательский режим	6
	3.	2.1. Завершение работы с С-Терра «Пост»	7
	3.3.	Диагностическая информация	8
	3.4.	Обновление настроек Продукта	8
4.	F	^р уководство по быстрому старту	9
	4.1.	Смена PIN-кода Администратора	9
	4.2.	Смена PIN-кода Пользователя	.10
	4.3.	Создание Клиента управления	.11
	4.4.	Подготовка скриптов для Клиента управления С-Терра «Пост»	.18
	4.5.	Настройка функционального программного обеспечения	.20
	4. co	5.1. Применение расширенных настроек до построения защищенного рединения с "С-Терра КП"	23
5.	Г	Триложение	.25
	5.1.	Процесс загрузки С-Терра «Пост» 4.1	.25

1. Комплект поставки

Продукт «С-Терра «Пост». Версия 4.1» поставляется в следующей комплектации:

- Специальный загрузочный носитель C3H «СПДС-USB-01» (общий объем 2ГБ или 4ГБ), на котором находится специальное и пользовательское программное обеспечение:
 - операционная система Debian GNU/Linux 6;
 - подготовленные к инициализации продукты: «Программный комплекс С-Терра Шлюз. Версия 4.1» и «КриптоПро CSP» версии 3.9:
 - пользовательское программное обеспечение.
- Компакт-диск «С-Терра «Пост». Версия 4.1. Релиз 14905». Диск содержит дистрибутивы продуктов S-Terra Gate 4.1, S-Terra KP 4.1, SPDS Editor и документацию по этим продуктам.
- Компакт-диск «S-Terra Post Disk Image» для восстановления образа C-Teppa «Пост».
- Копия сертификата соответствия ФСБ России.
- Лицензия на использование «Программного комплекса С-Терра Шлюз. Версия 4.1».
- Лицензия на использование программного продукта «КриптоПро CSP».

2. Подготовка С-Терра «Пост» к работе

Перед началом работы с Продуктом ознакомьтесь с Правилами пользования.

Подготовка С-Терра «Пост» к работе выполняется администратором.

Администратору потребуется выделенный компьютер под управлением OC Windows Server, на котором должны быть установлены:

- СКЗИ «КриптоПро CSP»,
- Сервер управления (продукт «С-Терра КП»),
- Программа персонализации «С-Терра Редактор СПДС» (инсталляционный файл размещен в каталоге SPDSEditor\setup.exe на диске с продуктом).

Сервер управления необходимо дополнительно настроить. Установка и настройка Сервера управления описаны в документе «Программный продукт «С-Терра КП. Версия 4.1» (http://www.s-terra.com/documents/R41/KP/S-Terra_KP_Admin_Guide.pdf).

Следует обратить внимание на задание дополнительных настроек для центрального шлюза, описанных в шаге 2 раздела 13.2.1 документа «Программный продукт «С-Терра КП. Версия 4.1» (<u>http://www.s-terra.com/documents/R41/KP/S-Terra_KP_Admin_Guide.pdf</u>).

Изначально на специальном загрузочном носителе C3H «СПДС-USB-01» установлено СКЗИ «С-Терра Шлюз» и пользовательское программное обеспечение, а также размещен дистрибутив Клиента управления.

Для проведения процедуры инициализации Администратор подключает специальный загрузочный носитель к USB-порту Сервера управления С-Терра КП и выполняет следующие действия:

- Устанавливает PIN администратора и PIN пользователя для доступа к специальному загрузочному носителю.
- Создает на Сервере управления Клиента управления для С-Терра «Пост».
- Формирует политику безопасности для пользователя С-Терра «Пост» и задает необходимые настройки.
- Создает установочные скрипты для Клиента и доставляет их на СЗН.
- Создает контейнер с ключевой парой и сертификатом и сохраняет их на СЗН.
- Подключает С-Терра «Пост» к тестовой аппаратной платформе для проведения инициализации и тестовой проверки.
- Создает на Сервере управления расширенное обновление с настройками функционального программного обеспечения.
- Отслеживает успешное применение обновления.
- Выключает тестовую аппаратную платформу.

В результате вышеописанных действий устройство готово к работе и может быть передано пользователю.

Дальнейшее техническое обслуживание продукта С-Терра «Пост» может выполняться дистанционно, по защищенному каналу, с рабочего места администратора С-Терра Шлюз с использованием встроенных в С-Терра «Пост» средств и при помощи Сервера управления и Клиента управления.

3. Работа с С-Терра «Пост»

С-Терра «Пост» поддерживает два режима работы

- Административный режим предназначен для Администратора и предоставляет возможность изменить PIN администратора, разблокировать PIN пользователя.
- Пользовательский режим предоставляет доступ к пользовательскому программному обеспечению.

Перейти в Административный режим работы возможно только во время загрузки.

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

Во время загрузки имеется возможность перейти в административный режим (Рисунок 1). Для входа требуется нажать клавишу «А», в противном случае, через 5 секунд начнется загрузка в пользовательском режиме.



Рисунок 1

Далее рассмотрим оба режима работы.

3.1. Административный режим

При входе в административный режим запрашивается PIN администратора:

```
Enter Administrator's PIN:
```

PIN-код Администратора и Пользователя по умолчанию: 12345678. При первичной инициализации PIN-коды необходимо сменить.

Примечание: Если PIN введен неправильно, дается еще 4 попытки, после чего специальный загрузочный носитель будет заблокирован и восстановлению не подлежит. Дальнейшее использование С-Терра «Пост» невозможно. При возникновении подобной ситуации обращайтесь в службу поддержки <u>support@s-terra.ru</u>.

В случае успешной аутентификации будет предложено выбрать одно из действий (Рисунок 2).

Gate 4.1 (SPDS-USB): Administrator mode SPDS-USB device serial number: 358107E4F9008BFD Press next keys to select sub-mode: 1. To change SPDS-USB Administrator's PIN 2. To unblock SPDS-USB User's PIN 3. To SPDS-USB image recovery 4. To continue OS loading

Рисунок 2

При выборе **To change SPDS-USB Administrator's PIN** – изменение PIN администратора С-Терра «Пост» будет предложено ввести новый PIN администратора и подтвердить его повторным вводом:

Enter new Administrator's PIN:

Retype new Administrator's PIN:

Длина пароля должна быть не менее 8 символов, пароль может содержать цифры, буквы верхнего и нижнего регистров, специальные символы: (@, #, \$, &, *, % и т.п.).

При несовпадении введенных PIN-кодов будет выведено сообщение: New PINs not match и будет предложено заново ввести PIN администратора. При совпадении введенных PIN-кодов выводится сообщение Administrator's PIN changed и предлагается нажать любую клавишу для перехода в административный режим.

При выборе **To unblock SPDS-USB User's PIN** – восстановление PIN пользователя С-Терра «Пост» будет предложено ввести новый PIN пользователя и подтвердить его повторным вводом:

```
Enter new User's PIN:
Retype new user's PIN:
```

Длина пароля должна быть не менее 4 символов, пароль может содержать цифры, буквы верхнего и нижнего регистров, специальные символы: (@, #, \$, &, *, % и т.п.). При совпадении введенных PIN-кодов выводится сообщение User's PIN unblocked и предлагается нажать любую клавишу для перехода в административный режим. При несовпадении введенных PIN-кодов будет выведено сообщение: New PINs not match и будет предложено заново ввести PIN пользователя.

Выбор действия **To SPDS-USB image recovery** запускает процесс восстановления образа С-Терра «Пост» с диска **S-Terra Post Disk Image**. Подробнее процедура восстановления описана в документе «Программный комплекс С-Терра Шлюз. Версия 4.1. Руководство администратора. Инструкции по восстановлению и обновлению ПАК» (<u>http://www.s-</u> <u>terra.com/documents/R41/Gate/Restore_image.pdf</u>), в разделе «Инструкция по восстановлению ПАК с S-Terra Gate, предустановленным на СЗН «СПДС-USB-01», и С-Терра «Пост»».

3.2. Пользовательский режим

Пользовательский режим по умолчанию запускается во время загрузки со специального загрузочного носителя.

Запрашивается PIN пользователя. После аутентификации пользователь получает доступ целевому программному обеспечению. Запуск целевого приложения доступен из пункта меню **Интернет** (Рисунок 3).

🔮 Интернет 💦 🔪	😫 Удаленный рабочий стол (Без настроек)
以 Стандартные 💦	
🖸 Завершить Сеанс	
(

Рисунок 3

В режиме пользователя доступны диагностические утилиты. Запуск утилит осуществляется из меню рабочей панели, раздел **Стандартные** (Рисунок 4).





Подробное описание утилит дано в <u>«Руководстве пользователя»</u>, в разделе «Диагностические утилиты».

По иконке в правом нижнем углу рабочей панели пользователь может определить наличие защищенного соединения (*Таблица* 1).

Таблица 1

Наличие защищенного соедин	ения
VPN соединение отсутствует	
Установлено соединение VPN	
VPN-сервис остановлен	2

Работа в пользовательском режиме подробнее описана в «Руководстве пользователя».

3.2.1. 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 5).



Рисунок 5

Появляется окно с выбором подтверждения выключения С-Терра «Пост» либо отменой действия (Рисунок 6).



Рисунок 6

3.3. Диагностическая информация

Диагностическая информация собирается для каждого сеанса и записывается на C3H «СПДС-USB-01 в каталог disk/diaginfo в виде архивного файла.

Имя архивного файла содержит идентификатор данного экземпляра С-Терра «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 С-Терра «Пост», 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 «С-Терра Шлюз. Версия 4.1».

3.4. 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. Можно задать подряд несколько обновлений с указанием времени создания каждого, и они будут применены в том порядке, в котором были созданы. Обновление применяется сразу, перезагрузка устройства не требуется. Во время выполнения обновления VPN-сервис может быть остановлен.

Описание создания и применения обновлений с использованием «С-Терра КП 4.1» смотрите в документе «Программный продукт С-Терра КП 4.1» ((<u>http://www.s-</u> terra.com/documents/R41/KP/S-Terra_KP_Admin_Guide.pdf).

4. Руководство по быстрому старту

Данное руководство содержит пошаговое описание ввода в эксплуатацию С-Терра «Пост».

4.1. Смена PIN-кода Администратора

Смена PIN-кода Администратора проводится при помощи программы персонализации «С-Терра Редактор СПДС».

- Шаг 1: Подключите С-Терра «Пост» к свободному USB-разъему Сервера управления.
- Шаг 2: Из пункта системного меню запустите программу «С-Терра Редактор СПДС». Программа выполнит поиск подключенных С-Терра «Пост»
- Шаг 3: В открывшемся окне программы будет отображена информация о найденных устройствах (Рисунок 7).

	🛛 С-Терра Редактор СПДС								
¢	айл Действия PIN-коды Справка								
	Тодключенные устройства:								
	Считыватель	Серийный номер	Размер диска	Доступ	Обновить список устройств				
	S-Terra CSP Specialized Bootable Storage 0	3460D65102101100	2F6	Чтение	Открыть сессию				
					Закрыть сессию				
					Изменить PIN пользователя Данных				
					Изменить PIN пользователя				
					Изменить PIN администратора,				
					Изменить транспортный PIN				
					Восстановить PIN-ы по умолчанию				

Рисунок 7

Шаг 4: Измените заводское значение PIN-кода Администратора, выбрав запись о нужном устройстве и нажав кнопку Изменить PIN администратора (Рисунок 8).

🗔 С-Терра Редактор СПДС				
Файл Действия PIN-коды Справка	1			
Подключенные устройства:				
Считыватель	Серийный номер	Размер диска	Доступ	Обновить список устройств
S-Terra CSP Specialized Bootable Storage 0	478107B602018BFD		Чтение/Запись	
				Открыть сессию
				Закрыть сессию
				Изменить PIN пользователя данных
				Изменить PIN пользователя
				Изменить PIN администратора
				Изменить транспортный PIN
				Восстановить PIN-ы по умолчанию

Рисунок 8

Шаг 5: В появившемся окне в поле PIN администратора: введите значение действующего PIN-кода Администратора. Если С-Терра «Пост» новый – введите PIN-код по умолчанию: 12345678. В поле Новый PIN: введите значение нового PIN-кода. В поле Подтверждение PIN: значение нового PIN-кода требуется повторить (Рисунок 9). Нажмите кнопку ОК.

Изменение PIN администратора					
PIN администратора:					

Новый PIN:	Сложность PIN:				
*****	Очень Высокая				
Подтверждение PIN:					

ОК	Отмена				

Рисунок 9

Шаг 6: Если был введен верный действующий PIN-код администратора и значения нового PIN-кода, в полях Новый PIN, Подтверждение PIN совпадают, то окно закроется без каких-либо сообщений. PIN-код администратора успешно изменен.

4.2. Смена PIN-кода Пользователя

Изменение PIN-кода пользователя производится аналогично изменению PIN-кода администратора. Для вызова окна изменения пользовательского PIN-кода нажмите кнопку Изменить PIN пользователя. В открывшемся окне в поле PIN администратора введите действующий PIN-код администратора, в полях Новый PIN и Подтверждение PIN - новый PIN-код пользователя (Рисунок 10). Нажмите кнопку OK. Если все сделано верно, то окно будет закрыто без каких-либо сообщений. PIN-код пользователя успешно изменен.

Изменение PIN пользователя						
PIN администратора:						

Новый PIN:	Сложность PIN:					
****	Очень Высокая					
Подтверждение PIN:						

ОК	Отмена					

Рисунок 10

4.3. Создание Клиента управления

Для настройки и проведения обновлений необходимо зарегистрировать новый С-Терра «Пост» на Сервере управления С-Терра КП. Для этого требуется создать Клиента управления.

Внимание: запись контейнера к локальному сертификату Клиента управления производится в paздел /gate_dat на C-Teppa «Пост». Этот paздел по умолчанию доступен в режиме «только для чтения». Для того, чтобы paзрешить запись в него, требуется открыть сессию пользователя. Эта процедура выполняется при помощи программы «С-Teppa Peдактор СПДС».

- Шаг 1: Запустите программу из системного меню «Пуск», в списке доступных устройств выберите требуемую запись.
- Шаг 2: Нажмите кнопку «Открыть сессию» для открытия Раздела данных на запись.
- Шаг 3: В окне Авторизация введите PIN пользователя и нажмите OK (Рисунок 11).

🔜 С-Терра Редактор СПДС				
Файл Действия PIN-коды Справ	a			
Подключенные устройства:				
Считыватель	Серийный номер	Размер диска	Доступ	Обновить список устройств
S-Terra CSP Specialized Bootable Storage	0 47810786020188FD		Чтение	
			-	Открыть сессию
	AB	оризация	×	
	PI	N пользователя:		Закрыть сессию
	*	*******		Изменить PIN пользователя
	_			данных
		ок о	тмена	Изменить PIN пользователя
				Изменить РІМ администратора
				Изменить транспортный PIN
				Восстановить PIN-ы по умолчанию
1				

Рисунок 11

Шаг 4: Устройство С-Терра «Пост» готово для записи (Рисунок 12).

	С-Терра Редак	тор СПДС					
¢	айл Действия	PIN-коды	Справка				
Г	юдключенные устр	ойства:					
	Считыватель			Серийный номер	Размер диска	Доступ	Обновить список устройств
	S-Terra CSP Speciali	zed Bootable (Storage 0	478107B602018BFD		Чтение/Запись	
							Открыть сессию
							Закрыть сессию
							Изменить PIN пользователя данных
							Изменить PIN пользователя
							Изменить PIN администратора
							Изменить транспортный PIN
							Восстановить PIN-ы по умолчанию



Шаг 5: Далее требуется получить сертификат Удостоверяющего центра и выпустить локальный сертификат управляемого устройства. Оба сертификата необходимо

доставить в файловую систему Сервера управления. При генерации запроса на локальный сертификат, в качестве носителя назначения указать предварительно открытый на запись раздел /gate_dat на C-Teppa «Пост» Подробно процедура создания ключевой пары и запроса на сертификат С-Teppa «Пост» описана в документе «Программный продукт «С-Teppa КП. Версия 4.1» (S-Terra_KP\S-Terra_KP_Admin_Guide.pdf) в разделе 12.2.

Шаг 6: На Сервере управления запустите консоль UPServer Console (Пуск-Программы-S-Terra-S-Terra KP-VPN UPServer Console). Во вкладке Clients в контекстном меню (правая кнопка мыши) выберите предложение *Create* для создания учетной записи клиента для устройства C-Teppa «Пост» (Рисунок 13).

👯 ¥PN UPServe	r console							
<u>File G</u> roups <u>C</u> li	ients <u>T</u> ools <u>H</u> elp							
Clients Setting	s							
List of groups	List of groups List of clients							
All clients	Condition							
Office1	gate0 active							
	<u>S</u> how							
	Properties							
	<u>C</u> reate							
	Update							



Шаг 7: В окне создания нового клиента в поле Client ID укажите идентификатор клиента для С-Терра «Пост» и нажмите Е. В составе идентификатора рекомендуется использовать серийный номер устройства, номер лицензии продукта или любой другой идентификатор, подходящий для учета оборудования. В данном случае в качестве идентификатора используется post (Рисунок 14).

Create new client	×
Client ID	post
Product package	E
Device password	
UPAgent settings	C:\ProgramData\UPServer\csettings.txt
	OK Cancel

Рисунок 14

Шаг 8: В окне VPN data maker в поле VPN product в выпадающем меню выберите продукт S-Terra Gate 4.1, а в поле Crypto provider - криптопровайдера CryptoPro. Нажмите кнопку Run Wizard, чтобы использовать окна мастера.

WPN data maker	
File Mode	
VPN product S-Terra Gate 4.1 Crypto provider CryptoPro 💌	
LSP Certificates Keys Settings License Interfaces RNG container Software	
LSP format is cisco-like	
T	
Load from file Check	
Run Wizard OK Canc	el



Шаг 9: В первом окне мастера при аутентификации с использованием сертификатов в области **Trusted certificates** отражается информация о корневом сертификате Удостоверяющего Центра (Trusted CA Certificate).

rusted certificates			
5ubject IN=S-Terra Dem	Issuer . CN=5-Terra De	Serial number 25 37 90 7D 52	Add View Remove
ocal certificates — Subject I=RU,L=Mosco	Issuer Serial nu CN= 67 B4 8.	Container name \\.\HDIMAGE\HDI	MA Modify Remove
reshared keys — Name	Value	Hex value	Add Modify Remove

Рисунок 16

Шаг 10: Для добавления сертификата нажмите кнопку Add, в открывшемся окне выберите файл с CA сертификатом (Рисунок 17). Обязательный параметр.

🎇 Open				×
Program	Data ▼ UPServer ▼ certs	- 🛃	Search	2
🕒 Organize 👻 📗 Views	▼ I New Folder			0
Favorite Links Desktop Computer Documents Pictures Music Recently Changed Searches Public	Name cacert.cer cacertist.p7b certnew.cer gate0.cer post.cer post2.cer workcert.cer	 Date modified 25.05.2015 13:03 25.05.2015 13:03 20.05.2015 13:12 22.05.2015 13:22 26.05.2015 15:22 26.05.2015 12:01 20.05.2015 11:42 25.05.2015 13:04 	Type Size Security Certificate PKCS #7 Certific Security Certificate Security Certificate Security Certificate Security Certificate Security Certificate Security Certificate	▼ Tag 1 KB 1 KB 2 KB 2 KB 2 KB 2 KB 2 KB 1 KB
Folders A	certnew.cer		X.509 Certificate (*.cer	;*.ort;*.j▼ Cancel

Рисунок 17

Шаг 11: В области Local certificates отражается информация о локальном сертификате управляемого устройства. Для этого в конце области нажмите кнопку Add, в открывшемся окне выберите файл с локальным сертификатом (Рисунок 18). Обязательный параметр.

🎆 Open			×
ProgramD	ata 🕶 UPServer 👻 certs	👻 🛃 Search	- 2
🕒 Organize 👻 📗 Views	▼ Sew Folder		0
Favorite Links Desktop Computer Documents Pictures Music Recently Changed Searches Public	Name Cacert.cer	• Date modified • Type • Size 25.05.2015 13:03 Security Certificate 25.05.2015 13:03 PKCS #7 Certific 20.05.2015 13:12 Security Certificate 28.05.2015 12:30 Security Certificate 22.05.2015 15:22 Security Certificate 20.05.2015 15:22 Security Certificate 20.05.2015 12:01 Security Certificate 20.05.2015 11:42 Security Certificate 25.05.2015 13:04 Security Certificate	▼ Tag 1 KB 2 KB 2 KB 2 KB 2 KB 2 KB 1 KB
Folders 🔨	•		
File name	post.cer	X.509 Certificate (*.cer; Open Ca	.crt;*.j 💌

Рисунок 18

Шаг 12: В окне Certificate description в поле Key container name необходимо задать местоположение и имя ключевого контейнера на управляемом устройстве, в который он будет скопирован с USB-флеш при инициализации C-Teppa «Пост».

В поле Key container password укажите пароль к контейнеру. Нажмите ОК.

Field Value Version 3 Serial number 4D 07 0F 22 00 01 00 00 0D 13 Signature algorithm GOST_R_341001_3411 (Crypto-Pro) Issuer DC=qastand,DC=RootCA,CN=SubCA CP36 Valid from Tue May 26 11:47:47 2015 Valid to Thu May 26 11:57:47 2016 Subject C=RU,L=Moscow,O=S-Terra CSP,OU=Development,CN Public key GOST R 341001(512) Alt-subject <none> Hash MD5 3C 37 3F D0 8A BF 39 94 60 74 AA DA EA DC FF B7 Hash SHA1 C8 BC 2C 99 EF 66 DB B0 E8 FD 2F D8 61 16 24 64 FB 2 Key container name \\.\HDIMAGE\HDIMAGE\post Key container password *****</none>	Certificate descripti	on	×
Version 3 Serial number 4D 07 0F 22 00 01 00 00 DD 13 Signature algorithm GOST_R_341001_3411 (Crypto-Pro) Issuer DC=qastand,DC=RootCA,CN=SubCA CP36 Valid from Tue May 26 11:47:47 2015 Valid to Thu May 26 11:57:47 2016 Subject C=RU,L=Moscow,O=S-Terra CSP,OU=Development,CN Public key GOST R 341001(512) Alt-subject <none> Hash MD5 3C 37 3F D0 8A BF 39 94 60 74 AA DA EA DC FF B7 Hash SHA1 C8 BC 2C 99 EF 66 DB B0 E8 FD 2F D8 61 16 24 64 FB 2 Key container name \\.\HDIMAGE\HDIMAGE\\post Key container password *****</none>	Field	Value	Т
Key container name \\.\HDIMAGE\HDIMAGE\\post	Version Serial number Signature algorithm Issuer Valid from Valid to Subject Public key Alt-subject Hash MD5 Hash SHA1	3 4D 07 0F 22 00 01 00 00 0D 13 GOST_R_341001_3411 (Crypto-Pro) DC=qastand,DC=RootCA,CN=SubCA CP36 Tue May 26 11:47:47 2015 Thu May 26 11:57:47 2016 C=RU,L=Moscow,O=S-Terra CSP,OU=Development,CN GOST R 341001(512) <none> 3C 37 3F D0 8A BF 39 94 60 74 AA DA EA DC FF B7 C8 BC 2C 99 EF 66 DB B0 E8 FD 2F D8 61 16 24 64 FB 2</none>	
OK Cancel	Key container name Key container passwo	\ \HDIMAGE \HDIMAGE \\post ord ***** OK Cancel	

Рисунок 19

Note

При создании контейнера к локальному сертификату устройства через вебформу рекомендовано использовать автоматическое задание имени контейнера. Если же имя было задано вручную, необходимо убедиться, что оно не совпадает с именем, прописанным в поле **Key container name** окна **Certificate description** на Сервере управления.

Нажмите кнопку Next в первом окне мастера.

Шаг 13: Во втором окне мастера (Рисунок 20) задайте правило, по которому будет пропускаться трафик от С-Терра «Пост» к Серверу управления и другим ресурсам в защищаемой подсети. Трафик между С-Терра «Пост» и центральным шлюзом должен защищаться по протоколу IPsec, для этого нажмите кнопку Add.

Wizard - make vpn configuration (2/3) × На этом шаге Вам необходимо задать правила обработки сетевого трафика. Добавьте необходимые правила обработки сетевого трафика и нажмите кнопку Next. Rule list: Rule list:								
Interface	Local IP	Partner IP	Services	Action				
Any	Any	Any	Any	Pass				
					Down			
		Add	Edit	Remove				
Load	Save	<	Back	lext > C	ancel			

Рисунок 20

Add Rule	×
Network interface alias	
Local IP Addresses	Partner IP Addresses
Any C Custom	C Any Custom
IP Address Subnet Mask	IP Address Subnet Mask
	192.168.10.0 255.255.255.0
Add Edit Remove	Add Edit Remove
Services and Protocols	Action
Any C Custom	Protect using IPsec
Name Ports	Auth object: Certificate: C=RU,L=Moscow,O=S-Terra
	Local ID: DistinguishedName: C=RU,L=Moscow,O
	Partner ID: Accept any ID
	Tunnel IP Addresses of IPsec partner:
	Use random IP Address order
	10.0.0.10
	Down
	Add Edit Remove
Add Edit Remove	Advanced settings
C Log packet matches	OK Cancel

Рисунок 21

- Шаг 14: В окне Add Rule (Рисунок 21) укажите следующее:
 - в области Local IP Addresses поставьте переключатель в положение Any.
 - в области **Partner IP Addresse**s поставьте переключатель в положение *Custom* и укажите адрес всей подсети Сервера управления, например, 192.168.10.0/24.
 - в области Action укажите IPsec-партнера, с которым будет построено защищенное соединение. Например, адрес интерфейса шлюза 10.0.0.10, защищающего подсеть с Сервером управления.

Нажмите кнопку ОК.

Шаг 15: Увеличьте приоритет созданного правила, используя кнопку Up. Затем нажмите кнопку Next.

Wizard - m	Wizard - make vpn configuration (2/3)								
На этом шаге Добавьте нес	На этом шаге Вам необходимо задать правила обработки сетевого трафика. Добавьте необходимые правила обработки сетевого трафика и нажмите кнопку Next.								
Rule list:									
Interface	Local IP	Partner IP	Services	Action					
Any	Any	192.168.10	Any	Tunnel(10					
Any	Any	Any	Any	Pass	Up Down				
,		Add	Edit	Remove]				
Load	Save	_	Back	Next > C	ancel				

Рисунок 22

Шаг 16: В следующем окне укажите лицензионные данные на продукт S-Terra Gate и СКЗИ «КриптоПро CSP 3.9» (Рисунок 23).

Wizard - make vpn configuration (3/3)								
На этом шаге Вам необходимо задать лицензии для работы VPN-устройства. Задайте параметры лицензий и нажмите кнопку Finish.								
VPN product license —								
Product:	GATE 100							
Customer code:	test							
License number:	1							
License code:	XXXXXXXXXXXXXX							
	Load from file Check License							
Crypto provider licens	2							
Serial number:	3939S-XXXXX-XXXXX-XXXXX-XXXXX							
Load Save < Back Finish Cancel								

Рисунок 23

Шаг 17: Далее нажмите кнопку Save для сохранения данных проекта (Рисунок 24).

Save	×
🕞 🕞 🗸 Local Disk (C:) 🕶 distr 👻	👻 🔽 Search
File name: post	
Save as type: Project file (*.dsc)	<u> </u>
Browse Folders	Save Cancel

Рисунок 24

- Шаг 18: Затем нажмите кнопку Finish.
- Шаг 19: В окне создания нового клиента также нажмите кнопку ОК (Рисунок 25).

Create new client	<u>></u>
Client ID	post
Product package	C:\ProgramData\UPServer\tmp\vpn_product_ E
Device password	
UPAgent settings	C:\ProgramData\UPServer\csettings.txt
	OK Cancel

Рисунок 25



VPN UPServer console						
File Groups Clients Tools	Help					
Cilents Settings						
List of groups	List of clients					
All dients	^ Client ID	Condition	Active updates	Applied updates	Administrative state	Fire time by certificates
Office 1	gate0	active	0	8	enabled	03/06/2016 15:13:02
	post	new	0	0	disabled	
					Show	
					Properties	
					Create	
					Update	
					Functions	F
					Get packages	
					Enable	
					Disable	
					Retry	
					Clear	
					Remove	
-						

Рисунок 26

4.4. Подготовка скриптов для Клиента управления С-Терра «Пост»

Далее следует создать и доставить на носитель С-Терра «Пост», в каталог customization, установочные скрипты клиента управления. Этот каталог по умолчанию доступен в режиме «только для чтения». Для того, чтобы разрешить запись в этот каталог была возможна, необходимо убедиться, что сессия пользователя была открыта ранее (см. п. 4.3, шаги 1-4).

Шаг 1: Перейдите в окно Сервера управления. В таблице выделите клиента post и в контекстном меню выберите предложение *Get packages* (Рисунок 27).

VPN UPServer console					
File Groups Clients Tools	Help				
Clients Settings					
List of groups	List of dients				
All clients	^ Client ID	Condition	Active updates	Applied updates	Administrative state
Office1	gate0	active	0	8	enabled
	post	new	0	0	oppled
				Snow	
				Properties	
				Ureate	
				Opuate	
				Cotroacka	200
				Get packa	ges
				Disable	
				Disable	
				Reury	
				ear	
				Remove	

Рисунок 27

Шаг 2: В открывшемся окне укажите каталог на C-Teppa «Пост» \gatedat\customization, в который будут сохранены скрипты и нажмите кнопку ОК (Рисунок 28).По окончании процедуры будет выдано сообщение об успешном ее завершении (Рисунок 29). Нажмите ОК.

emovable Disk	(E:)		
temovable Disk	(G:)		
ate-dat (H:)			
customization			
diaginfo			
emovable Disk	(I:)		
temovable Disk	(J:)		-
	gate-dat (H:) customization diaginfo Removable Disk Removable Disk	gate-dat (H:) customization diaginfo Removable Disk (I:) Removable Disk (J:)	gate-dat (H:) customization diaginfo Removable Disk (I:) Removable Disk (J:)

Рисунок 28



Рисунок 29

Шаг 3: Два файла будут сохранены в указанный каталог (Рисунок 30):

- setup product.sh скрипт для инициализации продукта S-Terra Gate
- setup_upagent.sh скрипт, содержащий данные для Клиента управления.



Рисунок 30

Шаг 4: Закройте сессию с С-Терра «Пост», нажав кнопку «Закрыть сессию» в Редакторе СПДС.

🔜 С-Терра Редактор СПДС				
Файл Действия PIN-коды Справка				
Подключенные устройства:				
Считыватель	Серийный номер	Размер диска	Доступ	Обновить список устройств
S-Terra CSP Specialized Bootable Storage 0	3460673A02068604	216	Чтение/Запись	Открыть сессию
				Закрыть сессию
				Изменить PIN пользователя данных
				Изменить PIN пользователя
				Изменить PIN администратора
				Изменить транспортный PIN
				Восстановить PIN-ы по умолчанию

Рисунок 31

- Шаг 5: Закройте приложение и выньте С-Терра «Пост» из USB-разъема Сервера управления.
- Шаг 6: Для применения и настройки параметров RDP-сессии администратором рекомендуется загрузить тестовую аппаратную платформу с подготовленного С-Терра «Пост».



Требуется обеспечить сетевую доступность Сервера управления и тестовой аппаратной платформы.

4.5. Настройка функционального программного обеспечения

- Шаг 1: Произведите загрузку тестовой аппаратной платформы с С-Терра «Пост». Если РІN пользователя был изменен ранее при помощи программы «С-Терра Редактор СПДС», то его следует ввести согласно запросу до загрузки графической оболочки.
- Шаг 2: Скрипты setup_product.sh и setup_upagent.sh должны примениться, о чем свидетельствует изменение состояния клиента post с new на active на Сервере управления (Рисунок 32).

***	WPN UPServer console								
File	ile Groups Clients Tools Help								
C	Clients Settings								
	List of groups	List of clients							
	All clients	^ Client ID	Condition	Active updates	Applied updates	Administrative state	Fire time by certificates	Last active time	Last active ip-address
	Office 1	gate0	active	0	8	enabled	03/06/2016 15:13:02	ONLINE	192.168.10.10
		post	active	0	0	enabled	26/05/2016 10:57:47	ONLINE	10.0.0.12

Рисунок 32

- **Шаг 3:** На Сервере управления в произвольной директории создайте файл **new.txt** (например, C:\new.txt) и в текстовом редакторе задайте требуемые значения следующих параметров (Рисунок 33):
 - EX_PASS_ROOT новый пароль учетной записи root. Если пароль не указан, то на конечном устройстве он изменен не будет.

- EX_RDP_AUTORUN позволяет добавить в автозагрузку старт RDP-сессии. При значении TRUE запись добавляется в автозагрузку. При значении FALSE – удаляется.
- EX_RDP_IP IP-адрес RDP-сервера.
- EX_RDP_USER имя учетной записи пользователя RDP-сервера.
- EX_RDP_PASS пароль учетной записи пользователя RDP-сервера.
- EX_RDP_RESOLUTION разрешение RDP-сессии. Можно указывать процент от экрана конечного устройства (80, 90), либо FULL (для использования full-screen).
- EX_SRC_IP и EX_DST_IP_1, EX_DST_IP_2, EX_DST_IP_<N> (где <N> любое целое число) и т.д. - IP-адреса для натирования пакетов. Пакеты, идущие на DST_IP_<N>, натируются и уходят с интерфейса с SRC_IP. На каждый адрес DST_IP создается правило натирования. В качестве адреса можно использовать как отдельный IP-адрес (например – 192.168.10.3), так и адрес подсети (например – 192.168.10.0/24). Количество переменных EX_DST_IP_<N> – не ограничено. В данном примере в качестве переменной EX_DST_IP_1 указан IP-адрес RDP-сервера, а в качестве переменной EX_DST_IP_2 - IP-адрес Сервера управления.



Рисунок 33



Адрес, получаемый АРМ по DHCP, заранее не может быть известен администратору и существует вероятность того, что два, или более, АРМ будут иметь одинаковые приватные адреса. Надежное построение защищенных соединений в этих условиях будет затруднено. Для предотвращения этой ситуации рекомендуется транслировать исходящий адрес средствами iptables. Это следует производить настройкой параметров EX_SRC_IP, EX_DST_IP_1, EX_DST_IP_2, EX_DST_IP_<N>.

Шаг 4: Все значения параметров должны задаваться в одной строке с именем параметра, через знак «=», без пробелов. <u>Рекомендуется после редактирования</u> сохранять файл в unix-формате. Если не требуется менять значение какого-либо параметра, нужно удалить из строки его значение, оставив в строке его имя.

Шаг 5: С помощью командной строки добавьте данные настройки в качестве параметров для устройства С-Терра «Пост»:

cd "C:\Program Files\S-Terra\S-Terra KP\"

upmgr.exe set prop -i "post" -ex var file "C:\new.txt"

где post - идентификатор клиента для С-Терра «Пост» на Сервере управления.

Шаг 6: На Сервере управления вызовите окно Client Properties (в контекстном меню клиента предложение *Properties...*), чтобы увидеть добавленные переменные (Рисунок 34).

Client properties			x
Client ID post			
Client description			
Device password			
Show devic	e password as plain text		
Client variables			
Name	Value		Modify
EX_DST_IP_1	192.168.10.2		
EX_DST_IP_2	192.168.10.3		Add
EX_PASS_ROOT			
EX_RDP_AUTORUN	TRUE		Remove
EX_RDP_IP	192.168.10.3		
EX_RDP_PASS	12345678		
EX_RDP_RESOLUTION	FULL		
EX_RDP_USER	user		
EX_SRC_IP	60.1.1.1		
UPAgentCPU	1686		
UPAgentGroup			
UPAgentiD	post		
UPAgentLastActive Time	22/09/2015 15:25:17		
	LINUXDERIANS	_	
I ≤	LINOXDEDIANO		
<u>1.1</u>			
		OK	Consul 1
		UK	Cancel

Рисунок 34

Шаг 7: На Сервере управления создайте директорию, например, C:\post (Рисунок 35), в которой разместите два скрипта – cook.bat и update.sh. Скрипт cook.bat (выполняется на Сервере управления, EX_- переменные устройства, которые будут записаны во временный файл в указанной директории):

@echo off
set | findstr EX_ > params
exit 0

Скрипт update.sh (выполняется на устройстве C-Teppa «Пост»):

cp params /home/user/params

/opt/utils/run.sh /home/user/params

	📗 post						
	G V V Computer - Local Disk (C:) - post						
	File Edit View Tools Help						
🄄 Organize 🔻 🏢 Views 👻 🚷 Burn							
	Eavorite Links	Name 🔺	Date modified Type	▼ Size ▼			
		🚳 cook.bat	20.08.2015 12:20 Windows Batch	File 1 KB			
	Document	update.sh	20.08.2015 12:21 SH File	1 KB			
	Pictures						

Рисунок 35

Шаг 8: Создайте расширенное обновление для клиента post на Сервере управления. В контекстном меню клиента выберите предложение **Update...** (Рисунок 36).

NP	N UPServer con	sole						
File	Groups Clients	Tools	Help					
Clier	ts Settings							
Lis	t of groups		List of clients					
A	dients		^ Client ID	Condition	Active updates	Applied updates	Administrative state	Fire time by certificates
	··· Office 1		gate0	active	0	8	enabled	03/06/2016 15:13:02
			post	active	0	0	enabled	26/05/2016 10:57:47
					Show			
					Properties			
					Create			
					Update			
					Functions	•		
					Get package	s		



Шаг 9: В поле **Extended data** укажите путь до созданной ранее директории со скриптами, например, C:\post (Рисунок 37). Нажмите кнопку OK.

Update client		×
Client ID	post	
Creation time	22.09.2015	
Product package	E	
	Do not send binary code of product package	
UPAgent folder		
UPAgent settings		
Extended data	C:\post	
Send current UP	Server CA certificates to dient	
	OK Cancel	

Рисунок 37

Шаг 10: Как только состояние клиента post изменится с *updating* на *active* процесс задания настроек RDP-сессии можно считать завершенным. После извлечения устройства C-Teppa «Пост» из аппаратной платформы администратора, оно готово для передачи пользователю.

4.5.1. Применение расширенных настроек до построения защищенного соединения с "С-Терра КП"

В некоторых случаях настройки функционального программного обеспечения, задаваемые с помощью "С-Терра КП", необходимо применить во время первоначальной настройки С-Терра "Пост", совместно со скриптами setup_upagent.sh, setup_product.sh, до построения защищенного соединения с "С-Терра КП".

- Шаг 1: Убедитесь, что сессия пользователя С-Терра «Пост» открыта для записи (см. <u>п.</u> <u>4.3</u>, шаги 1-4).
- **Шаг 2:** Перейдите в каталог на C-Teppa «Пост» \gate-dat\customization, в котором создайте два файла следующего содержания:
 - new.txt:

```
EX_PASS_ROOT=

EX_RDP_AUTORUN=TRUE

EX_RDP_IP=192.168.10.3

EX_RDP_USER=user

EX_RDP_PASS=12345678

EX_RDP_RESOLUTION=FULL

EX_SRC_IP=60.1.1.1

EX_DST_IP_1=192.168.10.2

EX_DST_IP_2=192.168.10.3
```

(подробное описание переменных см. в шаг 3 п. 4.5)

update.sh:

```
cp /rw dat/customization/new.txt /home/user/params
```

/opt/utils/run.sh /home/user/params

rm /rw_dat/customization/new.txt

- **Шаг 3:** В каталоге \gate-dat\customization будут находиться четыре файла:
 - setup product.sh скрипт для инициализации продукта S-Terra Gate;
 - setup_upagent.sh Скрипт, содержащий данные для Клиента управления;
 - new.txt файл с настройками функционального программного обеспечения пользователя;
 - update.sh скрипт, применяющий настройки из файла new.txt при загрузке C-Teppa «Пост».
- Шаг 4: Закройте сессию с С-Терра «Пост», нажав кнопку «Закрыть сессию» в Редакторе СПДС.
- Шаг 5: Закройте приложение и выньте С-Терра «Пост» из USB-разъема Сервера управления.
- Шаг 6: При загрузке тестовой аппаратной платформы с С-Терра «Пост» произойдет запуск скриптов setup_product.sh и setup_upagent.sh, а также скрипта update.sh, применяющего заданные настройки функционального программного обеспечения.
- Внимание: Выполнение шагов, описанных в данном подразделе, никак не отобразятся в настройках Сервера управления, поэтому после установления соединения с "С-Терра КП", рекомендуется произвести действия, описанные в <u>п. 4.5</u>.

5. Приложение

5.1. 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 38).



Рисунок 38

Загрузка после ввода PIN (Рисунок 39).



Рисунок 39





Рисунок 40