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



# Программный продукт С-Терра КП Версия 4.1

### Руководство администратора

# Инструкция по обновлению и миграции Сервера управления

РЛКЕ.00009-03 90 01

22.07.2015

# Содержание

1. Предварительные условия		цварительные условия	3
2.	Сценарий обновления Сервера управления с версии 3.11 до версии 4.1		
3.	Сценарий переноса Сервера управления версии 4.1 на другой компьютер		6
	3.1.	Сбор и сохранение данных Сервера управления	6
		3.1.1. Экспорт контейнеров к ГОСТ-сертификатам	7
		3.1.2. Экспорт контейнеров к RSA-сертификатам	13
	3.2.	Восстановление данных на новом ПК	22
		3.2.1. Импорт контейнеров к ГОСТ-сертификатам	22
		3.2.2. Импорт контейнеров к RSA-сертификатам	31

# 1. Предварительные условия

Для выполнения процедуры **обновления** Сервера управления версии 3.11 до версии 4.1 необходимо обратиться в отдел продаж компании «С-Терра СиЭсПи» по адресу <u>sales@sterra.com</u> для приобретения «Программного продукта С-Терра КП. Версия 4.1», который поставляется на CD-диске с названием «С-Терра Клиент CP/ST 4.1. Релиз 4.1.14905. С-Терра КП 4.1. Релиз 4.1.14905».

Для выполнения процедуры **переноса** Сервера управления с одного компьютера на другой с сохранением всех настроек Сервера управления, информации об учетных записях всех управляемых устройств, потребуется любой сменный носитель, например, USB-флеш.

# 2. Сценарий обновления Сервера управления с версии 3.11 до версии 4.1

Для проведения процедуры обновления Сервера управления на одном и том же компьютере выполните следующие шаги.

- Шаг 1: Скопируйте каталог с дистрибутивом С-Терра КП версии 4.1 на компьютер с Сервером управления старой версии.
- Шаг 2: Зайдите в Панель управления Программы и компоненты и удалите из списка продукт S-Terra KP, а также FileZilla Server (Рисунок 1).

🤚 Упорядочить 👻 🏢 Виды 🔻 🎎 Удалить	🛃 Изменить 🛛 🛃 Восстанови	ить	0
• кми	Издатель 👻	Устан 👻	Размер 🔻
Olasoft Packet Builder 1.0	Colasoft LLC.	27.02.2014	17,7 MB
🔁 FileZilla Server	FileZilla Project	17.02.2015	10,0 MB
Microsoft Visual C++ 2008 Redistributable - x86 9	Microsoft Corporation	09.02.2015	600 KE
S-Terra Client AdminTool (st)	S-Terra CSP	30.06.2014	72,8 MB
🔲 S-Terra KP	S-Terra CSP	17.02.2015	132 MB
📵 VMware Tools	VMware, Inc.	23.01.2014	26,7 MB
VPN UPAgent	S-Terra CSP	12.12.2014	77,0 KB
🐻 WinPcap 4.1.3	Riverbed Technology, Inc.	21.02.2014	240 KE
Wireshark 1.10.5 (32-bit)	The Wireshark developer com	21.02.2014	91,3 MB
👱 КриптоПро CSP	Компания КРИПТО-ПРО	20.06.2014	7,60 ME

### Рисунок 1

В процессе деинсталляции продукта FileZilla Server важно не удалить файл с настройками – об этом предупреждает всплывающее диалоговое окно (Рисунок 2). Необходимо нажать No.

🔀 FileZilla Server beta 0.9.	.41 Uninst 🔀
Delete settings?	
Yes	No

#### Рисунок 2

Оставшийся компонент, входивший в пакет установки С-Терра КП версии 3.11 (Рисунок 3), удалять необязательно.

Microsoft Visual C++ 2008 Redistributable - x86 9	Microsoft Corporation	09.02.2015	600 K
---	-----------------------	------------	-------

#### Рисунок 3

Шаг 3: Далее перейдите в каталог с дистрибутивом версии 4.1 и запустите setup.exe (Рисунок 4).

LINUXDEBIAN6	06.02.2015 14:52	Папка с файлами		
LINUXRHEL5	28.08.2014 19:57	Папка с файлами		
] Others	28.08.2014 19:56	Папка с файлами		
SOLARIS	28.08.2014 19:57	Папка с файлами		
MINDOWS	28.08.2014 19:57	Папка с файлами		
setup.exe	28.08.2014 19:56	Приложение	1 466 KB	
💼 setup.ini	28.08.2014 19:56	Параметры кон	1 KB	
🛃 updater_server.cab	28.08.2014 19:57	Cabinet File	195 597 KB	
🔀 updater_server.msi	28.08.2014 19:57	Пакет установ	477 KB	Installer,
upweb.war	28.08.2014 19:57	Файл "WAR"	6 231 KB	
version.txt	28.08.2014 19:57	Текстовый док	1 KĐ	

#### Рисунок 4

Шаг 4: В появившемся окне с запросом на установку необходимых компонент нажмите кнопку Установить (Рисунок 5). Начнется стандартный процесс установки, описанный в разделе 3.1 документа <u>«Программный продукт С-Терра КП. Версия 4.1. Руководство администратора»</u>.

	¥У	становщик продукта С-Терра КП	×
1	В пр комі	оцессе установки продукта С-Терра КП будут установлены следующие поненты:	
	۰	Microsoft Visual C++ 2008 Redistributable Package	
	٠	Microsoft Visual C++ 2010 Redistributable Package	
	•	FileZilla Server	
	٠	PostgreSQL Server	
	٠	Java JRE	
	٠	Apache Tomcat Server	
	•	S-Terra KP UPServer	
		Установить Отмена	Т
			_

Рисунок 5

В результате установки новой версии сохраняется вся информация о настройках Сервера управления, о сертификатах Сервера управления, все учетные записи об управляемых устройствах. По окончании установки Сервер управления готов к работе.

# 3. Сценарий переноса Сервера управления версии 4.1 на другой компьютер

## 3.1. Сбор и сохранение данных Сервера управления

Шаг 1: На компьютере с установленным Сервером управления при помощи утилиты upmgr coxpaните в файл, например, C:\backup01.bin, настройки Сервера управления, СА и рабочий сертификаты, данные о Клиентах управления управляемых устройств, выполнив команду:

C:\Program Files\S-Terra KP\upmgr backup -f C:\backup01.bin

Сохраняется вся информация, кроме контейнеров с секретными ключами сертификатов Сервера управления и статистической информации (Рисунок 6).

c:\Program Files\S-Terra\S-Terra KP>upmgr backup -f C:\backup01.bin Locking upserver data
7-Zip 9.20 Copyright (c) 1999-2010 Igor Pavlov 2010-11-18 Scanning
Creating archive C:\backup01.bin
Compressing authset.ini Compressing backup_info.txt Compressing certs\cacert.cer Compressing certs\workcert.cer Compressing certs\workcert.cer Compressing clients\client01\desc.txt Compressing clients\client01\ftp\data\notiflag.txt Compressing clients\client01\ftp\data\notiflag.txt Compressing clients\client01\state.txt Compressing clients\client01\state.txt Compressing clients\client01\state.txt Compressing clients\client01\updates\00000000hash1 Compressing clients\client01\updates\00000000hish1 Compressing clients\client01\updates\00000000\updates\cacert.cer Compressing clients\client01\updates\00000000\updates\000000\updates\0000000\updates\0000000\updates\0000000\updates\0000000\updates\0000000\updates\0000000\updates\0000000\updates\0000000\updates\0000000\updates\0000000\updates\0000000\updates\0000000\updates\0000000\updates\0000000\updates\0000000\updates\updates\0000000\updates\0000000\updates\updates\0000000\updates\0000000\updates\updates\0000000\updates\updates\0000000\updates\updates\updates\updates\0000000\updates\updates\updates\updates\0000000\updates\upda
Info: Product data have been backuped successfully to file C:\backup01.bin
C=\Program Files\5=leppa\5=leppa KP/

### Рисунок 6

Для переноса всех настроек и контейнеров сертификатов будет использоваться USB-флеш.

Шаг 2: Скопируйте файл backup01.bin с настройками Сервера управления на USBфлеш.

Для экспортирования контейнеров сертификатов Сервера управления на USB-флеш перейдите к разделу <u>«Экспорт контейнеров к ГОСТ-сертификатам»</u> либо к разделу <u>«Экспорт контейнеров к RSA-сертификатам»</u>.

### 3.1.1. Экспорт контейнеров к ГОСТ-сертификатам

- Шаг 1: Предварительно нужно добавить USB-флеш к списку типов ключевых носителей, распознаваемых «КриптоПро CSP». Для этого вставьте USB-флеш в USB-разъем ПК с Сервером управления и определите логическое имя (букву), под которым он отображается в системе.
- Шаг 2: Запустите CryptoPro CSP от имени Администратора. Перейдите во вкладку Hardware, нажмите кнопку Configurate readers... (Рисунок 7).

🙋 CryptoPro CSP	X		
Security Winlog General Hardware Servi	on TLS Settings ce Advanced Algorithms		
Private key readers Allows to add or remove	private key readers.		
Random number generators Random number generators Allows to add or remove random number generators. Configure RNGs			
Key carrier types Allows to add or remove key carrier types. Configure key carrier types			
Ok	Cancel Apply		

Рисунок 7

Шаг 3: Выберите All removable media и нажмите Add... (Рисунок 8).

💫 Readers' control	×
Readers	
The following readers are installed:	
₩ All SmartCard readers <mark>All removable media</mark> Registry	-
Add Remove Properties	
OK Cance	

Рисунок 8

Шаг 4: Появится Мастер установки считывателя – Reader installation wizard. Нажмите Next > (Рисунок 9).



Рисунок 9

Шаг 5: Из списка доступных считывателей выберите устройство (USB-флеш) под необходимой буквой и нажмите Next > (Рисунок 10).

腹 Reader Installation wizard		×
Select reader Which reader do you want t	o install?	
Select support libraries of your re	ader and then click Next.	
Manufacturers:	Available readers	
(All manufacturers)	Dallas (DS1410E)	<b>_</b>
Crypto-Pro LLC	Dallas (DS9097E) Dallas (DS9097U) Roppy A Sable	
	< Back	Next > Cancel

Рисунок 10

Шаг 6: Подтвердите имя считывателя, нажав Next > (Рисунок 11).

腹 Reader Installation wizard	×
Reader name You can assign a name for this reader	
You can type a name for this reader, or you can use the name supplied below. When you finished, click Next.	
Reader name	
Floppy E	
< Back Next	> Cancel

Рисунок 11

Шаг 7: Нажмите Finish и перезагрузите компьютер (Рисунок 12).

腹 Reader Installation wizar	d	×
	Reader installation completion.	
	To complete the reader installation, click Finish.	
	It is strongly recommended to REBOOT computer after the installation.	
	Click Back to modify any of the installation parameters.	
	< Back Finish Cancel	

Рисунок 12

Шаг 8: Для копирования контейнеров запустите CryptoPro CSP, во вкладке Service нажмите кнопку Сору... (Рисунок 13).

🙋 CryptoPro CSP						×
Security General Har	Winlogon TLS Settings ardware Service Advanced Algorith				ettings Algorithms	
Private key conta This wizards allow from a carrier. Check	iner to check, copy	or delete	a private	key con Delei	tainer	
Certificates in priv	/ate key contain	er				
This wizard allows and install them in	to view certificate s	ates locati store.	ed in a pr	ivate key	y container	
	View	certificat	es in con	tainer		
Private certificate						
This wizard allows container by insta	to link certificat Iling it into a cer	e from a f tificate st	île with a ore.	private	key	
	1	Install my	certificat	e		
Passwords on priv	/ate keys					
This wizards allow remove previously	to change pass y saved passwor	words (PI rds.	Ns) on pr	ivate ke	ys or	
Change pas	ssword	Del	ete saveo	d passwo	rds	
,		ОК	Car	ncel	Apply	

Рисунок 13

Шаг 9: В появившемся окне поставьте переключатель в положение Computer и нажмите Browse...(Рисунок 14), выберите необходимый контейнер CA сертификата, размещенный в реестре (Рисунок 15).

😥 Copy private key container	×
Private key container Type or choose private key container to copy	
Key container name:	
	Browse
This name specifies key container for: O User • Computer	By certificate
Choose CSP for key containers search:	
Crypto-Pro GOST R 34.10-2001 Cryptographic Service Provider	•
< Back Next	> Cancel

Рисунок 14

CryptoPro CS	5P	
Select key co	0:08:24 ntainer	
View		
C Friendly	y names 💿 Unique names	
Machine key o	container list:	
R 🔶	Unique	
Registry	REGISTRY\\89288321-0811-3bb7-4e43-ff0e1f5d4	
Registry	REGISTRY\\a1463bab-452e-a427-43a7-e9cad304	
	OK Cancel	//.

Рисунок 15

**Шаг 10:** Нажмите кнопку Next > (Рисунок 16).

Dopy private key container	×
Private key container Type or choose private key container to copy	
Key container name:	
REGISTRY\\89288321-0811-3bb7-4e43-ff0e1f5d4d67	Browse
This name specifies key container for: C User © Computer	By certificate
Choose CSP for key containers search:	
Crypto-Pro GOST R 34. 10-2001 Cryptographic Service Provider	<b>-</b>
< Back Next >	Cancel

Рисунок 16

Шаг 11 Введите пароль на контейнер с секретным ключом, который задавался при создании СА-сертификата на Сервере управления (Рисунок 17).

🗧 CryptoPro CSP	×
Type password for container "89288321-0811-3bb7-4e43-ff0e1f5d4d67"	0:09:29
	EN
Password: •••••	
Save password	
OK Cancel	

Рисунок 17

Шаг12: В появившемся окне введите имя нового контейнера, в который будет скопирован секретный ключ СА-сертификата, нажмите Finish (Рисунок 18).

🐌 Copy private key container		×
Private key container Type private key container to copy to		
Key container name:		
CA_gost		
,		
This name specifies key container for:		
C User		
Computer		
Choose CSP for key containers search		
Crypto-Pro GOST R 34 10-2001 Cryptograph		
	< Back Einish Cancel	ı I
	Carcer	1

Рисунок 18

Шаг 13: Выберите ключевой носитель для нового контейнера – USB-флеш, нажмите ОК (Рисунок 19).

CryptoPro CSP	×
Insert and select car "CA_gost".	0:09:43 rier media for storing private key container
Details	
Readers:	Carrier media inserted:
Floppy E	0358CEDA Status:
	K Cancel Details <<

Рисунок 19

Шаг 14: Установите пароль на новый контейнер, нажмите ОК (Рисунок 20).

CryptoPro CSP		×
Set password o	n produced container "CA_gost".	0:08:26
Set new password		EN
New password:	•••••	
Confirmation:	••••	
ОК	Cancel Details	; >>

Рисунок 20

Шаг 15: Аналогичным образом скопируйте контейнер с секретным ключом для рабочего сертификата Сервера управления на USB-флеш.

Далее перейдите к разделу «Восстановление данных на новом ПК».

### 3.1.2. Экспорт контейнеров к RSA-сертификатам

Если на Сервере управления используются сертификаты с ключами на RSA-алгоритме, то для переноса сертификатов с одного Сервера управления на другой экспортируем их вместе с секретными ключами в файл формата \*.pfx. Для переноса данных будем использовать USB-флеш, предварительно вставленную в USB-разъем.

Шаг 1: На компьютере с исходным Сервером управления из командной строки запустите: mmc. Откроется окно консоли (Рисунок 21).

🚟 Console1 - [Console Root]				
🚰 File Action View Favorites Window	v Help			_ & ×
Console Root	Name		Actions	
	There are no items to show in this	view.	Console Root	<b>^</b>
			More Actions	•
	l			
	Рисунок 2	21		

Шаг 2: Выберите в меню предложение File-Add/Remove Snap-in...(Рисунок 22).

File Action View Favori	tes Window	Help		_8
New Open Save	Ctrl+N Ctrl+O Ctrl+S	ne	Actions	
Save As	conto	There are no items to show in this view.	Console Root	
Add/Remove Snap-in Options	Ctrl+M		More Actions	
1 C:\Windows\\serverman	nager			
Exit				

Рисунок 22

# Шаг 3: В появившемся окне слева выберите Certificates и нажмите Add>, затем OK (Рисунок 23).

ktensible snap-ins, you can vailable snap-ins:	configure which e	xtensions a	are enable	ed. Selected snap-ins:	
Snap-in	Vendor	<b>_</b>		Console Root	Edit Extensions
📺 ActiveX Control	Microsoft Cor				
Authorization Manager	Microsoft Cor				Kemove
Certificates	Microsoft Cor				
Component Services	Microsoft Cor				Move Up
Computer Managem	Microsoft Cor				
CryptoPro License M					Move Down
CryptoPro PKI Mana	Crypto-Pro LLC	A	> 00		
Device Manager	Microsoft Cor				
📸 Disk Management	Microsoft and				
Event Viewer	Microsoft Cor				
Folder	Microsoft Cor				
Group Policy Object	Microsoft Cor				
IP Security Monitor	Microsoft Cor	-			Advanced
R IP Security Policy Ma	Microsoft Cor	<u> </u>			
escription:					
he Certificates snap-in allo	ws you to browse	the conter	nts of the	certificate stores for yourself, a se	ervice, or a computer.
					· · ·

Рисунок 23

Шаг 4: В следующем диалоговом окне поставьте переключатель в положение Computer account, нажмите Next > (Рисунок 24).

Certificates snap-in			×
This snap-in will always manage certificates for:			
O My user account			
C Service account			
Computer account			
	Z Rook	Next 5	Capaci
	1 Daux	IVEXI >	

Рисунок 24

Шаг 5: На вкладке Select Computer поставьте переключатель в положение Local computer и нажмите Finish (Рисунок 25).

Select Computer			×
Select the computer you want This snap-in will always mana C Local computer: (the co	this snap-in to manage. age: mputer this console is running or	٦)	
C Another computer:			Browse
Allow the selected com only applies if you save	outer to be changed when launc the console.	hing from the comman	d line. This
	< Bac	sk Finish	Cancel

Рисунок 25

Шаг 6: На вкладке Add or Remove Snap-ins в правом столбце появляется выбранная оснастка (Certificates). Нажмите OK (Рисунок 26) и перейдите в окно консоли (Рисунок 27).

ActiveX Control       Microsoft Cor         Authorization Manager       Microsoft Cor         Certificates       Microsoft Cor         Component Services       Microsoft Cor         Computer Manager       Microsoft Cor         Computer Manager       Microsoft Cor         CryptoPro License M       CryptoPro License M         CryptoPro PKI Mana       Crypto-Pro LLC         Device Manager       Microsoft Cor         Disk Management       Microsoft Cor         Folder       Microsoft Cor         Folder       Microsoft Cor         IP Security Monitor       Microsoft Cor         IP Security Policy Object       Microsoft Cor	hap-in	Vendor 🔺		Console Root	Edit Extensions
Authorization Manager       Microsoft Cor         Certificates       Microsoft Cor         Component Services       Microsoft Cor         Computer Managem       Microsoft Cor         CryptoPro License M       Move Up         CryptoPro License M       Move Down         CryptoPro PKI Mana       Crypto-Pro LLC         Device Manager       Microsoft Cor         Disk Management       Microsoft Cor         Folder       Microsoft Cor         Folder       Microsoft Cor         IP Security Monitor       Microsoft Cor         IP Security Policy Max       Microsoft Cor	ActiveX Control	Microsoft Cor		🗟 Certificates (Local Computer	)
Certificates       Microsoft Cor         Component Services       Microsoft Cor         Computer Managem       Microsoft Cor         CryptoPro License M       Move Up         CryptoPro License M       Move Down         CryptoPro PKI Mana       Crypto-Pro LLC         Device Manager       Microsoft Cor         Disk Management       Microsoft Cor         Folder       Microsoft Cor         Folder       Microsoft Cor         IP Security Monitor       Microsoft Cor         IP Security Policy Max       Microsoft Cor	Authorization Manager	Microsoft Cor			Remove
Component Services       Microsoft Cor         Computer Managem       Microsoft Cor         CryptoPro License M       Move Up         CryptoPro KI Mana       Crypto-Pro LLC         Device Manager       Microsoft Cor         Disk Management       Microsoft Cor         Folder       Microsoft Cor         Folder       Microsoft Cor         IP Security Monitor       Microsoft Cor         PS Security Policy Max       Microsoft Cor	Certificates	Microsoft Cor			
Computer Managem       Microsoft Cor         CryptoPro License M       CryptoPro License M         CryptoPro PKI Mana       Crypto-Pro LLC         Device Manager       Microsoft Cor         Disk Management       Microsoft Cor         Folder       Microsoft Cor         Folder       Microsoft Cor         IP Security Monitor       Microsoft Cor         P Security Policy Max       Microsoft Cor	Component Services	Microsoft Cor			Movellin
CryptoPro License M       Move Down         CryptoPro PKI Mana       Crypto-Pro LLC         Device Manager       Microsoft Cor         Disk Management       Microsoft and         Event Viewer       Microsoft Cor         Folder       Microsoft Cor         IP Security Monitor       Microsoft Cor         IP Security Policy Max       Microsoft Cor	Computer Managem	Microsoft Cor			
CryptoPro PKI Mana Crypto-Pro LLC Device Manager Microsoft Cor Disk Management Microsoft Cor Folder Microsoft Cor Folder Microsoft Cor IP Security Monitor Microsoft Cor IP Security Policy Ma Microsoft Cor P Security Policy Ma Microsoft Cor Add >	CryptoPro License M				Move Down
Device Manager       Microsoft Cor         Disk Management       Microsoft and         Event Viewer       Microsoft Cor         Folder       Microsoft Cor         Group Policy Object       Microsoft Cor         JP Security Monitor       Microsoft Cor         P Security Policy Max       Microsoft Cor	CryptoPro PKI Mana	Crypto-Pro LLC	Add >		
Disk Management       Microsoft and         Event Viewer       Microsoft Cor         Folder       Microsoft Cor         Group Policy Object       Microsoft Cor         IP Security Monitor       Microsoft Cor         IP Security Policy Ma       Microsoft Cor	Device Manager	Microsoft Cor			
Event Viewer       Microsoft Cor         Folder       Microsoft Cor         Group Policy Object       Microsoft Cor         IP Security Monitor       Microsoft Cor         IP Security Policy Ma       Microsoft Cor	Disk Management	Microsoft and			
Folder       Microsoft Cor         Group Policy Object       Microsoft Cor         IP Security Monitor       Microsoft Cor         IP Security Policy Ma       Microsoft Cor         Advanced       Advanced	Event Viewer	Microsoft Cor			
Group Policy Object Microsoft Cor IP Security Monitor Microsoft Cor IP Security Policy Ma Microsoft Cor Advanced	Folder	Microsoft Cor			
IP Security Monitor Microsoft Cor IP Security Policy Ma Microsoft Cor Advanced	Group Policy Object	Microsoft Cor			
IP Security Policy Ma Microsoft Cor	IP Security Monitor	Microsoft Cor			Advanced
	IP Security Policy Ma	Microsoft Cor		L	Auvanced
	•				

Рисунок 26

🚟 Console1 - [Console Root]		
🚡 File Action View Favorites	Window Help	
Console Root	Name	

Рисунок 27

### Шаг 7: В каталоге Trusted Root Certification Authorities выберите каталог Certificates, а справа выберите CA сертификат Сервера управления для копирования – UPServer CA certificate (Рисунок 28).

🚡 File Action View Favorites Window 🗢 🕪 🖄 📅 🔏 🕒 💥 📴 😖	Help				
Console Root  Certificates (Local Computer)  Certificates (Local Computer)  Certificates  Certificates  Certificates  Certificates  Certification Authoritie  Certificates  Cuntrusted Publishers  Cuntrusted Certificates  Cuntrusted Certificates  Cuntrusted Pacificates  Cuntrusted  C	Issued To Class 3 Public Primary Certification Class 3 Public Primary Certification Copyright (c) 1997 Microsoft Corp. Microsoft Authenticode(tm) Root Microsoft Root Authority Microsoft Root Certificate Authority NO LIABILITY ACCEPTED, (c)97 V Thawte Timestamping CA UPServer CA certificate 425ea565	Issued By Class 3 Public Primary Certification A Class 3 Public Primary Certification A Copyright (c) 1997 Microsoft Corp. Microsoft Authenticode(tm) Root Au Microsoft Root Authority Microsoft Root Authority NO LIABILITY ACCEPTED, (c)97 Veri Thawte Timestamping CA UPServer CA certificate 425ea565-8	Expiration Date 8/2/2028 1/8/2004 12/31/1999 1/1/2000 12/31/2020 5/10/2021 1/8/2004 1/1/2021 2/11/2025	Intended Purposes Secure Email, Client Secure Email, Client Time Stamping Secure Email, Code S <all> <all> Time Stamping Time Stamping Server Authentication</all></all>	Friend VeriSi VeriSi Micros Micros Micros VeriSi Thaw <non< th=""></non<>
<ul> <li>Smart Card Trusted Roots</li> </ul>	VeriSign Class 3 Public Primary Cer	UPServer CA certificate Seca70f9-6 VeriSign Class 3 Public Primary Certifi	2/13/2025 7/17/2036	<al> Server Authenticatio</al>	<non VeriSi</non 

#### Рисунок 28

# Шаг 8: Правой кнопкой мыши нажмите на имени сертификата и из выпадающего меню выберите All Tasks – Export... (Рисунок 29).



Рисунок 29

Шаг 9: Откроется окно Мастера экспорта сертификатов – Certificate Export Wizard, нажмите Next > (Рисунок 30).



Рисунок 30

Шаг 10: Для экспортирования секретного ключа вместе с сертификатом поставьте переключатель в положение Yes, export the private key, нажмите Next > (Рисунок 31).

Certificate Export Wizard	×
Export Private Key You can choose to export the private key with the certificate.	
Private keys are password protected. If you want to export the private key with the certificate, you must type a password on a later page.	
Do you want to export the private key with the certificate?	
Yes, export the private key	
🔿 No, do not export the private key	
Learn more about <u>exporting private keys</u>	
< Back Next > Cano	:el

Рисунок 31

Шаг 11: Экспортируйте сертификат и ключ в контейнер формата PKCS#12 (файл формата .pfx), нажмите Next > (Рисунок 31).

ertificate Export Wizard	<
Export File Format Certificates can be exported in a variety of file formats.	
Select the format you want to use:	
C DER encoded binary X.509 (.CER)	
C Base-64 encoded X.509 (,CER)	
C Cryptographic Message Syntax Standard - PKC5 #7 Certificates (.P7B)	
$\square$ Include all certificates in the certification path if possible	
Personal Information Exchange - PKCS #12 (.PFX)	
Include all certificates in the certification path if possible	
Delete the private key if the export is successful	
Export all extended properties	
C Microsoft Serialized Certificate Store (.SST)	
Learn more about <u>certificate file formats</u>	
< Back Next > Cancel	

Рисунок 32

Шаг 12: Для защиты контейнера установите пароль и подтвердите его, нажмите Next > (Рисунок 32).

ertificat	te Export Wizard	
Passw	rord	
	o maintain security, you must protect the private key by using a password.	
т.,		
I Y	peana conirm a passwora.	
	Type and confirm password (mandatory):	
	·····	
	< Back Next > Can	cel

Рисунок 33

Шаг 13: Сохраните контейнер на USB-флеш, указав имя файла, нажмите Save (Рисунок 34).

🚟 Save As		×
G - Computer - Removable Disk (E:) -	👻 🔀 Search	
File name: CA_RSA		•
Save as type: Personal Information Exchange (*.pfx)		•
Browse Folders	Save Cancel	

Рисунок 34

Шаг 14: В окне Мастера экспорта сертификатов проверьте правильность отображаемого имени файла, нажмите Next > (Рисунок 35).

ificate Export Wizard		
File to Export Specify the name of the file you wan	it to export	
File name:		
E:\CA_RSA.pfx	Browse	
,		
	< Back Next > Cance	1

Рисунок 35

Шаг 15: Подтвердите завершение операции, нажав Finish (Рисунок 36). Процедура экспорта СА-сертификата и секретного ключа успешно завершена (Рисунок 37).

Certificate Export Wizard		×
Certificate Export Wizard	Completing the Certificate E Wizard You have successfully completed the Certificate wizard. You have specified the following settings: File Name Export Keys Include all certificates in the certification path File Format	xport Export Export Yes No Person
	< Back Finish	Cancel

Рисунок 36

Certificate Export Wizard	×
The export was successful.	
ОК	

Рисунок 37

Процедура переноса рабочего сертификата Сервера управления и секретного ключа к нему аналогична вышеописанной для СА сертификата, однако, путь хранения рабочего сертификата несколько отличается – Certificates - Personal – Certificates, поэтому опишем отличающийся Шаг 7.

Шаг 7: Выбираем слева предложение Certificates и в выпадающих списках выбираем Personal - Certificates (Рисунок 38). Далее в столбце справа выбираем необходимый для копирования сертификат – UPServer work certificate.

Console1 - [Console Root\Certificates (Local Computer)\Personal\Certificates]						
🚘 File Action View Favorites Window	/ Help					
🗢 🔿 🙍 🐻 🔏 🖼 🖻 🖻	2					
Console Root	Issued To 🔺	Issued By	Expiration Date	Intended Purposes	Friend	
Certificates (Local Computer)	UPServer work certificate 601bf9	UPServer CA certificate 5eca70f9-6	2/13/2016	<all></all>	<non< td=""></non<>	
Personal	UPServer work certificate 9c95d0	UPServer CA certificate 5eca70f9-6	2/13/2016	<all></all>	<none< td=""></none<>	
Certificates	UPServer work certificate a05708	UPServer CA certificate 425ea565-8	2/11/2016	Server Authentication	<non< td=""></non<>	
Trusted Root Certification Authoritie	UPServer work certificate d35ed5	UPServer CA certificate 5eca70f9-6	2/16/2016	<al></al>	<non< td=""></non<>	
Certificates						
Interprise Host     Intermediate Certification Authoritie						
Trusted Publishers						
Untrusted Certificates						
🔹 🧮 Third-Party Root Certification Autho						
Smart Card Trusted Roots						
I	l					

Рисунок 38

Далее перейдите к разделу «Восстановление данных на новом ПК».

### 3.2. Восстановление данных на новом ПК

На новом ПК с установленной ОС, СКЗИ «КриптоПро CSP 3.6/3.6R2/3.6R4», Сервером управления из состава «Программного продукта С-Терра КП. Версия 4.1», для восстановления всех сохраненных настроек Сервера управления, сертификатов, учетных записей управляемых устройств выполните следующие процедуры.

- Шаг 1: Вставьте USB-флеш с сохранеными данными в USB-разъем нового ПК и скопируйте файл backup01.bin в любую директорию.
- **Шаг 2:** На новом ПК из консоли запустите команду для восстановления настроек (Рисунок 39), например:

C:\Program Files\S-Terra KP\upmgr restore -f C:\backup01.bin

После этого данные о клиентах, сертификатах и настройках будут доступны во вкладках Сервера управления.



Рисунок 39

Для импортирования контейнеров сертификатов Сервера управления с USB-флеш перейдите к разделу «Импорт контейнеров к ГОСТ-сертификатам» либо к разделу «Импорт контейнеров к RSA-сертификатам».

### 3.2.1. Импорт контейнеров к ГОСТ-сертификатам

Шаг 1: Скопируйте контейнеры с USB-флеш в реестр нового ПК. Процедура копирования аналогична описанной ранее (шаги 1-14 в разделе <u>«Экспорт</u> контейнеров к ГОСТ-сертификатам»), однако, вместо съемного носителя необходимо выбрать тип носителя – **Registry** (Рисунок 40).

CryptoPro CSP		×
() Insert and se	elect carrier media for storing private key conta	0:09:53 iner
CA_gost".		
Details		
Readers:	Carrier media inserted:	
臣	<b>_</b>	
	Status:	_
Eloppy E		
	OK Cancel Details	<<

Рисунок 40

Шаг 2: Перейдите на вкладку CryptoPro CSP – Service – Install my certificate... (Рисунок 42).

CryptoPro CSP					
Security General Hard	Winlogon Jware Service	TLS Settings Advanced Algorithms			
Private key contain This wizards allow from a carrier.	ner to check, copy or delete	e a private key container			
Certificates in priv	ate key container				
This wizard allows and install them in	to view certificates loca to a certificate store. View certifica	ates in container			
Private certificate This wizard allows	Private certificate This wizard allows to link certificate from a file with a private key				
container by installing it into a certificate store.					
Passwords on private keys This wizards allow to change passwords (PINs) on private keys or remove previously saved passwords.					
Change password Delete saved passwords					
	OK Cancel Apply				
Рисунок 41					

Шаг 3: В появившемся окне нажмите кнопку Browse для выбора перенесенных сертификатов (Рисунок 42).

Drivate certificate installation wizard	×
Certificate file location Type or choose installing certificate file location	
Certificate file name: Certificate file format can be one of the following: Certificate file - X.509 (.CERCRT) Message in PKCS #7 standard (.P7BP7M,.DER) Microsoft serialized certificate store (.SST) Note: More than one certificate can be stored in a single file in the some formats.	Browse
< Back Next >	Cancel

Рисунок 42

Шаг 4: В окне выбора сертификатов выберите путь до перенесенных сертификатов Сервера управления: C:\ProgramData\UPServer\certs (Рисунок 43). Выберите CA-сертификат и нажмите кнопку Open.

🜔 Open					×
Look in: 🚺	certs		• 6	1 🕫 🖻 🛙	
Name 🔺			- Type	-	Size
🔙 cacert		2/11/2015 12:4	8 Security	Certificate	1 K
workcert		2/11/2015 12:5	0 Security	Certificate	1 K
					_
•		_			Þ
File name:	cacert				Open
Files of type:	Certificate	Files (*.cer;*.crt)		•	Cancel
	🔽 Open a	s read-only			

Рисунок 43

Шаг 5: Путь до СА-сертификата будет прописан в окне Мастера установки личного сертификата. Нажмите кнопку Next > (Рисунок 44).

腹 Private certificate installation wizard		×
Certificate file location Type or choose installing certificate file locat	ion	
Certificate file name:		
C:\ProgramData\UPServer\certs\cacert.c	er	Browse
Certificate file format can be one of the follo Certificate file - X.509 (.CER,.CRT) Message in PKCS #7 standard (.P7B,.P Microsoft serialized certificate store (.SS	owing: 7MDER) ST)	
Note: More than one certificate can be stored in a formats.	a single file in the some	
	< Back Next >	Cancel

Рисунок 44

**Шаг 6:** Подтвердите данные о сертификате, нажав Next > (Рисунок 45).

腹 Private certific	cate installation wizard
Certificate to View and ch	install noose certificate to install
Certificate:	UPServer CA certificate 425ea565-8322-4441-971d-9472b257fbe8
Subject:	CN=UPServer CA certificate 425ea565-8322-4441-971d-9472b257/be8, OL
Issuer:	CN=UPServer CA certificate 425ea565-8322-4441-971d-9472b257/be8, OL
Valid from:	Wednesday, February 11, 2015 12:48:32 PM
Valid to:	Tuesday, February 11, 2025 12:48:32 PM
Serial number:	6BC3 2AB9 F9F6 8BE6
	Properties
	Browse
	< Back Next > Cancel

Рисунок 45

Шаг 7: В появившемся окне выбора ключевого контейнера поставьте переключатель в положение **Computer** и нажмите Browse (Рисунок 46).

⊵ Private certificate installation wizard	×
Private key container Type or choose private key container, corresponded to selected certificate	
Find container automatically Key container name:	
This name specifies key container for: C User C Computer	Browse
Choose CSP for key containers search: Crypto-Pro GOST R 34.10-2001 Cryptographic Service Provider	
< Back Next >	Cancel

Рисунок 46

Шаг 8: Выберите скопированный ранее в Registry ключевой контейнер для данного сертификата и нажмите ОК (Рисунок 47)..

CryptoPro CS	Р		
			0:08:31
Select key cor	ntainer		
View:			
C Friendly	names	Onique names	
Machine key c	ontainer list:		
R 🔶	Unique		
Registry	REGISTRY\\33333		
,			
		ОК	Cancel

Рисунок 47

Шаг 9: После этого имя контейнера прописывается в окне Мастера установки личного сертификата, нажмите Next (Рисунок 48).

腹 Private certificate installation wizard	×
Private key container Type or choose private key container, corresponded to selected certification	ate 📴
Find container automatically Key container name: REGISTRY\\33333 This name specifies key container for: <ul> <li>User</li> <li>Computer</li> </ul> Choose CSP for key containers search: Croto-Pro GOST B 34 10-2001 Contographic Service Provider	Browse
< Back Next >	Cancel

Рисунок 48

Шаг 10: Введите пароль к выбранному контейнеру, нажмите ОК. (Рисунок 49)

🗧 CryptoPro CSP	×
Type password for container "33333"	0:08:14
	EN
Password:	
Save password	
OK Cancel	

Рисунок 49

Шаг 11: В окне выбора хранилища сертификатов (Рисунок 50) при копировании СА сертификата важно указать папку корневых доверенных центров сертификации. Для этого нажмите Browse... и в появившемся окне выберите Trusted root Certification Authorities – ОК (Рисунок 51). В следующем окне нажмите Next > (Рисунок 52).

При копировании **рабочего** сертификата следует согласиться с предложенным по умолчанию хранилищем (Personal) и нажать Next >.

腹 Private certificate installation wizard			×
Certificate store Choose certificate store to install certificate			
Selection of certificate store constraints flag value	selected earlier (us	se user's or mad	hine's key)
Certificate store name:			
Personal			Browse
U	lsing certificate sto C Use © Con	ore: r iputer	
Install ceritificate to container			
	< Back	Next >	Cancel

### Рисунок 50

🐌 Select Certificate Store	×
Select the certificate store you want to use.	
Personal	•
Trusted Root Certification Authorities	
Intermediate Certification Authorities	
	_
Untrusted Certificates	-
Show physical stores	
OK Cancel	

Рисунок 51

Private certificate installation wiza	rd X
Certificate store Choose certificate store to install cert	lificate
Selection of certificate store constraints flag	value selected earlier (use user's or machine's key)
Certificate store name:	
Trusted Root Certification Authorities	Browse
	Using certificate store: O User O Computer
Install ceritificate to container	
	< Back Next > Cancel

Рисунок 52

Шаг 12: Подтвердите завершение операции - Finish (Рисунок 53).

腹 Private certificate installa	tion wizard		×
	Completing installation You have successful wizard. You have specified th	the private certifi wizard ly completed private certificate in: he following settings:	icate
	Get certificate from file certificate name subject issuer valid from valid to serial number Make sure you speci perform installation.	C:\ProgramData\UPServer\cer UPServer CA certificate 425ea CN=UPServer CA certificate 42 CN=UPServer CA certificate 42 Wednesday, February 11, 2015 Tuesday, February 11, 2025 12 6BC3 2AB9 F9F6 8BE6	▲ ts\cace 565-832 25ea565 512:48: 2:48:32 ↓ ↓ ↓ ↓ ↓ ↓ ↓ ↓ ↓ ↓ ↓ ↓ ↓
		< Back Finish	Cancel

Рисунок 53

Импортирование контейнера и привязка его к СА-сертификату завершена.

Шаг 13: Аналогичным образом импортируйте контейнер к рабочему сертификату и привяжите контейнер к сертификату (шаги 1-12). После запустите консоль Сервера управления и перейдите на вкладку Settings. В области Work certificate нажмите кнопку View... (Рисунок 54).

-Work certificate		
Organization	O= test organization	
Organization Unit	OU= test organization unit	View
Common Name	CN= UPServer work certificate <guid></guid>	Renew
Lifetime	12 months	Import

### Рисунок 54

**Шаг 14:** В появившемся окне описания рабочего сертификата введите имя контейнера и пароль к нему, которые были назначены при копировании контейнера с USB-флеш в Реестр (Рисунок 55).

C	ertificate descripti	on	x		
	r:-ld	Velue	Т		
	Field	value	1_		
	Version	3			
	Serial number	40 9E E1 31 1D 08 42 54			
	Signature algorithm	GOST_R_341001_3411 (Crypto-Pro)			
	Issuer	CN=UPServer CA certificate 4f90ecd6-bbc0-40cc-97/e			
	Valid from	Thu Mar 12 10:34:07 2015			
	Subject	Sal Mar 12 10:54:07 2010 CN-LIDSorver work contificate 2943b222 bdf0.41ff b1c2			
	Dublic key	COST P 341001(512)			
	Alt-subject	<none></none>			
	Hash MD5	47 C3 C2 0E C3 87 CC A9 73 39 FE C5 A3 F4 F8 F2			
	Hash SHA1	42 E3 55 CA 2E 4D 87 6B 71 80 EB A4 EA 1A D3 EB 8C 5			
	Key container name //. \REGISTRY \REGISTRY \\44444				
Key container password *****					
		Save as OK Cancel			

Рисунок 55

Процесс переноса Сервера управления на новый ПК завершен.

### 3.2.2. Импорт контейнеров к RSA-сертификатам

- Шаг 1: На новом ПК с установленным СКЗИ «КриптоПро CSP» и Сервером управления вставьте USB-флеш в USB-разъем, а затем повторите шаги 1-6 включительно раздела <u>3.1.2 «Экспорт контейнеров к RSA-сертификатам»</u>.
- Шаг 2: В окне консоли с добавленной оснасткой в левой области выберите Certificates – Trusted Root Certification Authorities – Certificates. При этом справа появится список сертификатов, лежащих в указанной директории. Правой кнопкой мыши кликните на пустом месте в этой области и выберите All Tasks – Import...(Рисунок 56).

• 🔷 🖸 🖬 🖸 💀 🚺 🖬		
Console Root	Issued To 🔺	Issued By
<ul> <li>Personal</li> <li>Trusted Root Certification Authoritie</li> <li>Certificates</li> <li>Enterprise Trust</li> <li>Intermediate Certification Authoritie</li> <li>Trusted Publishers</li> <li>Untrusted Certificates</li> <li>Trusted People</li> <li>Smart Card Trusted Roots</li> </ul>	Class 3 Public Primary Certification  Copyright (c) 1997 Microsoft Corp.  DigiCert High Assurance EV Root CA  Equifax Secure Certificate Authority  Go Daddy Class 2 Certification Au  GTE CyberTrust Global Root  Microsoft Authenticode(tm) Root  Microsoft Root Authority  Microsoft Root Certificate Authority  Microsoft Root Certificate Authority  NO LIABILITY ACCEPTED, (c)97 V  Thawte Timestamping CA  UPServer CA certificate a9083b24  VeriSign Class 3 Public Primary Cer  All Tasks  Im  Refresh  Export List,  View  Arrange Icons  Line up Icons	Class 3 Public Primary Certification A Copyright (c) 1997 Microsoft Corp. DigiCert High Assurance EV Root CA Equifax Secure Certificate Authority Go Daddy Class 2 Certification Auth GTE CyberTrust Global Root Microsoft Authenticode(tm) Root Au Microsoft Root Authority Microsoft Root Certificate Authority NO LIABILITY ACCEPTED, (c)97 Veri Thawte Timestamping CA UPServer CA certificate a9083b24-9 VeriSign Class 3 Public Primary Certifi
	Help	

Рисунок 56

Шаг 3: Откроется Мастер импорта сертификатов – Certificate Import Wizard, нажмите Next > (Рисунок 57).



Рисунок 57

Шаг 3: В следующем окне нажмите кнопку Browse для выбора переносимого контейнера (Рисунок 58).

Certificate Import Wizard	×
File to Import	
Specify the file you want to import.	
File name:	
Browse	1
	1
Note: More than one certificate can be stored in a single file in the following formats:	
Personal Information Exchange- PKCS #12 (.PFX,.P12)	
Cryptographic Message Syntax Standard-PKCS #7 Certificates (.P7B)	
Microsoft Serialized Certificate Store (.SST)	
Learn more about certificate file formats	
	. 1
< Back Next > Can	cel

Рисунок 58

Шаг 4: Укажите путь до файла с сертификатом, а также в поле задания формата укажите Personal Information Exchange (\*.pfx, \*.p12), либо All Files (\*.\*) и выберите нужный сертификат. Нажмите кнопку Open (Рисунок 59).

🚟 Open			×
Computer	· ▼ UP_FLASH (E:) ▼	👻 🕖 Search	
🕒 Organize 👻 📗 Views	▼ 📑 New Folder		0
Favorite Links  Eavorite Links  Computer  Computer  Documents  Pictures  Music  Recently Changed  Searches  Public	Name A .disk .44911aff.000 .casper .gate0.000 .install .syslinux .up_flash .CA_RSA.pfx	•         Date modified         •         Type         •         Size           26.04.2012 15:11         File Folder         -         -         Size           21.07.2015 17:48         File Folder         -         -         -         -         -         Size           26.04.2012 15:22         File Folder         - <th>3 KB</th>	3 KB
Folders ^	•		•
File name	CA_RSA.pfx	Personal Information Exc     Open     Ca	chang 💌 ancel

Рисунок 59

Шаг 5: Проверьте правильность указанного имени файла в следующем окне и нажмите Next > (Рисунок 60).

Certificate Import Wizard		×
File to Import		
Specify the file you want to import.		
·		
File name:		
E:\CA_RSA.pfx		Browse
Note: More than one certificate can be stored	l in a single file in the fo	bllowing formats:
Personal Information Exchange- PKCS #12	(.PFX,.P12)	
Cryptographic Message Syntax Standard-I	PKCS #7 Certificates (.	Р7В)
Microsoft Serialized Certificate Store (.SST)		
Learn more about certificate file formats		
	< Back Next	> Cancel

Рисунок 60

Шаг 6: Введите пароль на импортируемый контейнер с сертификатом и ключом, Next > (Рисунок 61).

Certificate Import Wizard	x
Password To maintain security, the private key was protected with a password.	
Type the password for the private key. Password:	
<ul> <li>Enable strong private key protection. You will be prompted every time the private key is used by an application if you enable this option.</li> <li>Mark this key as exportable. This will allow you to back up or transport your keys at a later time.</li> </ul>	
Include all extended properties.	
Learn more about <u>protecting private keys</u>	
< Back Next > Cancel	

Рисунок 61

Шаг 7: В окне выбора хранилища сертификатов проверьте правильность указанной директории – Trusted Root Certification Authorities и нажмите Next > (Рисунок 62).

Certificate Import Wizard	×
Certificate Store	
Certificate stores are system areas where certificates are kept.	
Windows can automatically select a certificate store, or you can specify a location for the certificate.	
O Automatically select the certificate store based on the type of certificate	
Place all certificates in the following store	
Certificate store:	
Trusted Root Certification Authorities Browse	
Learn more about <u>certificate stores</u>	

Рисунок 62



Шаг 8: Подтвердите завершение операции импорта, нажав Finish (Рисунок 63).

Рисунок 63

Шаг 9: Подтвердите установку СА сертификата в выбранную директорию, нажав Yes (Рисунок 64). Успешное завершение операции (Рисунок 65).



Рисунок 64



Рисунок 65

Процедура импорта СА-сертификата и секретного ключа завершена.

Процедура переноса рабочего сертификата Сервера управления и секретного ключа к нему аналогична вышеописанной для СА сертификата, однако, путь хранения рабочего сертификата несколько отличается – Certificates - Personal – Certificates, поэтому опишем отличающиеся Шаги 2 и 7.

Шаг 2: В окне консоли с добавленной оснасткой в левой области выберите Certificates – Personal – Certificates. При этом справа появится список сертификатов, лежащих в указанной директории. Правой кнопкой мыши кликните на пустом месте в этой области и выберите All Tasks – Import...(Рисунок 66).

🚟 Console1 - [Console Root\Certificates (	(Local Computer)\Personal\Certificates]			
藩 File Action View Favorites Window	v Help			
🗢 🔿 🗡 📊 📋 🙆 😹 🚺				
<ul> <li>Console Root</li> <li>Certificates (Local Computer)</li> <li>Personal</li> <li>Certificates</li> <li>Trusted Root Certification Authoritie</li> <li>Enterprise Trust</li> <li>Intermediate Certification Authoritie</li> <li>Trusted Publishers</li> <li>Untrusted Certificates</li> <li>Third-Party Root Certification Author</li> <li>Trusted People</li> <li>Smart Card Trusted Roots</li> </ul>	Issued To       Issued By         UPServer work certificate 1eca70       UPServer CA certificate 5eca70f9-6         UPServer work certificate 36c0d6       UPServer CA certificate a9083b24-9         UPServer work certificate 49fd2c1       UPServer CA certificate a9083b24-9         UPServer work certificate 927e50       UPServer CA certificate 5eca70f9-6         All Tasks       Import         Refresh       Advanced Operations +         Export List       View         Line up Icons       Line up Icons         Help       Help			
Рисунок 66				

Шаг 7: В окне выбора хранилища сертификатов проверьте правильность указанной директории – Personal и нажмите Next > (Рисунок 67).

Ce	ertificate Import Wizard	×
	Certificate Store	
	Certificate stores are system areas where certificates are kept.	
	Windows can automatically select a certificate store, or you can specify a location for the certificate.	
	$\bigcirc$ Automatically select the certificate store based on the type of certificate	
	Place all certificates in the following store	
	Certificate store:	
	Personal Drowse	
	Learn more about certificate stores	
-		_
	< Back Next > Cancel	

Рисунок 67

Процесс переноса Сервера управления на новый ПК завершен.