Программное изделие «Сервер кодов аутентификации»

11485466.5014.050

Инструкция по установке и эксплуатации

Содержание

1	Введение		3	
2	Назначение и	условия применения	3	
	2.1 Has	значение системы		
	2.2 Yes	ловия применения системы	3	
3	Установка про	граммного изделия «Сервер кодов аутентификации»	3	
	3.1 Заг	рузка с помощью меню ФПСУ-ІР		
	3.2 Заг	рузка с помощью АРМ удалённого администратора ФПСУ-ІР	5	
4	Удаление программного изделия «Сервер кодов аутентификации»			
5	Описание опер	раций	8	
	5.1 Hav	чало работы с программным изделием «Сервер кодов аутентификации»	8	
	5.2 Ад	министрирование сервера кодов аутентификации	8	
	5.2.1	Получение информации об устройстве		
	5.2.2	Получение информации о регистрации в регионах		
	5.2.3	Регистрация в регионе		
	5.2.4	Отмена регистрации в регионе		
	5.2.5	Загрузка ключа для региона		
	5.2.6	Установка входного системного номера		
	5.2.7	Персонализация		
	5.2.8	Проверка правильности хранения ключей	14	

1 Введение

Настоящий документ содержит руководство пользователя по работе с программным изделием «Сервер кодов аутентификации». Руководство включает в себя справочную информацию по работе программного изделия «Сервер кодов аутентификации».

2 Назначение и условия применения

2.1 Назначение системы

Программное изделие «Сервер кодов аутентификации» представляет собой программный модуль, работающий на базе ПАК ФПСУ-IP.

В программном изделии «Сервер кодов аутентификации» реализованы следующие основные функции:

- Загрузка и хранение кодов аутентификации.
- Формирование кодов аутентификации.
- Проверка кодов аутентификации.

2.2 Условия применения системы

Программное изделие «Сервер кодов аутентификации» устанавливается на ПАК ФПСУ-IP.

3 Установка программного изделия «Сервер кодов аутентификации»

Для того чтобы установить «Сервер кодов аутентификации», необходимо следовать инструкции производителя ПАК ФПСУ-IP.

Для установки программного изделия «Сервер кодов аутентификации» на ФПСУ-IP необходимы два файла: файл cписка sbkasrv3_addon.up0 и файл sbkasrv3_addon.upd, содержащий изменения, разрешённые для данного серийного номера ФПСУ-IP. Перед установкой необходимо проверить контрольные суммы файлов с изменениями.

3.1 Загрузка с помощью меню ФПСУ-IP

Для того чтобы установить «Сервер кодов аутентификации», необходимо в главном меню ПАК ФПСУ-IP (см. Рисунок 1) выбрать пункт **Настройка системы**.



Рисунок 1 – Главное меню ПАК ФПСУ-ІР

В открывшемся меню настройки системы ФПСУ-IP следует выбрать пункт Установка дополнений/изменений (см. Рисунок 2).



Рисунок 2 – Меню настройки системы ФПСУ-IP

В открывшемся окне выбора следует указать каталог на подключённом к ФПСУ-IP USB-носителе, в котором расположены файлы sbkasrv3_addon.up0 и sbkasrv3_addon.upd.

3.2 Загрузка с помощью АРМ удалённого администратора ФПСУ-IP

Для того чтобы установить «Сервер кодов аутентификации», необходимо в основном окне APM удалённого администратора ФПСУ-IP (см. Рисунок 3) выбрать в списке требуемое ФПСУ-IP и нажать кнопку **Ручное управление**.

ПАК "Удаленный администр ФПСУ- <u>I</u> P Операции Конфигу	атор "ФПСУ-IP" r 3.1.56.0 - рации Вид Параметры Параметры	[ZAKVYU] test Ключ УА Статист	— 🗆 ика ФПСУ-I <u>Р</u> ?	×		
принято пак, статистики: 0 0	Чередь:0 Скорость приема:	ое меню и панел О Скорость записи:0	ь инструментов			
Акт Название + Firewall	Aar 2.10 Firewall s/n AMIO	0012СО (основной)			
Список ФПСУ	Режим работь Канал связи с ФПСУ-IP	и: Основной акти : <mark>Готов</mark> Пане.	ивен с 03.03.2020 12:24 ть информации	:40.6.		
	Адрес 192.16	8.0.191				
	Состояние На связ	Состояние На связи 24 мин. 15 сек. (опрошен 05.03.2020 10:58:08)				
	Время ФПСУ-IP 05.03.2	Время ФПСУ-IP 05.03.2020 11:22:11 (разница: 36 сек.) отклик: <55мсек.				
	Резерв работает					
	Мониторинг: Панель команд					
	Состояние VPN	Абоненты	Клиенты ФПСУ-ІР			
	Удаленные АДМ	Обновления ПО	Состояние портов	1		
	ЦПУ	ARP	Общ. статистика	1		
	Очистить тревоги	Просмотр тревог	Подсистемы	1		
	Пинг от ФПСУ-ІР	Сессии МЭ	Блок. трафик	1		
	Управление:			_		
	Ручное управление	Изм. конфигурации	Сравнить конфиг	1		
	Установить конфиг	Получить конфиг	Статистика ФПСУ-ІР	1		
	Пороговые значения	F5 Обновить VPN УА				
				-		
	ΦΠCY-IP	время	(опис.		
Каральнать запрешенные	Onoser	цения				
Тоиск:	<			>		
сего: 1 Разрешено: 1	Активные: 1					

Рисунок 3 – Основное окно АРМ удалённого администратора ФПСУ-IP

В открывшемся меню ручного управления выбранным ФПСУ-IP (см. Рисунок 4) необходимо выбрать пункт **Передать изменения/дополнения**.

Ручное управление ФПСУ-IР - ФПСУ-2 - 10.10.2.1	×
ФПСУ-2 s/n AMI00015CO (основной)	
Состояние канала связи с ФПСУ-IP: Готов	
Получить статистику	
Конфигурация	
Получить	
Передать	
Состояние переданной	
Ключи	
ЦВК: установка/удаление ключей	
Срок использования ключей	
ЦПКК: установка/удаление ключей	
Изменения/дополнения	
Передать изменения/дополнения	
Состояние переданных	

Рисунок 4 – Ручное управление выбранным ФПСУ-IP

В открывшемся окне выбора следует указать каталог, в котором расположены файлы sbkasrv3_addon.up0 и sbkasrv3_addon.upd. В открывшемся окне со списком файлов, относящихся к программному обеспечению ФПСУ-IP (*.up0 и *.upd), необходимо выбрать нужный файл и нажать клавишу Enter или кнопку Установить (см. Рисунок 5).

апр.	Файл	Дата создания файла	Аннотация	Размер	
	ipg-3_0_1e_x86	13.07.2016 13:36:32	ФПСУ-IP v.2.6x->v.3.0.1e	7885202	
	ipg3_0_1e_x86	13.07.2016 13:36:32	ФПСУ-IP v.3.0.1е	7885202	
	upd_m08	Неизвестно		0	
		10/14			

Рисунок 5 – Выбор устанавливаемого ПО

После ряда служебных сообщений о передаче файла откроется окно запроса времени активизации (см. Рисунок 6).

Цата и время акти — Дата, время ФПС	зизации у ———		
13.02.2013	▼ 10:28:56	÷	
Активизировать	(
13.02.2013	10:28:56	÷ 2	
13.02.2013	10:28:56	± 2	
Устан	обить	🗶 Отказ	

Рисунок 6 – Окно запроса времени активизации

Далее следует выбрать дату и время активизации и нажать кнопку Установить.

4 Удаление программного изделия «Сервер кодов аутентификации»

Для того чтобы удалить программное изделие «Сервер кодов аутентификации», необходимо следовать инструкции производителя ПАК ФПСУ-IP.

5 Описание операций

5.1 Начало работы с программным изделием «Сервер кодов аутентификации»

Для начала работы с программным изделием «Сервер кодов аутентификации» следует запустить ПАК ФПСУ-IP, на котором установлен «Сервер кодов аутентификации».

5.2 Администрирование сервера кодов аутентификации

Для того чтобы изменить параметры работы сервера кодов аутентификации, в главном меню ПАК ФПСУ-IP (см. Рисунок 1) необходимо выбрать пункт **Настройка** дополнений. В открывшемся меню настройки дополнений (см. Рисунок 7) следует выбрать пункт **Все Подсистемы Инфокрипт**.



Рисунок 7 – Меню настройки дополнений

В открывшемся меню выбора подсистемы (см. Рисунок 8) необходимо выбрать пункт 6. Сервер SBKA – sbkasrv3.



Рисунок 8 – Меню выбора подсистемы

После появления соответствующего предложения (см. Рисунок 9) необходимо приложить к контактному устройству считывателя информации таблетку, на которой записан ключ главного администратора ПАК ФПСУ-IP.



Рисунок 9 – Предложение подтвердить полномочия главного администратора ПАК ФПСУ-ІР

Если аутентификация в качестве главного администратора ПАК ФПСУ-IP прошла успешно, при первом вызове утилиты необходимо выполнить процедуру персонализации (см. раздел 5.2.7).

После завершения процедуры персонализации при вызове утилиты будет отображён список возможных действий администратора сервера кодов аутентификации (см. Рисунок 10).



Рисунок 10 – Окно администрирования сервера кодов аутентификации

5.2.1 Получение информации об устройстве

Для того чтобы получить информацию об устройстве, необходимо ввести цифру 1 в окне администрирования сервера кодов аутентификации (см. Рисунок 10).

В результате на экране будет выведена информация об устройстве (см. Рисунок



Рисунок 11 – Информация об устройстве

5.2.2 Получение информации о регистрации в регионах

Для того чтобы получить информацию о регистрации в регионах, необходимо ввести цифру 2 в окне администрирования сервера кодов аутентификации (см. Рисунок 10).

В результате на экране будет выведена информация о регистрации в регионах (см. Рисунок 12).



Рисунок 12 – Информация о регистрации в регионах

5.2.3 Регистрация в регионе

Для того чтобы зарегистрировать устройство в регионе, необходимо ввести цифру

3 в окне администрирования сервера кодов аутентификации (см. Рисунок 10).

После появления соответствующего предложения необходимо вставить в дисковод дискету, содержащую созданные центром генерации ключей для данного региона файлы *.rkl и *.reg.

Далее необходимо приложить к считывателю ТМ, на которой записан ключ, созданный центром генерации ключей для данного региона (см. Рисунок 13).



Рисунок 13 – Регистрация в регионе

5.2.4 Отмена регистрации в регионе

Для того чтобы отменить регистрацию устройства в регионе, необходимо ввести цифру 4 в окне администрирования сервера кодов аутентификации (см. Рисунок 10).

В результате на экране будет выведена информация об отмене регистрации в регионе (см. Рисунок 14).



Рисунок 14 – Отмена регистрации в регионе

5.2.5 Загрузка ключа для региона

Для того чтобы загрузить ключ для региона (см. раздел 5.2.2), необходимо ввести цифру 5 в окне администрирования сервера кодов аутентификации (см. Рисунок 10).

Далее необходимо вставить в дисковод дискету, содержащую созданный центром генерации ключей для данного региона ключевой файл *.rkl, ввести полное имя этого файла и нажать клавишу Enter (см. Рисунок 15).



Рисунок 15 – Загрузка ключа

5.2.6 Установка входного системного номера

Для того чтобы установить входной системный номер, необходимо ввести цифру 6 в окне администрирования сервера кодов аутентификации (см. Рисунок 10).

Далее необходимо последовательно ввести номер региона, для которого устанавливается входной системный номер, и сам номер.

8	. Установить входной системный номер . Персонализация (сброс всех настроек) . Проверить правильность хранения ключей >> <u>6</u>	
E	ведите номер региона : 22_	
E	ведите входной системный номер : 2_	
E	ходной системный номер установлен	

Рисунок 16 – Установка входного системного номера

5.2.7 Персонализация

Для того чтобы сбросить все настройки (произвести процедуру персонализации), необходимо ввести цифру 7 в окне администрирования сервера кодов аутентификации (см. Рисунок 10). Для подтверждения удаления всех данных необходимо ввести букву Y и нажать клавишу Enter. Для отказа от очистки следует ввести любой другой символ и нажать клавишу Enter.

После подтверждения удаления всех данных необходимо ввести имя сервера кодов аутентификации, состоящее не более чем из 64 символов.

При появлении соответствующего предложения необходимо вставить дискету в дисковод и нажать клавишу Enter. В результате на дискету будет записан файл персонализации (см. Рисунок 17).



Рисунок 17 – Персонализация

Дискету с файлом персонализации следует передать на АРМ регистрации.

5.2.8 Проверка правильности хранения ключей

Для того чтобы проверить правильность хранения ключей, необходимо ввести цифру 8 в окне администрирования сервера кодов аутентификации (см. Рисунок 10).

В результате на экране будет выведена информация о проверке (см. Рисунок 18).



Рисунок 18 – Проверка правильности хранения ключей