Программное изделие «Сервер кодов аутентификации»

11485466.5014.050

Инструкция по установке и эксплуатации

Содержание

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 списка 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**.

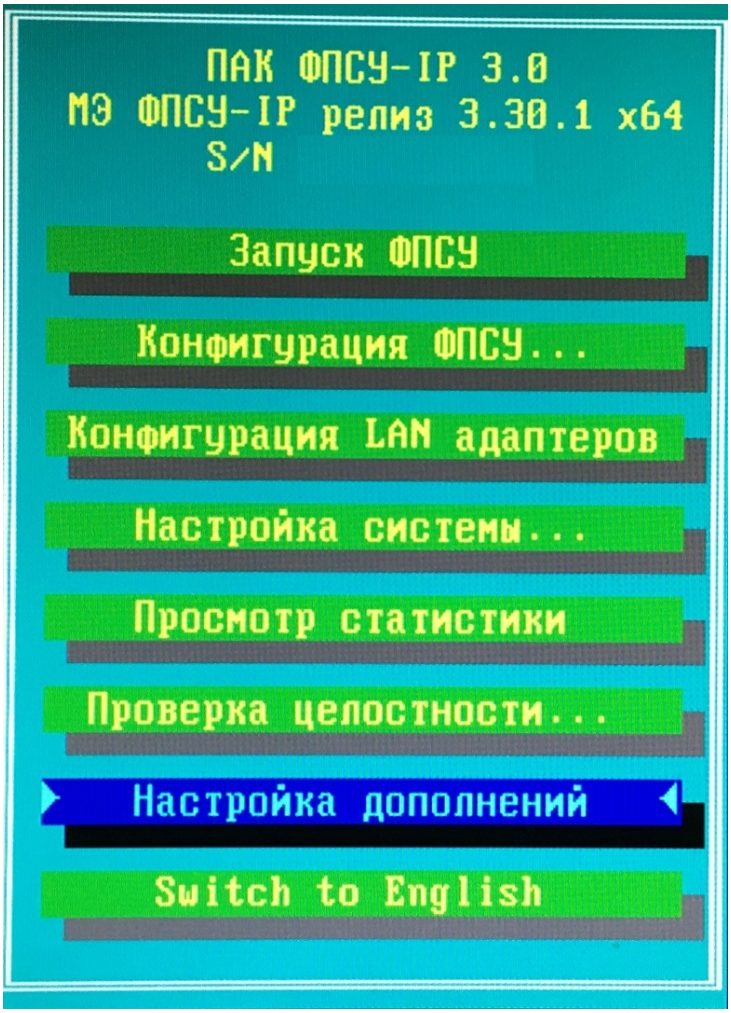

Рисунок 1 – Главное меню ПАК ФПСУ-IP

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

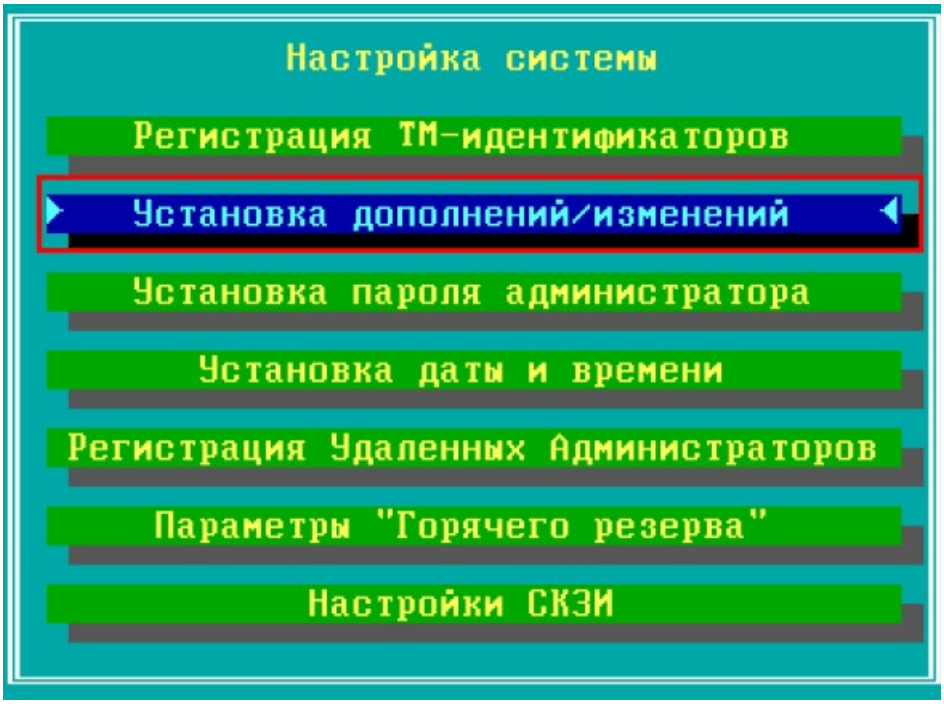

Рисунок 2 – Меню настройки системы ФПСУ-IP

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 АРМ удалённого администратора ФПСУ-IP (см. Рисунок 3) выбрать в списке требуемое ФПСУ-IP и нажать кнопку **Ручное управление**.

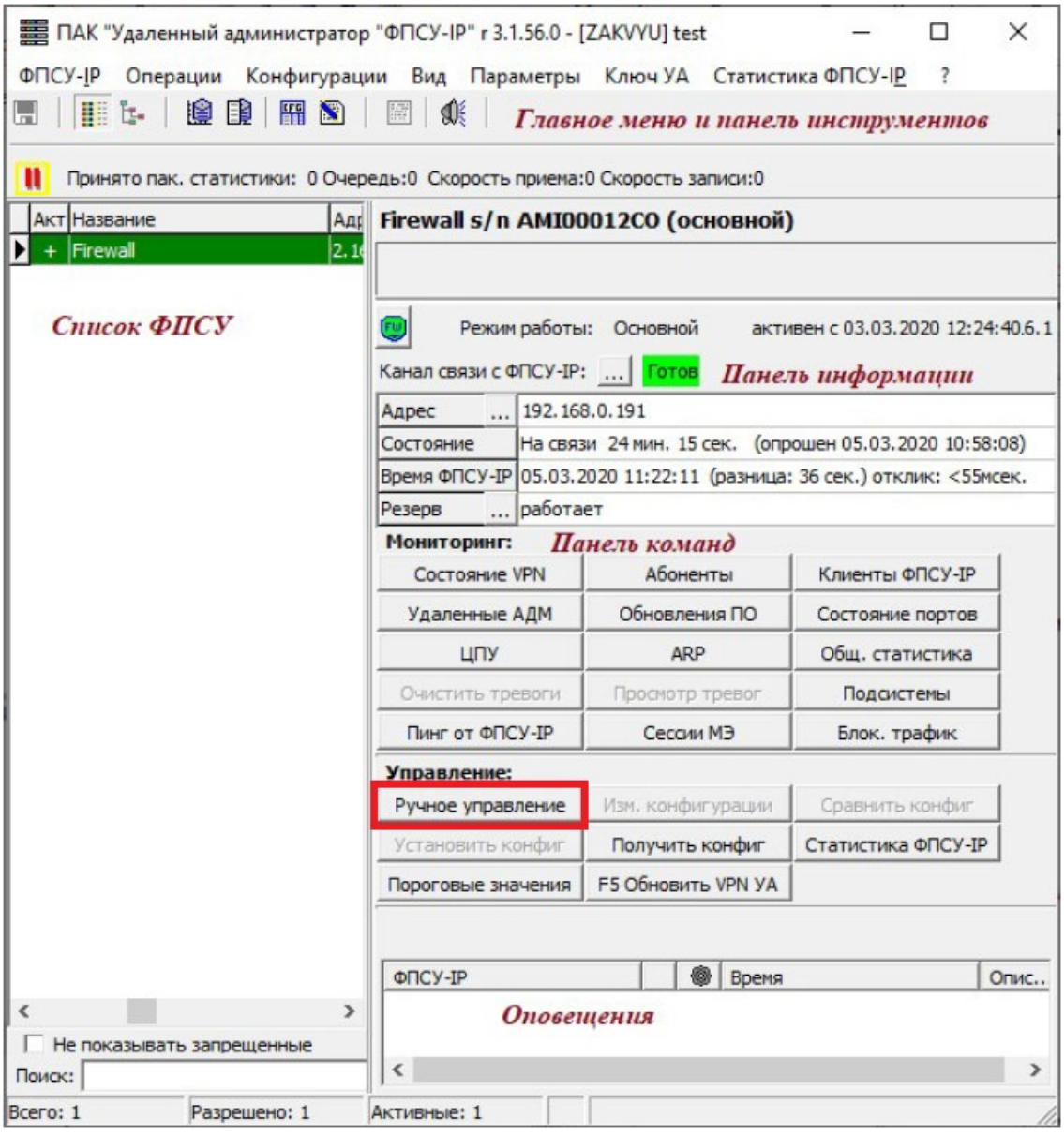

Рисунок 3 – Основное окно АРМ удалённого администратора ФПСУ-IP

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

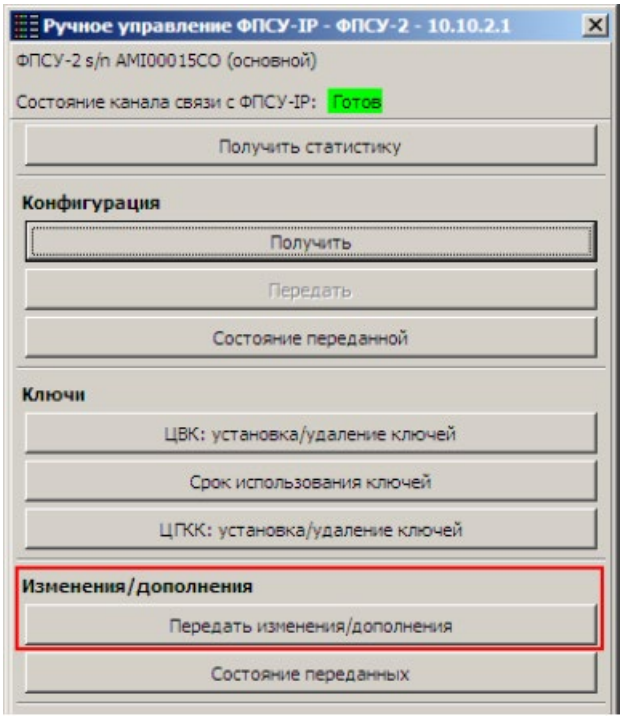

Рисунок 4 – Ручное управление выбранным ФПСУ-IP

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).

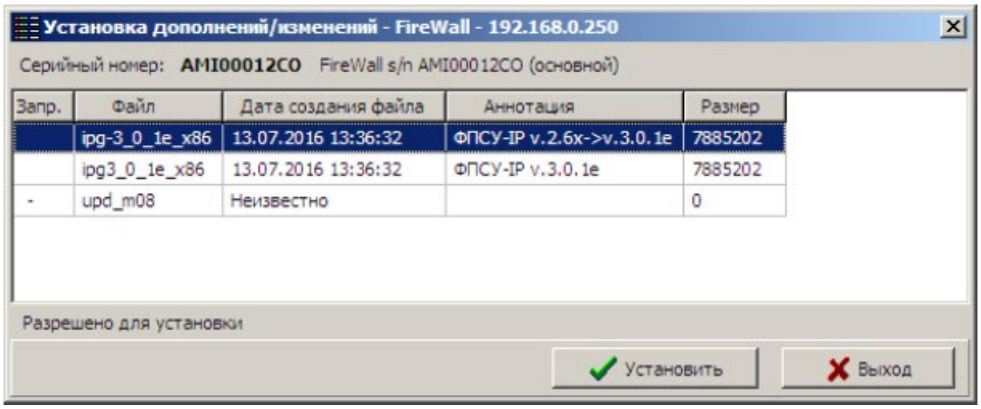

Рисунок 5 – Выбор устанавливаемого ПО

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

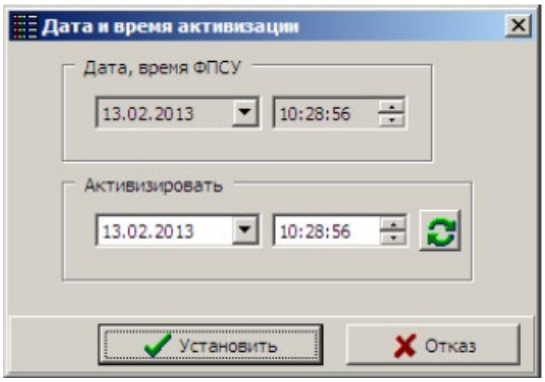

Рисунок 6 – Окно запроса времени активизации

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**.

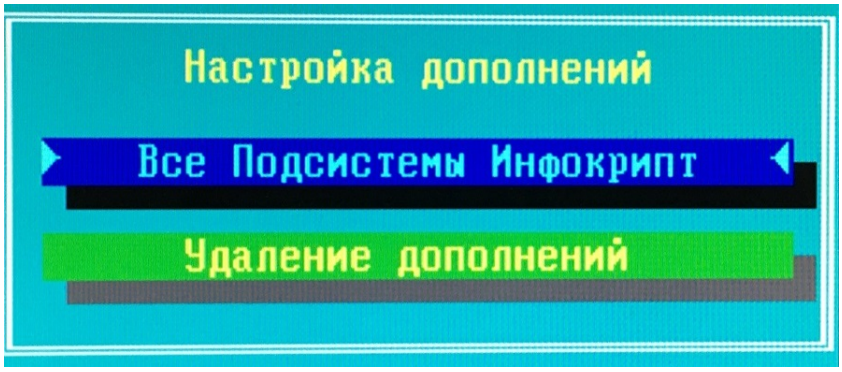

Рисунок 7 – Меню настройки дополнений

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

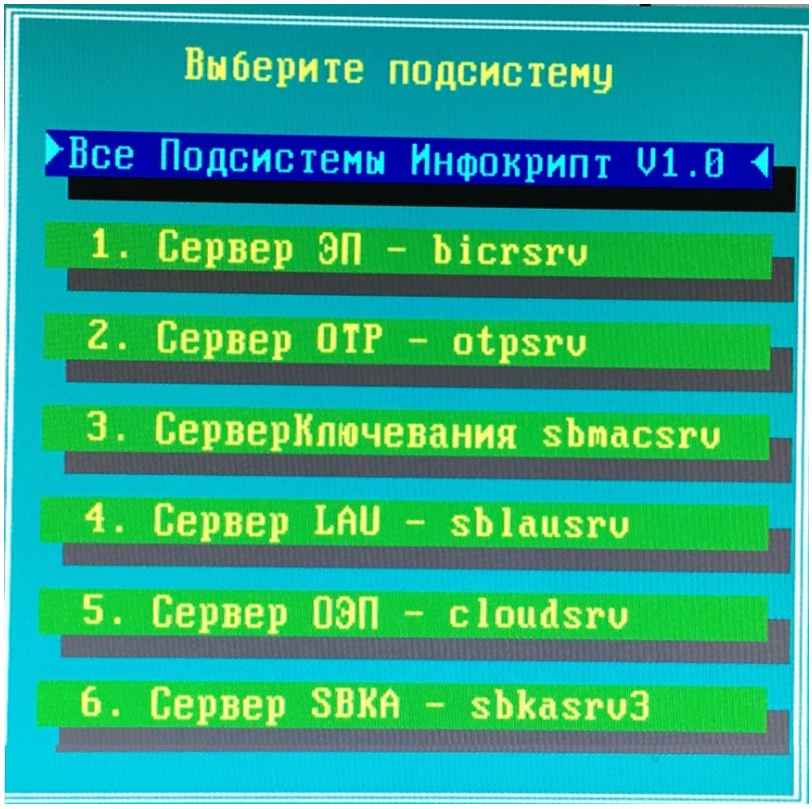

Рисунок 8 – Меню выбора подсистемы

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

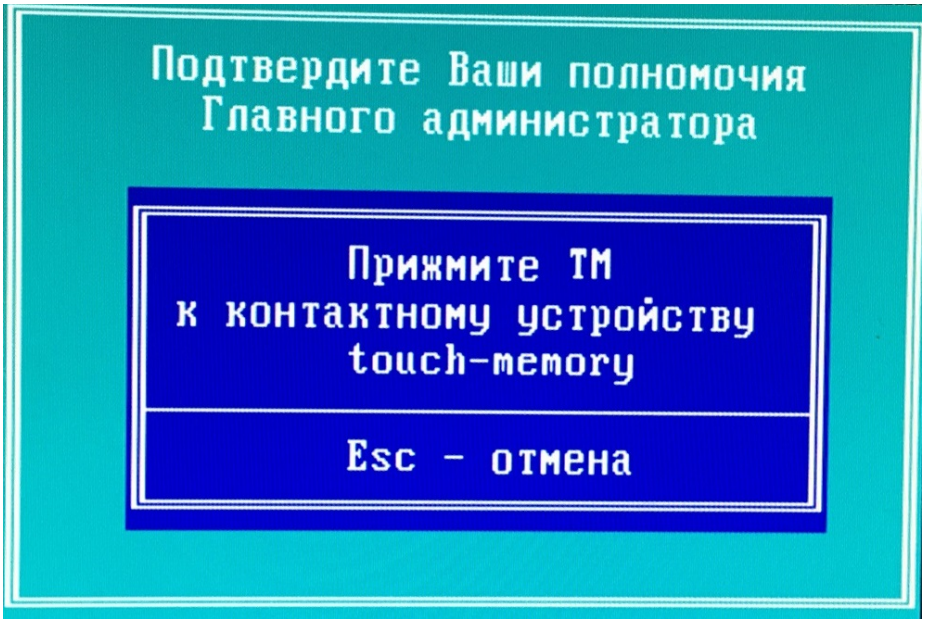

Рисунок 9 – Предложение подтвердить полномочия главного администратора ПАК ФПСУ-IP

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).

```
SBKASRV3 Утилита администрирования  V3.51  (C) ИнфоКрипт 26.11.2014

0.  Выход
1.  Информация об устройстве
2.  Информация о регистрации в регионах
3.  Регистрация в регионе
4.  Отменить регистрацию
5.  Загрузить ключ
6.  Установить входной системный номер
7.  Персонализация (сброс всех настроек)
8.  Проверить правильность хранения ключей
>>> _
```

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 11).

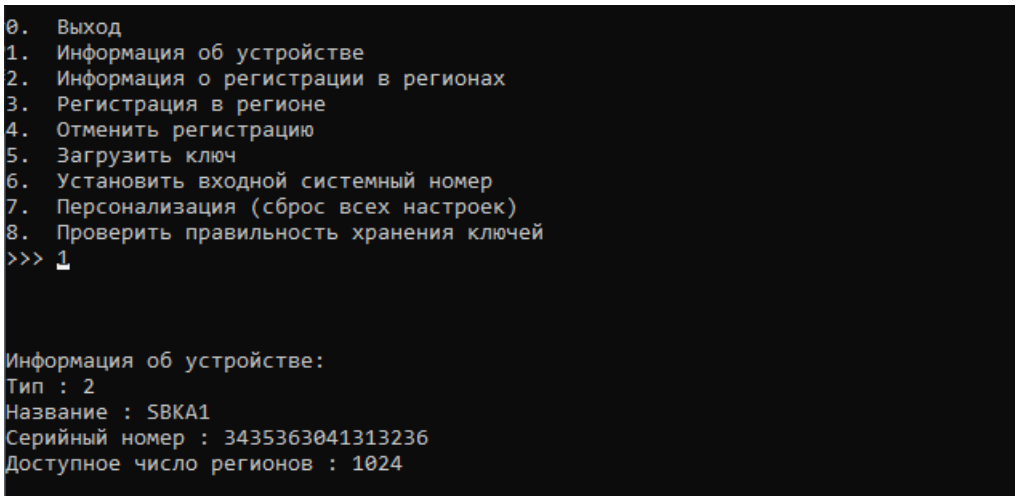

Рисунок 11 – Информация об устройстве

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).

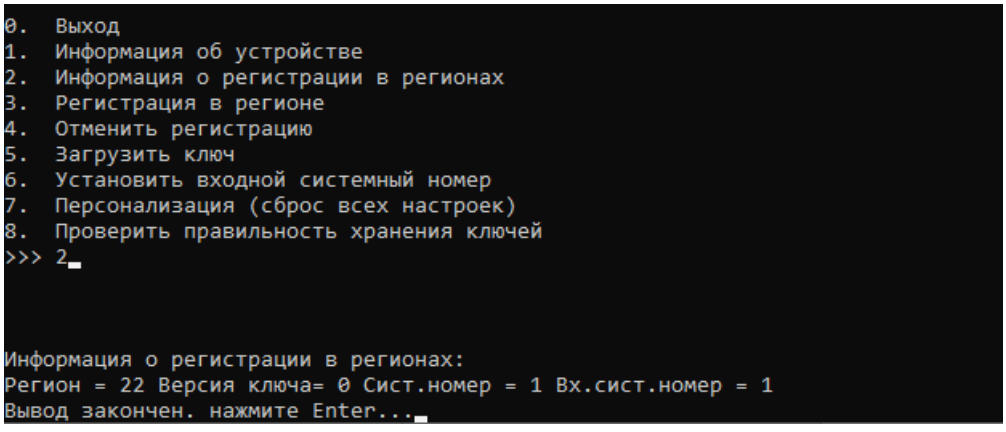

Рисунок 12 – Информация о регистрации в регионах

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).

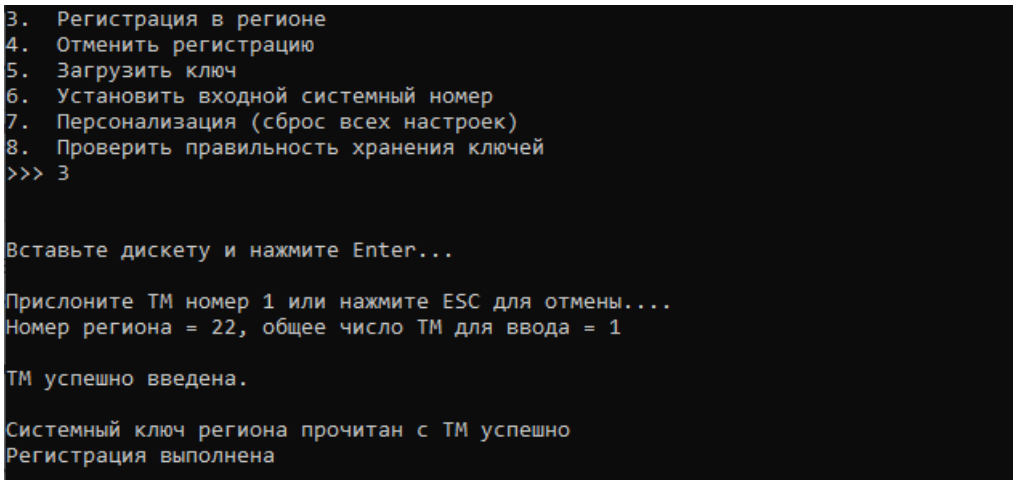

Рисунок 13 – Регистрация в регионе

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).

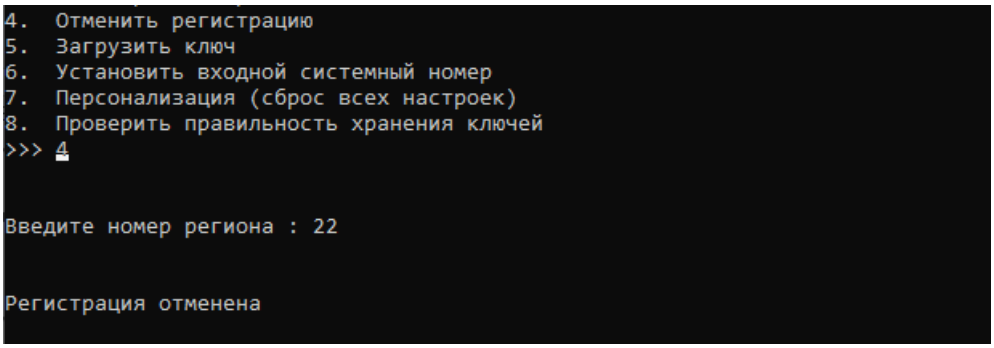

Рисунок 14 – Отмена регистрации в регионе

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).

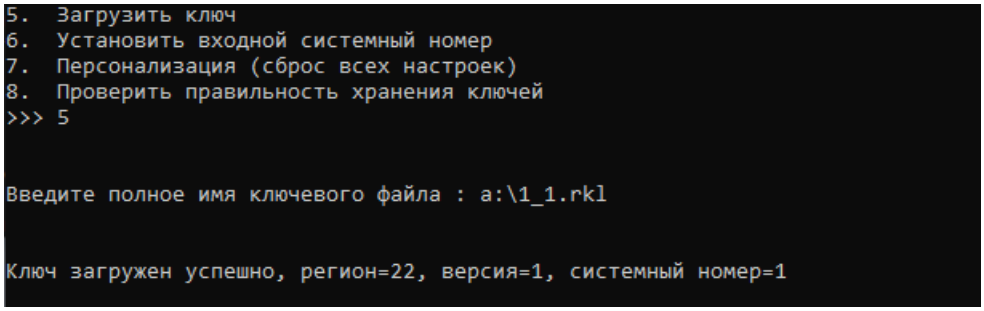

Рисунок 15 – Загрузка ключа

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.

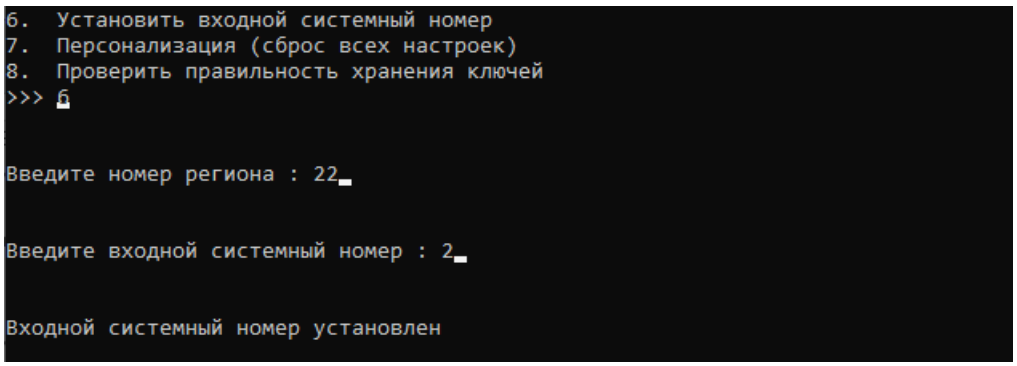

Рисунок 16 – Установка входного системного номера

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).

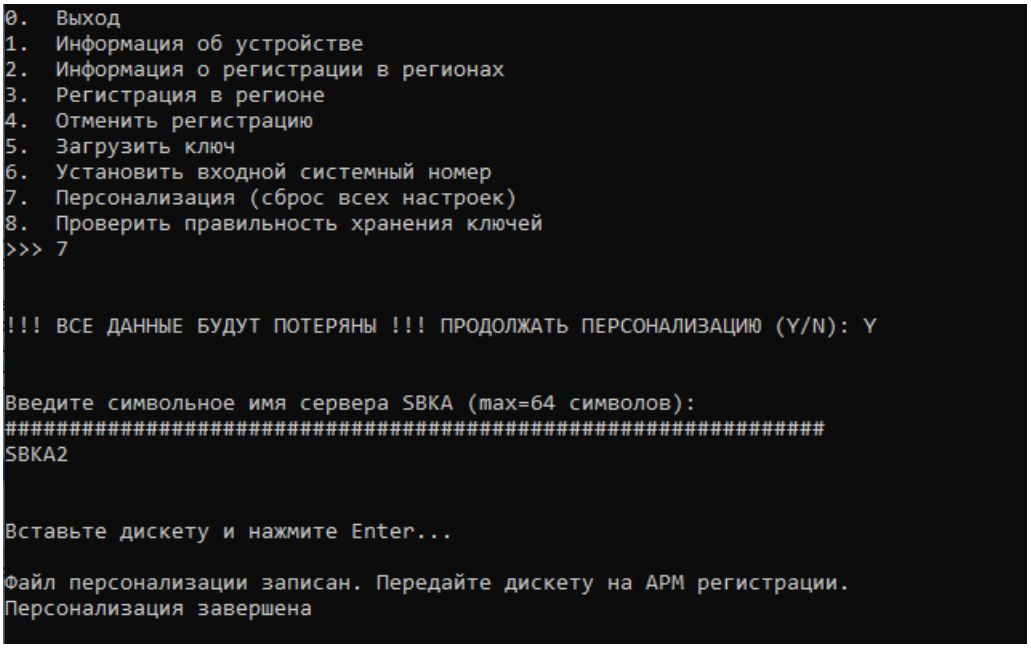

Рисунок 17 – Персонализация

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).

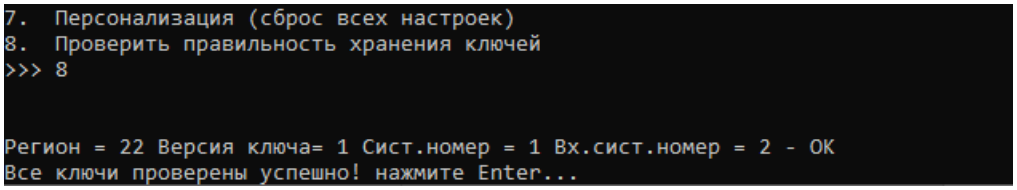

Рисунок 18 – Проверка правильности хранения ключей