

Программное изделие «Сервер ОЭП»

11485466.72.21.12.106

**Инструкция по установке
и эксплуатации**

Содержание

1	Введение	3
2	Назначение и условия применения	3
	2.1 Назначение системы	3
	2.2 Условия применения системы	3
3	Установка программного изделия «Сервер ОЭП»	3
	3.1 Загрузка с помощью меню ФПСУ-IP	4
	3.2 Загрузка с помощью АРМ удалённого администратора ФПСУ-IP	5
4	Удаление программного изделия «Сервер ОЭП»	8
5	Описание операций	8
	5.1 Начало работы с программным изделием «Сервер ОЭП»	8
	5.2 Администрирование сервера ОЭП	8
	5.2.1 Получение информации о ключах	10
	5.2.2 Задание системного имени ФПСУ	11
	5.2.3 Установка активного ключа	12
	5.2.4 Загрузка ключа	12
	5.2.5 Генерация основного ключа	13
	5.2.6 Генерация производного ключа по основному	14
	5.2.7 Удаление загруженного ключа	15
	5.2.8 Удаление всех ключей	16

1 Введение

Настоящий документ содержит руководство пользователя по работе с программным изделием «Сервер ОЭП» (далее «Сервер ОЭП»). Руководство включает в себя справочную информацию по работе программного изделия «Сервер ОЭП».

2 Назначение и условия применения

2.1 Назначение системы

Программное изделие «Сервер ОЭП» представляет собой специализированное программное обеспечение, которое предназначено для создания облачной электронной подписи.

В программном изделии «Сервер ОЭП» реализованы следующие основные функции:

- Создание облачных ключей электронной подписи.
- Формирование электронной подписи.
- Проверку электронной подписи.
- Создание общего ключа шифрования по алгоритму Диффи-Хеллмана.

2.2 Условия применения системы

Программное изделие «Сервер ОЭП» устанавливается на ПАК ФПСУ-IP с программным обеспечением ООО «АМИКОН» версии не ниже 3.20.1.

3 Установка программного изделия «Сервер ОЭП»

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

Для установки программного изделия «Сервер ОЭП» на ФПСУ-IP необходимы два файла: файл списка cloudsrv_addon.up0 и файл cloudsrv_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 ОЭП», необходимо в главном меню ПАК ФПСУ-IP (см. Рисунок 1) выбрать пункт **Настройка системы**.

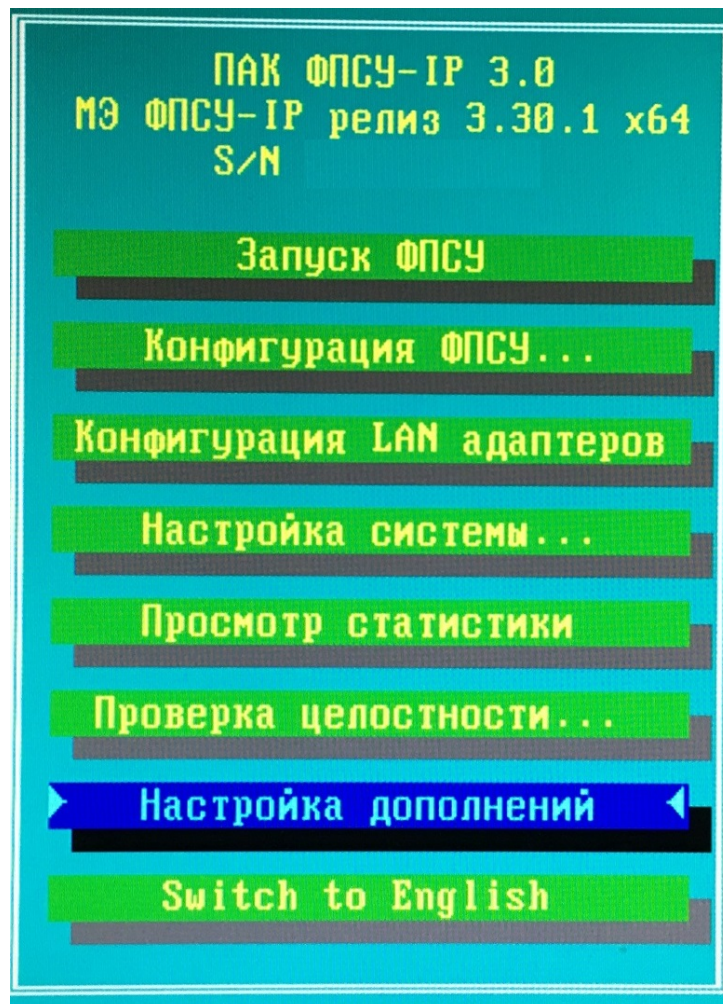


Рисунок 1 – Главное меню ПАК ФПСУ-IP

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

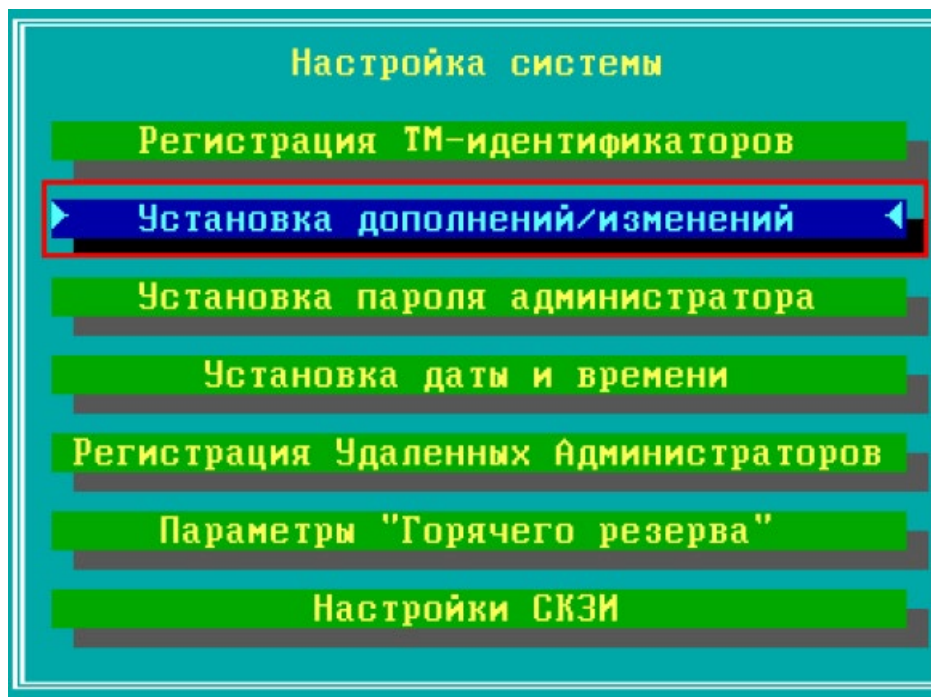


Рисунок 2 – Меню настройки системы ФПСУ-IP

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

3.2 Загрузка с помощью АРМ удалённого администратора ФПСУ-IP

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

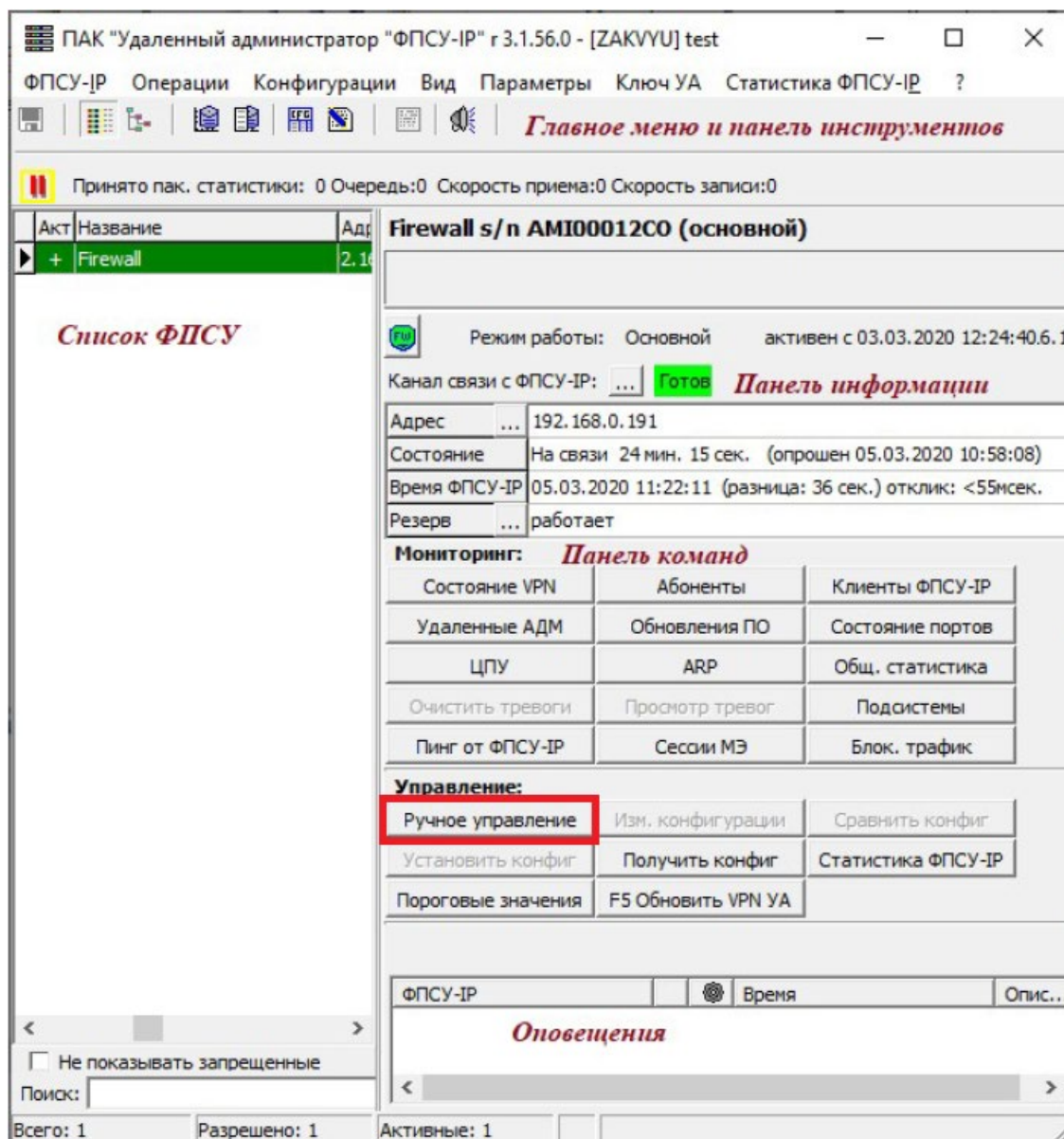


Рисунок 3 – Основное окно АРМ удалённого администратора ФПСУ-IP

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

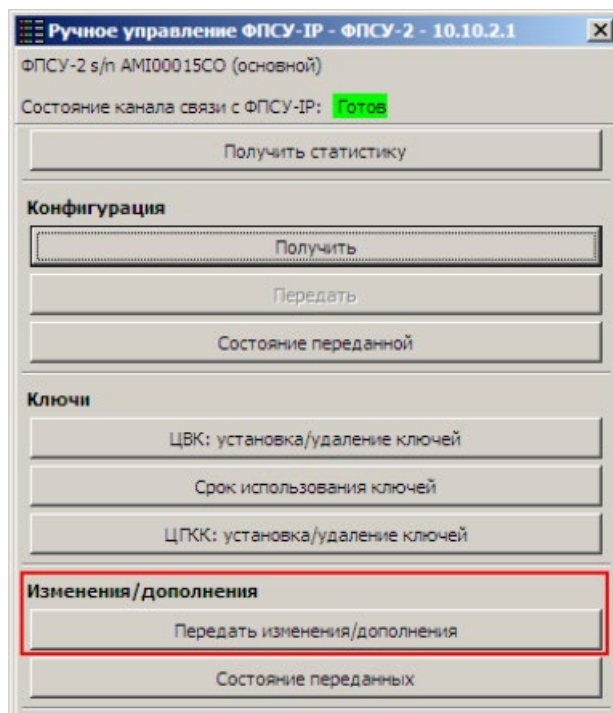


Рисунок 4 – Ручное управление выбранным ФПСУ-IP

В открывшемся окне выбора следует указать каталог, в котором расположены файлы cloudsrv_addon.up0 и cloudsrv_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).

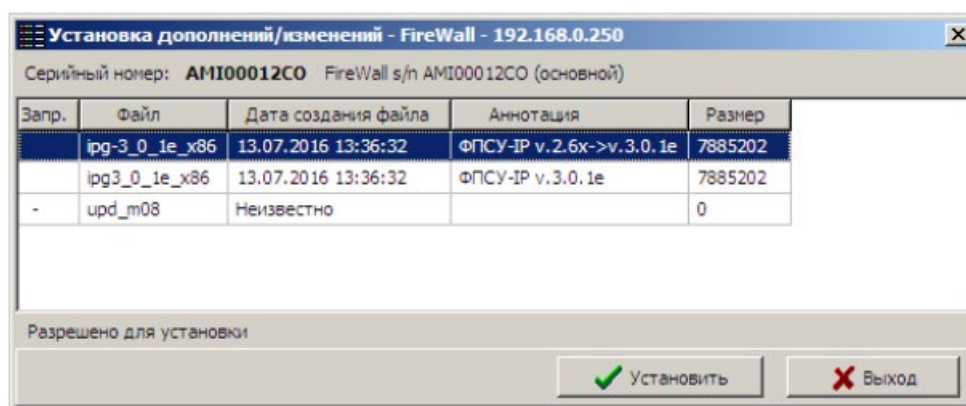


Рисунок 5 – Выбор устанавливаемого ПО

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

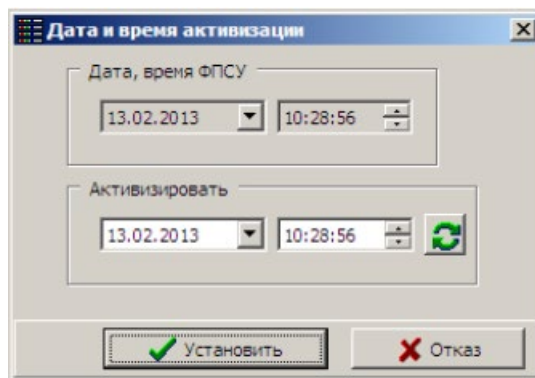


Рисунок 6 – Окно запроса времени активизации

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

4 Удаление программного изделия «Сервер ОЭП»

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

5 Описание операций

5.1 Начало работы с программным изделием «Сервер ОЭП»

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

5.2 Администрирование сервера ОЭП

Для того чтобы изменить параметры работы сервера ОЭП, 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**.

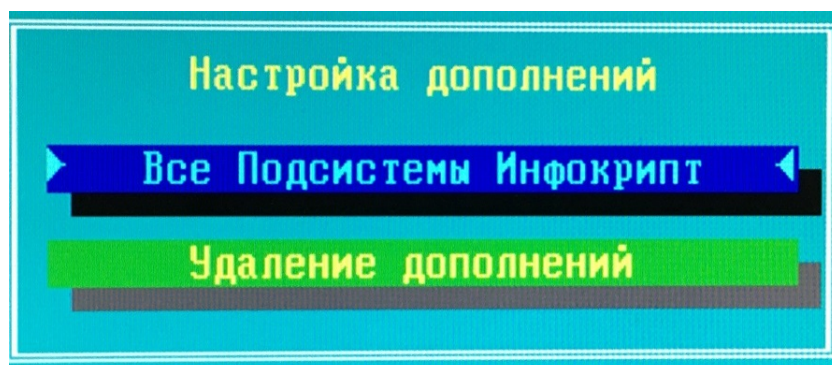


Рисунок 7 – Меню настройки дополнений

В открывшемся меню выбора подсистемы (см. Рисунок 8) необходимо выбрать пункт **5. Сервер ОЭП – cloudsrv**.

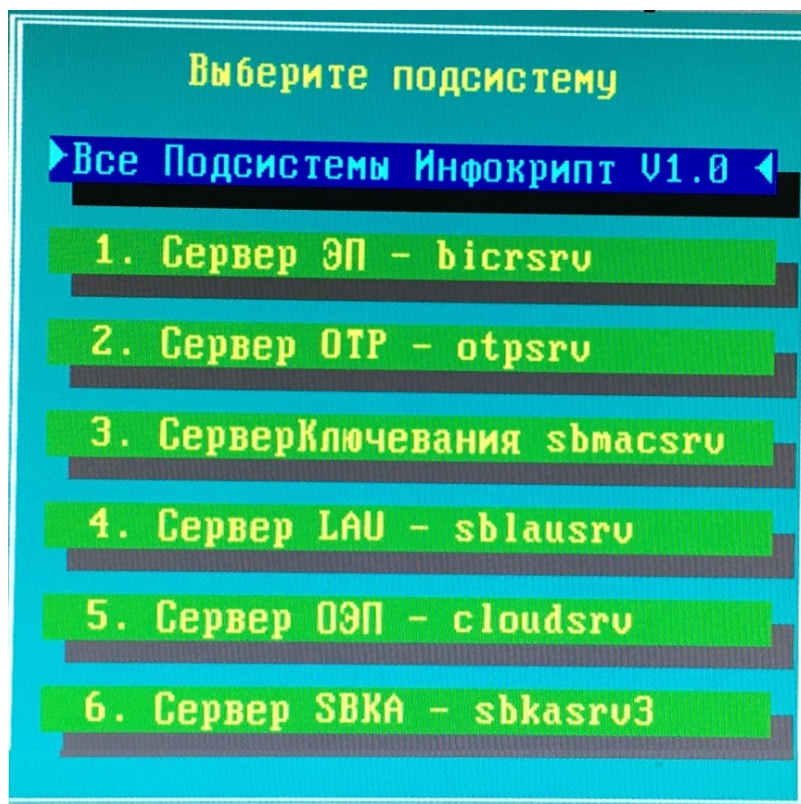


Рисунок 8 – Меню выбора подсистемы

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, в открывшемся окне будет отображён список возможных действий администратора сервера ОЭП (см. Рисунок 10).

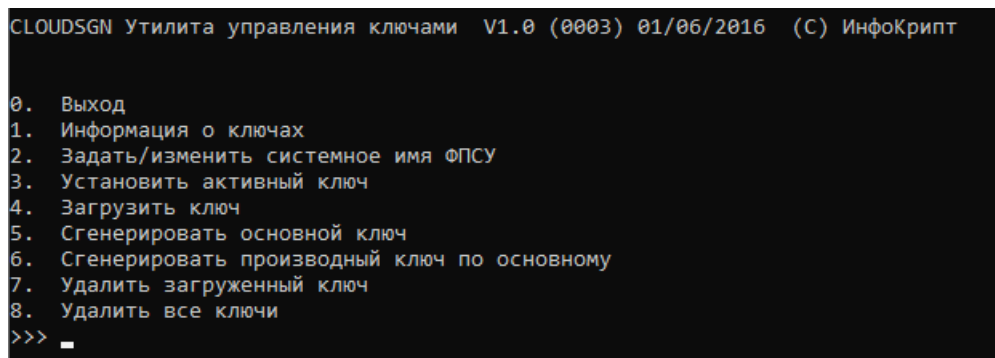


Рисунок 10 – Окно администрирования сервера ОЭП

5.2.1 Получение информации о ключах

Для того чтобы получить информацию о загруженных ключах и сроках их действия, необходимо ввести число 1 в окне администрирования сервера ОЭП и нажать клавишу Enter (см. Рисунок 10).

В результате на экране будет выведен список загруженных ключей (см. Рисунок 11).

```
0. Выход
1. Информация о ключах
2. Задать/изменить системное имя ФПСУ
3. Установить активный ключ
4. Загрузить ключ
5. Сгенерировать основной ключ
6. Сгенерировать производный ключ по основному
7. Удалить загруженный ключ
8. Удалить все ключи
>>> 1

Системное имя: infocrypt

Информация о ключах и сроках действия:

N 1 : Основной [ ОСНОВНОЙ ] [ активный ] с 05/04/2022 по 05/07/2023
N 2 : Key01 [ производный ] с 05/04/2022 по 05/07/2023
N 3 : Main02 [ ОСНОВНОЙ ] с 05/04/2022 по 05/07/2023
N 4 : Key02 [ производный ] с 05/04/2022 по 05/07/2023

Нажмите ENTER для продолжения...
```

Рисунок 11 – Информация о загруженных ключах

Загруженный ключ отображается в следующем виде:

$N = A : NAME [MAINorNOT] [Active] с Date1 по Date2$

Здесь:

A – номер ключа в списке,

NAME – название ключа (не более 10 символов),

MAINorNOT – признак «ОСНОВНОЙ» или «производный»,

Active – признак активности ключа,

Date1 – дата начала действия ключа,

Date2 – дата окончания действия ключа.

Список упорядочен по номеру A ключей.

5.2.2 Задание системного имени ФПСУ

Для того чтобы задать или изменить системное имя ФПСУ, необходимо ввести число 2 в окне администрирования сервера ЭП и нажать клавишу Enter (см. Рисунок 10).

Затем необходимо ввести в качестве системного имени ФПСУ идентификатор, состоящий из не более чем 10 символов (см. Рисунок 12).

```
2. Задать/изменить системное имя ФПСУ
3. Установить активный ключ
4. Загрузить ключ
5. Сгенерировать основной ключ
6. Сгенерировать производный ключ по основному
7. Удалить загруженный ключ
8. Удалить все ключи
>>> 2

Задать системное имя - введите идентификатор (не более 10 символов)
Нажмите левый Ctrl-Shift для перехода на русский шрифт
#####
>infocrypt

Системное имя сохранено!
Нажмите ENTER для продолжения...
```

Рисунок 12 – Задание системного имени ФПСУ

5.2.3 Установка активного ключа

Для того чтобы сделать загруженный ключ активным, необходимо ввести число 3 в окне администрирования сервера ЭП и нажать клавишу Enter (см. Рисунок 10).

Далее необходимо ввести номер ключа, который следует сделать активным, и нажать клавишу Enter. Процедура получения информации о загруженных ключах описана в разделе 5.2.1.

В случае успешного ввода появится соответствующее сообщение (см. Рисунок 13).

```
3. Установить активный ключ
4. Загрузить ключ
5. Сгенерировать основной ключ
6. Сгенерировать производный ключ по основному
7. Удалить загруженный ключ
8. Удалить все ключи
>>> 3

Установить активный ключ - введите номер ключа: 4

Ключ 4 активен!
Нажмите ENTER для продолжения...
```

Рисунок 13 – Установка активного ключа

5.2.4 Загрузка ключа

Для того чтобы загрузить ключ, необходимо ввести число 4 в окне администрирования сервера ОЭП и нажать клавишу Enter (см. Рисунок 10).

Далее необходимо ввести номер ключа, под которым он будет зарегистрирован в сервере ОЭП.

Затем для каждого компонента с номером **A** ключа после появления предложения «Прислоните ТМ номер **A** и нажмите любую клавишу или ESC для отмены...» необходимо приложить к контактному устройству считывателя информации таблетку, на которой записан компонент ключа с номером **A** (см. Рисунок 14).

После появления вопроса «Вы хотите сделать этот ключ активным?» для подтверждения необходимо ввести букву **Y**. Для отказа от активации загружаемого ключа следует нажать любую другую клавишу.

```
4. Загрузить ключ
5. Сгенерировать основной ключ
6. Сгенерировать производный ключ по основному
7. Удалить загруженный ключ
8. Удалить все ключи
>>> 4

Загрузить ключ - введите номер ключа: 1_

Прислоните ТМ номер 1 и нажмите любую клавишу или ESC для отмены...
Общее число ТМ для ввода = 2

ТМ успешно введена, осталось 1 таблеток для ввода!
Прислоните ТМ номер 2 и нажмите любую клавишу или ESC для отмены..._

Ключ 1 введен!

Вы хотите сделать этот ключ активным? (y/n) - y_

Ключ 1 активен!
Нажмите ENTER для продолжения..._
```

Рисунок 14 –Загрузка ключа

5.2.5 Генерация основного ключа

Для того чтобы создать основной ключ, необходимо ввести число 5 в окне администрирования сервера ОЭП и нажать клавишу Enter (см. Рисунок 10).

Далее необходимо ввести число компонентов основного ключа, т.е. число ТМ, на которые будут записаны части ключа.

После появления соответствующего предложения необходимо задать имя ключа, состоящее не более чем из 10 символов.

Затем для каждого компонента с номером **A** ключа после появления предложения «Прислоните ТМ номер **A** и нажмите любую клавишу или ESC для отмены...» необходимо приложить к контактному устройству считывателя информации таблетку, на которую будет записан компонент с номером **A** основного ключа (см. Рисунок 15).

```
0. Выход
1. Информация о ключах
2. Задать/изменить системное имя ФПСУ
3. Установить активный ключ
4. Загрузить ключ
5. Сгенерировать основной ключ
6. Сгенерировать производный ключ по основному
7. Удалить загруженный ключ
8. Удалить все ключи
>>> 5

Сгенерировать основной ключ
Введите число компонентов основного ключа (число ТМ-носителей): 2_

Введите имя основного ключа (не более 10 символов)
Нажмите правый Ctrl для перехода на русский шрифт
#####
>Основной

Прислоните ТМ номер 1 и нажмите любую клавишу или ESC для отмены...
Прислоните ТМ номер 2 и нажмите любую клавишу или ESC для отмены...
Ключ записан на 2 носителей!
Нажмите ENTER для продолжения..._
```

Рисунок 15 – Генерация основного ключа

5.2.6 Генерация производного ключа по основному

Производный ключ может быть создан только после того, как в сервер ОЭП загружен основной ключ. Процедура получения информации о загруженных ключах описана в разделе 5.2.1. Для одного основного ключа может быть создано не более 1000 производных ключей.

Для того чтобы создать производный ключ, необходимо ввести число 6 в окне администрирования сервера ОЭП и нажать клавишу Enter (см. Рисунок 10).

Далее необходимо ввести число компонентов производного ключа, т.е. число ТМ, на которые будут записаны части ключа.

После появления соответствующего предложения необходимо задать имя ключа, состоящее не более чем из 10 символов.

Затем для каждого компонента с номером **A** ключа после появления предложения «Прислоните ТМ номер **A** и нажмите любую клавишу или ESC для отмены...» необходимо приложить к контактному устройству считывателя информации таблетку, на которую будет записан компонент с номером **A** производного ключа (см. Рисунок 16).

```
6. Сгенерировать производный ключ по основному
7. Удалить загруженный ключ
8. Удалить все ключи
>>> 6

Сгенерировать производный ключ по основному
Введите номер основного ключа: 1

Введите число компонентов производного ключа (число ТМ-носителей): 1_

Введите имя производного ключа (не более 10 символов)
Нажмите правый Ctrl для перехода на русский шрифт
#####
>Key01

Прислоните ТМ номер 1 и нажмите любую клавишу или ESC для отмены...
Ключ записан на 1 носителей!
Нажмите ENTER для продолжения...
```

Рисунок 16 – Генерация производного ключа

5.2.7 Удаление загруженного ключа

Для того чтобы удалить ключ из системы, необходимо ввести число 7 в окне администрирования сервера ОЭП и нажать клавишу Enter (см. Рисунок 10).

После появления соответствующего предложения необходимо ввести номер удаляемого ключа и нажать клавишу Enter (см. Рисунок 17).

```
7. Удалить загруженный ключ
8. Удалить все ключи
>>> 7

Удалить загруженный ключ - введите номер ключа: 4

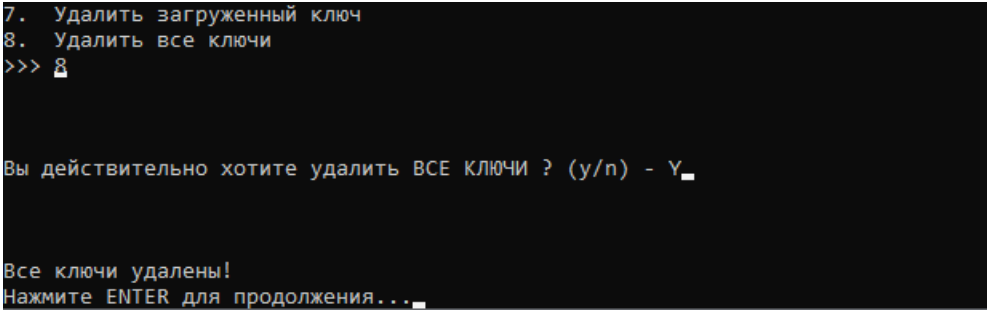
Ключ 4 удален!
Нажмите ENTER для продолжения...
```

Рисунок 17 – Удаление ключа

5.2.8 Удаление всех ключей

Для того чтобы удалить все загруженные ключи, необходимо ввести число 8 в окне администрирования сервера ЭП и нажать клавишу Enter (см. Рисунок 10).

После появления вопроса «Вы действительно хотите удалить ВСЕ КЛЮЧИ ?» для подтверждения необходимо ввести букву Y. Для отказа от удаления следует нажать любую другую клавишу (см. Рисунок 18).



```
7. Удалить загруженный ключ
8. Удалить все ключи
>>> 8

Вы действительно хотите удалить ВСЕ КЛЮЧИ ? (y/n) - Y_

Все ключи удалены!
Нажмите ENTER для продолжения...
```

Рисунок 18 – Удаление всех загруженных ключей