

**Руководство пользователя программы  
«АРМ генерации и загрузки ключей»  
Версия 1.0**

## Содержание

Содержание .....	2
Термины, перечень сокращений и условных наименований .....	3
Аннотация .....	4
1 Описание программы .....	5
2 Использование по назначению.....	6
Лист регистрации изменений .....	8

## Термины, перечень сокращений и условных наименований

<b>АРМ</b>	– Автоматизированное рабочее место
<b>БД</b>	– База данных
<b>ЭП</b>	– Электронная подпись
<b>Linux</b>	– Семейство операционных систем, работающих на основе одноименного ядра
<b>СУБД</b>	– Система управления базами данных
<b>ОС</b>	– Операционная система
<b>ПАКМ</b>	– Программно-аппаратный криптографический модуль
<b>СКЗИ</b>	– Средство криптографической защиты информации

## **Аннотация**

Настоящий документ содержит руководство пользователя программы «АРМ Генерации и записи ключей».

Руководство пользователя состоит из разделов:

- описание программы;
- использование программы.

Руководство пользователя предназначено для сотрудников служб технического сопровождения.

Для эксплуатации и поддержки функционирования программы сотрудникам служб технического сопровождения требуются практические навыки:

- установки, настройки и обслуживания операционной системы семейства Linux и прикладных сервисов в этих операционных системах, установленных, в том числе на виртуальных машинах.

Данное руководство пользователя распространяется на модификации программы «АРМ Генерации и записи ключей», если иное не указано в эксплуатационной документации с выпуском отдельной версии руководства по эксплуатации.

## **1 Описание программы**

Полное наименование – программа «АРМ Генерации и записи ключей».

Краткое наименование – программа «АРМ Генерации и записи ключей», «АРМ Генерации и записи ключей», программа.

«АРМ Генерации и записи ключей» предназначена для реализации полномочий доверенного лица по созданию ключей ЭП и ключей проверки ЭП по обращению заявителей.

## 2 Использование по назначению

### 2.1 Эксплуатационные ограничения

Использование программы отдельно от ПАКМ и среды эксплуатации не предусмотрено.

### 2.2 Использование программы

#### 2.2.1 Порядок действия при выполнении задач программы

В папке инсталляции дистрибутива после подготовительных мероприятий появится бинарный исполняемый файл «keys», являющийся самой программой. Для запуска программы в утилите «Терминал» требуется прописать команду:

```
$> keys
```

Сразу после запуска программы будет предложен выбор опций («0», «1» или «2») с соответствующими названиями действий («0» - выход из программы, «1» - генерация контейнера и запись на СКЗИ «Рутокен», «2» - генерация контейнера и запись на СКЗИ «Форос»). До выбора опции требуется подключить к АРМ СКЗИ «Рутокен» или СКЗИ «Форос». После подключения СКЗИ требуется сделать выбор операции путем ввода числа в строку ввода и последующим нажатием клавиши «return» запустить отработку программы. Требуется дождаться сообщения на экране о удаче/неудаче записи контейнера на СКЗИ, затем отключить СКЗИ из АРМ.

Для освоения программы администратору рекомендуется самостоятельное изучение предметной области назначения программы и смежных компонентов, в сочетании с изучением соответствующей рабочей и эксплуатационной документации.

#### 2.2.2 Порядок контроля работоспособности

Проверка работоспособности установленных компонентов программы осуществляется методом визуального контроля реакций на регламентные запросы и команды администратора.

#### 2.2.3 Перечень возможных неисправностей

В процессе эксплуатации могут возникать такие проблемы, как зависания программы, медленная работа, отказы в управлении или потери связи между ее компонентами или компонентами интеграционного взаимодействия.

При появлении данных проблем необходимо обратиться в службу технического сопровождения и эксплуатации в соответствии с регламентом взаимодействия.

#### 2.2.4 Действия в случаях обнаружения несанкционированного вмешательства в данные

В случае обнаружения несанкционированного вмешательства в данные, необходимо не совершая никаких действий в интерфейсе, сообщить о факте несанкционированного вмешательства Администратору информационной безопасности предприятия.

