



# DRECRYPT

Руководство по установке

## Содержание

|  |    |
|--|----|
| Аннотация .....                                    | 3  |
| Термины и сокращения .....                         | 4  |
| 1. Введение .....                                  | 5  |
| 1.1. Требования к квалификации установщика .....   | 5  |
| 1.2. Системные Требования .....                    | 5  |
| 1.2.1. Аппаратное Обеспечение .....                | 5  |
| 1.2.2. Программное Обеспечение .....               | 5  |
| 2. Состав компонентов для установки DRECRYPT ..... | 6  |
| 3. Установка и настройка основных пакетов .....    | 7  |
| 3.1. Установка пакетов .....                       | 7  |
| 3.2. Настройка локализации .....                   | 7  |
| 3.3. Настройка Postgres Pro и ODBC .....           | 8  |
| 3.4. Установка пакетов и библиотек DRECRYPT .....  | 8  |
| 4. Установка и наполнение БД .....                 | 10 |
| 4.1. Установка БД .....                            | 10 |
| 4.2. Наполнение CAS_DB .....                       | 10 |
| 4.3. Наполнение БД CRS .....                       | 10 |
| 5. Запуск DRE Скрыт .....                          | 12 |
| 6. Настройка работы с SMS .....                    | 13 |

## Аннотация

Данный документ содержит руководство по установке и первоначальной настройке комплекса DRECRYPT (далее - Система), а также описание системных требований для компонентов.

Документ предназначен для технических специалистов, в обязанности которых входит установка и первоначальная настройка комплекса DRECRYPT.

Перед установкой комплекса рекомендуется изучить технические особенности построения и функционирования DRECRYPT. Данная информация содержится в документах "DRECRYPT. Общее описание" и "DRECRYPT. Техническое описание".

Данное описание является документом для внутреннего пользования, т.е. распространяется среди сотрудников и партнеров компании.

## Термины и сокращения

| Термин                        | Определение  |
|-------------------------------|--|
| Система управления подписками | Система, принимающая, обрабатывающая и хранящая информацию о подписках абонентов и иную служебную информацию.  |
| Система условного доступа     | Система управления доступом абонентов к предоставляемым оператором услугам.  |
| DVB-Simulcrypt                | DVB-стандарт архитектуры, позволяющей функционировать множеству СУД в рамках единой головной станции. Этот стандарт определяет архитектуру головного оборудования и СУД, временные параметры взаимодействия компонентов, их интерфейсы и формат сообщений. |
| ECM-сообщение                 | Сообщение, которое передается ресиверу абонента и содержит в зашифрованном виде CW, дескремблирующие транслируемый поток.  |
| EMM-сообщение                 | Сообщение, которое передается ресиверу абонента и содержит CW_enc_key/служебные данные/информацию о правах доступа/специальные команды. Разные типы EMM передают разную информацию.  |

| Сокращение | Расшифровка   |
|------------|---|
| ECM        | Entitlement Control Message, ECM-сообщение                  |
| EMM        | Entitlement Management Message, EMM-сообщение               |
| CAS        | Conditional access system, система условного доступа        |
| SMS        | Subscriber Management System, система управления подписками |



## 1. Введение

### 1.1. Требования к квалификации установщика

Для установки DRE Срупт необходимо наличие навыков работы с ОС Debian, а именно:

- создание разделов дисков, установка пакетов
- создание и настройка сетевых подключений
- запуск служб, настройка автозапуска служб
- установка и настройка Postgres Pro
- создание и работа с БД под управлением Postgres Pro

### 1.2. Системные Требования

Для установки DRECRYPT желательно выделить отдельный сервер. Рекомендуется устанавливать сервер в локальной сети, защищенной от доступа извне.

#### 1.2.1. Аппаратное Обеспечение

- Процессор — 2 или 4 ядра;
- Оперативная память — 2 GB (рекомендуется 4 GB);
- Жесткий диск — 2 × 150 GB (зависит от объема БД);
- Головное оборудование, соответствующее стандарту DVB-Simulcrypt ver. 2.

#### 1.2.2. Программное Обеспечение

- Операционная система
  - Debian 8x64
- Пакеты:
  - postgrespro-std-11
  - build-essential
  - gcc-4.9
  - libjsoncpp-dev
  - libzmq3
  - libboost-all-dev версии 1.55 или более поздних + связанные пакеты (см. список библиотек ниже)
  - unixodbc-dev
  - odbc-postgresql
  - tdsodbc
  - libcurl3

## 2. Состав компонентов для установки DRECRYPT

При установке, настройке и работе DRE Crypt используются несколько подсистем, каждая из которых отвечает за часть общего функционала.

Ниже приводится перечень установочных компонентов данных подсистем, входящих в комплект поставки.

1. Архив ***cas\_db\_sch\_X.X.X.zip*** со сборкой для создания схемы баз данных, включающий:
  - папку *sql*, содержащую файлы скриптов создания схем баз данных, таблиц и пользователей
  - заголовочные файлы скриптов создания БД, схем, пользователей (*create\_schema.sh*, *create\_db.sh*, *create\_users.sh*, *install.sh*)
2. Архив ***cas\_db\_api\_X.X.X.zip*** со сборкой для установки API управления базами данных, включающий:
  - Папку *scripts* с файлами скриптов для создания, наполнения и поддержания БД.
  - Папку *sql* с процедурами работы с БД
  - Папку *types* со структурами *sql*
  - Файлы *install.sh* и *install.bat* для установки подсистемы.
3. ***cas\_emmg\_core\_X.X.X\_amd64.deb*** - файлы основного исполнительного модуля EMMG
4. ***cas\_emmg\_balancer\_X.X.X\_amd64.deb*** - дополнительные файлы модуля EMMG
5. ***injector\_lib-X.X.X-amd64.deb*** - дополнительная библиотека модуля EMMG
6. ***hes\_core-X.X.X-linux-x86\_64-gcc49.deb*** - дополнительная библиотека модуля EMMG
7. ***cas\_ecmg\_core\_X.X.X\_amd64.deb*** - файлы основного исполнительного модуля ECMG

## 3. Установка и настройка основных пакетов

### 3.1. Установка пакетов

На машину, которая будет использоваться как сервер DRECRYPT, необходимо предварительно установить ОС Debian 8 x64.

После этого необходимо выполнить следующее:

1. Подключите репозиторий пакетов, предназначенный для вашей операционной системы. Конкретные адреса репозитория и команды для их подключения в поддерживаемых дистрибутивах Linux вы можете найти на [Странице загрузки](#) для соответствующей версии Postgres Pro.
2. Установите следующие пакеты:

```
sudo apt-get install postgrespro-std-11 gcc-4.9 build-essential libjsoncpp-dev libzmq3 libboost-all-dev  
unixodbc-dev odbc-postgresql tdsodbc libcurl3
```



- libboost-all-dev (версия 1.55 или более поздняя + связанные пакеты. В процессе установки пакета libboost-all-dev возможны задержки до нескольких минут, что не является сбоем. Не прерывайте процесс установки)

В процессе эксплуатации DRE Crypt возможно обновление установленных системных пакетов. Для этого необходимо последовательно выполнить две команды:

```
sudo apt-get update  
sudo apt-get upgrade
```

### 3.2. Настройка локализации

1. Выполните команду:

```
sudo dpkg-reconfigure --plow locales
```

2. Убедитесь, что в списке локализаций отмечена **ru\_RU.UTF-8**. Если это не так, выберите её в добавок к уже имеющимся и нажмите *Ok*.
3. Проверьте, что вывод имеет вид:

```
Generating locales (this might take a while)...  
en_US.UTF-8... done  
ru_RU.UTF-8... done  
Generation complete.
```

### 3.3. Настройка Postgres Pro и ODBC

Следующие действия выполняются только после установки пакета Postgres Pro:

1. Открыть конфигурационный файл **postgresql.conf** для редактирования

```
sudo nano /etc/pgpro/std-11/main/postgresql.conf
```

2. В файле выполнить следующее:


- изменить значение параметра `listen_addresses`, как показано ниже, и раскомментировать соответствующую строку:

```
listen_addresses = '*'           # what IP address(es) to listen on;
```

3. Настройте конфигурационный файл **pg\_hba.conf**, чтобы БД Postgres Pro могли принимать соединения от DRE Crypt
4. Открыть конфигурационный файл **odbc.ini** для и пропишите ODBC для связи с БД CRS, CAS, SMS.
5. Перезапустить Postgres Pro:

```
sudo /etc/init.d/postgrespro-std-11 restart
```

### 3.4. Установка пакетов и библиотек DRE Crypt

 Установку основных функциональных компонентов проводить только после установки всех системных компонентов, а также дополнительных библиотек.

Компоненты ECMG и EMMG поставляются в виде *deb*-пакетов (см. выше, раздел "[Компоненты, необходимые для установки](#)").

Для установки требуется:

1. Убедиться, что текущий пользователь - администратор DRE Crypt (не postgres).
2. Скопировать файлы
  - a. **hes\_core-X.X.X-linux-x86\_64-gcc49.deb**
  - b. **injector\_lib-X.X.X-amd64.deb**
  - c. **cas\_emmg\_core\_X.X.X\_amd64.deb**
  - d. **cas\_emmg\_balancer\_X.X.X\_amd64.deb**
  - e. **cas\_ecmg\_core\_X.X.X\_amd64.deb** на сервер DRE Crypt.





В данный список дополнительно могут входить deb-пакеты, содержащие файлы подключаемых библиотек. Перечень таких библиотек и их назначение зависит от нужд Заказчика (определяется задачами, которые решает DRECRYPT).

3. Перейти в папку со скопированными пакетами.
4. Последовательно установить пакеты с помощью команды (заменяв `filename.deb` на название `deb`-пакета):

```
sudo dpkg -i [filename.deb]
```

5. После установки всех пакетов выполнить команду:

```
sudo ldconfig
```

В результате пакеты будут установлены в папках:

**/etc** - содержит подпапки, соответствующие названиям компонентов. В подпапках находятся конфигурационные файлы компонентов;

**/etc/init.d** - содержит файл скрипта для запуска `cas_ectg_core`, `cas_emtg_core`, `cas_emtg_balancer` в виде фоновых служб;

**/usr/local/bin** - содержит исполняемые файлы компонентов;

**/usr/local/lib** - содержит файлы библиотек компонентов.

## 4. Установка и наполнение БД

### 4.1. Установка БД

В DRE Crypt используются следующие БД:

- CAS\_DB;
- CRS:
  - Схема Carousel;
  - Схема OPKEY.

**Наполнение CAS\_DB будет различаться в зависимости от того, какие наборы ключей нужны для работы. Поэтому, если необходимо работать с разными наборами ключей, то под каждую задачу / приемное оборудование и т.д., требующую свой специфичный набор ключей, необходимо развернуть отдельный экземпляр DRE Crypt, каждый со своей базой CAS\_DB.**

Carousel и OPKEY являются схемами БД CRS. Carousel заполняется в процессе работы DRECRYPT и не требует дополнительных настроек. Начальная настройка схемы OPKEY описана в соответствующем разделе, а также в документе "DRE Crypt. Руководство администратора".

По умолчанию, БД будут созданы в табличном пространстве pg\_default (табличное пространство по умолчанию для Postgres Pro).

Для установки БД необходимо под пользователем postgres последовательно запустить следующие скрипты:

1. /home/cas\_db\_sch/create\_db.sh
2. /home/cas\_db\_sch/install\_full.sh
3. /home/cas\_db\_api/install\_full.sh

### 4.2. Наполнение CAS\_DB

Наполнение БД, с которыми работает DRE Crypt (в частности - CAS\_DB), должно осуществляться с помощью скриптов, которые должны храниться в папке scripts внутри распакованной сборки cas\_db\_api (в нашем примере это /home/cas\_db\_api/scripts/). Скрипты запускаются под пользователем postgres. После занесения данных с помощью скрипта необходимо проверить лог файл на отсутствие ошибок (находится в той же папке, что и скрипт), а также что в указанной схеме внесены соответствующие изменения. Дополнительно может потребоваться более тонкая настройка таблиц.

Особенности наполнения CAS\_DB зависят от многих факторов:

- нужд Заказчика (задач, которые решает DRE Crypt);
- источника данных для наполнения БД;
- СУБД, под которой работает источник данных (если он отличается от СУБД для CAS\_DB);
- оборудования, используемого на приемной стороне (в STB);
- и т.д.

### 4.3. Наполнение БД CRS

С помощью заполнения таблиц БД CRS производится настройка:

- забор данных из SMS
- генерации CW\_enc\_keys (хранятся в схеме OPKEY)
- генерации и рассылки EMM

При установке в БД CRS заносится начальное наполнение, с которым можно проводить тестовые запуски DRE Срут. В целом для тестового запуска необходимо добавить номер провайдера для всех заданий в таблице `opkey.resources`, и настроить задания в таблице `opkey.scheduler`.

Однако при разворачивании рабочего комплекса DRE Срут наполнение данной БД необходимо менять в соответствии с нуждами Заказчика.

Общие принципы наполнения БД CRS описаны в соответствующем разделе документа "DRECRYPT. Руководство администратора".

## 5. Запуск DRECRYPT

⚠ Перед запуском DRE Crypt необходимо убедиться, что запущена СУБД Postgres Pro.

Для начала работы основных функциональных компонентов DRE Crypt необходимо запустить исполняемые файлы, находящиеся в папке ***/usr/local/bin*** :

1. Убедиться, что текущий пользователь - администратор DRE Crypt (запуск от пользователя *postgres* невозможен).
2. Запуск Balancer:

```
/etc/init.d/cas_emmg_balancer start
```

3. Запуск EMMG:

```
cas_emmg_core
```

или (перенаправление лога в файл)

```
cas_emmg_core > log_file
```

или (перенаправление лога в файл и запуск процесса в фоновом режиме)

```
cas_emmg_core > log_file &
```

4. Запуск ECMG:

```
/etc/init.d/cas_ecmg_core start
```

Расположение лог-файлов основных компонентов задается в их конфигурационных файлах. По умолчанию лог-файлы будут создаваться в папке, из которой запускался исполняемый файл. Рекомендуется указать в конфигурационных файлах абсолютные пути к логам.

Подробное описание файлов конфигурации содержится в документе "DRE Crypt. Руководство администратора".



## 6. Настройка работы с SMS

Настройка взаимодействия DRE Срут и SMS может различаться в зависимости от СУБД, под которой работает SMS.

Если SMS работает под управлением Postgre Pro, то никаких дополнительных действий не требуется.



**Обратите внимание!** Одновременно DRE Срут может работать только с одним SMS.