КРИПТОКОМ

УТВЕРЖДЕН
СЕИУ.00009-04 34 10 - ЛУ

СРЕДСТВО КРИПТОГРАФИЧЕСКОЙ ЗАЩИТЫ ИНФОРМАЦИИ
«МагПро КриптоПакет» 3.0

Программа генерации файла инициализации программного ДСЧ mkseed.
Руководство по использованию

СЕИУ.00009-04 34 10
Листов 11

Литера О

2018

Подп. и дата | Инв. № дубл. | Взам. инв.№ | Подп. и дата | Инв.№ подп.

Аннотация

Настоящий документ содержит руководство по использованию программы mkseed из состава «МагПро КриптоПакет» 3.0.

Содержание

Порядковый № изменения	Подпись лица, ответственного за изменение	Дата внесения изменения

1 НАЗНАЧЕНИЕ ПРОГРАММЫ

Программа mkseed из комплекта «МагПро КриптоПакет» 3.0 выполняет создание файла инициализации программного датчика случайных чисел.

Порядковый № изменения	Подпись лица, ответственного за изменение	Дата внесения изменения

2 УСЛОВИЯ РАБОТЫ ПРОГРАММЫ

Для выполнения клавиатурной инициализации клавиатурного ДСЧ программа использует текстовый интерфейс.

Задание режимов работы выполняется с помощью опций командной строки.

Программа не должна запускаться в ssh-сессии.

Программа предназначена для работы в следующих операционных системах:

Windows 7 SP1/8.1/10;
Windows Server 2008R2 SP1/2012/2012R2/2016
Debian GNU/Linux 7(wheezy)/8(jessie)/stretch;
Linux Mint 17.x, 18.x, Linux Mint Debian Edition 2
Ubuntu 14.04, 16.04;
RedHat Enterprise Linux 6, 7;
CentOS 6, 7;
SUSE Linux 11, 12;
OpenSUSE 42.2, 42.3;
OS EMIAS 1.0;
Альт Линукс 6, 7, 8;
МСВСфера Сервер 6.3, МСВСфера АРМ 6.3;
Атликс 3.1;
Гослинукс ІС4;
FreeBSD 10.x, 11.x;
Oracle Solaris 10, 11;
MacOS 10.12;
Rosa Enterprise Desktop (RED) X2, X3;
Rosa Enterprise Linux Server (RELS) 6, 7; РОСА КОБАЛЬТ 1.0;
Astra Linux Special Edition РУСБ.10015-07.

Порядковый № изменения	Подпись лица, ответственного за изменение	Дата внесения изменения

3 ФУНКЦИИ ПРОГРАММЫ

Программа осуществляет формирование файла инициализации программного датчика случайных чисел.

Для формирования этого файла могут использоваться аппаратные генераторы случайных чисел изделий «Вьюга», «Аккорд», «Соболь» и «АПМДЗ-И/М2», а также клавиатурная инициализация, основанная на случайности времени нажатия пользователя на клавиши.

Порядковый № изменения	Подпись лица, ответственного за изменение	Дата внесения изменения

4 Обеспечение информационной безопасности при использовании «МагПро КриптоПакет» 3.0

Надежная криптографическая защита данных при использовании «МагПро КриптоПакет» 3.0 обеспечивается только в том случае, если эксплуатация «МагПро КриптоПакет» 3.0 осуществляется в строгом соответствии с требованиями документа «Средство криптографической защиты информации «МагПро КриптоПакет» 3.0. Правила пользования» (СЕИУ.СЕИУ.00009–04 94).

Порядковый № изменения	Подпись лица, ответственного за изменение	Дата внесения изменения

5 УСТАНОВКА И НАСТРОЙКА ПРОГРАММЫ

Программа устанавливается и настраивается автоматически при установке утилиты openssl (см. «Средство криптографической защиты информации «МагПро КриптоПакет» 3.0. Утилита openssl. Руководство по использованию», СЕИУ.00009-04 34 03).

Для формирования файла инициализации используется тот датчик случайных чисел, на использование которого настроен «МагПро КриптоПакет» 3.0. В случае, если «МагПро КриптоПакет» 3.0 настроен на программный ДСЧ, будет использована клавиатурная инициализация.

Параметр -c позволяет явно указать файл конфигурации «МагПро КриптоПакет» 3.0, который следует использовать.

Порядковый № изменения	Подпись лица, ответственного за изменение	Дата внесения изменения

6 ИСПОЛЬЗОВАНИЕ ПРОГРАММЫ

6.1 Формат запуска программы

Формат запуска программы:

```
mkeedey [опции]
```

По умолчанию (если не указаны опции) программа выводит краткую справку об опциях.

6.2 Доступные опции

```
-V              - отобразить номер версии программы
-r [имя файла] - запись файла инициализации программного ДСЧ
                 если имя файла не указано, будет использован файл
                 с именем, заданным конфигурацией системы
-c <имя файла> - использовать указанный файл конфигурации openssl
-f              - удалить существующий файл инициализации программного ДСЧ
                 перед созданием нового файла
```

6.3 Создание файла инициализации

Для создания файла инициализации программного ДСЧ необходимо запустить программу mkseed с параметром -r.

Стандартное (умолчательное) расположение файла инициализации:

В ОС Windows — `%APPDATA%\MagProCryptoPack\random_seed`

В POSIX-системах — `$HOME/.magprocryptopack/random_seed`

При использовании аппаратного ДСЧ возможно создание файла инициализации только с умолчательным расположением. В случае использования клавиатурной инциализации также возможно явное указание имени файла инициализации, которое указывается в качестве значения параметра -r.

6.4 Создание файла с использованием клавиатурной инициализации

В случае использования клавиатурной инициализации программа предлагает пользователю последовательно вводить с клавиатуры указанные цифры. Ввод осуществляется группами по 9 символов (последняя группа может быть короче). В начале каждой строки приглашения ввода символов в скобках выводится количество введенных символов и общее количество требуемых символов, разделенные косой чертой. По результатам статистического анализа накопленной случайности количество требуемых символов может увеличиваться.

6.5 Создание файла с использованием аппаратного ДСЧ

При использовании аппаратного ДСЧ создание файла инициализации производится без взаимодействия с пользователем.

Порядковый № изменения	Подпись лица, ответственного за изменение	Дата внесения изменения

6.6 Обновление файла инициализации

Если файл инициализации уже существует, программа завершит работу, не совершая никаких действий. Для обновления файла инициализации необходимо указать параметр -f, в этом случае программа сначала удалит существующий файл инициализации, а затем создаст новый обычным порядком.

Порядковый № изменения	Подпись лица, ответственного за изменение	Дата внесения изменения

Лист регистрации изменений									
Номера листов (страниц)					Всего листов (страниц) в докум.	№ документа	Входящий сопроводительного докум. и дата	Подпись	Дата
Изм.	измененных	замененных	новых	аннулированных					

Порядковый № изменения	Подпись лица, ответственного за изменение	Дата внесения изменения