КРИПТОКОМ

УТВЕРЖДЕН
СЕИУ.00009-05 34 10 - ЛУ

СРЕДСТВО КРИПТОГРАФИЧЕСКОЙ ЗАЩИТЫ ИНФОРМАЦИИ
«МагПро КриптоПакет» 4.0

Программа генерации файла инициализации программного ДСЧ mkseed. Руководство по использованию

СЕИУ.00009-05 34 10
Листов 11

Литера О

2022

Аннотация

Настоящий документ содержит руководство по использованию программы mkseed из состава «МагПро КриптоПакет» 4.0.

Содержание

1 Назначение программы 4

2 Условия работы программы 5

3 Функции программы 6

4 Обеспечение информационной безопасности при использовании «МагПро КриптоПакет» 4.0 7

5 Установка и настройка программы 8

6 Использование программы 9

6.1 Формат запуска программы 9
6.2 Доступные опции 9
6.3 Создание файла инициализации 9
6.4 Создание файла с использованием клавиатурной инициализации 10
6.5 Создание файла с использованием аппаратного ДСЧ 10
6.6 Обновление файла инициализации 10
6.7 Молчаливый режим работы 10
6.8 Код завершения программы 10

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

1 Назначение программы

Программа mkseed из комплекта «МагПро КриптоПакет» 4.0 выполняет создание файла инициализации программного датчика случайных чисел (далее — ДСЧ).

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

2 Условия работы программы

Для выполнения инициализации программного ДСЧ программа использует текстовый интерфейс.

Задание режимов работы выполняется с помощью опций командной строки.

Программа предназначена для работы в следующих операционных системах:

Windows 8.1/10;
Windows Server 2012/2016/2019;
Debian GNU/Linux 9(stretch)/10(buster)/11(bullseye);
Ubuntu 14.04, 16.04, 18.04, 20.04;
Linux Mint 19.x, 20.x, Linux Mint Debian Edition 4;
RedHat Enterprise Linux 7, 8;
CentOS 7, 8;
SUSE Linux 12, 15;
OpenSUSE 15.1, 15.2;
EMIAS OS 1.0, 2.0;
Дистрибутивы Альт на базе платформ 8 и 9, включая Альт Сервер, Альт Рабочая станция, Альт Рабочая станция К, Альт Образование, Альт 8 СП, Sipmly Linux;
МСВСфера Сервер 7.3, МСВСфера АРМ 7.3;
Гослинукс IC6;
РЕД ОС 7.2, 7.3;
Rosa Enterprise Desktop (RED) X4;
Rosa Enterprise Linux Server (RELS) 7.3;
Rosa Enterprise Linux Desktop (RELD) 7.3;
РОСА КОБАЛЬТ;
Astra Linux Special Edition Смоленск 1.6 aka исп.1, 1.7;
Astra Linux Special Edition Новороссийск;
Astra Linux Common Edition 2.12;
Numa Edge 1.0;
FreeBSD 12.x, 13.x;
MacOS 10.15, 11;
Sun Solaris 10, 11;
OpenWRT 19.07, 21.02.

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 «М-526», аппаратные ГСЧ сертифицированных устройств с интерфейсом PKCS#11, 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» 4.0

Надежная криптографическая защита данных при использовании «МагПро КриптоПакет» 4.0 обеспечивается только в том случае, если эксплуатация «МагПро КриптоПакет» 4.0 осуществляется в строгом соответствии с требованиями документа «Средство криптографической защиты информации «МагПро КриптоПакет» 4.0. Правила пользования» (СЕИУ.00009–05 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» 4.0. Утилита openssl. Руководство по использованию», СЕИУ.00009-05 34 03).

Для формирования файла инициализации используется тот датчик случайных чисел, на использование которого настроен «МагПро КриптоПакет» 4.0. В случае, если «МагПро КриптоПакет» 4.0 настроен на программный ДСЧ, будет использована клавиатурная инициализация.

Параметр -c позволяет явно указать файл конфигурации «МагПро КриптоПакет» 4.0, который следует использовать.

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

6 Использование программы

6.1 Формат запуска программы

Формат запуска программы:

```
mkseed [опции]
```

По умолчанию (если не указаны опции) программа создаст файл начального заполнения программного ДСЧ в соответствии с настройками СКЗИ «МагПро КриптоПакет».

Программа поддерживает следующие опции:

6.2 Доступные опции

```
-V              - отобразить номер версии программы;
-r <имя файла>  - запись файла инициализации программного ДСЧ,
                  если параметр не указан, будет использован файл
                  с именем, заданным конфигурацией системы;
-c <имя файла>  - использовать указанный файл конфигурации openssl
                  если параметр не указан, будет использован файл,
                  заданный переменной окружения OPENSSL_CONF,
                  а если и её нет, то файл с именем по умолчанию;
-f              - удалить существующий файл инициализации программного ДСЧ
                  перед созданием нового файла;
-q              - молчаливый режим работы: если файл инициализации уже
                  существует, то программа завершится с кодом 0, не выводя
                  никаких сообщений.
```

6.3 Создание файла инициализации

При создании файла инициализации программа зачитывает файл конфигурации СКЗИ «МагПро КриптоПакет». Имя этого файла может быть указано в параметре -c. Если этот параметр не задан, используется имя файла из переменной окружения `OPENSSL_CONF`, а если и эта переменная окружения не задана, то зачитывается файл по умолчательному пути /opt/cryptopack4/ssl/openssl.cnf (для ОС Windows уполчательного пути нет).

Далее программа определяет, какой ДСЧ будет использован при создании файла инициализации:

- если установлена переменная окружения `RNG`, будет использован ДСЧ, указанный в этой переменной;
- если переменная окружения `RNG` не установлена, то будет использован ДСЧ, указанный в одноименном параметре секции `cryptocom_options` файла конфигурации;
- если же такого параметра в файле конфигурации нет, будет использована клавиатурная инициализация.

При использовании аппаратного ДСЧ возможно создание файла инициализации только с умолчательным расположением:

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

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

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

В случае использования клавиатурной инициализации расположение создаваемого файла берётся из:

- переданного программе параметра -r;
- переменной окружения `RNG_PARAMS`;
- параметра `RNG_PARAMS` секции `cryptocom_options` файла конфигурации.

Если ничто из перечисленного не задано, используется умолчательное расположение файла инициализации (см.выше).

Программ выведет на экран имя создаваемого файла инициализации.

6.4 Создание файла с использованием клавиатурной инициализации

В случае использования клавиатурной инициализации программа предлагает пользователю последовательно вводить с клавиатуры указанные символы. Ввод осуществляется группами по 3 символа, по 3 группы в строке, (последняя строка и последняя группа могут быть неполными).

В начале каждой строки приглашения ввода символов в скобках выводится количество введенных символов и общее количество требуемых символов, разделенных косой чертой.

В случае некорректного ввода количество требуемых символов увеличивается.

6.5 Создание файла с использованием аппаратного ДСЧ

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

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.

6.7 Молчаливый режим работы

Если при запуске программа обнаруживает, что файл инициализации уже существует (и не указан параметр -f), то программа выдаст соответствующее сообщение и завершит работу. Параметр -q позволяет избежать вывода этого сообщения (полезно при использовании программы в скриптах).

6.8 Код завершения программы

Если программа завершила работу с кодом 0, это во всех случаях означает, что в системе имеется корректный, готовый к использованию файл инициализации (неважно, был ли он создан в ходе работы программы или уже существовал до её запуска).

Код, отличный от 0, (обычно это код 1) означает, что файла инициализации нет или что-то с ним не так.

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