КРИПТОКОМ

УТВЕРЖДЕН
СЕИУ.00009-05 34 11 - ЛУ

СРЕДСТВО КРИПТОГРАФИЧЕСКОЙ ЗАЩИТЫ ИНФОРМАЦИИ
«МагПро КриптоПакет» 4.0

Программа генерации файла инициализации программного ДСЧ gmkseed.
Руководство по использованию

СЕИУ.00009-05 34 11
Листов 14

Литера О

2022

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

Аннотация

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

Содержание

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

1 Назначение программы

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

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

2 Условия работы программы

Для выполнения инициализации программного ДСЧ программа использует графический интерфейс.

Задание режимов работы выполняется с помощью опций командной строки.

Программа предназначена для работы в операционных системах Windows, Linux и macOS.

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

3 Функции программы

Программа осуществляет формирование файла инициализации программного датчика случайных чисел с использованием графической инициализации.

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

Для ОС семейства Windows 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 ОС семейства Linux и macOS программа устанавливается из отдельного пакета gmkseed стандартными для ОС средствами.

Программа использует конфигурационный файл утилиты openssl и не требует отдельной настройки. 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 Запуск программы

6.1.1 Формат запуска программы

Программу можно запускать как двойным щелчком мыши, так и из командной строки. При запуске из командной строки можно указать дополнительный параметры работы программы.

Формат запуска программы из командной строки:

в ОС Windows находясь в папке установки СКЗМ «МагПро КриптоПакет»

```
gmkseed [опции]
```

в ОС Linux и macOS

```
/opt/cryptopack4/bin/gmkseed [опции]
```

Программа поддерживает следующие 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.
```

6.1.2 Особенности создания файла инициализации для пользователя root

В ОС Linux в процессе настройки СКЗИ часто требуется создать файл инициализации для пользователя root.

При работе с локальной консоли для этого следует использовать команду

```
sudo -H /opt/cryptopack4/bin/gmkseed
```

При удалённом запуске если есть возможность подключиться к серверу под пользователем root, создание файла инициализации выполняется простым вызовом из-под этого пользователя команды

```
/opt/cryptopack4/bin/gmkseed
```

Если подключиться к серверу под пользователем root невозможно, для удалённого создания файла инициализации необходимо

- проверить, есть ли в файле /etc/sudoers строка Defaults env_keep, если есть, то либо закомментировать её, либо добавить в неё переменные XAUTHORITY и DISPLAY;
- запустить gmkseed командой
  `XAUTHORITY=~/.Xauthority sudo -H /opt/cryptopack4/bin/gmkseed`

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

6.1.3 Как программа определяет, где создавать файл инициализации

При старте 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).

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:

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

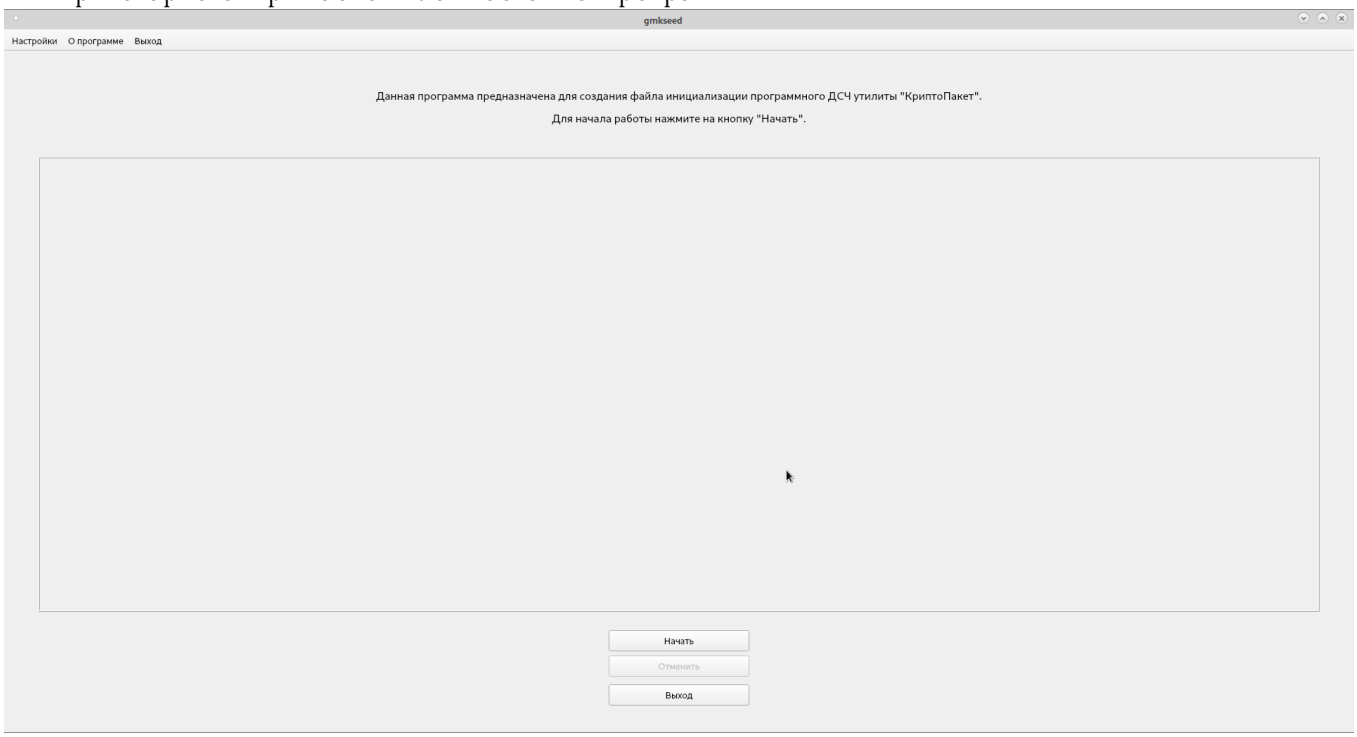
В ОС Linux и macOS — `$HOME/.magprocryptopack/random_seed`

Программ выведет на экран имя создаваемого файла инициализации.

При необходимости расположение файла инициализации можно изменить в окне настроек программы (см.6.6).

6.2 Главное окно программы

При старте открывается главное окно программы

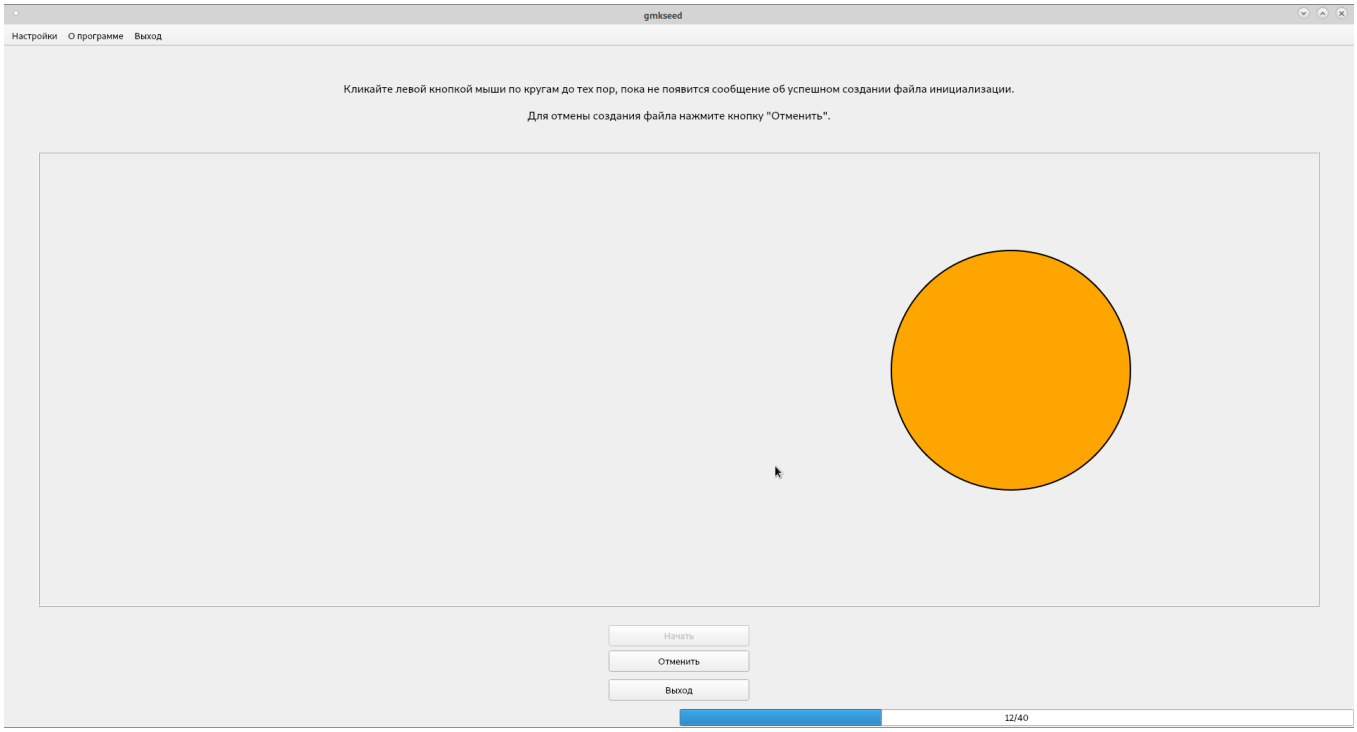


6.3 Создание файла инициализации

Для создания файла инициализации необходимо нажать кнопку «Начать».

Программа рисует в случайных местах экрана цветные круги, пользователь должен нажать мышкой на каждый круг. Всего будет нарисовано 40 кругов, то есть от пользователя потре-

буется 40 «попаданий» (в некоторых случаях требуемое число «попаданий» в процессе работы программы может быть увеличено).

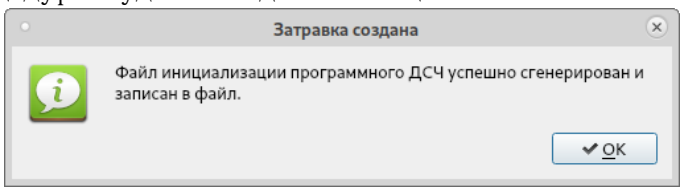


В правом нижнем улгу выводится количество «попаданий» и общее количество кругов, которые будут выведены, разделенные косой чертой.

В случае, если пользователь не попадёт в круг, ему назначается «штраф»: количество «попаданий» уменьшается.

Процедуру можно прервать, нажав на кнопку «Отменить» (программа вернётся в главное окно) или «Выход» (программа завершит работу). В этих случаях файл инициализации создан не будет.

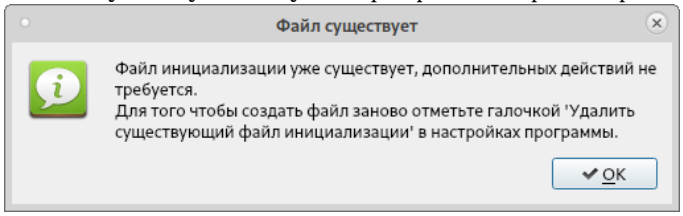
По завершении процедуры будет выведено сообщение



после чего программа завершит свою работу.

6.4 Обновление файла инициализации

Если файл инициализации уже существует, программа при старте выдаст предупреждение

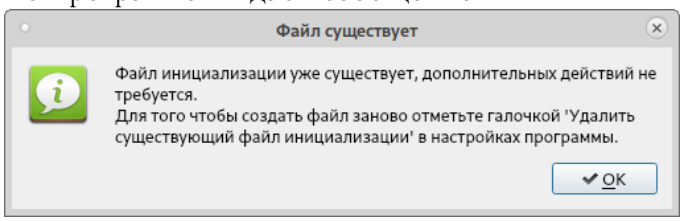


и кнопка «Начать» будет неактивна. Для того, чтобы пересоздать существующий файл инициализации, необходимо запустить программу с ключом -f или выставить в окне настроект программы флаг «Удалить существующий файл инициализации» (см.6.6).

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

6.5 Молчаливый режим работы

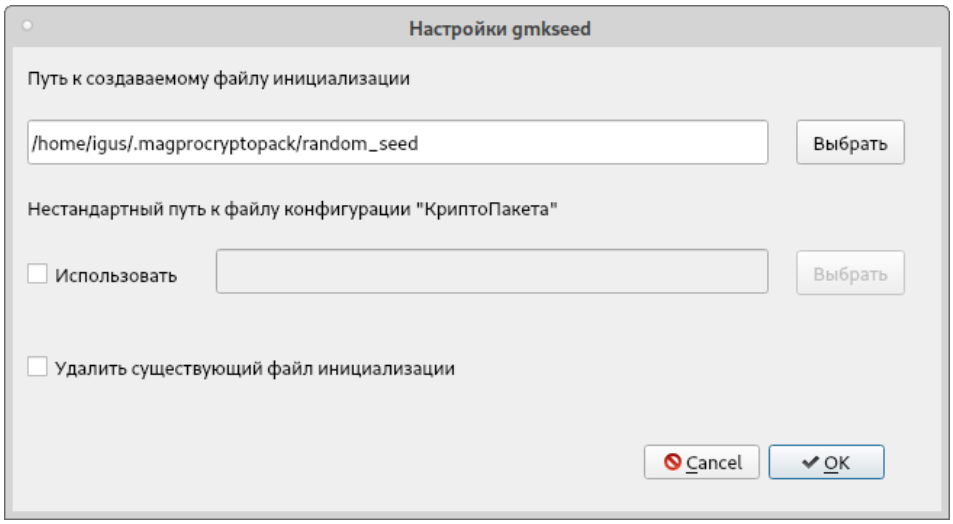
Если при запуске программа обнаруживает, что файл инициализации уже существует (и не указан параметр -f), то программа выдаст сообщение



Параметр -q позволяет избежать вывода этого сообщения, программа в этом случае завершит работу, никак не взаимодействуя с пользователем (полезно при использовании программы в скриптах).

6.6 Окно настроек программы

Если в главном окне программы выбрать пункт меню «Настройки», откроется окно настроек программы



В строке «Путь к создаваемому файлу инициализации» будет выведен путь к файлу инициализации, который программа определила при запуске (см.6.1.3). Можно вручную изменить этот путь, просто отредактировав эту строку или нажав на кнопку «Выбрать» и выбрав новое место расположения файла инициализации.

Окно настроек позволяет также зачитать альтернативный конфигурационный файл, для этого нужно в строке «Нестандартный путь к файлу конфигурации "КриптоПакета»> установить флаг «Использовать» и ввести (вручную или с использованием кнопки «Выбрать») путь к файлу конфигурации.

Флаг «Удалить существующий файл инициализации» позволяет пересоздать файл инициализации в случае, если он уже существует (старый файл будет удалён при нажатии кнопки «Начать»).

Поскольку создание файла инициализации в норме необходимо выполнять один раз при установке программы, возможность сохранения настроек не предусмотрена.

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

6.7 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