

УТВЕРЖДЕН

0230259.01428-01 92 01-ЛУ

ПРОГРАММНЫЙ ДАТЧИК ПСЕВДОСЛУЧАЙНЫХ ЧИСЕЛ

Руководство пользователя

0230259.01428-01 92 01

Листов 17

Инв. № подл.	Подп. И дата	Взам. Инв. №	Инв. № дубл.	Подп. И дата

2023

Литера О₁

СОДЕРЖАНИЕ

1. Общие сведения.....	3
2. Назначение и условия применения	4
2.1. Назначение и общие условия применения ПДСЧ	4
2.2. Условия применения ПДСЧ в ОС Windows	4
2.3. Условия применения ПДСЧ в ОС MCBC, Astra Linux, Эльбрус, Эльбрус-Д, ЗОСРВ «Нейтрино».....	4
2.4. Условия применения ПДСЧ в ОС QNX.....	4
3. Использование ПДСЧ в ОС Windows.....	5
3.1. Установка и удаление ПДСЧ в ОС Windows	5
3.2. Генерация паролей в ОС Windows	5
3.3. Настройка ПДСЧ в ОС Windows диалоговом режиме	6
3.4. Параметры командной строки ПДСЧ в ОС Windows	6
3.5. Сообщения пользователю об ошибках ПДСЧ в ОС Windows	6
4. Использование ПДСЧ в ОС MCBC	8
4.1. Установка и удаление ПДСЧ в ОС MCBC	8
4.2. Генерация паролей в ОС MCBC	8
4.3. Настройка ПДСЧ в диалоговом режиме в ОС MCBC.....	10
4.4. Параметры командной строки ПДСЧ в ОС MCBC	10
4.5. Сообщения пользователю об ошибках ПДСЧ в ОС MCBC	10
5. Использование ПДСЧ в ОС QNX.....	12
5.1. Установка и удаление ПДСЧ в ОС QNX.....	12
5.2. Генерация паролей в ОС QNX	12
5.3. Параметры командной строки ПДСЧ в ОС QNX	12
6. Использование ПДСЧ в ОС Эльбрус, Эльбрус-Д.....	13
6.1. Установка и удаление ПДСЧ в ОС Эльбрус, Эльбрус-Д.....	13
6.2. Работа с ПДСЧ в ОС Эльбрус, Эльбрус-Д	13
7. Использование ПДСЧ в ОС СН «Astra Linux Special Edition».....	14
7.1. Установка и удаление ПДСЧ в ОС СН «Astra Linux Special Edition»	14
7.2. Работа с ПДСЧ в ОС СН «Astra Linux Special Edition».....	14
8. Использование ПДСЧ в ЗОСРВ «Нейтрино».....	15
8.1. Установка и удаление ПДСЧ в ЗОСРВ «Нейтрино».....	15
8.2. Работа с ПДСЧ в ЗОСРВ «Нейтрино»	15
Перечень сокращений	16

1. ОБЩИЕ СВЕДЕНИЯ

В данном документе приведены сведения о назначении, возможностях и порядке работы с программным датчиком псевдослучайных чисел (ПДСЧ).

2. НАЗНАЧЕНИЕ И УСЛОВИЯ ПРИМЕНЕНИЯ

2.1. Назначение и общие условия применения ПДСЧ

ПДСЧ предназначен для генерирования последовательностей случайных паролей.

ПДСЧ функционирует на ЭВМ, работающих под управлением операционных систем (ОС) семейства Microsoft Windows (поддерживаются как 32-битные, так и 64-битные версии ОС), MCBC 3.0 (ФЛИР.80001-01 изменение № 13; ФЛИР.80001-12), MCBC 5.0 (ЦАВМ.11004-01), QNX 6.4.0, Эльбрус (ТВГИ.00316-10), Эльбрус-Д (ТВГИ.00950-01), Astra Linux Special Edition (РУСБ.10015-01, релиз «Смоленск», и РУСБ.10265-01, релиз «Ленинград») и ЗОСРВ «Нейтрино» (КПДА.10964-01, платформа x86).

Для работы справочной системы ПДСЧ необходимо наличие HTML-браузера.

Эксплуатация ПДСЧ допустима только при соблюдении следующих условий:

- в прикладном и общем программном обеспечении не должно быть средств программирования и отладки;
- на ЭВМ должна быть установлена система защиты информации от несанкционированного доступа, ограничивающая непосредственный доступ к модулям ПДСЧ (**prcg.exe**, **crypting.dll**, **prcg_lin** и **prcg_qnx**), с целью предотвращения возможности отладки и несанкционированного изменения кода.

2.2. Условия применения ПДСЧ в ОС Windows

Функционирование ПДСЧ под управлением ОС Windows обеспечивается исполняемым модулем **prcg.exe** и динамической библиотекой **crypting.dll**.

2.3. Условия применения ПДСЧ в ОС MCBC, Astra Linux, Эльбрус, Эльбрус-Д, ЗОСРВ «Нейтрино»

Функционирование ПДСЧ под управлением ОС MCBC, Astra Linux, Эльбрус, Эльбрус-Д, ЗОСРВ «Нейтрино» обеспечивается модулем **prcg_lin**. В ОС должны быть установлены библиотеки:

- для ОС MCBC, Эльбрус – Qt3;
- для ОС Astra Linux, Эльбрус-Д, ЗОСРВ «Нейтрино» – Qt4.

2.4. Условия применения ПДСЧ в ОС QNX

Функционирование ПДСЧ под управлением ОС QNX обеспечивается модулем **prcg_qnx**.

3. ИСПОЛЬЗОВАНИЕ ПДСЧ В ОС WINDOWS

3.1. Установка и удаление ПДСЧ в ОС Windows

Функционирование ПДСЧ под управлением ОС Windows обеспечивается исполняемым модулем **prcg.exe** с использованием динамической библиотеки **crypting.dll**. Для установки программы ПДСЧ под ОС Windows необходимо выполнить следующие действия:

- 1) создать рабочий каталог **PRCG** на жестком диске;
- 2) скопировать исполняемый модуль **prcg.exe** и библиотеку шифрования **crypting.dll** из каталога **ПДСЧ\Windows** дистрибутивного ЭН в созданный рабочий каталог.

Для удаления программы ПДСЧ необходимо выполнить следующие действия:

- 1) удалить рабочий каталог **PRCG** с жесткого диска;
- 2) удалить в реестре раздел **HKEY_LOCAL_MACHINE\Software\PRCG**.

3.2. Генерация паролей в ОС Windows

Для генерации паролей необходимо запустить программу ПДСЧ в диалоговом или автоматическом режиме.

Для запуска программы необходимо запустить исполняемый файл **prcg.exe**. При запуске происходит самопроверка ПДСЧ на предмет выявления несанкционированных изменений. Если проверка завершается успешно и фактов несанкционированного изменения ПДСЧ обнаружено не было, работа программы продолжается. В противном случае программа завершается.

Диалоговый режим работы активируется при запуске программы без параметров командной строки. При этом появляется главное окно, общий вид которого показан на рис. 1. Диалоговый режим позволяет осуществить настройку параметров генерации, генерацию паролей, а также сохранение полученных паролей в файл.

Главное окно ПДСЧ

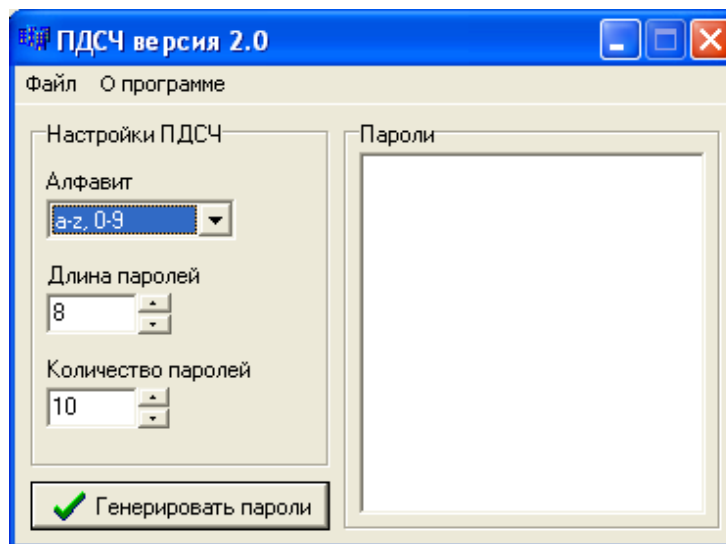


Рис. 1

Сразу после открытия диалогового окна ПДСЧ готов к работе. Для генерации массива паролей необходимо выполнить следующие действия:

- 1) настроить параметры ПДСЧ;
- 2) выполнить генерацию паролей, нажав кнопку «Генерировать пароли» в левой части графического окна. При этом ПДСЧ отображает результат генерации в правой части диалогового окна.

После успешной генерации паролей можно сохранить их в файл, выбрав пункт меню «Файл/Сохранить», после чего пользователю будет предложено выбрать имя файла для сохранения. До генерации паролей данный пункт меню недоступен для использования.

Для просмотра информации о программе необходимо выбрать пункт меню «О программе», для завершения программы – пункт меню «Файл/Выход».

Автоматический режим работы активируется при запуске программы с указанием в командной строке соответствующих параметров. При этом выполняется генерация паролей (с использованием параметров генерации, ранее заданных в диалоговом режиме), после чего программа автоматически завершается.

3.3. Настройка ПДСЧ в ОС Windows диалоговом режиме

ПДСЧ позволяет выполнять конфигурацию таких параметров, как алфавит, длина и количество паролей.

Алфавит определяет символы, которые будут использоваться для представления паролей. Пароли с алфавитом «a-z, 0-9» будут содержать символы латинского алфавита от a до z (только строчные буквы) и цифры от 0 до 9. Алфавит «A-Z, 0-9» означает, что в выходной генерации паролей будут содержаться только символы латинского алфавита от A до Z (только заглавные буквы) и цифры от 0 до 9. Пароли, образованные с помощью алфавита «A-Z, a-z, 0-9», будут содержать еще и строчные латинские буквы от a до z. Аналогично «A-Я, 0-9», «A-я, a-я, 0-9» задают алфавит из русских символов.

Длина пароля ограничивается интервалом от 8 до 16 символов.

Количество паролей ограничивается интервалом от 1 до 1200.

По умолчанию значения параметров следующие:

- алфавит – «a-z, 0-9»;
- длина пароля – 8 символов;
- количество паролей – 10.

3.4. Параметры командной строки ПДСЧ в ОС Windows

Формат параметров командной строки для запуска ПДСЧ:

`prcg.exe auto [filename]`

Параметр «auto» указывает на автоматическую работу ПДСЧ, при которой главное окно программы не отображается, а генерация паролей выполняется на текущих установках ПДСЧ. Необязательный параметр «filename» задает имя файла, в который будет сохранена последовательность паролей. Если этот параметр не указывать, то пароли будут сохранены в файл с именем **passauto.txt** в каталог, где содержится модуль **prcg.exe**.

3.5. Сообщения пользователю об ошибках ПДСЧ в ОС Windows

Модуль **prcg.exe** обрабатывает ряд возможных ошибок и выдает соответствующие сообщения, приведенные в таблице 1.

Таблица 1 – Возможные ошибки

Сообщение	Описание ошибки	Способ устранения
Некорректное значение длины пароля. Длина пароля может принимать значения от 8 до 16 символов. Возвращено последнее корректное значение	ПДСЧ выполняет генерацию паролей только длиной от 8 до 16 символов	Ввести целое десятичное положительное число от 8 до 16

Окончание таблицы 1

Сообщение	Описание ошибки	Способ устранения
Некорректное значение количества паролей. Количество паролей может принимать значения от 1 до 1200. Возвращено последнее корректное значение	ПДСЧ выполняет генерацию массива, содержащего только от 1 до 1200 паролей	Ввести целое десятичное положительное число от 1 до 1200
Ошибка записи настроек ПДСЧ в реестр	Невозможно сохранить настройки ПДСЧ в реестре. Возможно, обращение к реестру заблокировано каким-либо приложением	Закрыть выполняющиеся приложения, перезапустить ПДСЧ
Ошибка загрузки настроек ПДСЧ из реестра	Невозможно загрузить настройки ПДСЧ из реестра. Возможно, обращение к реестру заблокировано каким-либо приложением. Работа ПДСЧ будет продолжена с установками по умолчанию	Закрыть выполняющиеся приложения, перезапустить ПДСЧ
Не удалось подключить библиотеку шифрования	В каталоге, где находится prcg.exe , отсутствует файл библиотеки crypting.dll	Проверить название и путь библиотеки. При наличии файла убедиться, что доступ к файлу библиотеки не заблокирован каким-либо средством разграничения доступа. При отсутствии файла скопировать его с дистрибутивного диска
Библиотека crypting.dll не содержит поддерживаемую функцию шифрования	Библиотека не содержит корректную функцию шифрования	Обратиться к автору библиотеки шифрования
Библиотека crypting.dll не содержит функцию определения размера блока шифрования	Библиотека не содержит корректную функцию определения размера блока шифрования	Обратиться к автору библиотеки шифрования
Ошибка чтения модуля ПДСЧ	Невозможно открыть модуль ПДСЧ на чтение при проверке целостности и расчете контрольной суммы	Убедиться, что файл ПДСЧ доступен для чтения
Нарушена целостность модуля ПДСЧ	Модуль ПДСЧ prcg.exe был изменен	Восстановить исходную версию ПДСЧ
Не пройдена самопроверка	Модуль ПДСЧ prcg.exe был изменен	Восстановить исходную версию ПДСЧ

4. ИСПОЛЬЗОВАНИЕ ПДСЧ В ОС MCBC

4.1. Установка и удаление ПДСЧ в ОС MCBC

Под управлением ОС MCBC функционирование ПДСЧ обеспечивается модулем **prcg_lin**. Для установки ПДСЧ под ОС MCBC необходимо в командной строке от имени суперпользователя «root» выполнить следующие действия:

1) смонтировать устройство CD-ROM, выполнив следующую команду:

```
mount /mnt/cdrom
```

2) скопировать исполняемый модуль **prcg_lin** с компакт-диска, содержащего дистрибутив, в рабочий каталог с помощью следующей команды:

```
cp -f /mnt/cdrom/ПДСЧ/<каталог>/prcg_lin /usr/bin
```

где <каталог> принимает значение **MCBC** для ОС MCBC 3.0 и значение **MCBC5** для ОС MCBC 5.0;

3) размонтировать устройство CD-ROM посредством следующей команды:

```
umount /mnt/cdrom
```

4) назначить требуемые права доступа для пользователей ПДСЧ на исполняемый модуль **prcg_lin**.

Для удаления ПДСЧ необходимо удалить исполняемый модуль **prcg_lin** с помощью следующей команды:

```
rm -f /usr/bin/prcg_lin
```

4.2. Генерация паролей в ОС MCBC

Для генерации паролей необходимо запустить программу ПДСЧ в диалоговом или автоматическом режиме. Перед запуском программы ПДСЧ в диалоговом режиме необходимо убедиться, что загружен графический режим X-Window ОС MCBC.

После запуска исполняемого файла **prcg_lin** в диалоговом режиме на экране отображается диалоговое окно, показанное на рис. 2.

Диалоговое окно ПДСЧ вертикально разделено на две части. В левой части окна отображаются элементы управления, предназначенные для настройки ПДСЧ. Правая часть графического окна предназначена для вывода массива паролей на экран. Над левой и правой частями данного графического окна ПДСЧ располагается главное меню, состоящее из двух пунктов «Файл» и «Справка».

Диалоговое окно ПДСЧ в ОС MCBC

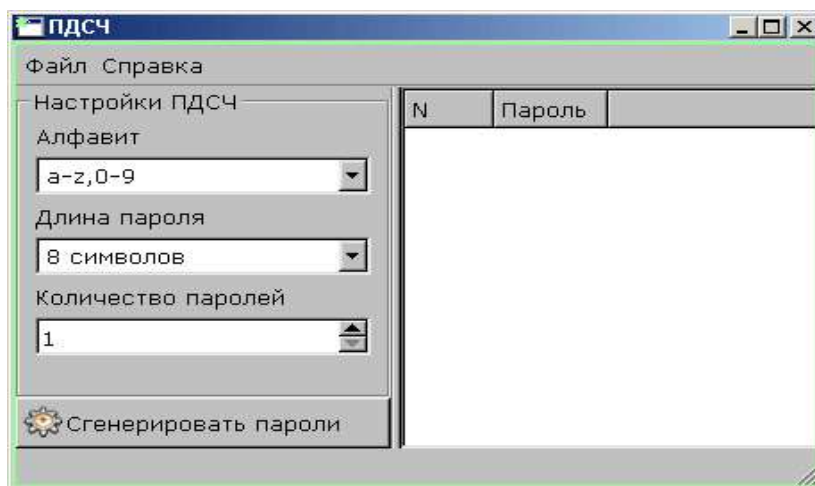


Рис. 2

Сразу после открытия диалогового окна ПДСЧ готов к работе. Для генерации массива паролей необходимо выполнить следующие действия:

- 1) настроить параметры ПДСЧ;
- 2) выполнить генерацию паролей, выбрав «Файл/Сгенерировать пароли» или нажав кнопку «Сгенерировать пароли» в левой части графического окна. При этом ПДСЧ отображает результат генерации в правой части диалогового окна, как показано на рис. 3.

После генерации массив паролей может быть сохранен в файл («Файл/Сохранить в файл»). В этом случае пользователю будет предложено выбрать имя файла и директорию его размещения. По умолчанию в программе предлагается сохранить массив паролей в файл **passwords.txt**, расположенный в каталоге размещения исполняемого модуля **prcg_lin**.

Генерация паролей в ОС МСВС

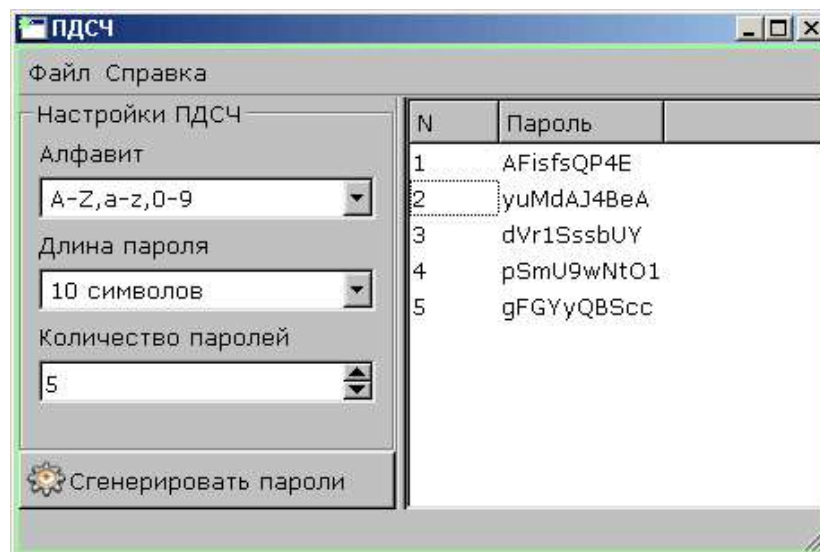


Рис. 3

Структура главного меню ПДСЧ имеет следующий вид:

- 1) Файл:
 - а) сгенерировать пароли;
 - б) сохранить в файл;
 - в) выход.
- 2) Справка о программе.

Функции пунктов и подпунктов главного меню программы представлены в таблице 2.

Таблица 2 – Функции пунктов и подпунктов главного меню

Пункт (подпункт) главного меню	Функция
Файл	Работа с ПДСЧ
Сгенерировать пароли	Непосредственная генерация массива паролей и, если установлено, вывод массива на экран/сохранение в файл
Сохранить в файл	Сохранение массива паролей в файл с предоставлением возможности выбора директории и имени файла
Выход	Выход из программы
Справка	Справочная информация
О программе	Краткая информация о программе

4.3. Настройка ПДСЧ в диалоговом режиме в ОС MCBC

ПДСЧ позволяет выполнять конфигурацию таких параметров, как алфавит, длина и количество паролей, отображать массив паролей на экране, а также сохранять в файл. Изменить можно каждый параметр в отдельности с помощью соответствующего элемента управления в левой части графического окна.

Алфавит определяет символы, которые будут использоваться для представления паролей. Пароли с алфавитом «a-z, 0-9» будут содержать символы латинского алфавита от a до z (только строчные буквы) и цифры от 0 до 9. Алфавит «A-Z, 0-9» означает, что в выходной генерации паролей будут содержаться только символы латинского алфавита от A до Z (только заглавные буквы) и цифры от 0 до 9. Пароли, образованные с помощью алфавита «A-Z, a-z, 0-9», будут содержать еще и строчные латинские буквы от a до z. Аналогично «A-Я, 0-9» и «A-я, a-я, 0-9» задают алфавит из русских символов.

Длина пароля ограничивается интервалом от 8 до 16 символов. Количество паролей ограничивается интервалом от 1 до 1200. Количество паролей можно ввести, уменьшая или увеличивая текущее значение при помощи стрелок либо с клавиатуры. При вводе количества паролей с клавиатуры необходимо нажать клавишу «Enter» перед генерацией паролей. При попытке ввода числа паролей, превышающего верхнюю границу интервала, число паролей автоматически сокращается до 1200.

Сохранить пароли в файл можно выбрав «Файл/Сохранить в файл».

По умолчанию значения параметров следующие:

- алфавит – «a-z, 0-9»;
- длина пароля – 8 символов;
- количество паролей – 1.

4.4. Параметры командной строки ПДСЧ в ОС MCBC

Для запуска модуля **prcg_lin** в автоматическом режиме в командной строке необходимо указать следующие параметры:

1) -l <len>, где <len> – длина пароля, ограничивается интервалом от 8 до 16 символов;
2) -c <num>, где <num> – количество генерируемых паролей, ограничивается интервалом от 1 до 1200;

3) -a <alf>, где <alf> – алфавит паролей, может принимать следующие значения:

- ES – строчные латинские буквы и цифры (a-z, 0-9);
- EF – все (заглавные и строчные) латинские буквы и цифры (A-Z, a-z, 0-9);
- EB – заглавные латинские буквы и цифры (A-Z, 0-9);
- RF – все (заглавные и строчные) русские буквы и цифры (A-Я, a-я, 0-9);
- RB – заглавные русские буквы и цифры (A-Я, 0-9);

4) <имя файла> – имя файла, куда необходимо вывести массив паролей.

Формат командной строки запуска модуля **prcg_lin** выглядит следующим образом:

`prcg_lin -l <len> -c <num> -a <alf> > <имя файла>`

Если имя файла для вывода паролей в командной строке не указано, массив паролей будет выведен на экран.

4.5. Сообщения пользователю об ошибках ПДСЧ в ОС MCBC

ПДСЧ обрабатывает ряд возможных ошибок и выдает соответствующие сообщения, приведенные в таблице 3.

Таблица 3 – Возможные ошибки

Сообщение	Описание ошибки	Способ устранения
Проверьте правильность ввода параметров	Ошибка ввода параметров командной строки	Проверить длину и количество паролей, выбор алфавита, путь к файлу вывода паролей
Список паролей пуст, сначала сгенерируйте пароли	Попытка сохранить массив паролей в файл до генерации паролей	Сгенерировать пароли, затем повторить сохранение в файл

5. ИСПОЛЬЗОВАНИЕ ПДСЧ В ОС QNX

5.1. Установка и удаление ПДСЧ в ОС QNX

Функционирование ПДСЧ под управлением ОС QNX обеспечивается модулем **prcg_qnx**. Для установки ПДСЧ под ОС QNX необходимо в командной строке от имени суперпользователя выполнить следующие действия:

1) смонтировать устройство CD-ROM, выполнив следующую команду:

```
mount /mnt/cdrom
```

2) скопировать исполняемый модуль **prcg_qnx** с компакт-диска, содержащего дистрибутив, в рабочий каталог с помощью следующей команды:

```
cp -f /mnt/cdrom/prcg_qnx/prcg_qnx /usr/bin
```

3) размонтировать устройство CD-ROM посредством следующей команды:

```
umount /mnt/cdrom
```

4) назначить требуемые права доступа для пользователей ПДСЧ на исполняемый модуль **prcg_qnx**.

Для удаления ПДСЧ необходимо удалить исполняемый модуль **prcg_qnx** с помощью следующей команды:

```
rm -f /usr/bin/prcg_qnx
```

5.2. Генерация паролей в ОС QNX

Модуль **prcg_qnx** не имеет графического интерфейса и запускается в командном интерпретаторе по запросу оператора.

Для генерации массива паролей необходимо выполнить модуль **prcg_qnx** в командном интерпретаторе с указанием параметров командной строки.

5.3. Параметры командной строки ПДСЧ в ОС QNX

Для запуска модуля **prcg_qnx** используются следующие параметры:

- -l <len>, где <len> – длина пароля от 6 до 16 символов;
- -c <num>, где <num> – количество генерируемых паролей в интервале от 1 до 1200;
- -a {ES, EB, EF, RB, RF} – выбор алфавита паролей, где ES – это строчные латинские буквы и цифры, EB – заглавные латинские буквы и цифры, EF – все (заглавные и строчные) латинские буквы и цифры, RB – заглавные русские буквы и цифры, RF – все (заглавные и строчные) русские буквы и цифры;
- -f <filename>, где <filename> является именем файла для сохранения паролей.

При запуске модуля **prcg_qnx** без параметров на экран будет выведена краткая справка по использованию ПДСЧ. Для генерации паролей необходимо указать, как минимум, один из параметров. Значения параметров ПДСЧ, не указанные в командной строке, будут установлены по умолчанию.

По умолчанию параметры ПДСЧ принимают следующие значения:

- длина пароля – 8 символов;
- количество паролей – 10;
- алфавит – строчные латинские буквы и цифры (ES).

Если файл, в который необходимо сохранить пароли, уже существует, он будет перезаписан. Если опция сохранения в файл не указана, список паролей будет выведен на экран.

6. ИСПОЛЬЗОВАНИЕ ПДСЧ В ОС ЭЛЬБРУС, ЭЛЬБРУС-Д

6.1. Установка и удаление ПДСЧ в ОС Эльбрус, Эльбрус-Д

Под управлением ОС Эльбрус, Эльбрус-Д функционирование ПДСЧ обеспечивается модулем **prcg_lin**. Для установки ПДСЧ необходимо в командной строке от имени суперпользователя «root» выполнить следующие действия:

- 1) смонтировать устройство CD-ROM, выполнив следующую команду:

```
mount <путь к устройству> /mnt/cdrom
```

где <путь к устройству> принимает значения **/dev/cdrom** для ОС Эльбрус и **/dev/sr0** для ОС Эльбрус-Д.

- 2) скопировать исполняемый модуль **prcg_lin** с компакт-диска, содержащего дистрибутив, в рабочий каталог с помощью следующей команды:

```
cp -f /mnt/cdrom/ПДСЧ/<ОС>/prcg_lin /usr/bin
```

где <ОС> принимает значения **Эльбрус** для ОС Эльбрус и **Эльбрус-Д** для ОС Эльбрус-Д.

- 3) размонтировать устройство CD-ROM посредством следующей команды:

```
umount /mnt/cdrom
```

- 4) назначить требуемые права доступа для пользователей ПДСЧ на исполняемый модуль **prcg_lin**.

В случае если на ЭВМ отсутствует встроенный CD/DVD-привод, необходимо использовать внешний CD/DVD-привод. Если внешний CD/DVD-привод также недоступен, необходимо копирование модуля в рабочий каталог выполнить с помощью отдельной ЭВМ, имеющей CD/DVD-привод, и USB-накопителя или локальной сети.

Для удаления ПДСЧ необходимо удалить исполняемый модуль **prcg_lin** с помощью следующей команды:

```
rm -f /usr/bin/prcg_lin
```

6.2. Работа с ПДСЧ в ОС Эльбрус, Эльбрус-Д

Работа с ПДСЧ в ОС Эльбрус, Эльбрус-Д осуществляется полностью аналогично работе с ПДСЧ в ОС МСВС, описанной в 4.2 – 4.5.

7. ИСПОЛЬЗОВАНИЕ ПДСЧ В ОС СН «ASTRA LINUX SPECIAL EDITION»

7.1. Установка и удаление ПДСЧ в ОС СН «Astra Linux Special Edition»

Под управлением ОС СН «Astra Linux Special Edition» функционирование ПДСЧ обеспечивается модулем **prcg_lin**. Для установки ПДСЧ под ОС СН «Astra Linux Special Edition» необходимо в командной строке от имени суперпользователя «root» выполнить следующие действия (если не предполагается использовать ОС в режиме замкнутой программной среды, то перечисления 1), 4) – 7) и 10) можно пропустить):

1) для ОС СН «Astra Linux Special Edition» версий 1.6 и выше, релиз «Смоленск», с дистрибутивного диска ОС установить пакет **astra-digsig-oldkeys**;

2) установить в привод CD/DVD дистрибутивный ЭН ПДСЧ и смонтировать его, выполнив следующую команду:

```
mount /dev/cdrom /media/cdrom -o utf8
```

3) скопировать исполняемый модуль **prcg_lin** с дистрибутивного ЭН в рабочий каталог с помощью следующей команды:

```
cp -f /media/cdrom/ПДСЧ/<ОС>/prcg_lin /usr/bin
```

где <ОС> принимает значения **AstraLinux** для релиза «Смоленск» и **AstraLinux-Ленинград** для релиза «Ленинград»;

4) для ОС СН «Astra Linux Special Edition» версий 1.4 и 1.5 релиз «Смоленск» в каталог **/etc/digsig/keys** поместить файл открытого ключа **cps.tver_pub_key.gpg**, находящийся в каталоге **/media/cdrom/ПДСЧ/AstraLinux** дистрибутивного ЭН. Если ключ уже существует, то осуществить его замену;

5) для ОС СН «Astra Linux Special Edition» версий 1.6 и выше, релиз «Смоленск», в каталог **/etc/digsig/keys/legacy/keys** поместить файл открытого ключа **cps.tver_pub_key.gpg**, находящийся в каталоге **/media/cdrom/ПДСЧ/AstraLinux** дистрибутивного ЭН. Если ключ уже существует, то осуществить его замену;

6) для ОС СН «Astra Linux Special Edition» релиз «Ленинград» в каталог **/etc/digsig/keys** поместить файл открытого ключа **cps.tver_pub_key.gpg**, находящийся в каталоге **/media/cdrom/ПДСЧ/AstraLinux-Ленинград** дистрибутивного ЭН. Если ключ уже существует, то осуществить его замену;

7) выполнить следующую команду:

```
update-initramfs -u -k all
```

8) размонтировать устройство CD-ROM посредством следующей команды:

```
umount /media/cdrom
```

9) назначить требуемые права доступа для пользователей ПДСЧ на исполняемый модуль **prcg_lin**;

10) осуществить перезагрузку ОС.

В случае если на ЭВМ отсутствует встроенный CD/DVD-привод, необходимо использовать внешний CD/DVD-привод. Если внешний CD/DVD-привод также недоступен, необходимо копирование требуемых файлов выполнить с помощью отдельной ЭВМ, имеющей CD/DVD-привод, и USB-накопителя или локальной сети.

Для удаления ПДСЧ необходимо от имени суперпользователя «root» удалить исполняемый модуль **prcg_lin** с помощью следующей команды:

```
rm -f /usr/bin/prcg_lin
```

7.2. Работа с ПДСЧ в ОС СН «Astra Linux Special Edition»

Работа с ПДСЧ в ОС СН «Astra Linux Special Edition» осуществляется полностью аналогично работе с ПДСЧ в ОС МСВС, описанной в 4.2 – 4.5.

8. ИСПОЛЬЗОВАНИЕ ПДСЧ В ЗОСРВ «НЕЙТРИНО»

8.1. Установка и удаление ПДСЧ в ЗОСРВ «Нейтрино»

Под управлением ЗОСРВ «Нейтрино» функционирование ПДСЧ обеспечивается модулем **prcg_lin**. Для установки ПДСЧ необходимо в командной строке от имени суперпользователя «root» выполнить следующие действия:

- 1) установить в привод CD/DVD дистрибутивный ЭН ПДСЧ;
- 2) скопировать исполняемый модуль **prcg_lin** с дистрибутивного ЭН в рабочий каталог с помощью следующей команды:

```
cp /fs/cd0/prcg_neutrino/prcg_lin /usr/bin
```

- 3) назначить требуемые права доступа для пользователей ПДСЧ на файл **/usr/bin/prcg_lin**.

В случае если на ЭВМ отсутствует встроенный CD/DVD-привод, необходимо использовать внешний CD/DVD-привод, либо выполнить копирование требуемых файлов с помощью отдельной ЭВМ, имеющей CD/DVD-привод, и USB-накопителя или локальной сети.

Для удаления ПДСЧ необходимо от имени суперпользователя «root» удалить файл **/usr/bin/prcg_lin** с помощью менеджера файлов или следующей команды:

```
rm /usr/bin/prcg_lin
```

8.2. Работа с ПДСЧ в ЗОСРВ «Нейтрино»

Работа с ПДСЧ в ЗОСРВ «Нейтрино» осуществляется полностью аналогично работе с ПДСЧ в ОС МСВС, описанной в 4.2 – 4.5.

При выдаче сгенерированных паролей в консоль или сохранении их в файл используется кодировка IBM 866 (CP866).

ПЕРЕЧЕНЬ СОКРАЩЕНИЙ

ЗОСРВ	– защищенная операционная система реального времени
МСВС	– мобильная система вооруженных сил
ОС	– операционная система
ОС СН	– операционная система специального назначения
ПДСЧ	– программный датчик псевдослучайных чисел
ЭВМ	– электронно-вычислительная машина
ЭН	– электронный носитель

[illegible]