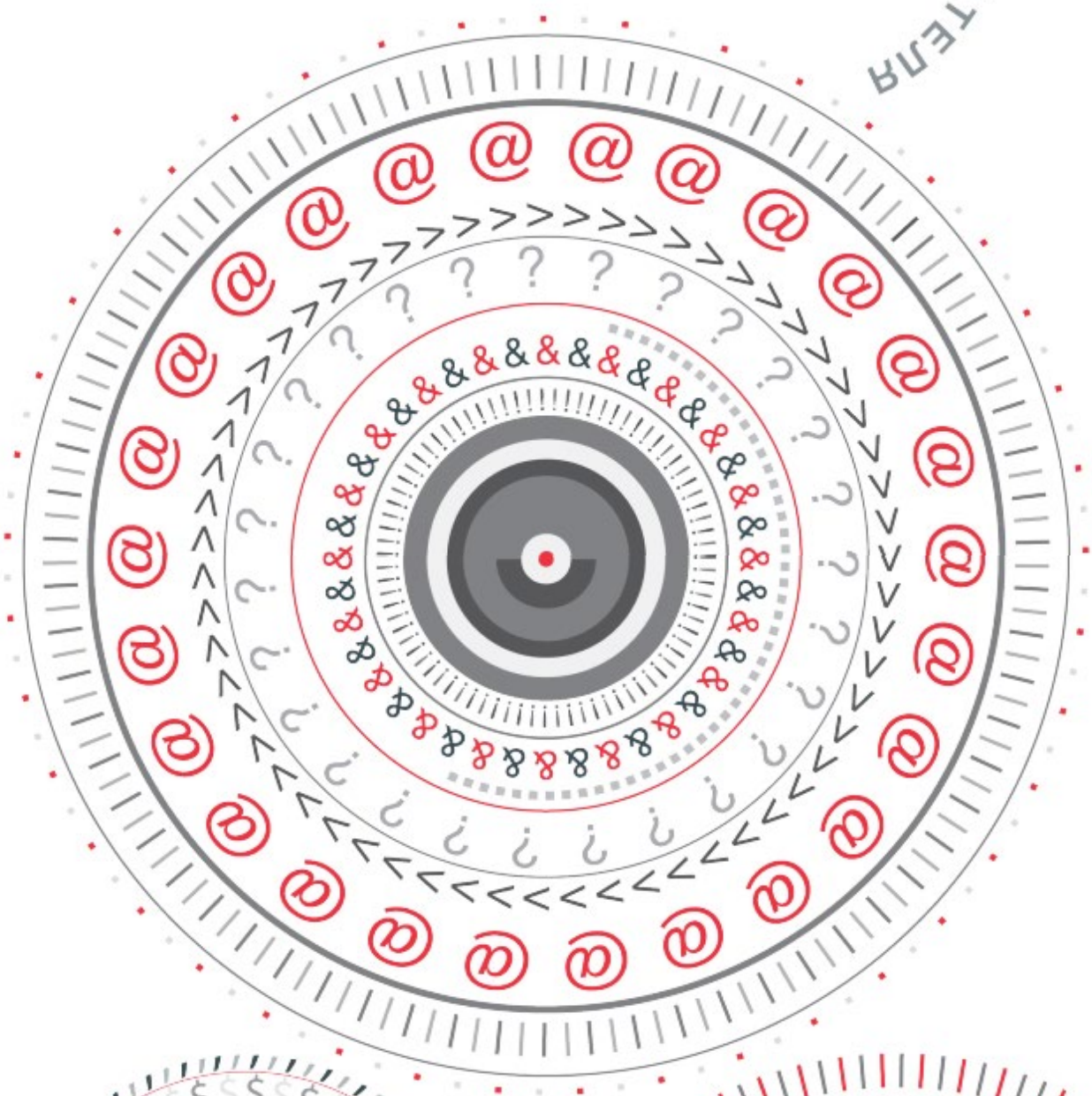
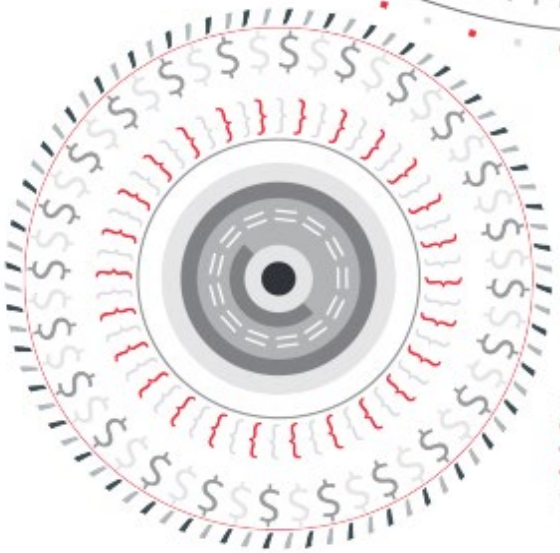
ПРОГРАММНЫЙ
ГЕНЕРАТОР
ПАРОЛЕЙ

«ГЕНЕРАТОР»

РУКОВОДСТВО ПОЛЬЗОВАТЕЛЯ

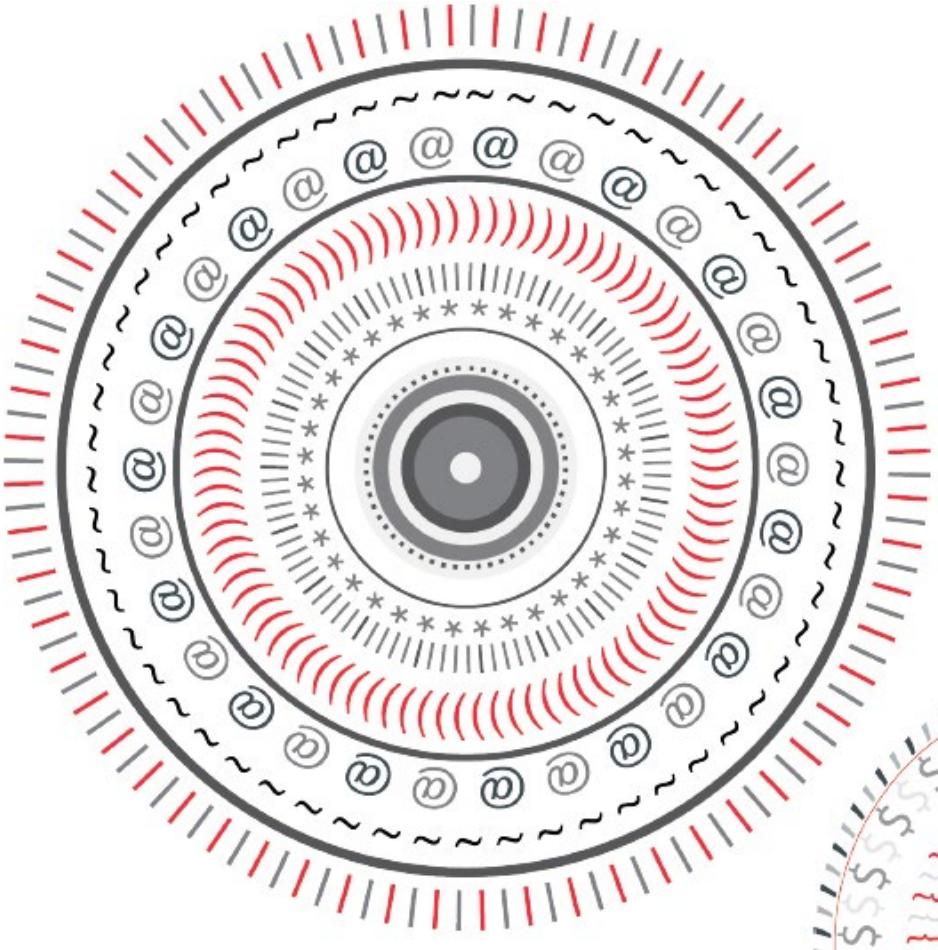


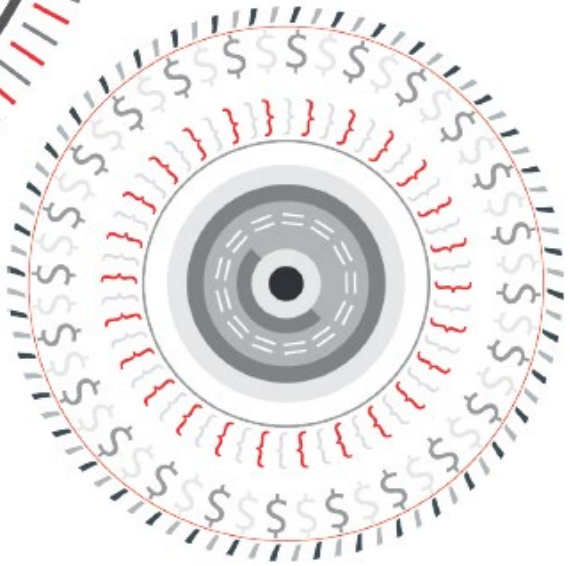


Аннотация

В документе содержатся сведения о назначении, условиях применения программы «Генератор», последовательности действий пользователя, обеспечивающих загрузку, запуск, выполнение и завершение программы.

Помимо этого приведены подробные описания функций, формата и возможных вариантов команд, с помощью которых пользователь осуществляет загрузку и управляет выполнением программы, ответы программы на эти команды, тексты сообщений, выдаваемых в ходе выполнения программы.





Содержание

1 НАЗНАЧЕНИЕ ПРОГРАММЫ....6
2 УСЛОВИЯ ВЫПОЛНЕНИЯ ПРОГРАММЫ....7
2.1 Рекомендуемые системные требования....7
2.2 Организационно-распорядительные меры....7
3 УСТАНОВКА ПРОГРАММЫ....8
3.1 Установка программы на ОС семейства Windows....8
3.2 Установка программы на ОС семейства Linux....11
4 ВЫПОЛНЕНИЕ ПРОГРАММЫ....12
4.1 Работа в графическом режиме....12
4.1.1 Запуск программы на ОС семейства Windows....12
4.1.2 Запуск программы на ОС семейства Linux....12
4.1.3 Активация продукта (на примере ОС Windows)....12
4.1.4 Списки пользователей....16
4.1.4.1 Импорт списка пользователей....19
4.1.4.1.1 Импорт из файла HTML....19
4.1.4.1.2 Импорт из файла XML....20
4.1.4.1.3 Импорт из файла CSV....20
4.1.4.1.4 Импорт из домена....21
4.1.4.1.5 Импорт локальных пользователей....23
4.1.4.1.6 Импорт из Active Directory (Astra Linux Directory)....24
4.1.4.2 Добавление новых учетных записей пользователей в список..24
4.1.4.3 Удаление учетных записей пользователей из списка....27
4.1.5 Генерация паролей....27
4.1.5.1 Сбор энтропии....28
4.1.5.2 Генерация паролей без привязки к конкретным пользователям...29
4.1.5.3 Генерация паролей для выбранных пользователей....30
4.1.6 Назначение паролей....31

4.1.7 Сохранение результатов....32
4.1.8 Параметры....33
4.1.8.1 Экспорт....34
4.1.8.2 Генерация....34
4.1.8.2.1 Требования к паролям....35
4.1.8.2.2 Профили....36
4.1.8.3 Основные....37
4.1.9 Журнал....38
4.1.10 Справочная информация....39
4.1.10.1 Справка....39
4.1.10.2 О программе....40
4.1.11 Завершение программы....41
4.2 Работа в консольном режиме....41
4.2.1 Консольная версия «Генератора»....42
4.2.1.1Опции для работы с консольной версией «Генератора»....43
4.2.1.2 Примеры использования....45
4.2.2 Менеджер лицензий....46
4.2.2.1 Опции для работы с Менеджером лицензий....46
4.2.2.2 Примеры использования....47
4.2.3 Генератор ПДСЧ....47
4.2.3.1 Опции для работы с Генератором ПДСЧ....47
4.2.3.2 Примеры использования....47
4.2.4 Генератор паролей....48
4.2.4.1 Опции для работы с Генератором паролей....48
4.2.4.2 Примеры использования....49
4.3 Работа в замкнутой программной среде Astra Linux....50
4.3.1 Включение режима замкнутой программной среды....50
4.3.2 Загрузка дополнительного ключа....52
4.3.2.1 Ручная загрузка дополнительного ключа....53

4.3.2.2 Автоматическая загрузка дополнительного ключа.....53
4.4 Взаимодействие с API утилит.....55
4.4.1 Запросы JSON.....55
4.4.2 Ответы JSON.....55
4.4.2.1 Успешный ответ.....56
4.4.2.2 Ошибки.....56
4.4.2.2.1 Пример ответа с ошибкой.....56
4.4.2.2.2 Примеры классов ошибок.....56
4.4.3 Методы API Генератора ПДСЧ.....57
4.4.3.1 Метод set_entropy.....57
4.4.3.2 Метод get_bytes.....58
4.4.3.3 Метод get_block.....58
4.4.3.4 Метод quit.....59
4.4.3.5 Методы API Генератора паролей.....59
4.4.3.6 Метод set_entropy.....60
4.4.3.7 Метод get_pass.....61
4.4.3.8 Метод quit.....62

1 Назначение программы

«Генератор» предназначен для генерации паролей, а также для назначения сгенерированных паролей пользователям.

Основные возможности «Генератора»:

- импорт списка пользователей:
  - из файлов в формате HTML, XML, CSV;
  - из домена;
  - с локального компьютера;
  - из службы каталогов (Microsoft Active Directory, Astra Linux Directory);
- добавление отдельного пользователя, которому необходимо назначить пароль;
- генерация паролей для отдельных учётных записей с возможностью задать:
  - множество допустимых символов для пароля;
  - длину пароля;
- назначение сгенерированных паролей отдельным пользователям;
- экспорт сгенерированных паролей в файлы форматов HTML, XML, CSV.

2 Условия выполнения программы

2.1 Рекомендуемые системные требования

ТАБЛИЦА 1

Рекомендуемые системные требования к рабочим станциям

Операционная система	Windows 7/8 Astra linux Special Edition 1.3 и выше Rosa Desktop 2012 LTS MARATHON Extended Edition (рабочие станции) ALT Linux СПТ 6.0 (рабочие станции)
Процессор	Intel Pentium 1.0 ГГц и выше
ПЗУ, Мб	256
ОЗУ, Мб	128

2.2 Организационно-распорядительные меры

«Генератор» обеспечивает функциональное назначение при реализации потребителем следующих предварительных организационно-распорядительных мер:

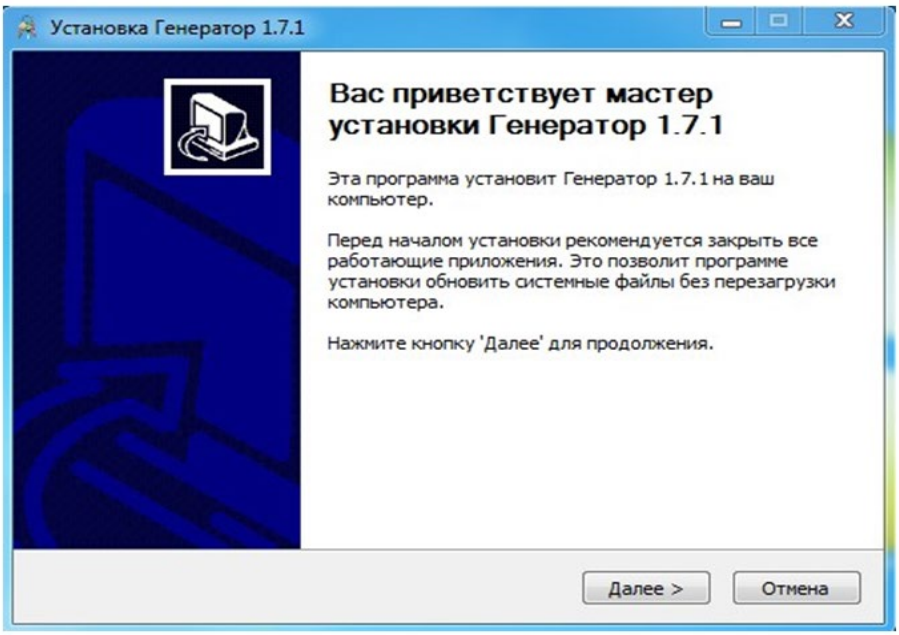
— обеспечение сохранности оборудования и физической целостности системных блоков компьютеров;
— ведение журнала учета работы рабочих станций, проведения регламентных мероприятий и внесения изменений в конфигурацию технических и программных средств;
— реализация мероприятий по антивирусной защите и обеспечение свободной от вирусов программной среды компьютеров.

3 Установка программы

3.1 Установка программы на ОС семейства Windows

Для установки «Генератора» запустить исполняемый файл на диске с дистрибутивом. Установка «Генератора» выполняется с помощью мастера установки (см. рис. 1). В открывшемся окне нажать «Далее».

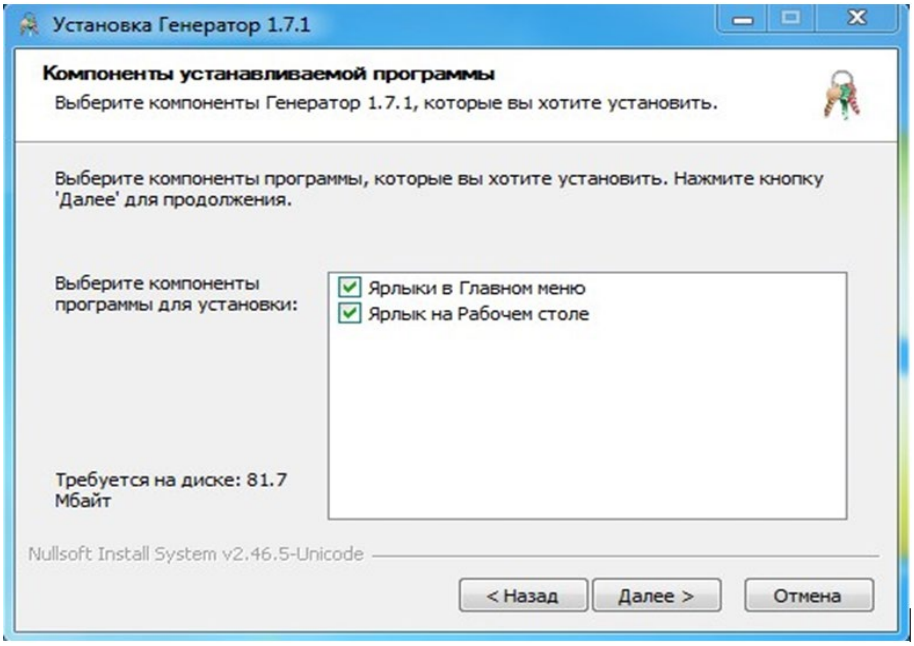
РИСУНОК 1
Окно мастера установки



В следующем окне (см. рис. 2) необходимо выбрать компоненты программы для установки (Ярлык в Главном меню, Ярлык на Рабочем столе), после выбора нажать «Далее».

РИСУНОК 2

Окно выбора компонентов установки



В следующем окне (см. рис. 3) следует выбрать папку, куда будет установлен «Генератор». После нажатия кнопки «Установить» начнется копирование файлов программы в выбранную папку (см. рис. 4).

РИСУНОК 3

Окно выбора папки для установки

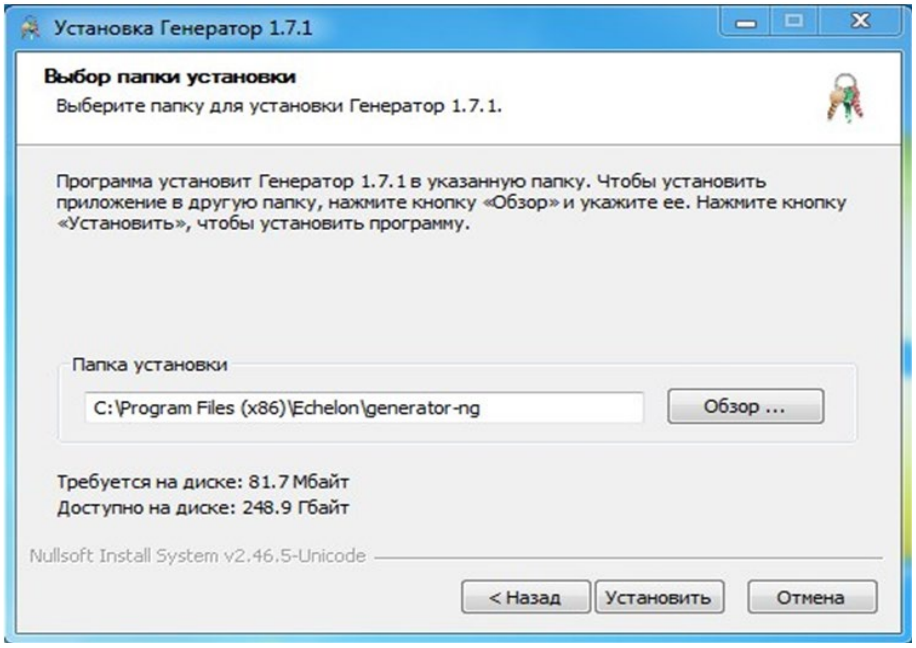
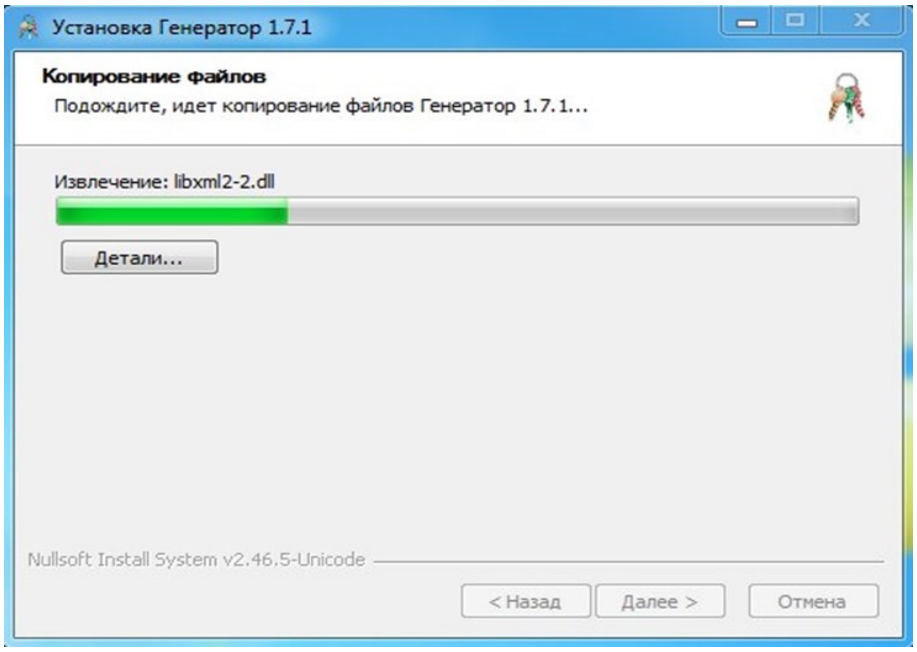


РИСУНОК 4

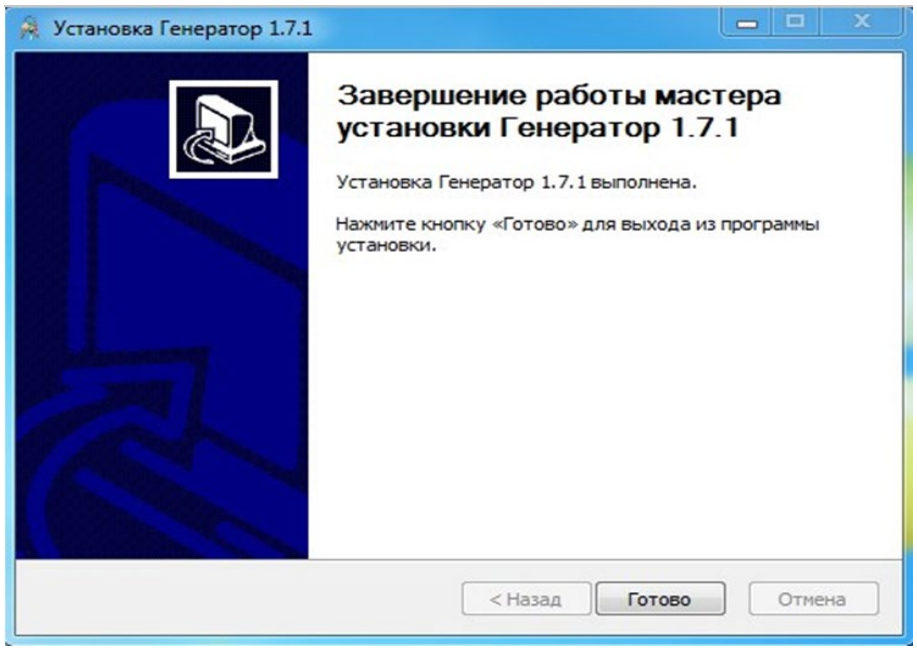
Копирование файлов программы



В случае успешной установки откроется окно завершения работы мастера установки (см. рис. 5). Для выхода нажать «Готово».

РИСУНОК 5

Окно завершения работы мастера установки



После завершения процесса установки ярлык «Генератора» будет доступен в меню Пуск, а также в Главном меню и на Рабочем столе (при выборе данных опций во время установки).

3.2 Установка программы на ОС семейства Linux

Для установки в папке с файлами пакетов выполнить команду с правами администратора:

```
dpkg -i generator_<version>.deb
```

где <version> — версия устанавливаемого пакета.

> **Примечание**: При установке программы на ОС Astra Linux необходимо войти в систему в режиме с мандатным уровнем 0. Текущий уровень в Astra Linux можно узнать на нижней панели в правом углу

> **Примечание**: при установке программы на ОС: Astra Linux, Alt Linux, Rosa Linux необходимо дополнительно установить пакет с утилитой **krb5-admin**.
>
> Для установки пакета следует выполнить соответствующую команду:

Операционная система	Команда
Astra Linux	*apt-get install krb5-user*
ALT Linux	*apt-get install krb5-kadmin*
Rosa Linux	*urpmi krb5-workstation*

4 Выполнение программы

4.1 Работа в графическом режиме

4.1.1 Запуск программы на ОС семейства Windows

После установки на рабочем столе появится ярлык программы, запустить можно двойным кликом мыши или выбрать в соответствующем разделе меню программ.

4.1.2 Запуск программы на ОС семейства Linux

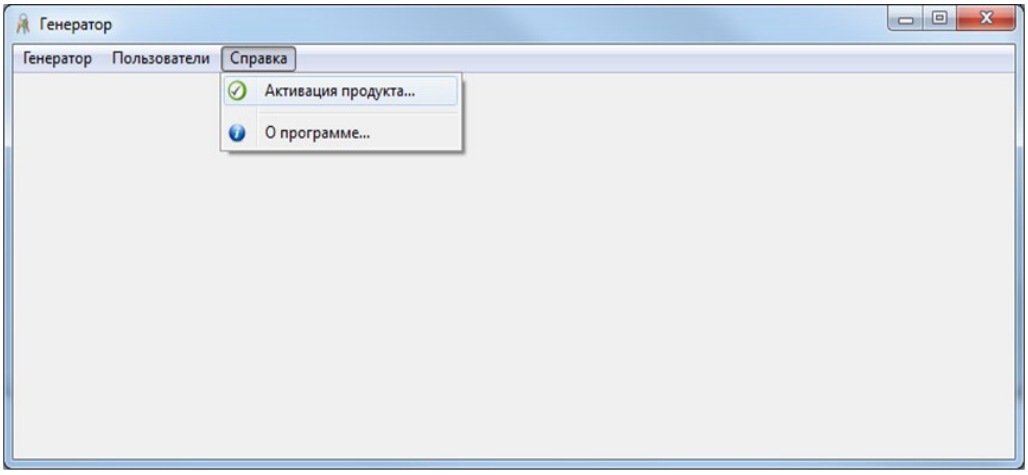
Запустить из консоли с правами администратора:

```
/usr/sbin/ech-generator-ui
```

4.1.3 Активация продукта (на примере ОС семейства Windows)

При первом запуске «Генератора» требуется активация продукта. Для этого необходимо зайти в пункт меню «Справка» и выбрать «Активация продукта…» (см. рис. 6).

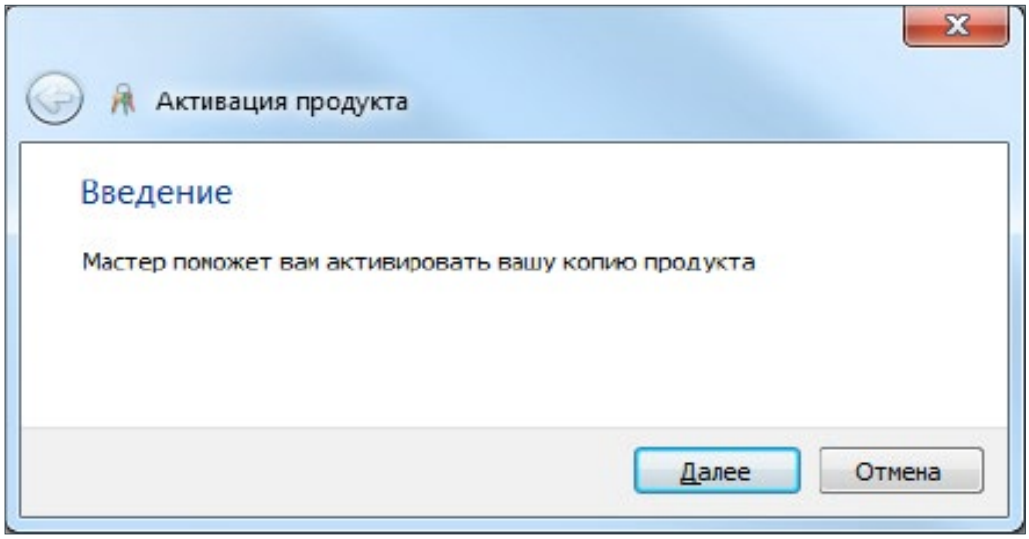
РИСУНОК 6
Активация продукта



Появится окно с уведомлением о том, что активация будет произведена при помощи мастера (см. рис. 7).

РИСУНОК 7

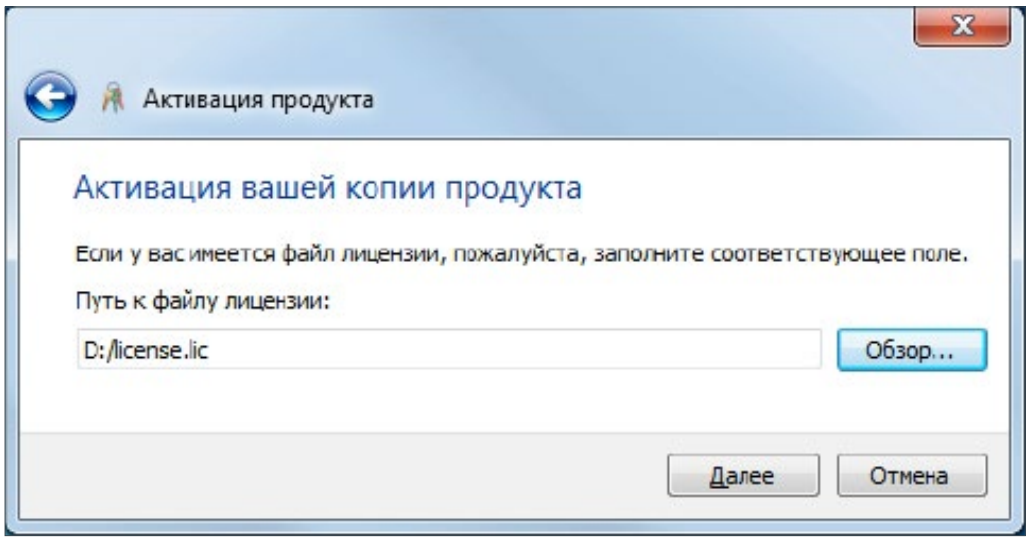
Активация продукта: введение



В следующем диалоговом окне (см. рис. 8) предлагается указать полный путь к файлу с лицензией копии продукта.

РИСУНОК 8

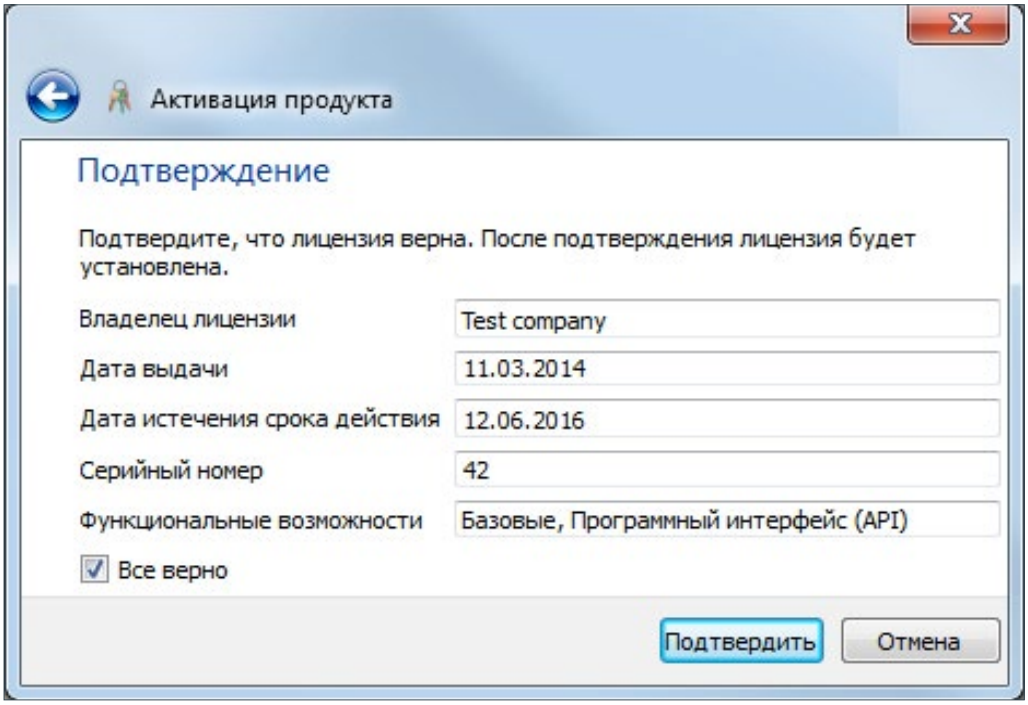
Активация продукта: путь к файлу лицензии



Далее требуется подтвердить информацию о владельце лицензии и сроках ее действия, серийном номере и функциональных возможностях, поставив отметку напротив пункта «Все верно» (см. рис. 9).

РИСУНОК 9

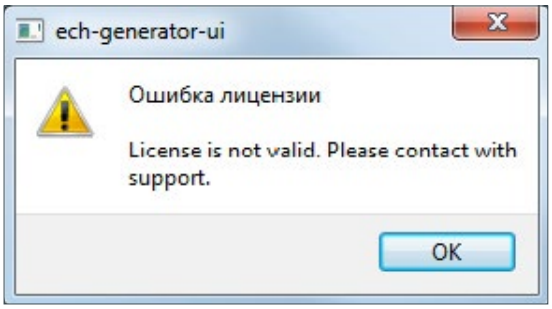
Активация продукта: подтверждение



Если файл лицензии некорректен (содержит некорректную ЭП или истек срок действия лицензии), выводится сообщение об ошибке (см. рис. 10).

РИСУНОК 10

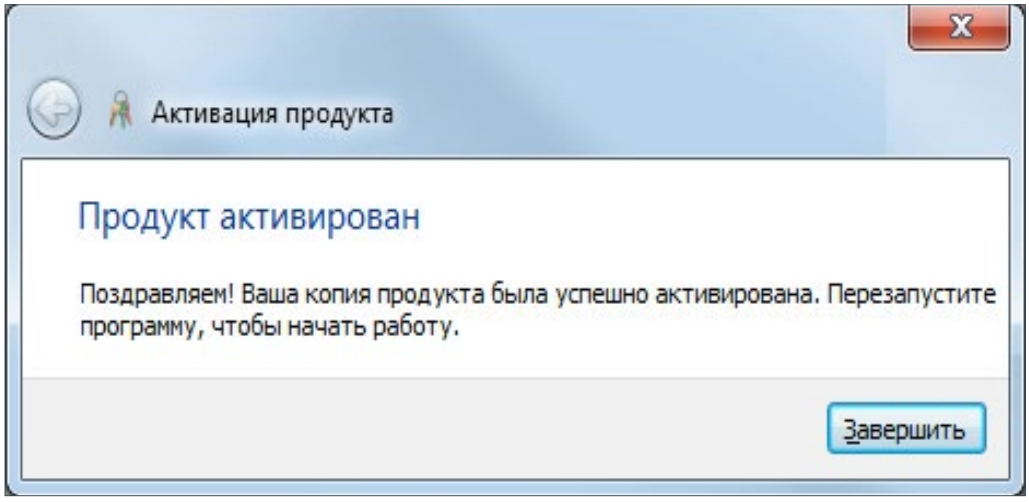
Уведомление об ошибке лицензии



При успешном прохождении предыдущих шагов появится финальное окно с предложением завершить процедуру прохождения активации (см. рис. 11).

РИСУНОК 11

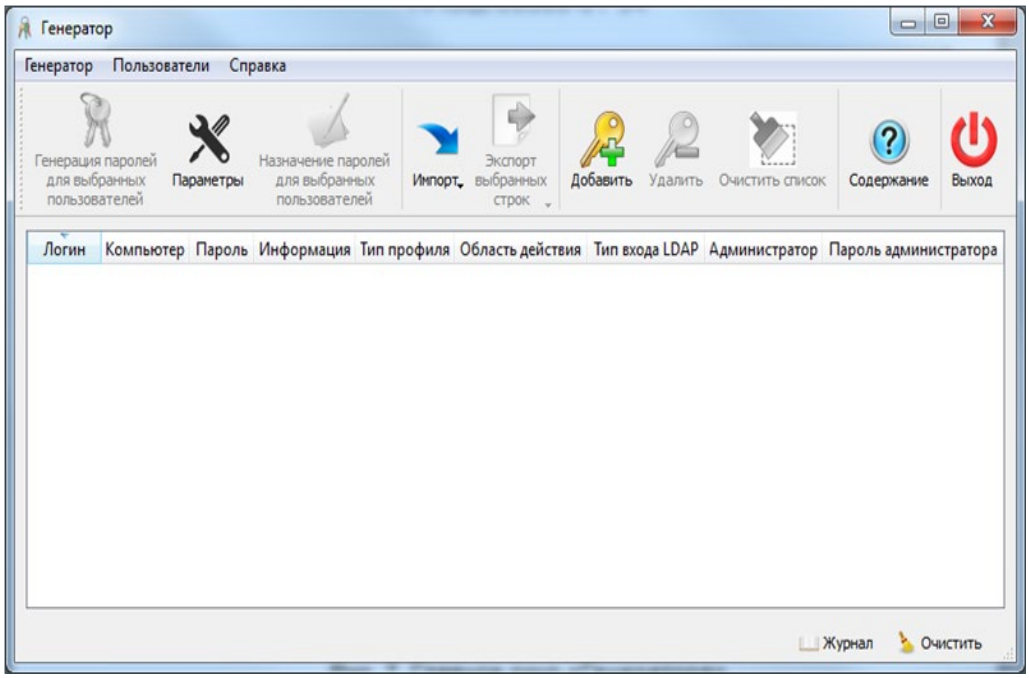
Активация продукта: продукт активирован



При завершении процедуры активации продукта оператор увидит главное окно программы (см. рис. 12).

РИСУНОК 12

Главное окно «Генератора»



4.1.4 Списки пользователей

Сформировать список пользователей, для которых необходимо сгенерировать пароли, можно с помощью импорта списка пользователей и с помощью процедуры добавления пользователя в список.

Каждая запись в списке пользователей состоит из следующих полей:

- Логин;
- Компьютер;
- Пароль;
- Информация;
- Тип профиля;
- Область действия;
- Тип входа LDAP;
- Администратор;
- Пароль администратора.

ТАБЛИЦА 2 // Типы профилей»

Тип профиля	Пояснение	«Получение» профиля	Назначение пароля
LDAP_AD	добавление учетной записи Microsoft AD	LDAP	LDAP
LOCAL	добавление учетной записи локального компьютера	Windows API (NetUserEnum) для Windows	Windows API (NetUserSetInfo) для Windows
		файл /etc/passwd для ОС семейства Linux	утилита chpasswd для ОС семейства Linux
AD[1]	добавление учетной записи Microsoft AD	ADSI	ADSI
LDAP_ALD[2]	добавление учетной записи ALD	LDAP	kadmin (kerberos admin protocol)
Kerberos[2]	добавление учетной записи ALD	kadmin (kerberos admin protocol)	kadmin (kerberos admin protocol)

[1] Данный тип профиля доступен только в ОС семейства Windows.

[2] Данный тип профиля доступен только в ОС семейства Linux.

В зависимости от выбранного **Типа профиля** заполнение остальных полей может не потребоваться (см. таблица 3).

ТАБЛИЦА 3

Необходимость заполнения полей от типа профиля

Поле	Тип профиля				
	LDAP_AP	LOCAL	AD	LDAP_ALD	Kerberos
Логин	+	+	+	+	+
Имя компьютера	+	—	—	+	—
Информация	+	+	+	+	+
Область действия Kerberos	—	—	—	—	+
Тип входа LDAP	+	—	—	+	—
Администратор	+/—	—	—	+/—	+
Пароль администратора					

Знак «+» в ячейке таблицы означает, что данное поле требуется заполнять при выборе данного типа профиля; знак «—» в ячейке таблицы означает, что данное поле не требуется заполнять при выборе данного типа профиля; знак «+/—» в ячейке таблицы означает, что необходимость заполнения данного поля зависит от значения поля Тип входа LDAP (см. таблица 4).

В зависимости от значения поля **Тип входа LDAP** для типов профилей **LDAP_AD, AD, LDAP_ALD** определяется необходимость заполнения поля для ввода идентификатора и пароля Администратора (см. таблица 4).

ТАБЛИЦА 4

Необходимость заполнения полей от типа входа LDAP

Поле	Тип входа LDAP						
	Anonymous	Simple	SASL GSSAPI	SASL EXTERNAL	SALS DIGEST-MD5	SALS PLAIN	SALS LOGIN
Администратор	—	+	—	—	+	+	+
Пароль администратора							

Знак «+» в ячейке таблицы означает, что данное поле требуется заполнять при выборе данного типа входа LDAP; знак «—» в ячейке таблицы означает, что данное поле не требуется заполнять при выборе данного типа входа LDAP.

Описание полей приведено в таблице 5.

ТАБЛИЦА 5 // Описание полей

(Знак «—» в ячейке таблицы означает, что данное поле не требуется заполнять при выборе данного типа профиля)

<table>
<tr><th rowspan="2">Поле</th><th colspan="5">Тип профиля</th></tr>
<tr><th>LDAP_AD</th><th>LDAP_ALD</th><th>AD</th><th>LOCAL</th><th>Kerberos</th></tr>
<tr><td>Логин</td><td colspan="3">Отличительное имя пользователя (User Destinguished Name, User DN)</td><td>Имя локального пользователя</td><td>Имя принципала Kerberos (Kerberos principal)</td></tr>
<tr><td>Имя компьютера</td><td colspan="2">Унифицированный идентификатор ресурса (LDAP URI) сервера службы каталогов по протоколу LDAP</td><td>Отличительное имя (DN, Distinguished Name) корня контекста имени по умолчанию</td><td>localhost</td><td>—</td></tr>
<tr><td>Информация</td><td colspan="3">Дополнительная информация о пользователе (displayName)</td><td>Полное имя пользователя в ОС семейства Windows и GECOS в ОС семейства Linux</td><td>—</td></tr>
<tr><td>Область действия Kerberos</td><td colspan="4">—</td><td>Область действия Kerberos (Kerberos realm)</td></tr>
<tr><td>Тип входа LDAP</td><td colspan="2">Метод/способ входа на сервер службы каталогов</td><td colspan="2" rowspan="3">—</td><td>—</td></tr>
<tr><td>Администратор</td><td colspan="2">User DN или samAccountName пользователя, под которым осуществляется вход на сервер службы каталогов</td><td>Имя принципала (Kerberos principal), от имени которого осуществляется вход на kadmind</td></tr>
<tr><td>Пароль администратора</td><td colspan="2">Пароль администратора</td><td>Пароль администратора</td></tr>
</table>

4.1.4.1 Импорт списка пользователей

Чтобы импортировать сформированный список пользователей, существует несколько способов:

— в строке меню выбрать «Пользователи» -> «Импорт»;

— на панели инструментов выбрать значок: 

Возможен импорт:

1) из файла HTML;
2) из файла XML;
3) из файла CSV;
4) из домена;
5) локальных пользователей;
6) из Active Directory (Astra Linux Directory)

> **Примечание:** При импорте списка пользователей из домена, локальных пользователей или пользователей из Active Directory (Astra Linux Directory) текущие пароли пользователей не импортируются, даже если они были назначены ранее.

4.1.4.1.1 Импорт из файла HTML

На рис. 13 приведен пример файла импорта в формате HTML, на рис. 14 соответствующий ему импортированный список.

РИСУНОК 13

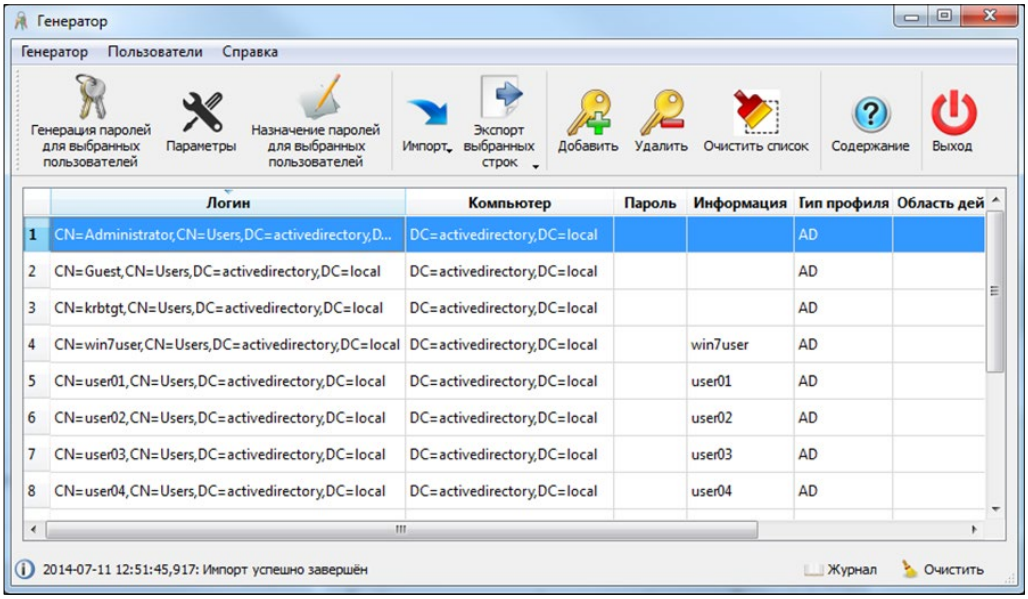
Файл для импорта в формате html

Список пользователей

Логин	Имя компьютера	Пароль	Информация	Тип профиля
CN=Administrator,CN=Users,DC=activedirectory,DC=local	DC=activedirectory,DC=local			AD
CN=Guest,CN=Users,DC=activedirectory,DC=local	DC=activedirectory,DC=local			AD
CN=krbtgt,CN=Users,DC=activedirectory,DC=local	DC=activedirectory,DC=local			AD
CN=win7user,CN=Users,DC=activedirectory,DC=local	DC=activedirectory,DC=local		win7user	AD
CN=user01,CN=Users,DC=activedirectory,DC=local	DC=activedirectory,DC=local		user01	AD
CN=user02,CN=Users,DC=activedirectory,DC=local	DC=activedirectory,DC=local		user02	AD
CN=user03,CN=Users,DC=activedirectory,DC=local	DC=activedirectory,DC=local		user03	AD
CN=user04,CN=Users,DC=activedirectory,DC=local	DC=activedirectory,DC=local		user04	AD
CN=user05,CN=Users,DC=activedirectory,DC=local	DC=activedirectory,DC=local		user05	AD
CN=user06,CN=Users,DC=activedirectory,DC=local	DC=activedirectory,DC=local		user06	AD
CN=user07,CN=Users,DC=activedirectory,DC=local	DC=activedirectory,DC=local		user07	AD
CN=user08,CN=Users,DC=activedirectory,DC=local	DC=activedirectory,DC=local		user08	AD
CN=user09,CN=Users,DC=activedirectory,DC=local	DC=activedirectory,DC=local		user09	AD
CN=user10,CN=Users,DC=activedirectory,DC=local	DC=activedirectory,DC=local		user10	AD

РИСУНОК 14

Импортированный список пользователей



4.1.4.1.2 Импорт из файла XML

На рис. 15 приведен пример файла импорта в формате XML. Соответствующий ему импортированный список пользователей совпадает со списком на рис. 14.

РИСУНОК 15

Файл для импорта в формате XML

```
<?xml version="1.0"?>
- <userlist>
    <user admin="" ldap_auth_method="" realm="" account_type="AD" password="" login="CN=Administrator,CN=Users,DC=activedirectory,DC=local" full_name=""
      host_name="DC=activedirectory,DC=local"/>
    <user admin="" ldap_auth_method="" realm="" account_type="AD" password="" login="CN=Guest,CN=Users,DC=activedirectory,DC=local" full_name=""
      host_name="DC=activedirectory,DC=local"/>
    <user admin="" ldap_auth_method="" realm="" account_type="AD" password="" login="CN=krbtgt,CN=Users,DC=activedirectory,DC=local" full_name=""
      host_name="DC=activedirectory,DC=local"/>
    <user admin="" ldap_auth_method="" realm="" account_type="AD" password="" login="CN=win7user,CN=Users,DC=activedirectory,DC=local" full_name="win7user"
      host_name="DC=activedirectory,DC=local"/>
    <user admin="" ldap_auth_method="" realm="" account_type="AD" password="" login="CN=user01,CN=Users,DC=activedirectory,DC=local" full_name="user01"
      host_name="DC=activedirectory,DC=local"/>
    <user admin="" ldap_auth_method="" realm="" account_type="AD" password="" login="CN=user02,CN=Users,DC=activedirectory,DC=local" full_name="user02"
      host_name="DC=activedirectory,DC=local"/>
    <user admin="" ldap_auth_method="" realm="" account_type="AD" password="" login="CN=user03,CN=Users,DC=activedirectory,DC=local" full_name="user03"
      host_name="DC=activedirectory,DC=local"/>
    <user admin="" ldap_auth_method="" realm="" account_type="AD" password="" login="CN=user04,CN=Users,DC=activedirectory,DC=local" full_name="user04"
      host_name="DC=activedirectory,DC=local"/>
    <user admin="" ldap_auth_method="" realm="" account_type="AD" password="" login="CN=user05,CN=Users,DC=activedirectory,DC=local" full_name="user05"
      host_name="DC=activedirectory,DC=local"/>
    <user admin="" ldap_auth_method="" realm="" account_type="AD" password="" login="CN=user06,CN=Users,DC=activedirectory,DC=local" full_name="user06"
      host_name="DC=activedirectory,DC=local"/>
    <user admin="" ldap_auth_method="" realm="" account_type="AD" password="" login="CN=user07,CN=Users,DC=activedirectory,DC=local" full_name="user07"
      host_name="DC=activedirectory,DC=local"/>
```

4.1.4.1.3 Импорт из файла CSV

На рис. 16 приведен пример файла импорта в формате CSV. Соответствующий ему импортированный список пользователей совпадает
со списком на рис. 14.

РИСУНОК 16

Файл для импорта в формате CSV

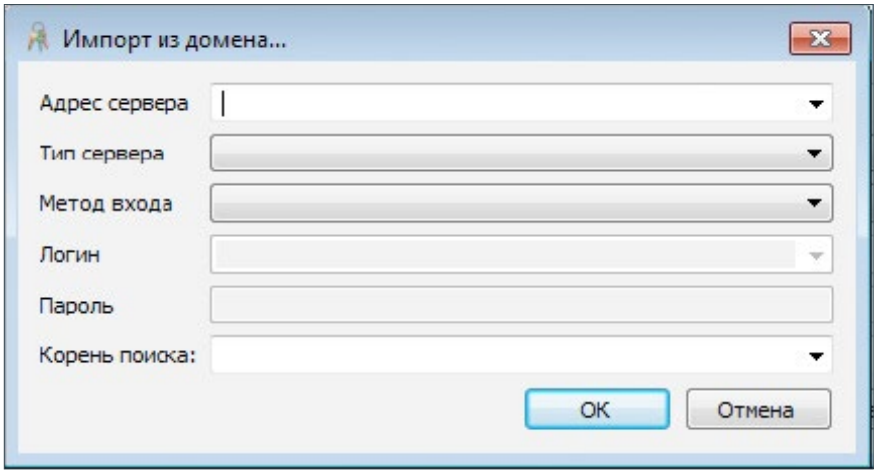
```
Логин,Компьютер,Пароль,Информация,Тип профиля,Область действия,Тип входа LDAP,Администратор
"CN=Administrator,CN=Users,DC=activedirectory,DC=local","DC=activedirectory,DC=local",,,AD,,,
"CN=Guest,CN=Users,DC=activedirectory,DC=local","DC=activedirectory,DC=local",,,AD,,,
"CN=krbtgt,CN=Users,DC=activedirectory,DC=local","DC=activedirectory,DC=local",,,AD,,,
"CN=win7user,CN=Users,DC=activedirectory,DC=local","DC=activedirectory,DC=local",,win7user,AD,,,
"CN=user01,CN=Users,DC=activedirectory,DC=local","DC=activedirectory,DC=local",,user01,AD,,,
"CN=user02,CN=Users,DC=activedirectory,DC=local","DC=activedirectory,DC=local",,user02,AD,,,
"CN=user03,CN=Users,DC=activedirectory,DC=local","DC=activedirectory,DC=local",,user03,AD,,,
"CN=user04,CN=Users,DC=activedirectory,DC=local","DC=activedirectory,DC=local",,user04,AD,,,
"CN=user05,CN=Users,DC=activedirectory,DC=local","DC=activedirectory,DC=local",,user05,AD,,,
"CN=user06,CN=Users,DC=activedirectory,DC=local","DC=activedirectory,DC=local",,user06,AD,,,
"CN=user07,CN=Users,DC=activedirectory,DC=local","DC=activedirectory,DC=local",,user07,AD,,,
```

4.1.4.1.4 Импорт из домена

При выборе данного пункта меню Импорт открывается диалоговое окно «Импорт из домена…» (см. рис. 17).

РИСУНОК 17

Диалоговое окно «Импорт из домена...»



Доступны следующие **Типы серверов**:

- Astra Linux Directory (ALD);
- Microsoft Active Directory (AD).

В качестве адреса сервера указывается LDAP URI сервера (согласно RFC-4516).

Доступные Методы входа:

- Anonymous;
- Simple;
- SASL GSSAPI;
- SASL EXTERNAL;
- SASL DIGEST-MD5;
- SASL PLAIN;
- SASL LOGIN.

Примеры заполнения полей диалогового окна «Импорт из домена в Astra Linux» приведены на рис. 18.

РИСУНОК 18 А

Примеры заполнения диалогового окна «Импорт из домена ...» Тип сервера: Microsoft Active Directory (AD)

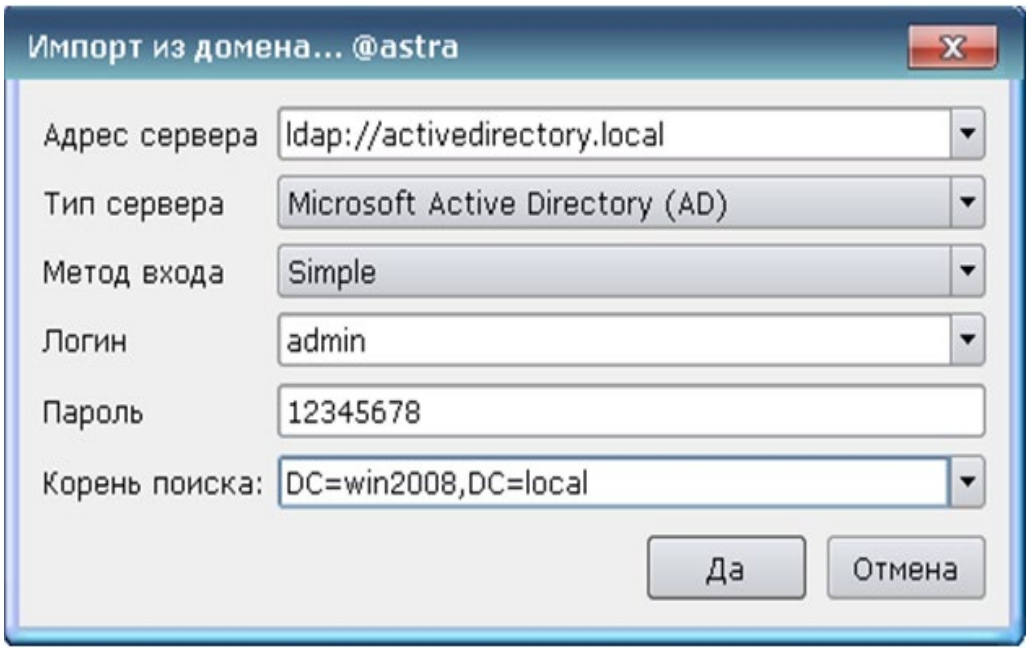
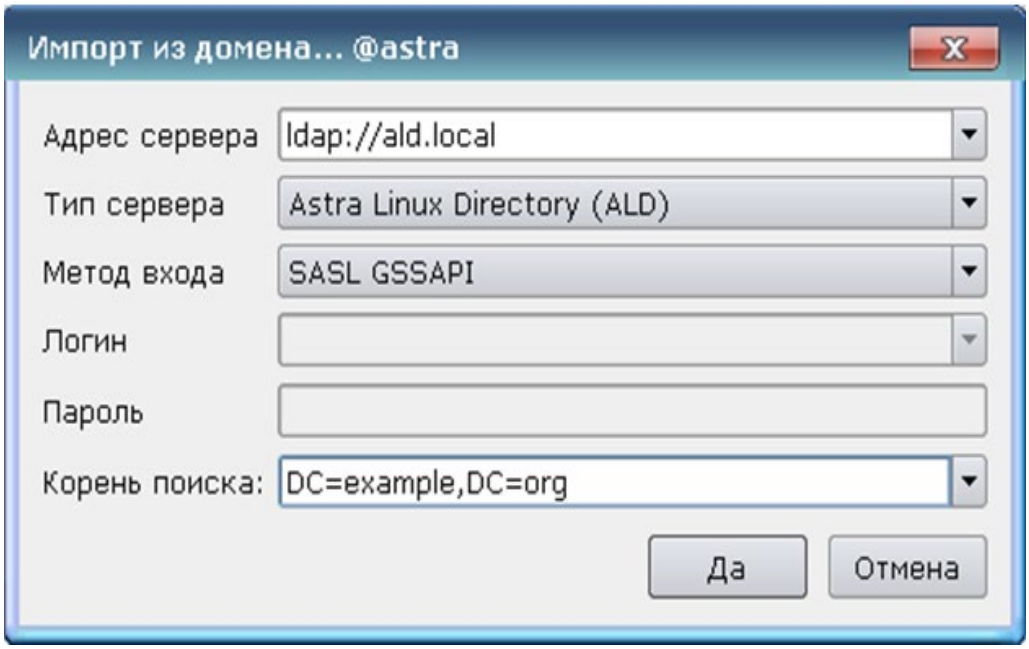


РИСУНОК 18 Б

Примеры заполнения диалогового окна «Импорт из домена ...» Тип сервера: Astra Linux Directory (ALD)



4.1.4.1.5 Импорт локальных пользователей

При выборе в ОС семейства Windows «Импорт» -> «Локальных пользователей» происходит импорт всех учетных записей локального компьютера (см. рис. 19).

В ОС семейства Linux есть возможность импорта всех локальных пользователей либо только несистемных пользователей (см. рис. 20).

РИСУНОК 19

«Импорт» -> «Локальных пользователей» в ОС семейства Windows

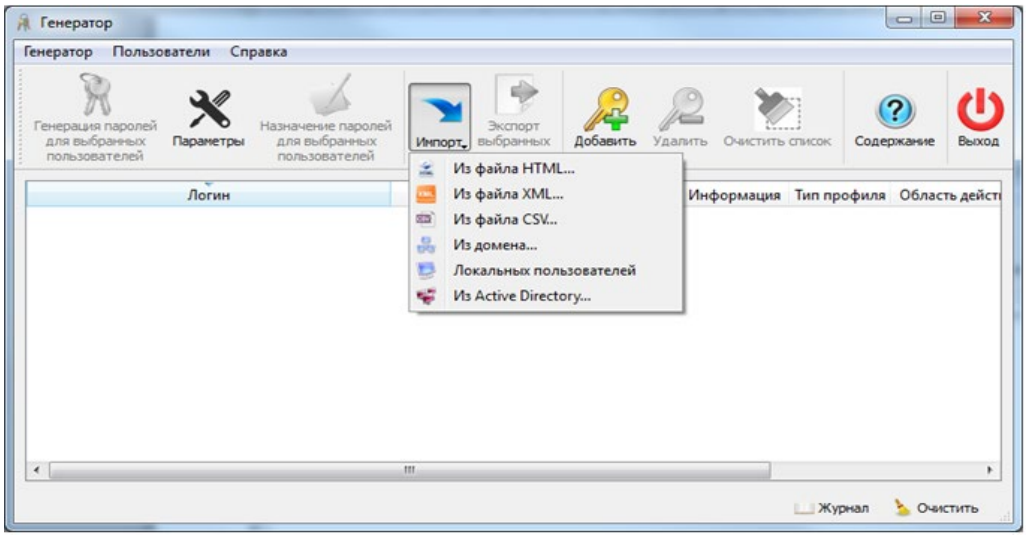
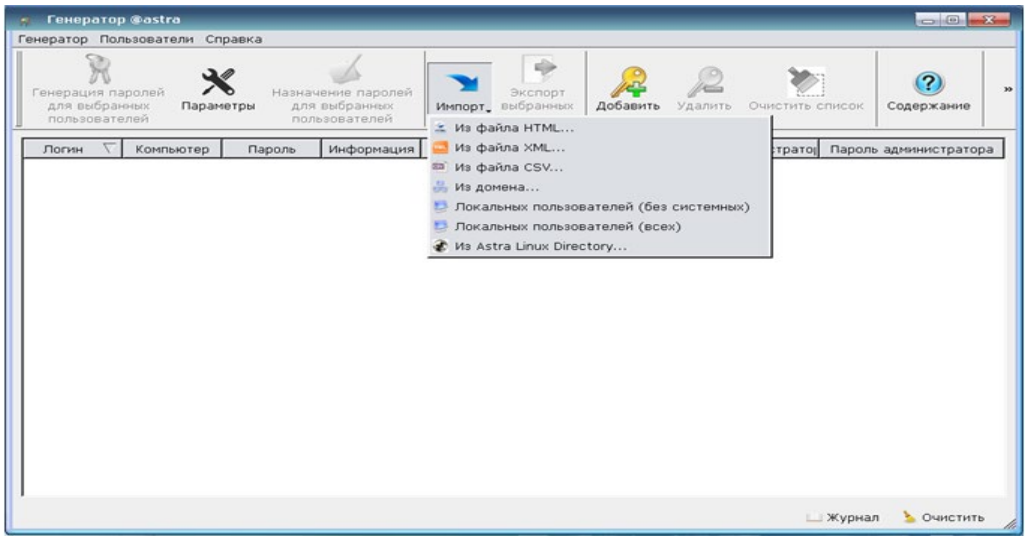


РИСУНОК 20

«Импорт» -> «Локальных пользователей (без системных)» и «Импорт» -> «Локальных пользователей (всех)» в ОС семейства Linux



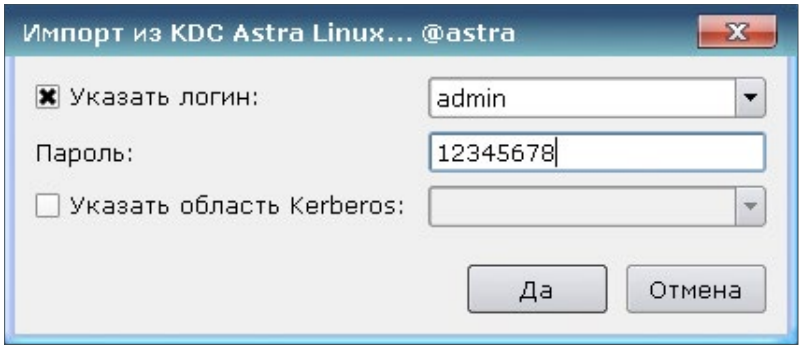
4.1.4.1.6 Импорт из Active Directory (Astra Linux Directory)

При выборе пункта меню «Импорт» -> «Из Active Directory…» в ОС семейства Windows происходит импорт учетных записей с компьютера, включенного в домен.

При выборе пункта меню «Импорт» -> «Из Astra Linux Directory…» в ОС семейства Linux откроется диалоговое окно (см. рис. 21).

РИСУНОК 21

«Импорт» -> «Из Astra Linux Directory…»



4.1.4.2 Добавление новых учетных записей пользователей в список

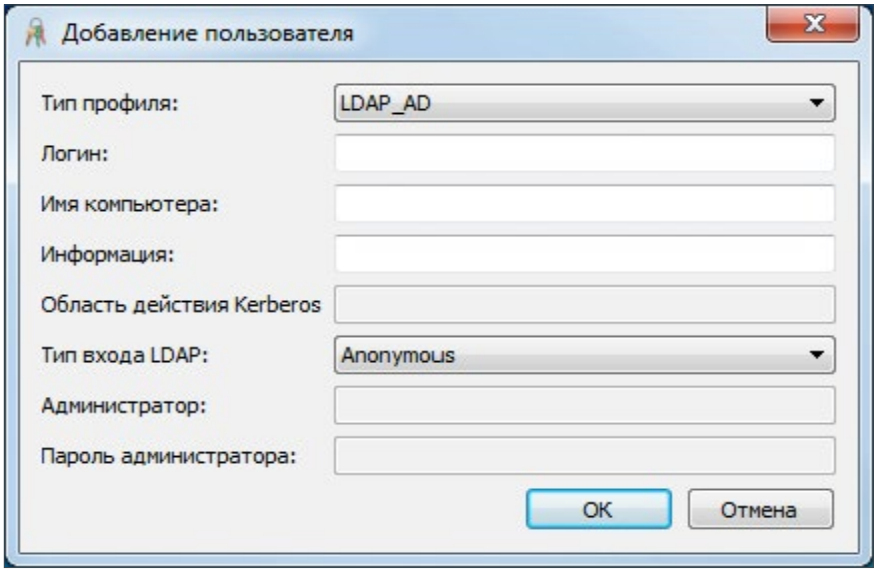
Чтобы добавить новую учетную запись пользователя в список пользователей, которым необходимо назначить пароли, существует несколько способов:

1) в строке меню выбрать «Пользователи» -> «Добавить…»;
2) на панели инструментов выбрать значок
3) использовать горячую клавишу Ins.

При использовании любого из этих способов откроется окно с параметрами для добавления нового пользователя (см. рис. 22).

РИСУНОК 22

Добавление пользователя



При добавлении пользователя необходимо выбрать один из **типов профилей** (см. таблица 2).

В зависимости от выбранного Типа профиля ряд полей активируются, а ряд полей становятся недоступными для заполнения (см. таблица 3).

Примеры заполнения полей диалогового окна «Добавление пользователя» в Astra Linux приведены на рис. 23.

РИСУНОК 23 А

Примеры заполнения полей диалогового окна «Добавление пользователя»: Тип профиля: LDAP_AD

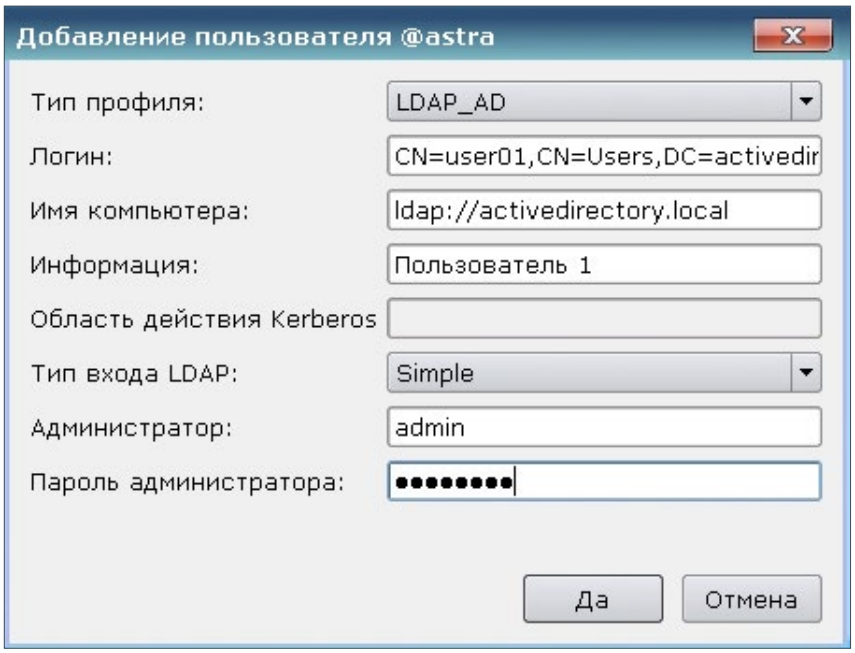


РИСУНОК 23 Б

Примеры заполнения полей диалогового окна «Добавление пользователя»: Тип профиля: LDAP_ALD

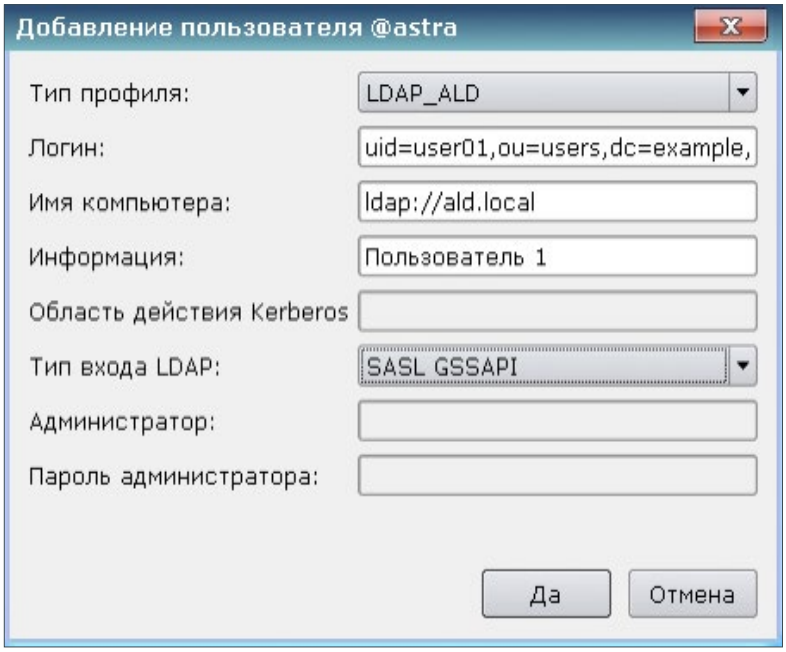
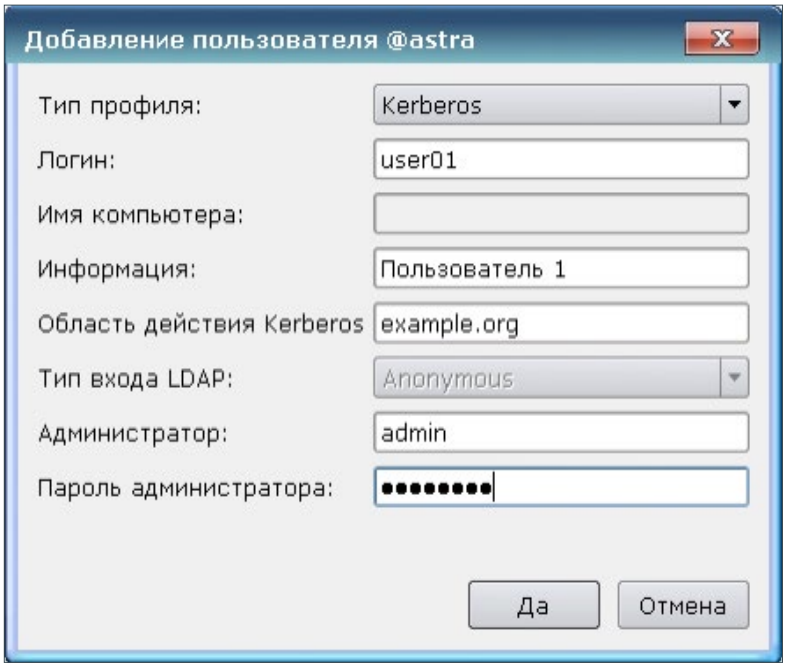


РИСУНОК 23 В

Примеры заполнения полей диалогового окна «Добавление пользователя»: Тип профиля: Kerberos



4.1.4.3 Удаление учетных записей пользователей из списка

Для удаления учетной записи пользователя* необходимо выполнить одно из следующих действий:

1) в строке меню выбрать «Пользователи» -> «Удалить»;
2) на панели инструментов нажать 

3) выделить нужную запись и нажать клавишу **Del**.

Для удаления всех записей из текущего списка пользователей необходимо выполнить одно из следующих действий:

1) в строке меню выбрать «Пользователи» -> «Очистить список»;
2) на панели инструментов нажать 

3) нажать сочетание клавиш **Ctrl+A**, убедиться в том, что все учетные записи выделены цветом, нажать клавишу **Del**.

4.1.5 Генерация паролей

В «Генераторе» предусмотрена генерация паролей без привязки к конкретным пользователям, а также генерация паролей с последующим присвоением их конкретным пользователям.

---

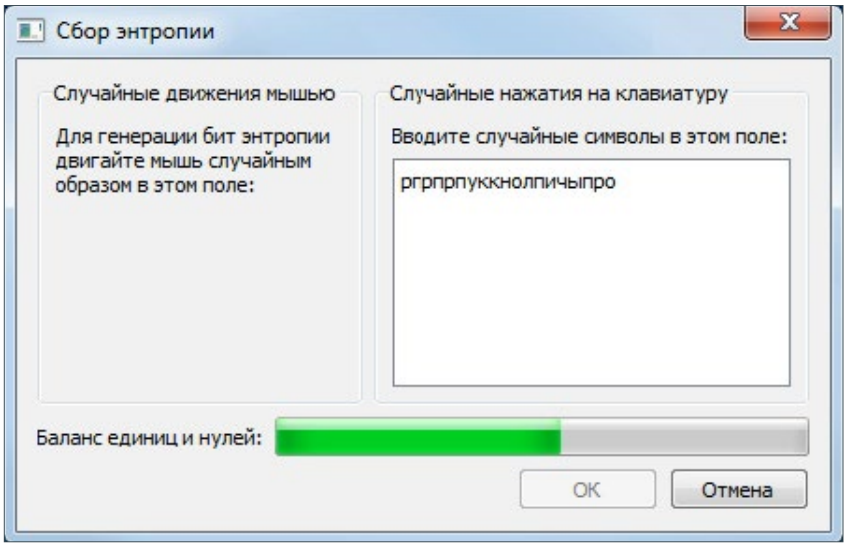
* — По умолчанию, в сформированном списке пользователей (см. пункт 4.1.4 Списки пользователей) выделена первая запись. Это означает, что действие будет произведено только для первого пользователя в списке. Однако оператор может самостоятельно выбирать пользователей, для которых необходимо совершить действие. Для этого необходимо выделить соответствующие строки, удерживая клавишу Ctrl. Для отмены выделения следует повторно кликнуть мышью по соответствующей записи, продолжая удерживать клавишу Ctrl. Для выбора всех пользователей в списке необходимо нажать сочетание клавиш Ctrl+A.

4.1.5.1 Сбор энтропии

При первой генерации паролей (см. пункт 4.1.5.2. Генерация паролей без привязки к конкретным пользователям, пункт 4.1.5.3 Генерация паролей для выбранных пользователей) происходит сбор энтропии.

После выбора пунктов меню «Генерация паролей для выбранных пользователей» или «Генерация списка паролей…» откроется диалоговое окно «Сбор энтропии» (см. рис. 24).

РИСУНОК 24
Диалоговое окно «Сбор энтропии»



В качестве источников энтропии используются:

- системное время;
- нажатия пользователя на клавиатуру;
- движения мышью (только в графической версии);
- PID текущего процесса;
- UID и GID (только для ОС семейства Linux);
- значения переменных из загруженной библиотеки user32.dll (только для ОС семейства Windows).

Диалоговое окно «Сбор энтропии» предназначено для получения данных от таких источников, как клавиатура и мышь. Пользователю предлагается перемещать курсор мыши случайным образом в левом поле рабочего окна и/или вводить случайные символы с клавиатуры в правом

поле окна до тех пор, пока индикатор баланса нулей и единиц не станет полностью зеленым.

На этом сбор энтропии от клавиатуры и мыши закончен. Пользователь может нажать кнопку «OK» для перехода к генерации паролей.

4.1.5.2 Генерация паролей без привязки к конкретным пользователям

Чтобы запустить процесс генерации паролей без привязки к конкретным пользователям, существует несколько способов:

1) в строке меню выбрать «Генератор» -> «Генерация списка паролей…»;
2) использовать сочетание клавиш Ctrl+L.

При использовании любого из этих способов откроется окно генерации списка паролей (см. рис. 25а). В данном окне задается количество необходимых для генерации паролей (по умолчанию 20).

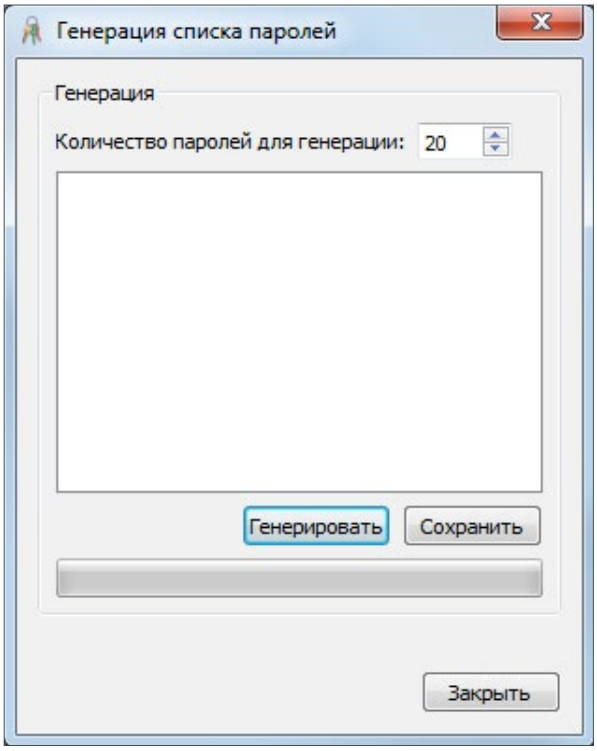
Для запуска процесса генерации паролей нажать на кнопку «Генерировать». При первой генерации откроется диалоговое окно «Сбор энтропии». Дальнейшие действия описаны в пункте 4.1.5.1 Сбор энтропии.

После окончания процесса генерации паролей отображается список сгенерированных паролей (см. рис.25б).

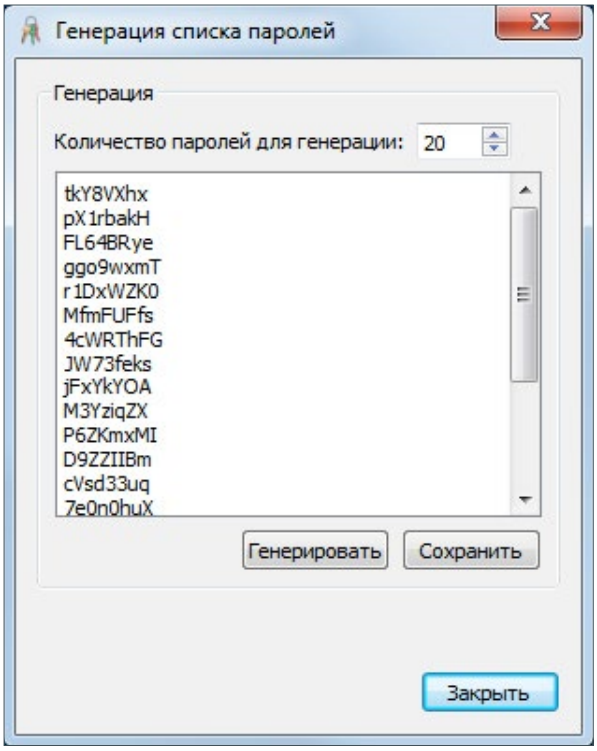
Предусмотрена возможность сохранения сгенерированного списка паролей в формате CSV. Для этого после окончания процедуры генерации необходимо нажать на кнопку «Сохранить».

РИСУНОК 25 // Окно генерации списка паролей

А) — перед началом генерации



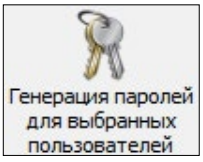
Б) — после завершения процедуры генерации



4.1.5.3 Генерация паролей для выбранных пользователей

Чтобы запустить процесс генерации паролей для выбранных пользователей, необходимо выполнить одно из следующих действий:

1) в строке меню выбрать «Генератор» -> «Генерация паролей для выбранных пользователей»;
2) на панели инструментов выбрать значок
3) использовать сочетание клавиш **Ctrl+G**.

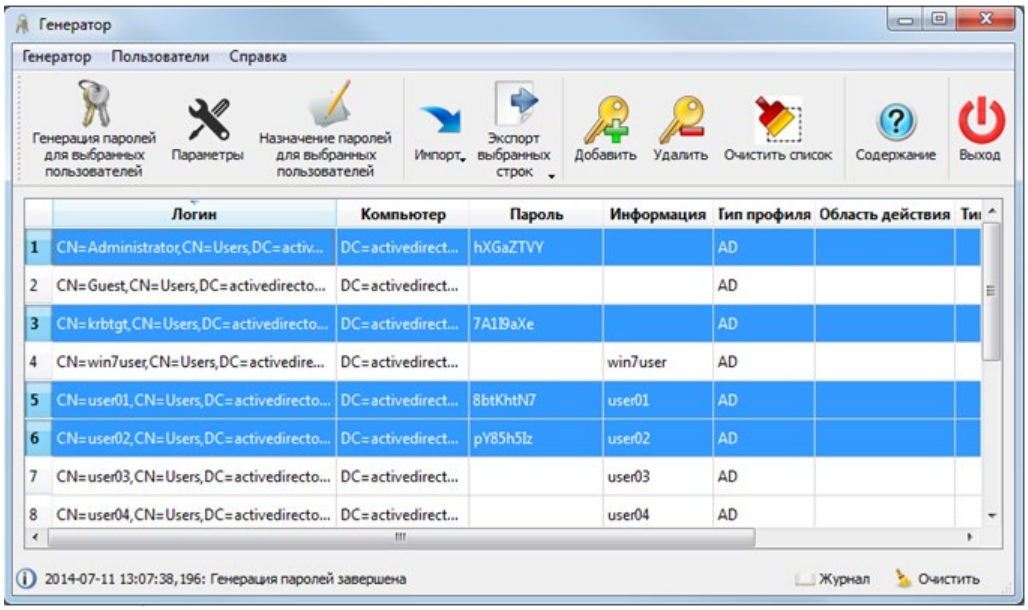


При первой генерации откроется диалоговое окно «Сбор энтропии». Дальнейшие действия описаны в пункте 4.1.5.1 Сбор энтропии.

Пример списка пользователей со сгенерированными паролями для отдельных пользователей приведен на рис. 26.

РИСУНОК 26

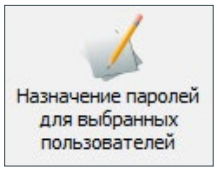
Список пользователей со сгенерированными паролями



4.1.6 Назначение паролей

Чтобы запустить процесс назначения сгенерированных паролей выбранным пользователям, необходимо выполнить одно из следующих действий:

1) в строке меню выбрать «Пользователи» -> «Назначение паролей для выбранных пользователей»;
2) на панели инструментов выбрать значок

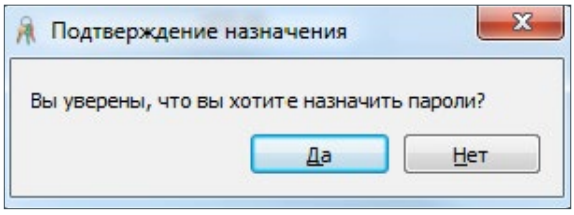


3) использовать горячую клавишу **F5**.

При использовании любого из этих способов откроется диалоговое окно «Подтверждение назначения» (см. рис. 27).

РИСУНОК 27

Диалоговое окно «Подтверждение назначения»

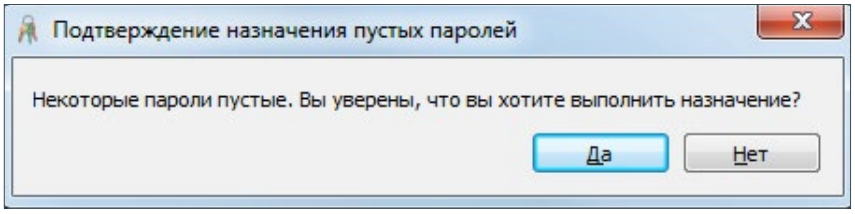


Оператор должен подтвердить свое намерение назначить пароли пользователям, нажав кнопку «Да».

Если среди назначаемых паролей есть пустые, откроется диалоговое окно «Подтверждение назначения пустых паролей» (см. рис. 28).

РИСУНОК 28

Диалоговое окно «Подтверждение назначения пустых паролей»



Чтобы отключить необходимость подтверждения назначения любых паролей, необходимо снять соответствующие отметки в меню «Генератор» -> «Параметры…» -> «Основные» (см. пункт 4.1.8.3. Основные)

4.1.7 Сохранение результатов

Чтобы сохранить списки пользователей со сгенерированными паролями, существует несколько способов:

1) в строке меню выбрать «Пользователи» -> «Экспорт выбранных строк»;
2) на панели инструментов выбрать значок

.

Экспортировать списки пользователей можно:

— в файл HTML;
— в файл XML;
— в файл CSV.

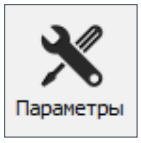
4.1.8 Параметры

Существует три группы параметров:

1) **Экспорт**: настройки, связанные с форматом сохранения результатов;
2) **Генерация**: настройки связанные с различными требованиями к сложности генерируемых паролей;
3) **Основные**: настройки, касающиеся всей логики работы программы.
1)

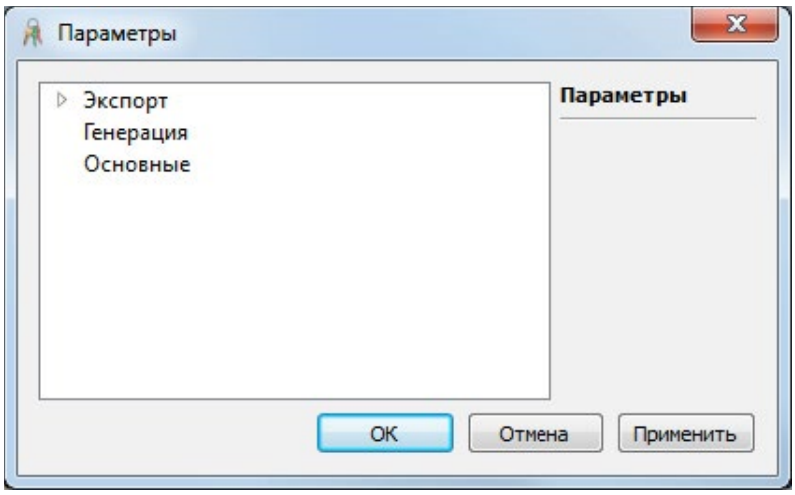
Чтобы вызвать диалоговое окно «Параметры» (см. рис. 29), существует несколько способов:

1) в строке меню выбрать «Генератор» -> «Параметры…»;
2) на панели инструментов выбрать значок



;
3) использовать сочетание клавиш **Ctrl+P**.

РИСУНОК 29
Диалоговое окно «Параметры»

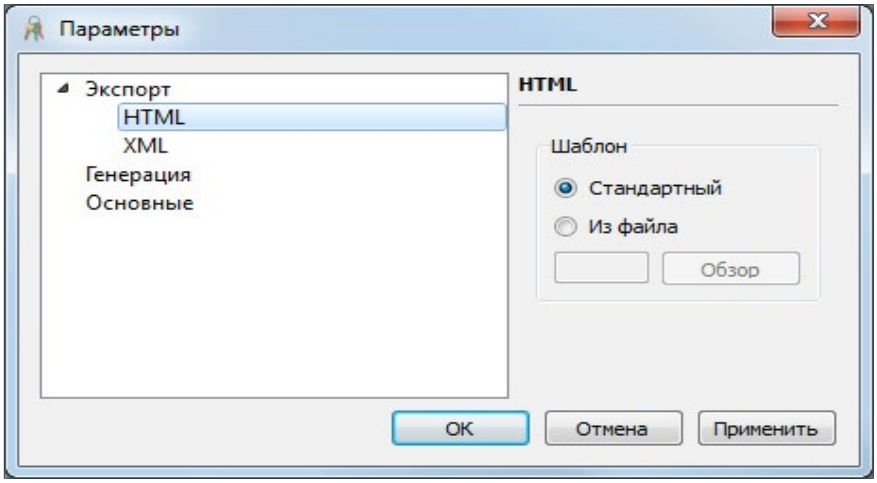


4.1.8.1 Экспорт

Данная группа параметров позволяет настраивать шаблоны для файлов экспорта (в форматах HTML и XML) (см. рис. 30).

РИСУНОК 30

Группа параметров «Экспорт»



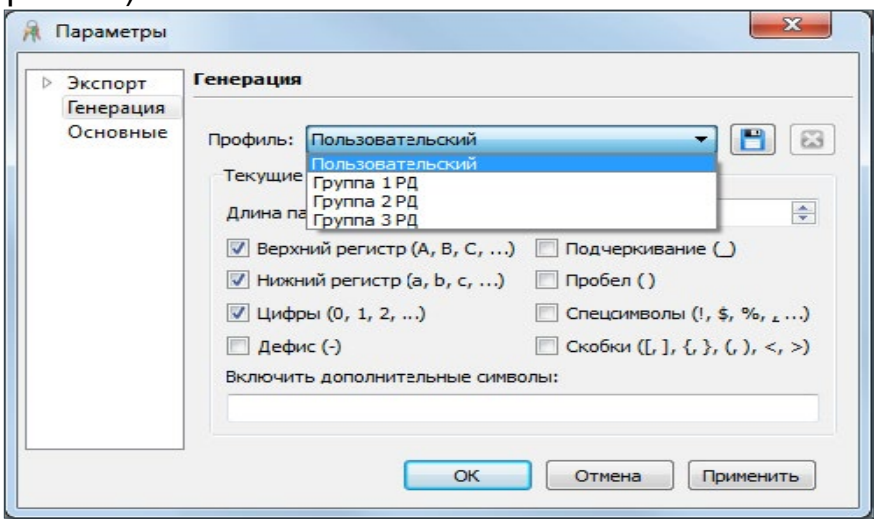
По умолчанию, используется стандартный шаблон «Генератора». Для использования пользовательского шаблона файла экспорта, необходимо поставить отметку напротив соответствующего пункта и указать путь до шаблона.

4.1.8.2 Генерация

Данная группа параметров позволяет задавать различные требования к паролям, сохранять требования в виде профилей, использовать встроенные профили «Генератора» (см. рис. 31).

РИСУНОК 31

Группа параметров «Генерация»



Список требований к паролям представлен в таблице 6.

ТАБЛИЦА 6
Требования к паролям

Требование	Диапазон	Комментарии
Длина пароля	2 — 99	количество символов в пароле (по умолчанию, 8)
Верхний регистр	A — Z	в совокупность используемых символов включены заглавные буквы латинского алфавита
Нижний регистр	a — z	в совокупность используемых символов включены прописные буквы латинского алфавита
Цифры	0 — 9	в совокупность используемых символов включены цифры
Дефис	—	в совокупность используемых символов включен дефис
Подчеркивание	_	в совокупность используемых символов включен знак подчеркивания
Пробел		в совокупность используемых символов включен знак пробела
Спецсимволы	; * % / . ^ ,! @ | $ + # : & ~ \ = ? ` «	в совокупность используемых символов включены спецсимволы
Скобки	[ ] { } ( ) < >	в совокупность используемых символов включены открывающие и закрывающие скобки

Также имеется возможность включить любые другие символы в совокупность используемых символов, написав их в поле «Включить дополнительные символы».

4.1.8.2.2 Профили

Профиль — совокупность требований к алфавиту и длине пароля.

4.1.8.2.2.1 Встроенные профили

Предусмотрено 4 встроенных профиля (см. таблица 7): Профиль **Пользовательский** не подлежит удалению. Профили **Группа 1 РД, Группа 2 РД, Группа 3 РД** не подлежат удалению и модификации.

ТАБЛИЦА 7
Встроенные профили

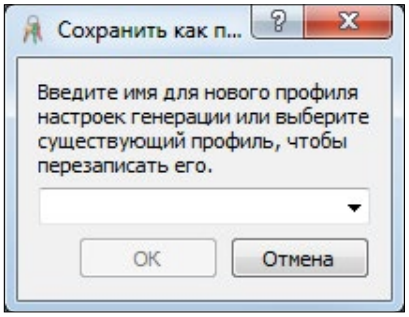
Название профиля	**Состав требований**	**Примечание**
Пользовательский	Установленные пользователем в данный момент времени	Используется по умолчанию
Группа 1 РД	Длина пароля: 8, Верхний регистр, Нижний регистр Цифры	Позволяют генерировать пароли, удовлетворяющие Руководящему документу «Автоматизированные системы. Защита от несанкционированного доступа к информации. Классификация автоматизированных систем и требования по защите информации»
Группа 2 РД	Длина пароля: 6, Верхний регистр, Нижний регистр Цифры	
Группа 3 РД		

4.1.8.2.2 Собственные профили

Пользователь может настроить требования и сохранить настройки в виде профиля. Для этого необходимо задать требования и нажать на кнопку  . Появится диалоговое окно для ввода имени профиля (см. рис. 31).

РИСУНОК 32

Диалоговое окно с предложением ввода имени профиля



Для удаления собственного профиля необходимо выбрать нужный профиль в списке профилей и нажать на кнопку .

4.1.8.3 Основные

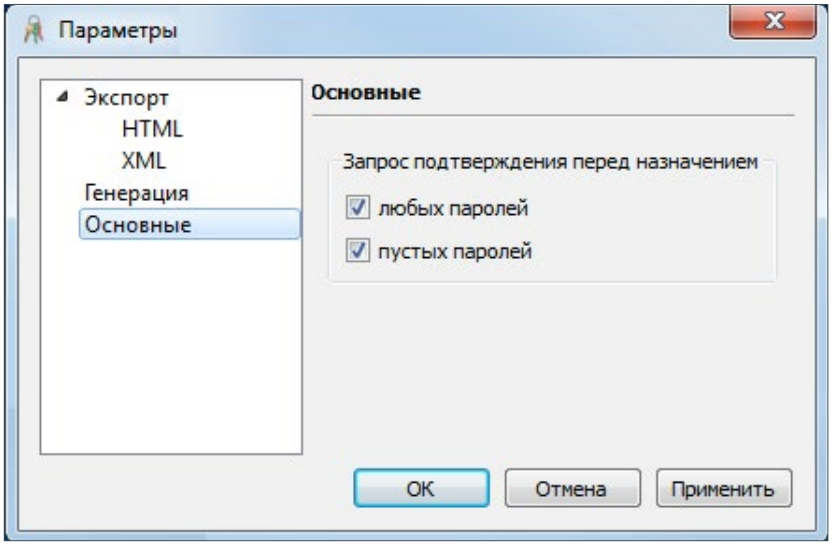
Данная группа параметров (см. рис. 33) включает возможность запрашивать подтверждение перед назначением:

— любых паролей;
— пустых паролей.

Чтобы активировать данные возможности, необходимо выставить отметки напротив соответствующих пунктов.

РИСУНОК 33

Группа параметров «Основные»



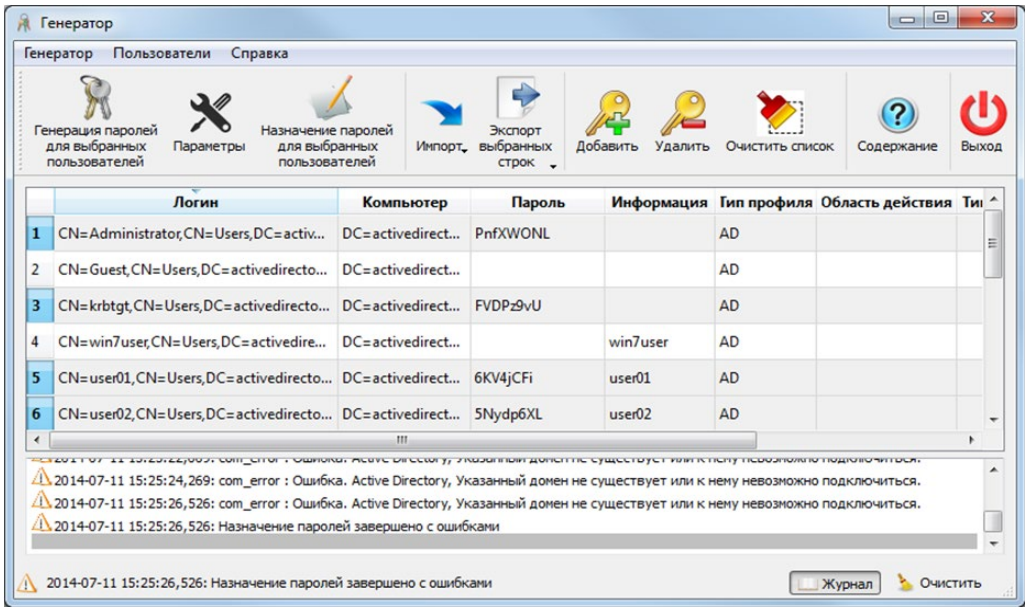
4.1.9 Журнал

В «Генераторе» имеется возможность журналирования следующих событий:

- запуск/завершение генерации паролей;
- запуск/завершение импорта списка пользователей;
- запуск/завершение экспорта списка пользователей;
- запуск/завершение назначения паролей;
- возникновение ошибки (например, ошибки подключения к домену, отсутствие прав для назначения паролей и др.).

Для просмотра журнала необходимо нажать на кнопку «Журнал» (см. рис. 34). Если отображение записей журнала отключено (кнопка «Журнал» не нажата), в нижней части экрана отображается информация только о последнем событии.

РИСУНОК 34
Просмотр журнала



Сообщения в журнале представлены в формате:

«YYYY-MM-DD hh:mm:ss,mmm: Текст сообщения».

Все записи о событиях в журнале сопровождаются графическим знаком:

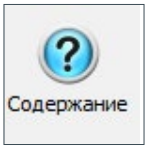
	информационное сообщение, которое следует принять к сведению;
	предупреждение о возможной ошибке, а также о важных моментах, на которые следует особо обратить внимание;
	информационное сообщение об ошибке, критичной для работы «Генератора».

Кнопка «Очистить» удаляет все записи из журнала.

4.1.10 Справочная информация

4.1.10.1 Справка

Чтобы просмотреть электронную версию настоящего руководства, существует несколько способов:

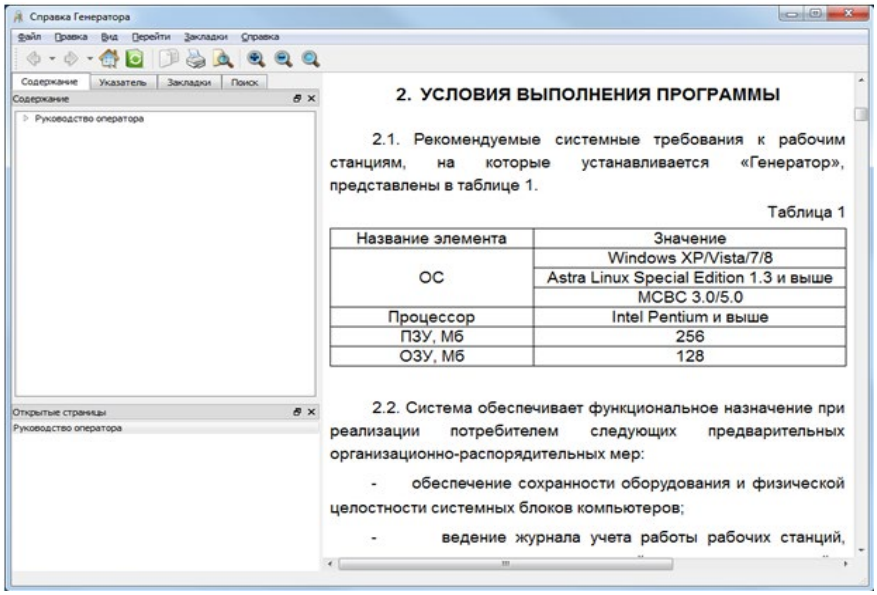
1) в строке меню выбрать «Справка» -> «Содержание…»;
2) на панели инструментов выбрать значок 

;
3) использовать горячую клавишу **F1**.

При использовании любого из этих способов откроется окно «Справка Генератора» (см. рис. 35).

РИСУНОК 35

Окно
«Справка Генератора»

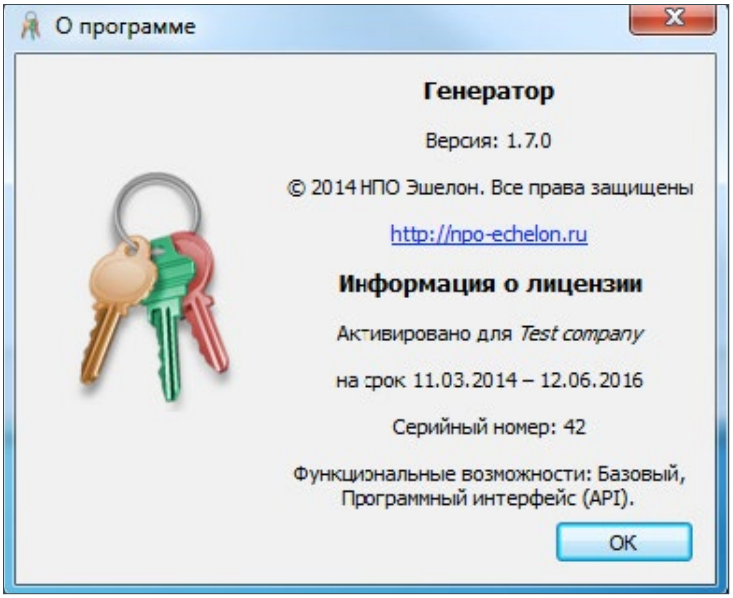


4.1.10.2 О программе

Чтобы просмотреть информацию о программе и лицензии на ее использование, необходимо перейти в пункт меню «Справка» -> «О программе…». Откроется диалоговое окно «О программе» (см. рис. 36).

РИСУНОК 36

Диалоговое окно
«О программе»



4.1.11 Завершение программы

Чтобы завершить программу, существует несколько способов:

1) в строке меню выбрать «Генератор» -> «Выход»;
2) на панели инструментов выбрать значок

;
3) использовать сочетание клавиш **Ctrl+Q**.

4.2 Работа в консольном режиме

Для работы в консольном режиме предусмотрены утилиты (см. таблица 8):

- **Консольная версия «Генератора»** (ech-generator);
- **Менеджер лицензий** (ech-license-manager);
- **Генератор ПДСЧ** (ech-prng);
- **Генератор паролей** (ech-pwgen).

Генератор ПДСЧ (ech-prng) может работать в интерактивном режиме (самостоятельная утилита) либо в режиме приема запросов (JSON API, для интеграции с другой программой).

Генератор паролей (ech-pwgen) также может использоваться в двух режимах: как самостоятельная утилита либо для интеграции с другой программой по JSON API.

ТАБЛИЦА 8

* — Для 64-битных версий каталог Program Files имеет название Program Files (x86)

Утилита	Путь к файлу по умолчанию	
	ОС семейства Windows*	ОС семейства Linux
Консольная версия «Генератора»	C:\Program Files\Echelon\ generator-ng\ ech-generator.exe	/usr/bin/ech-generator
Менеджер лицензий	C:\Program Files\Echelon\ generator-ng\ ech-license-manager.exe	usr/sbin/ech-license-manager
Генератор ПДСЧ	C:\Program Files\Echelon\ generator-ng\ ech-prng. exe	/usr/bin/ech-prng
Генератор паролей	C:\Program Files\Echelon\ generator-ng\ ech-pwgen. exe	/usr/bin/ech-pwgen

4.2.1 Консольная версия «Генератора»

Основные функциональные возможности консольной версии «Генератора»:

- импорт списка пользователей:
  - из файлов в формате HTML, XML, CSV;
  - из домена;
  - с локального компьютера;
  - из службы каталогов (Microsoft Active Directory, Astra Linux Directory);
- генерация паролей для отдельных учётных записей с возможностью задать:
  - множество допустимых символов для пароля;
  - длину пароля;
- экспорт сгенерированных паролей в файлы форматов HTML, XML, CSV.

4.2.1.1 Опции для работы с консольной версией «Генератора»

ech-generator	[-h] [-c COUNT] [-l LENGTH] [-y]
	[--additional ADDITIONAL] [--custom CUSTOM]
	[-if {html, xml, csv, ldap, pam_unix_regular, pam_unix, kerberos}] [-of {html, xml, csv}]
	[-a LICENSE_FILE] [-i INPUT]
	[--html-export-template HTML_EXPORT_TEMPLATE]
	[--xml-export-template XML_EXPORT_TEMPLATE]
	[--ldap-uri LDAP_URI] [--ldap-directory-type {ald, ad}]
	[--ldap-auth-method {anonymous, simple, sasl_gssapi, sasl_digest_md5,
	sasl_external, sasl_login, sasl_plain}]
	[--ldap-user LDAP_USER]
	[--ldap-search-base LDAP_SEARCH_BASE]
	[--kerberos-principal KERBEROS_PRINCIPAL]
	[--kerberos-realm KERBEROS_REALM]
	[output]

-h, --help	просмотреть справочное сообщение и выйти
-c COUNT, --count COUNT	количество паролей
-l LENGTH, --length LENGTH	длина пароля
-y, --symbols	специальные символы
--additional ADDITIONAL	дополнительные символы
--custom CUSTOM	только указанные символы
-if {html, xml, csv, ldap, pam_unix_regular, pam_unix,kerberos}, --input-format {html, xml, csv, ldap, pam_unix_regular, pam_unix, kerberos}	входной тип
-of {html, xml, csv}, --output-format {html, xml, csv}	выходной тип
-a LICENSE_FILE, --activation LICENSE_FILE	активация лицензии
-i INPUT, --input INPUT	входной файл
--html-export-template HTML_EXPORT_TEMPLATE	файл HTML-шаблона
--xml-export-template XML_EXPORT_TEMPLATE	файл XML-шаблона
--ldap-uri LDAP_URI	URI-адрес, ссылающийся на LDAP сервер
--ldap-directory-type {ald,ad}	тип LDAP сервера
--ldap-auth-method {anonymous, simple, sasl_gssapi, sasl_digest_md5, sasl_external, sasl_login, sasl_plain}	способ аутентификации на сервере
--ldap-user LDAP_USER	уникальное имя пользователя (DN) входа на LDAP-сервер
--ldap-search-base LDAP_SEARCH_BASE	корневой уровень для поиска пользователей
--kerberos-principal KERBEROS_PRINCIPAL	аутентифицирующееся лицо
-kerberos-realm KERBEROS_REALM	область действия (realm) базы данных Kerberos

4.2.1.2 Примеры использования

4.2.1.2.1Сгенерировать пароли (4 символа) для несистемных локальных учетных записей и сохранить результат в файл /tmp/pam.html:

```
ech-generator --length 4 -if pam_unix_regular -of html /tmp/pam.html
```

4.2.1.2.2 Сгенерировать пароли (4 символа) для всех локальных учетных записей и сохранить результат в файл /tmp/pam.html:

```
ech-generator --length 4 -if pam_unix -of html /tmp/pam.html
```

4.2.1.2.3 Сгенерировать пароли (4 символа) для учетных записей из файла /tmp/input.html и сохранить результат в файл /tmp/output.xml:

```
ech-generator --length 4 -if html -of xml -i /tmp/input.html /tmp/output.xml
```

4.2.1.2.4 Сгенерировать пароли (4 символа) для всех локальных учетных записей и сохранить результат в файл /tmp/pam.xml:

```
ech-generator --length 4 -if pam_unix -of xml /tmp/pam.xml
```

4.2.1.2.5 Сгенерировать пароли (4 символа) для несистемных локальных учетных записей и сохранить результат в файл /tmp/pam.csv:

```
ech-generator --length 4 -if pam_unix_regular -of csv /tmp/pam.csv
```

4.2.1.2.6 Сгенерировать список паролей в количестве 20 длиной 8 и сохранить в файл /tmp/passlist.xml:

```
ech-generator --length 8 -c 20 -of xml /tmp/passlist.xml
```

4.2.1.2.7 Kerberos: получение учетных записей от имени admin (утилита предложит ввести пароль), область действия — example.org:

```
ech-generator --length 4 --kerberos-principal admin  \ --kerberos-realm
example.org -if kerberos -of xml /tmp/output.xml
```

4.2.1.2.8 LDAP (AD): импорт пользователей из дерева Active Directory под корнем «DC=activedirectory, DC=local» от имени admin (утилита предложит ввести пароль):

```
ech-generator --length 4 -if ldap --ldap-uri ldap://activedirectory.local
\ --ldap-directory-type ad --ldap-auth-method simple --ldap-user admin \
--ldap-search-base DC=activedirectory,DC=local -of xml /tmp/output.xml
```

4.2.1.2.9 LDAP (ALD): импорт пользователей из дерева Astra Linux Directory под корнем «DC=example, DC=org» от имени admin (утилита предложит ввести пароль):

```
ech-generator --length 4 -if ldap --ldap-uri ldap://ald.local --ldap-
directory-type ald \
--ldap-auth-method simple --ldap-user admin --ldap-search-base
DC=example,DC=org \
-of xml /tmp/output.xml
```

4.2.2 Менеджер лицензий

Мастер лицензий Генератора. Позволяет активировать лицензию и выводить информацию об установленной лицензии.

4.2.2.1 Опции для работы с Менеджером лицензий

`ech-license-manager [-h] [-a FILE]`	
`-h, --help`	просмотреть справочное сообщение и выйти
`-a FILE, --activate FILE`	файл лицензии для активации (*.lic)

4.2.2.2 Примеры использования

4.2.2.2.1 Активировать лицензию из файла license.lic:

```
ech-license-manager -a license.lic
```

4.2.2.2.2 Просмотреть данные об установленной лицензии:

```
ech-license-manager
```

4.2.3 Генератор ПДСЧ

Утилита для генерации псевдослучайных чисел.

4.2.3.1 Опции для работы с Генератором ПДСЧ

ech-prng [-h] [-e FILE] [-s BYTES] [-o FILE] [-a]	
-h, --help	просмотреть справочное сообщение и выйти
-e FILE, --entropy FILE	файл, содержащий энтропию
-s BYTES, --output-size BYTES	размер генерируемого блока, в байтах
-o FILE, --output-file FILE	выходной файл
-a, --api	запуск в режиме демона, использующего JSON API

4.2.3.2 Примеры использования

4.2.3.2.1 Сгенерировать 42 псевдослучайных байта с выводом в консоль:

```
ech-prng -s 42
```

4.2.3.2.2 Сгенерировать псевдослучайные 2 байта, 2 Кб, 2 Кб, 2 Мб и 2 Мб соответственно в файл с названием out.bin:

```
ech-prng -s 2 -o out.bin
ech-prng -s 2k -o out.bin
ech-prng -s 2K -o out.bin
ech-prng -s 2m -o out.bin
ech-prng -s 2M -o out.bin
```

4.2.3.2.3 Инициализировать Генератор файлом с энтропией entropy.bin и сгенерировать 42 псевдослучайных байта в файл с названием out.bin:

```
ech-prng -e entropy.bin -s 42 -o out.bin
```

4.2.4 Генератор паролей

Утилита для генерации списка паролей в формате CSV.

4.2.4.1 Опции для работы с Генератором паролей

```
ech-pwgen       [-h] [-e FILE] [-o CSV_FILE] [-n NUMBER] [-l LENGTH]
                [-s] [-m CHARSET] [--custom CHARSET] [-a]
```

`-h, --help`	просмотреть справочное сообщение и выйти
`-e FILE, --entropy FILE`	файл, содержащий энтропию
`-o CSV_FILE, --output-file CSV_FILE`	выходной файл
`-n NUMBER, --number NUMBER`	количество паролей
`-l LENGTH, --length LENGTH`	длина пароля
`-s, --special`	спецсимволы (;*%/.^,!@|$+#':&~\=?`»_-<>(){}[])
`-m CHARSET, --more CHARSET`	дополнительные символы
`--custom CHARSET`	только указанные символы
`-a, --api`	запуск в режиме демона, использующего JSON API

4.2.4.2 Примеры использования

4.2.4.2.1 Сгенерировать 42 пароля длины 4, состоящих из символов букв в верхнем и нижнем регистрах и цифр, сохранить пароли в файле с названием passlist.csv:

```
ech-pwgen -l 4 -n 42 -o passlist.csv
```

4.2.4.2.2 Сгенерировать 42 пароля длины 4, состоящих из символов букв в верхнем и нижнем регистрах и цифр, используя для инициализации Генератора ech-prng файл ecntropy.bin, вывести пароли в стандартный вывод:

```
ech-pwgen -e entropy.bin -l 4 -n 42
```

4.2.4.2.3 Сгенерировать 42 пароля длины 4, состоящих из символов букв в верхнем и нижнем регистрах, цифр и спецсимволов, вывести пароли в стандартный вывод:

```
ech-pwgen -l 4 -n 42 –s
```

4.2.4.2.4 Сгенерировать 42 пароля длины 4, состоящих из символов букв в верхнем и нижнем регистрах, цифр и дополнительных символов (= + ; * #), вывести пароли в стандартный вывод:

1) для ОС семейства Windows:

```
ech-pwgen -l 4 -n 42  -m =+;*#
```

2) для ОС семейства Linux:

```
ech-pwgen -l 4 -n 42  -m «=+;*#»
```

4.2.4.2.5 Сгенерировать 42 пароля длины 4, состоящих только из указанных символов (= + ; * #), вывести пароли в стандартный вывод:

1) для ОС семейства Windows:

```
ech-pwgen -l 4 -n 42 --custom =+;*#
```

2) для ОС семейства Linux:

```
ech-pwgen -l 4 -n 42 --custom «=+;*#»
```

4.3 Работа в замкнутой программной среде Astra Linux

В «Генераторе» реализована возможность работы в операционной системе Astra Linux, находящейся в режиме замкнутой программной среды. Для обеспечения такой работы необходимо:

- включить режим замкнутой программной среды в Astra Linux;
- обеспечить загрузку дополнительного ключа «Генератора» механизмом замкнутой программной среды.

Средства создания замкнутой программной среды в Astra Linux более подробно описаны в документах:

- «ОПЕРАЦИОННАЯ СИСТЕМА СПЕЦИАЛЬНОГО НАЗНАЧЕНИЯ «ASTRA LINUX SPECIAL EDITION» Руководство по КСЗ. Часть 1 РУСБ.10015-01 97 01-1», пункт 12.4. Средства создания замкнутой программной среды, страница 78
- «ОПЕРАЦИОННАЯ СИСТЕМА СПЕЦИАЛЬНОГО НАЗНАЧЕНИЯ «ASTRA LINUX SPECIAL EDITION» Руководство администратора. РУСБ.10015-01 95 01», пункт 14.4. Средства создания замкнутой программной среды, страница 163

4.3.1 Включение режима замкнутой программной среды

Для включения режима замкнутой программной среды с возможностью загрузки дополнительных ключей (штатный

режим функционирования механизма контроля целостности) следует настроить модуль digsig_verif в стартовом загрузочном образе initrd. Для этого необходимо выполнить следующие действия от имени суперпользователя root:

> **Примечание**: далее в качестве образа initrd используется файл /boot/initrd.img-3.2.0-27-generic, но в зависимости от версии пакетов с ядром Linux имя файла в вашей системе может отличаться.

1) Рекомендуется сделать резервную копию образа initrd:

```
cp /boot/initrd.img-3.2.0-27-generic /root/backup-initrd.gz
```

2) Скопировать стартовый загрузочный образ initrd в отдельный каталог:

```
mkdir /root/initrd
cp /boot/initrd.img-3.2.0-27-generic /root/initrd/
```

3) Распаковать стартовый загрузочный образ:

```
mkdir /root/initrd/unpacked
cd /root/initrd/unpacked
gunzip < ../initrd* | cpio -i --make-directories
```

4) Отредактировать файл настройки модуля контроля целостности /root/initrd/unpacked/etc/digsig/digsig_initramfs.conf так, чтобы он содержал следующие строки:

```
DIGSIG_LOAD_KEYS=1
DIGSIG_ENFORCE=1
```

Первая строка позволит загрузить дополнительный ключ, которым подписаны файлы «Генератора», вторая строка включит механизм проверки целостности ELF-файлов.

5) Запаковать стартовый загрузочный образ:

```
cd /root/initrd/unpacked
find | cpio -H newc -o | gzip -9 > ../initrd*
```

6) Скопировать полученный образ в каталог /boot:

```
cp /root/initrd/initrd* /boot/initrd.img-3.2.0-27-generic
```

7) Удалить файлы распакованного образа:

```
rm -rf /root/initrd
```

8) Выполнить перезагрузку:

```
reboot
```

9) Убедиться, что система работает в режиме замкнутой программной среды, можно, выполнив команду:

```
cat /sys/digsig/enforce
```

Если команда выведет в консоли 1, то активен режим замкнутой программной среды, если же выведет 0, то система работает в обычном режиме (отладочный режим для тестирования СПО).

4.3.2 Загрузка дополнительного ключа

Загрузка дополнительного ключа может осуществляться двумя способами:

- загрузка дополнительного ключа после загрузки системы («ручная» загрузка дополнительного ключа, см. раздел 4.3.2.1. Ручная загрузка дополнительного ключа); в этом случае необходимо после запуска системы вручную выполнить команду, передающую дополнительный ключ модулю digsig_verif, либо каким-либо образом автоматизировать процесс (например, добавлением этой команды в планировщик или в /etc/rc.local).
- загрузка дополнительного ключа при инициализации системы (на этапе использования ядром Linux временной файловой системы initrd, см. раздел 4.3.2.2. Автоматическая загрузка дополнительного ключа).

4.3.2.1 Ручная загрузка дополнительного ключа

Для обеспечения работы установленного «Генератора» в штатном режиме функционирования механизма контроля целостности необходимо обеспечить загрузку модулем digsig_verif дополнительного ключа, которым подписаны файлы «Генератора». Для этого необходимо воспользоваться интерфейсом sysfs (следующую команду необходимо выполнить от имени суперпользователя root):

```
cat /<каталог ключа>/zao_npo_echelon_pub_key.gpg >
/sys/digsig/additional
```

После этого «Генератор» будет готов для использования в режиме замкнутой среды, однако дополнительный ключ не сохранится модулем digsig_verif при перезагрузке, и описанную выше команду необходимо будет повторить снова.

4.3.2.2 Автоматическая загрузка дополнительного ключа

Автоматическая загрузка дополнительного ключа заключается в изменении соответствующим образом стартового загрузочного образа initrd. Для этого необходимо выполнить следующие действия от имени суперпользователя root:

> **Примечание**: далее в качестве образа initrd используется файл /boot/initrd.img-3.2.0-27-generic, но в зависимости от версии пакетов с ядром Linux имя файла в вашей системе может отличаться.

1) Рекомендуется сделать резервную копию образа initrd:

```
cp /boot/initrd.img-3.2.0-27-generic /root/backup-initrd.gz
```

2) Скопировать стартовый загрузочный образ initrd в отдельный каталог:

```
mkdir /root/initrd
cp /boot/initrd.img-3.2.0-27-generic /root/initrd/
```

3) Распаковать стартовый загрузочный образ:

```
mkdir /root/initrd/unpacked
cd /root/initrd/unpacked
gunzip < ../initrd* | cpio -i --make-directories
```

4) Скопировать дополнительный ключ в распакованный образ initrd:

```
cp /<каталог ключа>/zao_npo_echelon_pub_key.gpg
/root/initrd/unpacked/etc/digsig/
```

5) Отредактировать скрипт

/root/initrd/unpacked/scripts/init-top/digsig_initramfs, добавив в него после строки:

```
cat /etc/digsig/key_for_signing.gpg >
/sys/digsig/additional 2>/dev/null
```

строку:

```
cat /etc/digsig/zao_npo_echelon_pub_key.gpg >>
/sys/digsig/additional 2>/dev/null
```

6) Запаковать стартовый загрузочный образ:

```
cd /root/initrd/unpacked
find | cpio -H newc -o | gzip -9 > ../initrd*
```

7) Скопировать полученный образ в каталог /boot:

```
cp /root/initrd/initrd* /boot/initrd.img-3.2.0-27-generic
```

8) Удалить файлы распакованного образа:

```
rm -rf /root/initrd
```

9) Выполнить перезагрузку:

```
reboot
```

При успешном выполнении вышеперечисленных действий «Генератор» будет готов к работе в замкнутой программной среде сразу после перезагрузки.

4.4 Взаимодействие с API утилит

Утилиты Генератор ПДСЧ (ech-prng) и Генератор паролей (ech-pwgen) запускаются в режиме демона, использующего JSON API, по ключу -a (или --api).

4.4.1 Запросы JSON

Утилита принимает со стандартного ввода запросы (request), являющиеся JSON-объектами. Разделителем запросов является символ конца строки UNIX (\n).

Каждый JSON-объект запроса (request) должен содержать:

- JSON-строку имени метода по ключу «method»;
- JSON-объект, описывающий аргументы по ключу «args».

Запрос {«method»: «quit», «args»: {}}, либо символ конца строки UNIX (\n) вместо запроса означают конец работы с утилитой и приводит к её завершению.

4.4.2 Ответы JSON

Результат запроса (response) представляет собой JSON-объект и выводится в стандартный вывод. Разделителем между результатами запросов также является символ конца строки UNIX (\n).

Каждый JSON-объект ответа (response) содержит либо результат успешного выполнения запроса по ключу «response», либо данные об ошибке по ключу «error».

4.4.2.1 Успешный ответ

Пример ответа на успешное выполнение метода:

```
{«response»: [«password1», «password2», «password3»]}
```

4.4.2.2 Ошибки

Данные об ошибке являются JSON-объектом и содержат следующие поля:

`error_class`	класс ошибки (String)
`error_msg`	описание ошибки (String)

4.2.2.2.1 Пример ответа с ошибкой:

```
{«error»: {«error_class»: «Base64DecodeError», «error_msg»:
«TypeError: Incorrect padding»}}
```

4.4.2.2.2 Примеры классов ошибок:

`JSONParseError`	проблема при синтаксическом анализе запроса из формата JSON
`Base64DecodeError`	проблема при декодировании данных запроса из base64
`PrngProtocolError`	общая ошибка в запросе для утилиты ech-prng (проблема в наборе аргументов, последовательности запросов, в названии метода запроса и т.п.)
`PwgenProtocolError`	общая ошибка в запросе для утилиты ech-pwgen (проблема в наборе аргументов, последовательности запросов, в названии метода запроса и т.п.)

4.4.3 Методы API Генератора ПДСЧ

Для использования Генератора ПДСЧ в режиме API необходимо инициализировать его энтропией, используя метод set_entropy. Далее можно использовать методы get_block и get_bytes для генерации случайных бит. Возможно повторно проинициализировать Генератор ПДСЧ с помощью метода set_entropy перед любым вызовом методов get_block и get_bytes. Для завершения работы утилиты используется метод quit. Более подробное описание методов и примеры их использования приведены ниже.

4.4.3.1 Метод set_entropy

Описание	Инициализирует Генератор псевдослучайных чисел	
Аргументы	Имя:	entropy
	Тип:	Array
	Описание:	энтропия, взятая из различных источников; каждый элемент массива — байты с источника энтропии, закодированные в base64 и представленные типом String; количество источников энтропии (размер массива) должен быть больше или равен 2; суммарная длина всей энтропии должна быть больше или равной 8 (или 8 символов, 8 байт).
Тип возвращаемого значения	null	
Пример запроса	`{«method»: «set_entropy», «args»: {«entropy»: [«HuMP», «+efo», «xJlp», «Atu4»]}}`	
Пример ответа	`{«response»: null}`	

4.4.3.2 Метод get_bytes

Описание	Возвращает строку, содержащую закодированную в base64 последовательность случайных байтов. Метод должен вызываться после инициализации Генератора энтропией	
Аргументы	Имя:	bytes
	Тип:	Number
	Описание:	требуемое количество байтов; должно быть больше нуля
Тип возвращаемого значения	String	
Пример запроса	`{«method»: «get_bytes», «args»: {«bytes»: 8}}`	
Пример ответа	`{«response»: «VKNxaxt6oCs=»}`	

4.4.3.3 Метод get_block

Описание	Выдаёт 2500 случайных байтов, закодированных в base64. Метод должен вызываться после инициализации Генератора энтропией. Метод аналогичен методу get_bytes с аргументом bytes равным 2500
Аргументы	Нет аргументов
Тип возвращаемого значения	String
Пример запроса	`{«method»: «get_block», «args»: {}}`
Пример ответа	`{«response»: «R...AAAAAAAAAAJi/EVA==»}`

4.4.3.4 Метод quit

Описание	Завершает выполнение
Аргументы	Нет аргументов
Тип возвращаемого значения	null
Пример запроса	`{«method»: «quit», «args»: {}}`
Пример ответа	`{«response»: null}`

4.4.3.5 Методы API Генератора паролей

Для использования Генератора паролей в режиме API необходимо инициализировать его энтропией, используя метод set_entropy. Далее используется метод get_pass для формирования паролей. Возможно повторно проинициализировать Генератор паролей с помощью метода set_entropy перед любым вызовом метода get_pass. Для завершения работы утилиты используется метод quit. Более подробное описание методов и примеры их использования приведены ниже.

4.4.3.6 Метод set_entropy

Описание	Инициализирует Генератор псевдослучайных чисел	
Аргументы	Имя:	entropy
	Тип:	Array
	Описание:	Энтропия, взятая из различных источников; каждый элемент массива — байты с источника энтропии, закодированные в base64 и представленные типом String; количество источников энтропии (размер массива) должен быть больше или равен 2; суммарная длина всей энтропии должна быть больше или равной 8 (или 8 символов, 8 байт).
Тип возвращаемого значения	null	
Пример запроса	`{«method»: «set_entropy», «args»: {«entropy»: [«HuMP», «+efo», «xJlp», «Atu4»]}}`	
Пример ответа	`{« response»: null}`	

4.4.3.7 Метод get_pass

Описание	Возвращает массив паролей. Метод должен вызываться после инициализации Генератора энтропией	
Аргументы	Имя:	length
	Тип:	Number
	Описание:	длина генерируемых паролей; число должно быть больше нуля и меньше размера алфавита (размер алфавита подсчитывается по уникальным символам)
	Имя:	number
	Тип:	Number
	Описание:	количество генерируемых паролей; число должно быть больше нуля
	Имя:	charset
	Тип:	Array
	Описание:	массив символов для генерации паролей (алфавит); элементы массива являются символами, представленными типом String
Тип возвращаемого значения	null	
Пример запроса	{«method»: «get_pass», «args»: {«length»: 2, «number»: 3, «charset»: [«0», «1», «2»]}}	
Пример ответа	{«response»: [«02», «01», «10»]}	

4.4.3.8 Метод quit

Описание	Завершает выполнение
Аргументы	Нет аргументов
Тип возвращаемого значения	null
Пример запроса	`{«method»: «quit», «args»: {}}`
Пример ответа	`{«response»: null}`