



АКЦИОНЕРНОЕ ОБЩЕСТВО  
«Аладдин Р.Д.»

УТВЕРЖДЕН  
RU.АЛДЕ.03.12.004 32 01–ЛУ

## СРЕДСТВО ОБМЕНА ДАННЫМИ НА ОПТИЧЕСКИХ ДИСКАХ

Руководство администратора

RU.АЛДЕ.03.12.004 32 01

Листов 29

2023

Литера О<sub>1</sub>

## АННОТАЦИЯ

Настоящий документ представляет собой руководство администратора программного средства RU.АЛДЕ.03.12.004 «Средство обмена данными на оптических дисках» (далее – программное средство). Документ содержит общие сведения о данном программном средстве, его структуре, установке и настройке для операционных систем Windows и Linux, а также о работе с программой RU.АЛДЕ.03.12.005 «Средство обмена данными на оптических дисках. Программа управления SecurCD Admin» (далее — программа управления SecurCD Admin), которая входит в состав программного средства и предназначена для его администрирования.

## СОДЕРЖАНИЕ

Термины и обозначения .....	4
1 Общие сведения о программе .....	5
2 Требования к ОС и аппаратному обеспечению .....	6
2.1 Требования к ОС .....	6
2.2 Требования к аппаратному обеспечению .....	6
3 Установка и настройка программы .....	7
3.1 Информация о нахождении установочных пакетов для программного средства .....	7
3.2 Установка и настройка программы для ОС Linux .....	7
3.3 Установка и настройка программы для ОС Windows .....	8
4 Удаление программы .....	11
4.1 Удаление программы для ОС Linux .....	11
4.2 Удаление программы для ОС Windows .....	11
5 Запуск программы SecurCD Admin .....	12
6 Остановка программы .....	13
7 Выполнение программы SecurCD Admin.....	14
7.1 Генерация атрибутов безопасности в токен или файл-контейнер .....	14
7.2 Срок действия пары атрибутов безопасности .....	15
7.3 Работа с атрибутом безопасности в программе управления SecurCD Admin .....	17
7.4 Удаление и редактирование пары атрибутов безопасности в программе управления SecurCD Admin .....	18
7.5 Запись стандартного диска с использованием старой пары атрибутов безопасности .....	19
7.6 Изменение пароля токена .....	19
7.7 Регистрация событий безопасности при доступе к операциям чтения/записи .....	21
8 Решение типовых проблем .....	22
8.1 Совместимость с ОС Windows .....	22
8.2 Совместимость с ОС Linux .....	22
8.3 Дополнительные возможности при установке на ОС Linux .....	23
8.4 Ручная активация и деактивация механизма защиты .....	24
8.5 Изменение шрифтов .....	26
9 Обращение в службу технической поддержки .....	28

## ТЕРМИНЫ И ОБОЗНАЧЕНИЯ

АРМ	Автоматизированное рабочее место
СВТ	Средство вычислительной техники
SecurCD	Средство обмена данными на оптических дисках
Взаимосвязанная пара атрибутов безопасности	Для специального преобразования данных на оптических дисках используется пара атрибутов безопасности: получателя и отправителя. Атрибут безопасности получателя должен быть передан получателю, а он должен передать свой атрибут безопасности получателю отправителю, который затем преобразовывает данные перед их отправкой с помощью средства обмена данными на оптических дисках. Может храниться в токене или файле-контейнере
Токен	USB-носитель «JaCarta SF/ГОСТ», персональное средство защиты информации и специализированное средство для безопасного хранения и переноса информации. Изделие предназначено для хранения атрибутов безопасности
Файл-контейнер	Файл-контейнер хранения атрибутов безопасности
Администратор программного средства	Лицо, осуществляющее установку, настройку и администрирование программного средства. Пользователь программы управления SecurCD Admin.
ОС	Операционная система
Пользователь программного средства	Лицо, производящее запись на оптические диски и чтение с них информации с помощью программы чтения-записи SecurCD Burner. Пользователь программы чтения-записи SecurCD Burner.

## 1 ОБЩИЕ СВЕДЕНИЯ О ПРОГРАММЕ

Программное средство «Средство обмена данными на оптических дисках» (RU.АЛДЕ.03.12.004), включает в свой состав следующие программные компоненты:

- программа управления SecurCD Admin (RU.АЛДЕ.03.12.005) — предназначена для генерации, назначения, редактирования и удаления атрибутов безопасности для управления доступом к информации, хранящейся на оптических дисках, просмотра журнала событий безопасности;

- программа чтения-записи SecurCD Burner (RU.АЛДЕ.02.02.008) — предназначена для предоставления доступа на чтение и/или запись информации с оптических дисков, в зависимости от назначенных атрибутов безопасности.

## 2 ТРЕБОВАНИЯ К ОС И АППАРАТНОМУ ОБЕСПЕЧЕНИЮ

### 2.1 Требования к ОС

Для функционирования программы чтения-записи SecurCD Burner с функцией записи информации на оптические диски на АРМ должна быть установлена операционная система Astra Linux 1.6, Astra Linux 1.7 или Альт 8 СП.

Для функционирования программы чтения-записи SecurCD Burner с функцией чтения информации с оптических дисков и функционирования программы управления SecurCD Admin, на АРМ должна быть установлена одна из следующих операционных систем:

- Astra Linux 1.6, 1.7;
- Windows 10;
- Альт 8 СП.

### 2.2 Требования к аппаратному обеспечению

Требования к средствам вычислительной техники для программного средства соответствуют минимальным требованиям к средствам вычислительной техники, на которые устанавливаются операционные системы Astra Linux 1.6, 1.7 x64, Альт 8 СП x64 и Windows 10 x86/x64.

Разрешение экрана монитора АРМ должно быть не менее 1024x768 точек.

Для обращения программного средства к изделиям USB-носитель «JaCarta SF/ГОСТ» используются свободные USB-порты 2.0 (full speed) типа А.

Для функционирования программы чтения-записи SecurCD Burner АРМ должно быть оборудовано приводом оптических дисков.

## 3 УСТАНОВКА И НАСТРОЙКА ПРОГРАММЫ

### 3.1 Информация о нахождении установочных пакетов для программного средства

Установочные пакеты программного средства будут доступны по предоставленной ссылке вида <https://dms.aladdin-rd.ru/910b23a1-43a0-445c-893b-1372d6ee2530>.

### 3.2 Установка и настройка программы для ОС Linux

Установочный пакет по имени операционной системы (например, `astra_linux_1_7`) рекомендуется скопировать на АРМ. Номер сборки представляет из себя четыре числа, разделенные точками, например: `secur-cd-1.0.0.77_amd64.deb`.

Названия исполняемых файлов и пути распаковки программ из состава программного средства для ОС Linux приведены в таблице ниже (Таблица 1)

Таблица 1 – Названия исполняемых файлов и пути распаковки программ для ОС Astra Linux или ОС Альт 8 СП

Имя пакета	Путь распаковки и имя файла
SecurCD Admin	
<code>secur-cd-1.0.0.77_amd64.deb/rpm</code>	<code>/opt/Aladdin/SecurCD/util/jc2sf.secur_cd.util-admin</code>
SecurCD Burner	
<code>secur-cd-1.0.0.77_amd64.deb/rpm</code>	<code>/opt/Aladdin/SecurCD/util/jc2sf.secur_cd.util-cdsec</code>

Чтобы установить программное средство необходимо выполнить следующие шаги:

1) Распаковать установочный архив для подходящей ОС в домашний каталог пользователя.

2) Закомментировать все имеющиеся активные репозитории, указанные в файле `/etc/apt/sources.list`.

3) Выполнить команду `sudo apt update`.

4) Перейти в каталог, куда был распакован архив из п.1, выполнив команду:

```
cd /*путь до каталога*
```

5) Выполнить скрипт установки программного средства командой:

```
bash -xe ./install.sh
```

6) Подтвердить установку недостающих пакетов.

### 3.3 Установка и настройка программы для ОС Windows

1) Для установки программы на ОС Windows необходимо запустить исполняемый файл `secur-cd-1.0.0.77-x86_64-setup.exe`.

2) Появится окно выбора режима установки программы (см. Рисунок 1)

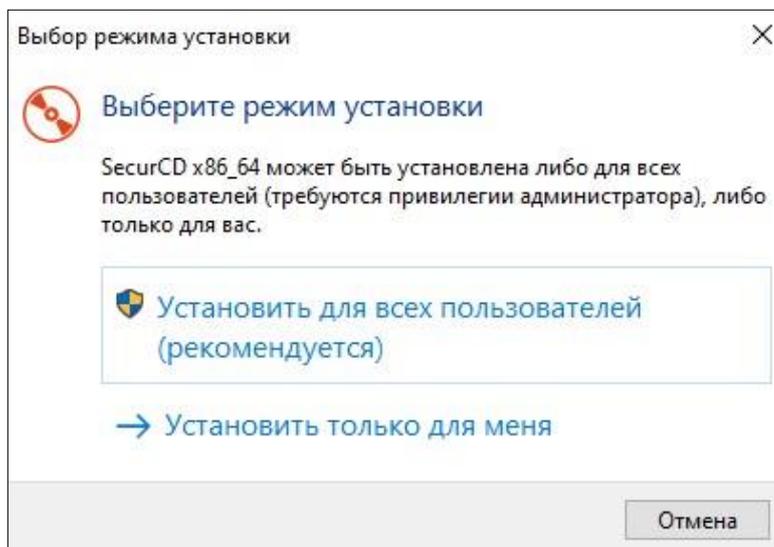


Рисунок 1 — Окно выбора режима установки

3) В следующем окне необходимо ознакомиться с лицензионным соглашением на устанавливаемую программу, принять его и нажать кнопку «Далее».

4) Затем в программе установки появится окно выбора папки установки программного средства. По умолчанию, директорией установки является папка `C:\Program Files\Aladdin\SecurCD\util`. Задайте папку установки программы и для продолжения нажмите на кнопку «Далее» (см. Рисунок 2).

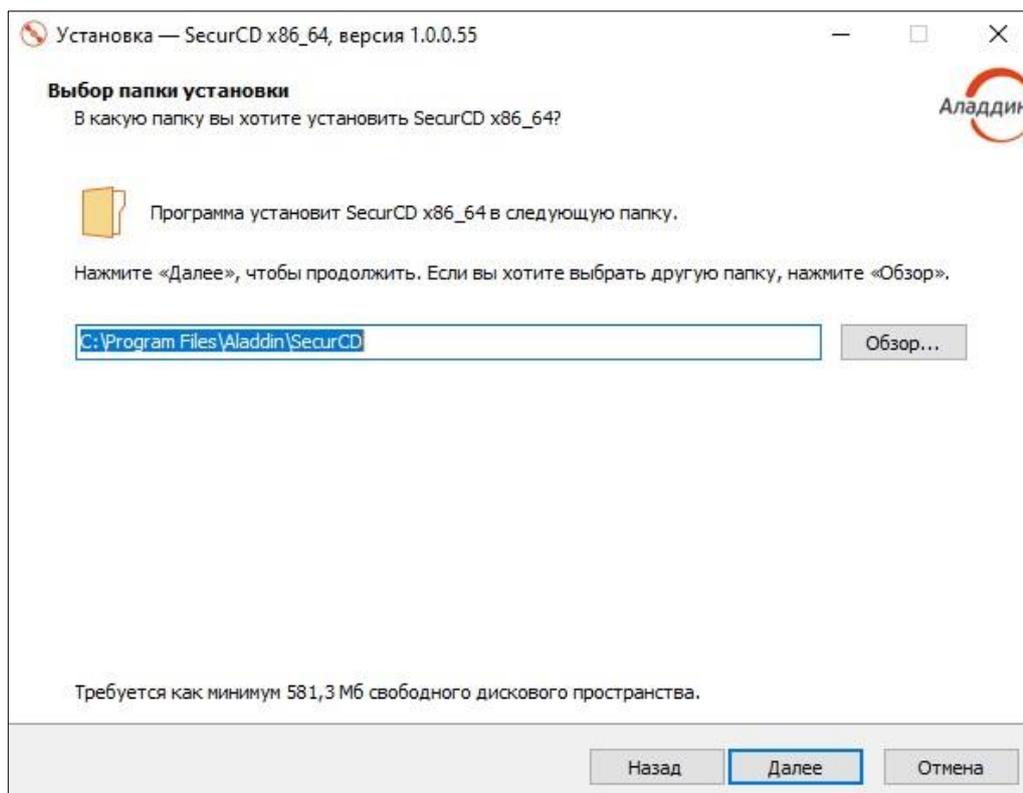


Рисунок 2 — Окно выбора директории установки программы

5) Далее программа предложит создать ярлыки на рабочем столе и активировать механизм защиты. Установите или снимите нужные флаги и для продолжения нажмите на кнопку «Далее» (см. Рисунок 3).

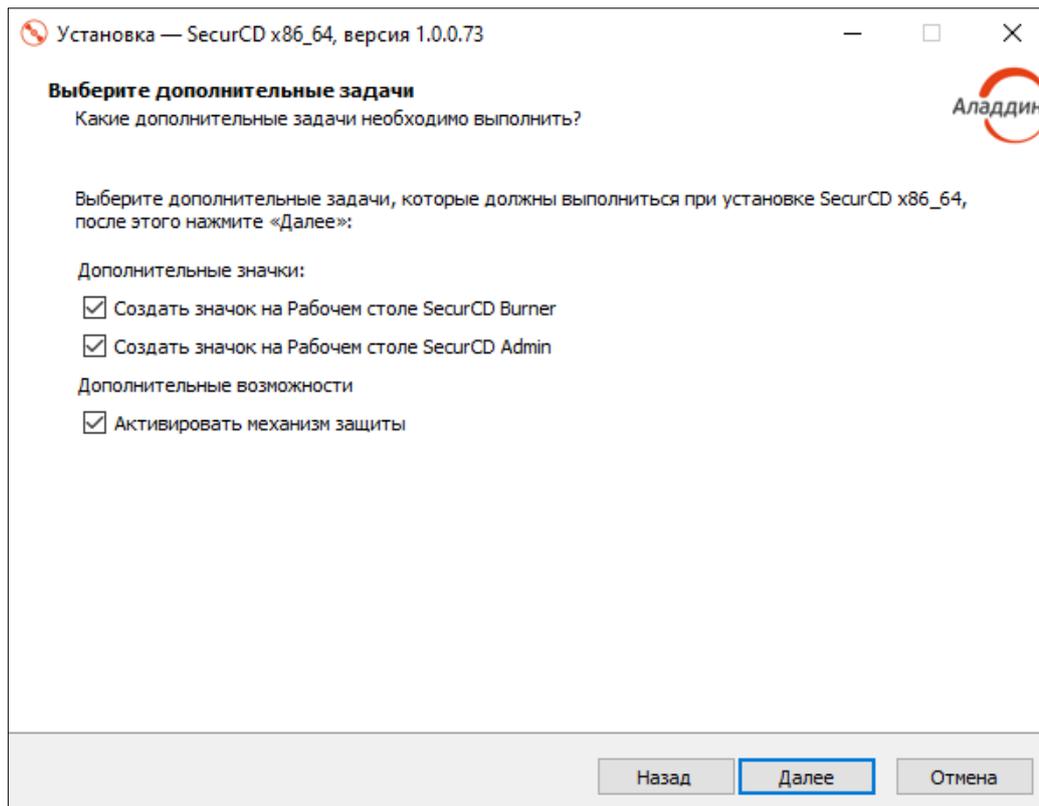


Рисунок 3 — Активация механизма защиты в Windows

6) Следующим этапом программа запросит подтверждение установки программы. Для подтверждения установки необходимо нажать на кнопку «Установить» после чего начнется установка программного средства.

7) Через некоторое время появится окно завершения работы программы установки.

8) Программное средство установлено на АРМ, нажмите на кнопку «Завершить».

## 4 УДАЛЕНИЕ ПРОГРАММЫ

### 4.1 Удаление программы для ОС Linux

Удаление установленного пакета программы осуществляется штатными средствами операционной системы. Удаление пакетов происходит таким же образом, как и любых других.

Пример команды для Astra Linux:

```
sudo apt-get purge secur-cd
```

Пример команды для Альт 8 СП:

```
sudo apt-get remove secur-cd
```

### 4.2 Удаление программы для ОС Windows

Удаление установленного пакета программы осуществляется штатными средствами операционной системы:

- 1) выберите программу через меню «Пуск»;
- 1) щелкните по программе правой кнопкой мыши и выберите «Удалить»;
- 2) подтвердите удаление программы.

## 5 ЗАПУСК ПРОГРАММЫ SECURCD ADMIN

Чтобы запустить программу SecurCD Admin:

- в ОС Linux щелкните левой кнопкой мыши по иконке  «SecurCD Admin», либо нажмите по иконке  «SecurCD Admin» во вкладке «Приложения → Инструменты» или «Приложения → Мультимедиа» в ОС Альт 8 СП или во вкладке «Меню «Пуск» → Утилиты» в ОС Astra Linux.
- в ОС Windows щелкните левой кнопкой мыши по иконке  «SecurCD Admin», либо выберите программу через меню «Пуск».

## 6 ОСТАНОВКА ПРОГРАММЫ

Завершение работы программы осуществляется по нажатию на крестик в заголовке окна либо по нажатию кнопки «Выход».

## 7 ВЫПОЛНЕНИЕ ПРОГРАММЫ SECURCD ADMIN

Допускается единовременная работа только одного экземпляра программы управления SecurCD Admin.

### 7.1 Генерация атрибутов безопасности в токен или файл-контейнер

Для того чтобы выполнить генерацию взаимосвязанной пары атрибутов безопасности:

1) Запустите программу управления SecurCD Admin и введите пароль пользователя персонального компьютера в появившейся форме, если механизм защиты активирован. Вход будет выполнен от пользователя `admsecd`, созданного при активации механизма защиты.

2) Нажмите кнопку «Каталог атрибутов безопасности».

3) Если база данных атрибутов безопасности получателей не была создана ранее, то она будет создана автоматически.

4) Если контейнер-хранилище атрибутов безопасности отправителей не был создан ранее, то пользователю будет предложено задать к нему пароль, после чего он будет создан в автоматическом режиме. Если требуется сгенерировать атрибуты безопасности на токен, то нажмите «Отмена», выберите токен в каталоге и введите его ПИН-код.

5) При открытии хранилища атрибутов отправителя (файла-контейнера) или токена и хранилища атрибутов безопасности получателя они будут автоматически отмечены как хранилища атрибутов безопасности под их генерацию (Рисунок 4). Если в хранилище нет атрибутов безопасности, то кнопка «Генерировать» будет выделена оранжевым и будет выведено сообщение о необходимости генерации атрибутов безопасности.

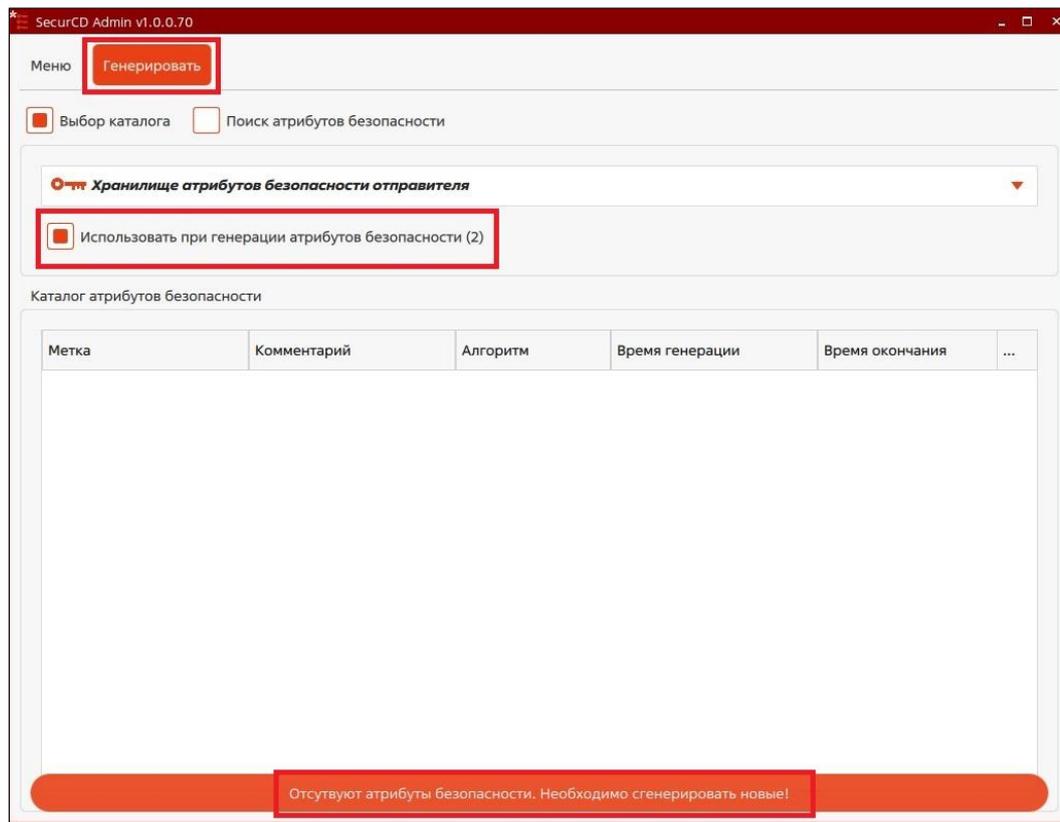


Рисунок 4 — Генерация взаимосвязанной пары атрибутов безопасности

6) Неинициализированное хранилище атрибутов безопасности отправителя (хранилище, в которое не выполнен вход) или токен маркируется серым «ключом». Инициализированное хранилище или токен, не выбранный под генерацию атрибутов безопасности, — желтым. Выбранное под генерацию хранилище атрибутов безопасности получателя — зеленым. Выбранное под генерацию атрибутов безопасности отправителя или токен — красным (как на рисунке выше).

7) Для генерации атрибутов безопасности необходимо нажать на кнопку «Генерировать» — задать метку, комментарий и срок действия атрибутов безопасности, а потом нажать «Сохранить».

8) После этого атрибуты безопасности будут доступны для использования при записи и чтении данных, а также для удаления, редактирования и импорта/экспорта (только атрибуты безопасности получателей).

При переходе с окна на окно боковое меню сворачивается для повышения удобства интерфейса открытого окна. Чтобы вновь открыть меню требуется нажать на кнопку «Меню».

## 7.2 Срок действия пары атрибутов безопасности

У каждой взаимосвязанной пары атрибутов безопасности имеется срок действия (по умолчанию — 3 года). Данный срок отображается в «Каталоге атрибутов безопасности» в столбце «Срок действия» (Рисунок 5).

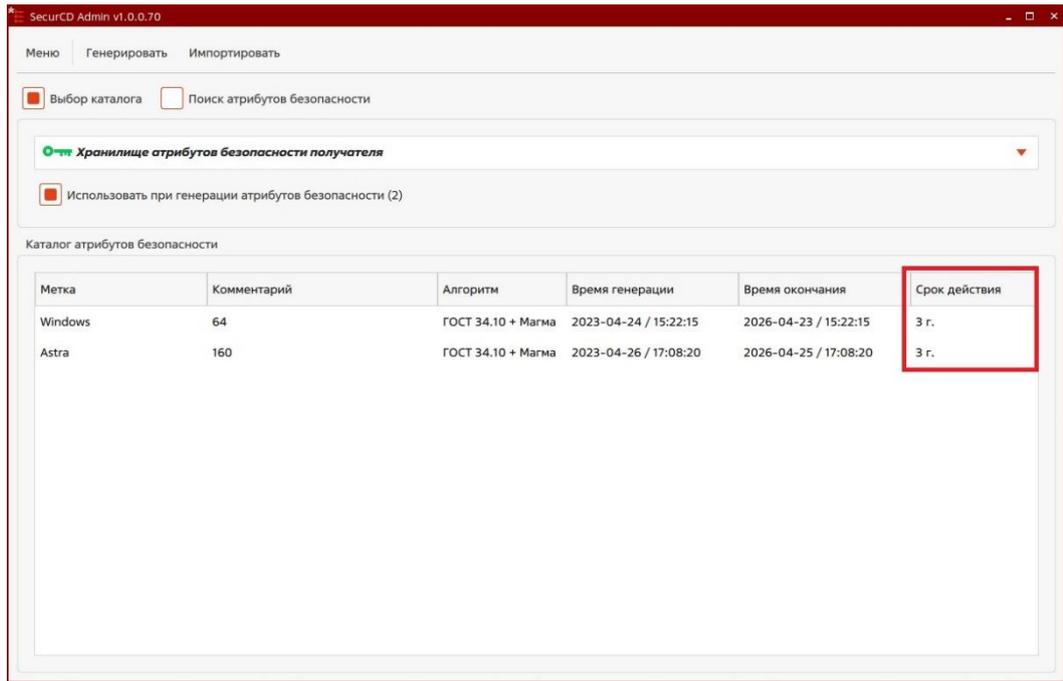


Рисунок 5 — Срок действия атрибутов безопасности

Также имеется опция маркировки атрибутов безопасности, когда их срок действия подходит к концу (Рисунок 6). Если срок действия атрибутов безопасности подходит к концу или уже завершился, то пользователь получит уведомление о необходимости сгенерировать новые атрибуты безопасности, а кнопка «Генерировать» будет окрашена оранжевым цветом:

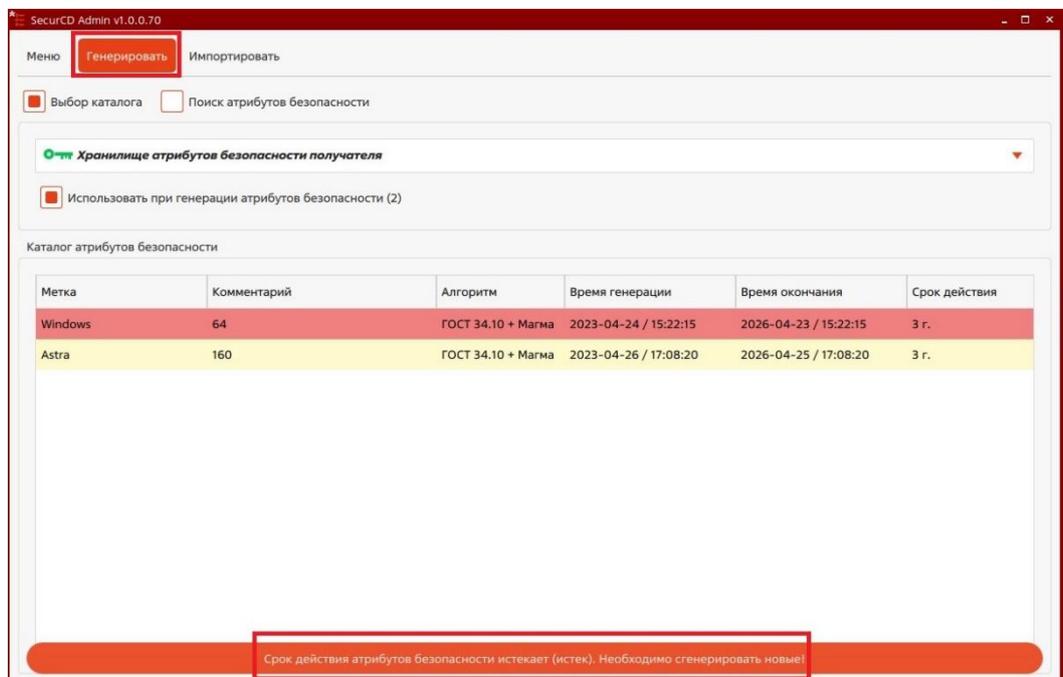


Рисунок 6 — Маркировка срока действия атрибутов безопасности

– Желтый цвет — предупреждение, срок действия атрибутов безопасности подходит к концу (по умолчанию отображается за 3 дня до конца срока).

- Красный цвет — срок действия атрибутов безопасности истек, их требуется заменить.

Если атрибут безопасности маркирован желтым, то следует сгенерировать новые атрибуты безопасности, поместив атрибут безопасности отправителя в тот же контейнер, что и старый. Программа будет автоматически использовать новые атрибуты безопасности, но при этом читать данные, записанные под старые атрибуты безопасности, если та все еще находится в контейнере. Когда атрибут безопасности маркируется красным — следует удалить атрибуты безопасности из-за истечения ее срока годности и использовать только новую.

Время активации предупреждения (желтого цвета) можно менять при помощи параметра `warning_days` в файле `util-admin`.

### 7.3 Работа с атрибутом безопасности в программе управления SecurCD Admin

Для того, чтобы экспортировать атрибут безопасности:

- 1) Запустите программу управления SecurCD Admin.
- 2) Нажмите кнопку «Каталог атрибутов безопасности».
- 3) Отобразится окно ввода пароля для хранилища атрибутов безопасности отправителя (Рисунок 7). Так как экспорт атрибутов безопасности из хранилища отправителя невозможен, то нажмите «Отмена» и перейдите в хранилище атрибутов безопасности получателя:

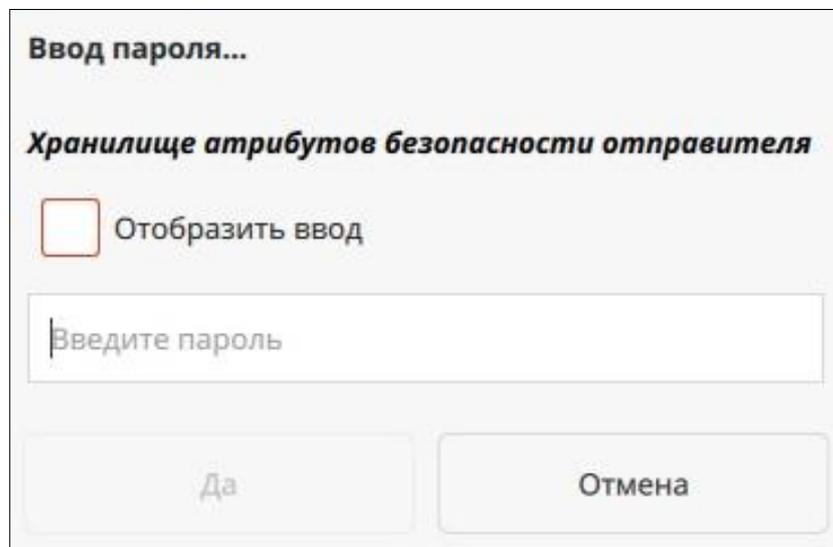


Рисунок 7 — Окно ввода пароля для токена

- 4) Выделите атрибут безопасности, который необходимо экспортировать и нажмите кнопку «Экспортировать». Выберите точку экспорта и подтвердите экспорт.

- 5) Для того, чтобы импортировать атрибут безопасности – нажмите кнопку «Импортировать». Выберите файл атрибута безопасности в файловой системе и подтвердите импорт.

6) Для того, чтобы удалить атрибут безопасности – выделите атрибут безопасности, который необходимо удалить из памяти токена или хранилища и нажмите кнопку «Удалить» (Рисунок 8):

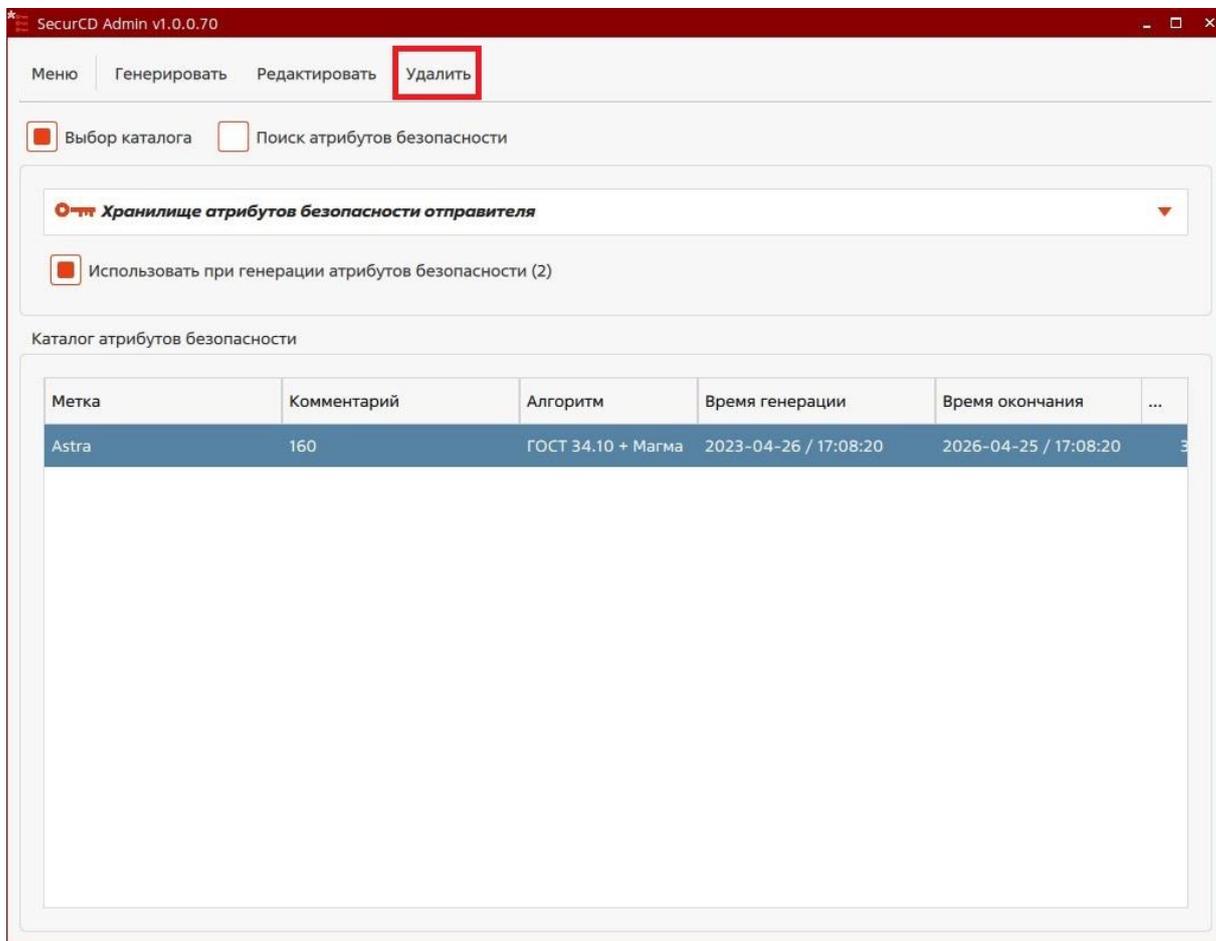


Рисунок 8 — Удаление атрибута безопасности из памяти хранилища

Программа поддерживает одновременный импорт, экспорт и удаление сразу нескольких атрибутов безопасности одновременно. Для этого необходимо перед нажатием кнопки «Экспортировать» или «Удалить» выбрать несколько атрибутов безопасности. Также возможен импорт файла с набором ранее экспортированных атрибутов безопасности (аналогично обычному импорту).

#### 7.4 Удаление и редактирование пары атрибутов безопасности в программе управления SecurCD Admin

Для того, чтобы удалить пару атрибутов безопасности:

- 1) Запустите программу управления SecurCD Admin.
- 2) Нажмите кнопку «Каталог атрибутов безопасности».

3) Отобразится окно ввода ПИН-кода для токена или пароля хранилища атрибутов безопасности отправителя.

4) Введите ПИН-код токена или пароль от хранилища атрибутов безопасности отправителя.

5) Выделите атрибут безопасности, который необходимо удалить из памяти токена или хранилища, и нажмите кнопку «Удалить».

6) В появившемся диалоговом окне укажите «Все каталоги» и подтвердите удаление. Таким образом удалятся сразу все атрибуты безопасности из пары.

Аналогичным образом возможно применить изменения к комментарию и метке атрибута безопасности — в окне редактирования необходимо отметить «Все каталоги».

## 7.5 Запись стандартного диска с использованием старой пары атрибутов безопасности

Также возможна работа одновременно с двумя парами атрибутов безопасности во время переходного периода, когда срок действия одной пары подходит к концу, а пара на замену ей уже сгенерирована. Старая пара еще сохраняется в каталоге, чтобы была возможность прочитать данные, записанные для нее — обновление атрибута безопасности получателя на всех APM происходит не мгновенно, а также имеется ранее записанная информация.

В таком случае для записи автоматически используется последняя сгенерированная пара атрибутов безопасности. Но чтение данных доступно как с помощью старой пары, так и с помощью новой.

Чтобы для записи использовать старую пару атрибутов безопасности, добавьте строку `use_older_key=true` в секции `form` файла `util-cdsec.ini`, хранящегося в папке `util` внутри папки `SecurCD`.

## 7.6 Изменение пароля токена

Для того, чтобы изменить пароль для токена:

- 1) Запустите программу управления SecurCD Admin.
- 2) Подключите токен к USB-порту.
- 3) Нажмите кнопку «Каталог атрибутов безопасности».
- 4) Введите ПИН-код токена.
- 5) Нажмите кнопку «Сменить пароль» (Рисунок 9).
- 6) Введите текущий пароль, затем новый пароль и повторите ввод нового пароля, соответствующего политике безопасности паролей (Рисунок 10).

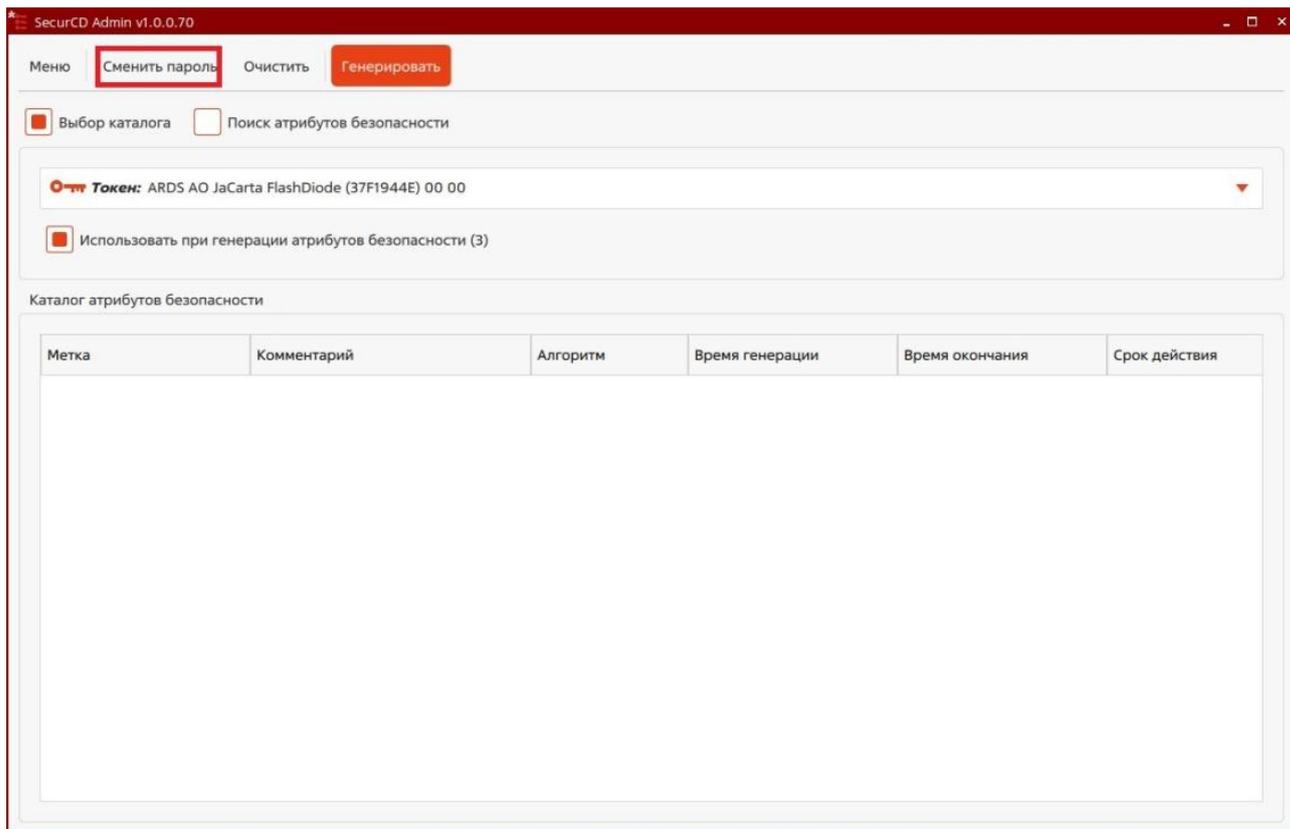


Рисунок 9 — Изменение пароля токена

**Изменение пароля...**

**Токен:** ARDS AO JaCarta FlashDiode (37F1944E) 00 00

Отобразить ввод Генерировать

Введите старый пароль

Введите новый пароль

Введите новый пароль еще раз

Символов должно быть не менее: 8

Рисунок 10 — Ввод нового пароля токена

## 7.7 Регистрация событий безопасности при доступе к операциям чтения/записи

Для того чтобы просмотреть журналы программного средства нажмите кнопку «Журнал событий» (Рисунок 11). Выгрузка журналов выполняется с помощью утилиты `cdsec_events_dump`, который находится внутри папки `util` каталога SecurCD. Имеется опция обновления (кнопка «Обновить») журнала в режиме реального времени, а также его очистки (кнопка «Очистить»). Также возможен поиск событий по имени и типу события («Ошибки», «Предупреждения», «Уведомления») с интерфейса, открывающегося после нажатия на кнопку «Поиск».

Программа	Тип	Описание	Пользователь	Время
Admin	⚠	Программа завершена	admin-test	2026-04-25 / 19:18:37
Admin	ℹ	Атрибуты безопасности загружены Хранилище: /opt/Aladdin/Secur...	admin-test	2026-04-25 / 19:18:34
Admin	⚠	Программа запущена	admin-test	2026-04-25 / 19:18:29
Burner	⚠	Программа завершена	admin-test	2026-04-25 / 19:18:23
Burner	✖	Присутствуют атрибуты безопасности отправителя с завершенным ...	admin-test	2026-04-25 / 19:18:21
Burner	ℹ	Атрибуты безопасности загружены: /opt/Aladdin/SecurCD/util/keys.s...	admin-test	2026-04-25 / 19:18:21
Burner	ℹ	Используется: /opt/Aladdin/SecurCD/util/keys.swt	admin-test	2026-04-25 / 19:18:20
Burner	⚠	Программа запущена	admin-test	2026-04-25 / 19:18:17
Admin	ℹ	Атрибуты безопасности загружены Хранилище: ARDS AO JaCarta Fla...	admin-test	2026-04-24 / 17:14:33
Admin	✖	Ошибка загрузки атрибутов безопасности: ARDS AO JaCarta FlashDio...	admin-test	2026-04-24 / 17:14:23
Admin	✖	Ошибка загрузки атрибутов безопасности! Хранилище: ARDS AO Ja...	admin-test	2026-04-24 / 17:14:23
Admin	ℹ	Атрибуты безопасности загружены Хранилище: /opt/Aladdin/Secur...	admin-test	2026-04-24 / 17:11:49
Admin	⚠	Программа запущена	admin-test	2026-04-24 / 17:11:41
Admin	⚠	Программа завершена	admin-test	2026-04-24 / 17:11:26
Admin	ℹ	Атрибуты безопасности загружены Хранилище: /opt/Aladdin/Secur...	admin-test	2026-04-24 / 17:11:21
Admin	✖	Ошибка загрузки атрибутов безопасности: /opt/Aladdin/SecurCD/uti...	admin-test	2026-04-24 / 17:11:06

Рисунок 11 — Журнал событий программного средства

## 8 РЕШЕНИЕ ТИПОВЫХ ПРОБЛЕМ

### 8.1 Совместимость с ОС Windows

Если при экспорте атрибутов безопасности с именами в кириллице внутри файловой системы персонального компьютера отображаются «битые» символы, то высока вероятность, что проблема в языковом пакете Windows.

Для исправления требуется выполнить следующее:

- 1) Перейти в «Параметры»
- 2) Выбрать «Время и язык».
- 3) В меню выбрать параметр «Язык».
- 4) В сопутствующих параметрах выбрать «Административные языковые параметры».
- 5) В панели «Язык программ, не поддерживающих Юникод» выбрать «Русский (Россия)».
- 6) Перезагрузить систему.

### 8.2 Совместимость с ОС Linux

На ОС Astra Linux возможен случай, что вставленный в привод диск будет невозможно примонтировать к системе. Для решения данной проблемы следует:

- 1) Выполнить команду `sudo rmmod cdrom_hooker`.
- 2) Закомментировать строчку `cdrom_hooker` в файле:
- 3) `/etc/modules-load.d/cdrom_hooker.conf`.
- 4) Перезапустить систему.

Если же при попытке монтирования диска возникает ошибка, то следует добавить информацию о диске в файл `fstab` (находится в папке `/etc`). Запись будет выглядеть следующим образом: `/dev/sr2 /mnt udf,iso9660,user,noauto 0 0`, где:

- `/dev/sr2` — адрес файловой системы диска.
- `/mnt` — точка подключения диска.

Для удаления программного средства на ОС Альт 8 СП необходимо использовать не просто команду `sudo`, а `sudo -E` или `su` из-за некорректной работы утилит XDG с командой `sudo` (иконки программы не удалятся).

Для верного отображения иконок программного средства на ОС Альт 8 СП требуется удалить опцию монтирования `noexec` каталога `/home` в файле `/etc/fstab`, т.е. в строке монтирования из `/home` убрать параметр `noexec`, а остальные параметры можно оставить. Затем необходимо перезагрузить систему.

Чтобы убрать ошибку «Ошибка поиска токенов» на ОС Альт 8 СП при использовании программы управления SecurCD Admin необходимо перезагрузить систему.

### 8.3 Дополнительные возможности при установке на ОС Linux

На ОС Astra Linux и ОС Альт 8 СП предусмотрены возможности отключения опции активации механизма защиты, отключения переноса точки монтирования, а также отключения создания ярлыков программ. Для этого используются следующие переменные окружения:

1) `SCD_NO_MENUITEM` — отключает создание ярлыков и элементов меню для запуска программ из программного средства;

2) `SCD_NO_PROTECT` — отключает активацию механизма защиты во время установки программы включая перенос точки монтирования в `/media`;

3) `SCD_NO_SHARE_MOUNTPOINT` — отключает перенос и настройку прав точки монтирования в каталог.

В ОС Astra 1.7 необходимо найти версию установленной ОС (можно посмотреть командой `cat /etc/astra_version`) и определить переменную окружения до команды `apt-get` к пакету `secur-cd`, как показано на рисунке ниже (Рисунок 12):

```
# оперативное обновление 1.7.3.00.1
if [ "$astra_version" = "1.7.3" ] && [ "$astra_version_package" = "8.1.34+ci4+v1.7.3.10" ]; then
    sudo apt-get install "$tmpdir"/packages/2022-1221SE17MD/*
    sudo SCD_NO_MENUITEM=true apt-get install "$dir"/debs/secur-cd*1.7.2*.deb
```

Рисунок 12 – Дополнительные возможности установки

В ОС Astra 1.6 необходимо изменить аналогичную строку, общую для всех обновлений ОС, схожим образом.

В ОС Альт 8 СП необходимо также изменить «установочную» строку, определив переменную окружения до команды установки `apt-get`, как показано на рисунке ниже (Рисунок 13):

```
su -c "apt-get install "$tmpdir"/packages/base/*"
su -c "SCD_NO_MENUITEM=true apt-get install "$dir"/rpms/*.rpm"
```

Рисунок 13 – Дополнительные возможности установки

Если механизм защиты уже активирован, то опция `SCD_NO_PROTECT` его не деактивирует. Таким образом, если требуется обновить уже имеющуюся версию программного средства, то необходимо производить установку новой версии с определенной переменной окружения `SCD_NO_PROTECT`.

## 8.4 Ручная активация и деактивация механизма защиты

Ручная активация механизма защиты выполняется следующим порядком использования скриптов, находящихся в каталоге `/opt/Aladdin/SecurCD/util` для ОС Linux и `C:\Program Files\Aladdin\SecurCD\util` для ОС Windows:

1) `./admin_add.sh` — добавляется в систему набор пользователей и групп, необходимых для активации механизма защиты. По умолчанию создает двух пользователей (`admscd` и `usrscd`), включенных в группу `securcd`. Пользователь `admscd` используется для запуска программы управления SecurCD Admin, пользователь `usrscd` — для запуска программы чтения-записи SecurCD Burner.

2) `./admin_protect.sh` — активирует механизм защиты программы управления SecurCD Admin.

3) `./cdsec_protect.sh` — активирует механизм защиты программы чтения-записи SecurCD Burner.

При необходимости добавить новых пользователей в «белый список» на запуск программы чтения-записи SecurCD Burner необходимо применить скрипт `cdsec_user` в формате `./cdsec_user.sh -a *пользователь*`.

Ручная активация механизма защиты выполняется следующим порядком использования скриптов, находящихся в каталоге `/opt/Aladdin/SecurCD/util` для ОС Linux и `C:\Program Files\Aladdin\SecurCD\util` для ОС Windows:

1) `./cdsec_protect.sh -r` — деактивирует механизм защиты программы чтения-записи SecurCD Burner.

2) `./admin_protect.sh -r` — деактивирует механизм защиты программы управления SecurCD Admin.

3) `./admin_del.sh` — удаляет пользователей и группу, созданных под активацию механизма защиты (выполнение скрипта опционально).

Также после скриптов активации/деактивации можно отдельно прописать значение `пользователь:группа`, чтобы активировать или деактивировать механизм защиты для конкретного пользователя в группе.

При необходимости с помощью скрипта `admin_del.sh` можно удалить пользователей и группу SecurCD, созданных с помощью `admin_add.sh`. При этом переменные окружения в данном скрипте указаны без привязки к `admin_add.sh`, т.е. за их совпадением требуется следить вручную.

Активация и деактивация на ОС Windows производятся аналогично (для выполнения скриптов необходимы права администратора системы).

При удалении программы механизм защиты деактивируется, а пользователи и группа под него удаляются.

При переустановке программы поверх уже имеющейся версии механизм защиты «пересоздается», то есть уже имеющиеся пользователи и группа удаляются и создаются новые. Для отмены удаления уже имеющихся пользователей следует использовать переменную окружения `SCD_NO_MENUITEM` при установке (подробнее в п. 8.3).

#### 8.4.1 Параметры активации механизма защиты

Имеется отдельный набор ключей, задающий дополнительные параметры при активации/деактивации механизма защиты:

1) `-p` — используется скриптом `admin_add.sh` для установки пароля при запуске программы управления SecurCD Admin.

2) `-r` “пользователь:группа” — применим к скриптам типа `*_protect.sh`. Деактивирует механизм защиты. При использовании необходимо указывать владельца программы в качестве пользователя (если не указывать, то берутся значения по умолчанию).

3) `-a` “пользователь” — используется скриптом `cdsec_user.sh` для добавления нового пользователя в «белый список» на запуск программы чтения-записи SecurCD Burner.

4) `-d` “пользователь” — используется скриптом `cdsec_user.sh` для удаления пользователя из «белого списка» на запуск программы чтения-записи SecurCD Burner.

5) `-l` — используется скриптом `cdsec_user.sh` для отображения «белого списка» на запуск программы чтения-записи SecurCD Burner.

6) `-swt` — изменяет расширение файла и тип контейнера в переменной окружения `SECURE_STORAGE` (см. следующий пункт). Обязательно использовать вместе с `admin_protect.sh` при активации/деактивации механизма защиты для верного функционирования контейнеров типа `*.swt`.

#### 8.4.2 Переменные окружения механизма защиты

Переменные окружения, связанные с механизмом защиты, отвечают за параметры функционирования и запуска программ после активации механизма защиты. Они указаны в двух скриптах, используемых для активации/деактивации механизма защиты — `admin_protect.sh` и `cdsec_protect.sh`, а также в `admin_add.sh` и `admin_del.sh`.

Переменные окружения, которые содержатся в `cdsec_protect.sh`:

– `CDSEC_OWNER` — владелец программы чтения-записи SecurCD Burner в формате “пользователь:группа” (по умолчанию — `usrscd:securcd`);

– `CDSEC_UTIL` — путь к программе чтения-записи SecurCD Burner;

- CDSEC\_CONFIG — путь к INI-файлу программы чтения-записи SecurCD Burner;
- CDSEC\_RUN — путь к скрипту запуска программы чтения-записи SecurCD Burner;

Переменные окружения, которые содержатся в `admin_protect.sh`:

- ADMIN\_OWNER — владелец программы управления SecurCD Admin в формате "пользователь: группа" (по умолчанию — `admscd:securcd`);
- ADMIN\_UTIL — путь к программе управления SecurCD Admin;
- ADMIN\_CONFIG — путь к INI-файлу программы управления SecurCD Admin;
- CDSEC\_UTIL — путь к программе чтения-записи SecurCD Burner;
- CDSEC\_CONFIG — путь к INI-файлу программы чтения-записи SecurCD Burner;
- OPEN\_STORAGE — файл базы данных SQLite для хранения атрибутов безопасности получателя (по умолчанию — `keys.db`);
- SECURE\_STORAGE — файл контейнера для хранения атрибутов безопасности отправителя (по умолчанию — `keys.cnt`);
- EVENT\_LOG — файл базы данных SQLite журнала событий программного средства (по умолчанию — `events.db`).

Переменные окружения, которые содержатся в `admin_add.sh` и `admin_del.sh`:

- SCD\_USER — пользователь, от лица которого запускается программа чтения-записи SecurCD Burner (по умолчанию — `usrscd`);
- SCD\_ADMIN — пользователь, используемый для запуска программы управления SecurCD Admin (по умолчанию — `admscd`);
- SCD\_GROUP — первичная группа в которую входят пользователи `SECURECD_USER` и `SECURECD_ADMIN`.

## 8.5 Изменение шрифтов

Также в программном средстве реализована функция изменения шрифтов. Для изменения шрифта внутри программы управления SecurCD Admin или программы чтения-записи SecurCD Burner требуется изменить две строки в секции `common` файла `util-admin.ini` или `util-cdsec.ini`:

- `font_family` — название семейства шрифтов (к примеру, `Courier new`).
- `font_style` — стиль отображения шрифта. Используется для поиска подходящего семейства шрифтов, если выбранное семейство шрифтов недоступно.

Возможные значения для `font_style`:

- 5 — Использовать алгоритм сопоставления шрифтов (по умолчанию);

- 0 — Предпочитать Sans Serif при выборе шрифтов;
- 1 — Предпочитать Serif при выборе шрифтов;
- 2 — Предпочитать Courier при выборе шрифтов;
- 7 — Предпочитать CSS Monospace при выборе шрифтов;
- 8 — Предпочитать CSS Fantasy при выборе шрифтов;
- 6 — Предпочитать CSS Cursive при выборе шрифтов;
- 4 — Предпочитать системные шрифты.

Для изменения масштабирования окон программ для лучшего отображения на различных разрешениях экрана, следует изменить базовое значение параметра `scale_percent` в секции `common` файла `util-admin.ini` или `util-cdsec.ini`.

## 9 ОБРАЩЕНИЕ В СЛУЖБУ ТЕХНИЧЕСКОЙ ПОДДЕРЖКИ

Время работы службы технической поддержки изготовителя с 09:00 до 18:00 по московскому времени (GMT+3), кроме выходных и праздничных дней.

Запросы на техническую поддержку оформляются в виде электронного документа через Web-сайт изготовителя (производителя) или по электронной почте.

Контактные данные службы технической поддержки изготовителя (производителя):

- URL-адрес для обращений: <https://www.aladdin-rd.ru/support/tickets/create>;
- телефон: +7 (499) 702-39-68;
- адрес электронной почты: [support.sf@aladdin.ru](mailto:support.sf@aladdin.ru).

Техническая поддержка программного средства «Средство обмена данными на оптических дисках» оказывается в течение гарантийного срока.

Для всех случаев обращения в службу технической поддержки должен быть указан идентификатор сертифицированного средства (номер программного средства предприятия), при этом обращение обязательно регистрируется в службе технической поддержки.

Техническая поддержка изделия в течение гарантийного срока включает:

- возможность консультаций по настройке, а также особенностям эксплуатации и применения программного средства;
- возможность моделирования неисправного (неработоспособного) состояния программы на стенде изготовителя (производителя) и помощь в решении возникшей проблемы/затруднения при работе с программой;
- исправление программных дефектов, обнаруженных в программе владельцем (пользователем) программного средства или производителем (изготовителем) и не относящихся к недостаткам безопасности;
- обновление программного средства для устранения программных дефектов, не относящихся к недостаткам безопасности.

