



SoftControl

SysContainer 6.0.55

Руководство администратора

Уважаемый пользователь!

ООО «АРУДИТ СЕКЬЮРИТИ» благодарит Вас за то, что выбрали продукт SoftControl SysContainer. Специалисты компании постарались, чтобы наше программное обеспечение отвечало самым высоким требованиям в области защиты информации и в то же время было простым и удобным в работе. Мы надеемся, что SoftControl SysContainer будет Вам полезен.

АВТОРСКИЕ ПРАВА

Материалы, приведенные в настоящем документе, являются собственностью ООО «АРУДИТ СЕКЬЮРИТИ» и могут быть использованы только для личных целей приобретателя продукта. Запрещается воспроизведение отдельных частей документа, внесение правок, размещение на сетевых ресурсах, распространение в любой форме (в том числе в переводе) на бумажных и электронных носителях, посредством каналов связи и средств массовой информации или каким-либо другим способом без специального письменного разрешения компании и ссылки на источник. Наименования и товарные знаки, приведённые в документе, являются собственностью своих законных владельцев.

ОГРАНИЧЕНИЕ ОТВЕТСТВЕННОСТИ

Содержание данного документа может изменяться без предварительного уведомления. ООО «АРУДИТ СЕКЬЮРИТИ» не несёт ответственности за неточности и/или ошибки, допущенные в данном документе, и возможный ущерб, связанный с этим.

ООО «АРУДИТ СЕКЬЮРИТИ», 2021 г.

Почтовый адрес:

127106, Россия, Москва

Нововладыкинский проезд, дом 8, стр. 3

ООО «АРУДИТ СЕКЬЮРИТИ»

Телефон:

+7 (499) 201-55-12

Электронная почта:

Общие вопросы и предложения: support@sns-control.ru

Коммерческие вопросы: sales@sns-control.ru

Веб-сайт компании: <http://www.sns-control.ru>

Содержание

| | |
|--|----|
| 1. Введение | 4 |
| 1.1 Назначение | 4 |
| 1.2 Условные обозначения и термины | 5 |
| 1.2.1 Обозначения | 5 |
| 2. Требования к аппаратному и программному обеспечению | 6 |
| 2.1 Системные требования SoftControl SysContainer | 6 |
| 3. Установка SoftControl SysContainer | 7 |
| 3.1 Установка в обычном режиме | 7 |
| 3.2 Установка в тихом режиме | 9 |
| 4. Работа с SoftControl SysContainer | 11 |
| 4.1 Помещение содержимого диска в контейнер | 12 |
| 4.2 Изменение подключённых аппаратных устройств | 20 |
| 4.3 Извлечение содержимого диска из контейнера | 21 |
| 4.4 Смена пароля | 24 |
| 4.5 Обновление списка устройств | 25 |
| 4.6 Запуск из командной строки | 26 |
| 4.7 Журналы | 29 |
| 4.8 Список игнорируемых устройств и отложенный запуск | 30 |
| 4.9 Генерация блоков данных в контейнере | 31 |
| 4.10 Истечение лицензии | 32 |
| 5. Обновление SoftControl SysContainer | 34 |
| 5.1 Обновление в обычном режиме | 34 |
| 5.2 Обновление в тихом режиме | 38 |
| 6. Удаление SoftControl SysContainer | 39 |
| 6.1 Удаление в обычном режиме | 39 |
| 6.2 Удаление в тихом режиме | 40 |
| 7. Техническая поддержка | 41 |
| 8. Приложение | 42 |
| 8.1 Настройка раздела диска | 42 |

1. Введение

1.1 Назначение

Инструмент SoftControl SysContainer предназначен для сокрытия содержимого системного диска компьютера в контейнере, доступ к которому прекращается, если сменилось аппаратное обеспечение компьютера. SoftControl SysContainer помогает защититься от атак, проводимых по следующим сценариям:

1. Злоумышленник похищает жесткий диск компьютера. Злоумышленник анализирует содержимое диска в лаборатории, находит уязвимости в ПО и впоследствии проводит атаку на устройства самообслуживания (банкоматы, терминалы).
2. Злоумышленник обходит защиту BIOS, загружает компьютер с внешнего носителя и анализирует содержимое жесткого диска.

При запуске процесса помещения данных в контейнер SoftControl SysContainer считывает параметры всех устройств, подключенных к компьютеру. Если при последующих запусках компьютера критических изменений в конфигурации не было обнаружено, загрузка ОС происходит на основе параметров устройств. Критическим изменением считается удаление или замена трех и более устройств. Допустима замена меньшего количества устройств*⁴.

Если имело место критическое изменение конфигурации компьютера, для загрузки ОС у пользователя запрашивается пароль, указанный им при помещении содержимого диска в контейнер.

SoftControl SysContainer является клиентским компонентом и способен работать как автономно, так и в совокупности с SoftControl Service Center. Для работы с SoftControl Service Center на компьютере с SoftControl SysContainer также должен быть установлен клиентский компонент SoftControl SysWatch, с помощью которого на SoftControl Server передаются события SoftControl SysContainer. Документ «Service Center. Руководство администратора» подробно описывает систему SoftControl Service Center.

* Формирование ключа из подмножества устройств является криптографически надежным благодаря использованию [схемы разделения секрета Шамира](#).

SoftControl SysContainer можно применять для системных дисков компьютеров, функционирующих под управлением ОС семейства Microsoft® Windows®.

Данный продукт разработан с использованием исходных кодов VeraCrypt, лицензированных при помощи VeraCrypt License, объединяющей Apache License 2.0 и TrueCrypt License 3.0. Копия лицензии находится в папке с установленным приложением в файле *VCLicense.txt*.

1.2 Условные обозначения и термины

1.2.1 Обозначения

Условные обозначения, применяемые в данном документе, приведены в табл. 1.

Таблица 1. Условные обозначения

| Пример обозначения | Описание |
|---|--|
|  | Важная информация. |
| <u>Условие</u> | Условие выполнения, примечание, пример. |
| Обновить | – заголовки и сокращения; – названия экранных кнопок, ссылок, пунктов меню, других элементов программного интерфейса. |
| <i>Политика контроля</i> | – термины (определения); – имена файлов и других объектов; – тексты сообщений, выводимых пользователю. |
| C:\Program Files\SoftControl | Пути к файлам, каталогам, ключам системного реестра. |
| %windir%\system32 \msiexec.exe /i | Фрагменты программного кода, командных и конфигурационных файлов. |
| <каталог установки SoftControl SysContainer> | Поля для замены функциональных названий фактическими значениями. |
| Приложение ⁽⁵⁾ | Ссылки на внутренние ресурсы (разделы документа) с указанием номера страницы или на внешние ресурсы (URL-адреса). |

2. Требования к аппаратному и программному обеспечению

2.1 Системные требования SoftControl SysContainer

Таблица 2. Минимальные системные требования

| ОС | Частота ЦП | Объем ОЗУ | Объем свободного пространства на жестком диске |
|--|------------|-----------|---|
| Клиентские операционные системы: | | | |
| Microsoft® Windows® 7 (SP1) 64-разрядная ¹ | 1 ГГц | 2 ГБ | 100 МБ + дополнительно 10 МБ на UEFI-разделе |
| Microsoft® Windows® 8 32-разрядная | 1 ГГц | 1 ГБ | |
| Microsoft® Windows® 8 64-разрядная | 1 ГГц | 2 ГБ | |
| Microsoft® Windows® 8.1 32-разрядная | 1 ГГц | 1 ГБ | |
| Microsoft® Windows® 8.1 64-разрядная | 1 ГГц | 2 ГБ | |
| Microsoft® Windows® 10 32-разрядная | 1 ГГц | 1 ГБ | |
| Microsoft® Windows® 10 64-разрядная | 1 ГГц | 2 ГБ | |
| Microsoft® Windows® 10 IoT Enterprise 32-разрядная | 1 ГГц | 1 ГБ | |
| Microsoft® Windows® 10 IoT Enterprise 64-разрядная | 1 ГГц | 2 ГБ | |
| Серверные операционные системы: | | | |
| Microsoft® Windows® Server 2008 R2 64-разрядная ^{1,2} | 1,4 ГГц | 512 МБ | |
| Microsoft® Windows® Server 2012 64-разрядная ² | 1,4 ГГц | 512 МБ | |
| Microsoft® Windows® Server 2012 R2 64-разрядная ² | 1,4 ГГц | 512 МБ | |
| Microsoft® Windows® Server 2016 64-разрядная ² | 1,4 ГГц | 512 МБ | |

Примечания:

1. Требуется обновление KB3033929 (поддержка алгоритма хэширования SHA-256 при проверке цифровой подписи) или любое его замещающее.
2. Поддерживаются только варианты установки ОС с рабочим столом.

Дополнительные требования:

- Тип BIOS должен быть UEFI. Также рекомендуется отключить опцию SecureBoot.
- Системный диск должен быть разбит в формате GPT (GUID Partition Table). В начале диска необходимо наличие нераспределенного пространства размером не менее 32 КБ.

3. Установка SoftControl SysContainer

Возможны следующие варианты установки SoftControl SysContainer:

- [в обычном режиме \(с использованием интерфейса пользователя\)](#) ⁷;
- [в тихом режиме](#) ⁹.

3.1 Установка в обычном режиме

- 1) Запустите установочный пакет *SoftControl SysContainer Setup.exe*.
- 2) В случае вашего согласия, выберите параметр **I accept the license terms** (Я принимаю условия лицензионного соглашения) и нажмите **Next** (рис. [Лицензионное соглашение](#) ⁷).

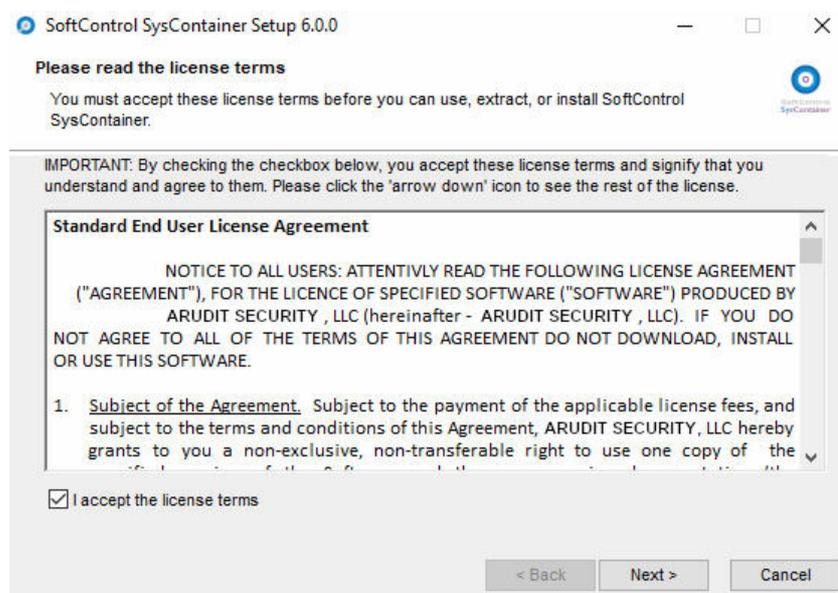


Рисунок 1. Лицензионное соглашение

- 3) Выберите требуемую опцию в окне **Wizard Mode** и нажмите **Next** (рис. [Выбор варианта установки](#) ⁸).

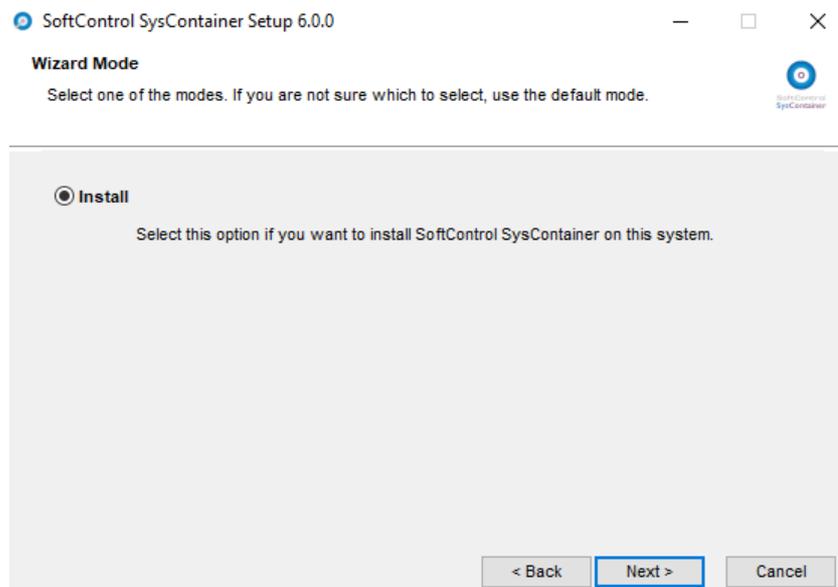


Рисунок 2. Выбор варианта установки

4) С помощью кнопки **Browse** выберите каталог для установки SoftControl SysContainer и нажмите **Install** (рис. [Путь установки](#)⁸).

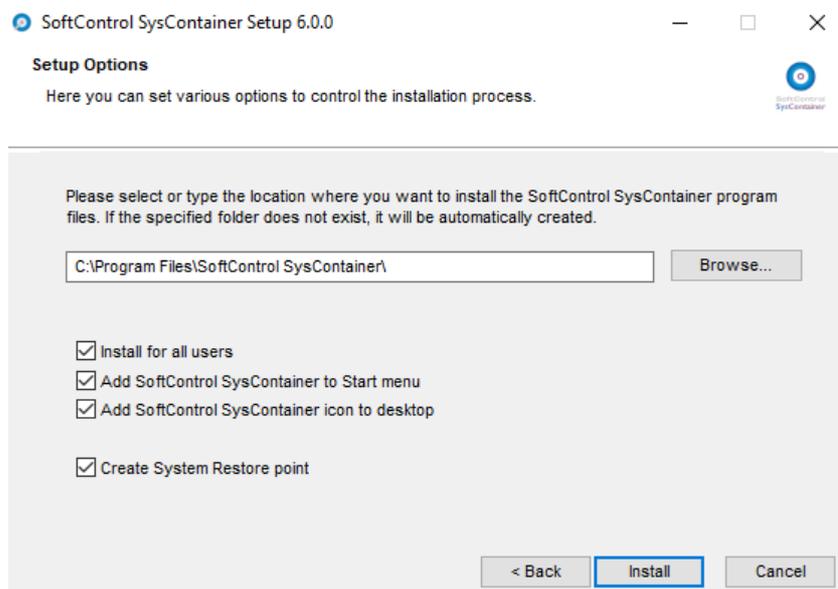


Рисунок 3. Путь установки

5) Дождитесь окончания процесса установки (рис. [Процесс установки](#)⁹).

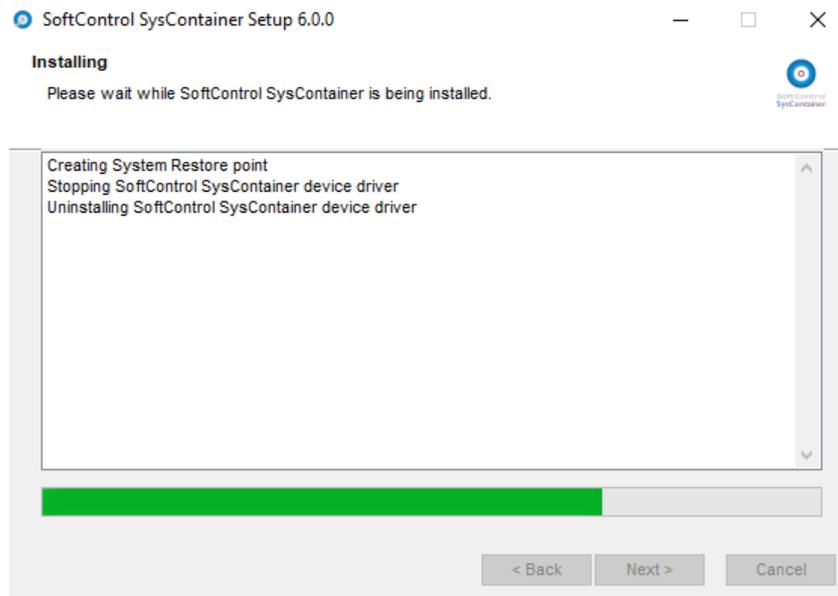


Рисунок 4. Процесс установки

6) После появления сообщения **Установка SoftControl SysContainer завершена** нажмите **Finish** (рис. [Завершение установки](#)⁹).

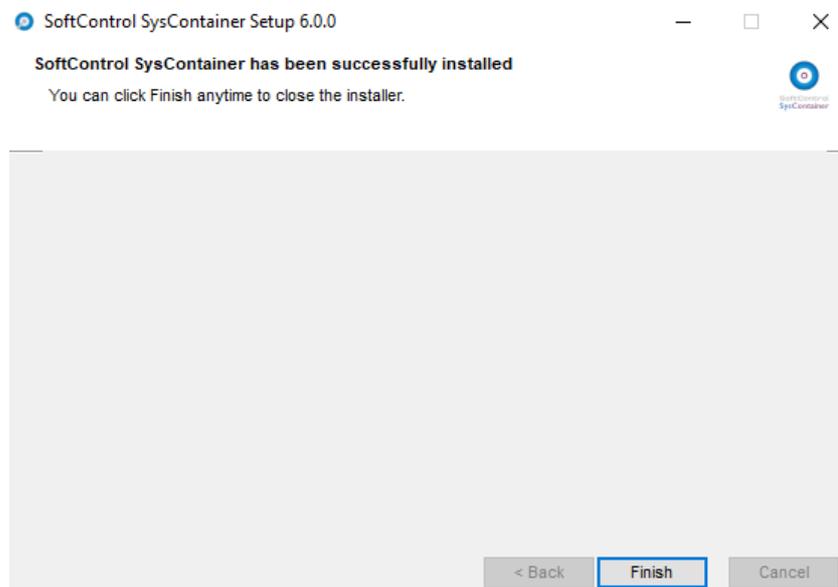


Рисунок 5. Завершение установки

3.2 Установка в тихом режиме

Условие: все шаги выполняются под учетной записью с правами администратора.

1) Скопируйте установочный пакет *SoftControl SysContainer Setup.exe* в какой-либо каталог клиентского хоста.

2) Запустите командную строку Windows и выполните следующую команду:

```
"<каталог с установочным пакетом>\SoftControl SysContainer Setup.exe" /q [/folder  
"<каталог для установки>"]
```

Если необязательный параметр `/folder` не используется, SoftControl SysContainer будет установлен в папку `C:\Program Files\SoftControl SysContainer`.

4. Работа с SoftControl SysContainer

В данном разделе приведены инструкции по работе с основными функциями SoftControl SysContainer.

Условие: все действия выполняются под учетной записью с правами администратора.

Внешний вид программы показан на рис. [Элементы интерфейса программы](#)¹¹.

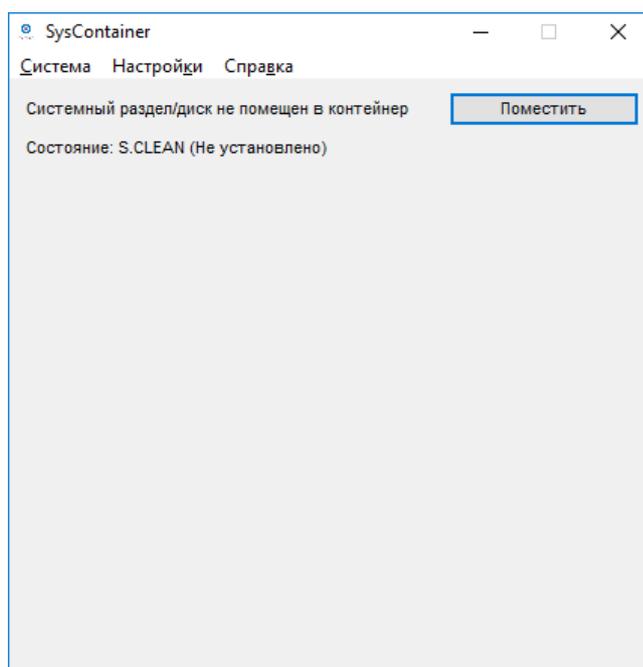


Рисунок 6. Элементы интерфейса программы

Команды меню описаны в табл. 3.

Таблица 3. Описание команд меню SoftControl SysContainer

| Команда меню | Действие |
|---|--|
| Поместить содержимое системного раздела/диска в контейнер | Запуск процесса помещения содержимого системного раздела или диска в контейнер. |
| Извлечь содержимое системного раздела/диска из контейнера | Запуск процесса извлечения содержимого системного раздела или диска из контейнера. |
| Возобновить прерванный процесс | Возобновление остановленного процесса помещения в контейнер или извлечения из контейнера. |
| Удалить загрузчик | Удаление загрузчика системы помещения данных в контейнер/извлечения данных из контейнера без удаления SoftControl SysContainer (требуется перезагрузка клиентского хоста). |
| Изменить пароль | Смена пароля, используемого для загрузки системы в случае критического изменения набора аппаратных устройств. |
| Обновить список устройств | Добавление новых аппаратных устройств в список. |

| Команда меню | Действие |
|--------------------------|-------------------------|
| Язык (language) | Смена языка интерфейса. |
| Руководство пользователя | Вызов справки. |

Состояния системы перечислены в табл. 4.

Таблица 4. Состояния SoftControl SysContainer

| Состояние | Описание |
|-------------------------------------|---|
| S.CLEAN (Не установлено) | Система SoftControl SysContainer установлена на клиентском хосте, но диск не содержит загрузчик системы помещения в контейнер/извлечения из контейнера. |
| S.INST (Установлено) | Загрузчик системы помещения в контейнер/извлечения из контейнера установлен, но еще не запускался (перезагрузка клиентского хоста не была выполнена). |
| S.MNT (Загружено) | Загрузчик системы помещения в контейнер/извлечения из контейнера установлен, клиентский хост был перезагружен, но операции по помещению содержимого диска в контейнер еще не выполнялись. |
| S.PART_ENC (Частично закодировано) | Выполняется помещение в контейнер или извлечение из контейнера содержимого системного диска. |
| S.FULL_ENC (Полностью закодировано) | Содержимое системного диска помещено в контейнер. |

4.1 Помещение содержимого диска в контейнер

В основном окне SoftControl SysContainer нажмите **Поместить** (рис. [Элементы интерфейса программы](#)⁽¹¹⁾).

В появившемся окне в выпадающих списках выберите **Алгоритм помещения в контейнер** и **Алгоритм хэширования** и нажмите **Далее** (рис. [Настройки помещения данных в контейнер](#)⁽¹³⁾). Хэширование используется для формирования ключей из пароля и других данных, а также для генерации случайных чисел.

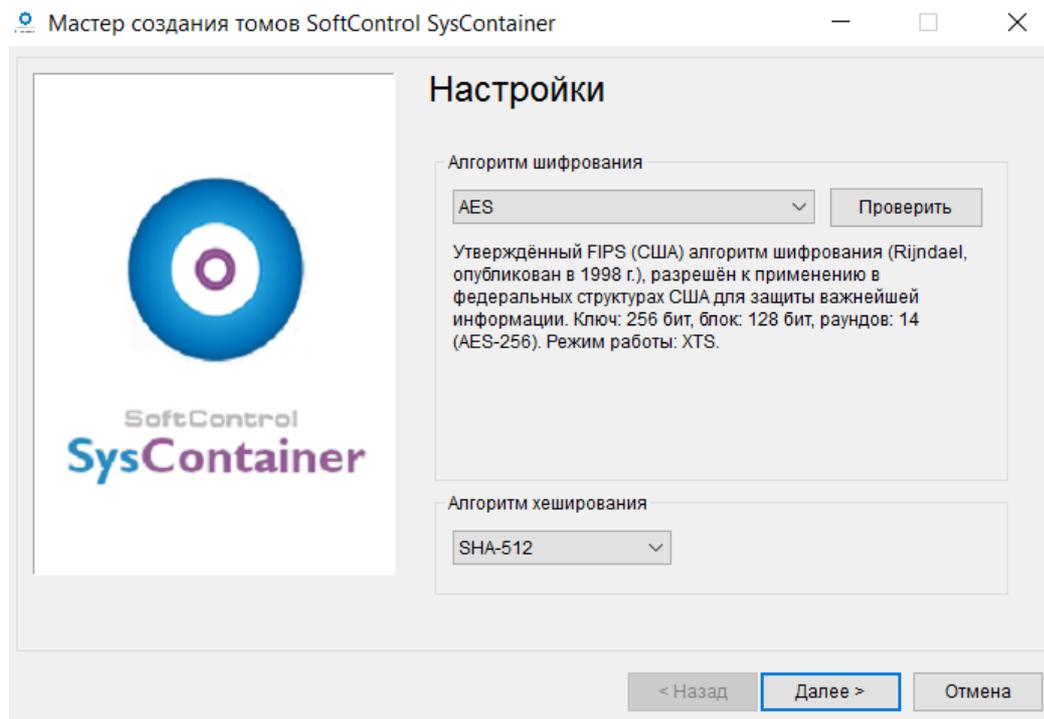


Рисунок 7. Настройки помещения данных в контейнер

Задайте **Пароль** и его подтверждение (рис. [Задание пароля](#)¹³).

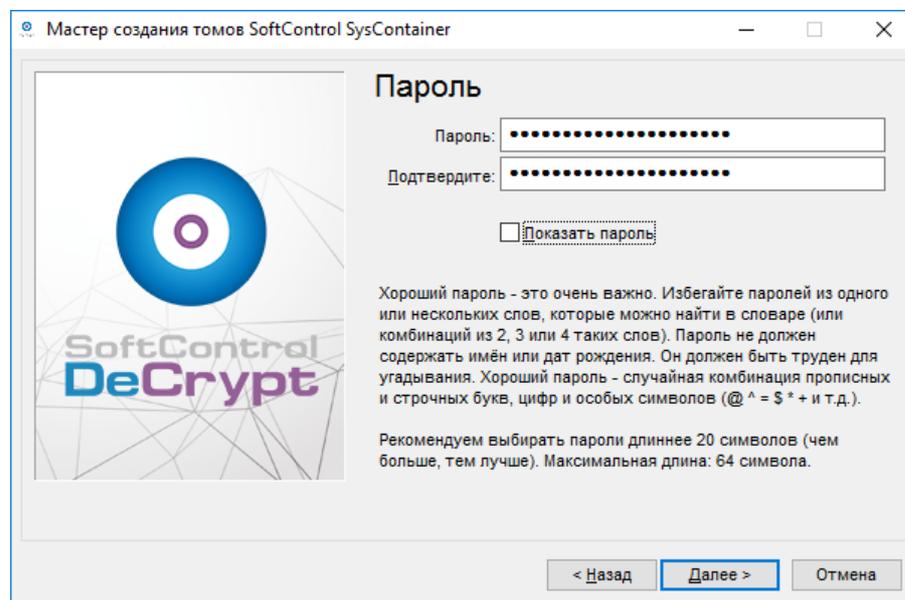


Рисунок 8. Задание пароля

В следующем окне происходит сбор случайных данных из движений мыши. Перемещайте указатель внутри окна. Рекомендуется делать это до тех пор, пока цвет индикатора выполнения не станет зеленым. Затем нажмите **Далее** (рис. [Сбор случайных данных](#)¹⁴).

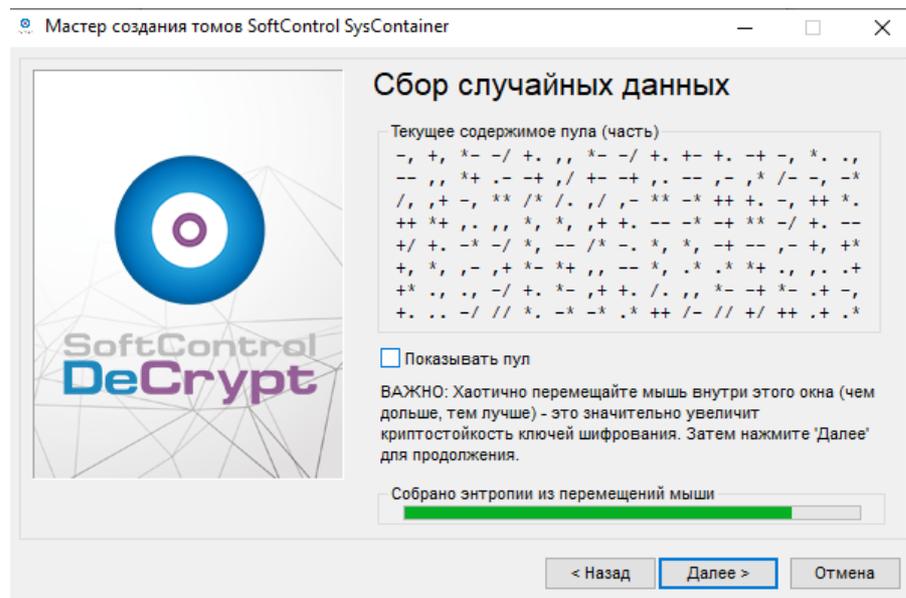


Рисунок 9. Сбор случайных данных

Для просмотра ключей в следующем окне (рис. [Сгенерированные ключи](#)⁽¹⁴⁾) выставите флажок **Показ созданных ключей (их частей)**.

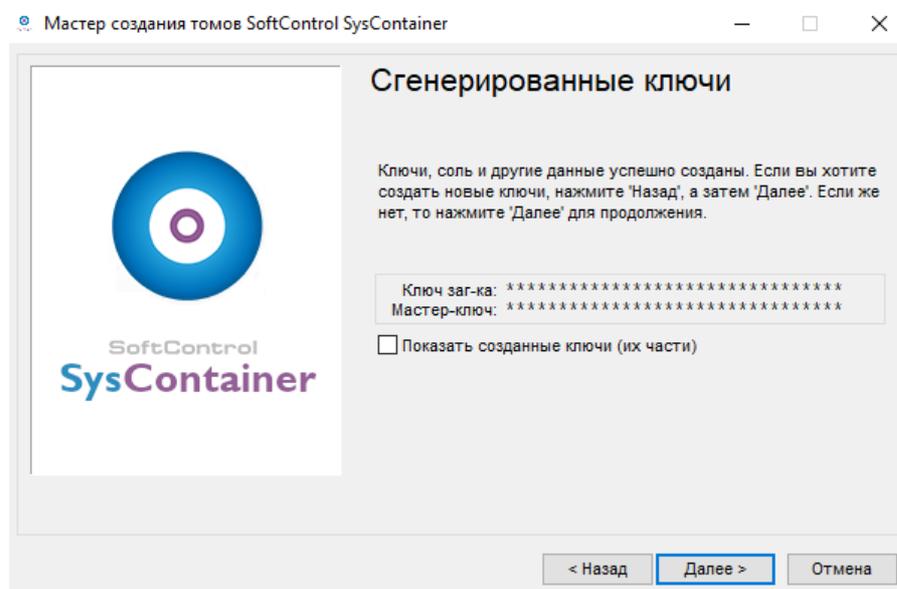


Рисунок 10. Сгенерированные ключи

Выберите **Режим очистки** в выпадающем списке (рис. [Выбор режима очистки](#)⁽¹⁵⁾).

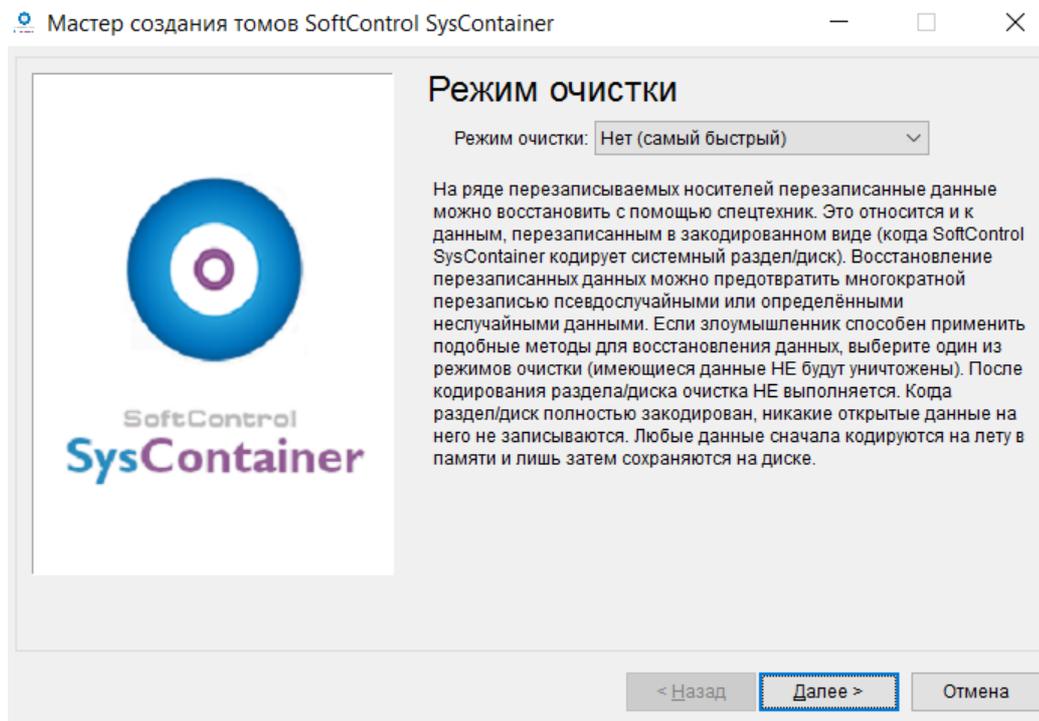


Рисунок 11. Выбор режима очистки

i Включение режима очистки значительно увеличивает время помещения содержимого системного раздела/диска в контейнер.

После нажатия на кнопку **Далее** в окне **Режим очистки** (см. [выше](#)⁽¹⁵⁾) SoftControl SysContainer предлагает провести предварительный тест, цель которого – убедиться, что система подготовлена к помещению данных в контейнер. Во время предварительного теста устанавливается загрузчик SoftControl SysContainer (рис. [Запуск предварительного теста](#)⁽¹⁶⁾).

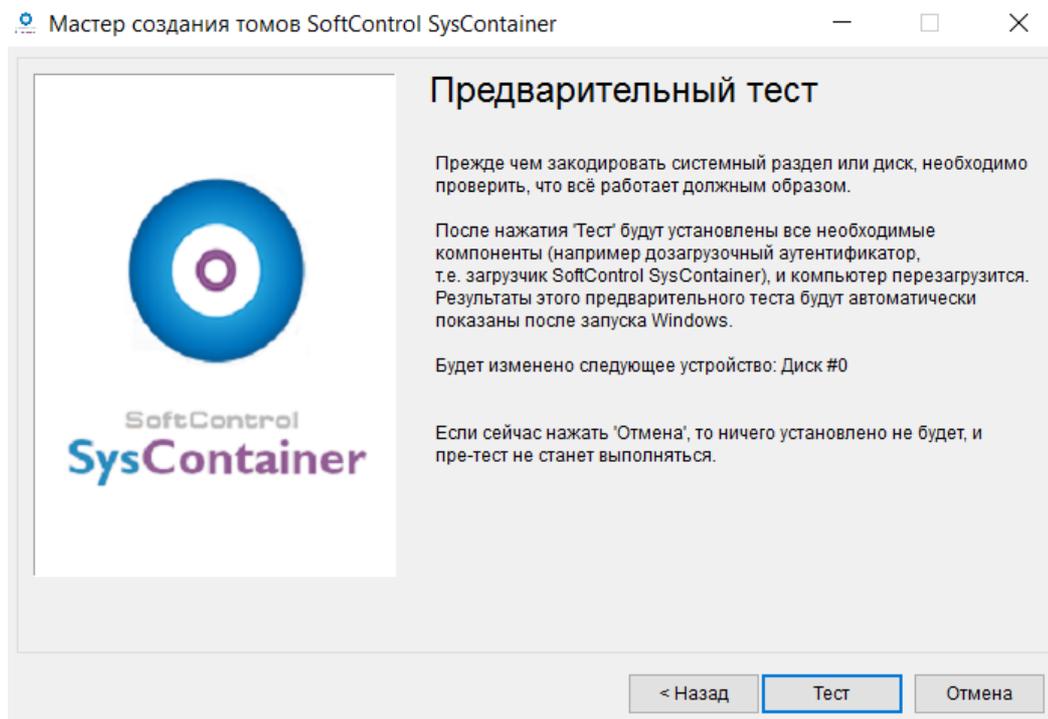


Рисунок 12. Запуск предварительного теста

i Все сообщения, выдаваемые во время предварительного теста, отображаются только на английском языке.

В диалоговом окне с предложением выключить клиентский хост нажмите **Да**. Для проведения предварительного теста вам потребуется включить компьютер вручную (рис. [Выключение системы](#)⁽¹⁶⁾).

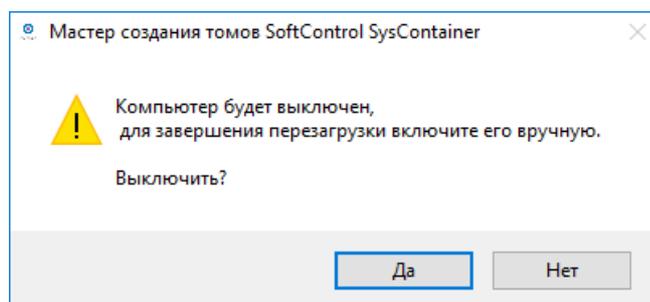


Рисунок 13. Выключение системы

После включения клиентского хоста SoftControl SysContainer выдаст сообщение о [возобновлении помещения содержимого диска в контейнер](#)⁽¹⁷⁾ (в случае входа в систему под той же учетной записью, под которой был запущен процесс помещения в контейнер), а затем сообщение о завершении предварительного теста (рис. [Завершение предварительного теста](#)⁽¹⁷⁾).

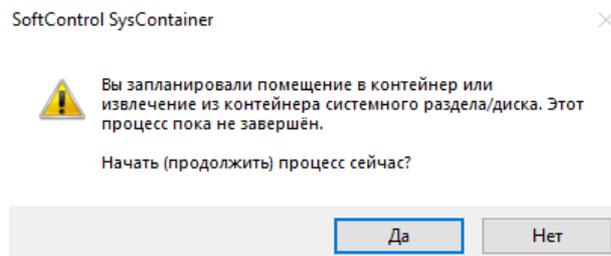


Рисунок 14. Возобновление помещения содержимого диска в контейнер

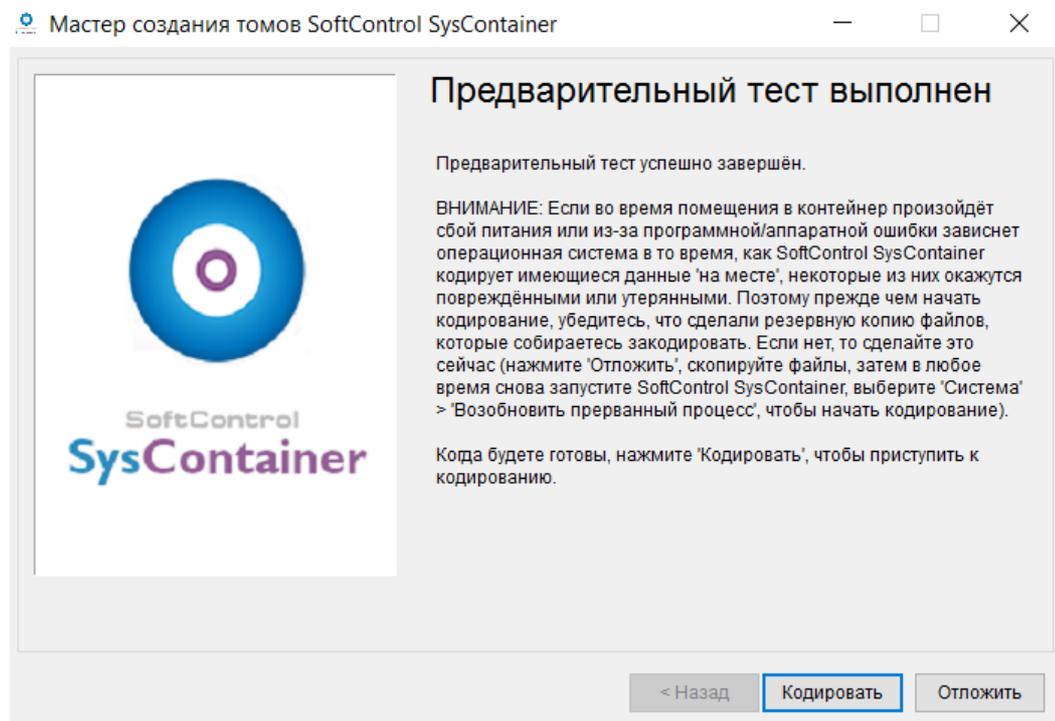


Рисунок 15. Завершение предварительного теста

Нажмите **Кодировать** для запуска помещения содержимого системного раздела/диска в контейнер. Окно **Кодирование** содержит индикатор выполнения и примерное время до окончания процесса (рис. [Процесс помещения данных в контейнер](#)¹⁸).

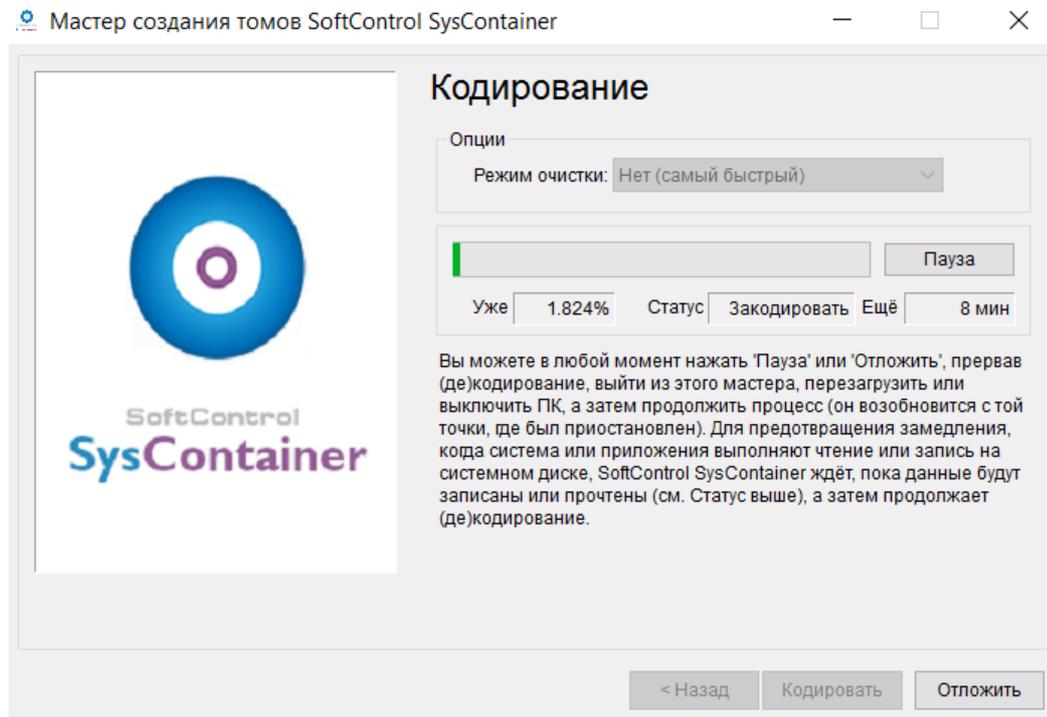


Рисунок 16. Процесс помещения данных в контейнер

При необходимости вы можете прервать процесс помещения в контейнер, нажав на кнопку **Пауза**, а затем запустить его снова, нажав **Возобновить**.

Чтобы запустить процесс помещения данных в контейнер в другое время, нажмите **Отложить**. Для возобновления выберите команду **Возобновить прерванный процесс** в основном окне SoftControl SysContainer (табл. [Описание команд меню SoftControl SysContainer](#)⁽¹¹⁾).



Отменить процесс помещения данных в контейнер невозможно.

Примечание. Сообщение о возобновлении процесса помещения данных в контейнер (см. рис. [выше](#)⁽¹⁷⁾) также будет показано, если данный процесс был отложен, а клиентский хост перезагружен (в случае входа в систему под той же учетной записью, под которой был запущен процесс помещения в контейнер).

В появившемся после завершения помещения данных в контейнер окне нажмите **ОК**, а затем **Готово** в окне Мастера создания томов (рис. [Содержимое системного раздела/диска помещено в контейнер](#)⁽¹⁹⁾).

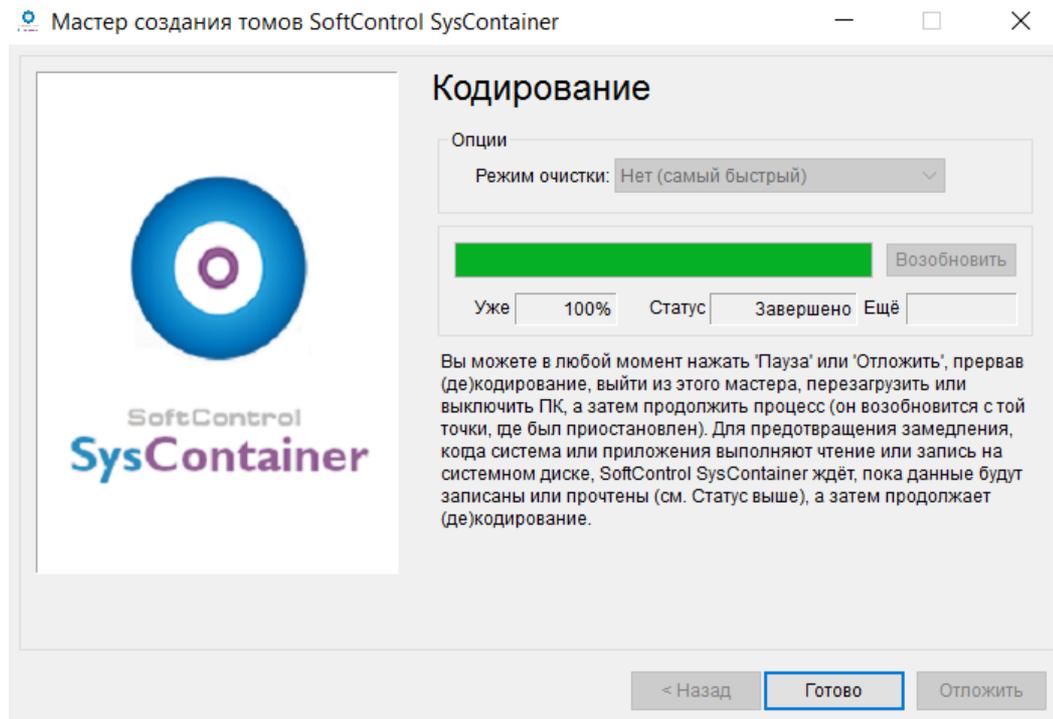


Рисунок 17. Содержимое системного раздела/диска помещено в контейнер

При следующем запуске SoftControl SysContainer в основном окне программы отображается информация о параметрах помещения данных в контейнер (рис. [Параметры помещения данных в контейнер](#)⁽²⁰⁾).

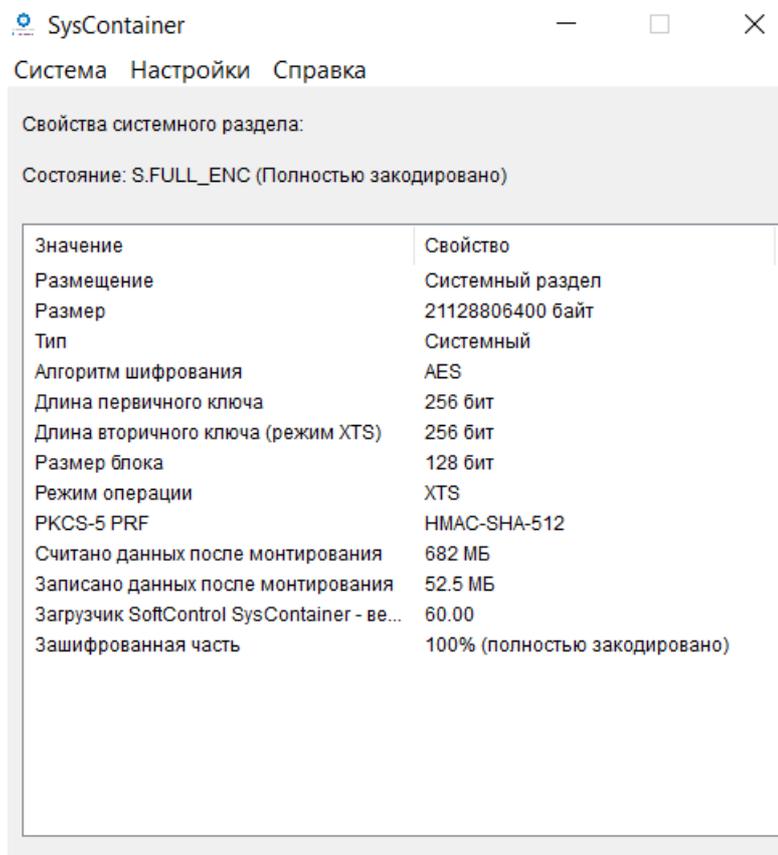


Рисунок 18. Параметры помещения данных в контейнер

4.2 Изменение подключённых аппаратных устройств

Система SoftControl SysContainer при запуске помещения данных в контейнер считывает параметры следующих аппаратных устройств:

- MAC-адреса сетевых карт;
- VID, PID и серийные номера USB-накопителей;
- BIOS (информация о процессоре на материнской плате).

Минимальное число устройств, поддерживаемых SoftControl SysContainer, – 2 (на клиентском хосте должны иметься сетевые карты или должны быть подключены USB-накопители). Список устройств, параметры которых считывались, выводится в журнал событий.

При изменении (удалении) одного устройства запуск диска разрешается. В лог выводится соответствующее сообщение. При изменении (удалении) любых двух устройств из набора запуск диска также разрешается; в лог выводится сообщение о критическом изменении набора аппаратных устройств.

Если было изменено (удалено) более двух устройств, при загрузке клиентского хоста

пользователю необходимо будет ввести пароль, заданный при помещении данных в контейнер (рис. [Запрос пароля при загрузке клиентского хоста](#)⁽²¹⁾).

```
PlatformInfo create Unsupported
00:0C:29:3A:51:95
DcsInt: Got 4 USB handles
DCApplyBinding: enter
DecryptBlob: good magic - 4B534344
DecryptMaster: decrypted 6 shares
DecryptMaster: recoveredShares = 6, recoveredKey[0..3] = 8B DC 1C E0
DecryptMaster: MasterBlob was not decrypted correctly
DCApplyBinding: leave
DcsInt: after ApplyBinding
Enter Password: _
```

Рисунок 19. Запрос пароля при загрузке клиентского хоста

i При запуске помещения содержимого диска в контейнер SoftControl SysContainer считывает параметры тех устройств, которые были обнаружены в момент загрузки клиентского хоста. Если после завершения помещения данных в контейнер было отключено критическое количество устройств, работа клиентского хоста не будет прервана. Однако при его перезагрузке SoftControl SysContainer запросит пароль для загрузки системного диска.

4.3 Извлечение содержимого диска из контейнера

В основном окне программы выберите команду **Извлечь содержимое системного раздела/диска из контейнера** в меню **Система** (табл. [Описание команд меню SoftControl SysContainer](#)⁽¹¹⁾). В окне предупреждения выберите **Да** (рис. [Подтверждение извлечения данных из контейнера](#)⁽²²⁾) и дождитесь окончания процесса (рис. [Содержимое диска извлечено из контейнера](#)⁽²³⁾).

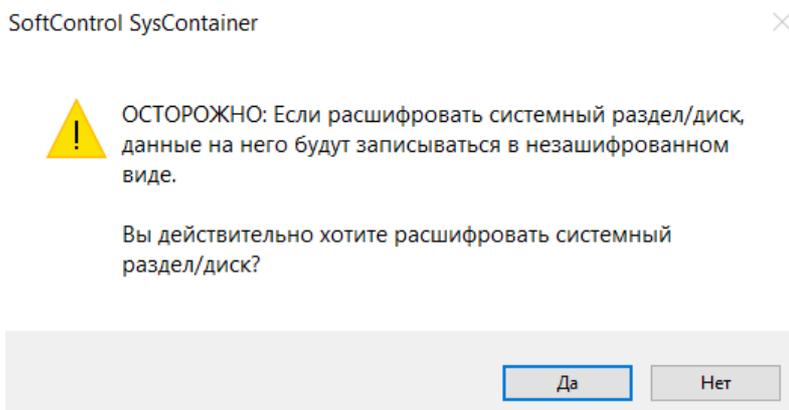


Рисунок 20. Подтверждение извлечения содержимого диска из контейнера

Как и в случае с помещением данных в контейнер (см. раздел [Помещение содержимого диска в контейнер](#)⁽¹⁸⁾), вы можете приостановить или отложить этот процесс, нажав **Пауза** или **Отложить** (рис. [Извлечение содержимого диска из контейнера](#)⁽²²⁾).

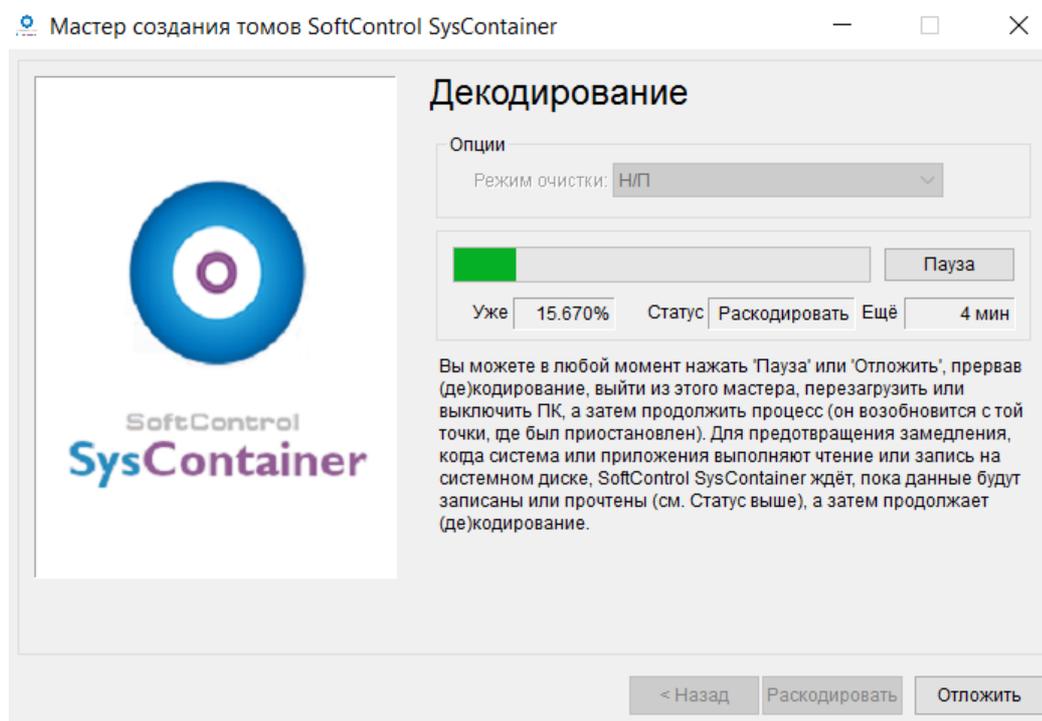


Рисунок 21. Извлечение содержимого диска из контейнера

i Отменить процесс извлечения содержимого диска из контейнера невозможно.

Примечание. Если процесс извлечения данных из контейнера был отложен, а клиентский хост выключен или перезагружен, то после включения клиентского хоста SoftControl SysContainer выдаст следующее сообщение (рис. [Возобновление извлечения](#)

[содержимого диска из контейнера](#)⁽²³⁾) (в случае входа в систему под той же учетной записью, под которой был запущен процесс извлечения содержимого диска из контейнера).

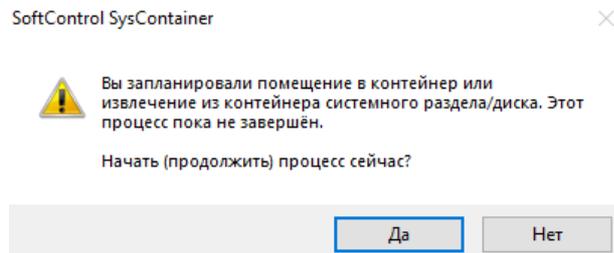


Рисунок 22. Возобновление извлечения содержимого диска из контейнера

В появившемся окне (рис. [Содержимое диска извлечено из контейнера](#)⁽²³⁾) нажмите **ОК**.

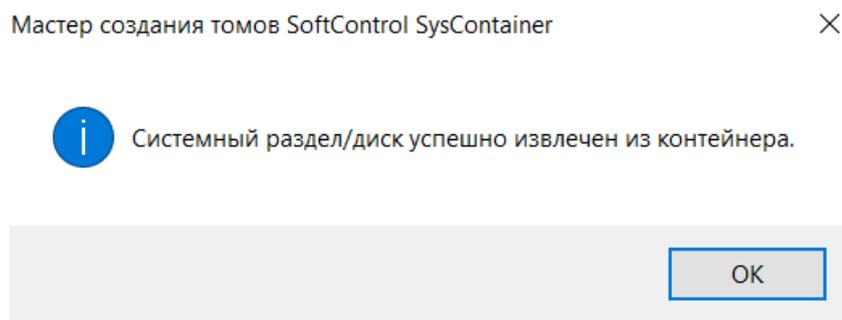


Рисунок 23. Содержимое диска извлечено из контейнера

В диалоговом окне с предложением перезапуска клиентского хоста выберите **Да**, после чего система будет отправлена на перезагрузку для завершения процесса.

4.4 Смена пароля

Для смены пароля, заданного при запуске помещения данных в контейнер, выберите команду **Изменить пароль...** в меню **Система** (рис. [Смена пароля](#)⁽²⁴⁾).

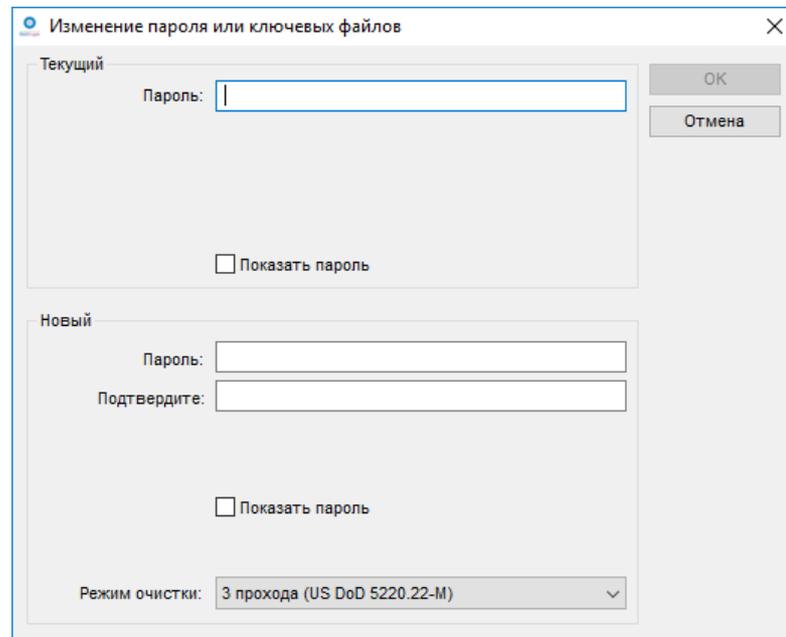


Рисунок 24. Смена пароля

Введите текущий пароль, новый пароль и его подтверждение и нажмите **ОК**. В окне **Обогащение случайного пула** перемещайте мышь для сбора случайных данных, аналогично действиям при генерации ключей для помещения данных в контейнер (рис. [Сбор случайных данных для смены пароля](#)⁽²⁵⁾).

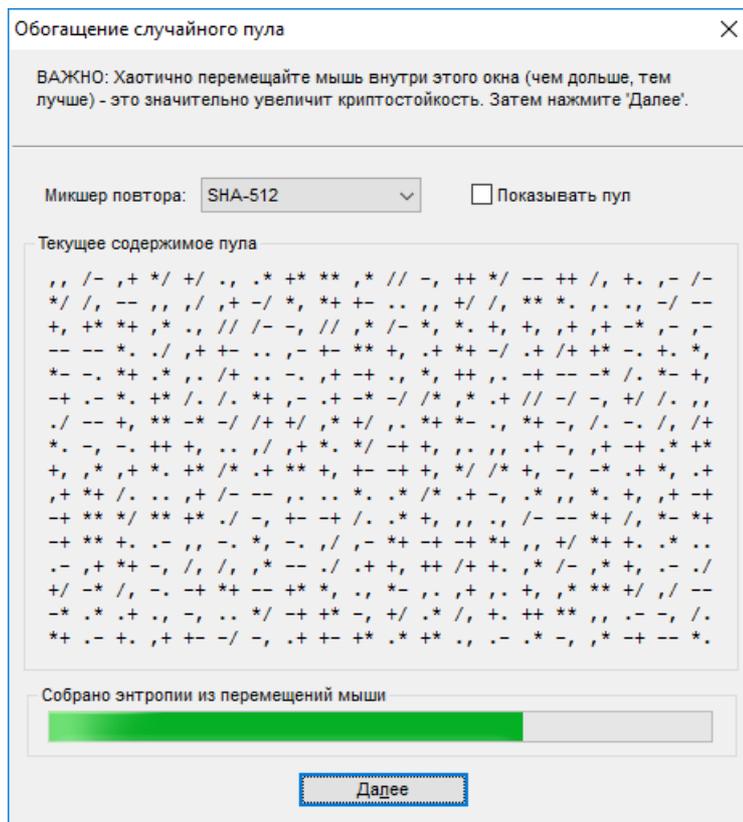


Рисунок 25. Сбор случайных данных для смены пароля

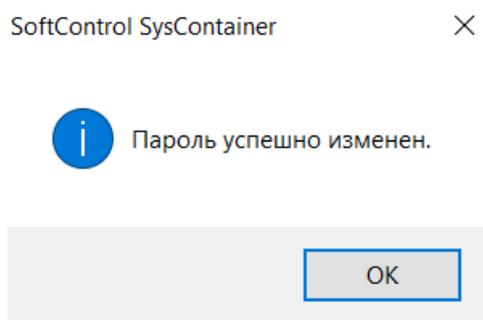


Рисунок 26. Пароль изменен

После завершения процесса нажмите **Далее** (см. [выше](#)²⁵) и **ОК** (рис. [Пароль изменен](#)²⁵).

4.5 Обновление списка устройств

Вы можете изменить список устройств, составленный при помещении содержимого диска в контейнер, без извлечения содержимого. Для этого после изменения набора устройств выберите команду **Обновить список устройств...** в меню **Система**, и введите пароль (рис. [Ввод пароля при смене подключенных устройств](#)²⁶).

Рисунок 27. Ввод пароля при смене подключенных устройств

SoftControl SysContainer находит все аппаратные устройства поддерживаемых типов, обнаруженные при загрузке ОС, считывает их параметры и выдает сообщение об успешном завершении операции (рис. [Список устройств обновлен](#)⁽²⁶⁾).

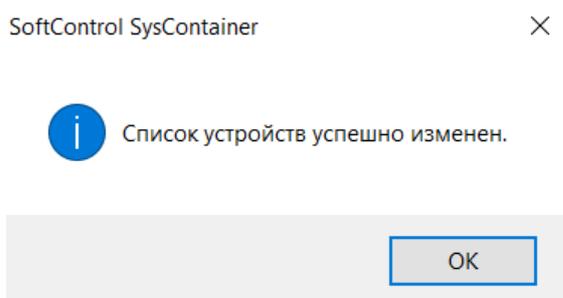


Рисунок 28. Список устройств обновлен

4.6 Запуск из командной строки

Все операции, перечисленные в разделах выше, можно выполнить из командной строки Windows с помощью команды вида:

```
"<каталог установки SoftControl SysContainer>\DcConsole.exe" /<команда> [<параметры>]
```

Возможные команды и их параметры перечислены в табл. 5.

Условие: все шаги выполняются под учетной записью с правами администратора.

Таблица 5. Параметры командной строки SoftControl SysContainer

| Команда/Параметр | Действие/возможные значения |
|---|--|
| <pre> /boot-prepare (/newpass пароль /newpassfile файл_с_паролем /cryptpass блок_данных_в_контейнере /cryptpassfile файл_с_блоком_данных_в_контейнере) [/ha 1 2 3 4 5] [/ea 1 2 3 4 6 7 8 9 10 11] </pre> | <p>Установить загрузчик системы помещения данных в контейнер/извлечения данных из контейнера.</p> <p>Пароль для помещения содержимого диска в контейнер можно задать следующими способами:</p> <p>а) указать явным образом с помощью параметра /newpass;</p> <p>б) записать в файл с любым расширением и кодировкой ASCII и указать имя файла с помощью параметра /newpassfile.</p> <p>Пароль должен содержать латинские буквы a-z, A-Z, цифры 0-9 и специальные символы !@#%\$%^&*()_+.</p> <p>с) указать <i>блок_данных_в_контейнере</i> (генерируется утилитой DcUtil.exe⁽³¹⁾ с помощью параметра /cryptpass.</p> <p>д) указать <i>файл_с_блоком_данных_в_контейнере</i> (генерируется утилитой DcUtil.exe⁽³¹⁾ с помощью параметра /cryptpassfile.</p> <p>Если алгоритмы хэширования и помещения данных в контейнер не заданы, используются значения по умолчанию, указанные ниже.</p> <p>Значения для алгоритма хэширования (параметр /ha):</p> <ul style="list-style-type: none"> 1 – SHA-512 (по умолчанию) 2 – Whirlpool 3 – SHA-256 4 – RIPEMD-160 5 – Streebog <p>Значения для алгоритма помещения данных в контейнер (параметр /ea):</p> <ul style="list-style-type: none"> 1 – AES (по умолчанию) 2 – Serpent 3 – Twofish 4 – Camellia 5 – (зарезервированное имя) 6 – Kuznyechik 7 – Twofish+AES 8 – Serpent+Twofish+AES 9 – AES+Serpent 10 – AES+Twofish+Serpent 11 – Serpent+Twofish |
| /disk-enc | <p>Начать помещение содержимого системного раздела/диска в контейнер.</p> <p>Если процесс помещения данных в контейнер был прерван, например, при выключении или перезагрузке клиентского хоста, то после включения последнего он автоматически возобновится.</p> |

| Команда/Параметр | Действие/возможные значения |
|--|---|
| /disk-dec [/noreboot] | Начать извлечение содержимого системного раздела/диска из контейнера. Если процесс извлечения данных из контейнера был прерван, например, при выключении или перезагрузке клиентского хоста, то после включения последнего он автоматически возобновится. Если используется параметр /noreboot, то после окончания извлечения данных из контейнера клиентский хост не будет перезагружен. |
| /state | Показать состояние системы SoftControl SysContainer. |
| /lic-set <i>лицензионный_ключ</i> | Активировать лицензионный ключ, полученный при покупке SoftControl SysContainer. |
| /pw-change (/currpass <i>текущий_пароль</i> /currpassfile <i>файл_с_текущим_паролем</i>) (/newpass <i>новый_пароль</i> /newpassfile <i>файл_с_новым_паролем</i>) | Изменить <i>текущий_пароль</i> , используемый для загрузки системы в случае критического изменения набора аппаратных устройств. Текущий пароль указывается явным образом (с помощью параметра /currpass) или через <i>файл_с_текущим_паролем</i> . Новый пароль указывается явным образом (с помощью параметра /newpass) или через <i>файл_с_новым_паролем</i> . |
| /pw-change (/cryptpass <i>блок_данных_в_контейнере</i> /cryptpassfile <i>файл_с_блоком_данных_в_контейнере</i>) | Изменить пароль, используемый для загрузки системы в случае критического изменения набора аппаратных устройств. И текущий, и новый пароль указываются с помощью одного <i>блока_данных_в_контейнере</i> или <i>файла_с_блоком_данных_в_контейнере</i> . |
| /dev-change (/currpass <i>текущий_пароль</i> /currpassfile <i>файл_с_текущим_паролем</i> /cryptpass <i>блок_данных_в_контейнере</i> /cryptpassfile <i>файл_с_блоком_данных_в_контейнере</i>) | Создать новый список устройств, используемых для загрузки ОС. Пароль указывается явным образом (с помощью параметра /currpass), через <i>файл_с_текущим_паролем</i> , через <i>блок_данных_в_контейнере</i> или через <i>файл_с_блоком_данных_в_контейнере</i> . |
| /dev-get (/currpass <i>текущий_пароль</i> /currpassfile <i>файл_с_текущим_паролем</i> /cryptpass <i>блок_данных_в_контейнере</i> /cryptpassfile <i>файл_с_блоком_данных_в_контейнере</i>) | Вывести в журнал информацию о подключенных устройствах. Пароль указывается явным образом (с помощью параметра /currpass), через <i>файл_с_текущим_паролем</i> , через <i>блок_данных_в_контейнере</i> или через <i>файл_с_блоком_данных_в_контейнере</i> . |
| /boot-clear | Удалить загрузчик системы SoftControl SysContainer из ОС. |
| /stop | Остановить процесс помещения данных в контейнер/извлечения данных из контейнера. После перезагрузки клиентского хоста прерванный процесс автоматически возобновится. |
| /seed-get | Получить блок данных для передачи пароля. Сгенерированное значение является одноразовым; после выполнения любой команды на компьютере с SoftControl SysContainer или после его перезагрузки необходимо выполнить команду /seed-get еще раз. |

Пример: Полную процедуру установки SoftControl SysContainer можно выполнить с помощью следующих скриптов установки (файлов с расширением .cmd или .bat).

Для установки SoftControl SysContainer и загрузчика системы помещения данных в

контейнер/извлечения данных из контейнера:

```
"<каталог с установочным пакетом>\SoftControl SysContainer Setup.exe" /q [/folder "<каталог для установки>"]  
"<каталог установки SoftControl SysContainer>\DcConsole.exe" /boot-prepare /newpassfile  
<файл_с_паролем>
```

i Если для команды /boot-prepare используется параметр /newpass, пароль для помещения содержимого диска в контейнер/извлечения содержимого диска из контейнера будет лежать в файле скрипта или в журнале событий в открытом виде.

Для проверки состояния системы и запуска процесса помещения данных в контейнер (скрипт запускается после перезагрузки клиентского хоста):

```
"<каталог установки SoftControl SysContainer>\DcConsole.exe" /state  
"<каталог установки SoftControl SysContainer>\DcConsole.exe" /disk-enc
```

i Команда /disk-enc начнет выполняться (т.е. процесс помещения данных в контейнер запустится), только если код возврата команды /state – S.MNT (Mounted). В противном случае скрипт выдаст ошибку.

Проверить состояние процесса помещения данных в контейнер можно с помощью команды /state (код возврата при завершении – S.FULL_ENC (Fully encrypted)).

4.7 Журналы

В SoftControl SysContainer реализовано протоколирование событий и статусов программы в журнал событий. Стандартный файл журнала содержит список устройств и уведомления о следующих событиях:

- **Изменение набора аппаратных устройств** – одно устройство не обнаружено.
- **Критическое изменение набора аппаратных устройств** – два устройства не обнаружены.
- **Загрузка с паролем.**
- **Выполнение основных функций системы:** помещение в контейнер/извлечение из контейнера содержимого системного раздела или диска, установка/удаление загрузчика системы помещения данных в контейнер/извлечения данных из контейнера, изменение пароля, изменение набора аппаратных устройств.

Стандартный файл журнала доступен по следующему пути:

C:\Windows\DecryptLog.log

Расширенная информация о событиях системы SoftControl SysContainer и причинах неудачного завершения операций содержится в подробном файле журнала, который доступен по следующему пути:

C:\ProgramData\DeCrypt\DeCrypt.log

Для обоих типов файлов в SoftControl SysContainer поддерживается ротация, помогающая контролировать их размер. Ротация позволяет формировать файлы, автоматически разбиваемые на идентичные по своим параметрам части вида:

- *DeCryptLog(rotated dd.mm.yyyy).log* для стандартных файлов, где dd.mm.yyyy – дата ротации файла;
- *DeCrypt.log_old1*, *DeCrypt.log_old2* и т.д. для подробных файлов.

Лимит по размеру файла журнала, по достижении которого происходит ротация, – 100Мб.

Примечание. Дублирующиеся USB-накопители указываются в стандартном файле журнала DecryptLog.log один раз. Однако если у двух USB-накопителей одинаковые параметры VID и PID, но один из них имеет серийный номер, а другой – нет, то в файле журнала будут указаны оба устройства (записи будут дублироваться).

4.8 Список игнорируемых устройств и отложенный запуск

Если к клиентскому хосту подключены устройства, инициализация которых происходит медленно, существует два способа оптимизации его работы:

- A. Отложить запуск загрузчика системы помещения данных в контейнер/извлечения данных из контейнера (задать задержку при загрузке ОС). В этом случае общее время загрузки клиентского хоста увеличится.
- B. Игнорировать эти устройства при формировании или обновлении списка устройств. В этом случае время загрузки не изменится, однако исключенные устройства не будут требоваться для извлечения содержимого диска.

Для внесения USB-накопителей в список игнорируемых устройств выполните описанные ниже действия:

- 1) Найдите в журнале DecryptLog.log (расположен по следующему пути: C:\Windows\DecryptLog.log) идентификатор того устройства, которое не должно проверяться. USB-накопители указываются в журнале в формате VID_PID_SERIALNUMBER.

Условие: запись будет присутствовать в логе, только если устройство обнаружилось хотя бы при одной загрузке клиентского хоста.

- 2) Запустите командную строку Windows с правами администратора. Подключите EFI-раздел к диску с помощью следующей команды:

```
mountvol u: /s
```

где u: – название диска для подключения.

- 3) Откройте в Блокноте файл с настройками с помощью следующей команды:

```
notepad.exe u:\EFI\DeCrypt\DcsProp
```

- 4) Измените в файле строку

```
<config key="BlacklistDevices"></config>
```

на

```
<config key="BlacklistDevices">устройство1;устройство2;...;устройствоN</config>
```

где устройствоN – полный идентификатор устройства (как указано в журнале) или начальная часть идентификатора и маска * (латинские буквы, цифры и символ подчеркивания).

Пример:

```
<config key="BlacklistDevices">13FE_4200_P16019100703681B1EDD8A13;0E0F_*</config>
```

- 5) Обновите список устройств с помощью следующей команды:

```
"<каталог_установки_SoftControl_SysContainer>\DcConsole.exe" /dev-change /currpassfile  
<файл_с_текущим_паролем>
```

Чтобы задать время задержки при загрузке ОС, выполните следующие действия:

- 1) Откройте файл с настройками с помощью следующей команды:

```
notepad.exe u:\EFI\DeCrypt\DcsProp
```

- 2) Выставьте для параметра `UsbInitDelay` требуемое значение задержки (в секундах).

4.9 Генерация блоков данных в контейнере

Утилита `DcUtil.exe` предназначена для генерации блоков данных в контейнере. При автоматизации управления системой SoftControl SysContainer с помощью сторонних средств данная утилита позволяет безопасно пересылать пароли.

Утилита входит в дистрибутив SoftControl SysContainer, однако не устанавливается на компьютер вместе с SoftControl SysContainer. Для работы с ней ее необходимо скопировать вручную на управляющий компьютер.

Последовательность действий при работе с *DcUtil.exe* описана ниже.

- 1) Запустите с управляющего компьютера на компьютере с SoftControl SysContainer следующую команду:

```
"<каталог установки SoftControl SysContainer>\DcConsole.exe" /seed-get
```

Результат выполнения команды – одноразовый блок данных в контейнере вида:

```
242d3695c45b5...9fch
```

- 2) Скопируйте блок данных на управляющий компьютер.
- 3) Запустите на управляющем компьютере команду вида:

```
"<каталог с DcUtil.exe>\DcUtil.exe" /<команда> [<параметры>]
```

Результат выполнения команды – одноразовый блок данных в контейнере (значение_seed) вида:

```
bb4e05cdc6c6bca94506b4dce81fd7791fa9cdf0...4258527h
```

- 4) Запустите с управляющего компьютера на компьютере с SoftControl SysContainer требуемую команду (см. таблицу [выше](#)⁽²⁷⁾), передав в качестве пароля полученный в п. 3) блок данных.

Возможные команды для утилиты *DcUtil.exe* и их параметры перечислены в табл. 6.

Условие: все шаги выполняются под учетной записью с правами администратора.

Таблица 6. Параметры командной строки DcUtil.exe

| Команда/Параметр | Действие/возможные значения |
|--|---|
| /help | Вывести список команд |
| /encryptpasswords [/currpass <i>текущий_пароль</i>] [/newpass <i>новый_пароль</i>] (/seed <i>значение_seed</i> /seedfile <i>файл_со_значением_seed</i>) | Зашифровать текущий и/или новый пароль. Пароль можно задать следующими способами: а) указать явным образом <i>текущий_пароль</i> и <i>новый_пароль</i> . Формат задания пароля см. выше ⁽²⁷⁾ . б) указать <i>значение_seed</i> , сгенерированное утилитой <i>DcConsole.exe</i> (см. выше ⁽³²⁾), с помощью параметра /seed. в) указать <i>файл_со_значением_seed</i> , сгенерированный утилитой <i>DcConsole.exe</i> , с помощью параметра /seedfile. |

4.10 Истечение лицензии

После истечения лицензии SoftControl SysContainer перестают работать следующие функции системы:

- Установка загрузчика системы помещения данных в контейнер/извлечения данных из контейнера.
- Помещение содержимого диска в контейнер.

- Создание нового списка устройств, используемых для загрузки ОС.
- Изменение пароля, используемого для загрузки ОС в случае критического изменения набора аппаратных устройств.

При попытке выполнить одну из перечисленных выше операций выдается сообщение об истечении лицензии с предложением ввести лицензионный ключ.

Остальные функции SoftControl SysContainer (извлечение содержимого диска из контейнера, удаление загрузчика и др.) остаются доступными.

5. Обновление SoftControl SysContainer

В данном разделе описаны необходимые действия по обновлению SoftControl SysContainer:

- [обновление в обычном режиме](#)⁽³⁴⁾;
- [обновление в тихом режиме](#)⁽³⁸⁾.



Обновление можно проводить, не извлекая содержимое системного диска из контейнера.

5.1 Обновление в обычном режиме

- 1) Запустите установочный пакет *SoftControl SysContainer Setup <product version>.exe* версии, на которую необходимо произвести обновление.
- 2) В случае вашего согласия, выберите параметр **I accept the license terms** (Я принимаю условия лицензионного соглашения) и нажмите **Next** (рис. [Лицензионное соглашение](#)⁽³⁴⁾).

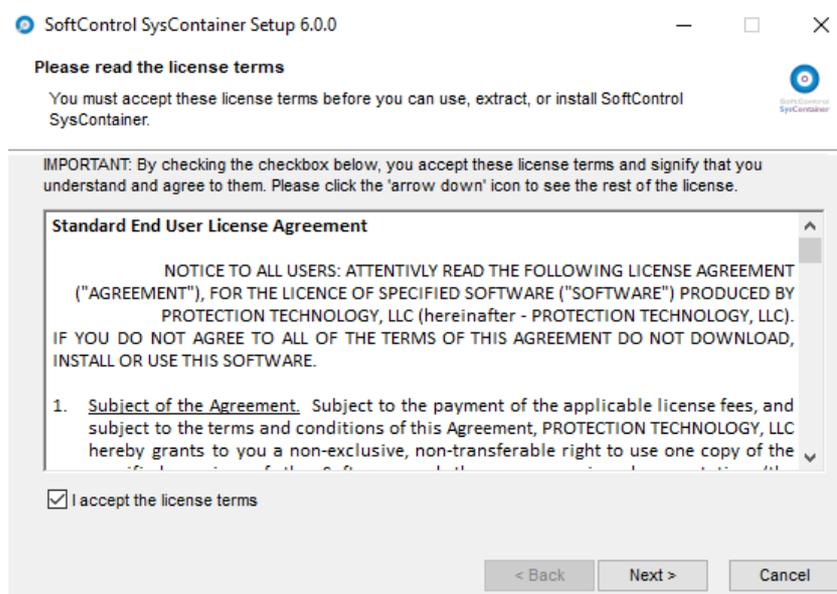


Рисунок 29. Лицензионное соглашение

- 3) Выберите требуемую опцию в окне **Wizard Mode** и нажмите **Next** (рис. [Выбор режима](#)⁽³⁵⁾).

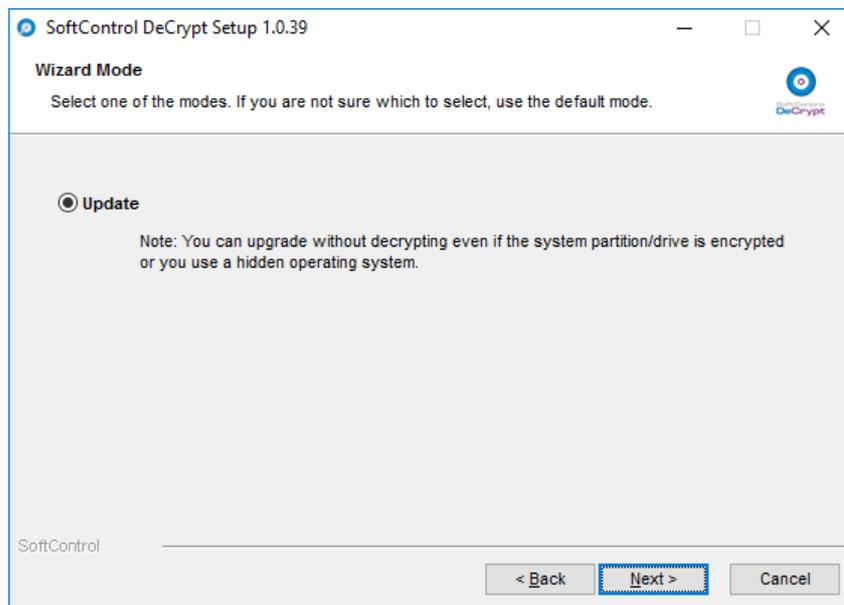


Рисунок 30. Выбор режима

4) Выберите требуемые опции в окне **Setup options** и нажмите **Update** (рис. [Выбор опций](#)⁽³⁵⁾).

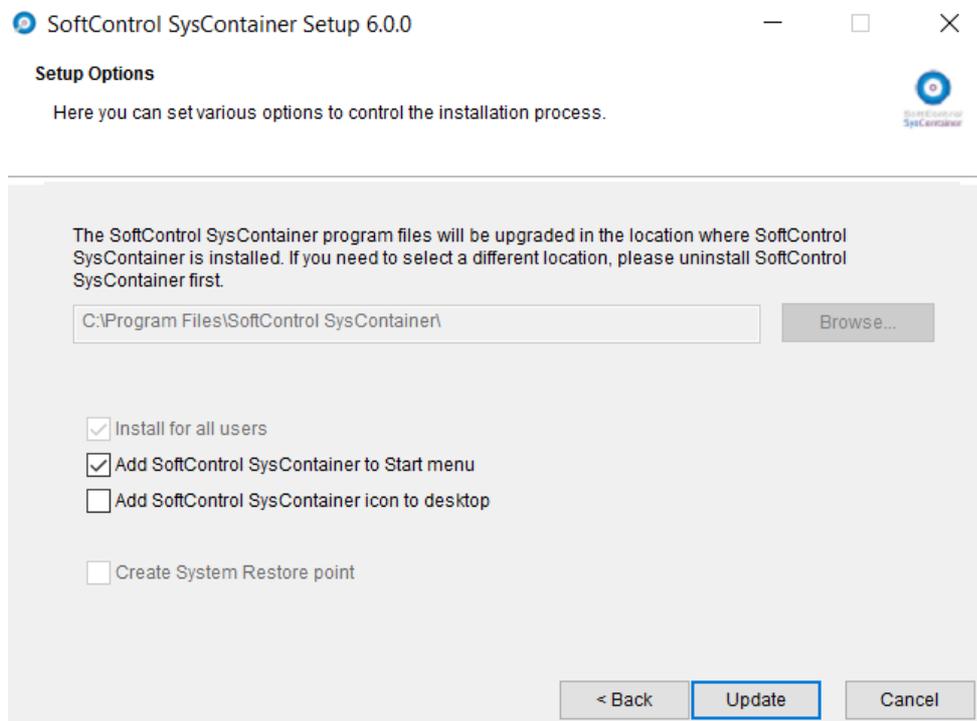


Рисунок 31. Выбор опций

5) Дождитесь окончания процесса обновления (рис. [Процесс обновления](#)⁽³⁶⁾).

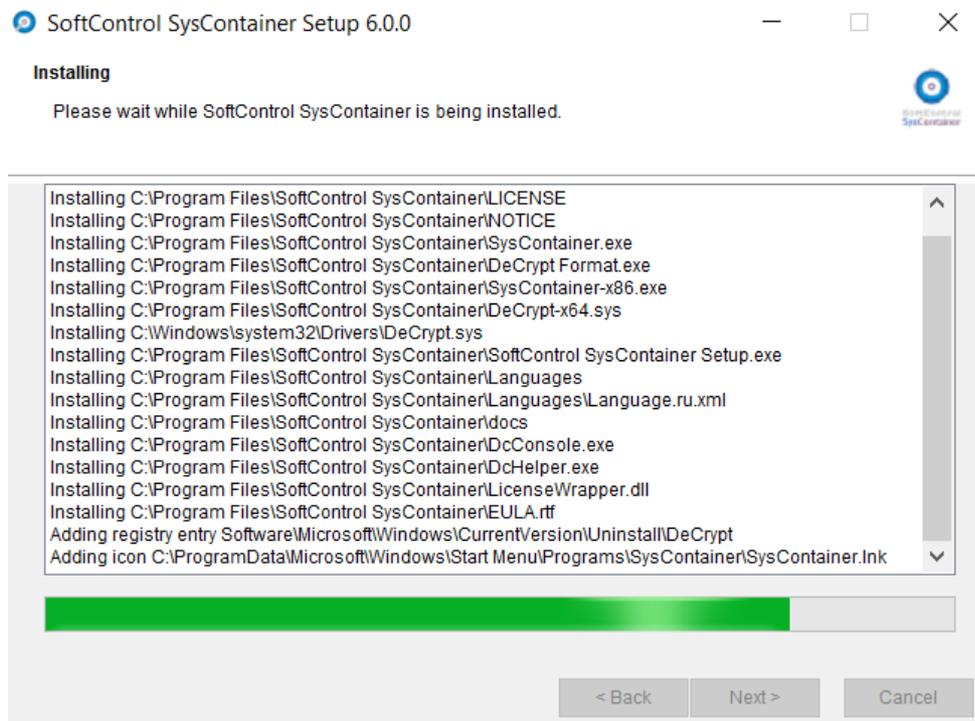


Рисунок 32. Процесс обновления

- 6) После появления сообщения **SoftControl SysContainer has been successfully upgraded** (Установка SoftControl SysContainer завершена) нажмите **Finish** (рис. [Завершение обновления](#)³⁷).

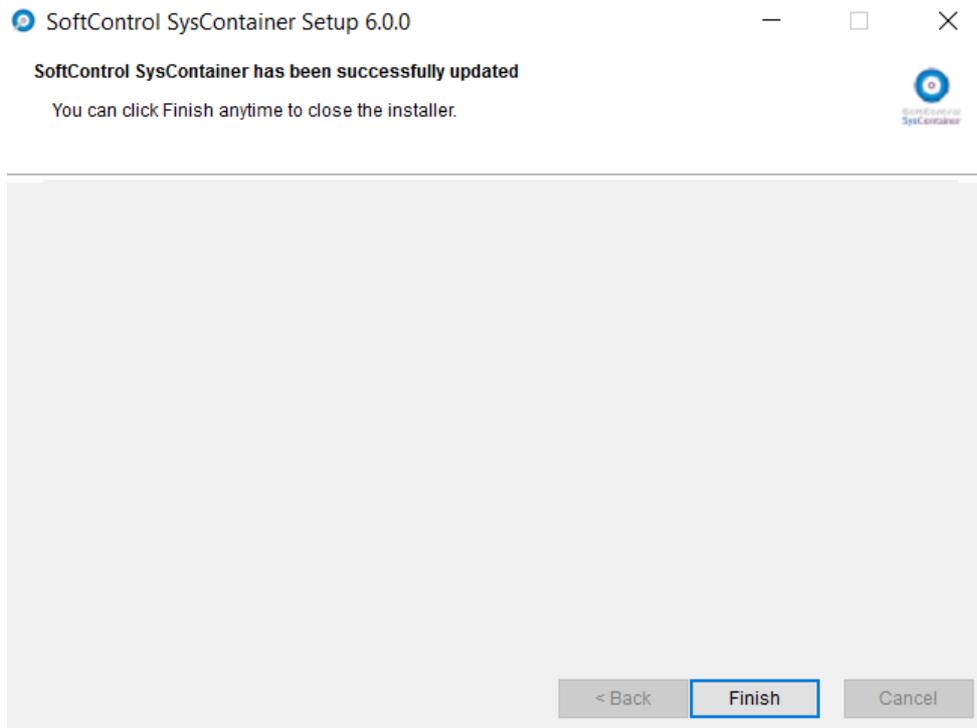


Рисунок 33. Завершение обновления

7) В диалоговом окне с предложением перезапуска системы выберите **Да/Yes**, после чего система будет отправлена на перезагрузку для завершения обновления (рис. [Запрос перезагрузки системы](#)³⁷).

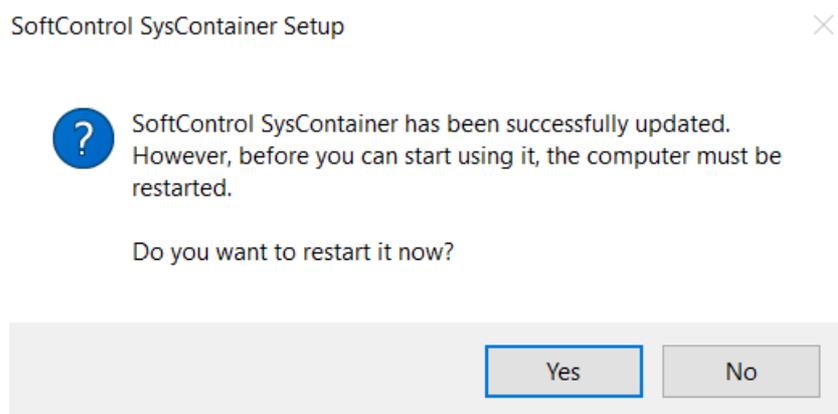


Рисунок 34. Запрос перезагрузки системы

5.2 Обновление в тихом режиме

Условие: все шаги выполняются под учетной записью с правами администратора.

- 1) Скопируйте установочный пакет *SoftControl SysContainer Setup <product version>.exe* версии, до которой необходимо произвести обновление, в какой-либо каталог клиентского хоста.
- 2) Запустите командную строку Windows и выполните следующую команду:

```
"<каталог с установочным пакетом>\SoftControl SysContainer Setup <product version>.exe" /q
```

Для корректной работы компонента SoftControl SysContainer после обновления в тихом режиме перезагрузите вручную операционную систему. Это необходимо для обновления драйвера.

6. Удаление SoftControl SysContainer

В данном разделе описана процедура деинсталляции SoftControl SysContainer:

- [в обычном режиме \(с использованием интерфейса пользователя\)](#)⁽³⁹⁾;
- [в тихом режиме](#)⁽⁴⁰⁾.

i Перед удалением SoftControl SysContainer необходимо [извлечь из контейнера помещенные в него данные](#)⁽²¹⁾. В противном случае восстановить содержимое диска будет невозможно.

6.1 Удаление в обычном режиме

- 1) Для ОС Microsoft® Windows® 7, Microsoft® Windows® Server 2008, Microsoft® Windows® 8, Microsoft® Windows® Server 2012, Microsoft® Windows® 10, Microsoft® Windows® Server 2016: в Панели управления Windows в разделе **Программы** (Programs) → **Удалить программу** (Uninstall program) выберите *SoftControl SysContainer* и нажмите **Удалить** (Uninstall).
- 2) В появившемся окне нажмите **Удалить** (рис. [Подтверждение удаления программы](#)⁽³⁹⁾).

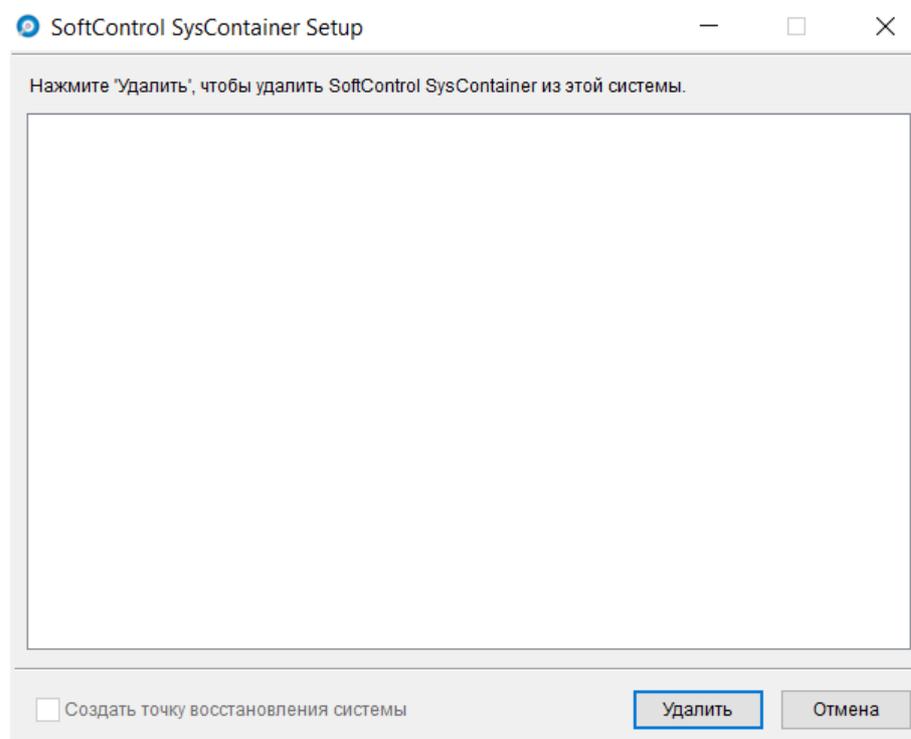


Рисунок 35. Подтверждение удаления программы

Примечание: Если вы добавляли какие-либо файлы в папку с SoftControl SysContainer,

она не будет удалена.

Нажмите **Готово** для завершения удаления программы (рис. [Завершение удаления программы](#) ⁽⁴⁰⁾).

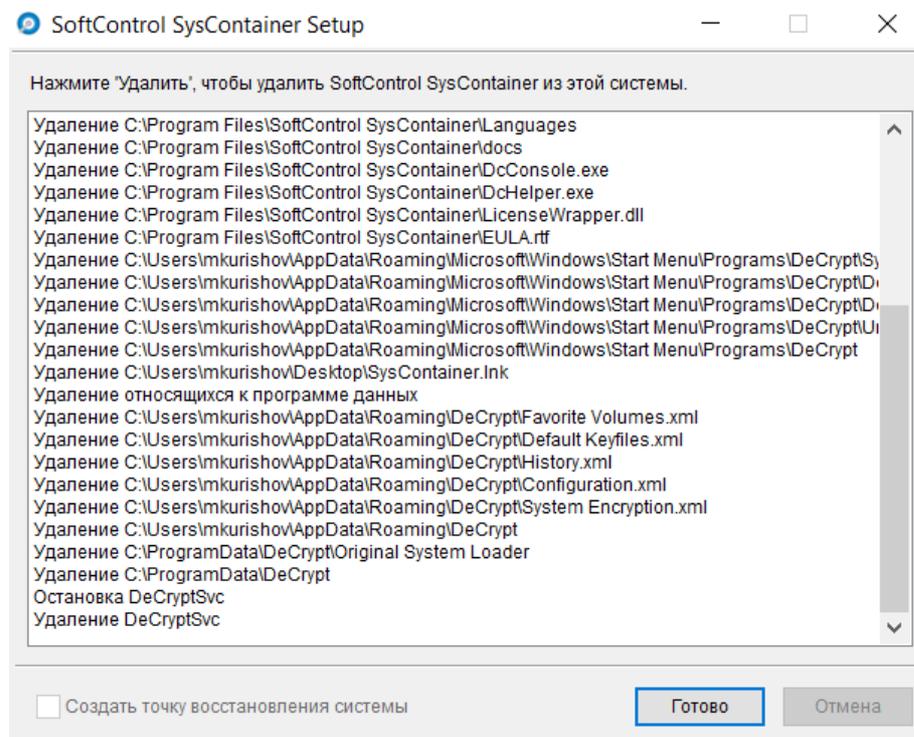


Рисунок 36. Завершение удаления программы

6.2 Удаление в тихом режиме

Условие: все шаги выполняются под учетной записью с правами администратора.

Запустите командную строку Windows и выполните следующую команду:

```
"<каталог установки SoftControl SysContainer>\SoftControl SysContainer Setup.exe" /q /u
```

7. Техническая поддержка

При возникновении вопросов по установке, настройке и работе SoftControl SysContainer вы можете обращаться в техническую поддержку по электронной почте support@sns-control.ru.

8. Приложение

8.1 Настройка раздела диска

В данном разделе представлена общая информация по подготовке первого раздела системного диска для установки SoftControl SysContainer. Информация носит рекомендательный характер и может применяться в случае возникновения ошибок при установке SoftControl SysContainer.

Если инсталлятор SoftControl SysContainer выдает ошибку о нехватке свободного места на диске, можно выполнить следующие действия.

Условие: все шаги выполняются под учетной записью с правами администратора.

Как правило, первый раздел на диске зарезервирован Windows под восстановление системы и не используется при обычной работе системы. Такой раздел можно удалить. Для этого запустите командную строку Windows и выполните следующую команду:

```
compmgmt.msc
```

В открывшейся оснастке **Управление компьютером** выберите пункт **Управление дисками**. Щелкните по первому разделу правой кнопкой мыши и выберите **Удалить том...** Следуйте инструкциям в появившемся окне для удаления раздела.



Данную операцию можно выполнять, только если вы уверены в отсутствии в первом разделе диска важных данных, и если при нарушении работы операционной системы нет необходимости восстанавливать ее с системного диска. Если после удаления раздела вам потребуется восстановить операционную систему, вы можете сделать это, загрузив ее с USB-накопителя или оптического диска.

Если информацию необходимо сохранить, воспользуйтесь одной из программ управления дисками, чтобы уменьшить раздел и передвинуть его от начала диска таким образом, чтобы перед ним образовалось свободное пространство для установки SoftControl SysContainer. Примеры таких программ:

- GParted (live-cd);
- Acronis Disk Director;
- Paragon Partition Manager;
- EaseUS Partition Master;

- Windows Image Backup;
- Clonezilla;
- GParted;
- Acronis True Image;
- HDClone.

Примечание. Если на вашей ОС первый раздел не отображается в оснастке **Управление компьютером**, вы можете использовать утилиту командной строки `diskpart.exe`.