SoftControl

DeCrypt 5.0.18

Руководство администратора

Уважаемый пользователь!

Safe'N'Sec Corporation благодарит Вас за то, что выбрали продукт SoftControl DeCrypt. 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 DeCrypt будет Вам полезен.

Почтовый адрес:
127106, Россия, Москва
Ботаническая ул., дом 10Д строение 1
Safe'N'Sec Corporation
Телефон:
+7 (495) 967-14-51
Факс:
+ 7 (495) 967-14-52
Электронная почта:
Общие вопросы и предложения: support@safensoft.com
Коммерческие вопросы: sales@safensoft.com
Веб-сайт компании: http://www.safensoft.com

Содержание

1. Введение

1.1 Назначение

Система шифрования SoftControl DeCrypt предназначена для шифрования системных дисков устройств самообслуживания (банкоматов, терминалов), функционирующих под управлением ОС семейства Microsoft® Windows®. SoftControl DeCrypt помогает защититься от атак, проводимых по следующим сценариям:

1. Злоумышленник похищает жесткий диск устройств самообслуживания (банкоматов, терминалов). 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 устройств самообслуживания (банкоматов, терминалов) с внешнего носителя и анализирует содержимое жесткого диска.

При запуске процесса шифрования SoftControl DeCrypt 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* 5.

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

SoftControl DeCrypt 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 DeCrypt также должен быть установлен клиентский компонент SoftControl SysWatch, с помощью которого на SoftControl Server передаются события системы шифрования.

Информацию о просмотре отчетов о событиях SoftControl DeCrypt см. в документе «Руководство администратора SoftControl Service Center».

* Формирование ключа из подмножества устройств является криптографически надежным благодаря использованию схемы разделения секрета Шамира.

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.
Условие	Условие выполнения, примечание, пример.
Обновить	– заголовки и сокращения; – названия экранных кнопок, ссылок, пунктов меню, других элементов программного интерфейса.
Политика контроля	– 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 DeCrypt>	Поля для замены функциональных названий фактическими значениями.
Приложение 6	Ссылки на внутренние ресурсы (разделы документа) с указанием номера страницы или на внешние ресурсы (URL-адреса).

1.2.2 Сокращения

В данном документе употребляются без расшифровки следующие сокращения:

- **ОЗУ** – оперативное запоминающее устройство;
- **ОС** – операционная система;
- **ПО** – программное обеспечение;
- **УС** – устройство самообслуживания;

1.2.3 Глоссарий

Таблица 2. Глоссарий

Термин	Пояснение
Клиентский хост	Средство вычислительной техники (рабочая станция, сервер, терминал самообслуживания), на котором установлен SoftControl DeCrypt.

Загрузчик системы шифрования	Компонент системы шифрования SoftControl DeCrypt, загружающий операционную систему с использованием параметров аппаратных устройств либо с использованием пароля (если загрузка с помощью параметров аппаратных устройств невозможна).

2. Требования к аппаратному и программному обеспечению

2.1 Системные требования SoftControl DeCrypt

Таблица 3. Минимальные системные требования

ОС	Частота ЦП	Объем ОЗУ	Объем свободного пространства на жестком диске
Клиентские операционные системы:			100 МБ + дополнительно 10 МБ на UEFI-разделе
Microsoft® Windows® 7 (SP1) *64-разрядная*	1 ГГц	2 ГБ	
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	
Серверные операционные системы:			
Microsoft® Windows® Server 2003 (SP2) *32-разрядная*	800 МГц	512 МБ	
Microsoft® Windows® Server 2003 (SP2) *64-разрядная*	800 МГц	512 МБ	
Microsoft® Windows® Server 2008 R2 *64-разрядная*	1,4 ГГц	512 МБ	
Microsoft® Windows® Server 2012 *64-разрядная*	1,4 ГГц	512 МБ	
Microsoft® Windows® Server 2012 R2 *64-разрядная*	1,4 ГГц	512 МБ	
Microsoft® Windows® Server 2016 *64-разрядная*	1,4 ГГц	512 МБ	
Microsoft® Windows® Server 2016 *64-разрядная* (для варианта установки «Сервер с рабочим столом»)	1,4 ГГц	2 ГБ	

Дополнительные требования:

- Тип BIOS: UEFI; рекомендуется отключить опцию **SecureBoot**.
- Системный диск должен быть разбит в формате GPT (GUID Partition Table); в начале диска необходимо наличие нераспределенного пространства (не менее 32 КБ). См. также информацию в Приложении 40.
- Для Windows 7 и Windows Server 2008 R2: обновление KB3033929 (поддержка алгоритма хэширования SHA-256 при проверке цифровой подписи) или любое его замещающее.

3. Установка SoftControl DeCrypt

Возможны следующие варианты установки SoftControl DeCrypt:

- в обычном режиме (с использованием интерфейса пользователя)[9];
- в тихом режиме[12].

3.1 Установка в обычном режиме

1) Запустите установочный пакет *SoftControl DeCrypt Setup 5.0.18.exe*.
2) В случае вашего согласия, выберите параметр **I accept the license terms** (Я принимаю условия лицензионного соглашения) и нажмите **Next** (рис. Лицензионное соглашение[9]).

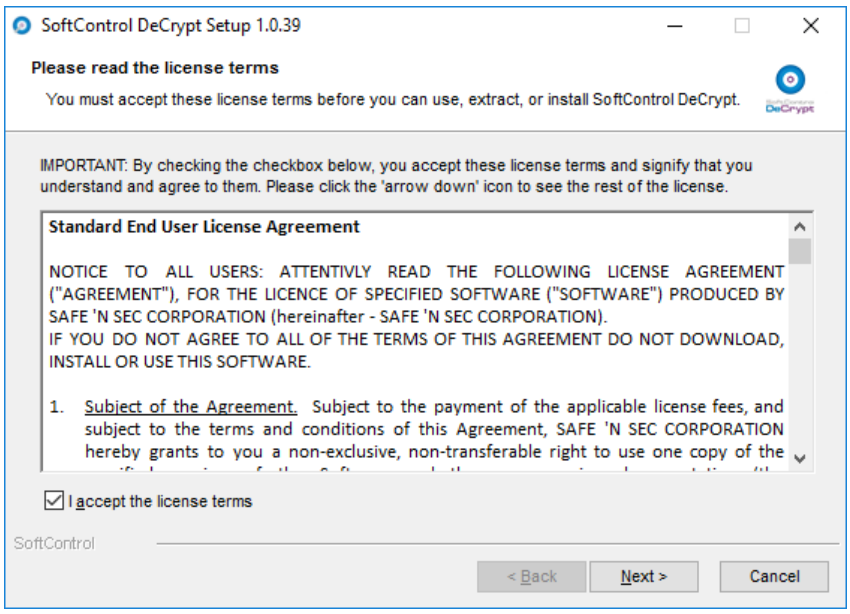

Рисунок 1. Лицензионное соглашение

3) Выберите требуемую опцию в окне **Wizard Mode** и нажмите **Next** (рис. Выбор варианта установки[10]).

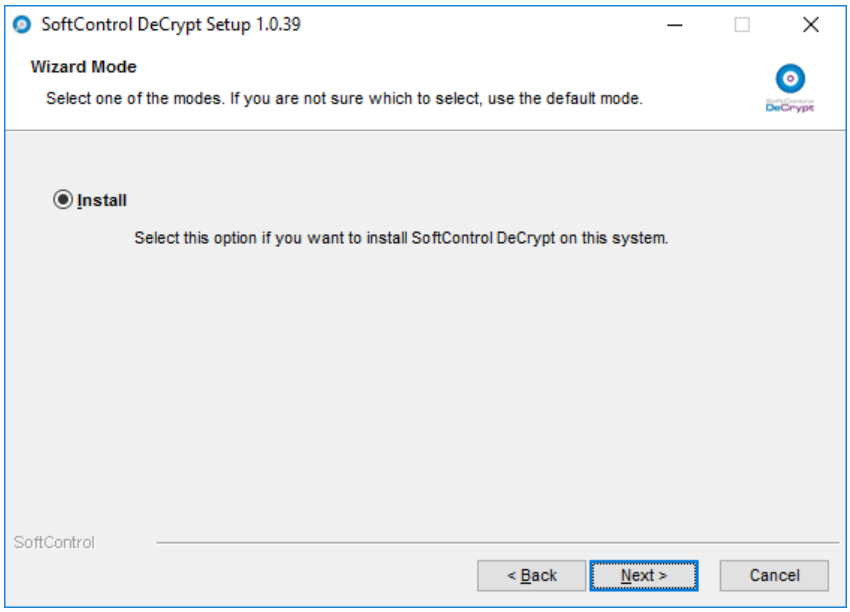

Рисунок 2. Выбор варианта установки

4) С помощью кнопки **Browse** выберите каталог для установки SoftControl DeCrypt и нажмите **Install** (рис. Путь установки[10]).

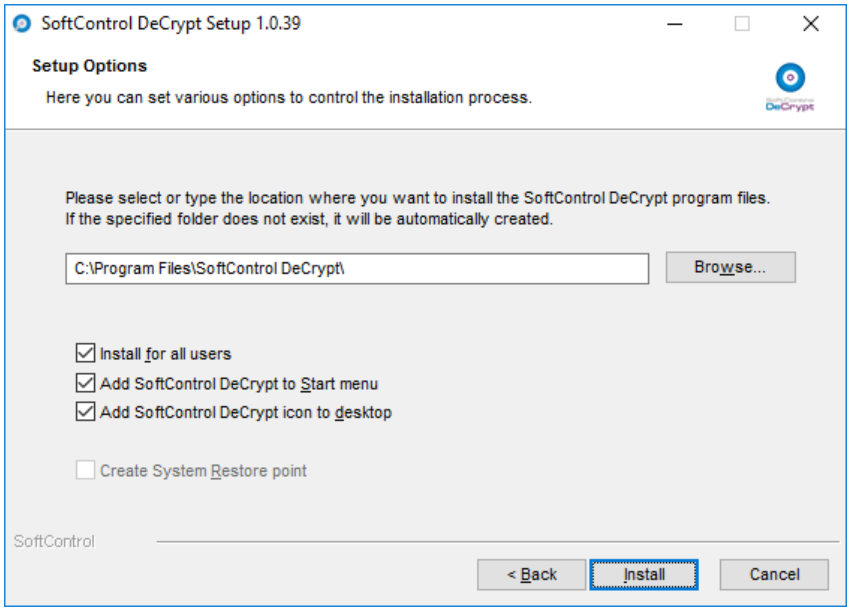

Рисунок 3. Путь установки

5) Дождитесь окончания процесса установки (рис. Процесс установки[11]).

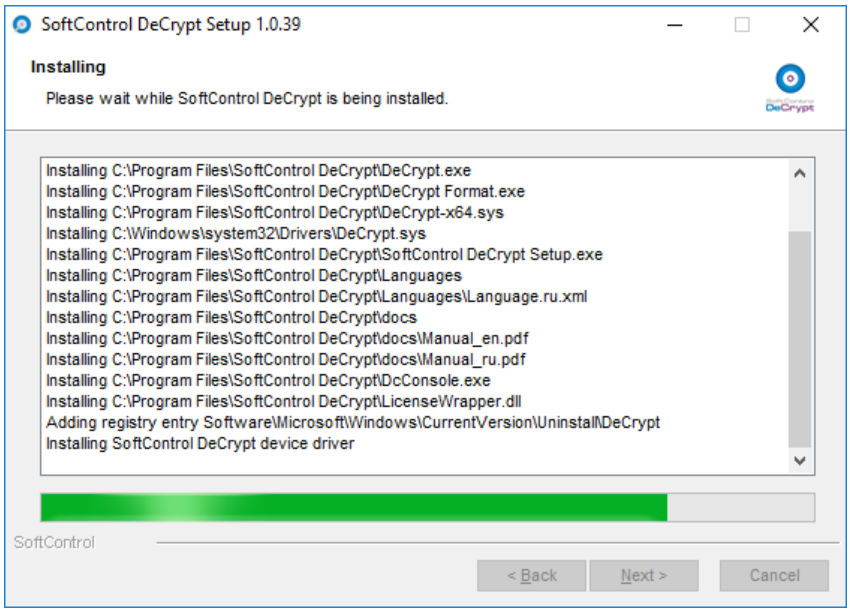

Рисунок 4. Процесс установки

6) После появления сообщения **Установка SoftControl DeCrypt завершена** нажмите **Finish** (рис. Завершение установки 11).

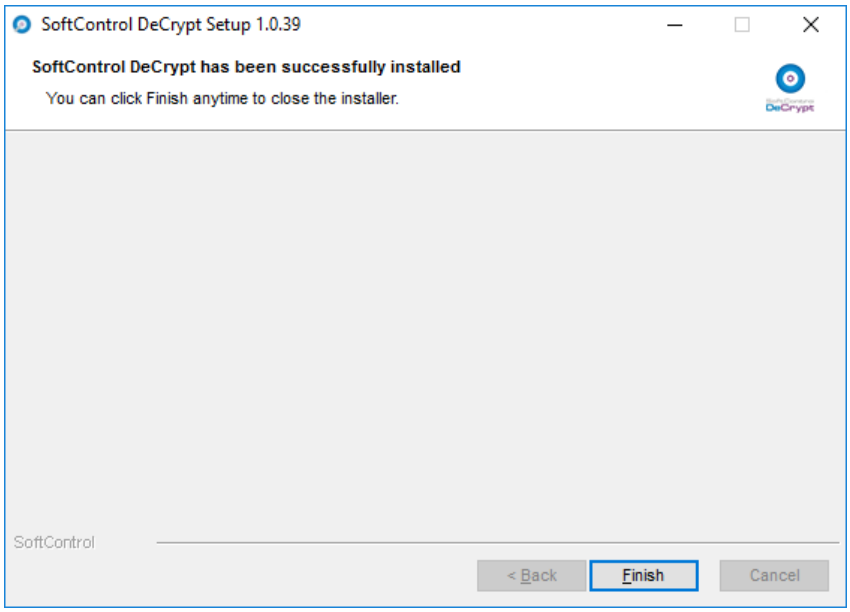

Рисунок 5. Завершение установки

3.2 Установка в тихом режиме

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

1) Скопируйте установочный пакет *SoftControl DeCrypt Setup 5.0.18.exe* в какой-либо каталог клиентского хоста.
2) Запустите командную строку Windows и выполните следующую команду:

```
"<каталог с установочным пакетом>\SoftControl DeCrypt Setup 5.0.18.exe" /q [/folder "<каталог для установки>"]
```

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

4. Работа с SoftControl DeCrypt

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

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

Внешний вид программы показан на рис. Элементы интерфейса программы 13.

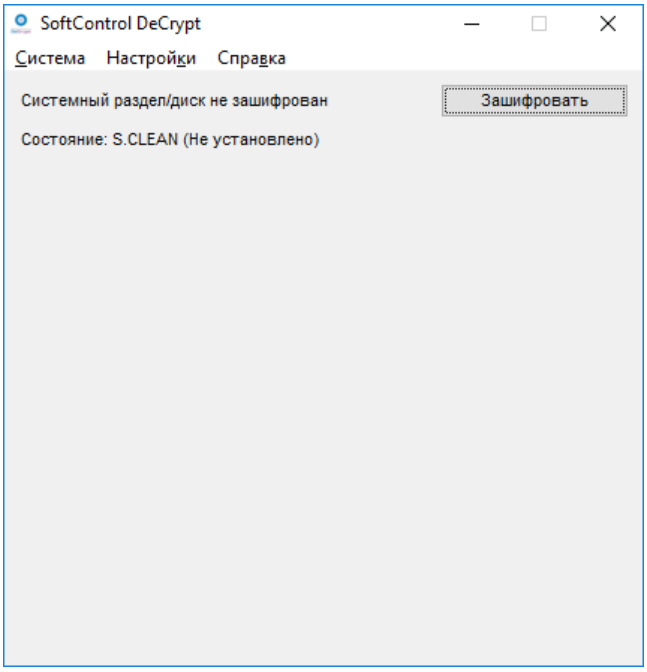

Рисунок 6. Элементы интерфейса программы

Команды меню описаны в табл. 4.

Таблица 4. Описание команд меню SoftControl DeCrypt

Команда меню	Действие
Зашифровать системный раздел/диск...	Запуск процесса шифрования системного раздела или диска.
Расшифровать системный раздел/диск	Запуск процесса дешифрования системного раздела или диска.
Возобновить прерванный процесс	Возобновление остановленного процесса шифрования или дешифрования.
Удалить загрузчик	Удаление загрузчика системы шифрования без удаления SoftControl DeCrypt (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.
Язык (language)...	Смена языка интерфейса.
Руководство пользователя	Вызов справки.

Состояния системы перечислены в табл. 5.

Таблица 5. Состояния SoftControl DeCrypt

Состояние	Описание
S.CLEAN (Не установлено)	Система шифрования SoftControl DeCrypt установлена на клиентском хосте, но диск не содержит загрузчик системы шифрования.
S.INST (Установлено)	Загрузчик системы шифрования установлен, но еще не запускался (перезагрузка клиентского хоста не была выполнена).
S.MNT (Загружено)	Загрузчик системы шифрования установлен, клиентский хост был перезагружен, но операции по шифрованию диска еще не выполнялись.
S.PART_ENC (Частично зашифровано)	Выполняется шифрование или расшифровка системного диска.
S.FULL_ENC (Полностью зашифровано)	Системный диск зашифрован.

4.1 Шифрование диска

В основном окне SoftControl DeCrypt нажмите **Зашифровать** (рис. Элементы интерфейса программы 13).

В появившемся окне в выпадающих списках выберите **Алгоритм шифрования** и **Алгоритм хэширования** и нажмите **Далее** (рис. Настройки шифрования 14). Хэширование используется для формирование ключей из пароля и других данных, а также для генерации случайных чисел.

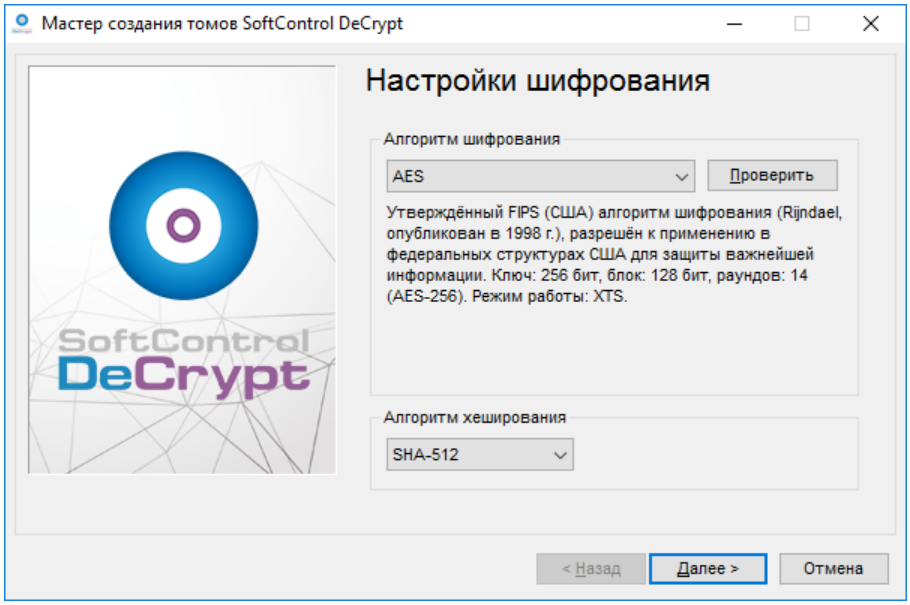

Рисунок 7. Настройки шифрования

Задайте **Пароль** и его подтверждение (рис. Задание пароля 15).

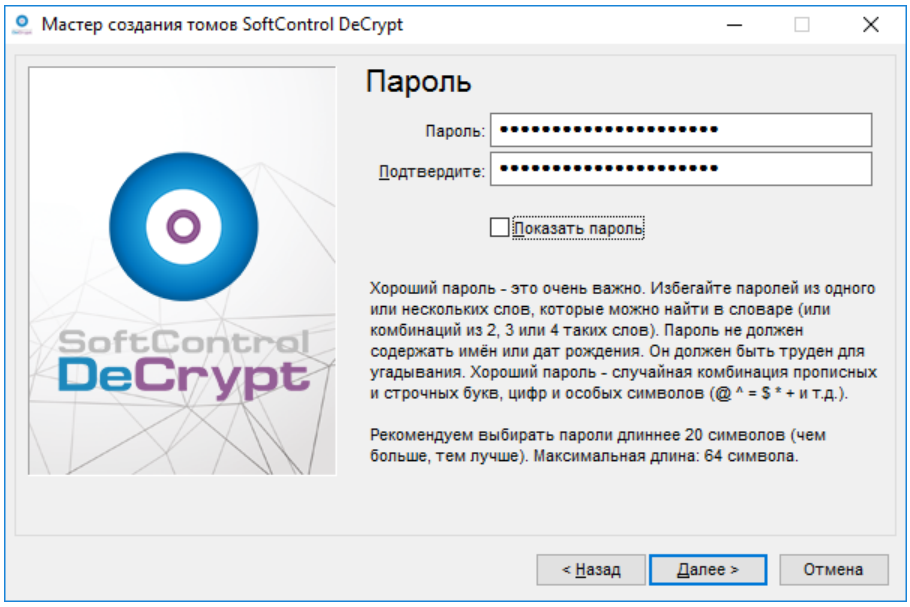

Рисунок 8. Задание пароля

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[15]).

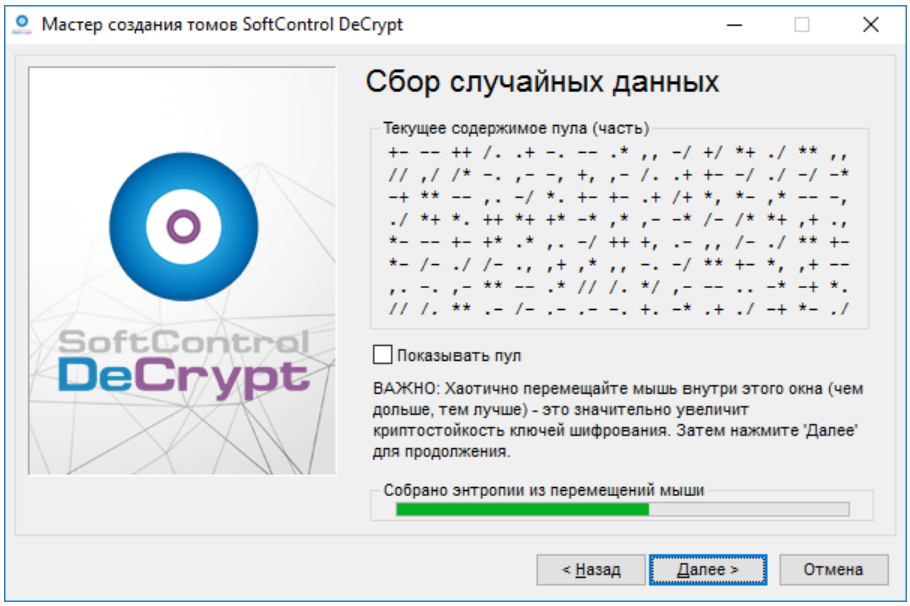

Рисунок 9. Сбор случайных данных

Для просмотра ключей в следующем окне (рис. Сгенерированные ключи[16]) выставите флажок **Показ созданных ключей (их частей)**.

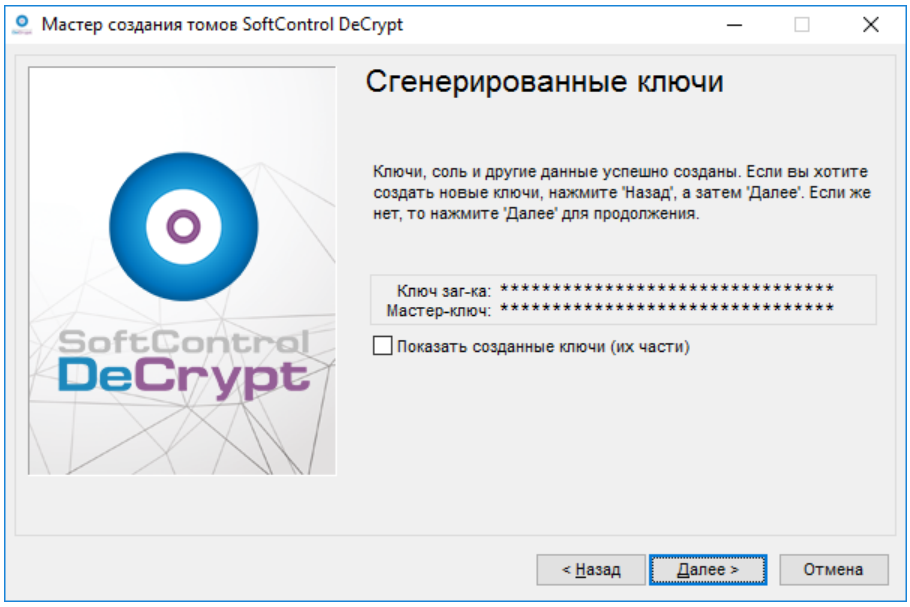

Рисунок 10. Сгенерированные ключи

Выберите **Режим очистки** в выпадающем списке (рис. Выбор режима очистки 16).

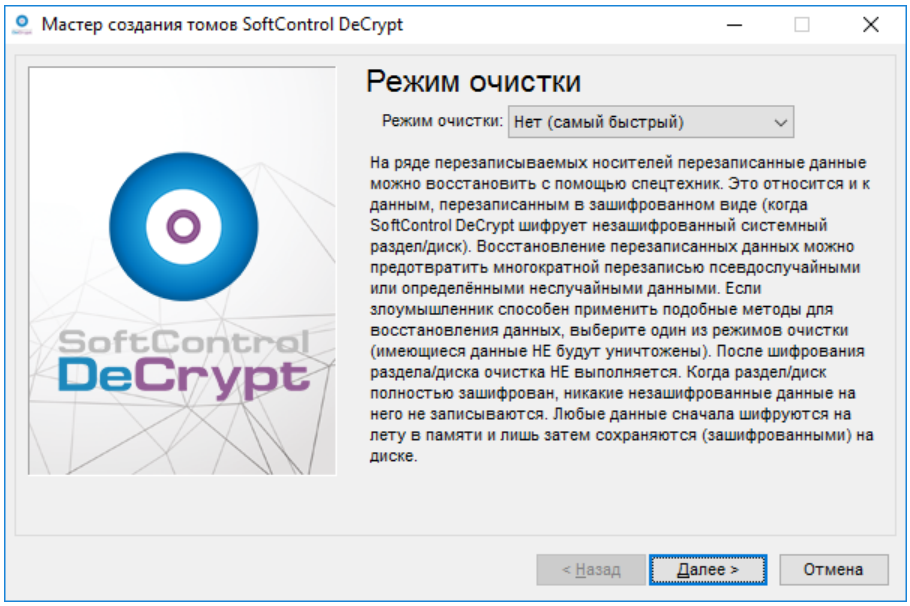

Рисунок 11. Выбор режима очистки

Включение режима очистки значительно увеличивает время шифрования системного раздела/диска.

После нажатия на кнопку **Далее** в окне **Режим очистки** (см. выше 16) SoftControl DeCrypt предлагает провести предварительный тест, цель которого – убедиться, что система подготовлена к шифрованию. Во время предварительного теста устанавливается загрузчик SoftControl DeCrypt (рис. Запуск предварительного теста 17).

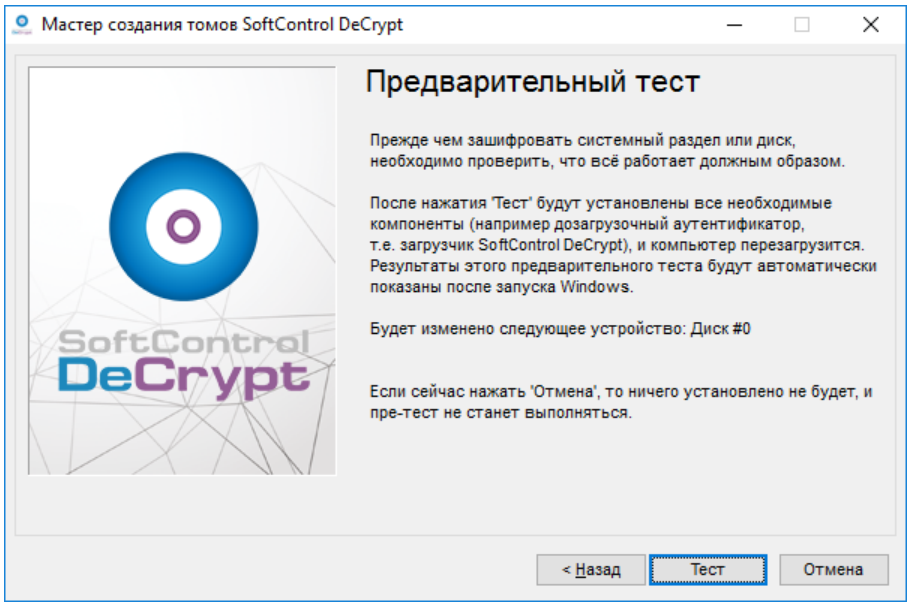

Рисунок 12. Запуск предварительного теста

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 17).

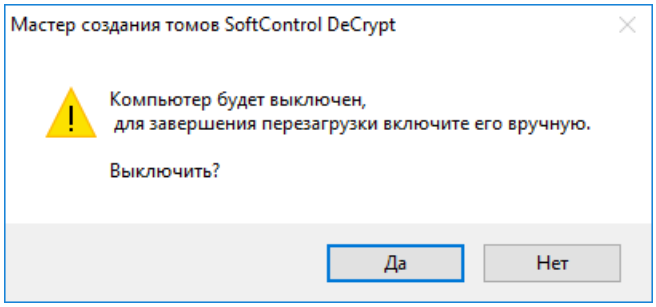

Рисунок 13. Выключение системы

После включения клиентского хоста SoftControl DeCrypt выдаст сообщение о возобновлении шифрования диска 18 (в случае входа в систему под той же учетной записью, под которой был запущен процесс шифрования), а затем сообщение о завершении предварительного теста (рис. Завершение предварительного теста 18).

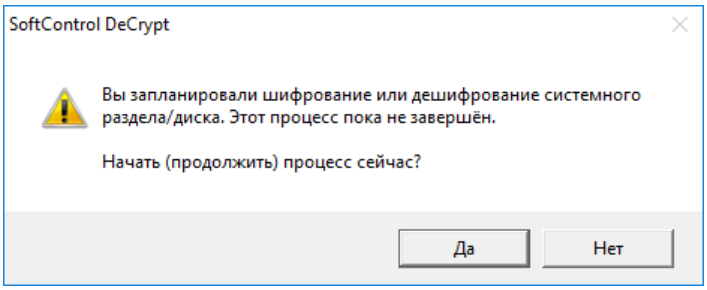

Рисунок 14. Возобновление шифрования диска

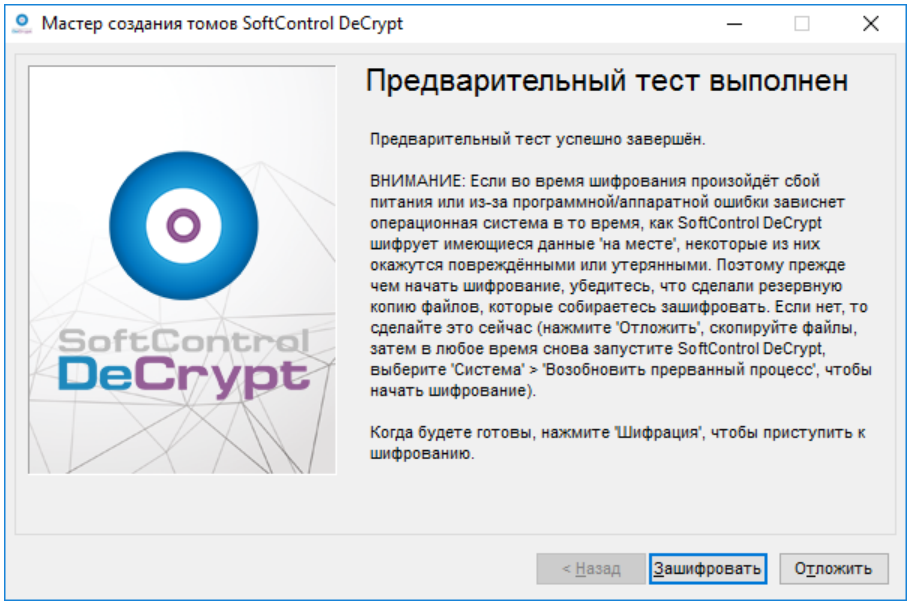

Рисунок 15. Завершение предварительного теста

Нажмите **Зашифровать** для запуска шифрования системного раздела/диска. Окно **Шифрование** содержит индикатор выполнения и примерное время до окончания процесса (рис. Процесс шифрования диска 19).

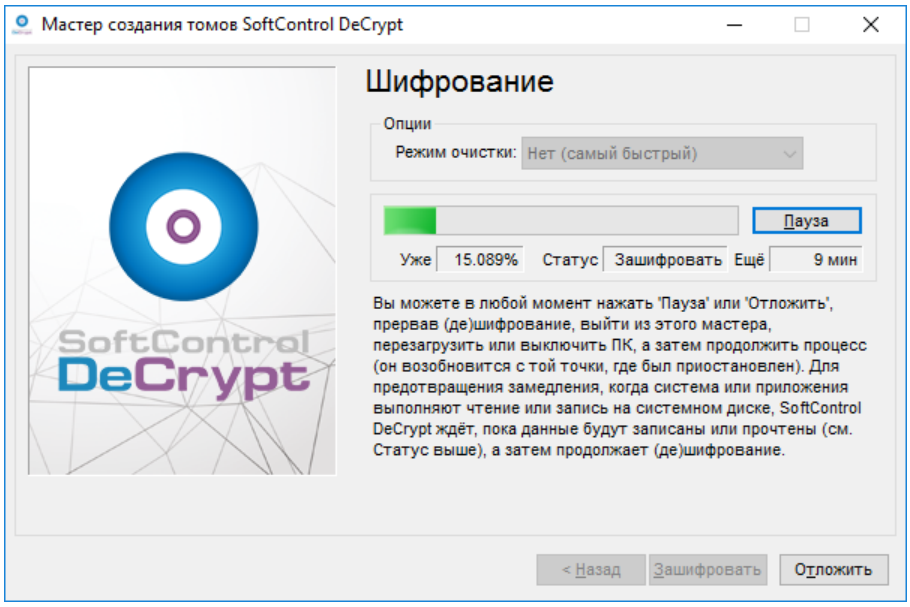

Рисунок 16. Процесс шифрования диска

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

Чтобы запустить процесс шифрования в другое время, нажмите **Отложить**. Для возобновления выберите команду **Возобновить прерванный процесс** в основном окне SoftControl DeCrypt (табл. Описание команд меню SoftControl DeCrypt 13).

Отменить процесс шифрования невозможно.

Примечание. Сообщение о возобновлении процесса шифрования (см. рис. выше 18) также будет показано, если процесс шифрования был отложен, а клиентский хост перезагружен (в случае входа в систему под той же учетной записью, под которой был запущен процесс шифрования).

В появившемся после завершения процесса шифрования окне (рис. Завершение шифрования 20) нажмите **OK**, а затем **Готово** в окне Мастера создания томов (рис. Системный раздел/диск зашифрован 20).

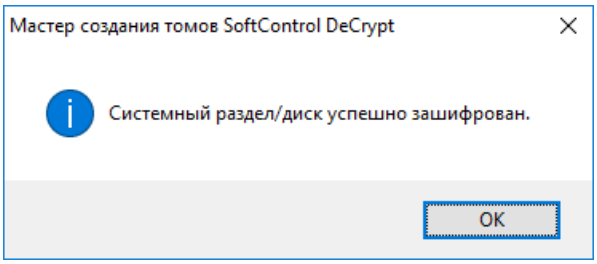

Рисунок 17. Завершение шифрования

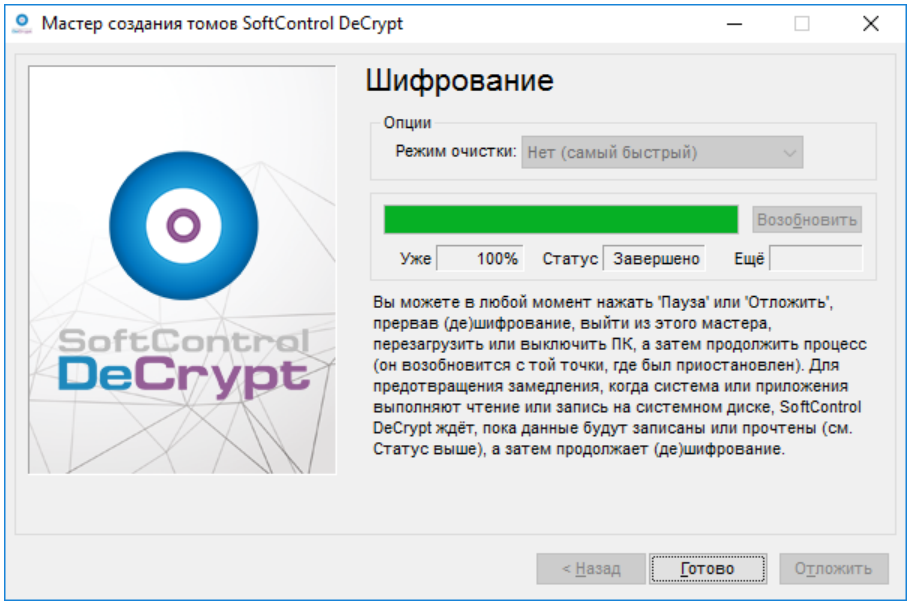

Рисунок 18. Системный раздел/диск зашифрован

При следующем запуске SoftControl DeCrypt в основном окне программы отображается информация о параметрах шифрования (рис. Данные шифрования 21).

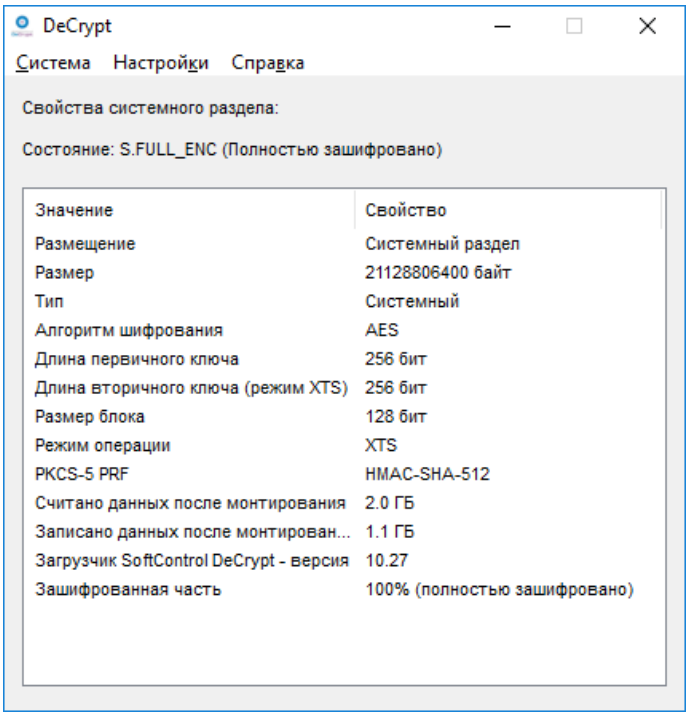

Рисунок 19. Параметры шифрования

4.2 Изменение подключённых аппаратных устройств

Система SoftControl DeCrypt при запуске шифрования 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 DeCrypt, – 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 зашифрованного 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 шифровании системы (рис. Запрос пароля при загрузке клиентского хоста 22).

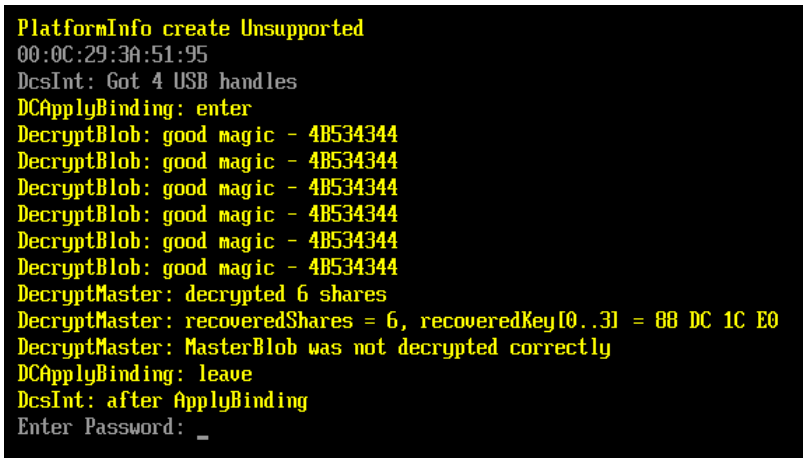

Рисунок 20. Запрос пароля при загрузке клиентского хоста

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

4.3 Расшифровка диска

В основном окне программы выберите команду **Расшифровать системный раздел/диск** в меню **Система** (табл. Описание команд меню SoftControl DeCrypt 13). В окне предупреждения выберите **Да** (рис. Подтверждение расшифровки диска 22) и дождитесь окончания процесса (рис. Диск расшифрован 24).

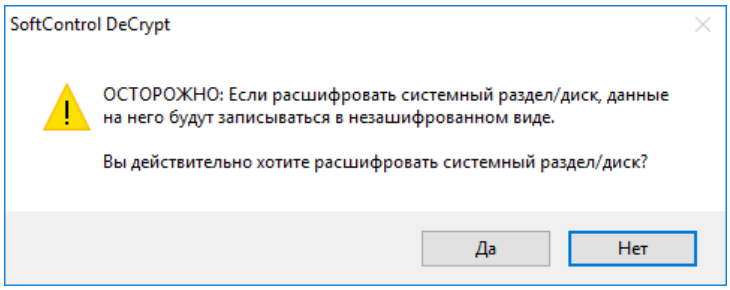

Рисунок 21. Подтверждение расшифровки диска

Как и в случае с шифрованием (см. раздел Шифрование диска 19), вы можете приостановить или отложить этот процесс, нажав **Пауза** или **Отложить** (рис. Расшифровка диска 23).

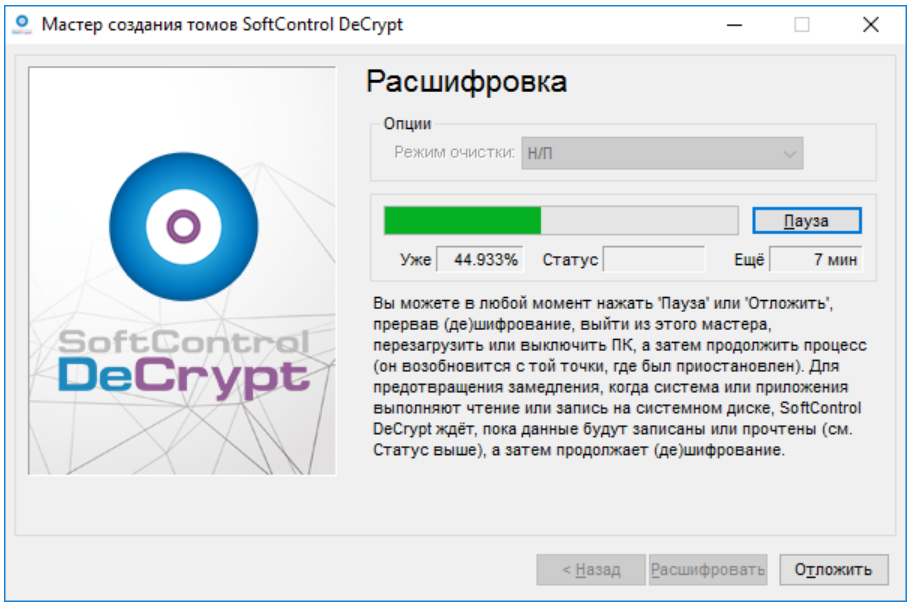

Рисунок 22. Расшифровка диска

Отменить процесс расшифровки невозможно.

Примечание. Если процесс расшифровки был отложен, а клиентский хост выключен или перезагружен, то после включения клиентского хоста SoftControl DeCrypt выдаст следующее сообщение (рис. Возобновление расшифровки диска [23]) (в случае входа в систему под той же учетной записью, под которой был запущен процесс расшифровки).

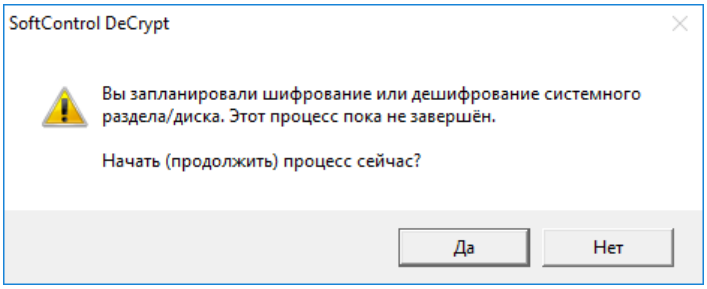

Рисунок 23. Возобновление расшифровки диска

В появившемся окне (рис. Диск расшифрован [24]) нажмите **OK**.

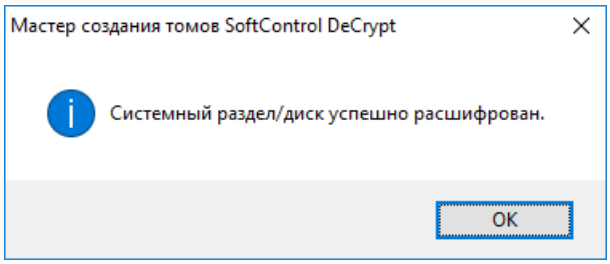

Рисунок 24. Диск расшифрован

В диалоговом окне с предложением перезапуска клиентского хоста выберите **Да**, после чего система будет отправлена на перезагрузку для завершения процесса (рис. Запрос перезагрузки системы 24).

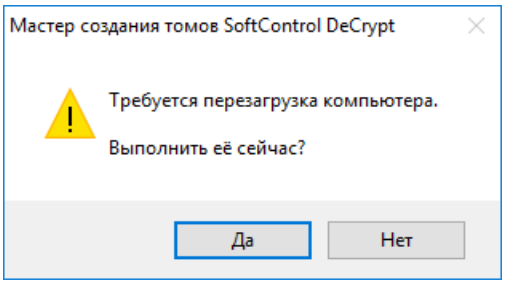

Рисунок 25. Запрос перезагрузки системы

4.4 Смена пароля

Для смены пароля, заданного при запуске шифрования, выберите команду **Изменить пароль...** в меню **Система** (рис. Смена пароля 24).

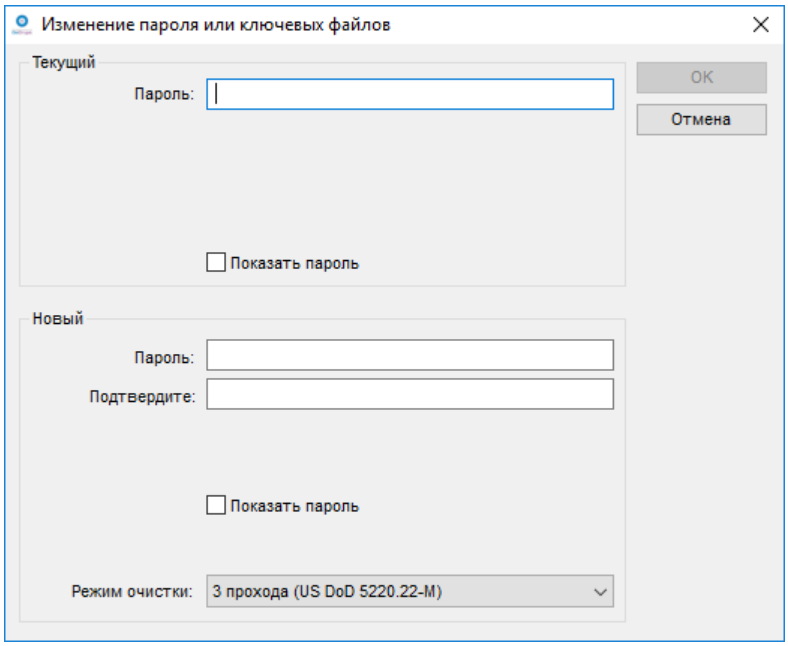

Рисунок 26. Смена пароля

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 шифрования (рис. Сбор случайных данных для смены пароля [25]).

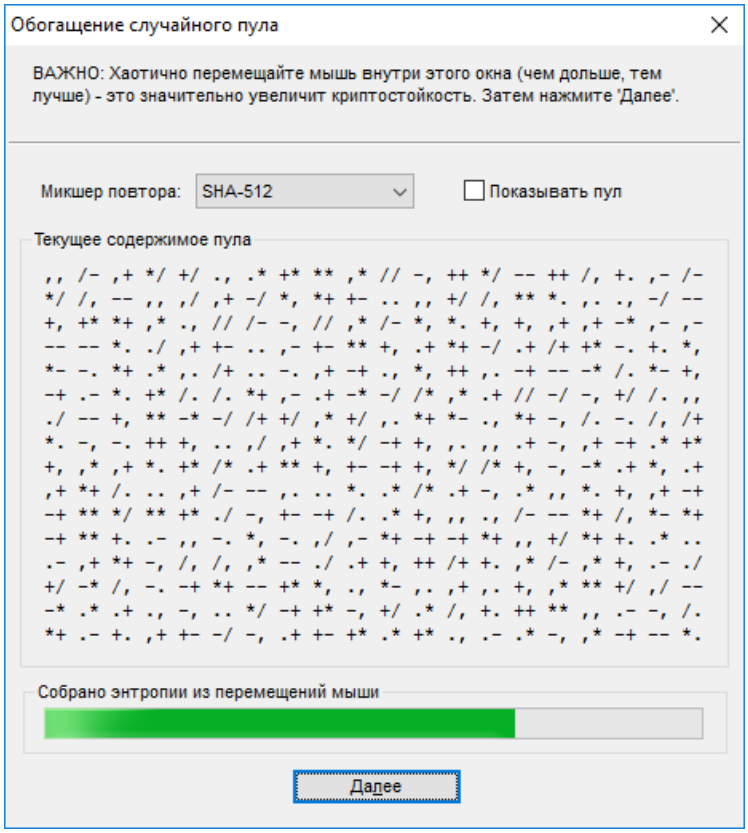

Рисунок 27. Сбор случайных данных для смены пароля

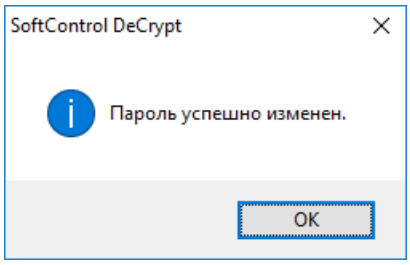

Рисунок 28. Пароль изменён

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 шифровании диска, без его расшифровки. 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]).

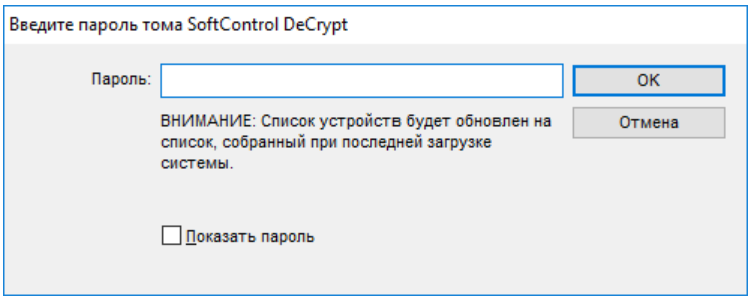

Рисунок 29. Ввод пароля при смене подключенных устройств

SoftControl DeCrypt 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]).

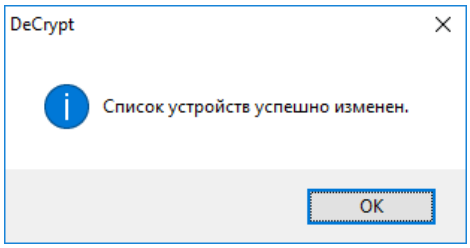

Рисунок 30. Список устройств обновлен

4.6 Запуск из командной строки

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

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

Возможные команды и их параметры перечислены в табл. 6.

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

Таблица 6. Параметры командной строки SoftControl DeCrypt

Команда/Параметр	Действие/возможные значения
/boot-prepare (/newpass *пароль*| /newpassfile *файл_с_паролем*| /cryptpass *блок_зашифрованных_данных*| /cryptpassfile *файл_с_блоком_зашифрованных_данных*) [/ha 1|2|3|4|5] [/ea 1|2|3|4|6|7|8|9| 10|11]	Установить загрузчик системы шифрования. Пароль для шифрования диска можно задать следующими способами: a) указать явным образом с помощью параметра /newpass; b) записать в файл с любым расширением и кодировкой ASCII и указать имя файла с помощью параметра /newpassfile. Пароль должен содержать латинские буквы a-z, A-Z, цифры 0-9 и специальные символы !@#$%^&*()_+. c) указать *блок_зашифрованных_данных* (генерируется утилитой DcUtil.exe (31)) с помощью параметра /cryptpass. d) указать *файл_с_блоком_зашифрованных_данных* (генерируется утилитой DcUtil.exe (31)) с помощью параметра /cryptpassfile. Если алгоритмы хэширования и шифрования не заданы, используются значения по умолчанию, указанные ниже. Значения для алгоритма хэширования (параметр /ha): 1 – SHA-512 (по умолчанию) 2 – Whirlpool 3 – SHA-256 4 – RIPEMD-160 5 – Streebog Значения для алгоритма шифрования (параметр /ea): 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	Начать шифрование системного раздела/диска. Если процесс шифрования был прерван, например, при выключении или перезагрузке клиентского хоста, то после включения последнего он автоматически возобновится.
/disk-dec [/noreboot]	Начать расшифровку системного раздела/диска. Если процесс расшифровки был прерван, например, при выключении или перезагрузке клиентского хоста, то после включения последнего он автоматически возобновится. Если используется параметр /noreboot, то после окончания расшифровки клиентский хост не будет перезагружен.
/state	Показать состояние системы шифрования SoftControl DeCrypt.
/lic-set *лицензионный_ключ*	Активировать лицензионный ключ, полученный при покупке SoftControl DeCrypt.

Команда/Параметр	Действие/возможные значения
/pw-change (/currpass *текущий_пароль*| /currpassfile *файл_с_текущим_паролем*) (/newpass *новый_пароль*| /newpassfile *файл_с_новым_паролем*)	Изменить *текущий_пароль*, используемый для загрузки системы в случае критического изменения набора аппаратных устройств. Текущий пароль указывается явным образом (с помощью параметра /currpass) или через *файл_с_текущим_паролем*. Новый пароль указывается явным образом (с помощью параметра /newpass) или через *файл_с_новым_паролем*.
/pw-change (/cryptpass *блок_зашифрованных_данных*| /cryptpassfile *файл_с_блоком_зашифрованных_данных*)	Изменить пароль, используемый для загрузки системы в случае критического изменения набора аппаратных устройств. И текущий, и новый пароль указываются с помощью одного *блока_зашифрованных_данных* или *файла_с_блоком_зашифрованных_данных*.
/dev-change (/currpass *текущий_пароль*| /currpassfile *файл_с_текущим_паролем*| /cryptpass *блок_зашифрованных_данных*| /cryptpassfile *файл_с_блоком_зашифрованных_данных*)	Создать новый список устройств, используемых для загрузки ОС. Пароль указывается явным образом (с помощью параметра /currpass), через *файл_с_текущим_паролем*, через *блок_зашифрованных_данных* или через *файл_с_блоком_зашифрованных_данных*.
/dev-get (/currpass *текущий_пароль*| /currpassfile *файл_с_текущим_паролем*| /cryptpass *блок_зашифрованных_данных*| /cryptpassfile *файл_с_блоком_зашифрованных_данных*)	Вывести в журнал информацию о подключенных устройствах. Пароль указывается явным образом (с помощью параметра /currpass), через *файл_с_текущим_паролем*, через *блок_зашифрованных_данных* или через *файл_с_блоком_зашифрованных_данных*.
/boot-clear	Удалить загрузчик системы шифрования из ОС.
/stop	Остановить процесс шифрования/расшифровки. 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 DeCrypt или после его перезагрузки необходимо выполнить команду /seed-get еще раз.

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

Для установки SoftControl DeCrypt и загрузчика системы шифрования:

```
"<каталог с установочным пакетом>\SoftControl DeCrypt Setup 5.0.18.exe" /q [/folder "<каталог для установки>"]
"<каталог установки SoftControl DeCrypt>\DcConsole.exe" /boot-prepare /newpassfile <файл_с_паролем>
```

Если для команды /boot-prepare используется параметр /newpass, пароль для шифрования/расшифровки диска будет лежать в файле скрипта или в журнале событий в открытом виде.

Для проверки состояния системы и запуска процесса шифрования (скрипт запускается после перезагрузки клиентского хоста):

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

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

Проверить состояние процесса шифрования можно с помощью команды `/state` (код возврата при завершении – `S.FULL_ENC (Fully encrypted)`).

4.7 Журналы

В SoftControl DeCrypt 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**: шифрование/расшифровка системного раздела или диска, установка/удаление загрузчика системы шифрования, изменение пароля, изменение набора аппаратных устройств.

Стандартный файл журнала доступен по следующему пути:

`C:\Windows\DecryptLog.log`

Расширенная информация о событиях системы шифрования 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 DeCrypt 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 шифрования (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 расшифровки 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 DeCrypt>\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) Выставите для параметра UsbInitDelay требуемое значение задержки (в секундах).

4.9 Генерация зашифрованных данных

Утилита *DcUtil.exe* предназначена для генерации блоков зашифрованных данных. При автоматизации управления системой шифрования SoftControl DeCrypt с помощью сторонних средств данная утилита позволяет безопасно пересылать пароли.

Утилита входит в дистрибутив SoftControl DeCrypt, однако не устанавливается на компьютер вместе с SoftControl DeCrypt. 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 DeCrypt следующую команду:

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

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

```
bb4e05cdc6c6bca94506b4dce81fd7791fa9cdff0...4258527h
```

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

Возможные команды для утилиты *DcUtil.exe* и их параметры перечислены в табл. 7.

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

Таблица 7. Параметры командной строки DcUtil.exe

Команда/Параметр	Действие/возможные значения
`/help`	Вывести список команд
`/encryptpasswords [/currpass` *`текущий_пароль`*`] [/newpass` *`новый_пароль`*`] (/seed` *`значение_seed`*`| /seedfile` *`файл_со_значением_seed`*`)`	Зашифровать текущий и/или новый пароль. Пароль можно задать следующими способами: a) указать явным образом *текущий_пароль* и *новый_пароль*. Формат задания пароля см. выше[27]. b) указать значение_seed, сгенерированное утилитой *DcConsole.exe* (см. выше[31]), с помощью параметра `/seed`. c) указать *файл_со_значением_seed*, сгенерированный утилитой *DcConsole.exe*, с помощью параметра `/seedfile`.

4.10 Истечение лицензии

После истечения лицензии SoftControl DeCrypt перестают работать следующие функции системы шифрования:

- Установка загрузчика системы шифрования.
- Шифрование диска.
- 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 DeCrypt (расшифровка диска, удаление загрузчика и др.) остаются доступными.

5. Обновление SoftControl DeCrypt

В данном разделе описаны необходимые действия по обновлению SoftControl DeCrypt:

- обновление в обычном режиме [33];
- обновление в тихом режиме [36].

Обновление можно проводить, не расшифровывая системный диск.

5.1 Обновление в обычном режиме

1) Запустите установочный пакет *SoftControl DeCrypt 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 [33]).

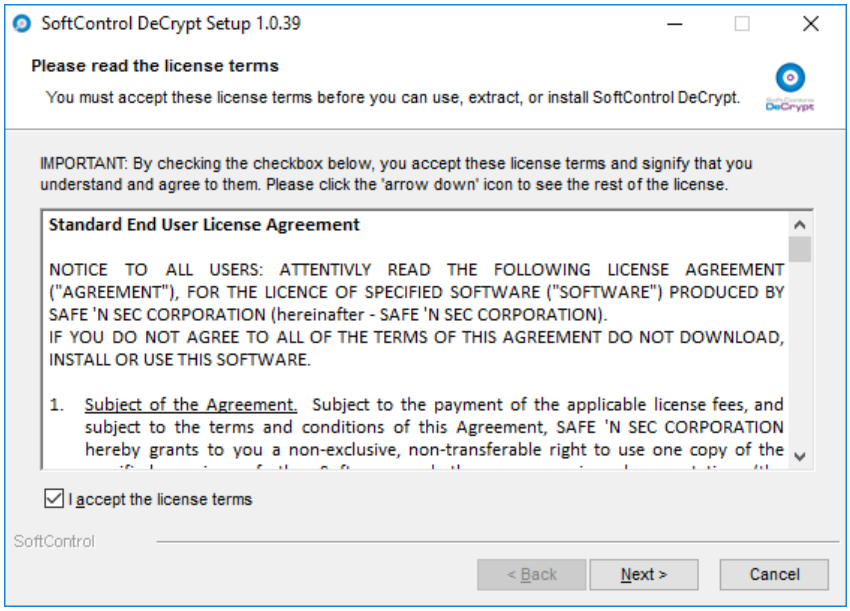

Рисунок 31. Лицензионное соглашение

3) Выберите требуемую опцию в окне **Wizard Mode** и нажмите **Next** (рис. Выбор режима [34]).

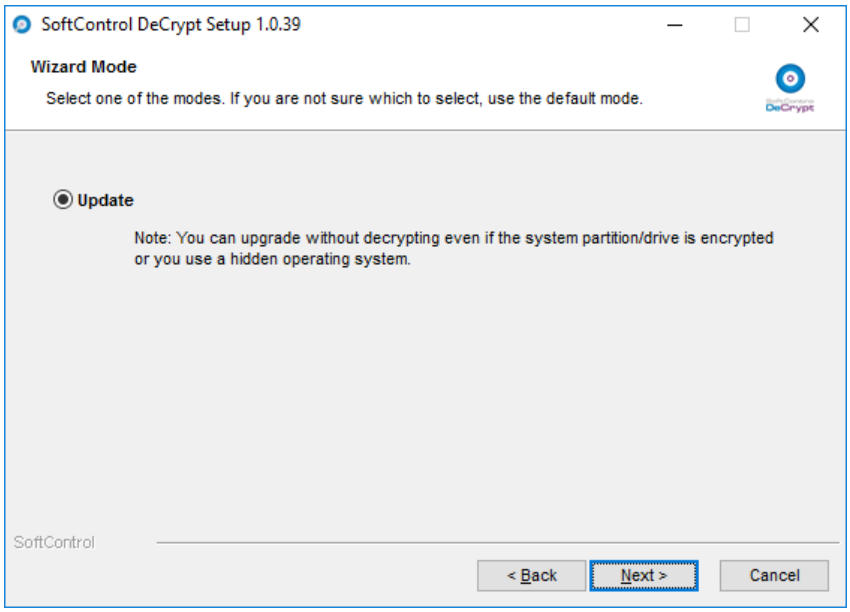

Рисунок 32. Выбор режима

4) Выберите требуемые опции в окне **Setup options** и нажмите **Update** (рис. Выбор опций [34]).

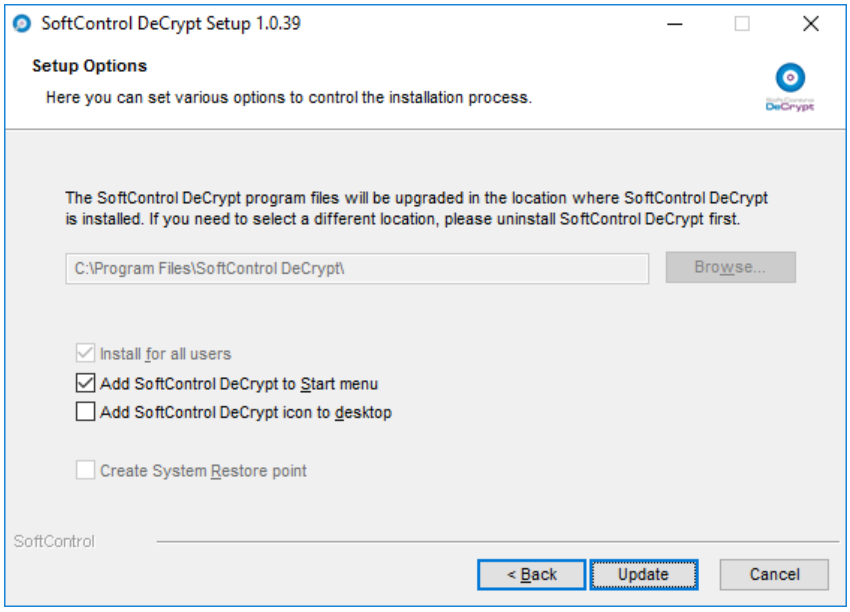

Рисунок 33. Выбор опций

5) Дождитесь окончания процесса обновления (рис. Процесс обновления [35]).

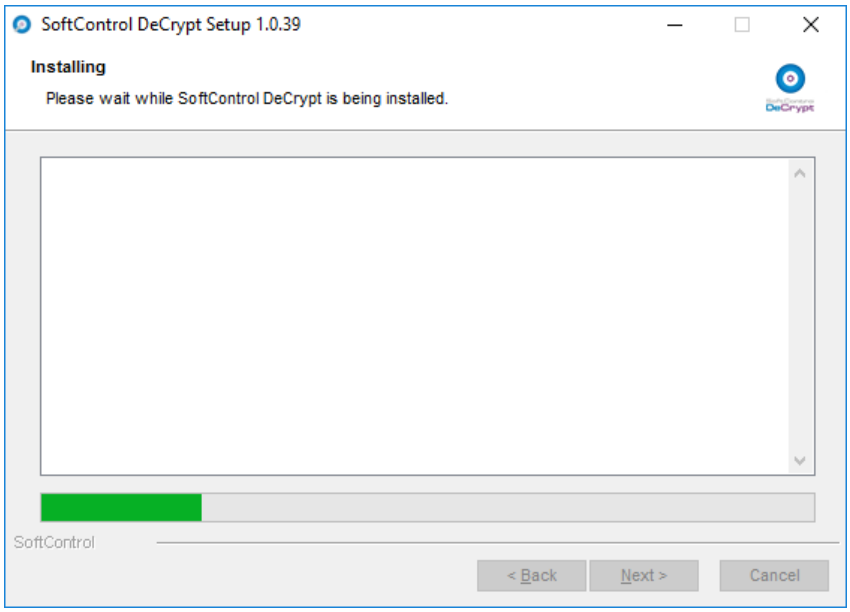

Рисунок 34. Процесс обновления

6) После появления сообщения **SoftControl DeCrypt has been successfully upgraded** (Установка SoftControl DeCrypt завершена) нажмите **Finish** (рис. Завершение обновления 35).

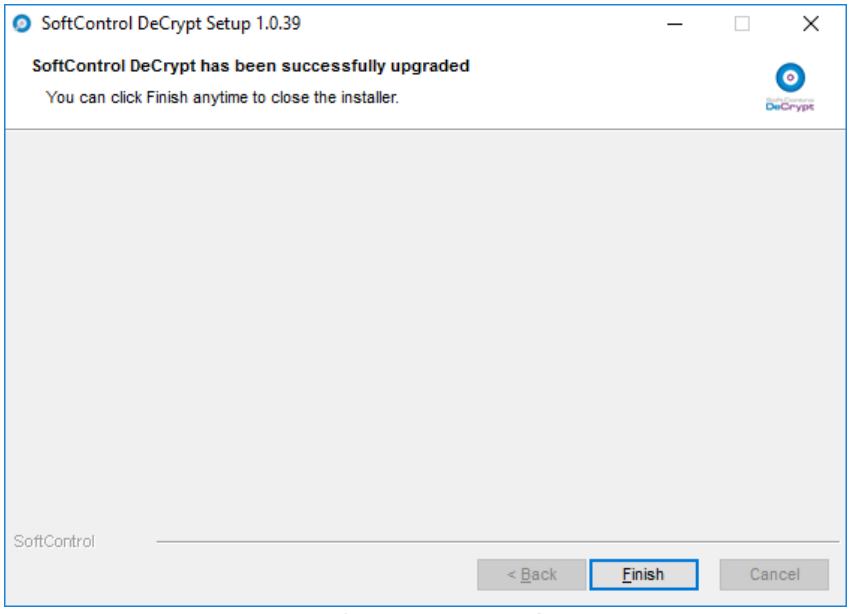

Рисунок 35. Завершение обновления

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 36).

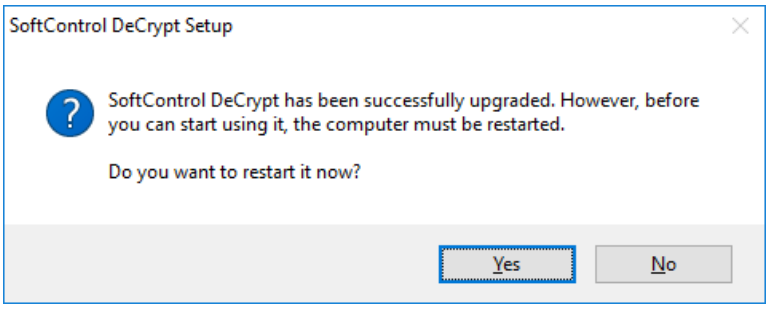

Рисунок 36. Запрос перезагрузки системы

5.2 Обновление в тихом режиме

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

1) Скопируйте установочный пакет *SoftControl DeCrypt 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 DeCrypt Setup <product version>.exe" /q
```

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

6. Удаление SoftControl DeCrypt

В данном разделе описана процедура деинсталляции SoftControl DeCrypt:

- в обычном режиме (с использованием интерфейса пользователя)[37];
- в тихом режиме[38].

Перед удалением SoftControl DeCrypt необходимо расшифровать[22] содержимое диска. В противном случае восстановить его содержимое будет невозможно.

6.1 Удаление в обычном режиме

1) Для ОС Microsoft® Windows® Server 2003: в Панели управления Windows в разделе **Установка и удаление программ** (Add or Remove Programs) на вкладке **Изменение или удаление программ** (Change or Remove Programs) выберите *SoftControl DeCrypt* и нажмите на кнопку **Удалить** (Remove).

   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 DeCrypt* и нажмите **Удалить** (Uninstall).

2) В появившемся окне нажмите **Удалить** (рис. Подтверждение удаления программы[37]).

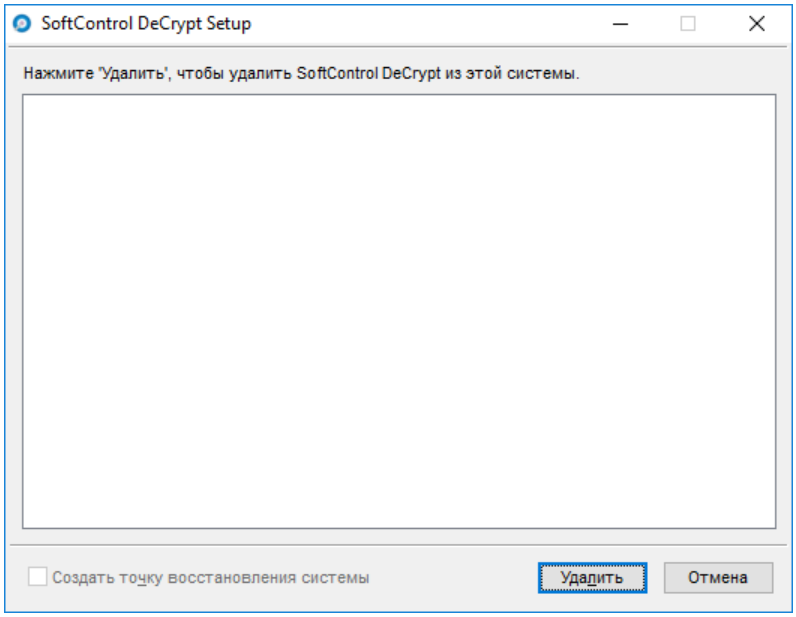

Рисунок 37. Подтверждение удаления программы

Примечание: Если вы добавляли какие-либо файлы в папку с SoftControl DeCrypt, она не будет удалена.

Нажмите **Готово** для завершения удаления программы (рис. Завершение удаления программы 38).

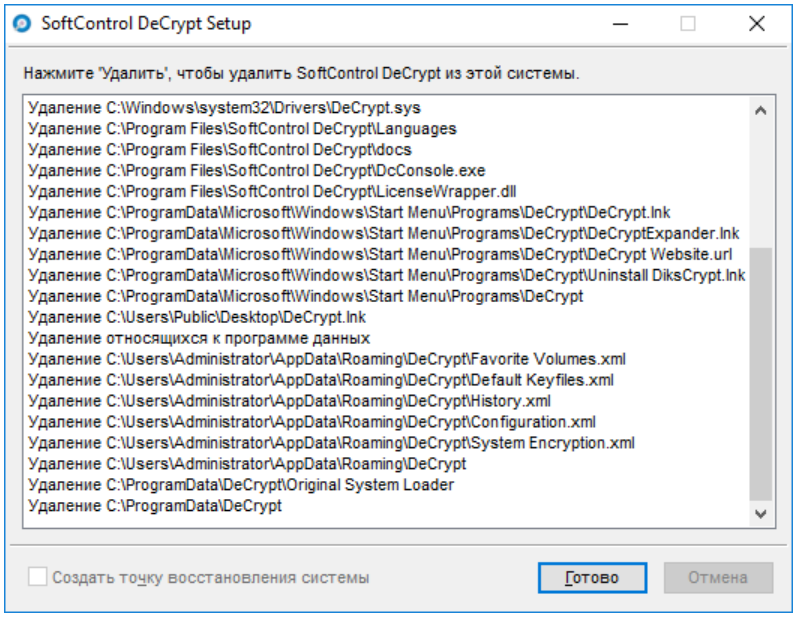

Рисунок 38. Завершение удаления программы

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 DeCrypt>\SoftControl DeCrypt Setup.exe" /q /u
```

7. Техническая поддержка

При возникновении вопросов по установке, настройке и работе SoftControl DeCrypt вы можете обращаться в техническую поддержку по электронной почте support@safensoft.com.

8. Приложение

8.1 Настройка раздела диска

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

Если инсталлятор SoftControl DeCrypt 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 DeCrypt. 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`.