

МИНИСТЕРСТВО ОБРАЗОВАНИЯ И НАУКИ РОССИЙСКОЙ  
ФЕДЕРАЦИИ  
ФЕДЕРАЛЬНОЕ ГОСУДАРСТВЕННОЕ БЮДЖЕТНОЕ  
ОБРАЗОВАТЕЛЬНОЕ УЧРЕЖДЕНИЕ  
ВЫСШЕГО ОБРАЗОВАНИЯ  
«ИЖЕВСКИЙ ГОСУДАРСТВЕННЫЙ ТЕХНИЧЕСКИЙ УНИВЕРСИТЕТ  
им. М.Т. Калашникова»

Факультет «Информатики и вычислительной техники»  
Кафедра «Защита информации в компьютеризированных системах»

Пояснительная записка к курсовой работе по дисциплине  
«Разработка и эксплуатация защищенных автоматизированных систем»  
на тему «Внедрение и эксплуатация СЗИ от НСД Dallas Lock 8.0 - К»

Выполнил:

студент группы С09-361-1

Максимова А.В.

Проверил:

к.т.н, доцент

Стукалина Е. Ф.

Ижевск 2017

## Содержание

Введение .....	3
1. Основные сведения о продукте Dallas Lock 8.0 .....	4
2. Установка СЗИ Dallas Lock 8.0 .....	6
2.1. Подготовка компьютера к установке .....	6
2.2. Установка системы защиты.....	9
3. Очистка остаточной информации в СЗИ Dallas Lock 8.0 .....	15
3.1. Настройка .....	16
3.1.1. Регистрация действий по очистке остаточной информации .....	16
3.1.2. Параметры очистки остаточной информации.....	17
3.1.3. Запрет смены пользователя без перезагрузки.....	19
3.2. Эксплуатация .....	21
3.2.1. Удаление файлов и зачистка остаточной информации.....	21
3.2.2. Зачистка диска .....	23
Заключение .....	25
Используемая литература.....	26

## Введение

Актуальность проблемы защиты конфиденциальной информации с каждым годом набирает обороты. Документооборот и информационные потоки всё больше уходят в область электронной сферы, как никогда остро стоит вопрос о создании комплексной, централизованной и всеобъемлющей системы контроля над информацией, циркулирующей внутри локальных сетей предприятий.

Одной из причин непреднамеренного распространения конфиденциальной и секретной информации является игнорирование очистки остаточной информации в ОС. При удалении файла удаляется лишь запись о файле из директории файловой системы, но реальное содержимое остается на запоминающем устройстве, и его можно достаточно легко просмотреть до тех пор, пока операционная система заново не использует это пространство для хранения новых данных.

В данной курсовой работе рассматривается система защиты информации от НСД Dallas Lock 8.0-К, включающая подсистему очистки остаточной информации, которая гарантирует предотвращение восстановления удаленных данных.

## 1. Основные сведения о продукте Dallas Lock 8.0

Dallas Lock 8.0 – сертифицированная система защиты информации накладного типа для автономных и сетевых АРМ (применима для сложных сетевых инфраструктур)[1].

Предназначена для защиты конфиденциальной информации (редакции «К» и «С»), в том числе содержащейся в автоматизированных системах (АС) до класса защищенности 1Г включительно, в государственных информационных системах (ГИС) до 1 класса защищенности включительно, в информационных системах персональных данных (ИСПДн) для обеспечения 1 уровня защищенности ПДн, в автоматизированных системах управления производственными и технологическими процессами (АСУ ТП) до 1 класса защищенности включительно.

Использование СЗИ необходимо в соответствии с закрепленными в приказах и руководящих документах регулятора группами мер, которые являются обязательными для выполнения:

- идентификация и аутентификация в информационной системе,
- управление доступом к компонентам информационной системы и информационным ресурсам,
- ограничение программной среды,
- регистрация событий безопасности в информационной системе,
- обеспечение целостности информационной системы и информации.

Указанные группы мер должны быть реализованы в ИСПДн (Приказ ФСТЭК России № 21)[5], в ГИС (Приказ ФСТЭК России № 17)[6], в АСУ ТП (Приказ ФСТЭК России № 31)[7], а также в автоматизированных системах классов 1Д и выше (Руководящий документ. Автоматизированные системы. Защиты от несанкционированного доступа к информации. Классификация автоматизированных систем и требования по защите информации).

СЗИ Dallas Lock отмечена в государственном реестре сертифицированных средств защиты информации на сайте ФСТЭК[2]:

Наименование	Значение
№ сертификата	2720
Дата внесения в реестр	25.09.2012
Срок действия сертификата	25.09.2018
Наименование средства (шифр)	«Dallas Lock 8.0-К»
Предназначение средства	Система защиты информации от несанкционированного доступа «Dallas Lock 8.0-К»- по 4 уровню контроля НДВ, по 5 классу СВТ, по 3 классу РД МЭ, Требования к СКСМНИ (ИТ.СКН.П4.ПЗ) по 4 классу защиты, Требования к СОВ уровня узла 4 класса
Схема сертификации	серия
Испытательная лаборатория	ЗАО «Лаборатория ППШ»
Орган по сертификации	ЗАО «НПО «Эшелон»
Заявитель	ООО «Конфидент»
Реквизиты заявителя	192029, г. Санкт-Петербург, пр. Обуховской обороны, д. 51, лит. К, (812) 325 1037

Система защиты Dallas Lock 8.0 состоит из следующих основных компонентов:

1. Программное ядро (Драйвер защиты).
2. Подсистема администрирования.
3. Подсистема управления доступом.
4. Подсистема регистрации и учета.
5. Подсистема идентификации и аутентификации.
6. Подсистема гарантированной зачистки информации.
7. Подсистема преобразования информации.
8. Подсистема контроля устройств.
9. Подсистема межсетевого экранирования.
10. Подсистема контроля целостности.
11. Подсистема восстановления после сбоев.
12. Подсистема развертывания (установочные модули).

## 2. Установка СЗИ Dallas Lock 8.0

### 2.1. Подготовка компьютера к установке

Система защиты Dallas Lock 8.0 может быть установлена на персональные компьютеры, портативные и мобильные ПК (ноутбуки и планшетные ПК), сервера (файловые, контроллеры домена, терминального доступа) и виртуальные машины (например, VMware), работающие как в автономном режиме, так и в составе локально-вычислительной сети.

Система защиты Dallas Lock 8.0 может работать на любом компьютере, работающем под управлением следующих ОС:

- Windows XP (SP 3) (Professional, Home, Starter);
- Windows Server 2003 (R2) (SP 2) (Web, Standard, Enterprise, Datacenter);
- Windows Vista (SP 2) (Ultimate, Enterprise, Business, Home Premium, Home Basic, Starter);
- Windows Server 2008 (SP 2) (Standard, Enterprise, Datacenter, Web Server 2008, Storage Server 2008);
- Windows 7 (SP 1) (Ultimate, Enterprise, Professional, Home Premium, Home Basic, Starter);
- Windows Server 2008 R2 (SP 1) (Foundation, Standard, Web, Enterprise, Datacenter);
- Windows 8 (Core, Pro, Enterprise);
- Windows Server 2012 (Foundation, Essentials, Standard, Datacenter);
- Windows 8.1 (Core, Pro, Enterprise);
- Windows Server 2012 (R2) (Foundation, Essentials, Standard, Datacenter);
- Windows 10.

Система защиты Dallas Lock 8.0 поддерживает 32- и 64-битные версии ОС Windows.

Система защиты Dallas Lock 8.0 имеет следующие ограничения при установке:

1. При наличии на компьютере нескольких жестких дисков, операционная система должна быть установлена на первый жесткий диск.
2. При наличии на жестком диске нескольких разделов, операционная система должна быть установлена на диск С.
3. Установка Dallas Lock 8.0 всегда производится в каталог C:\DLLOCK80.
4. На время установки и удаления СЗИ НСД необходимо отключить программные антивирусные средства.

Перед установкой системы защиты Dallas Lock 8.0 необходимо выполнить следующие действия:

1. Если на компьютере уже установлена система защиты, ее необходимо удалить.
2. Необходимо убедиться, что на диске С имеется необходимое свободное пространство для установки системы защиты.
3. Проверить состояние жестких дисков компьютера, например, при помощи приложения chkdsk.exe или служебной программы проверки диска из состава ОС Windows, и устранить выявленные дефекты.
4. Рекомендуется произвести дефрагментацию диска.
5. Проверить компьютер на отсутствие вирусов.
6. Перед установкой системы защиты необходимо выгрузить из памяти все резидентные антивирусы.
7. Закрывать все запущенные приложения, так как установка системы потребует принудительной перезагрузки.

Пользователь, установивший систему защиты, автоматически становится привилегированным пользователем – суперадминистратором.

Необходимо запомнить имя и пароль этого пользователя, так как некоторые операции можно выполнить только из-под его учетной записи. Изменять учетную запись суперадминистратора средствами Windows запрещено.



## 2.2. Установка системы защиты

Установка производится на ОС Windows 7 Professional Service Pack 1.

1. Для установки СЗИ НСД Dallas Lock 8.0 необходимо запустить приложение DallasLock8.0C.msi (DallasLock8.0K.msi), которое находится в корневой директории дистрибутива (или выбрать данное действие в меню окна autorun).



Рис. 2.1 – Окно autorun с вариантом установки

2. Выберем установку Dallas Lock 8.0-K. Запустится программа установки (Рис. 2.2)

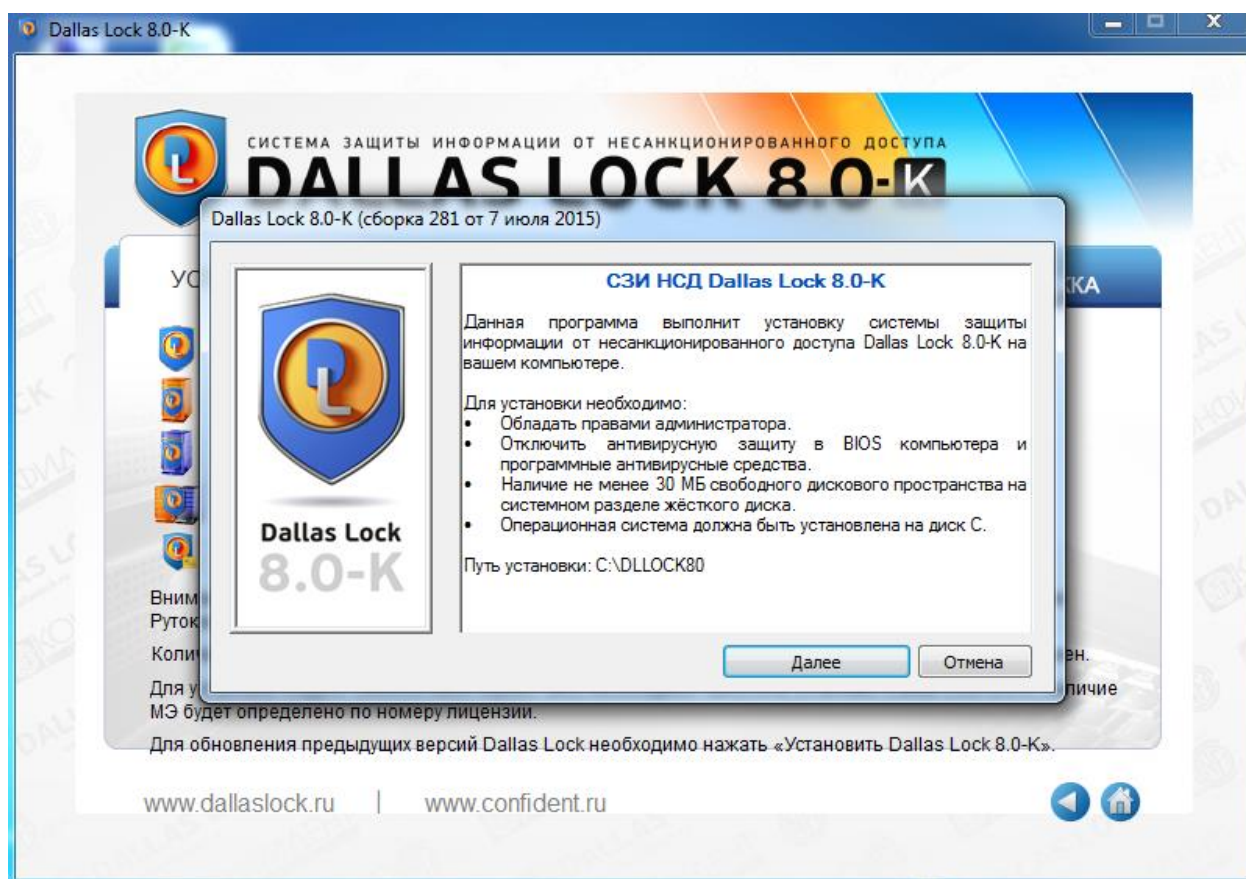


Рис. 2.2 – Окно начала установки системы защиты

3. Для установки необходимо нажать кнопку «Далее», после чего программа установки приступит к инсталляции. На данном этапе программа установки попросит осуществить ввод параметров установки (Рис. 2.3).

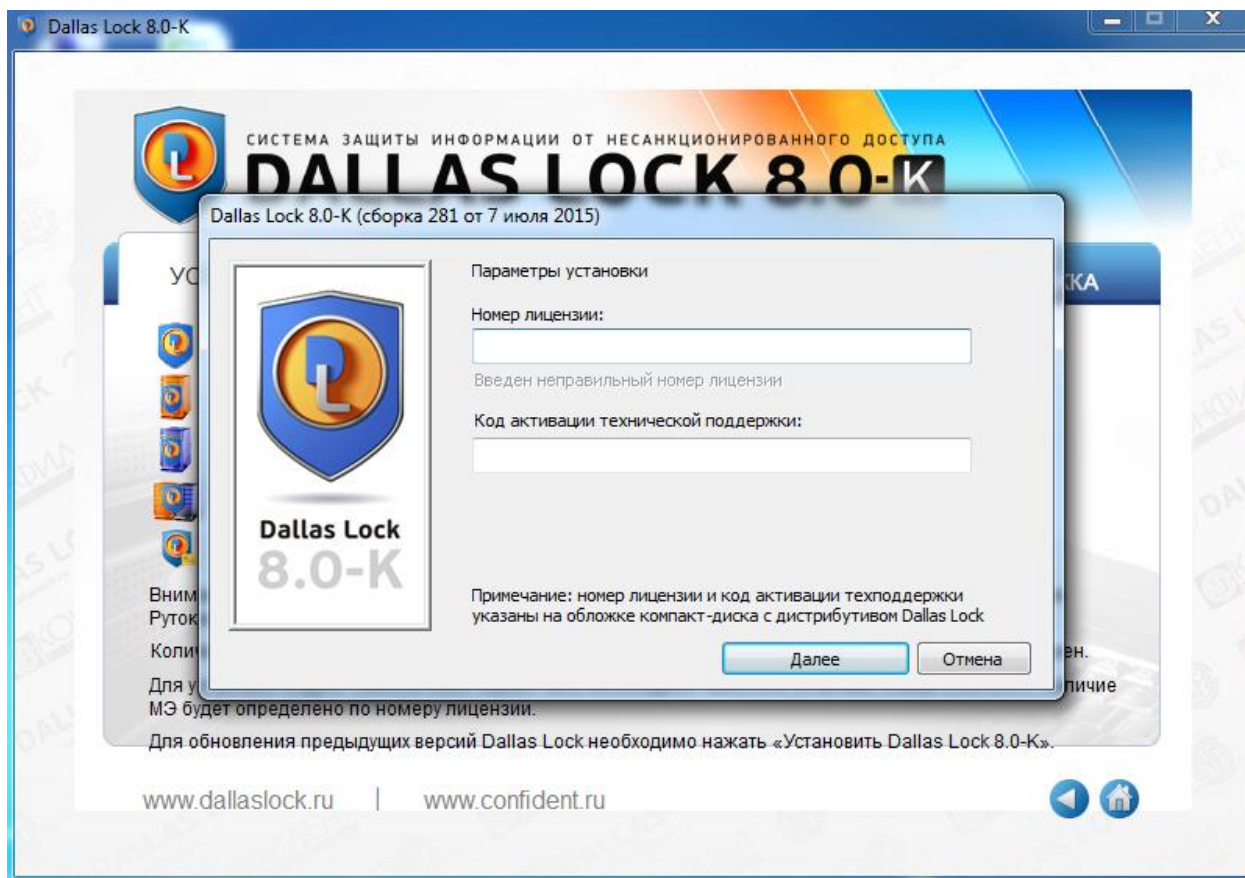


Рис. 2.3 – Ввод параметров установки

4. Для защиты от нелегального использования продукта необходимо ввести номер лицензии Dallas Lock 8.0 и код технической поддержки, которые указаны на обложке компакт-диска с дистрибутивом в соответствующих полях.

5. В том случае, когда необходимо ввести компьютер в Домен безопасности в процессе установки системы, то в соответствующие поля необходимо ввести имя Сервера безопасности и его ключ доступа. Если этого не сделать на этапе установки, то компьютер не будет введен в Домен безопасности, но это можно будет сделать и после установки СЗИ НСД.



Рис. 2.4 – Введение в домен безопасности на этапе установки

6. После нажатия кнопки «Далее» процесс установки системы защиты будет завершен. После нажатия кнопки «Перезагрузка» через 30 секунд произойдет автоматическая перезагрузка ПК (Рис. 2.5).





Рис. 2.5 – Завершение установки программы

После перезагрузки первый вход на защищенный компьютер сможет осуществить пользователь, под учетной записью которого выполнялась инсталляция системы защиты Dallas Lock 8.0.

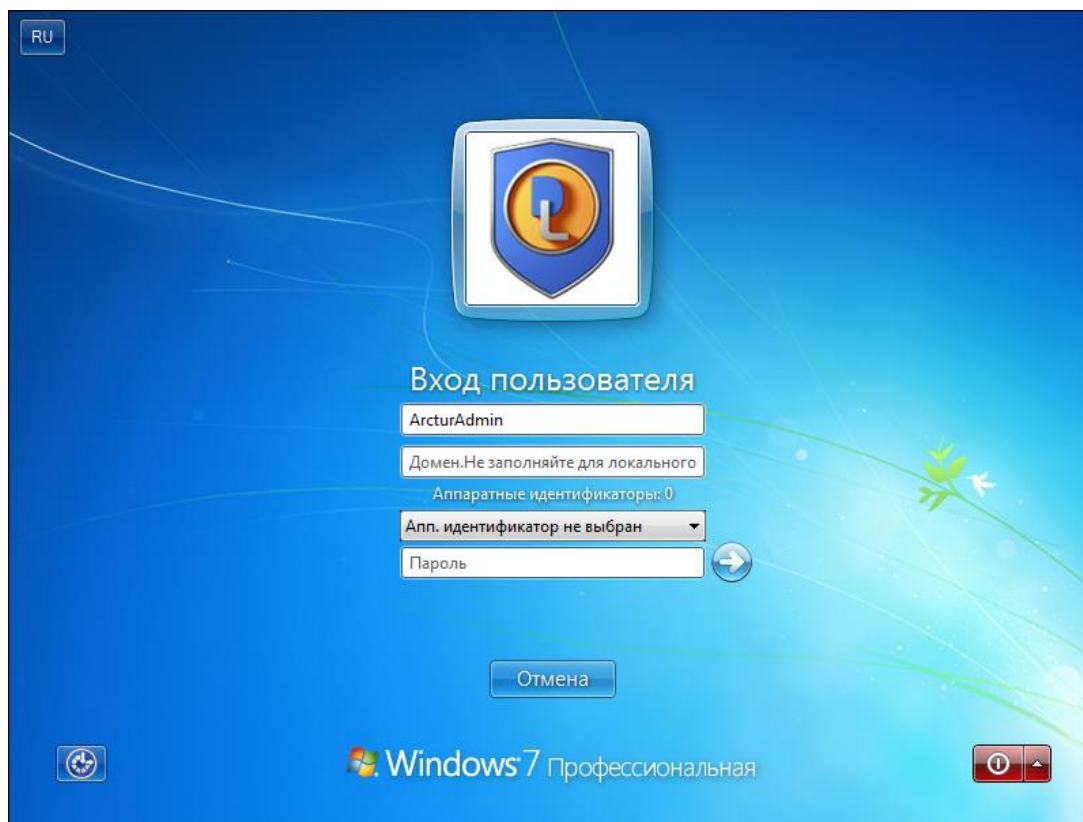


Рис. 2.6 – Окно авторизации пользователя после успешной установки Dallas Lock 8.0.

После установки системы защиты и перезагрузки компьютера в меню «Пуск» появится ярлык оболочки администратора СЗИ НСД Dallas Lock 8.0.

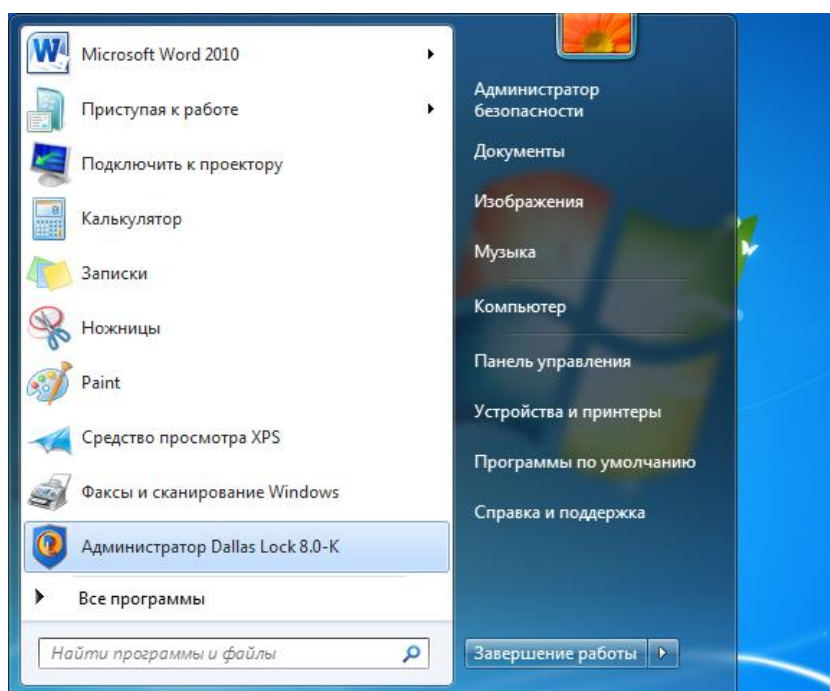


Рис. 2.7 – Ярлык оболочки администратора в меню «Пуск»

### 3. Очистка остаточной информации в СЗИ Dallas Lock 8.0

Большинство операционных систем при удалении файла не удаляют содержимое файла непосредственно, а всего лишь удаляют запись о файле из директории файловой системы. Так сделано для ускорения работы системы.

Реальное содержимое файла остается на запоминающем устройстве, и его можно достаточно легко просмотреть, по крайней мере, до тех пор, пока операционная система заново не использует это пространство для хранения новых данных. Данная остаточная информация может легко привести к непреднамеренному распространению конфиденциальной и секретной информации.

СЗИ НСД Dallas Lock 8.0 включает подсистему очистки остаточной информации. Возможности подсистемы:

- Затирать всю остаточную информацию при освобождении областей на дисках, т.е. при удалении файлов или при перемещении файлов или при уменьшении размеров файлов.
- Затирать всю остаточную информацию в файле подкачки Windows. Затирание производится записью маскирующей последовательности поверх файла подкачки. Очистка производится при завершении работы (закрытии файла подкачки) и, если очистка была прервана, при старте системы (открытии файла подкачки).
- Принудительно зачищать конкретную папку/файл, выбрав соответствующий пункт в контекстном меню данного файла.
- Проверять корректное завершение процесса очистки информации.
- Предотвращать возможность завершения сеанса работы одного пользователя и начала работы другого без перезагрузки, что гарантирует освобождение используемых областей оперативной памяти, с помощью параметра «Запрет смены пользователя без перезагрузки».

### 3.1. Настройка

#### 3.1.1. Регистрация действий по очистке остаточной информации

Для того чтобы фиксировать события зачистки остаточной информации (успешные и неуспешные), необходимо включить (значение «Вкл.») отвечающий за это параметр аудита: «Параметры безопасности» => «Аудит» => параметр «Аудит событий зачистки».

При включенном данном параметре события очистки остаточной информации, будут заноситься в журнал ресурсов, который также должен быть включен («Параметры безопасности» => «Аудит» => параметр «Журнал ресурсов», значение «Вкл.»).

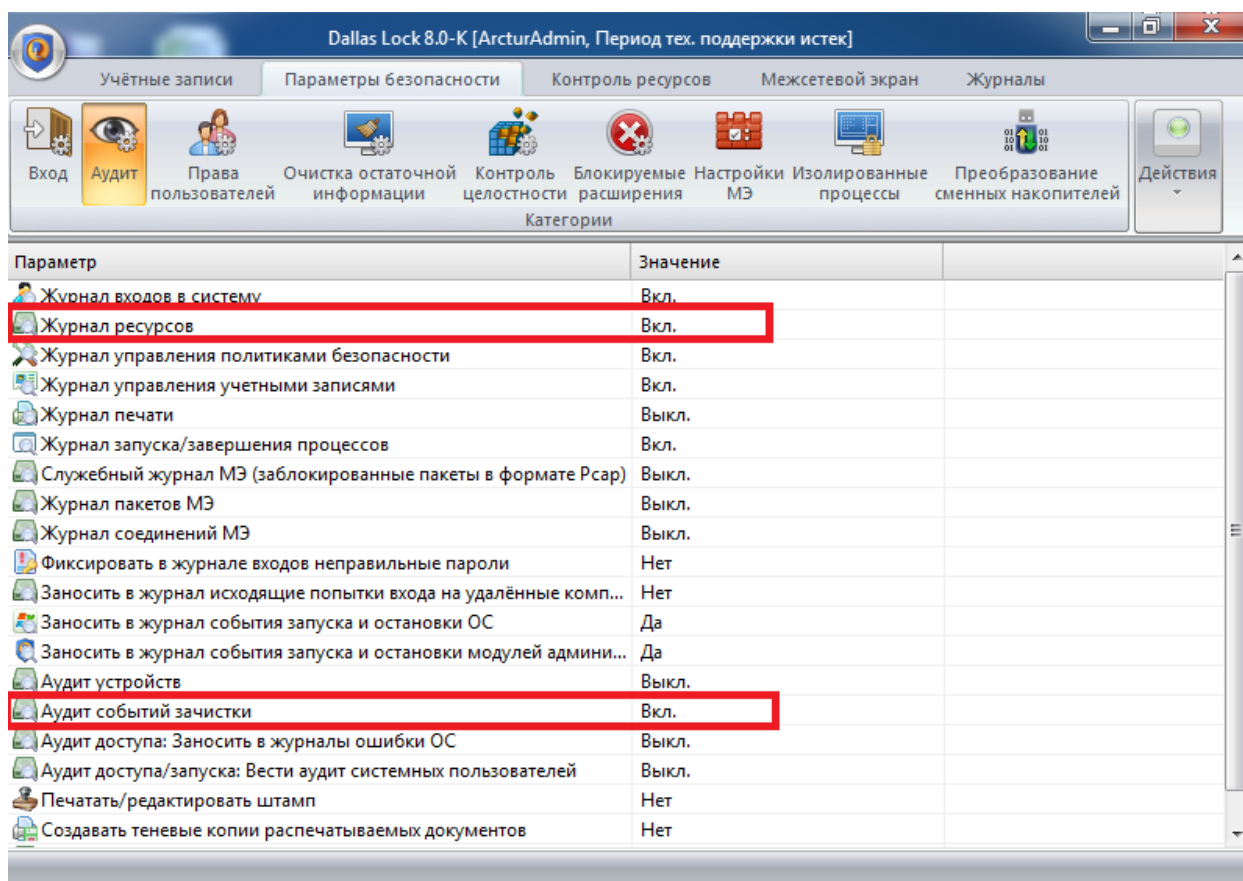


Рис. 3.1 – Параметры аудита СЗИ Dallas Lock 8.0 – К





2. «Очищать файл подкачки виртуальной памяти». Включение параметра позволяет автоматически затирать всю остаточную информацию в файле подкачки Windows. Затирание производится записью маскирующей последовательности поверх файла подкачки. Очистка производится при завершении работы (закрытии файла подкачки) и, если очистка была прервана, при старте системы (открытии файла подкачки).

3. «Проверять очистку информации». При включении параметра после проведения очистки объектов ФС, дополнительно выполняется проверка того, что очистка действительно осуществлена. В случае если проверка выявила, что очистка не осуществлена или завершена с ошибкой, то в журнал ресурсов заносится соответствующее событие. Проверка осуществляется при очистке остаточной информации, выполняемой по команде администратора, в автоматическом режиме, и при зачистке накопителя целиком

4. «Количество циклов затирания». Данным параметром устанавливается число циклов затирания, от которого зависит степень надежности зачистки информации и время процедуры зачистки.

5. «Затирающая последовательность». Данным параметром определяется метод затирания остаточной информации путем установки числовых байтовых значений (от 0 до F) для каждого из четырех циклов затирания. Если эти значения не установлены, или установлены не для каждого цикла, то по умолчанию для затирающей последовательности циклов используется последовательность, установленная в Dallas Lock.

### 3.1.3. Запрет смены пользователя без перезагрузки

В соответствии с требованиями политик безопасности организации возможно включение запрета смены пользователя компьютером без его перезагрузки.

Чтобы установить данный запрет необходимо включить параметр входа «Вход: запрет смены пользователя без перезагрузки» («Параметры безопасности» => «Вход»). Параметр может принимать значение «Включен» или «Выключен». Включение данной политики («Вкл.») не позволит осуществить смену пользователя без перезагрузки компьютера.

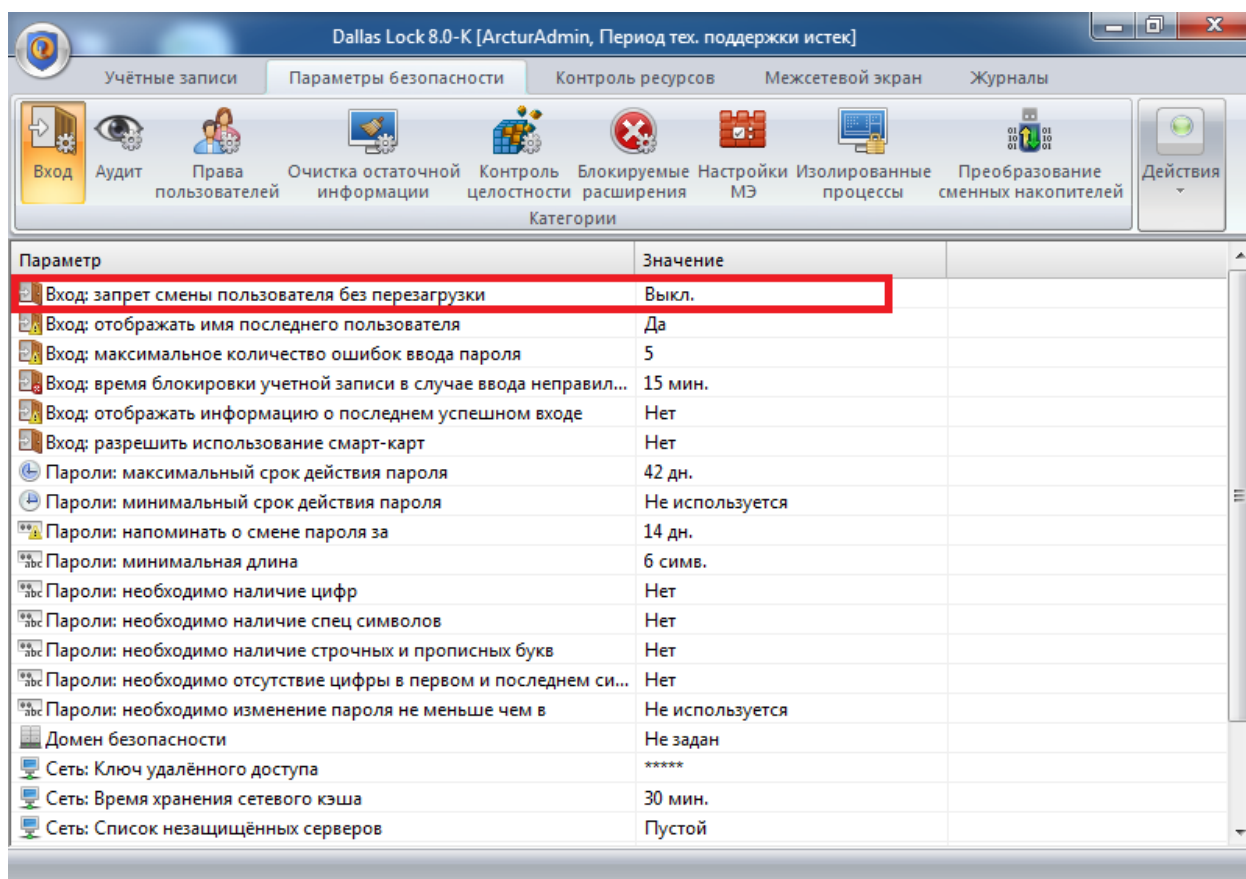


Рис. 3.3 – Параметры безопасности

Если установлено значение «Включен», то при выборе пункта «Завершение сеанса» в окне «Завершение работы Windows», компьютер автоматически уйдет на перезагрузку (Рис. 3.4).

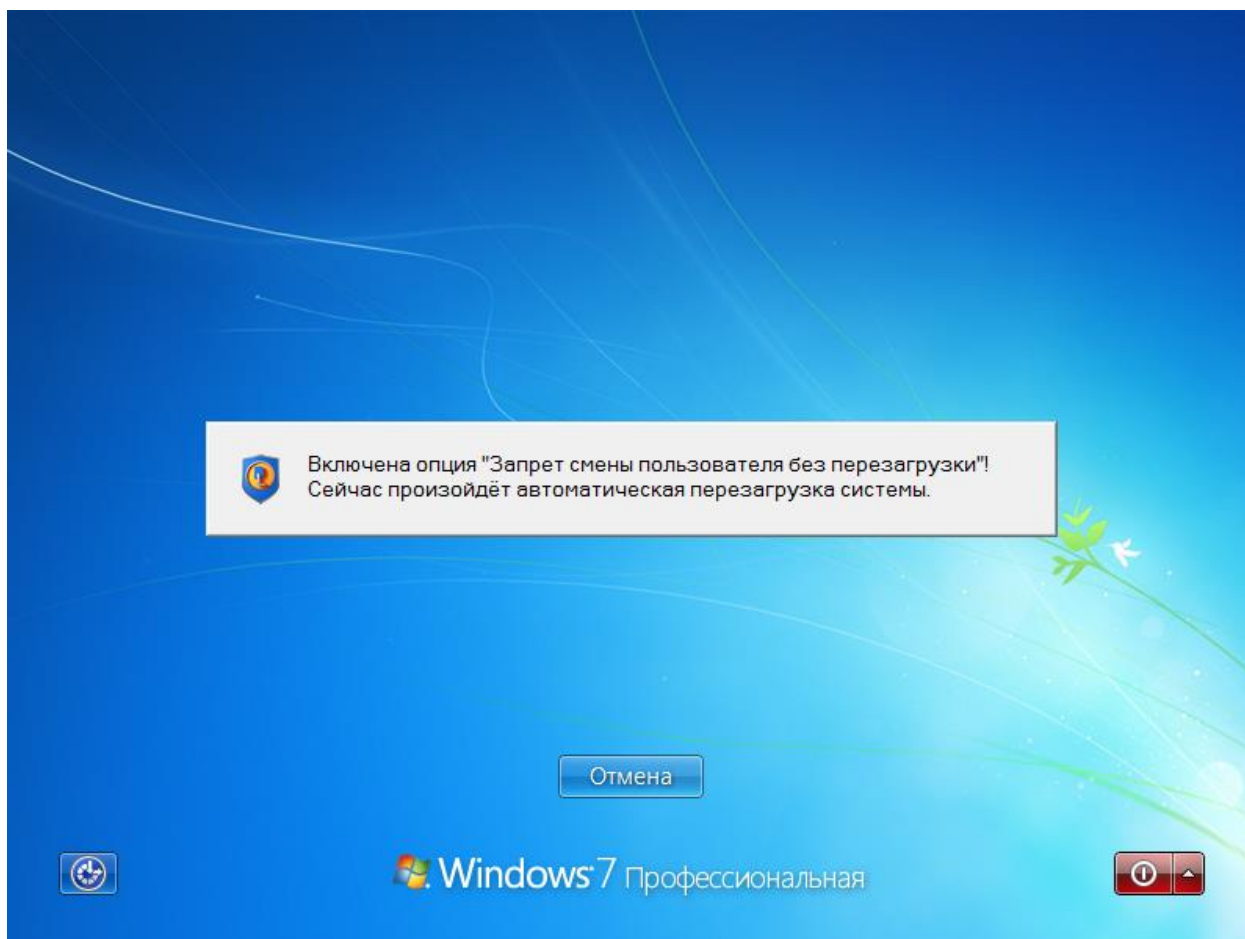


Рис. 3.4 – Сообщение системы об автоматической перезагрузке

Данная политика позволяет предотвратить теоретическую возможность извлечения какой-либо информации из оперативной памяти ПК, оставшуюся там после завершения сеанса работы другого пользователя.

## 3.2. Эксплуатация

### 3.2.1. Удаление файлов и зачистка остаточной информации

При необходимости удалить какие-либо данные без возможности их восстановления нужно воспользоваться контекстным меню данного объекта файловой системы и выбрать пункт «DL8.0: Удалить и зачистить» (Рис. 3.5):

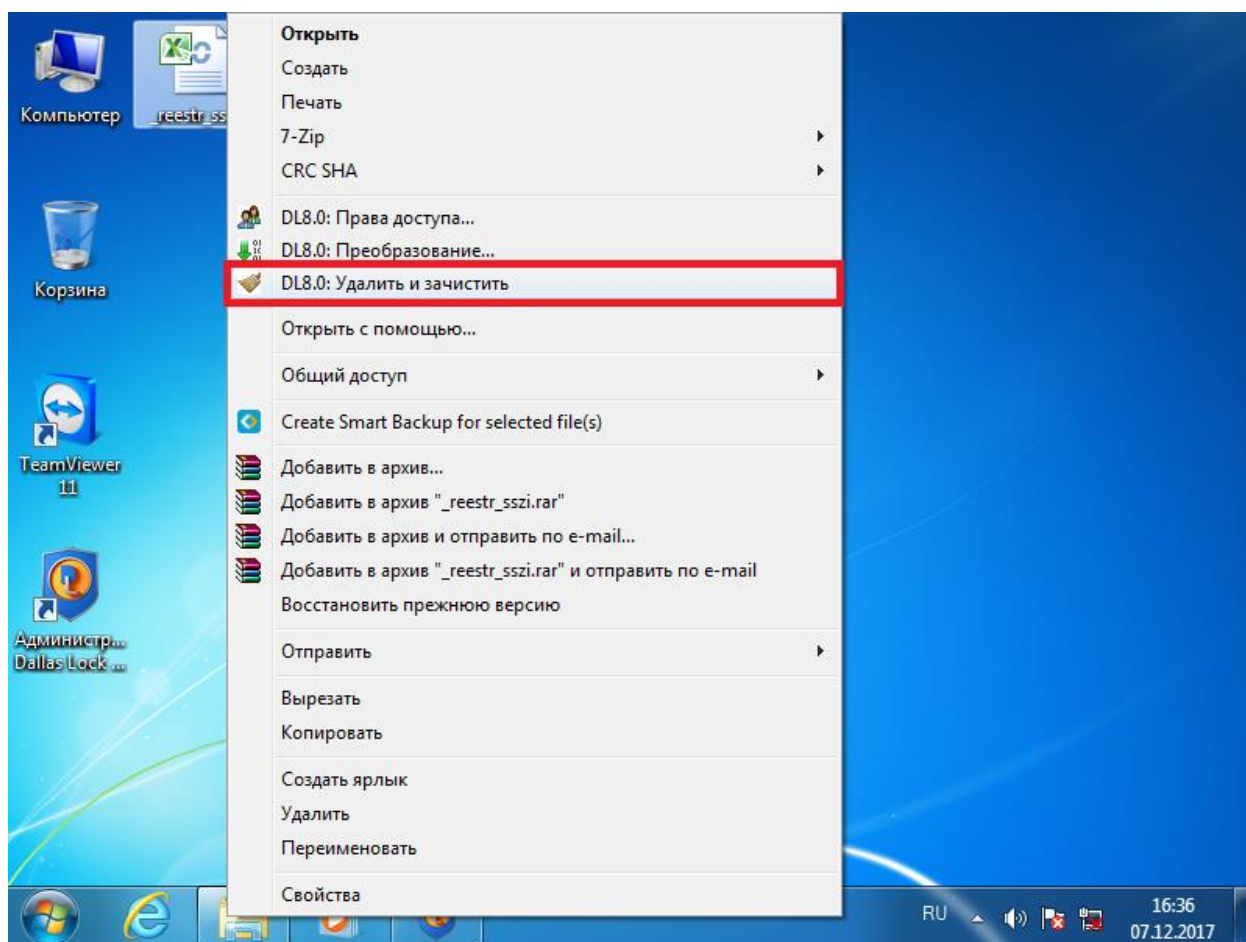


Рис. 3.5 – Контекстное меню

Появится окно с просьбой подтвердить операцию (Рис. 3.6).

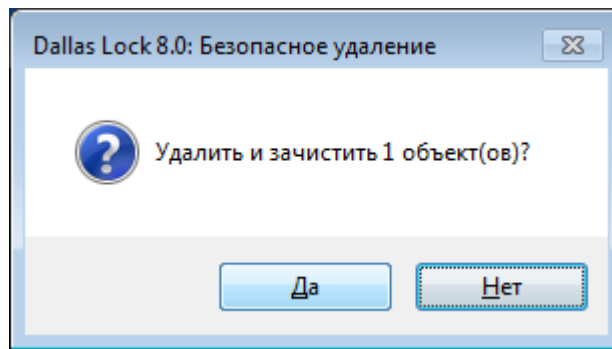


Рис. 3.6 – Подтверждение удаления файла

При активации удаления происходит зачистка данного объекта путем перезаписи файла. Количество циклов затирания определяется соответствующей политикой. После перезаписи восстановить хоть сколько-нибудь значимый фрагмент файла становится практически невозможно. После успешного удаления объектов система выведет соответствующее подтверждение (Рис3.7).

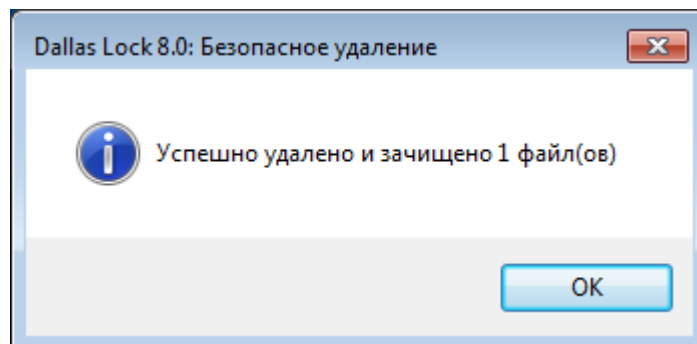



Рис. 3.7 – Сообщение системы об успешном удалении

### 3.2.2. Зачистка диска

Система защиты Dallas Lock 8.0 позволяет полностью зачищать остаточные данные всего диска или его разделов. Для этого служит функция «Зачистка диска». Данная функция может применяться к разделам фиксированных и съемных жестких дисков и к USB-Flash-накопителям. Системный раздел с установленной операционной системой для данной операции будет недоступен.

Зачистка диска может быть полезна при снятии носителей с учета и необходимости полного удаления данных без возможности их восстановления по остаточной информации.

Для вызова данной функции необходимо в оболочке администратора нажать кнопку  основного меню и в списке дополнительных функций выбрать пункт «Зачистка диска» (Рис. 3.8).

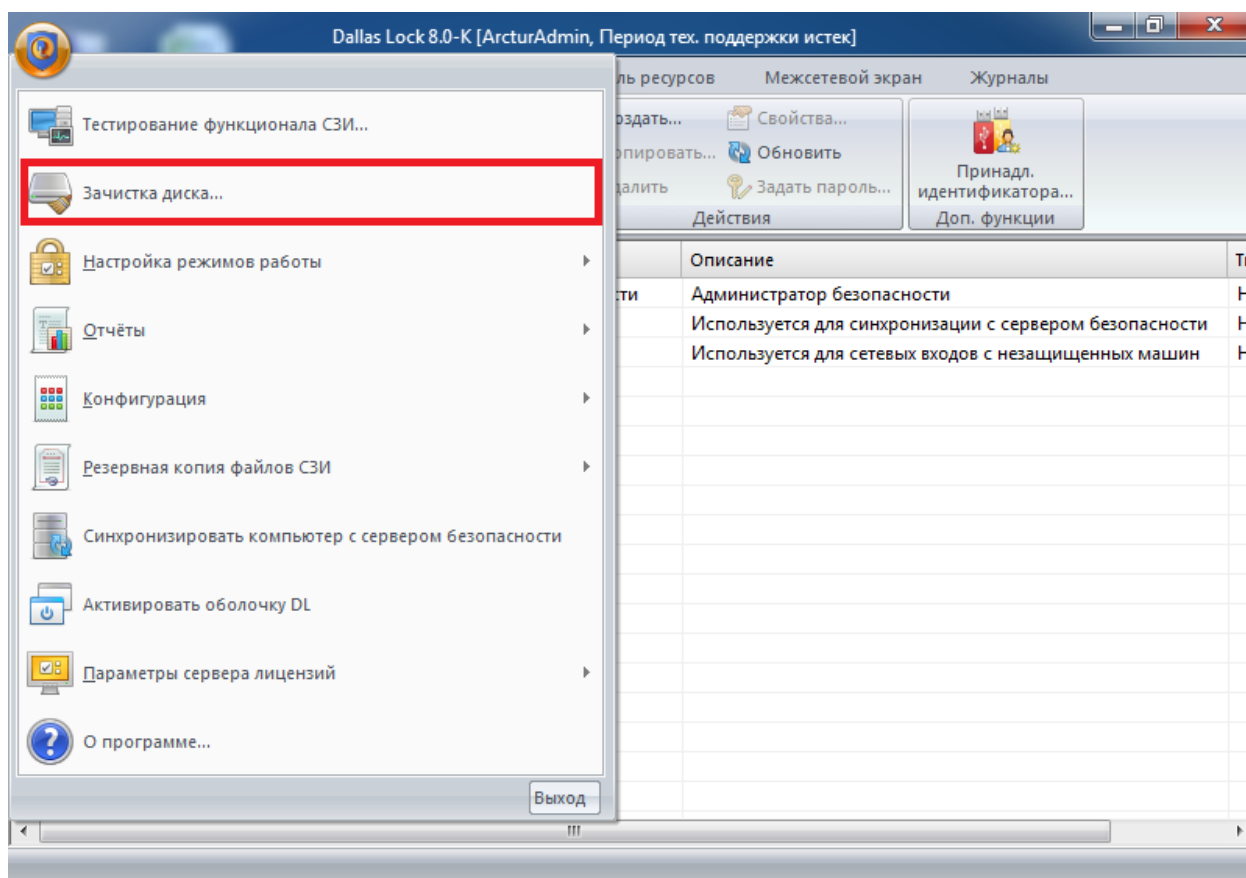


Рис. 3.8 – Выбор функции «Зачистка диска»

Появится окно, в котором необходимо выбрать жесткий диск из списка обнаруженных в системе и нажать «Зачистить».

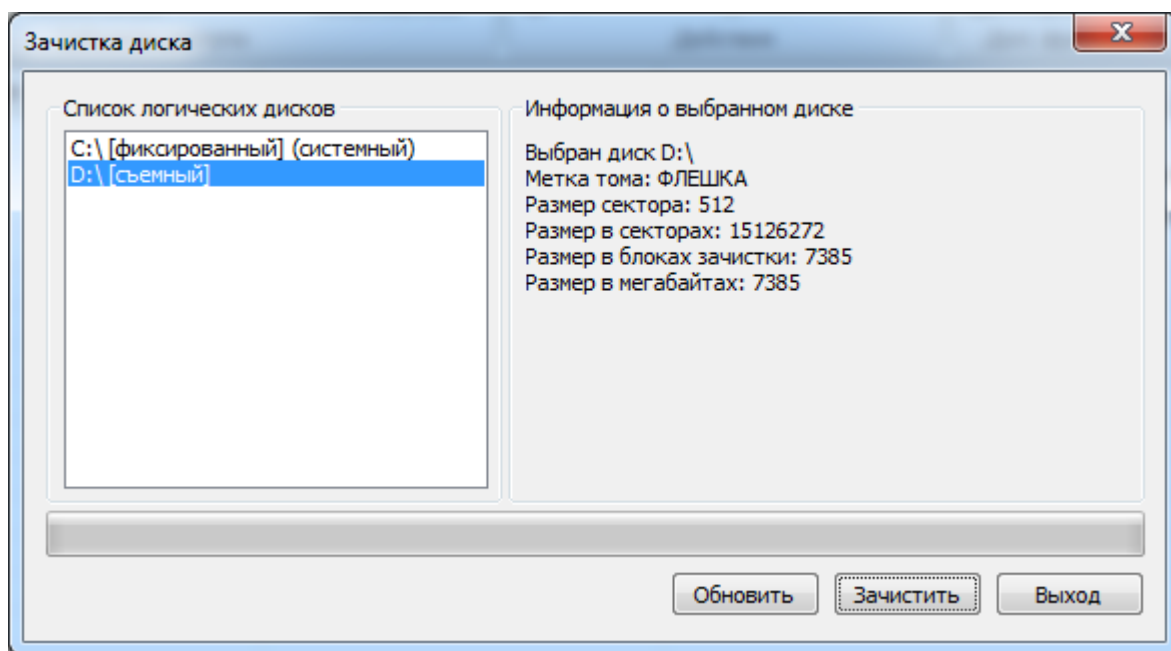


Рис. 3.9 – Окно зачистки диска

Запустится процесс зачистки остаточных данных жесткого диска. Процесс будет сопровождаться заполнением полосы индикатора прогресса. По окончании процесса на экран будет выведено сообщение об успешном окончании операции.



## Заключение

В результате выполнения данной курсовой работы были разработаны руководства по установке, настройке и эксплуатации подсистемы очистки остаточной информации СЗИ НСД Dallas Lock 8.0. Система обеспечивает защиту информации от несанкционированного доступа на ПК в ЛВС через локальный, сетевой и терминальный входы. Подсистема гарантирует предотвращение восстановления удаленных данных, очистку остаточной информации при смене пользователя, зачистку диска и регистрацию действий по очистке.

## Используемая литература

1. <https://dallaslock.ru/products/szi-nsd-dallas-lock/> - СЗИ Dallas Lock (дата обращения 04.12.2017)
2. <http://fstec.ru/tekhnicheskaya-zashchita-informatsii/dokumenty-po-sertifikatsii/153-sistema-sertifikatsii/591-gosudarstvennyj-reestr-sertifitsirovannykh-sredstv-zashchity-informatsii-n-ross-ru-0001-01bi00> - ФСТЭК. Реестр сертифицированных средств защиты информации (дата обращения 04.12.2017)
3. ГОСТ Р ИСО/МЭК 15910-2002 «Информационная технология. Процесс создания документации пользователя программного средства»
4. <http://www.online-academy.ru/demo/docs/urok1/index.html> - Курс «Этапы работы над пользовательской документацией» (дата обращения 04.12.2017)
5. Приказ ФСТЭК от 18 февраля 2013 г. № 21 «Об утверждении состава и содержания организационных и технических мер по обеспечению безопасности персональных данных при их обработке в информационных системах персональных данных»
6. Приказ ФСТЭК от 11 февраля 2013 г. №17 «Об утверждении Требований по защите информации, не составляющей государственную тайну, содержащейся в государственных информационных системах»
7. Приказ от 14 марта 2014 г. №31 «Об утверждении требований к обеспечению защиты информации в автоматизированных системах управления производственными и технологическими процессами на критически важных объектах, потенциально опасных объектах, а также объектах, представляющих повышенную опасность для жизни и здоровья людей и для окружающей природной среды»
8. Руководство по эксплуатации СЗИ от НСД Dallas Lock 8.0.