

**Министерство науки и высшего образования Российской Федерации  
ФЕДЕРАЛЬНОЕ ГОСУДАРСТВЕННОЕ АВТОНОМНОЕ ОБРАЗОВАТЕЛЬНОЕ  
УЧРЕЖДЕНИЕ ВЫСШЕГО ОБРАЗОВАНИЯ  
НАЦИОНАЛЬНЫЙ ИССЛЕДОВАТЕЛЬСКИЙ УНИВЕРСИТЕТ ИТМО**

**Факультет безопасности информационных технологий**

**Дисциплина:**

«Вычислительные сети и контроль безопасности в компьютерных сетях»

**ОТЧЕТ ПО ЛАБОРАТОРНОЙ РАБОТЕ №3**

«Системы обеспечения информационной безопасности от НСД. DallasLock»

**Выполнили:**

Нгуен Тхе Вьет, студент группы N3347



(подпись)

Чу Ван Доан, студент группы N3347



(подпись)

Доан Тхи Хоай Тхыонг, студентка группы N3345



(подпись)

Чан Бао Линь, студентка группы N3346



**Проверил:**

Калабишка Михаил Михайлович

(отметка о выполнении)

(подпись)

Санкт-Петербург

2024 г.

## СОДЕРЖАНИЕ

Содержание .....	2
Введение .....	3
1     Настройка функций в программе Dallas Lock.....	4
1.1     Настройка Dallas Lock.....	4
1.2     Настроить политику аудита для 2 пользователей, параметры взять у преподавателя	5
1.3     Просмотреть и сохранить журналы аудита. Настроить фильтр на просмотр	
событий текущей недели, месяца, года .....	7
1.4     Произвести предоставление полномочий некоторого пользователя другому	
пользователю, используя функционал Dallas Lock.....	13
1.5     Настроить контроль целостности для жесткого диска, USB-устройства, папки,	
файла. Для расчета контрольных сумм использовать встроенные алгоритмы.....	14
1.6     Удалить и очистить с помощью Dallas Lock информацию о сохраненных	
журналах. ....	15
1.7     Настроить запрет смены пользователей без перезагрузки .....	16
1.8     Создать папки, файлы, зашифровать их, используя встроенные криптоалгоритмы	
17	
1.9     Заблокировать для различных групп пользователей работу с mp3, mpeg, docx, djvu	
18	
1.10    Создать отчет о правах и конфигурациях Dallas Lock.....	19
1.11    Создать резервную копию файлов СЗИ от НСД Dallas Lock.....	20
2     Тестирование настроенного функционала .....	22
2.1     Тестирование запрета смены пользователей без перезагрузки.....	22
2.2     Тестирование декодирования контейнера .....	22
2.3     Тестирование открытия файла запрещено .....	24
ЗАКЛЮЧЕНИЕ.....	25

## ВВЕДЕНИЕ

Цель работы – ознакомление с функционалом ПО Dallas Lock.

Для достижения цели работы, необходимо решать следующие задачи:

- настроить политику аудита для 2 пользователей;
- просмотреть и сохранить журналы аудита, настроить фильтр на просмотр событий текущей недели, месяца, года;
- произвести предоставление полномочий некоторого пользователя другому пользователю, используя функционал Dallas Lock;
- настроить контроль целостности для жесткого диска, USB-устройства, папки, файла;
- удалить и очистить с помощью Dallas Lock информацию о сохраненных журналах;
- настроить запрет смены пользователей без перезагрузки;
- создать папки, файлы, зашифровать их;
- заблокировать для различных групп пользователей работу с mp3, mpeg, docx, djvu;
- создать отчет о правах и конфигурациях Dallas Lock;
- создать резервную копию файлов СЗИ от НСД Dallas Lock;
- протестировать функционал Dallas Lock.

# 1 НАСТРОЙКА ФУНКЦИЙ В ПРОГРАММЕ DALLAS LOCK

## 1.1 Настройка Dallas Lock

Установка программного обеспечения (ПО) для запуска виртуальных машин, таких как Virtualbox, Vmware (рис. 1).



Рисунок 1 – ПО для запуска виртуальных машин

Переход по ссылке яндекс «<https://disk.yandex.ru/d/Hvn-llK0T7yPyQ>» и скачивание файла PAZ\_DALLAS.ova (рис. 2).

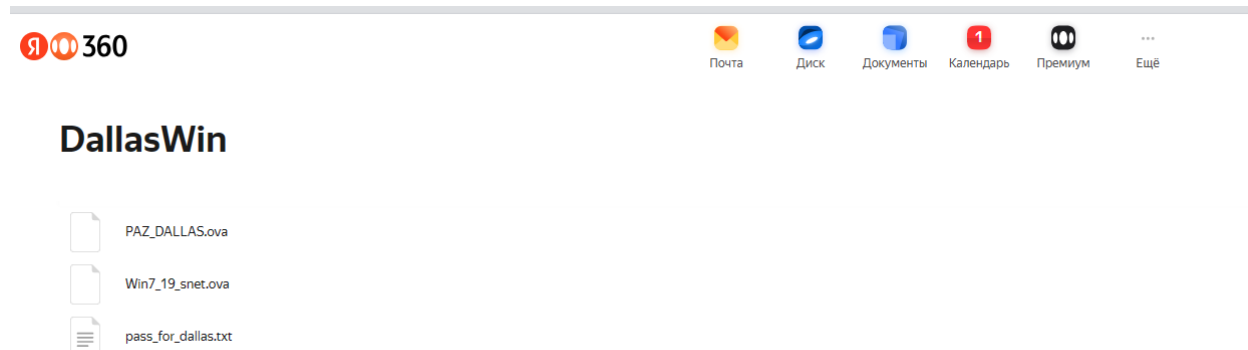


Рисунок 2 – DallasWin

Доступ к учетной записи «admin» с паролем: «PAZ\_LOCAL1» (рис. 3)

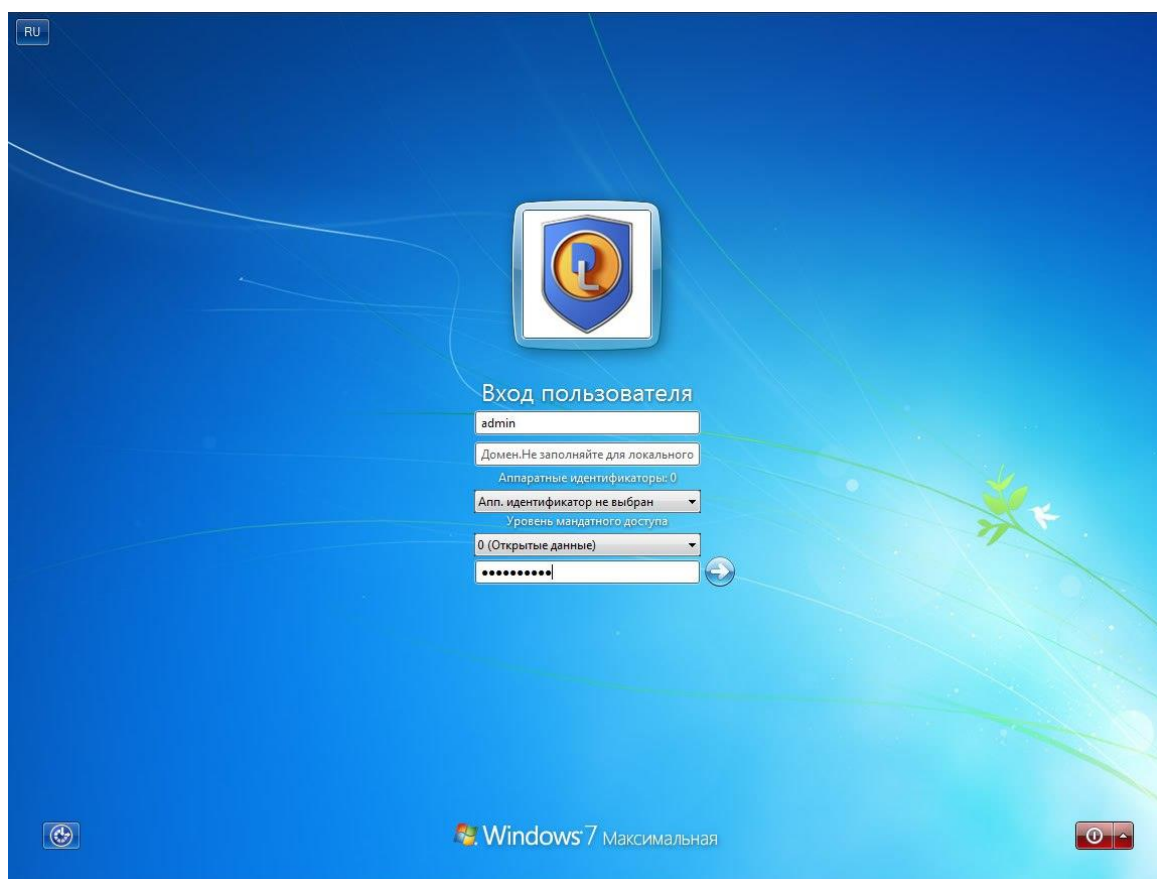


Рисунок 3 – Вход в ОС

## 1.2 Настроить политику аудита для 2 пользователей, параметры взять у преподавателя

Создание 3 учетных записей с параметрами, как показано на рисунках 4, 5, 6.

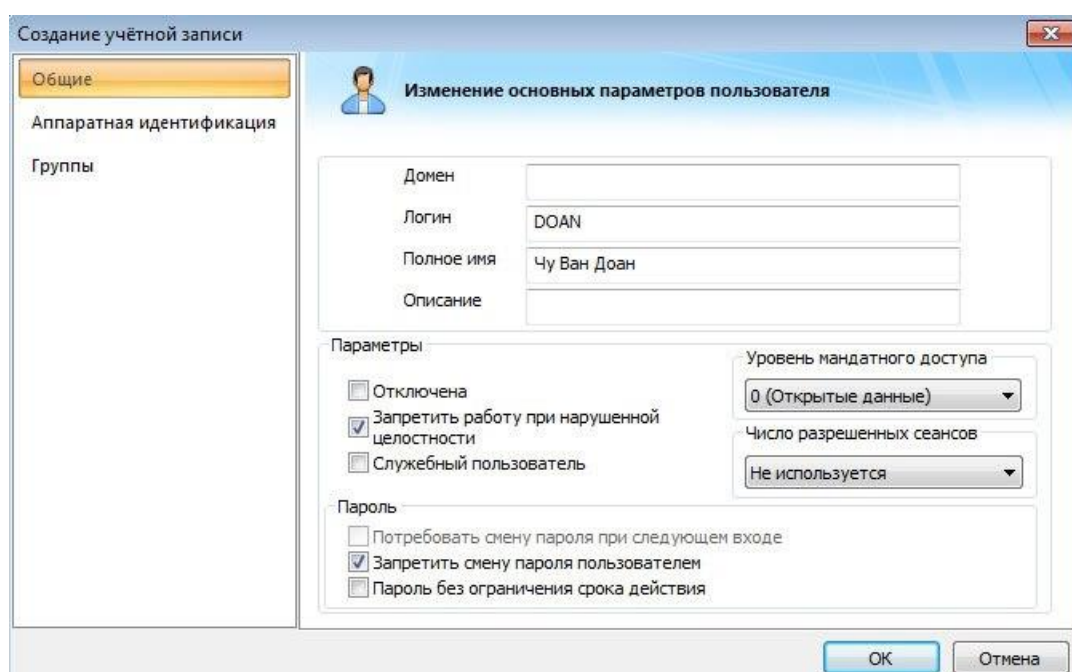



Рисунок 4 – Пользователь Чу Ван Доан

Создание учётной записи

Общие  
Аппаратная идентификация  
Группы

 **Изменение основных параметров пользователя**

Домен

Логин: THUONG

Полное имя: Доан Тхи Хоай Тхьонг

Описание

Параметры

☐ Отключена

☒ Запретить работу при нарушенной целостности

☒ Служебный пользователь

Уровень мандатного доступа: 3 (Секретно)

Число разрешенных сеансов: Не используется

Пароль

☐ Потребовать смену пароля при следующем входе

☐ Запретить смену пароля пользователем


☐ Пароль без ограничения срока действия

OK Отмена

Рисунок 5 – Пользователь Доан Тхи Хоай Тхьонг

Создание учётной записи

Общие  
Аппаратная идентификация  
Группы

 **Изменение основных параметров пользователя**

Домен

Логин: LINH

Полное имя: Чан Бао Линь

Описание

Параметры

☒ Отключена

☒ Запретить работу при нарушенной целостности

☐ Служебный пользователь

Уровень мандатного доступа: 4 (Сов. секретно)

Число разрешенных сеансов: Не используется

Пароль

☐ Потребовать смену пароля при следующем входе

☐ Запретить смену пароля пользователем

☐ Пароль без ограничения срока действия

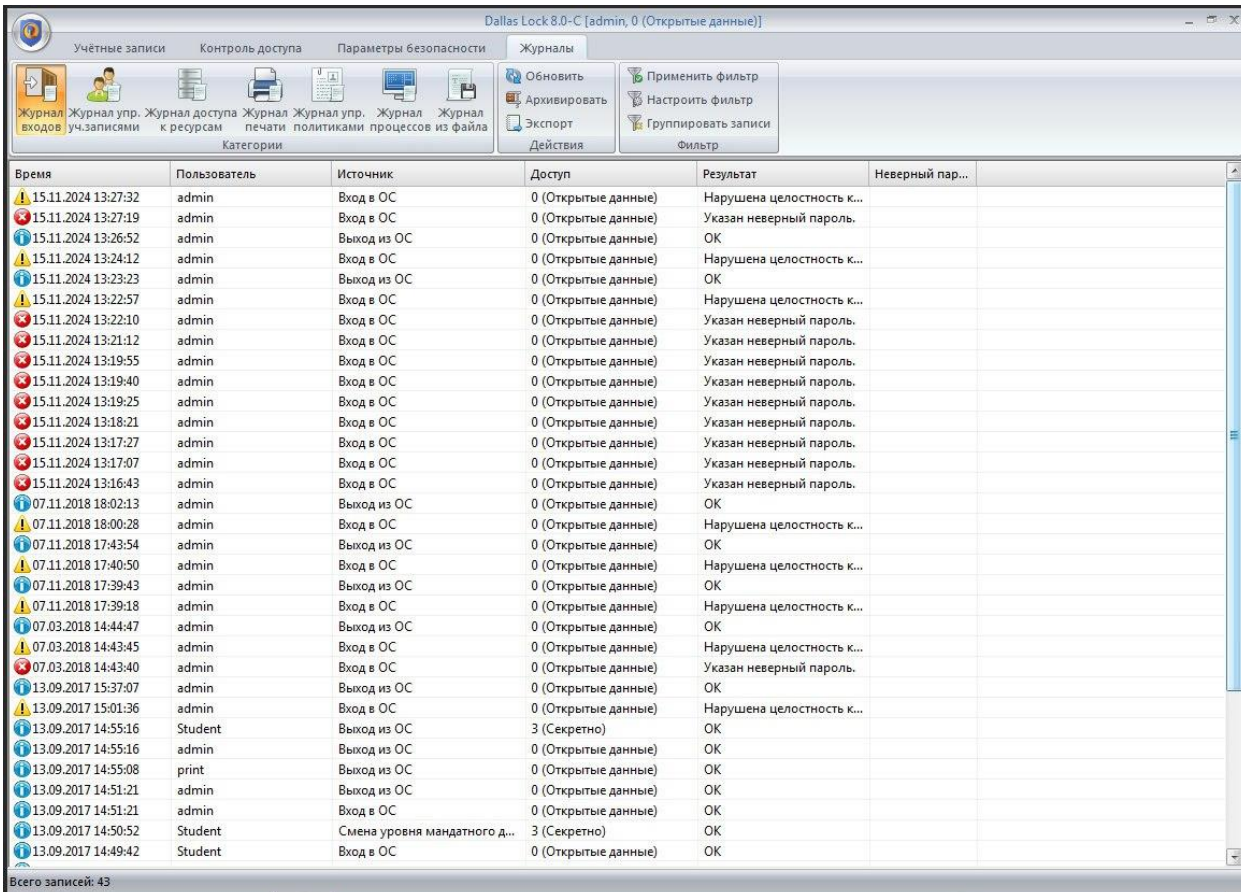
OK Отмена

Рисунок 6 – Пользователь Чан Бао Линь

### 1.3 Просмотреть и сохранить журналы аудита. Настроить фильтр на просмотр событий текущей недели, месяца, года.

Dallas Lock 8.0-K обеспечивает системное ведение шести электронных журналов, фиксируя разнообразные действия пользователей. Эти журналы предоставляют обширную информацию о действиях пользователей и событиях в системе, обеспечивая эффективный мониторинг и анализ безопасности.

Журнал Входов (рис. 7): Записывает все входы и выходы пользователей ПЭВМ, включая локальные, сетевые, терминальные входы и входы для удаленного администрирования. Отмечаются как успешные входы, так и попытки с указанием причины отказа.



Время	Пользователь	Источник	Доступ	Результат	Неверный пар...
15.11.2024 13:27:32	admin	Вход в ОС	0 (Открытые данные)	Нарушена целостность к...	
15.11.2024 13:27:19	admin	Вход в ОС	0 (Открытые данные)	Указан неверный пароль.	
15.11.2024 13:26:52	admin	Выход из ОС	0 (Открытые данные)	ОК	
15.11.2024 13:24:12	admin	Вход в ОС	0 (Открытые данные)	Нарушена целостность к...	
15.11.2024 13:23:23	admin	Выход из ОС	0 (Открытые данные)	ОК	
15.11.2024 13:22:57	admin	Вход в ОС	0 (Открытые данные)	Нарушена целостность к...	
15.11.2024 13:22:10	admin	Вход в ОС	0 (Открытые данные)	Указан неверный пароль.	
15.11.2024 13:21:12	admin	Вход в ОС	0 (Открытые данные)	Указан неверный пароль.	
15.11.2024 13:19:55	admin	Вход в ОС	0 (Открытые данные)	Указан неверный пароль.	
15.11.2024 13:19:40	admin	Вход в ОС	0 (Открытые данные)	Указан неверный пароль.	
15.11.2024 13:19:25	admin	Вход в ОС	0 (Открытые данные)	Указан неверный пароль.	
15.11.2024 13:18:21	admin	Вход в ОС	0 (Открытые данные)	Указан неверный пароль.	
15.11.2024 13:17:27	admin	Вход в ОС	0 (Открытые данные)	Указан неверный пароль.	
15.11.2024 13:17:07	admin	Вход в ОС	0 (Открытые данные)	Указан неверный пароль.	
15.11.2024 13:16:43	admin	Вход в ОС	0 (Открытые данные)	Указан неверный пароль.	
07.11.2018 18:02:13	admin	Выход из ОС	0 (Открытые данные)	ОК	
07.11.2018 18:00:28	admin	Вход в ОС	0 (Открытые данные)	Нарушена целостность к...	
07.11.2018 17:43:54	admin	Выход из ОС	0 (Открытые данные)	ОК	
07.11.2018 17:40:50	admin	Вход в ОС	0 (Открытые данные)	Нарушена целостность к...	
07.11.2018 17:39:43	admin	Выход из ОС	0 (Открытые данные)	ОК	
07.11.2018 17:39:18	admin	Вход в ОС	0 (Открытые данные)	Нарушена целостность к...	
07.03.2018 14:44:47	admin	Выход из ОС	0 (Открытые данные)	ОК	
07.03.2018 14:43:45	admin	Вход в ОС	0 (Открытые данные)	Нарушена целостность к...	
07.03.2018 14:43:40	admin	Вход в ОС	0 (Открытые данные)	Указан неверный пароль.	
13.09.2017 15:37:07	admin	Выход из ОС	0 (Открытые данные)	ОК	
13.09.2017 15:01:36	admin	Вход в ОС	0 (Открытые данные)	Нарушена целостность к...	
13.09.2017 14:55:16	Student	Выход из ОС	3 (Секретно)	ОК	
13.09.2017 14:55:16	admin	Выход из ОС	0 (Открытые данные)	ОК	
13.09.2017 14:55:08	print	Выход из ОС	0 (Открытые данные)	ОК	
13.09.2017 14:51:21	admin	Выход из ОС	0 (Открытые данные)	ОК	
13.09.2017 14:51:21	admin	Вход в ОС	0 (Открытые данные)	ОК	
13.09.2017 14:50:52	Student	Смена уровня мандатного д...	3 (Секретно)	ОК	
13.09.2017 14:49:42	Student	Вход в ОС	0 (Открытые данные)	ОК	

Рисунок 7 – Журнал Входов

Журнал Управления Учетными Записями (рис. 8): Регистрирует события, связанные с созданием, удалением или изменением параметров пользовательских учетных записей.



Dallas Lock 8.0-C [admin, 0 (Открытые данные)]						
Учётные записи		Контроль доступа		Параметры безопасности		Журналы
Журнал входов	Журнал уч. записями	Журнал доступа к ресурсам	Журнал печати	Журнал политикami	Журнал процессов из файла	
Обновить		Архивировать		Экспорт		Применить фильтр
Настроить фильтр		Группировать записи		Фильтр		
Время	Пользователь	Компьютер	Имя	Результат	Операция	
15.11.2024 13:39:48	admin		LINH	OK	Создать пользователя	
15.11.2024 13:38:22	admin		THUONG	OK	Создать пользователя	
15.11.2024 13:36:02	admin		DOAN	OK	Создать пользователя	
13.09.2017 15:01:23	LOCAL_SYSTEM		Student	OK	Установить параметры пользователя	
13.09.2017 15:01:23	LOCAL_SYSTEM		print	OK	Установить параметры пользователя	
13.09.2017 15:01:23	LOCAL_SYSTEM		anonymous	OK	Установить параметры пользователя	
13.09.2017 14:47:46	admin		Student	OK	Создать пользователя	
13.09.2017 14:45:01	admin		print	OK	Создать пользователя	
13.09.2017 14:44:09	admin		Konnichiwa!	OK	Удалить пользователя	
13.09.2017 14:42:13	admin		Konnichiwa!	OK	Создать пользователя	
24.02.2014 19:15:40	LOCAL_SYSTEM		anonymous	OK	Установить параметры пользователя	

Рисунок 8 – Журнал Управления Учетными Записями

Журнал Доступа к Ресурсам (рис. 9): Регистрирует обращения к объектам файловой системы, для которых настроен аудит. Позволяет гибко настраивать, какие события требуется фиксировать.

Dallas Lock 8.0-C [admin, 0 (Открытые данные)]							
Учётные записи		Контроль доступа		Параметры безопасности		Журналы	
Журнал входов	Журнал уч. записями	Журнал доступа к ресурсам	Журнал печати	Журнал политикami	Журнал процессов из файла	Обновить	Архивировать
Экспорт		Правда для файлов		Применить фильтр		Настроить фильтр	
Группировать записи		Фильтр					
Время	Пользователь	Компьютер	Объект доступа	Результат	Операция	Доступ	Права
15.11.2024 13:27:32			C:\Users\admin\Desktop\ывалыв...	Нарушена це...	Проверка целостности о...	0 (Открытые данные)	
15.11.2024 13:24:12			C:\Users\admin\Desktop\ывалыв...	Нарушена це...	Проверка целостности о...	0 (Открытые данные)	
15.11.2024 13:22:57			C:\Users\admin\Desktop\ывалыв...	Нарушена це...	Проверка целостности о...	0 (Открытые данные)	
07.11.2018 18:00:28			C:\Users\admin\Desktop\ывалыв...	Нарушена це...	Проверка целостности о...	0 (Открытые данные)	
07.11.2018 17:40:50			C:\Users\admin\Desktop\ывалыв...	Нарушена це...	Проверка целостности о...	0 (Открытые данные)	
07.11.2018 17:39:18			C:\Users\admin\Desktop\ывалыв...	Нарушена це...	Проверка целостности о...	0 (Открытые данные)	
07.03.2018 14:43:45			C:\Users\admin\Desktop\ывалыв...	Нарушена це...	Проверка целостности о...	0 (Открытые данные)	
13.09.2017 15:33:20	admin		C:\Users\admin\Desktop\ывалыв...	OK	Запись параметров конт...	0 (Открытые данные)	
13.09.2017 15:32:52			C:\Users\admin\Desktop\ывалыв...	Нарушена це...	Проверка целостности о...	0 (Открытые данные)	
13.09.2017 15:05:23	admin		C:\Users\admin\Desktop\ывалыв...	OK	Запись параметров конт...	0 (Открытые данные)	
13.09.2017 15:05:21			C:\Users\admin\Desktop\ывалыв...	Нарушена це...	Проверка целостности о...	0 (Открытые данные)	
13.09.2017 15:04:17	admin		C:\Users\admin\Desktop\ывалыв...	OK	Запись параметров конт...	0 (Открытые данные)	
13.09.2017 15:01:36			C:\Users\admin\Desktop\ывалыв...	Нарушена це...	Проверка целостности о...	0 (Открытые данные)	
13.09.2017 14:55:07	Student		C:\Папка мандата	OK	Закрытие объекта	3 (Секретно)	R RA
13.09.2017 14:55:07	Student		C:\Папка мандата	OK	Закрытие объекта	3 (Секретно)	R RA
13.09.2017 14:55:07	Student		C:\Папка мандата	OK	Закрытие объекта	3 (Секретно)	R RA
13.09.2017 14:55:07	Student		C:\Папка мандата	OK	Закрытие объекта	3 (Секретно)	R RA
13.09.2017 14:53:57			C:\Users\admin\Desktop\ывалыв...	Нарушена це...	Проверка целостности о...	0 (Открытые данные)	
13.09.2017 14:53:46	admin		C:\Users\admin\Desktop\ывалыв...	OK	Запись параметров конт...	0 (Открытые данные)	
13.09.2017 14:53:40			C:\Users\admin\Desktop\ывалыв...	Нарушена це...	Проверка целостности о...	0 (Открытые данные)	
13.09.2017 14:52:06	admin		C:\Users\admin\Desktop\ывалыв...	OK	Запись параметров конт...	0 (Открытые данные)	
13.09.2017 14:51:02	Student		C:\Папка мандата	OK	Закрытие объекта	3 (Секретно)	RA
13.09.2017 14:51:02	Student		C:\Папка мандата	OK	Закрытие объекта	3 (Секретно)	RA
13.09.2017 14:51:02	Student		C:\Папка мандата	OK	Открытие каталога	3 (Секретно)	RA
13.09.2017 14:51:02	Student		C:\Папка мандата	OK	Закрытие объекта	3 (Секретно)	RA
13.09.2017 14:51:02	Student		C:\Папка мандата	OK	Закрытие объекта	3 (Секретно)	RA
13.09.2017 14:51:02	Student		C:\Папка мандата	OK	Открытие каталога	3 (Секретно)	RA
13.09.2017 14:51:02	Student		C:\Папка мандата	OK	Открытие каталога	3 (Секретно)	RA
13.09.2017 14:51:02	Student		C:\Папка мандата	OK	Закрытие объекта	3 (Секретно)	RA
13.09.2017 14:51:02	Student		C:\Папка мандата	OK	Закрытие объекта	3 (Секретно)	RA
13.09.2017 14:51:02	Student		C:\Папка мандата	OK	Закрытие объекта	3 (Секретно)	RA

Рисунок 9 – Журнал Доступа к Ресурсам

Журнал Печати (рис. 10): Отслеживает все события, связанные с печатью документов на локальных или сетевых принтерах. Важно отметить, что данный журнал в настоящий момент выключен.



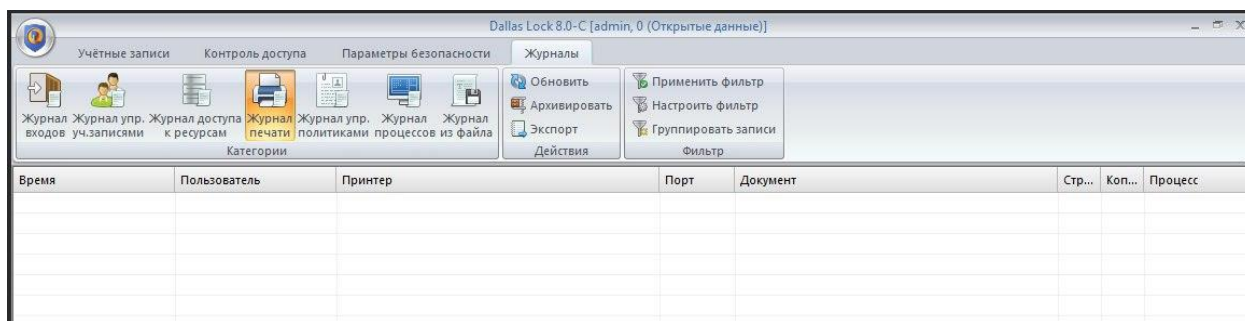


Рисунок 10 – Журнал Печати

Журнал Управления Политиками (рис. 11): Отражает все события, связанные с изменением конфигурации системы защиты информации. Включает события запуска/завершения модулей администрирования и события запуска/завершения работы системы.

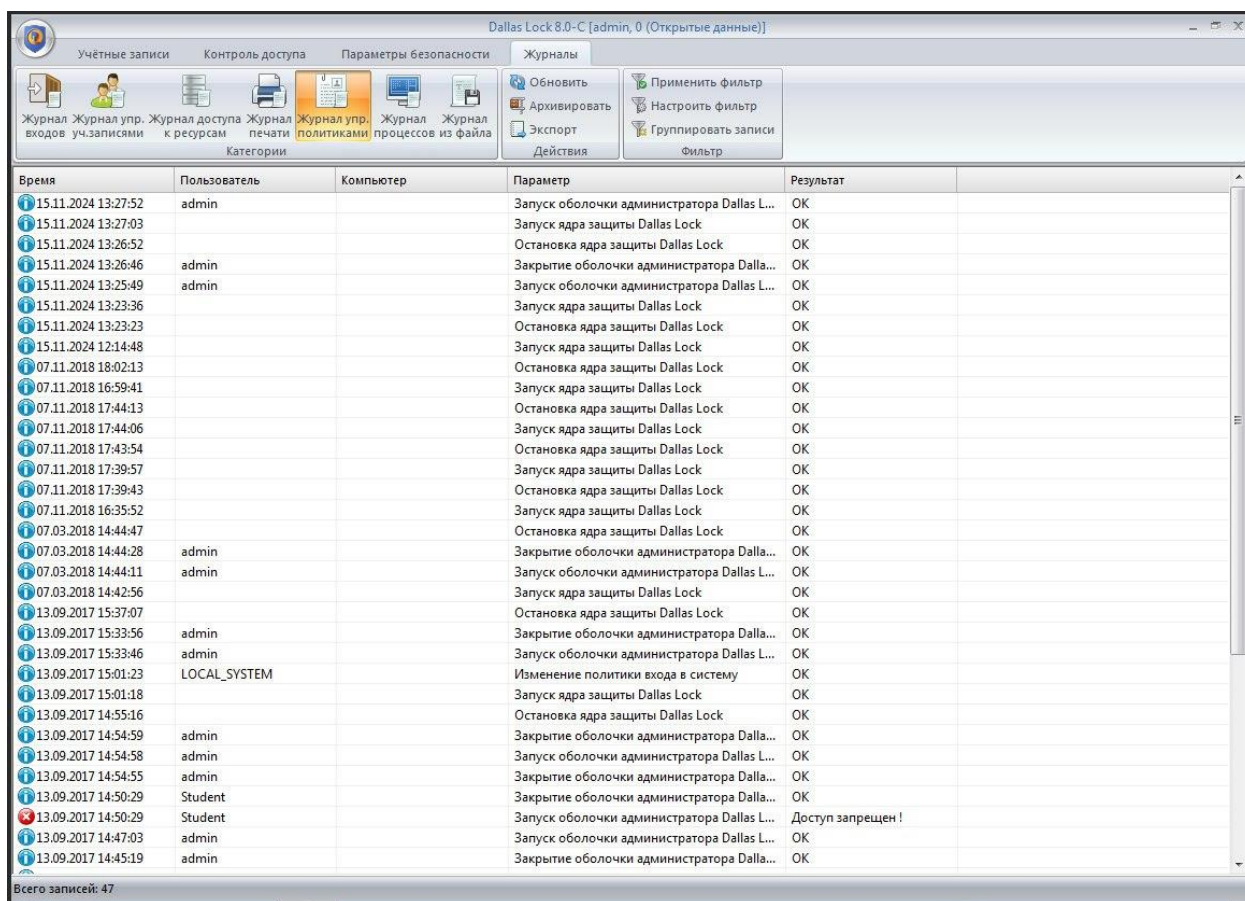


Рисунок 11 – Журнал Управления Политиками

Журнал Процессов (рис. 12): Фиксирует события запуска и завершения процессов. Примером может служить регистрация запущенного процесса, такого как " Chess Titans ".



Рисунок 12 – Журнал Процессов

Журнал из Файла (рис. 13): Просмотр сохраненного файла журнала путем загрузки файла

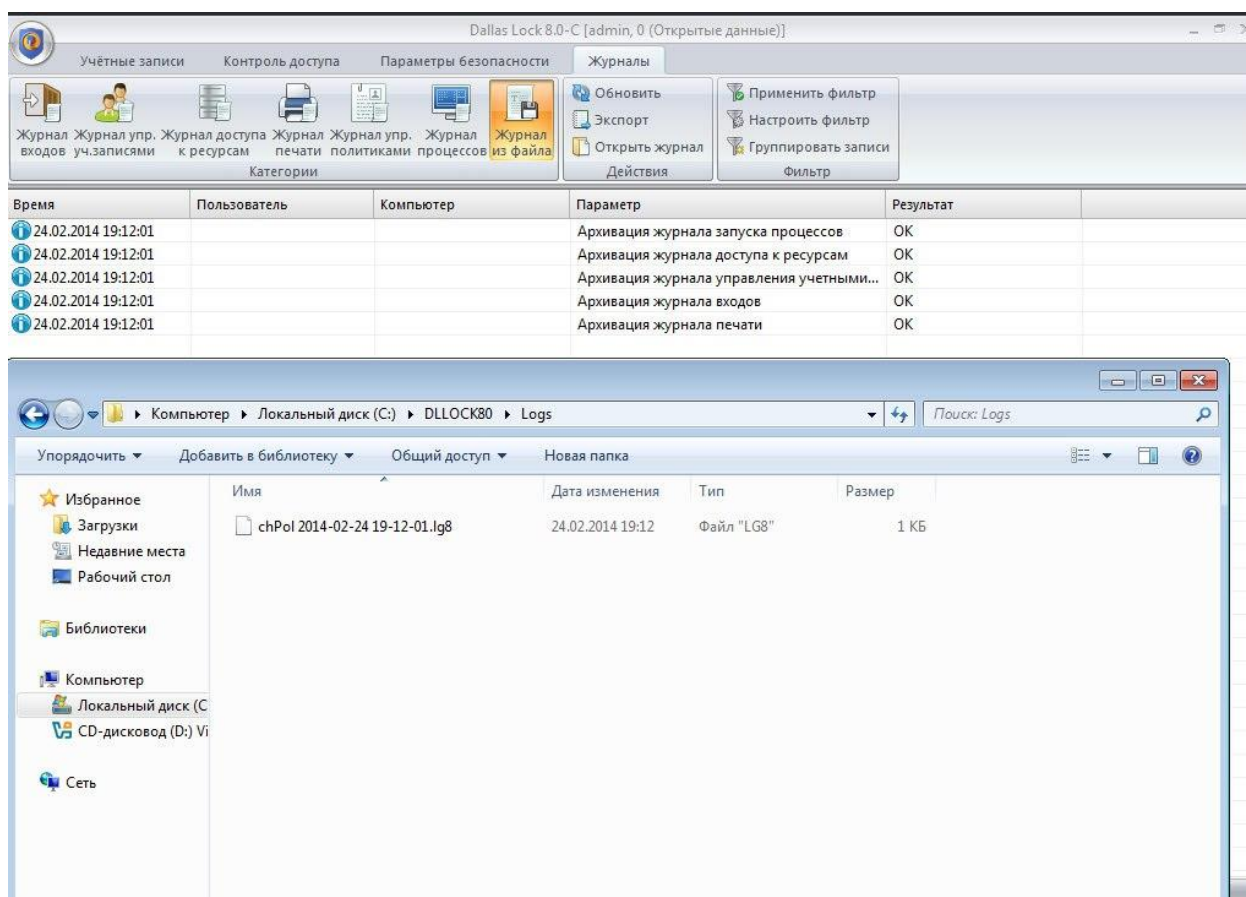


Рисунок 13 – Журнал из файла

Сохранение файла журнала, выбрав «Экспорт» (рис. 14)

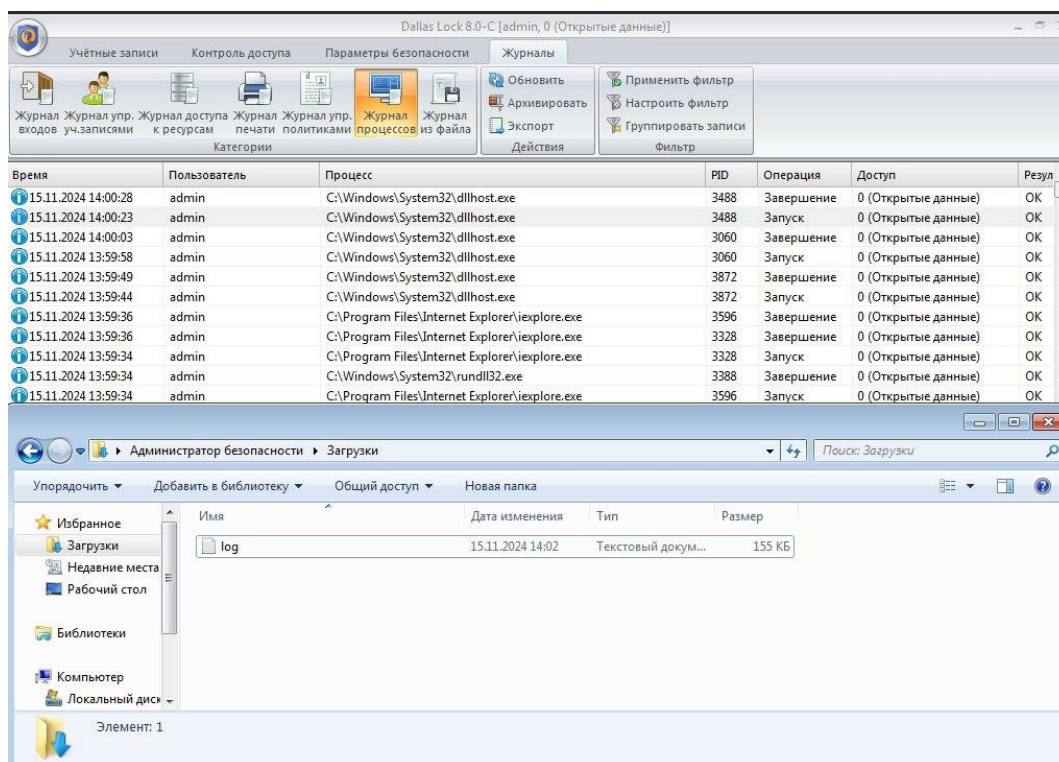


Рисунок 14 – Сохранение файла журнала



## Настройка фильтра на просмотр событий текущей недели (рис. 15)

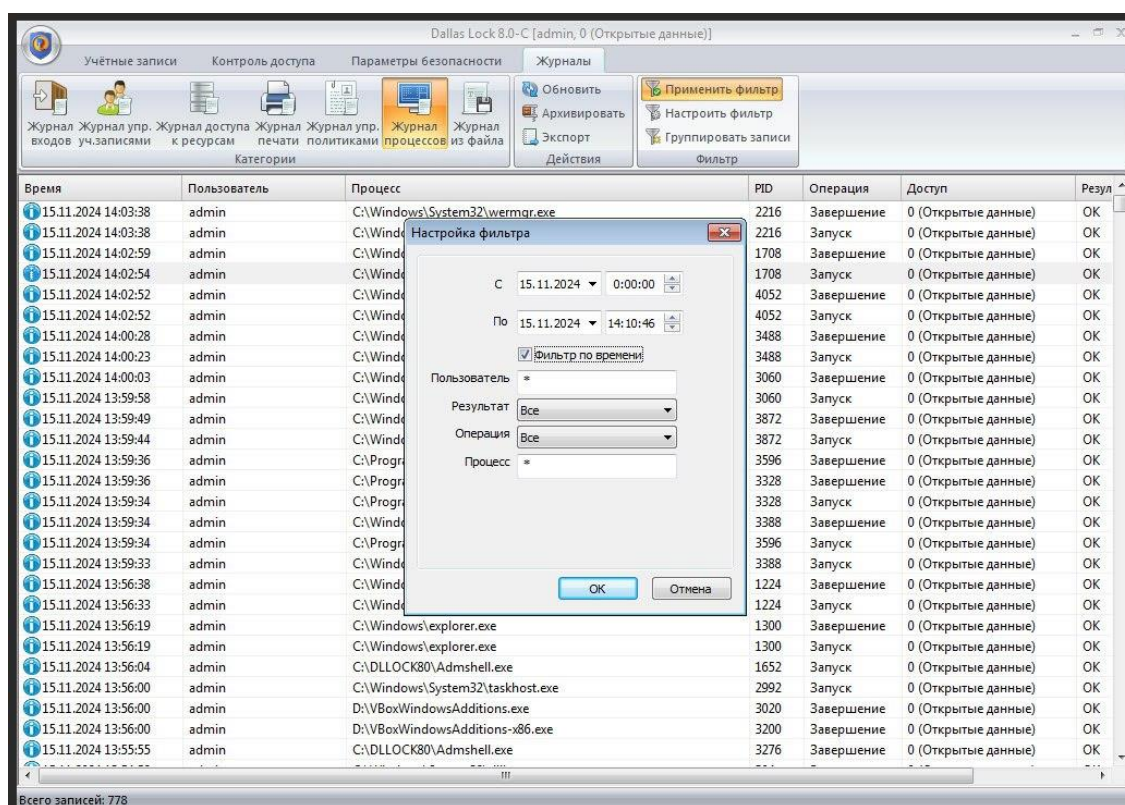


Рисунок 15 – Фильтр на сутки

## Настройка фильтра на просмотр событий месяца (рис. 16)

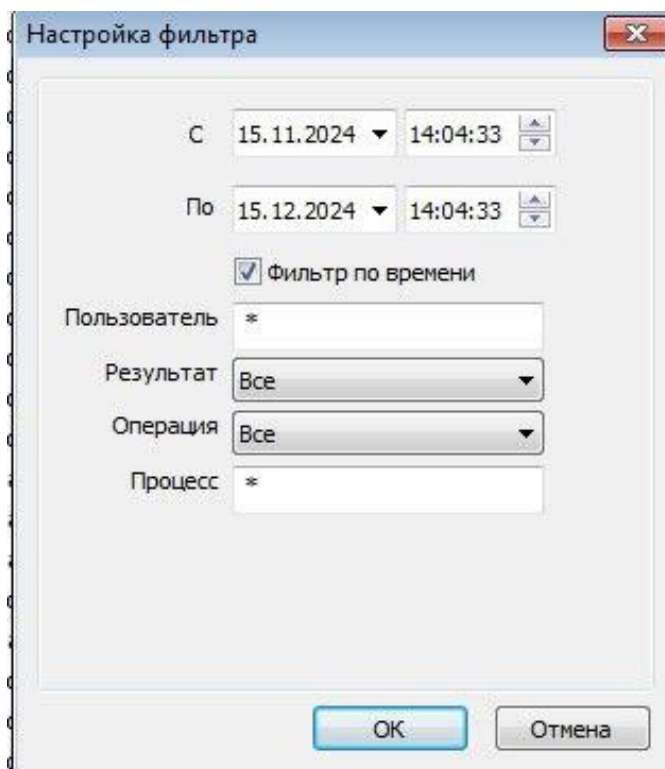


Рисунок 16 – Фильтр на 1 неделю

## Настройка фильтра на просмотр событий года (рис. 17)

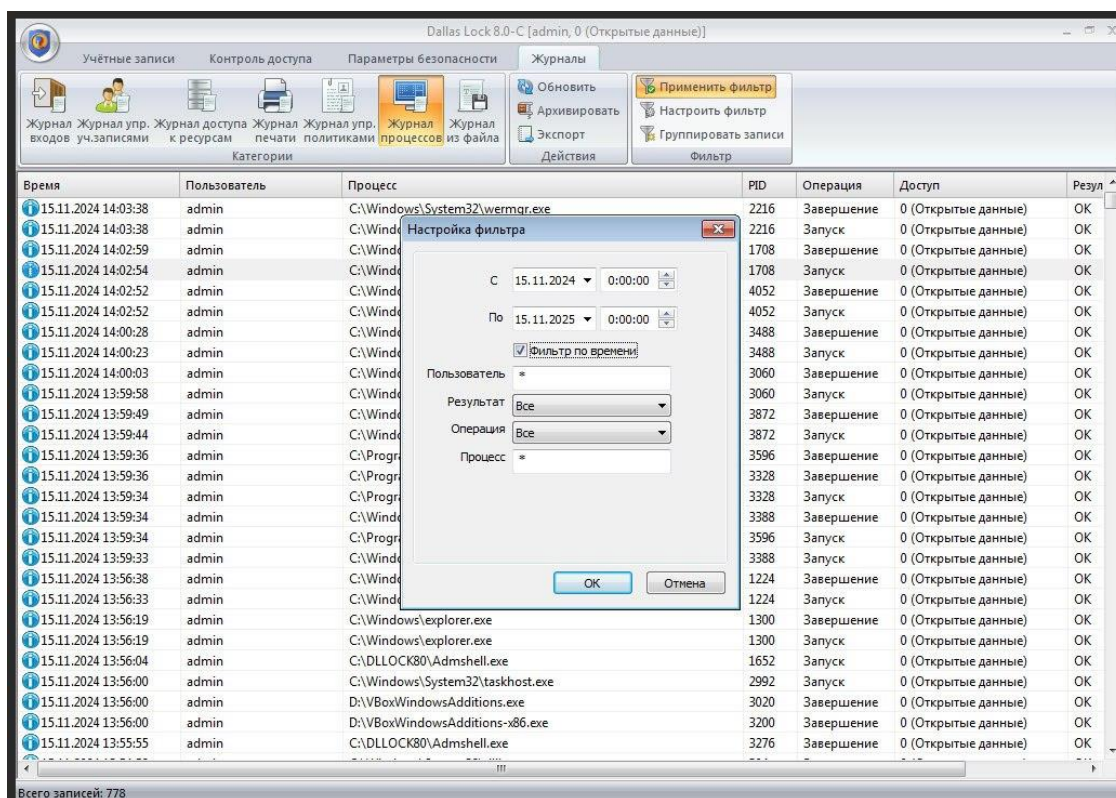


Рисунок 17 – Фильтр на 1 год

## 1.4 Произвести предоставление полномочий некоторого пользователя другому пользователю, используя функционал Dallas Lock.

Пользователю «DOAN» предоставили права на просмотр аудита (рис. 18).

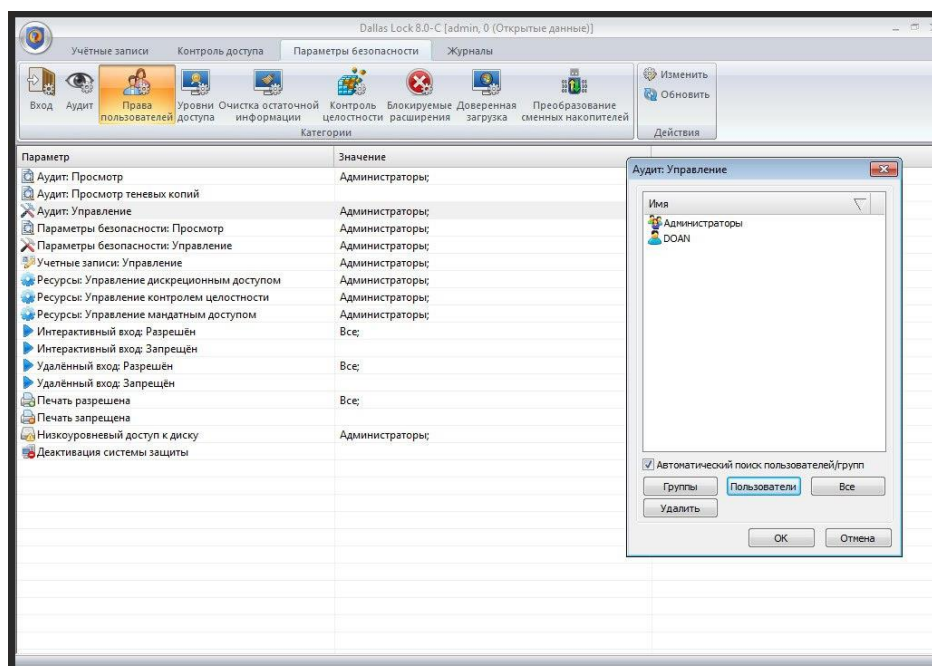


Рисунок 18 – Аудит – Управление

## 1.5 Настроить контроль целостности для жесткого диска, USB-устройства, папки, файла. Для расчета контрольных сумм использовать встроенные алгоритмы.

Настройка контроля целостности жесткого диска, USB-устройства и папки. Мы используем алгоритмы хеширования MD5 (алгоритм дайджеста сообщений MD5 — это широко используемая хеш-функция, производящая 128-битное хэш-значение) (рис. 19).

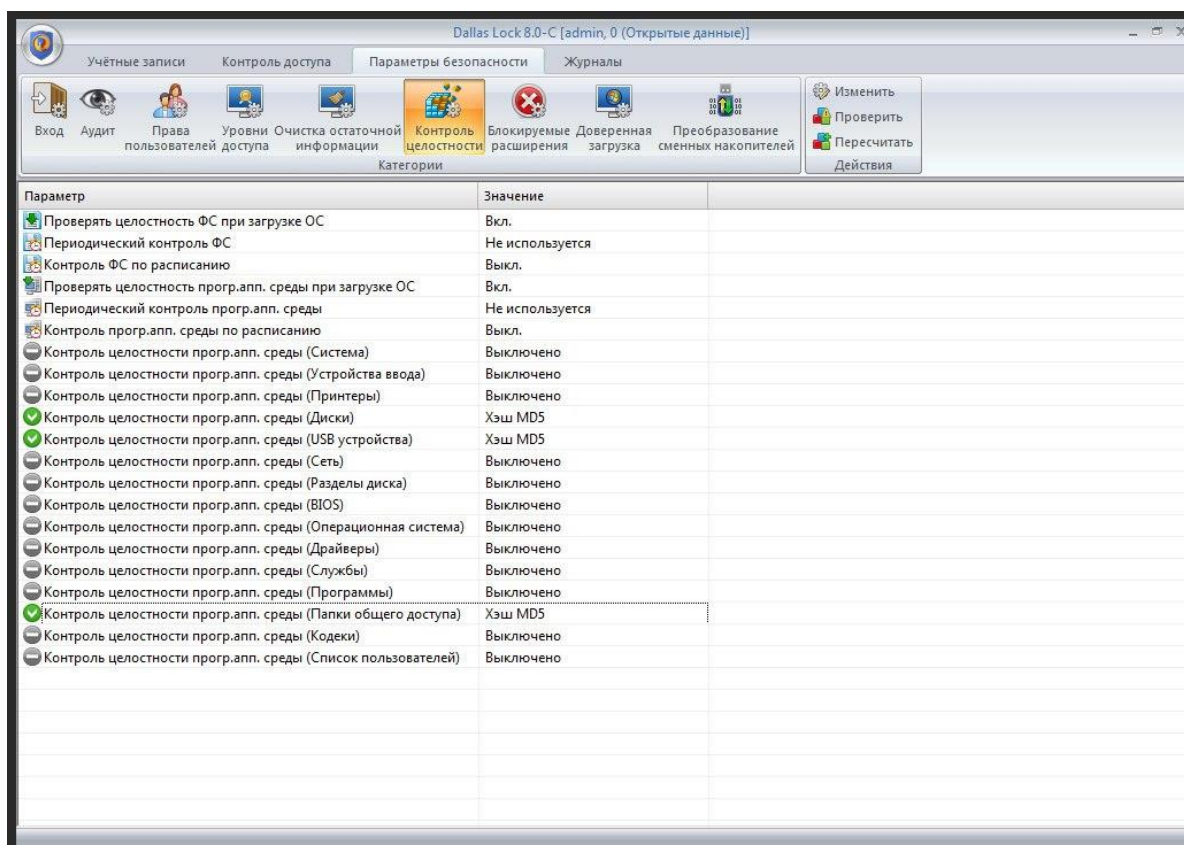
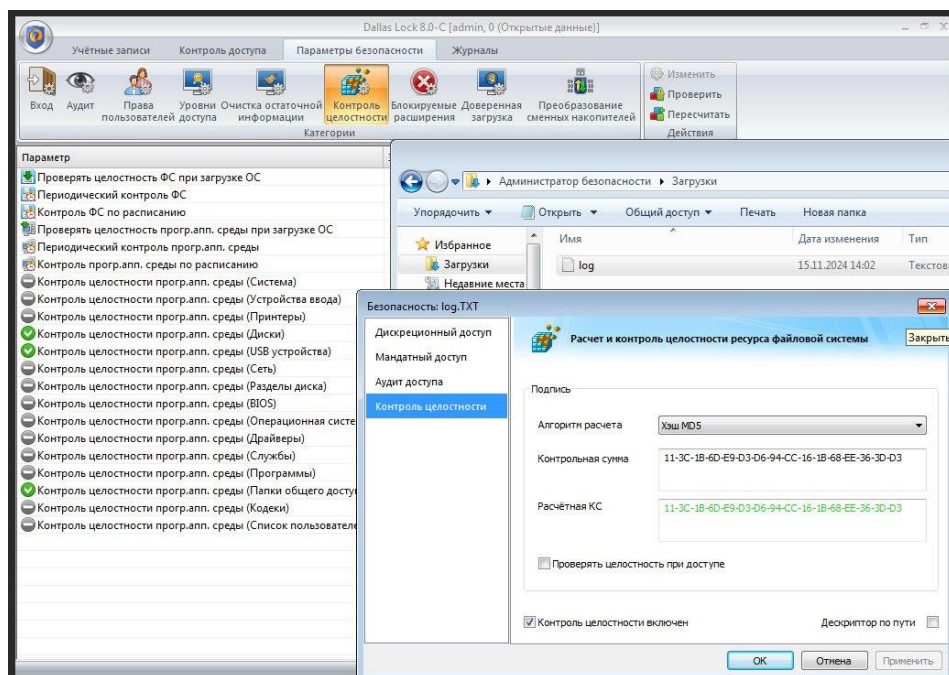


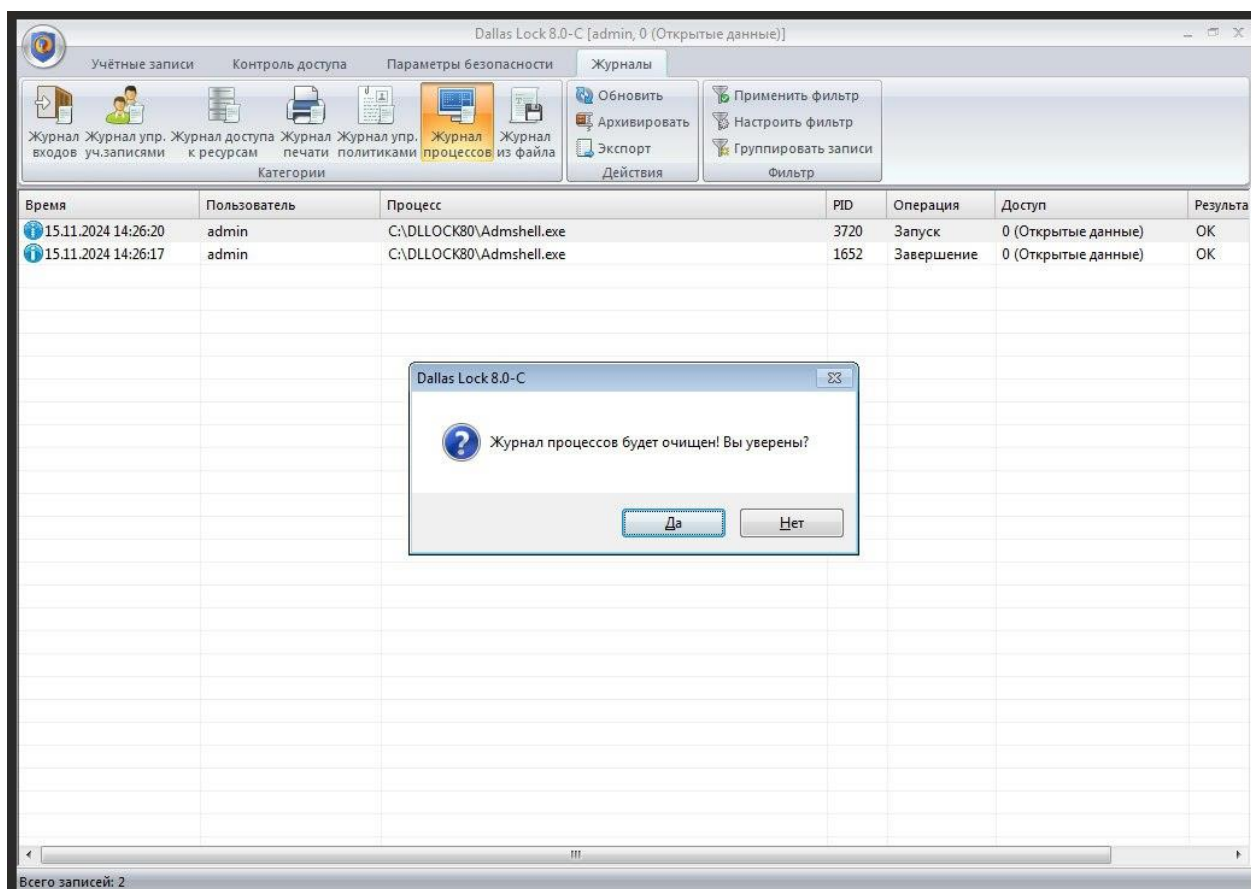
Рисунок 19 – Настройка контроля целостности

Настройка контроля целостности файла log.txt (рис. 20).





## 1.6 Удалить и очистить с помощью Dallas Lock информацию о сохраненных журналах.



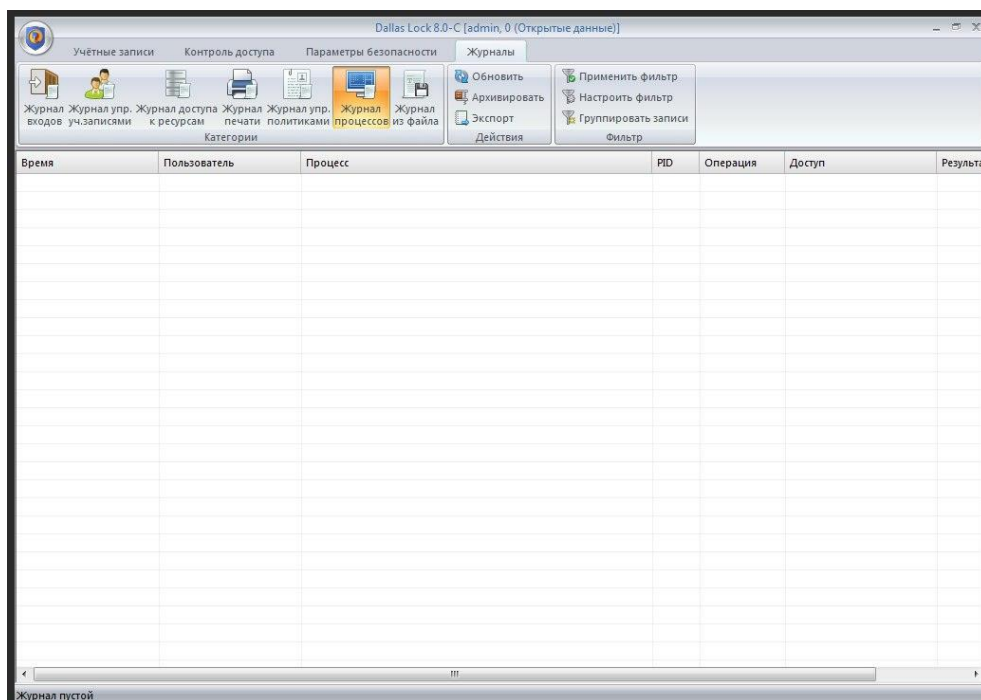


Рисунок 22 – После удаления журнала

## 1.7 Настроить запрет смены пользователей без перезагрузки

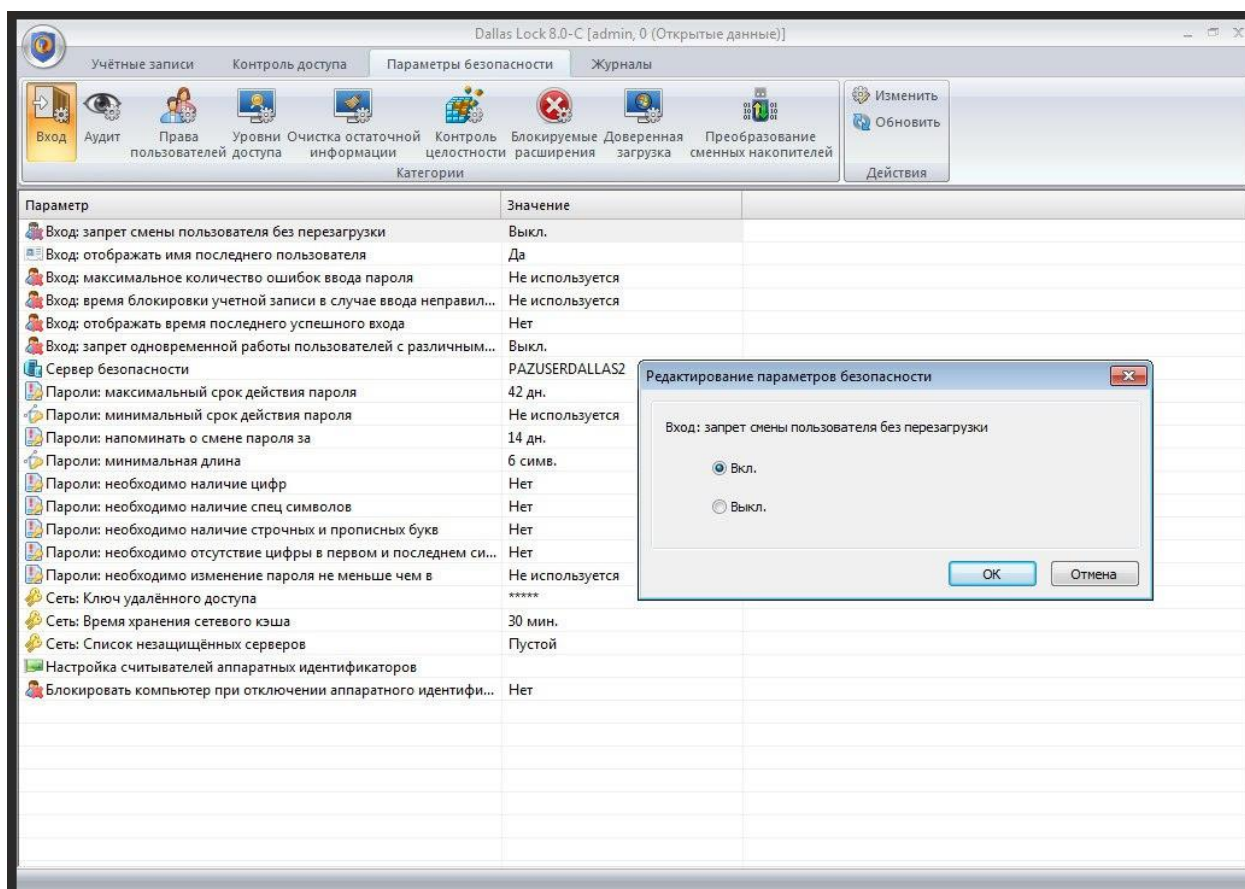


Рисунок 23 – Запрет смены пользователя без перезагрузки

## 1.8 Создать папки, файлы, зашифровать их, используя встроенные криптоалгоритмы

Выбор файла «log.txt» и его шифрование с помощью программы Dallas Lock, выбрав «DL8.0: Закодировать» (рис. 24).

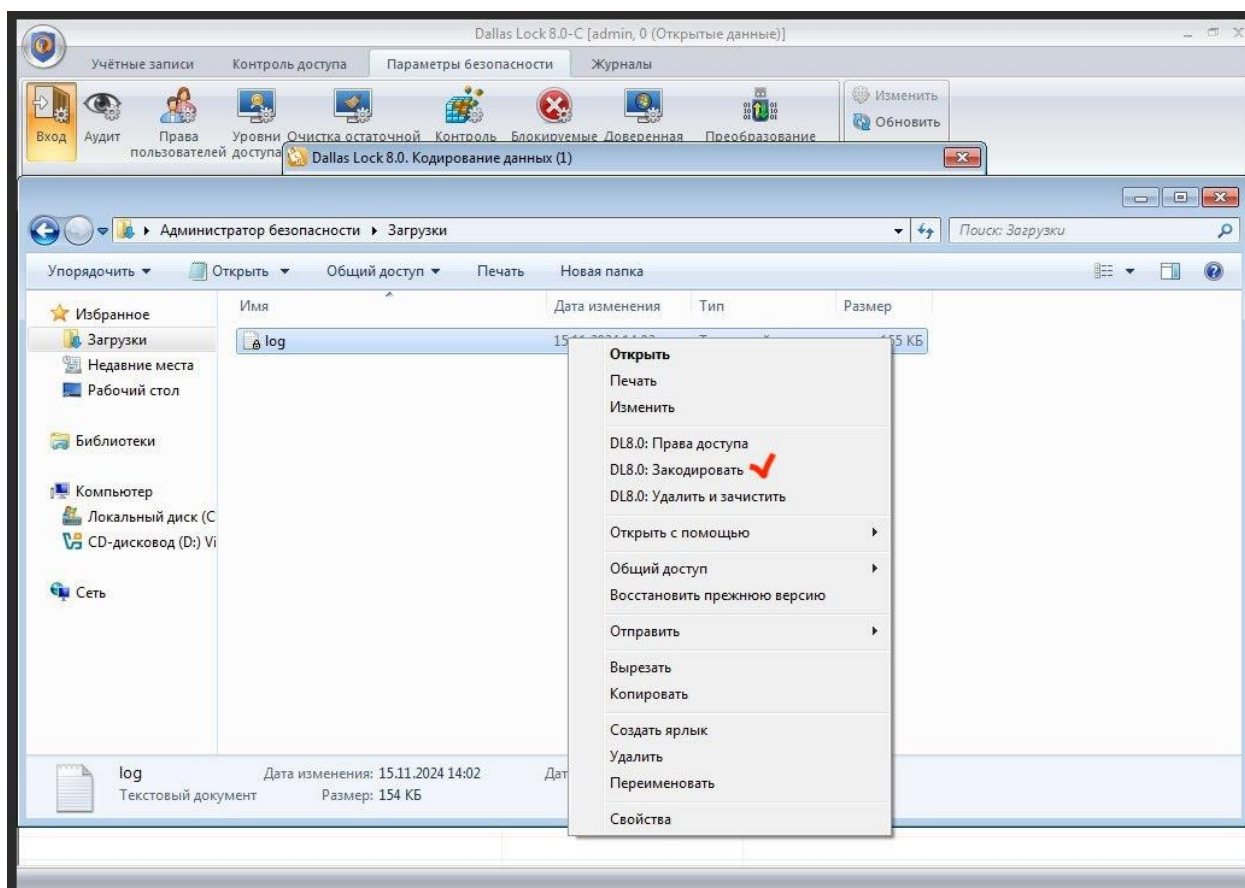


Рисунок 24 – Выбор файла для создание нового файла

Закодирование (рис. 25)

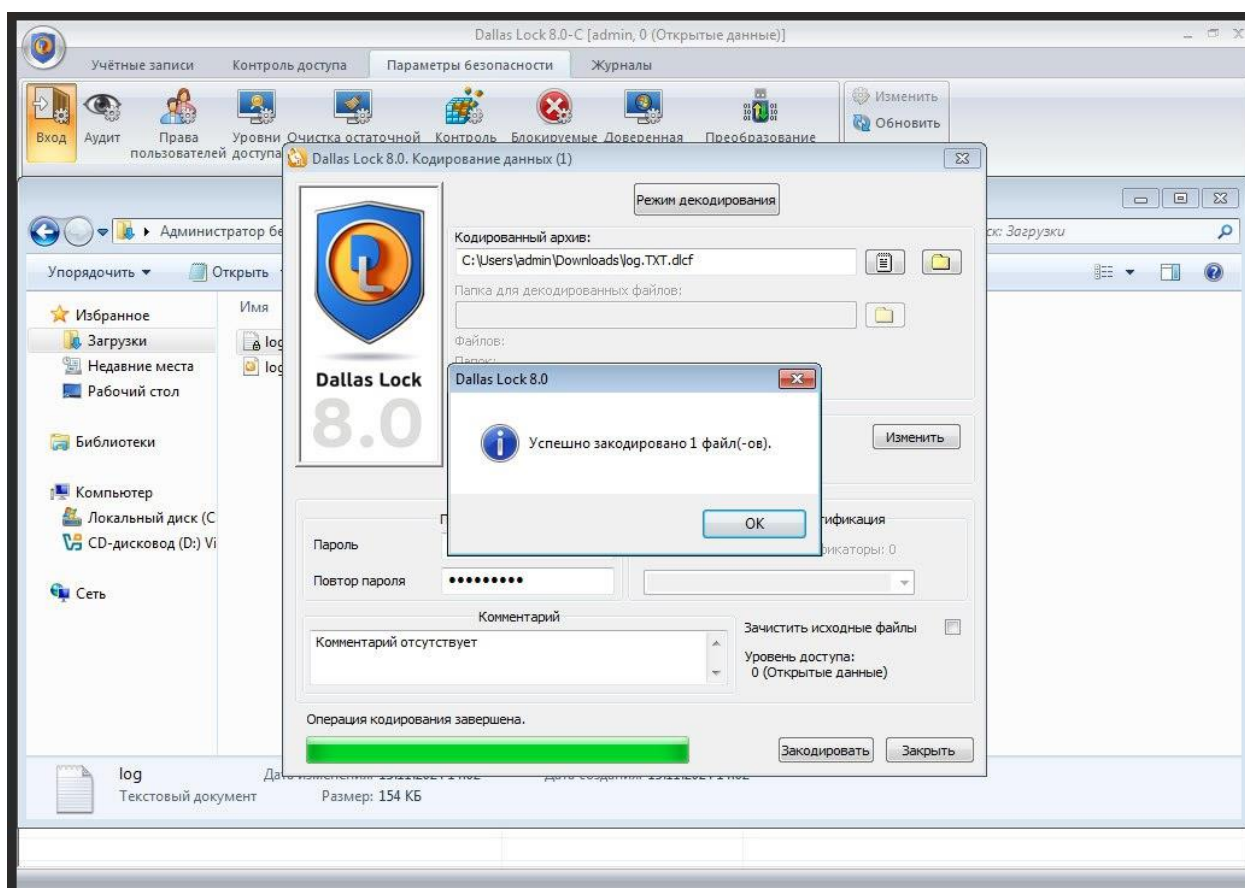


Рисунок 25 – Закодирование файла «log.txt»

## 1.9 Заблокировать для различных групп пользователей работу с mp3, mpeg, docx, djvu

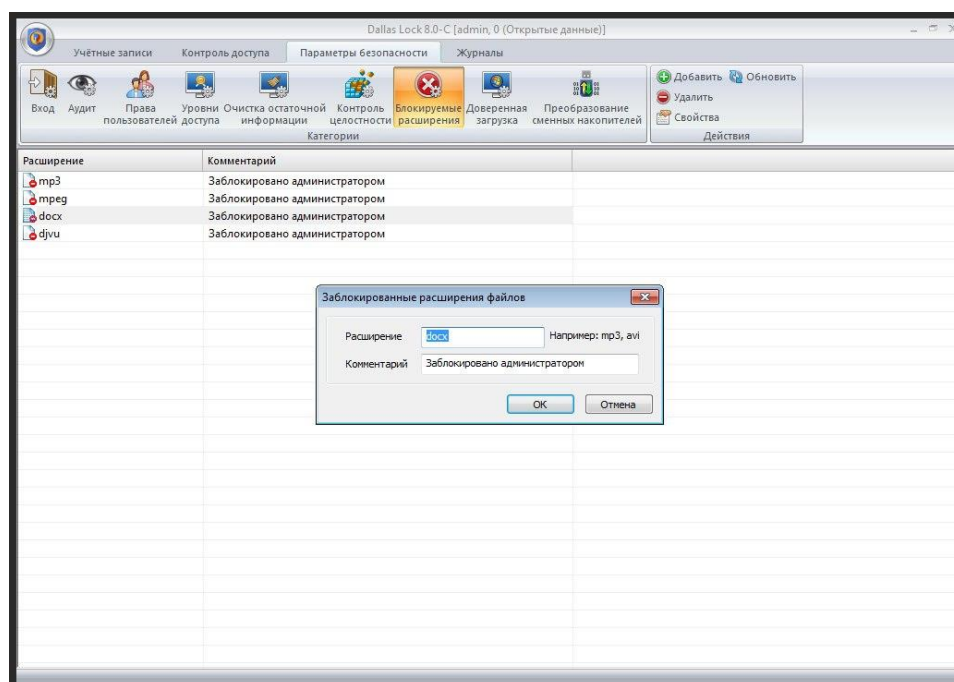


Рисунок 26 – Заблокирование расширения файлов

## 1.10 Создать отчет о правах и конфигурациях Dallas Lock

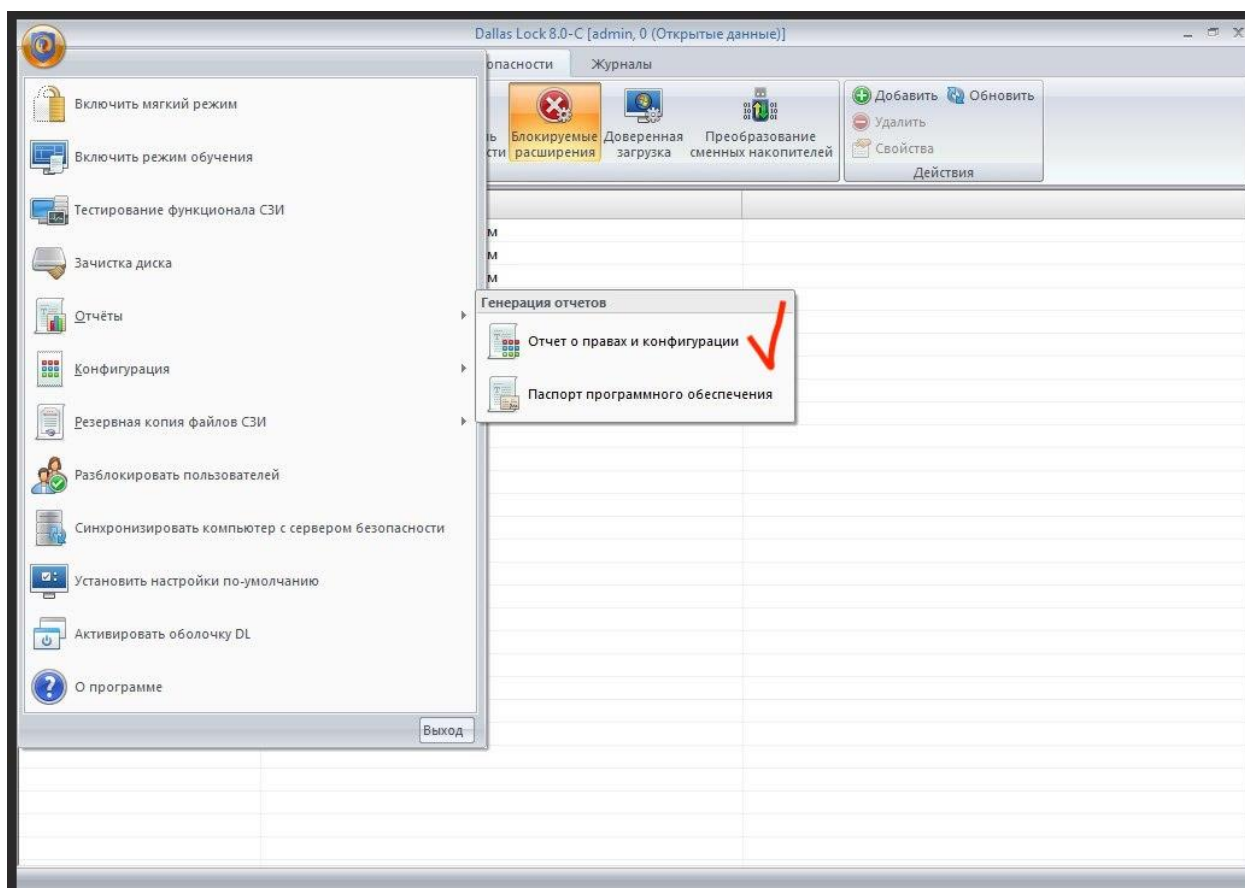


Рисунок 27 – Создание отчет о правах и конфигурациях (1)

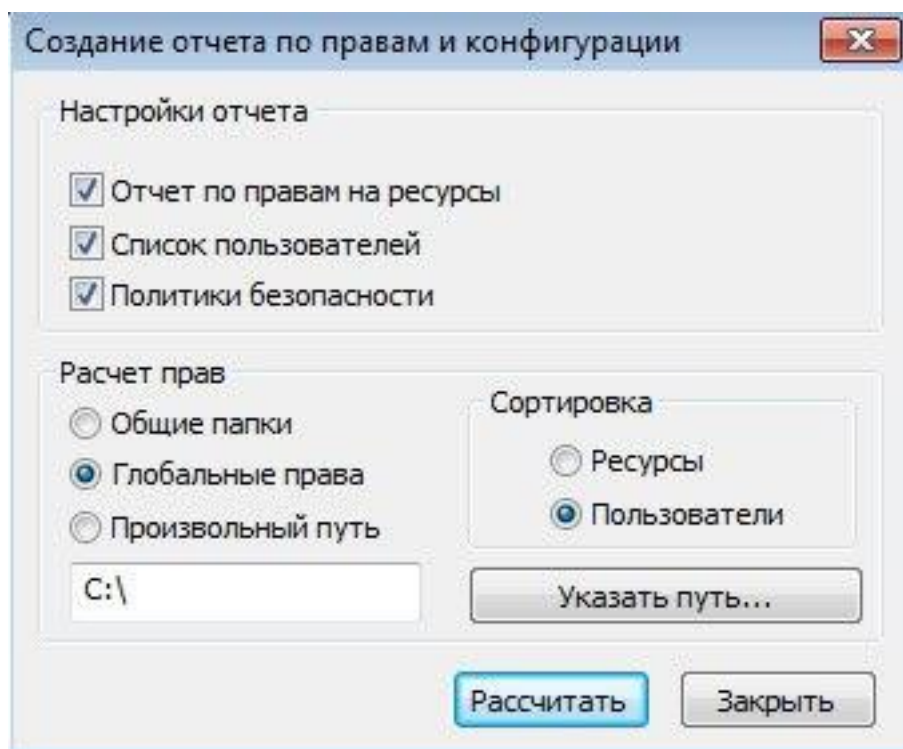


Рисунок 28 – Создание отчет о правах и конфигурациях (2)



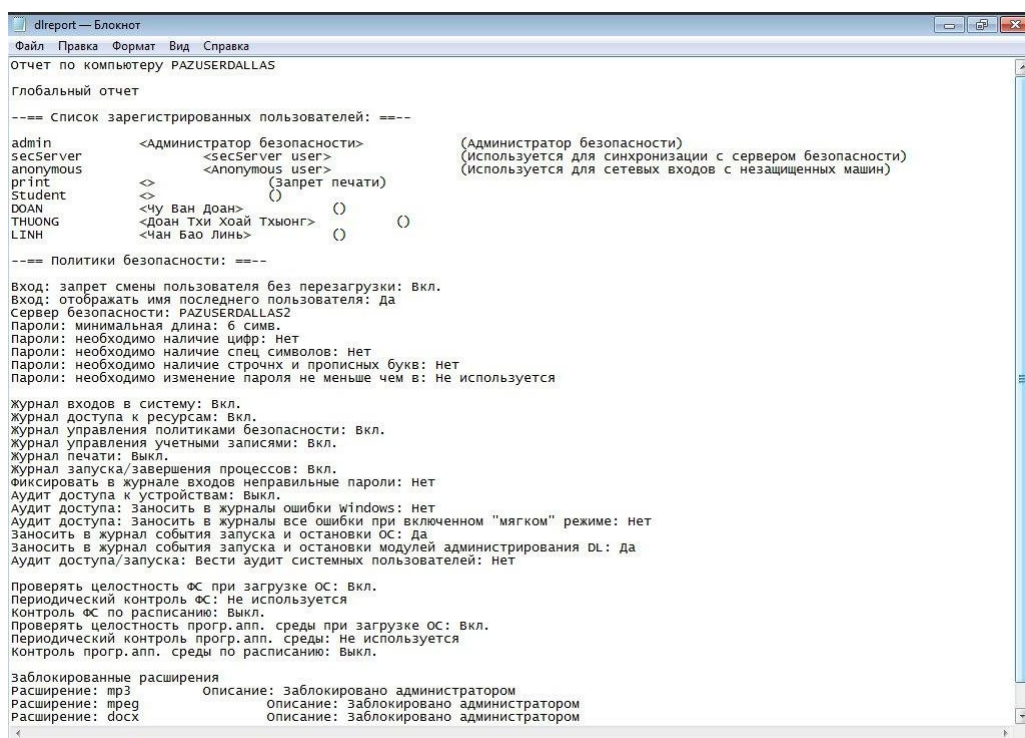


Рисунок 29 – Файл отчета

## 1.11 Создать резервную копию файлов СЗИ от НСД Dallas Lock

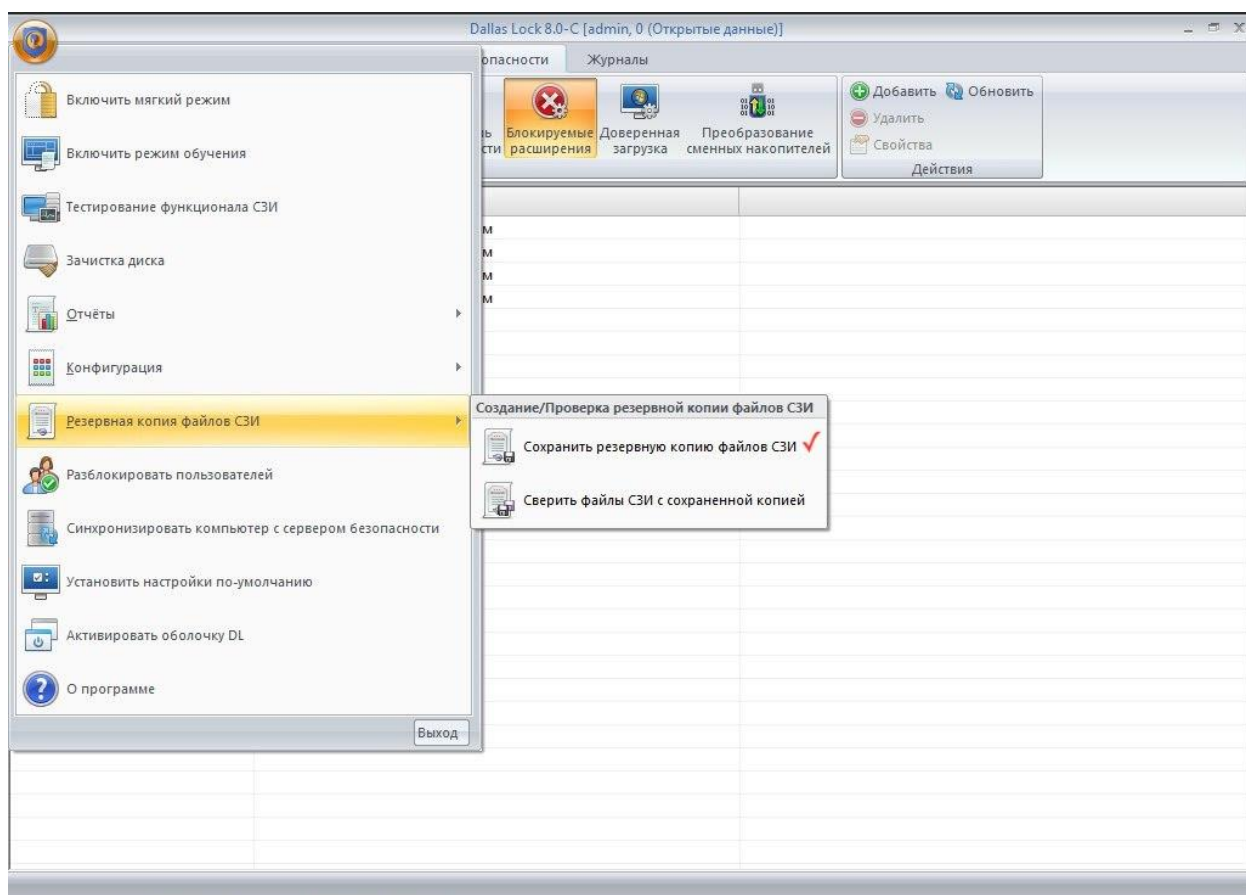


Рисунок 30 – Создание резервной копии файлов СЗИ



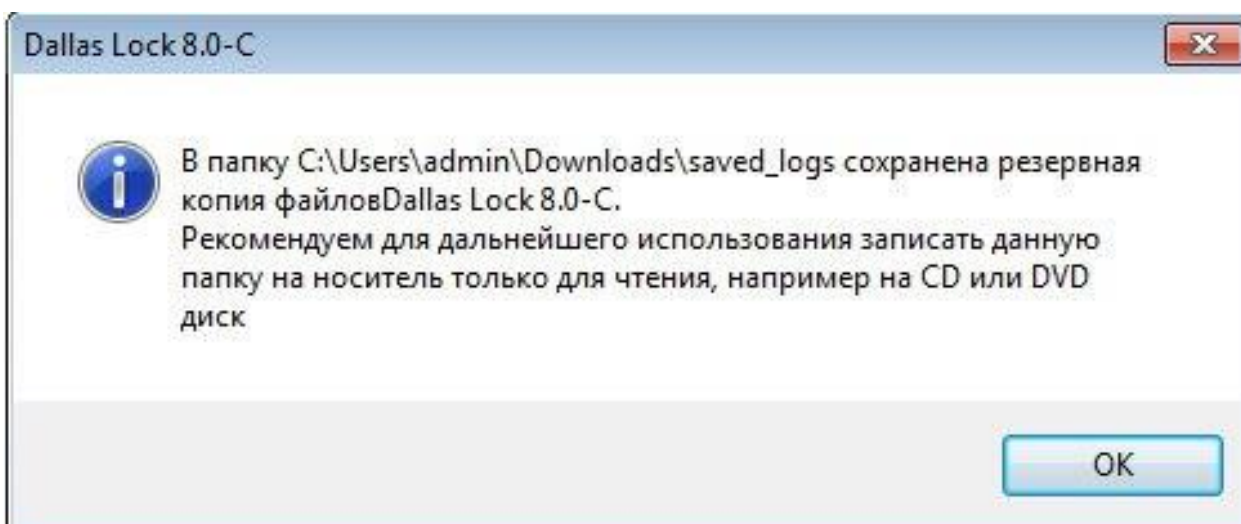


Рисунок 31 – Успеш создания файлов

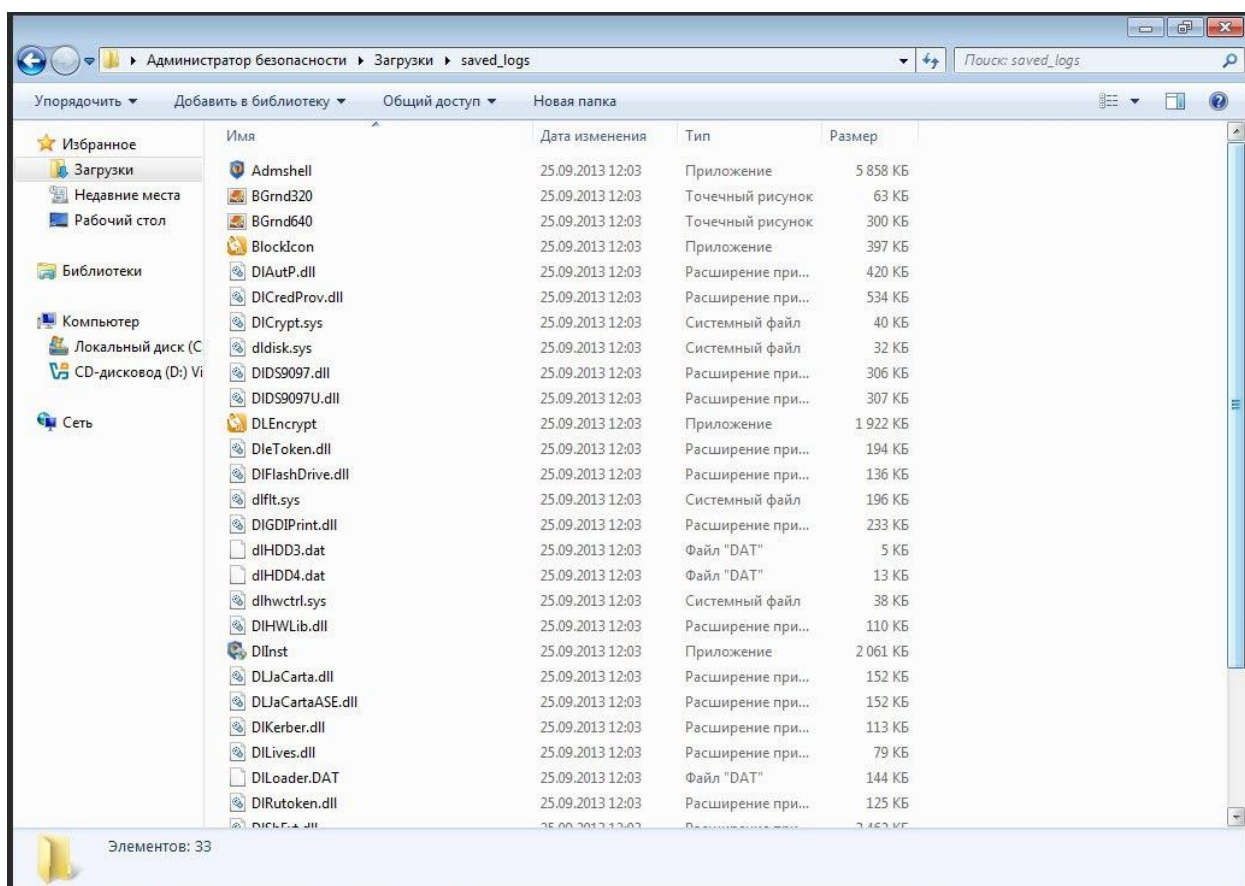


Рисунок 32 – Папка хранения

## 2 ТЕСТИРОВАНИЕ НАСТРОЕННОГО ФУНКЦИОНАЛА

### 2.1 Тестирование запрета смены пользователей без перезагрузки

Мы попытались выйти из учетной записи «DOAN» и перешли на другую учетную запись, но это не сработало. Если учетная запись «DOAN» настроена на обход конфиденциальных правил безопасности, перезагрузка не потребуется (рис. 33).

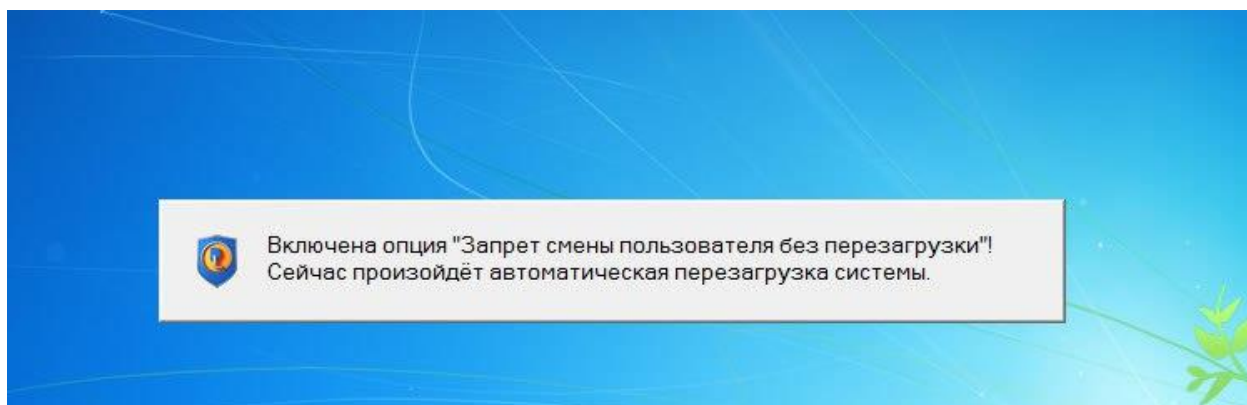


Рисунок 33 – Запрет смены пользователей без перезагрузки

### 2.2 Тестирование декодирования контейнера

Мы попытались декодировать файл с неправильным паролем (рис. 34).

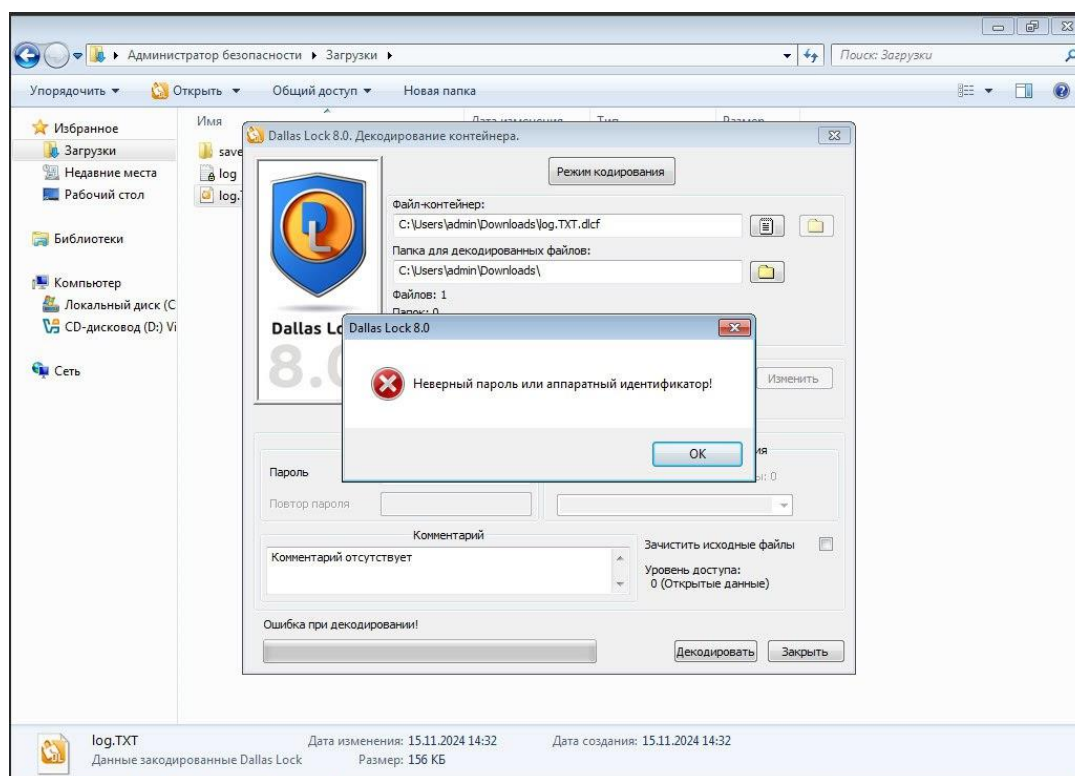


Рисунок 34 – Ввод неверного пароля

Мы успешно расшифровали файл с правильным паролем (рис. 35, 36)

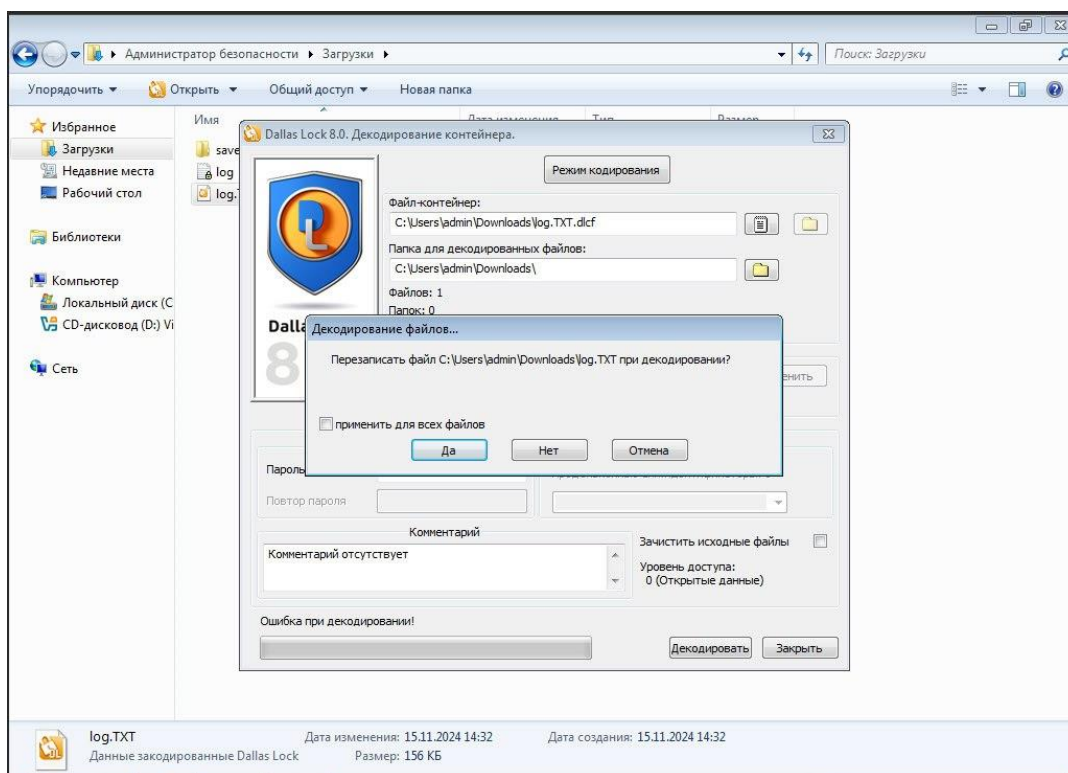


Рисунок 35 – Декодирование контейнера (1)

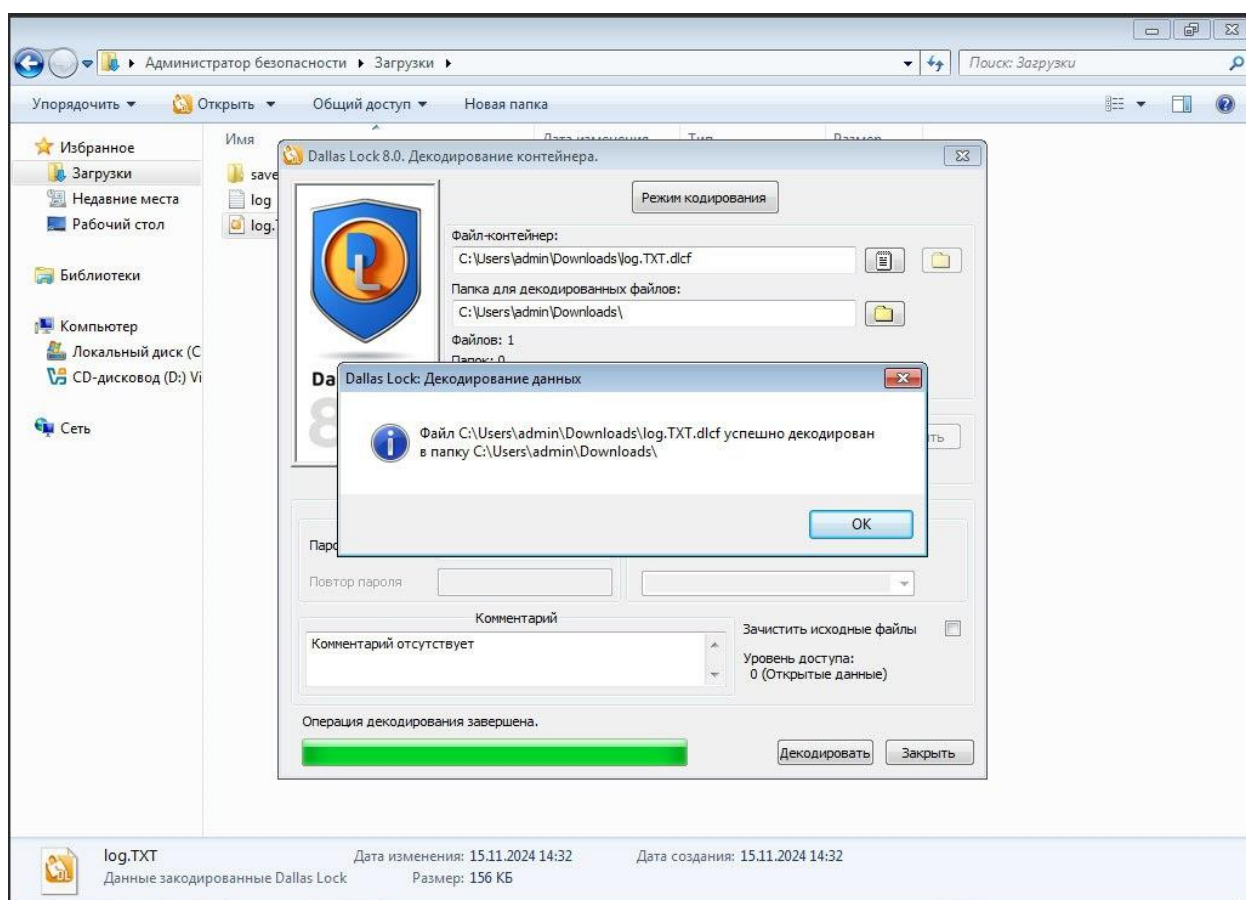


Рисунок 36 – Декодирование контейнера (2)

## 2.3 Тестирование открытия файла запрещено

Использование учетной записи «linh» для создания файла и его сохранения, но это не удастся, поскольку нет доступа к файлу с расширением .docx (рис. 37).

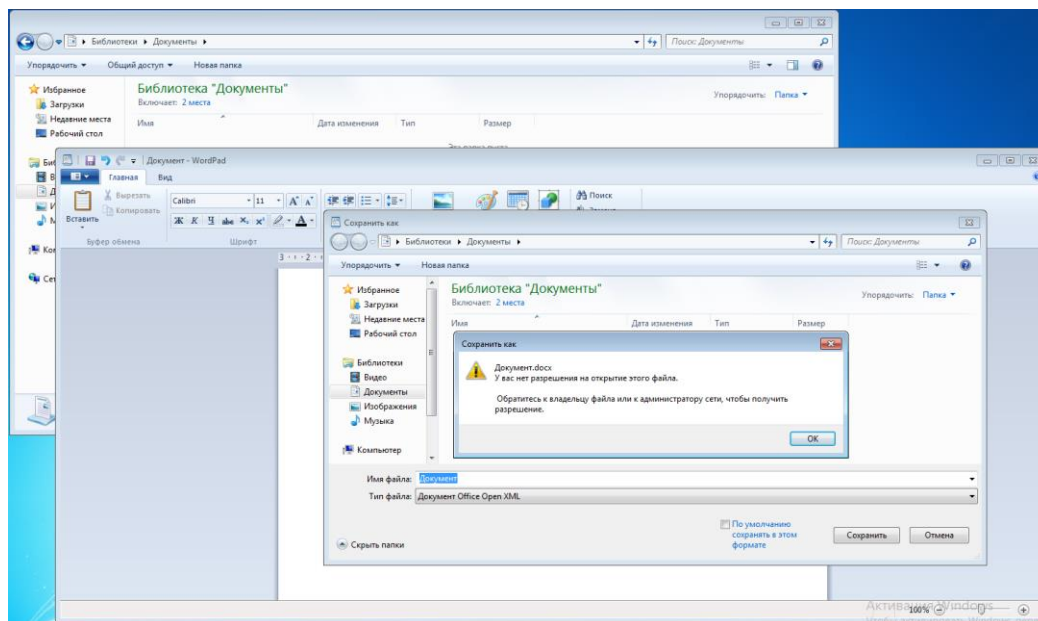


Рисунок 37 – Тестирование открытия файла «.docx»

Невозможно открыть файл «.mp3» (рис. 38).

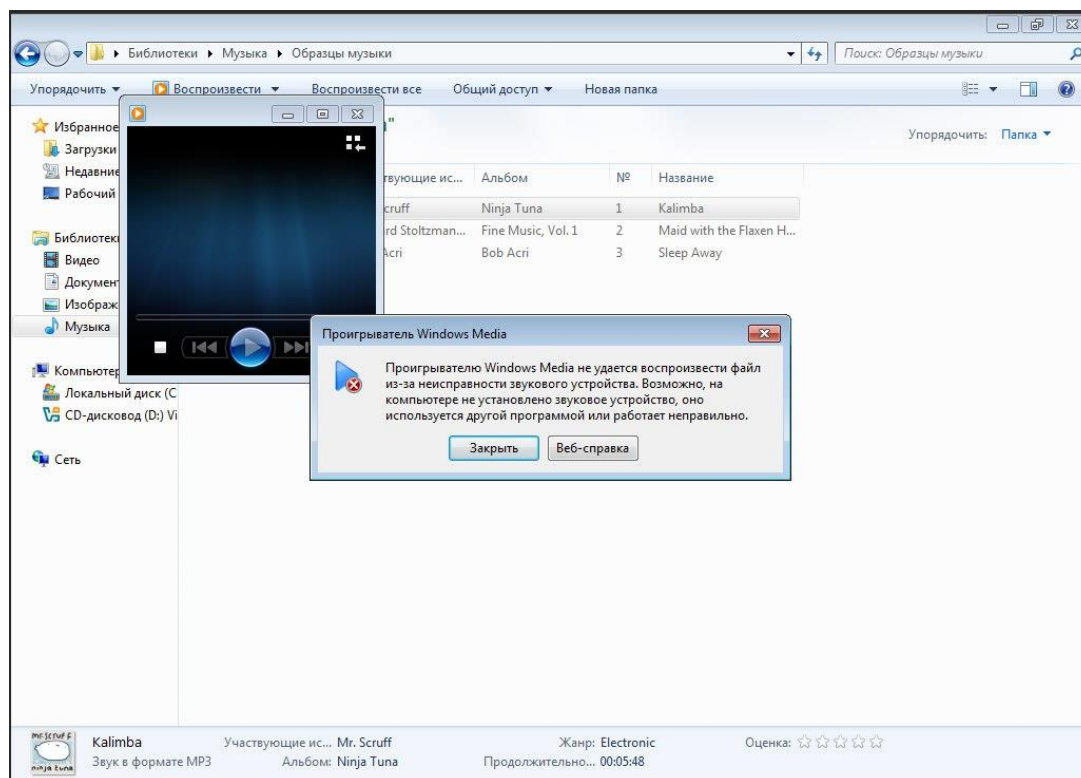


Рисунок 38 – Тестирование открытия файла «.mp3»

## **ЗАКЛЮЧЕНИЕ**

В этой лаборатории нас познакомили с системой защиты информации от несанкционированного доступа в процессе её хранения и обработки. Мы узнали, как настраивать такие функции, как запрет определенных типов файлов, таких как mp3, docx, необходимость перезагрузки операционной системы, если вы хотите изменить учетные записи пользователей и т. д.