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

Факультет безопасности информационных технологий

Дисциплина:

«Программно-аппаратные средства защиты информации»

ОТЧЕТ ПО ЛАБОРАТОРНОЙ РАБОТЕ №2

«Системы обеспечения информационной безопасности от НСД. DallasLock»

Выполнили:

Суханкулиев Мухаммет,

студент группы N3346

_____

(подпись)

Бардышев Артём Антонович,

студент группы N3346

_____

(подпись)

Проверил:

Чешев Никита Игоревич

_____

(отметка о выполнении)

_____

(подпись)

Санкт-Петербург

2025 г.

СОДЕРЖАНИЕ

ВВЕДЕНИЕ

Цель работы – получение практических навыков по настройке и администрированию основных подсистем средства защиты информации от несанкционированного доступа (СЗИ от НСД) Dallas Lock 8.0.

Для достижения поставленной цели были решены следующие задачи:

- Изучение и настройка подсистемы аудита для контроля доступа к объектам файловой системы.
- Освоение инструментов просмотра, фильтрации и экспорта журналов безопасности.
- Изучение и применение механизма делегирования административных полномочий.
- Настройка и проверка работы подсистемы контроля целостности для различных типов объектов.
- Применение функции гарантированного уничтожения информации (зачистки).
- Настройка системных политик безопасности на примере запрета смены пользователя.
- Изучение и применение подсистемы шифрования для защиты данных в файлах-контейнерах.
- Настройка политики блокировки доступа к файлам по их расширениям.
- Формирование отчетной документации по конфигурации СЗИ.
- Создание резервной копии программных файлов СЗИ и запуск процедуры самодиагностики.

1 DALLAS LOCK

Для выполнения лабораторной работы была использована предоставленная виртуальная машина с предустановленной ОС Windows 7 и СЗИ от НСД Dallas Lock 8.0-C. Вход в систему осуществлялся под учетной записью администратора admin.

1.1 Настроить политику аудита для 2 пользователей

Подсистема регистрации и учета Dallas Lock обеспечивает ведение электронных журналов, в которых фиксируются действия пользователей. Для этого необходимо настроить политику аудита, указав, какие именно события и для каких объектов должны протоколироваться.

Для контроля доступа к файлам были созданы два тестовых пользователя: `User1` и `User2`. Затем для объекта `C:\secret.txt` была настроена политика аудита, регистрирующая как успешные, так и неуспешные попытки чтения файла. Включение подсистемы аудита производилось через `Параметры безопасности – Аудит – Журнал доступа к ресурсам`.

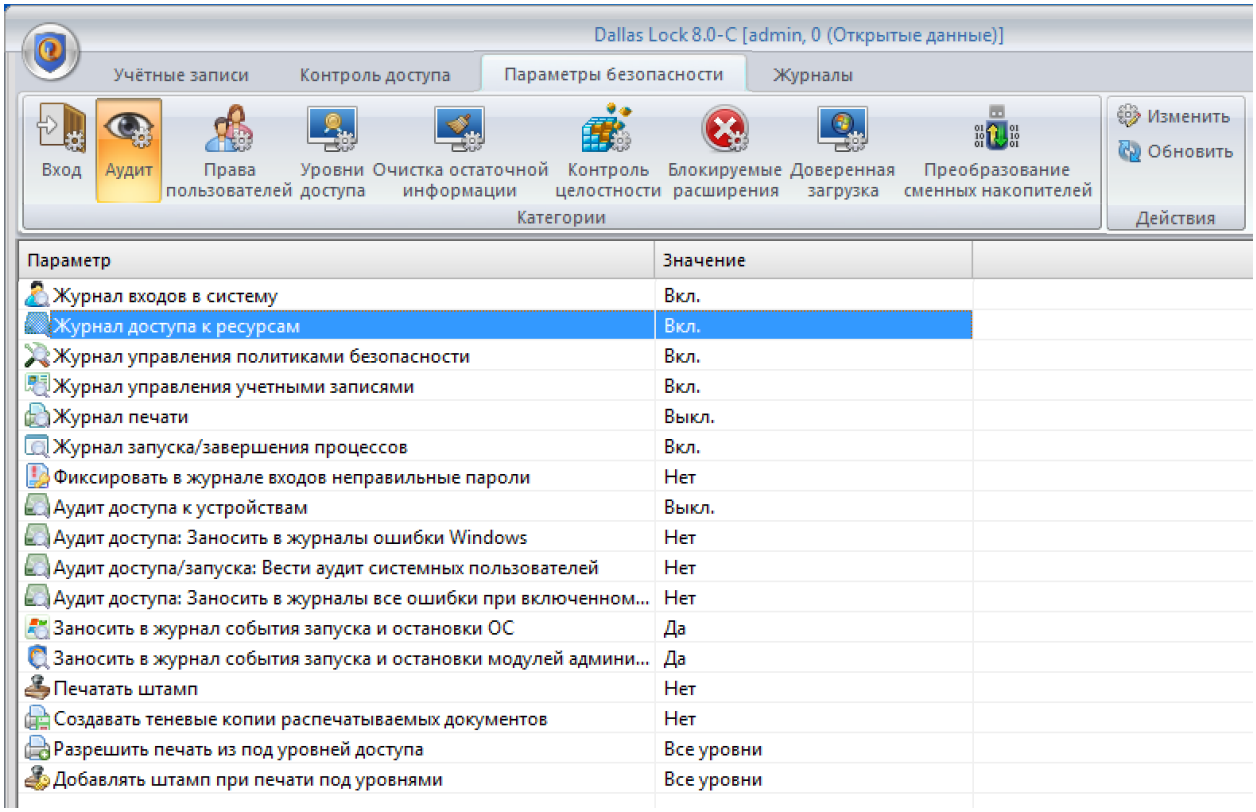

Рисунок 1 – Включение «Журнала доступа к ресурсам»

Настройка аудита для конкретного файла выполнялась через его контекстное меню `DL8.0: Права доступа` на вкладке «Аудит доступа».

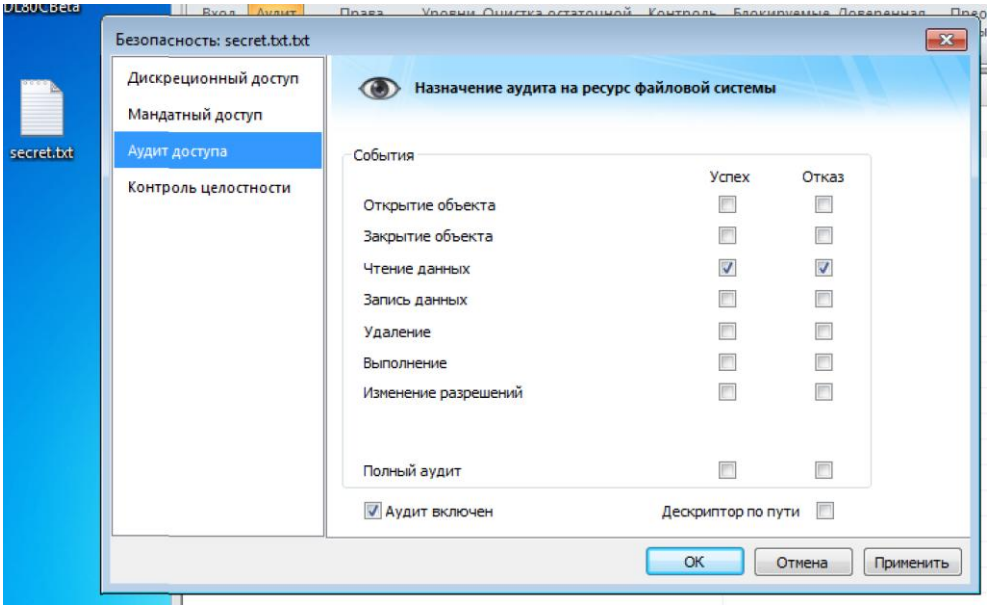

Рисунок 2 – Настройка аудита для файла

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

Для облегчения работы с журналами в Dallas Lock предусмотрена возможность фильтрации записей по определенному признаку и экспортирования журналов в различные форматы, что обеспечивает удобство анализа и отчетности.

В консоли Dallas Lock открываем: `Журналы – Журнал входов`.

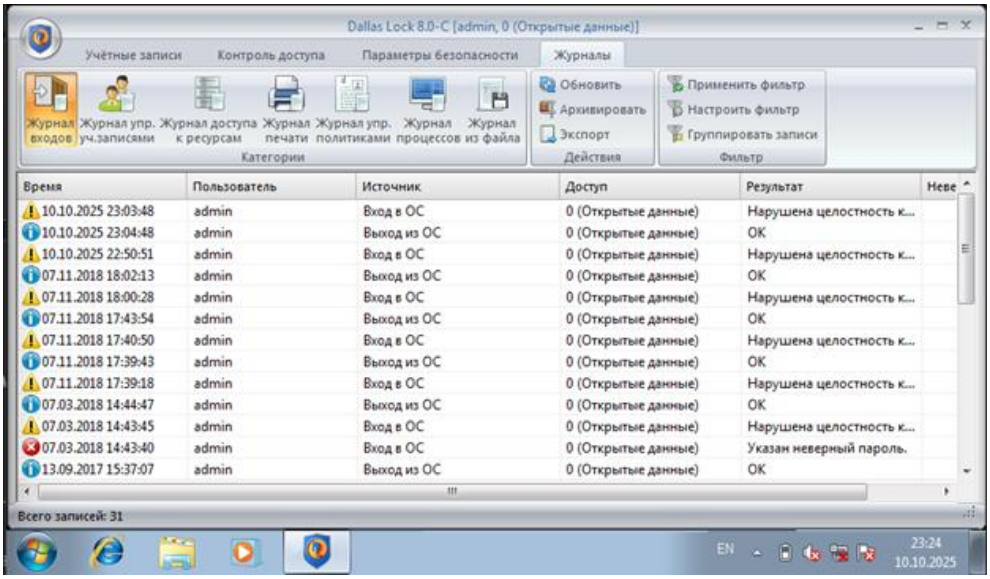

Рисунок 3 – Общий вид журнала входов

С помощью фильтра можно отсортировать нужную нам дату и время и увидеть именно те события, которые были совершены в указанную дату. Был задан временной диапазон «Текущая неделя» для отображения событий в «Журнале ресурсов».

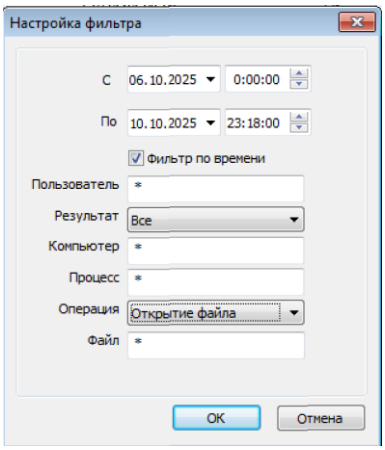

Рисунок 4 – Настройка фильтра

Впоследствии, если есть такая цель, то можно выгрузить необходимую информацию в формате `.txt` или `.csv`. Отфильтрованные данные были экспортированы в файл для дальнейшего анализа.

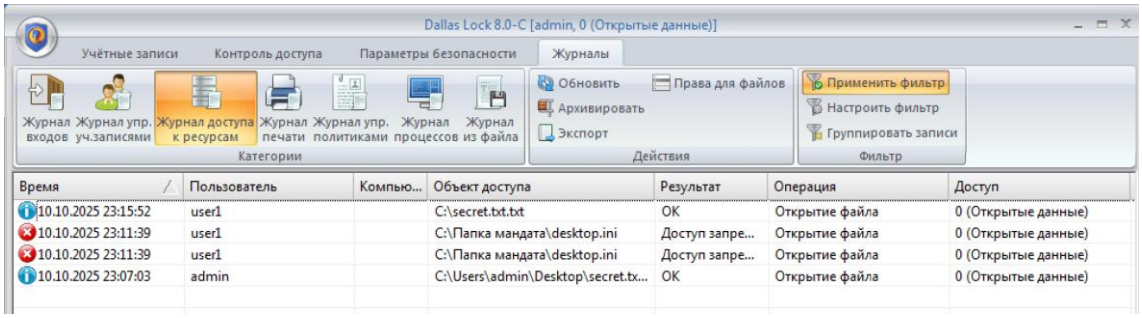

Рисунок 5 – Результат применения фильтра

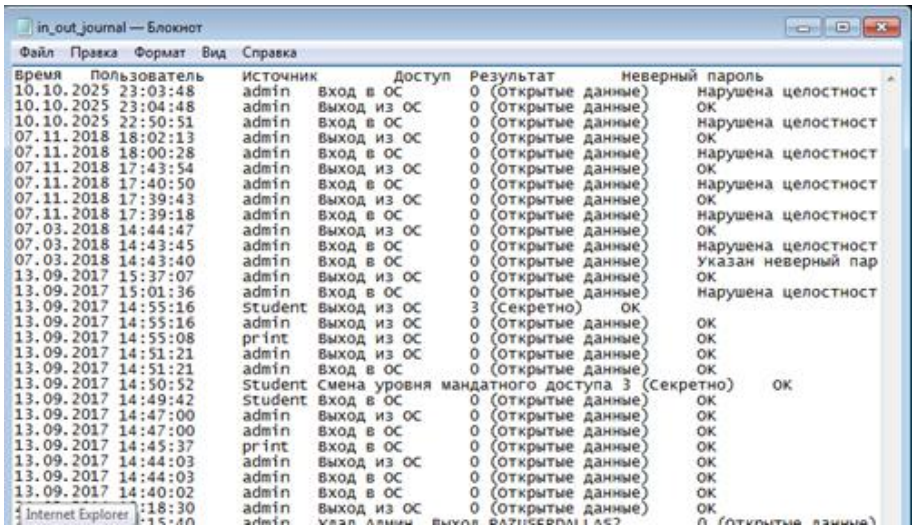

Рисунок 6 – Экспортированный файл журнала

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

Механизм делегирования полномочий позволяет администратору предоставлять другим пользователям часть своих прав на управление системой, не давая полного доступа.

Для предоставления пользователю `User1` прав были выполнены следующие шаги:

В разделе `Параметры безопасности – Права пользователей` для полномочия `Учётные записи: Управление` был добавлен `User1`.

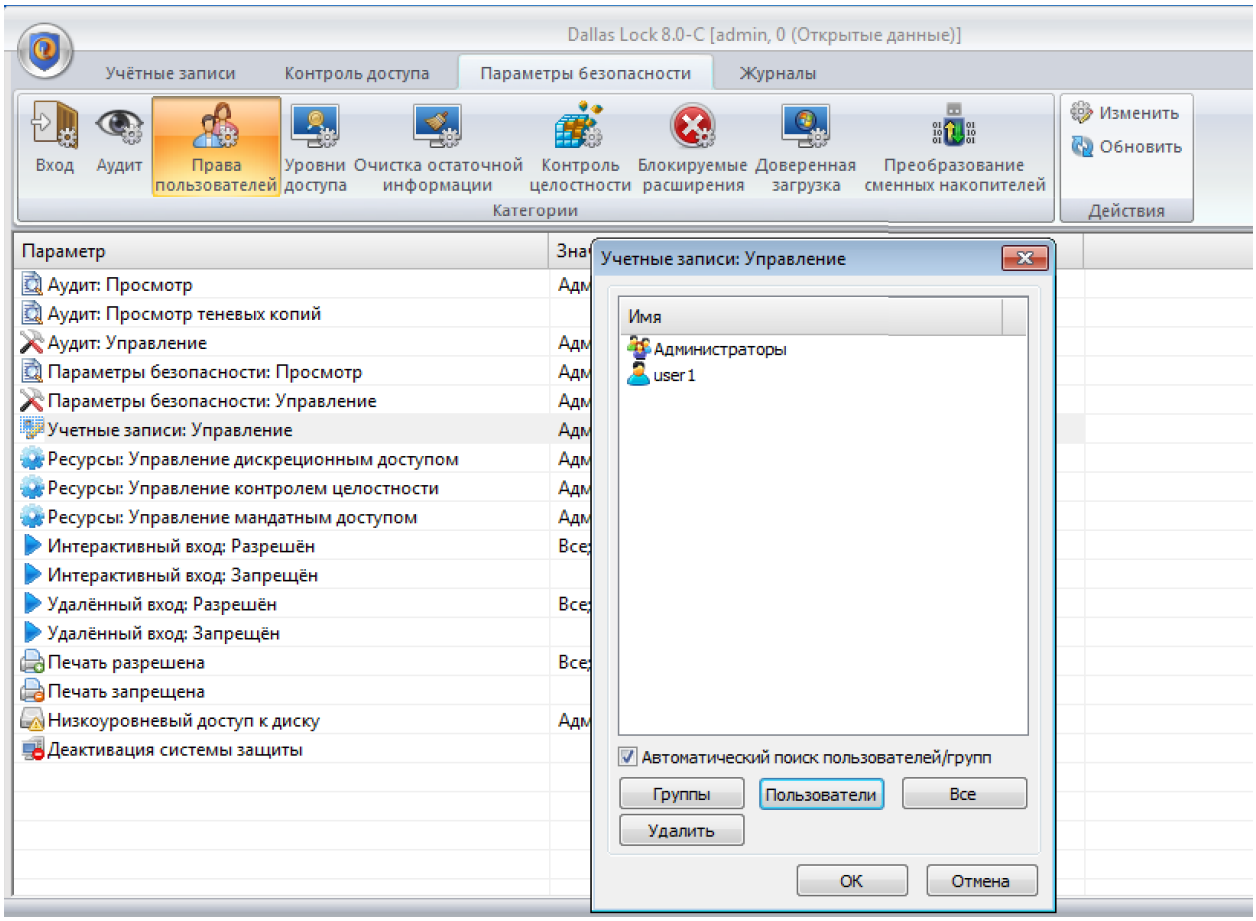

Рисунок 7 – Делегирование права управления учетными записями

Также были предоставлены права на просмотр параметров и журналов для входа в консоль.

Произведена проверка: вход под `User1`. Проверка показала, что `User1` действительно может управлять пользователями (например, удалить `User2`), но не менять системные параметры.

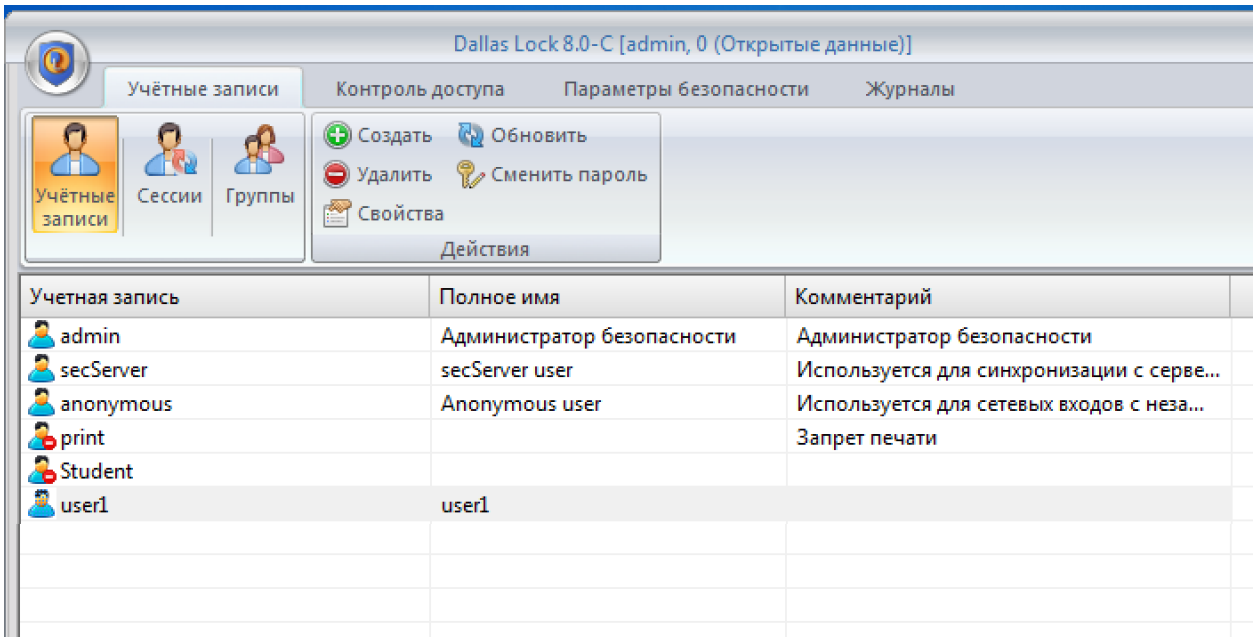

Рисунок 8 – Проверка полномочий: User1 удаляет User2

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

Открываем контроль целостности в меню. В этом пункте вычисляется контрольная сумма и сверяется с расчетной для того, чтобы фиксировать нарушения, связанные с целостностью файлов. Если хеш не совпадает, то Dallas Lock сообщает об этом.

Контрольная сумма – это уникальный цифровой отпечаток (хэш) файла, папки или системного ресурса, который вычисляется по выбранному алгоритму:

• CRC32 – простой контрольный код (для быстрой проверки, не криптостойкий);

• MD5 – хэш-функция (128 бит, надёжная для целостности, но не для криптографии);

• ГОСТ Р 34.11-94 – отечественный стандарт, криптографически устойчивый хэш.

Система хранит рассчитанные суммы и при каждой проверке сравнивает их с текущими.

Была произведена настройка контроля целостности для файла secret.txt с использованием алгоритма ГОСТ Р 34.11-94.

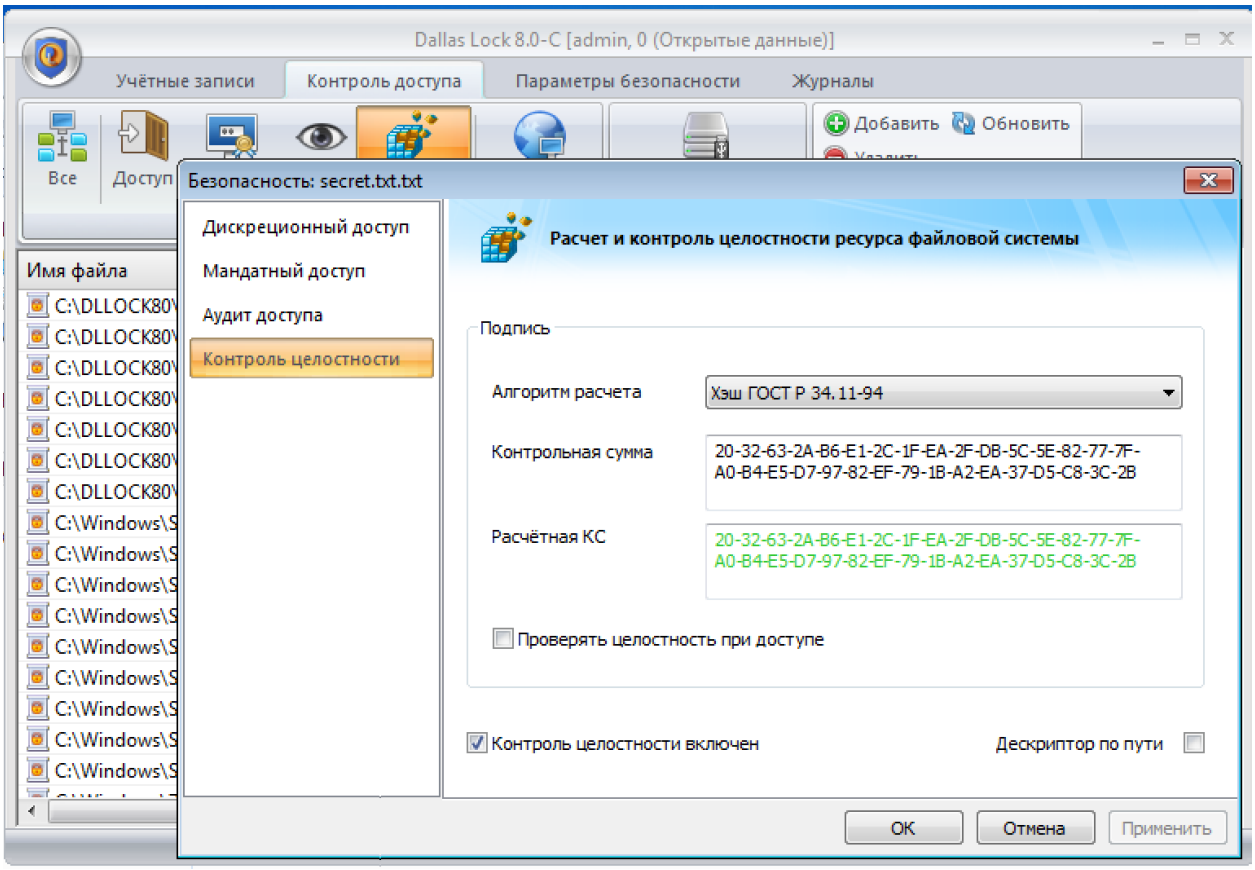

Рисунок 9 – Настройка контроля целостности файла

При попытке настроить контроль для папок и дисков система выдавала ошибку, что является особенностью данной виртуальной среды.

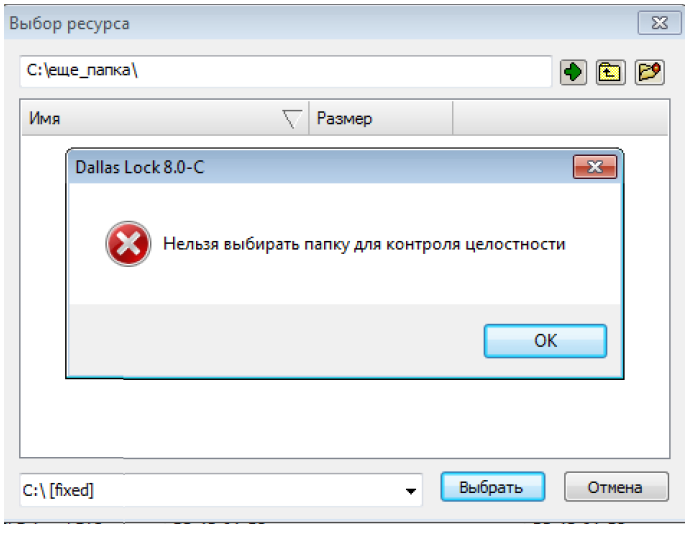

Рисунок 10 – Ошибка при добавлении папки на контроль

Таким образом мы контролируем целостность: при попытке изменить информацию действие будет зафиксировано. Содержимое файла secret.txt было изменено, после чего система корректно зафиксировала нарушение.

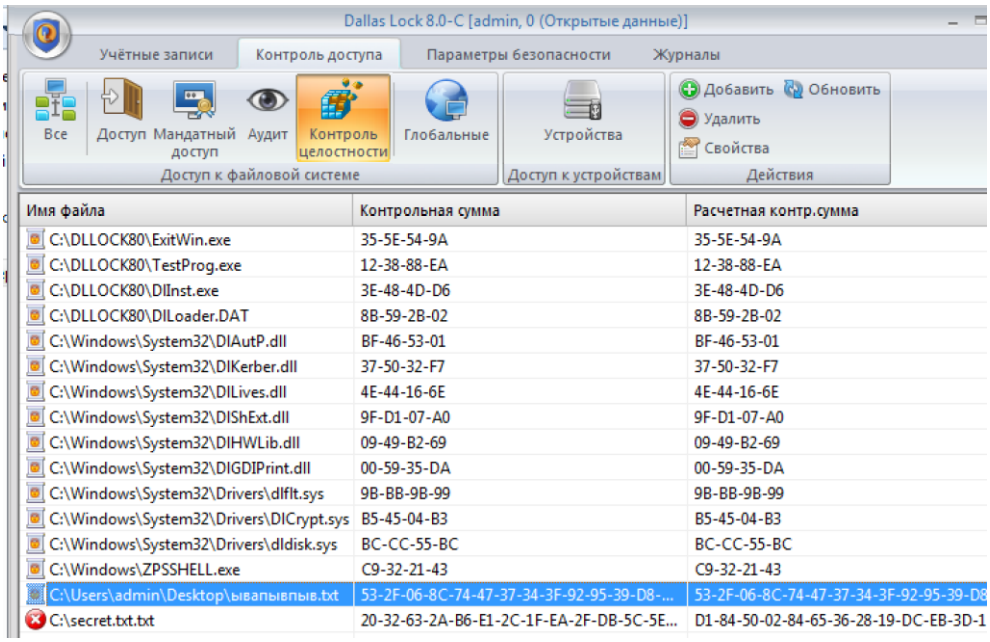

Рисунок 11 – Фиксация нарушения целостности

1.5 Удалить и очистить с помощью Dallas Lock информацию о сохраненных журналах

Подсистема очистки остаточной информации гарантирует предотвращение восстановления удаленных данных путем многократной перезаписи секторов диска, где располагался файл.

Текущий журнал был принудительно заархивирован. Для контроля открываем каталог: `C:\DLLOCK80\Logs`.

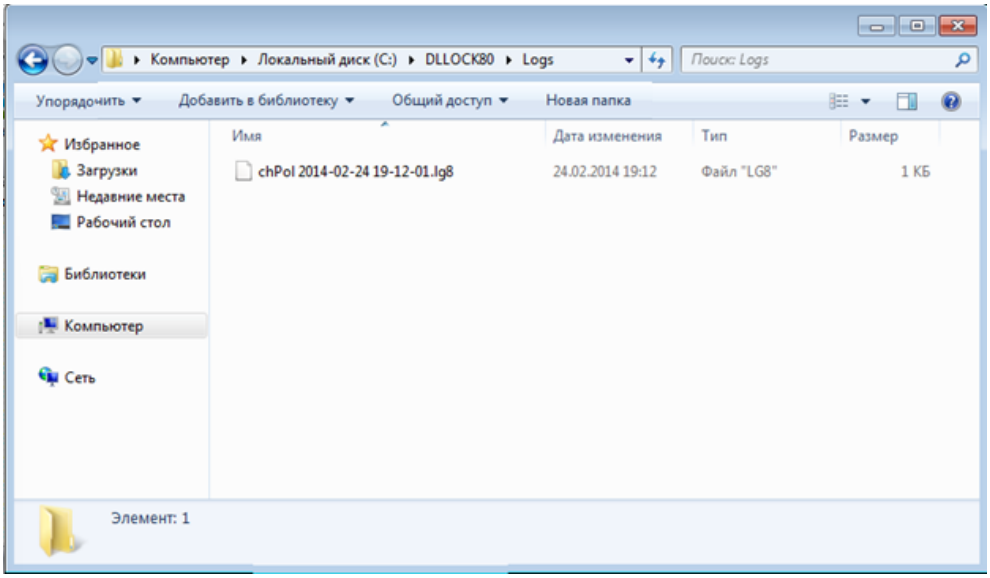

Рисунок 12 – Папка с архивами журналов

Для гарантированного уничтожения файла архива была использована специальная функция из контекстного меню `DL8.0: Удалить и зачистить`.

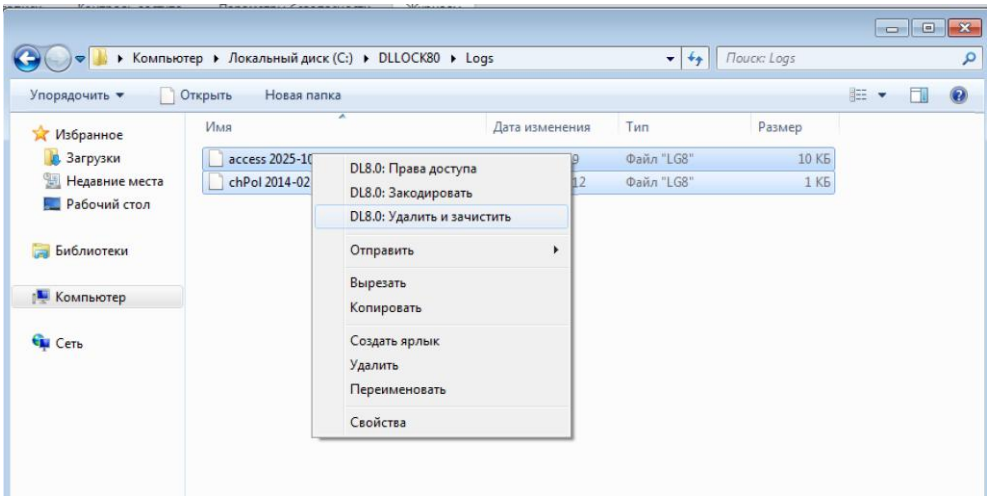

Рисунок 13 – Использование функции «Удалить и зачистить»

1.6 Настроить запрет смены пользователей без перезагрузки

Политика «Запрет смены пользователя без перезагрузки» предотвращает возможность завершения сеанса одного пользователя и начала работы другого без полной очистки оперативной памяти, что является мерой защиты от анализа остаточной информации.

Для повышения уровня безопасности была активирована данная политика. Настройка производилась в `Параметры безопасности – Вход – Вход: запрет смены пользователя без перезагрузки`.

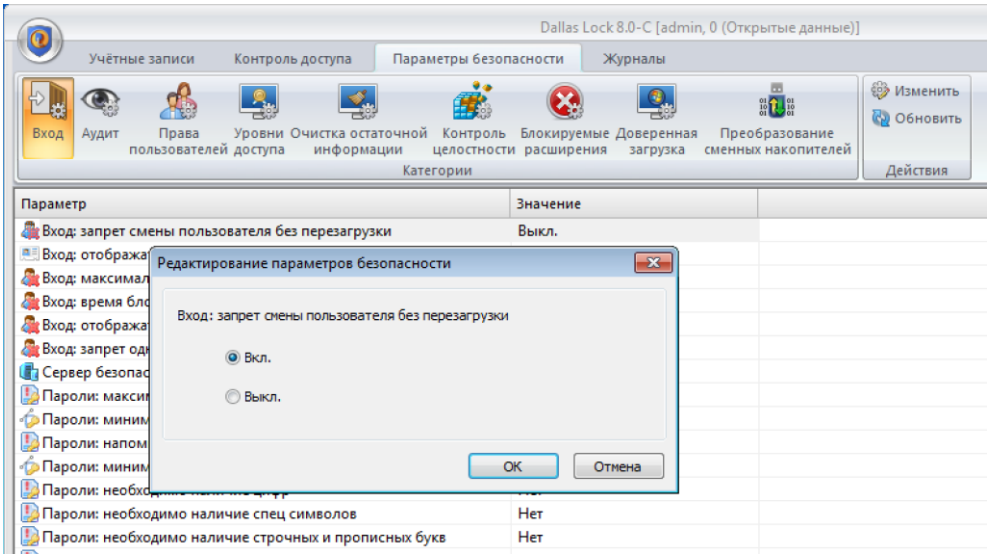

Рисунок 14 – Активация политики запрета смены пользователя без перезагрузки

Проверка показала, что при попытке сменить пользователя система корректно инициирует перезагрузку.

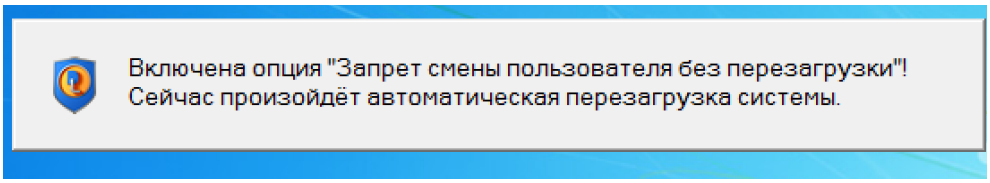

Рисунок 15 – Результат: инициирование перезагрузки

1.7 Создать папки, файлы, зашифровать их, используя встроенные криптоалгоритмы

Подсистема преобразования информации обеспечивает кодирование данных в файлы-контейнеры для защиты при хранении или передаче по открытым каналам. В качестве ключа используется пароль и, опционально, аппаратный идентификатор.

Был изучен механизм шифрования данных. Опытным путем установлено, что шифрование отдельных файлов работает корректно, в то время как при кодировании папок их содержимое не переносится в контейнер. Был успешно создан зашифрованный файл-контейнер с использованием пароля и алгоритма ГОСТ, а затем успешно декодирован обратно.

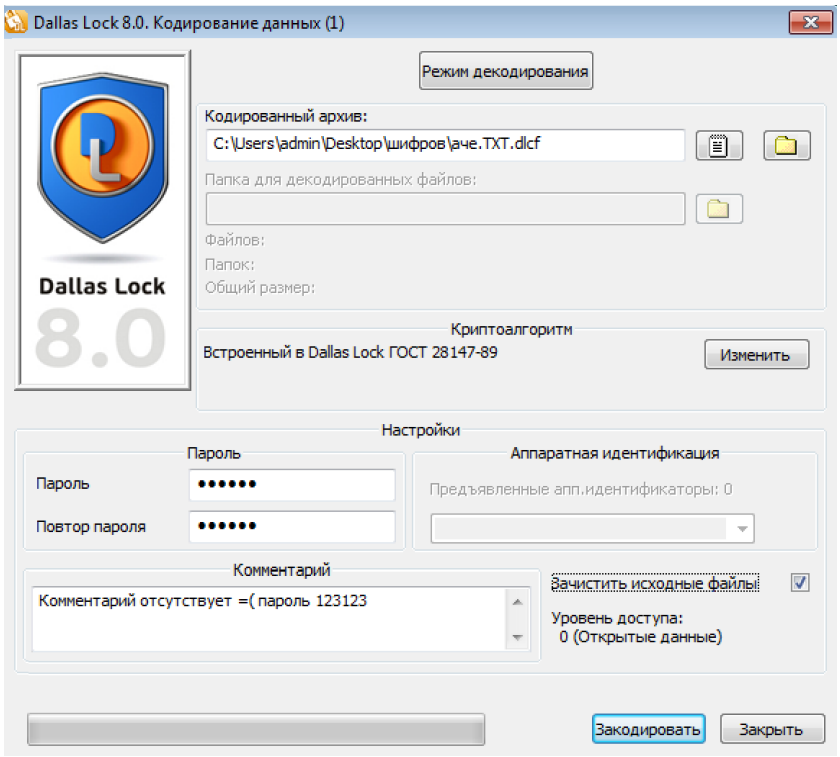

Рисунок 16 – Процесс кодирования файла в контейнер

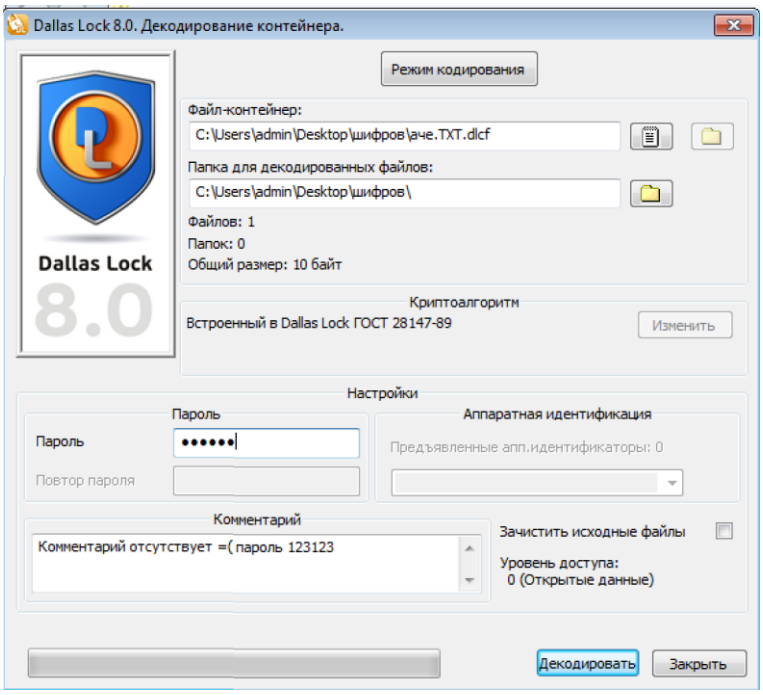

Рисунок 17 – Процесс декодирования файла

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

Dallas Lock позволяет задавать список расширений файлов, работа с которыми будет блокирована. Это позволяет запретить сотрудникам работу с файлами, не имеющими отношения к их профессиональным обязанностям.

Для ограничения использования нежелательных типов файлов была настроена политика блокировки в `Параметры безопасности – Блокируемые расширения`. В список были добавлены расширения `mp3`, `mpeg`, `docx` и `djvu`.

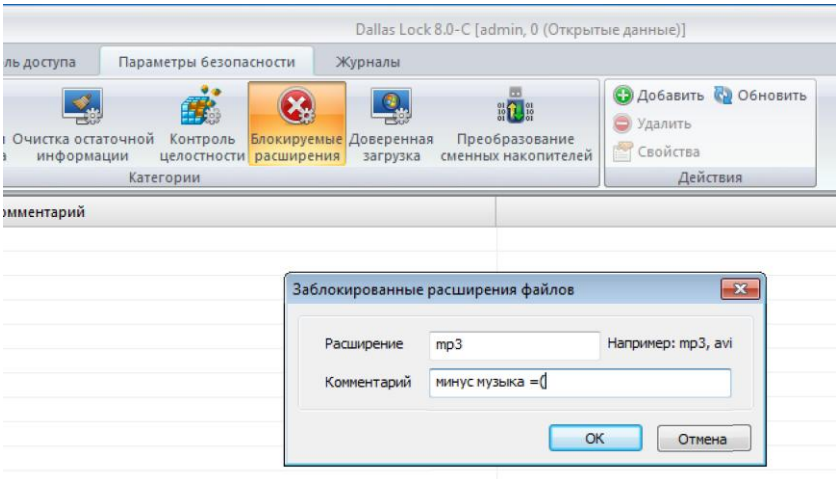

Рисунок 18 – Настройка блокируемого расширения

Проверка под учетной записью `User1` показала, что попытка открытия файла с расширением `.docx` успешно блокируется системой.

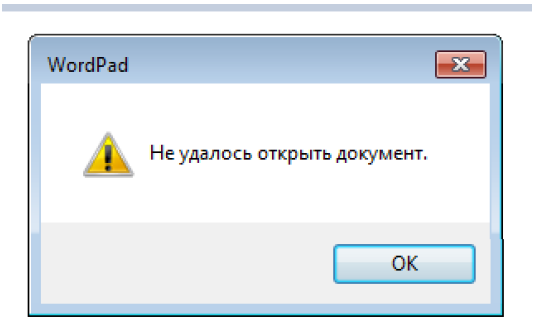

Рисунок 19 – Результат: блокировка доступа к файлу

1.9 Создать отчет о правах и конфигурациях Dallas Lock

Для проверки соответствия настроек СЗИ существует возможность создания отчетов по назначенным правам и конфигурациям, что является важным элементом аудита и документирования системы защиты.

Для документирования текущих настроек был использован встроенный генератор отчетов, запущенный из главного меню консоли.

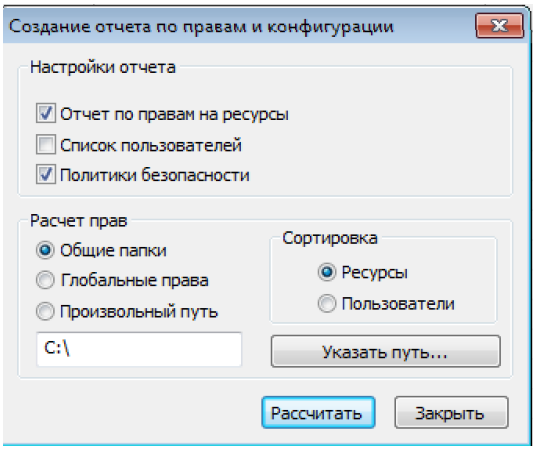

Рисунок 20 – Мастер создания отчета

Был сформирован комплексный отчет, включающий список пользователей, политики безопасности и матрицу прав доступа.

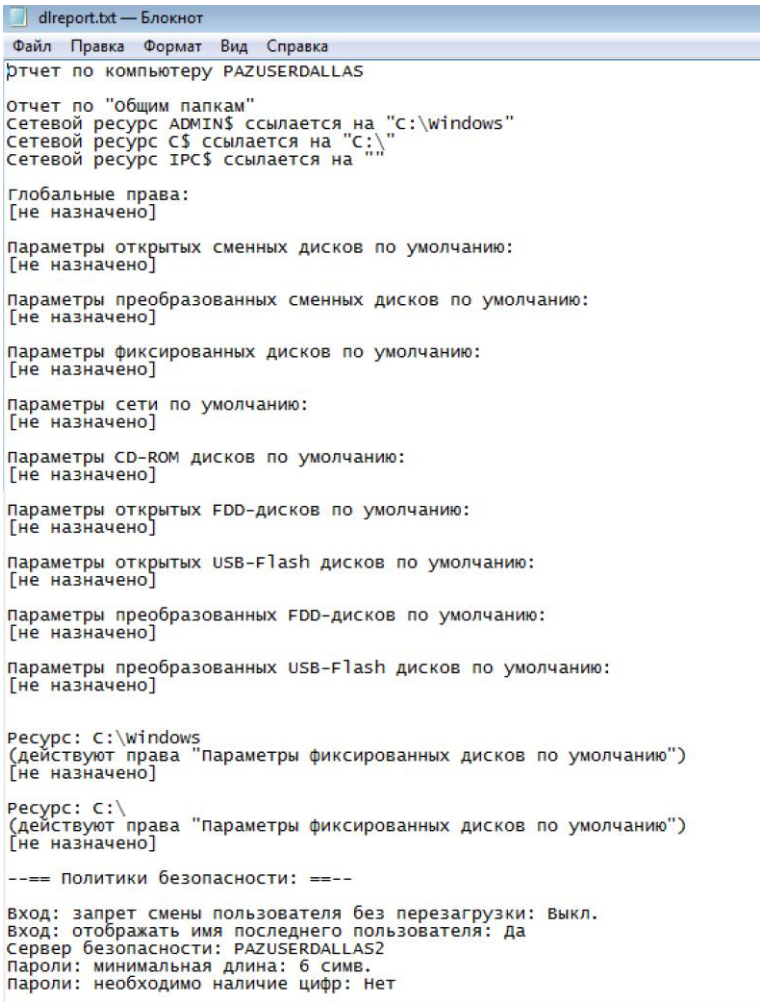

Рисунок 21 – Фрагмент сгенерированного отчета

1.10 Создать резервную копию файлов СЗИ от НСД Dallas Lock

Предусматривается ведение резервных копий программных средств защиты информации, их периодическое обновление и контроль работоспособности для обеспечения отказоустойчивости СЗИ.

Для обеспечения возможности восстановления программных компонентов СЗИ была создана резервная копия ее системных файлов. Функция была вызвана из главного меню консоли. Копия была успешно сохранена в указанную директорию.

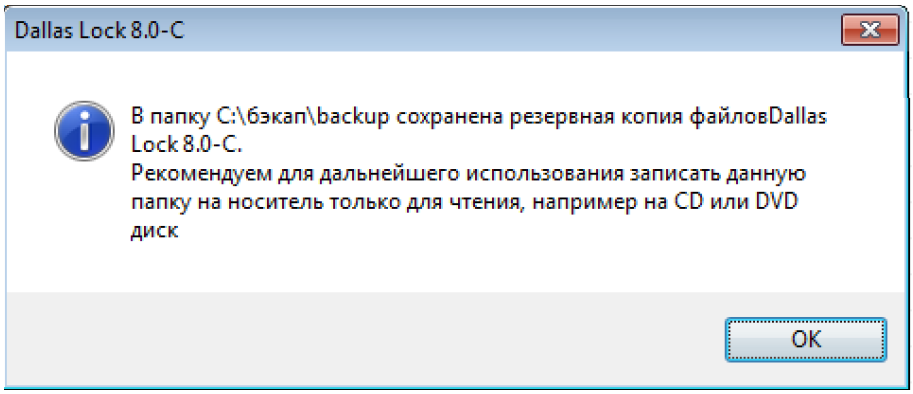

Рисунок 22 – Сообщение об успешном создании бэкапа

1.11 Протестировать функционал Dallas Lock

СЗИ НСД Dallas Lock 8.0 содержит подсистему самодиагностики основного функционала, которая позволяет в автоматическом режиме проверить работоспособность ключевых механизмов защиты.

В завершение работы была запущена процедура самодиагностики СЗИ.

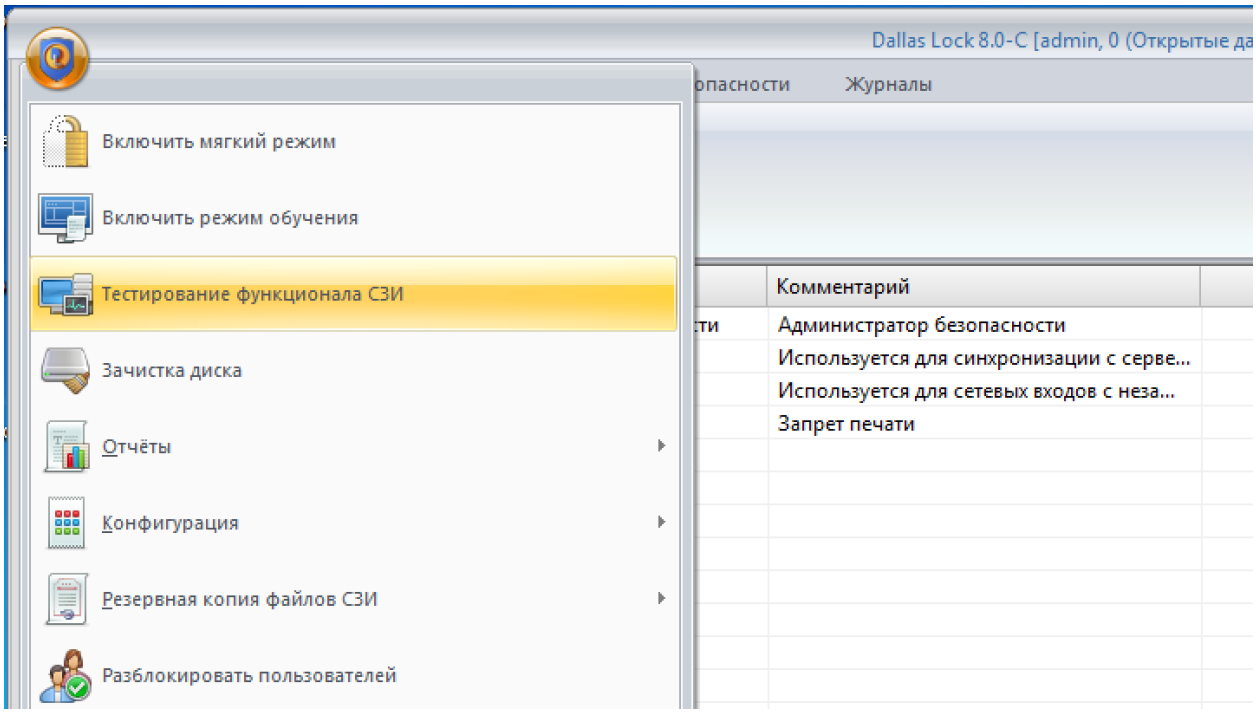

Рисунок 23 – Запуск процедуры тестирования

Система автоматически проверила все ключевые подсистемы. Отчет о тестировании показал, что все проверки пройдены успешно.

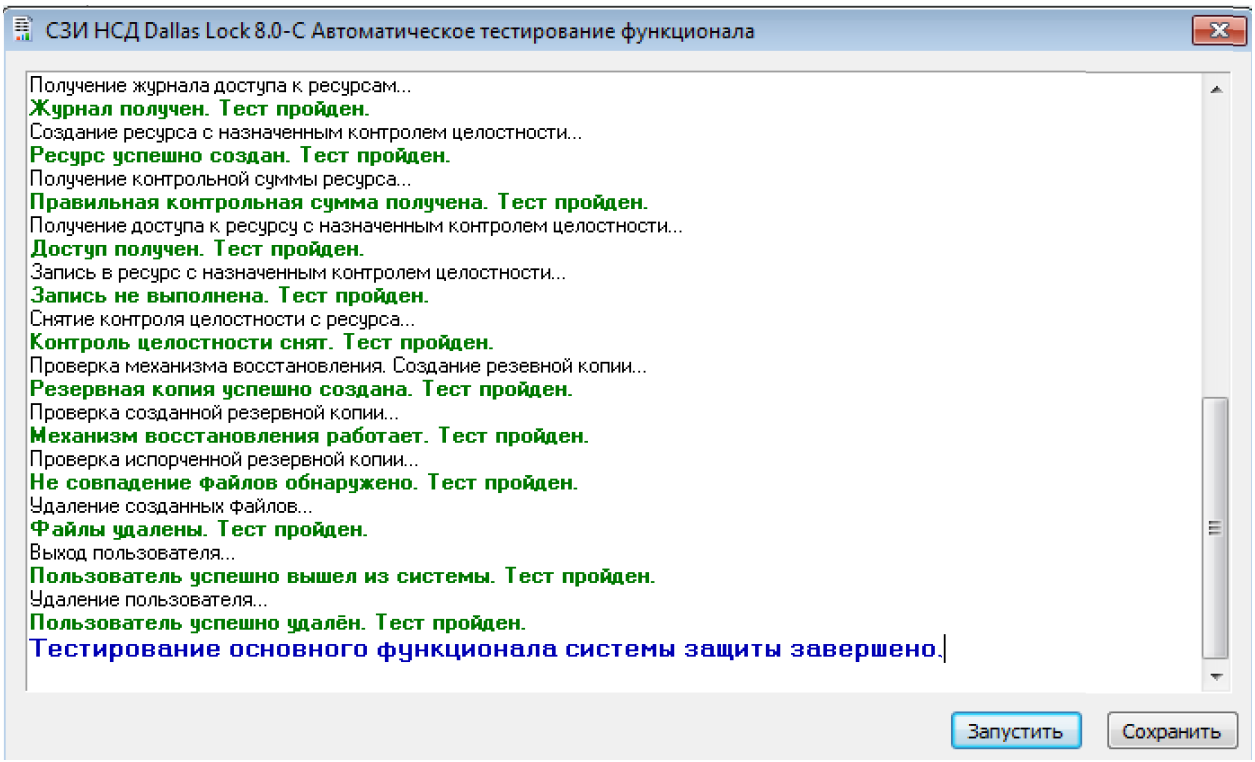

Рисунок 24 – Результаты самодиагностики системы

ЗАКЛЮЧЕНИЕ

В ходе выполнения лабораторной работы была достигнута поставленная цель: были получены практические навыки администрирования СЗИ от НСД Dallas Lock 8.0.

Были решены все поставленные задачи: изучены и настроены подсистемы аудита, контроля целостности, разграничения доступа и шифрования. Освоены механизмы делегирования полномочий, применения политик безопасности, а также инструменты документирования и самодиагностики системы. Были выявлены и проанализированы особенности работы некоторых функций в предоставленной виртуальной среде.

СПИСОК ИСПОЛЬЗОВАННЫХ ИСТОЧНИКОВ

1. Лазутин А. И. Курс лекций по дисциплине «Программно-аппаратные средства защиты информации» / А. И. Лазутин, Армавир, 2023. – Текст: непосредственный.
2. Система защиты информации Dallas Lock 8.0. Руководство по эксплуатации : RU.48957919.501410-02 92. – Текст : непосредственный.