МИНОБРНАУКИ РОССИИ

Федеральное государственное бюджетное образовательное учреждение

высшего образования

«МИРЭА – Российский технологический университет»

РТУ МИРЭА

Колледж программирования и кибербезопасности

Отчет о выполнении практического задания

по дисциплине «МДК.01.04 Эксплуатация автоматизированных

(информационных)

систем в защищенном исполнении»
на тему «Защита входа в систему (идентификация и аутентификация пользователей)»
Практическое задание № 11

Специальность – 10.05.02 Информационная безопасность

автоматизированных систем

Выполнил студент:

_____Маркаров М. О.

Группа: ИБ-32

Руководитель:

_____Герасин В. Ю.

Работа защищена с оценкой _____

Дата защиты _____

Москва

2025

Практическое занятие № 11

Тема: Защита входа в систему (идентификация и аутентификация пользователей)

Цель: познакомиться с системами защиты информации от несанкционированного доступа

Ход работы:

Для начала с клонируем виртуальную машину Windows Pro далее в настройках задаём пароль.

После этого в настройках виртуальной машины добавляем общую папку с дистрибутивом Dalls Lock.

Установка автономной версии СЗИ от НСД Dallas Lock 8.0.

Рис. 1 Файл для установки Dallas Locker с версией 8.0 с расширением .msi

Выполните установку «Клиент Dallas Lock 8.0-K» на виртуальную машину запустив файл DallasLock8.0K.msi.

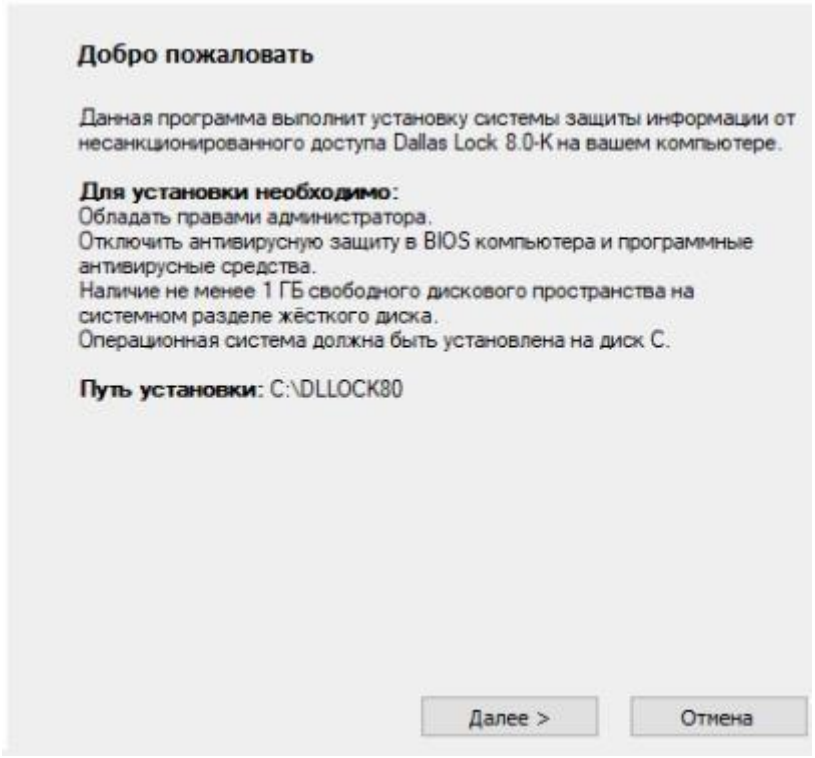

Рис. 2 Начала установки

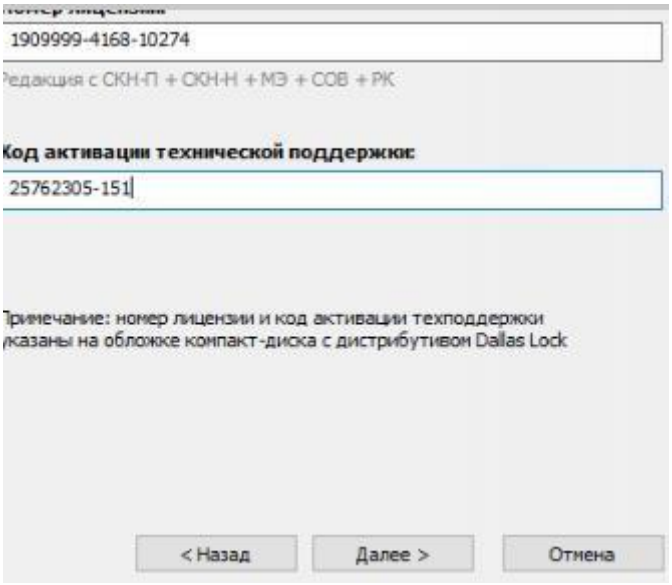

Рис. 3 параметры установки

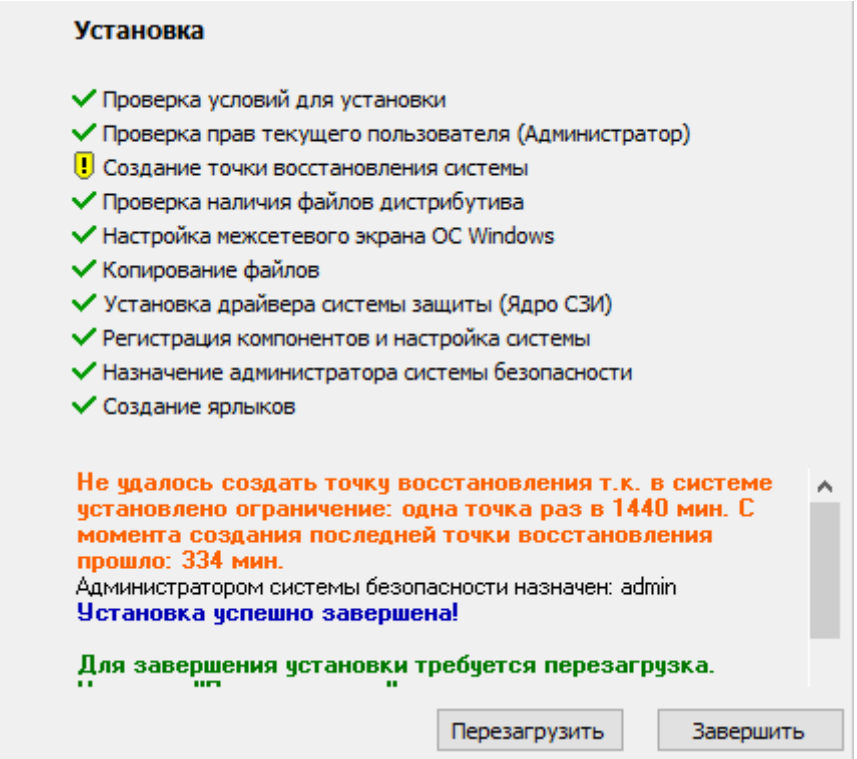

Рис. 4 Завершение установки

После создания новой учётной записи устанавливаем логин как для пользователя admin так и для пользователя User.

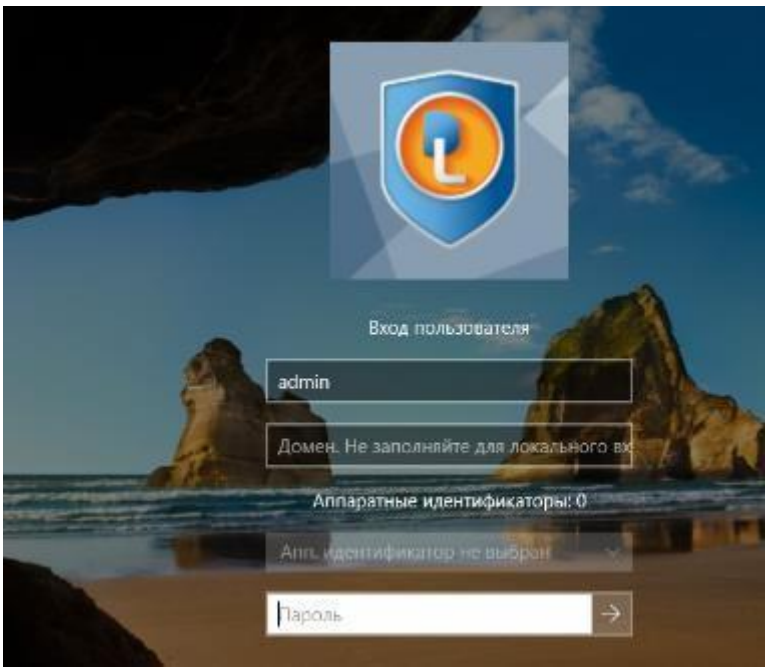

Рис. 5 Результат вида с пользователя admin

После входа через admin мы видими то что демонстрируется на (рис. 5). После входа через admin поаторим тоже самое но с пониженными привимлегиями и с обычного User.

Задание 1. Опишите четыре шага, которые необходимо пройти субъекту для получения доступа к объекту.

1. Идентификация

На этом этапе субъект (пользователь, система или устройство) предоставляет свою личность системе. Это может быть сделано с помощью уникального идентификатора, например, имени пользователя или номера учетной записи. Идентификация — это первый шаг, который позволяет системе узнать, кто пытается получить доступ.

2. Аутентификация

После идентификации система проверяет, действительно ли субъект является тем, за кого себя выдает. Это делается с помощью различных методов аутентификации, таких как:

Ввод пароля или PIN-кода.

Использование биометрических данных (отпечатки пальцев, распознавание лица).

Многофакторная аутентификация (MFA), которая может включать в

себя комбинацию различных методов (например, пароль и SMS-код).

3. Авторизация

После успешной аутентификации система определяет, какие права и уровни доступа имеет субъект. Этот процесс включает проверку разрешений и ролей, чтобы удостовериться, что субъект имеет право выполнять определенные действия или получать доступ к определенным ресурсам. Например, администратор может иметь полный доступ, в то время как обычный пользователь может иметь ограниченные права.

4. Подотчетность

Этот шаг включает в себя отслеживание и регистрацию действий субъекта в системе. Подотчетность позволяет вести учет всех действий, связанных с доступом и использованием ресурсов, что важно для обеспечения безопасности и расследования инцидентов. Это может включать ведение журналов доступа, запись времени входа и выхода, а также действия, выполненные пользователем в системе.

Задание 2. Опишите правила выбора и использования пароля.

Правила выбора пароля

Длина пароля:

Пароль должен содержать не менее 12-16 символов. Длинные пароли сложнее подбирать.

Сложность пароля:

Используйте комбинацию букв верхнего и нижнего регистра, цифр и специальных символов (например, !, @, #, $). Это значительно увеличивает сложность пароля.

Избегайте очевидных слов и фраз:

Не используйте личные данные, такие как имя, дата рождения, имена домашних животных или общепринятые слова и фразы. Такие пароли легко угадать.

Использование уникальных паролей:

Для каждого аккаунта или сервиса используйте уникальный пароль.

Это предотвращает компрометацию нескольких аккаунтов в случае утечки.

Фразы вместо паролей:

Рассмотрите возможность использования фраз вместо традиционных паролей. Например, «МойКотЛюбитИгратьСМячом123!». Это легче запомнить и сложнее угадать.

Правила использования пароля

Регулярная смена паролей:

Меняйте пароли каждые 3-6 месяцев, особенно для важных аккаунтов, таких как банковские и корпоративные.

Не делитесь паролями:

Никогда не передавайте свои пароли другим людям. Если необходимо предоставить доступ, используйте функции, которые позволяют делиться доступом без раскрытия пароля.

Используйте менеджеры паролей:

Менеджеры паролей могут помочь генерировать и хранить сложные пароли, избавляя от необходимости запоминать их.

Включите многофакторную аутентификацию (MFA):

Если это возможно, активируйте MFA для своих аккаунтов. Это добавляет дополнительный уровень безопасности, требуя подтверждения входа через SMS, электронную почту или приложение.

Обратите внимание на безопасность устройства:

Убедитесь, что ваше устройство защищено от вирусов и вредоносных программ. Используйте антивирусное ПО и регулярно обновляйте операционную систему и приложения.

Не используйте один и тот же пароль для разных аккаунтов:

Если один из ваших аккаунтов будет скомпрометирован, это может привести к взлому других, если вы используете один и тот же пароль.

Задание 3. Поясните формулу:

Формула помогает оценить, как долго пароль сможет защитить информацию, прежде чем злоумышленник сможет его подобрать. Чем

больше длина пароля и чем меньше скорость его набора, тем выше среднее время безопасности.

Задание 4. Выполнить установкуDallas Lock.

На (рис. 5) демонстрируется результат установки программы соответственно она установлена.

Задание 5. Вход на защищенный компьютер.

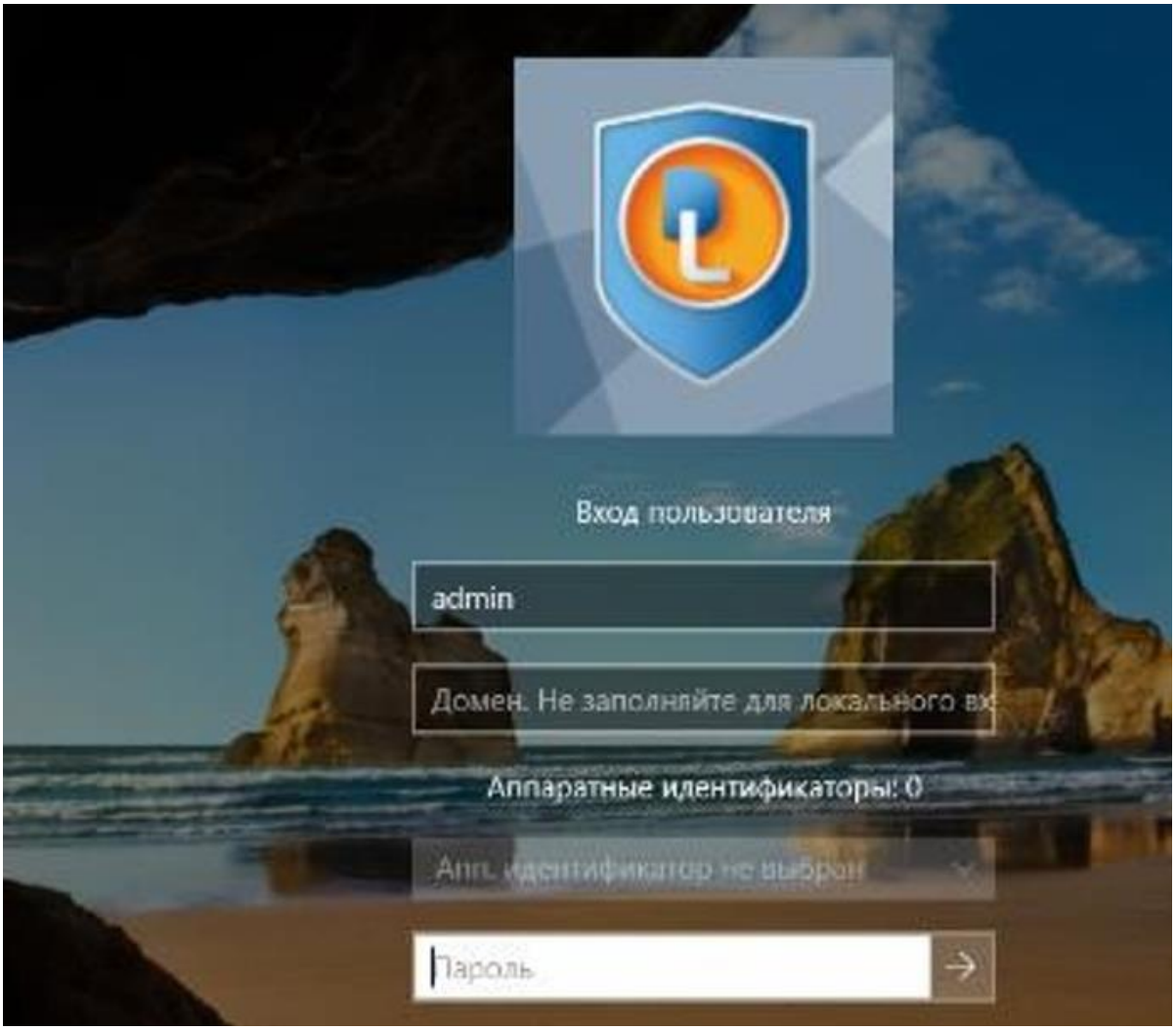

Рис. 6 Поле для домена не заполняем

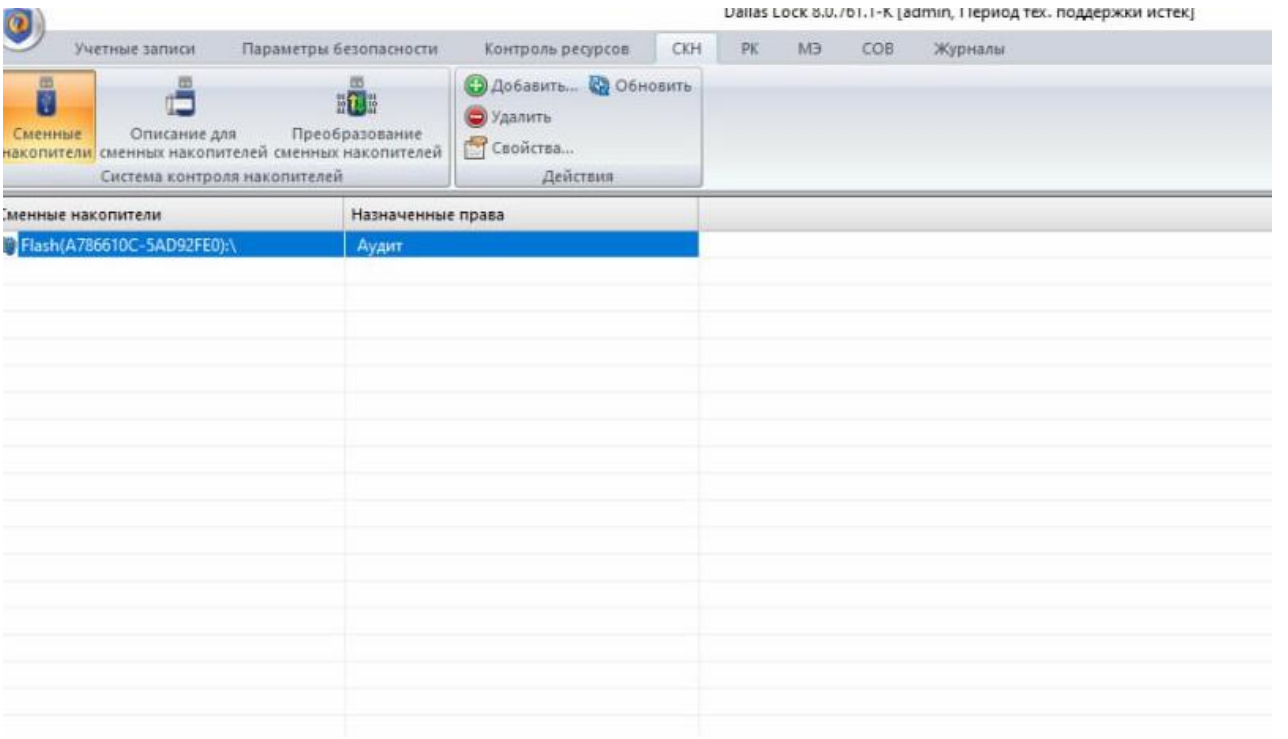

Рис. 7 Вставляем незарегистрированный носитель, проверяем доступ

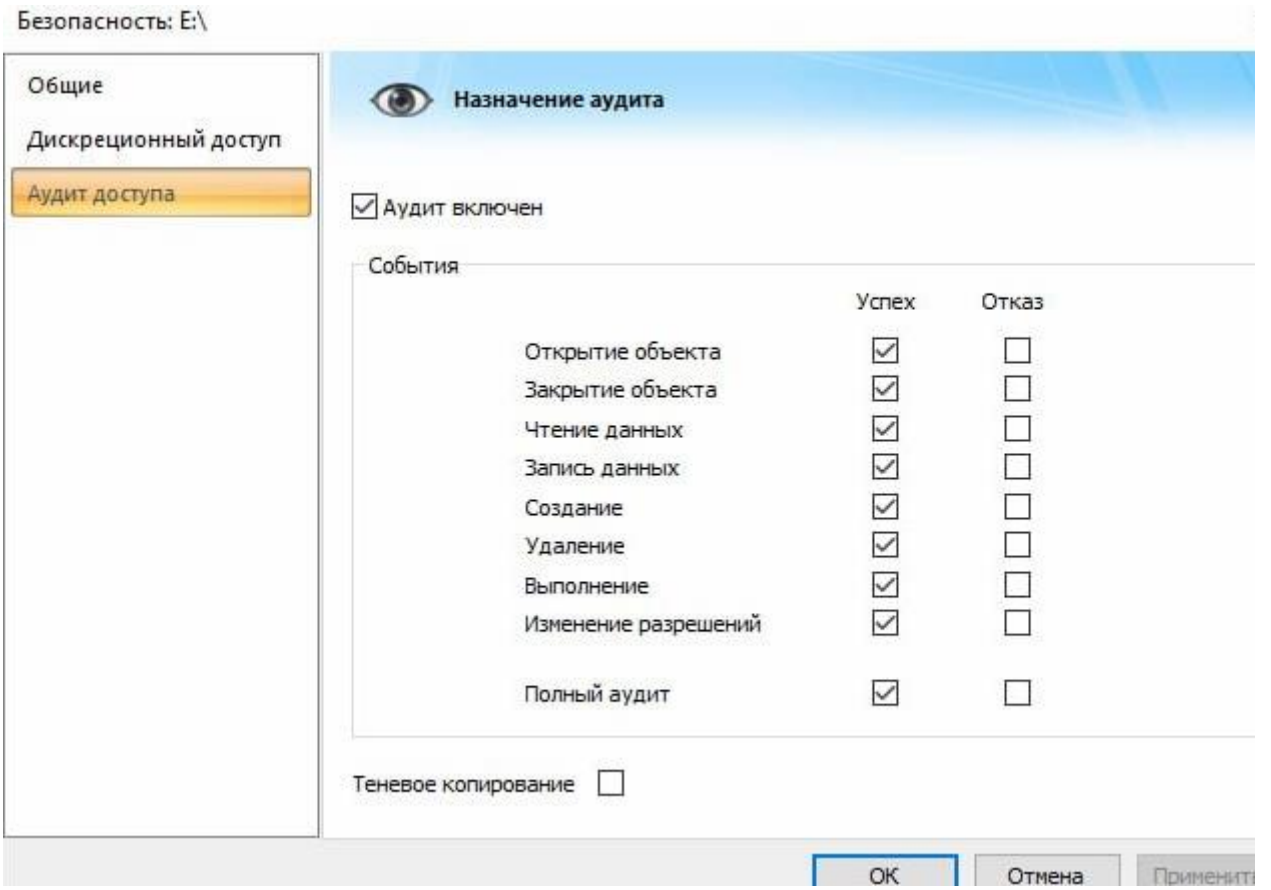

Рис. 8 настройка разграничения доступа

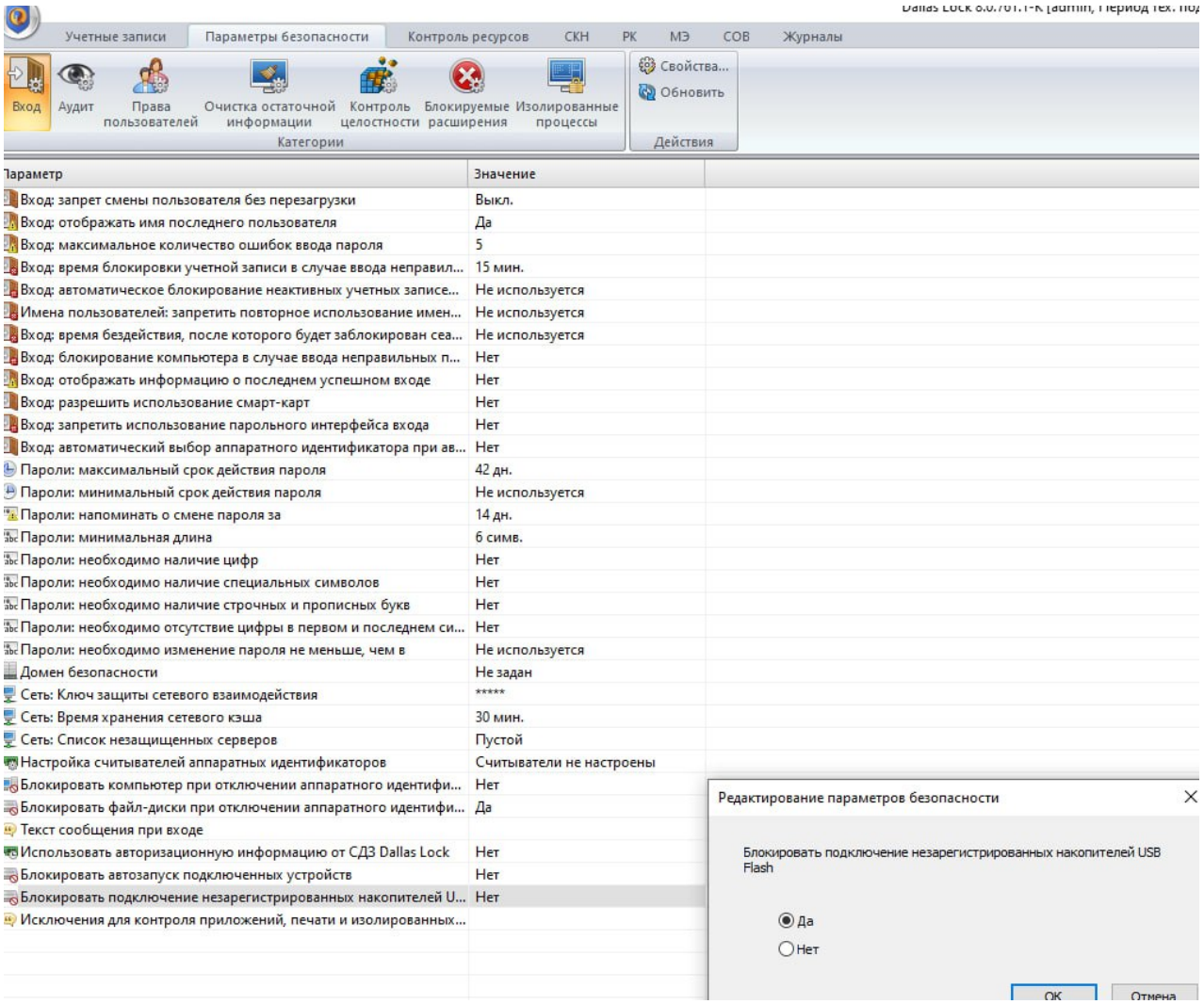

Рис. 9 Процесс редактирования параметров блокировки

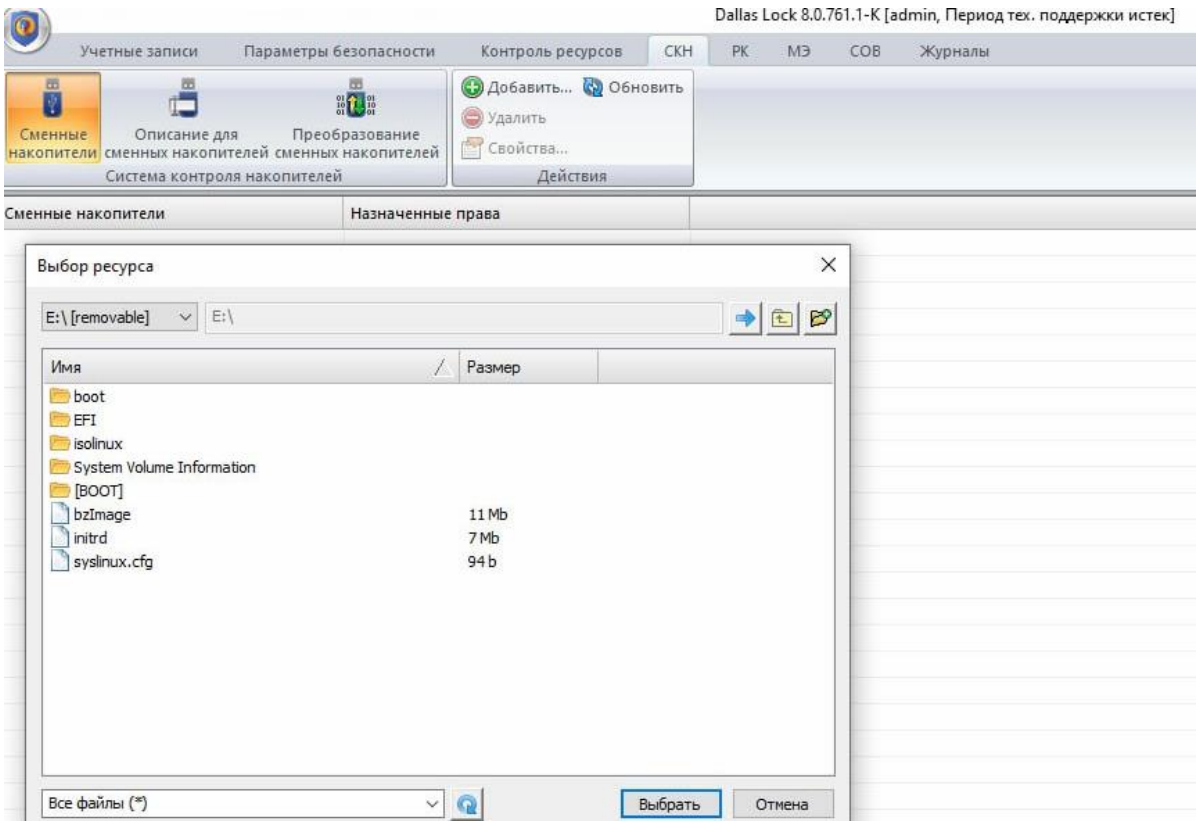

Рис. 10 Настроить аудит событий, связанных с накопителем.

Регистрация флэш-накопителя демонстрируется на (рис. 6).

Задача 6. Определите степень защиты информации организации, защищенной с применением пароля, а также исследуйте методы противодействия атакам на пароль.

Степень защиты информации с помощью пароля

Сложность пароля:

Сложные пароли (длинные, содержащие буквы верхнего и нижнего регистра, цифры и специальные символы) обеспечивают более высокий уровень защиты.

Рекомендуется использовать пароли длиной не менее 12-16 символов.

Управление паролями:

Использование менеджеров паролей для генерации и хранения паролей может значительно повысить уровень безопасности.

Регулярная смена паролей и использование уникальных паролей для разных сервисов также увеличивают защиту.

Многофакторная аутентификация (MFA):

Внедрение MFA (например, SMS-коды, приложения для аутентификации) значительно усиливает защиту, так как даже если пароль будет скомпрометирован, доступ к информации останется ограниченным.

Политики безопасности:

Четкие политики по созданию и использованию паролей, а также обучение сотрудников основам безопасности также играют важную роль в защите информации.

Методы противодействия атакам на пароль.

Атаки на пароли могут быть различных типов, включая атаки методом подбора (brute force), атаки с использованием словарей (dictionary attacks) и фишинг. Для защиты от этих атак можно использовать следующие методы:

Сложные пароли:

Как уже упоминалось, использование сложных и уникальных паролей для каждого аккаунта помогает предотвратить атаки.

Блокировка аккаунта:

Внедрение механизма блокировки аккаунта после нескольких неудачных попыток входа. Это затрудняет атаки методом подбора.

Мониторинг и уведомления:

Настройка систем мониторинга для отслеживания подозрительной активности и уведомления пользователей о возможных попытках взлома.

Использование хэширования:

Хранение паролей в виде хэшированных значений с использованием современных алгоритмов (например, bcrypt, Argon2) для защиты данных в случае утечки базы данных.

Обучение сотрудников:

Обучение сотрудников основам кибербезопасности, включая распознавание фишинга и других методов социальной инженерии.

Вывод в результате выполнения практической работы мы выполнили настройку и установку Dallas Lock 8.0-K1.