

## **Практическое занятие № 31**

### **Разработка политики безопасности корпоративной сети**

**Цель занятия:** получить навыки использования системы защиты информации в корпоративной сети.

#### **Практические задания**

Создайте политику безопасности операционной системы для трех пользователей с заданными правами использования файлов и папок при данных условиях:

1. Администратор компьютера имеет доступ ко всем папкам пользователей на чтение, но не имеет право удалять или изменять файлы. Папка администратора C:\Admin.

2. Бухгалтер – пользователь, имеет право записи и чтения в своей папке C:\bukh, не имеет доступа к папкам администратора, имеет доступ на запись к папке пользователя Начальник.

3. Начальник – пользователь, имеет право записи и чтения в своей папке C:\chief, не имеет доступа к папкам администратора, имеет доступ на чтение к папке пользователя

Бухгалтер. Все нарушения системы защиты записываются в журнал безопасности системы.

Установите следующие настройки: количество циклов затирания (3), ограничения по паролю пользователей (минимальная длина – 6 символов, требования к сложности, требования к неповторяемости, время действия – 45 дней), максимальное число попыток входа – 5, аудит событий НСД (контролируется в журнале «Безопасность», находящемся «Панель управления /Администрирование/ Просмотр событий»), невозможность запуска программ из папки пользователя.

В каждой папке должны быть два файла, содержащие текстовую информацию, и один файл программы (с расширением .exe).

#### **1. Создание папок и файлов для каждого пользователя**

Перед настройкой безопасности нужно подготовить структуры каталогов и файлы для каждого пользователя. Для этого:

- Администратор: Создайте папку C:\Admin для администратора.
- Бухгалтер: Создайте папку C:\bukh для бухгалтера.
- Начальник: Создайте папку C:\chief для начальника.

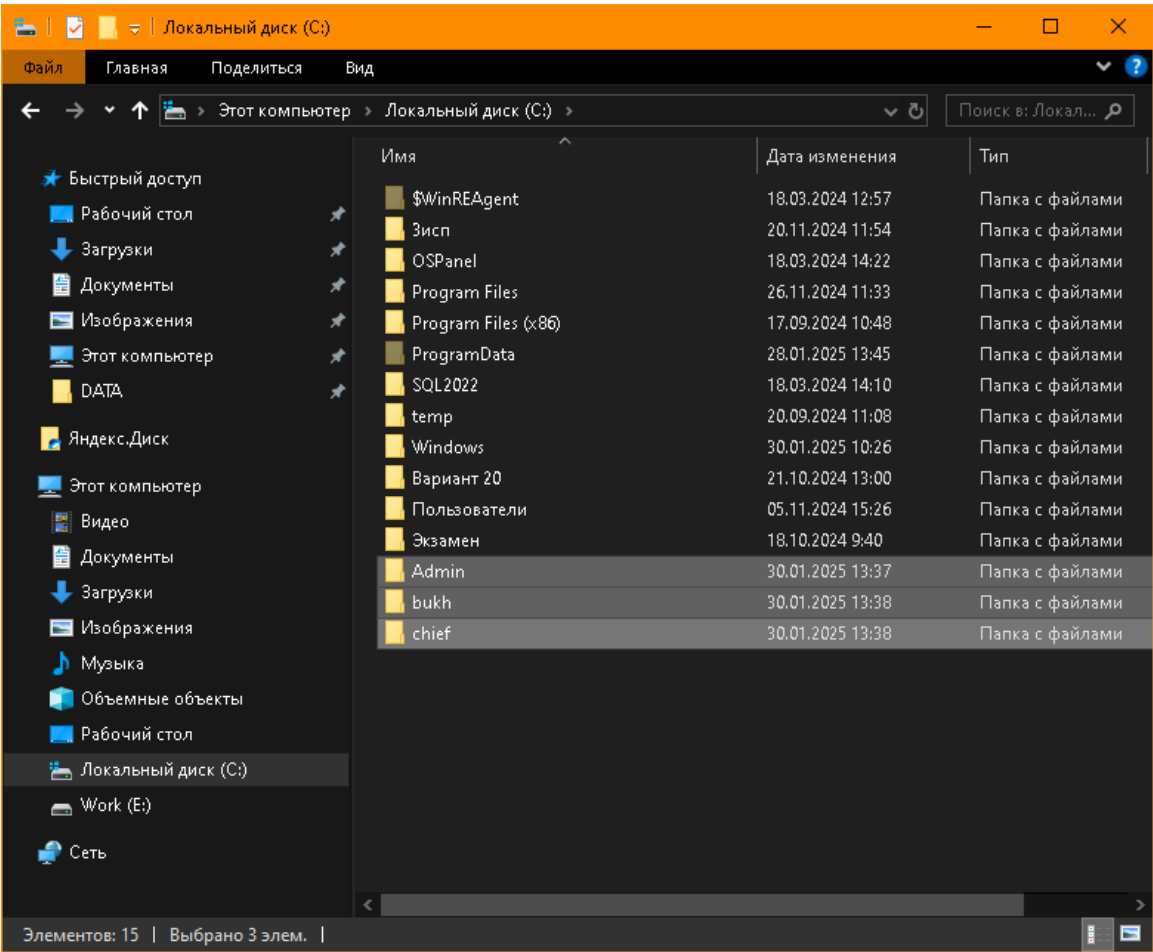


Рисунок 1 – Созданные папки

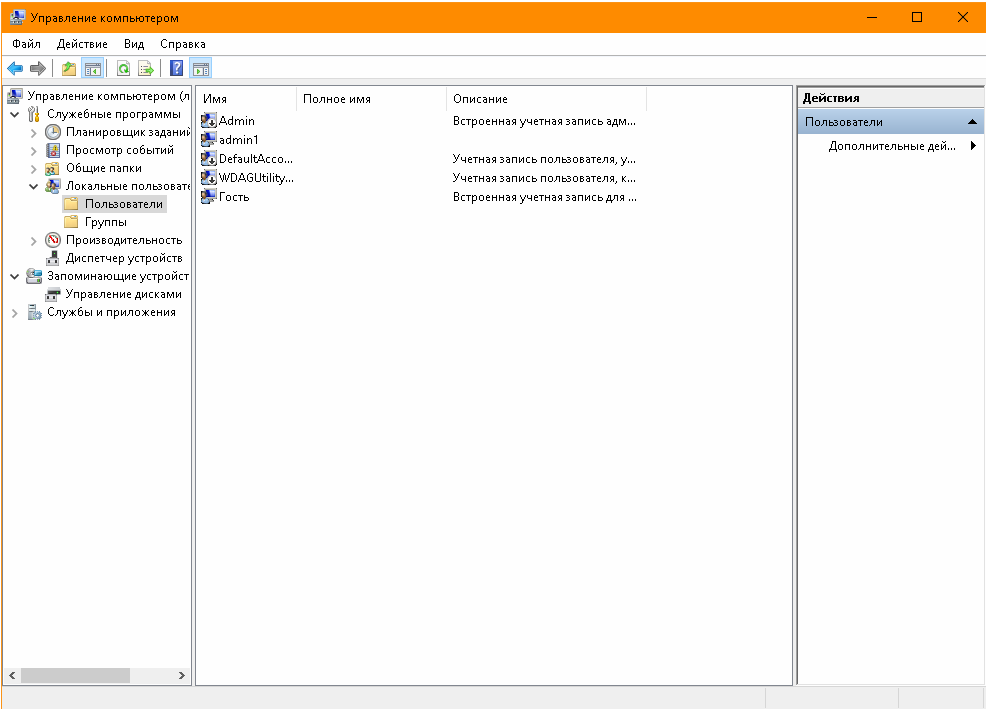


Рисунок 2 – Управление компьютером

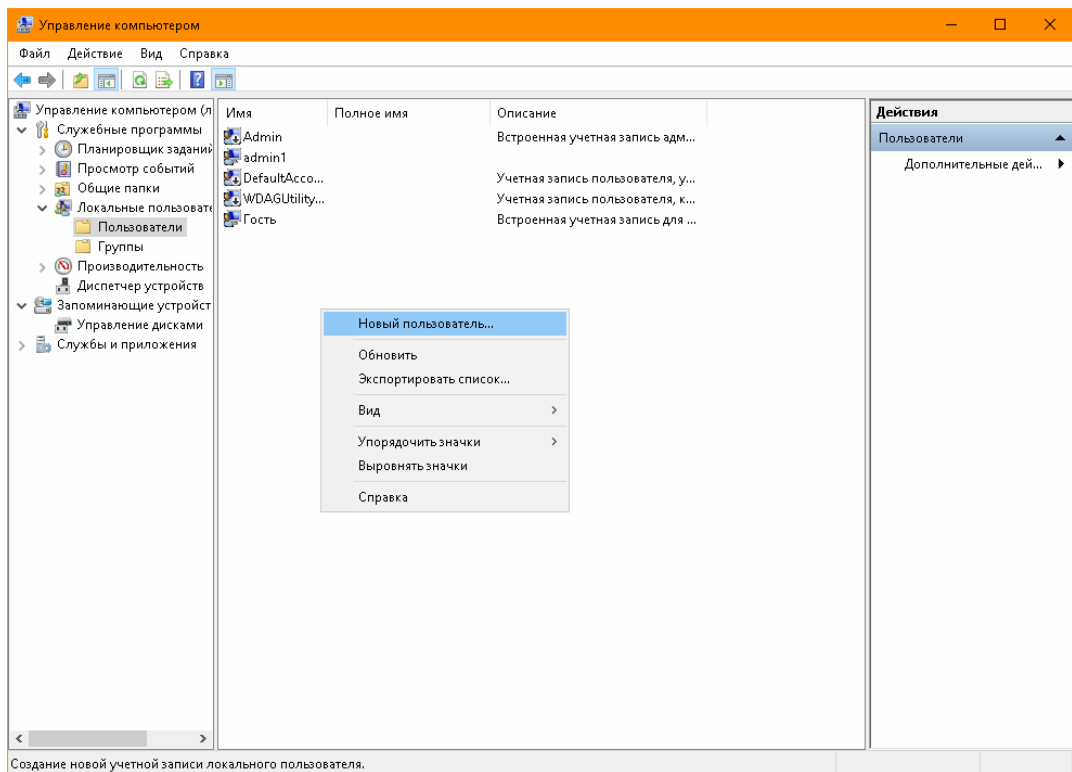


Рисунок 3 – Контекстное меню

**Новый пользователь** ? X

Пользователь:

Полное имя:

Описание:

---

Пароль:

Подтверждение:

☒ Требовать смены пароля при следующем входе в систему

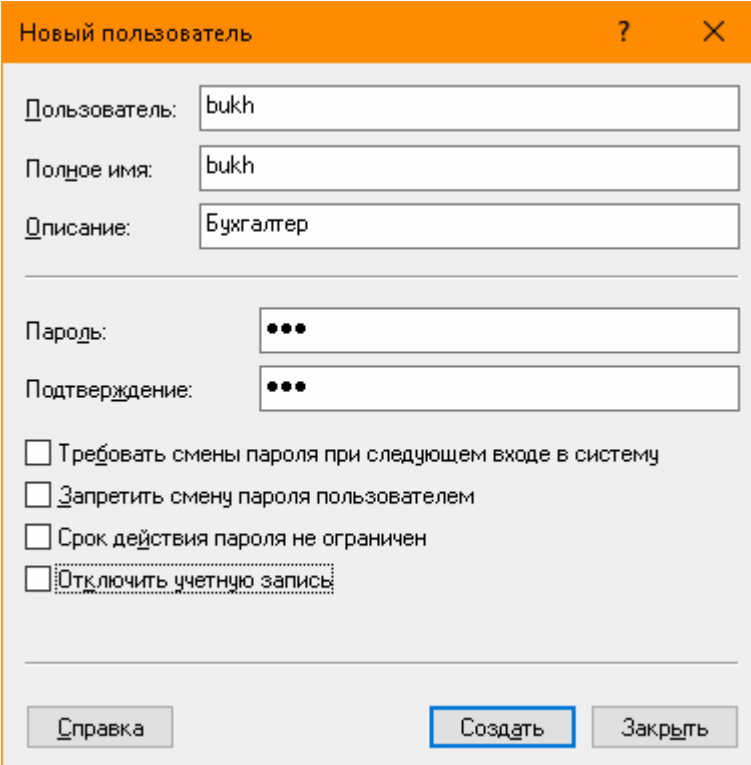
☐ Запретить смену пароля пользователем

☐ Срок действия пароля не ограничен

☐ Отключить учетную запись

---

Рисунок 4 - Окно создания нового пользователя



Новый пользователь

Пользователь: bukh

Полное имя: bukh

Описание: Бухгалтер

Пароль: ●●●

Подтверждение: ●●●

☐ Требуется смены пароля при следующем входе в систему

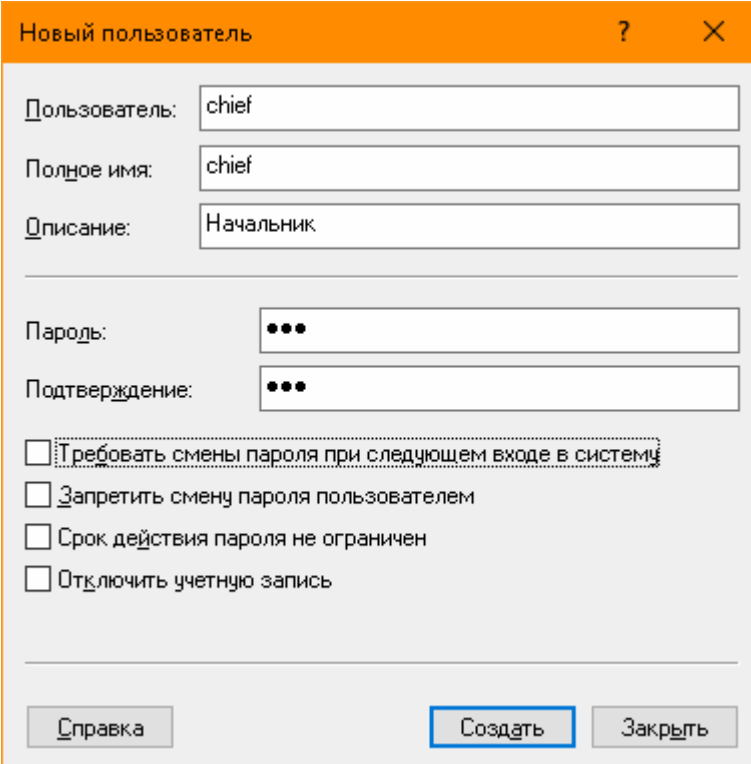
☐ Запретить смену пароля пользователем

☐ Срок действия пароля не ограничен

☐ Отключить учетную запись

[Справка](#) [Создать](#) [Закреть](#)

Рисунок 5 – Создание пользователя Бухгалтер



Новый пользователь

Пользователь: chief

Полное имя: chief

Описание: Начальник

Пароль: ●●●

Подтверждение: ●●●

☐ Требуется смены пароля при следующем входе в систему

☐ Запретить смену пароля пользователем

☐ Срок действия пароля не ограничен

☐ Отключить учетную запись

[Справка](#) [Создать](#) [Закреть](#)

Рисунок 6 – Создание пользователя Начальник

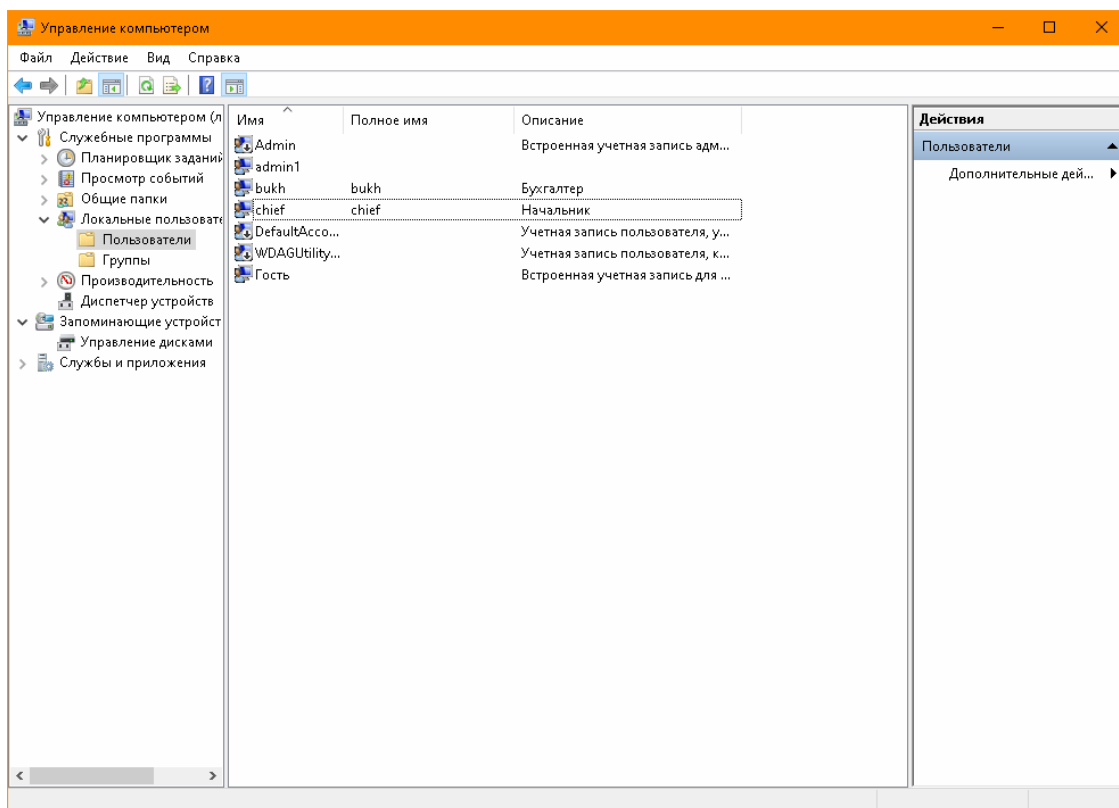


Рисунок 7 – Все созданные пользователи

## 2. Настройка прав доступа к папкам

Администратор:

1. Для папки C:\Admin установите права только для чтения для всех пользователей (включая себя как администратора).

2. Запрещаем изменение и удаление файлов.

Чтобы это настроить:

1. Кликните правой кнопкой мыши на папке C:\Admin → Свойства → Безопасность.

2. Выберите Изменить и настройте права:

- Убедитесь, что у Администратора есть права на Чтение и Список содержимого папки.

- Уберите галочки с Записи и Удаления.

- Убедитесь, что другие пользователи (Бухгалтер, Начальник) не имеют доступа к этой папке.

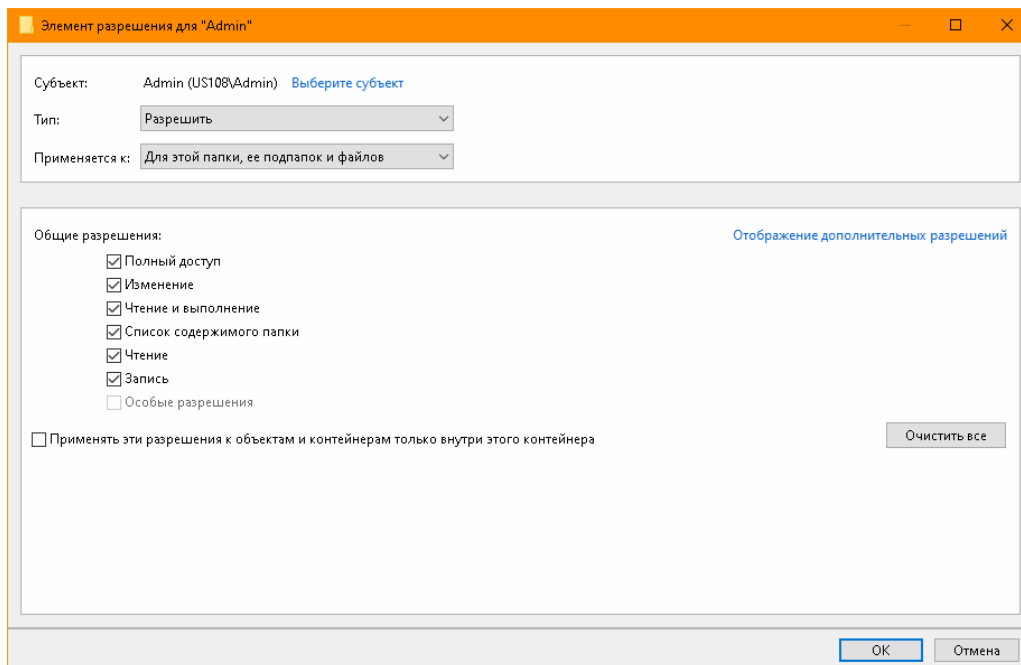


Рисунок 8 – Разрешения для Администратора

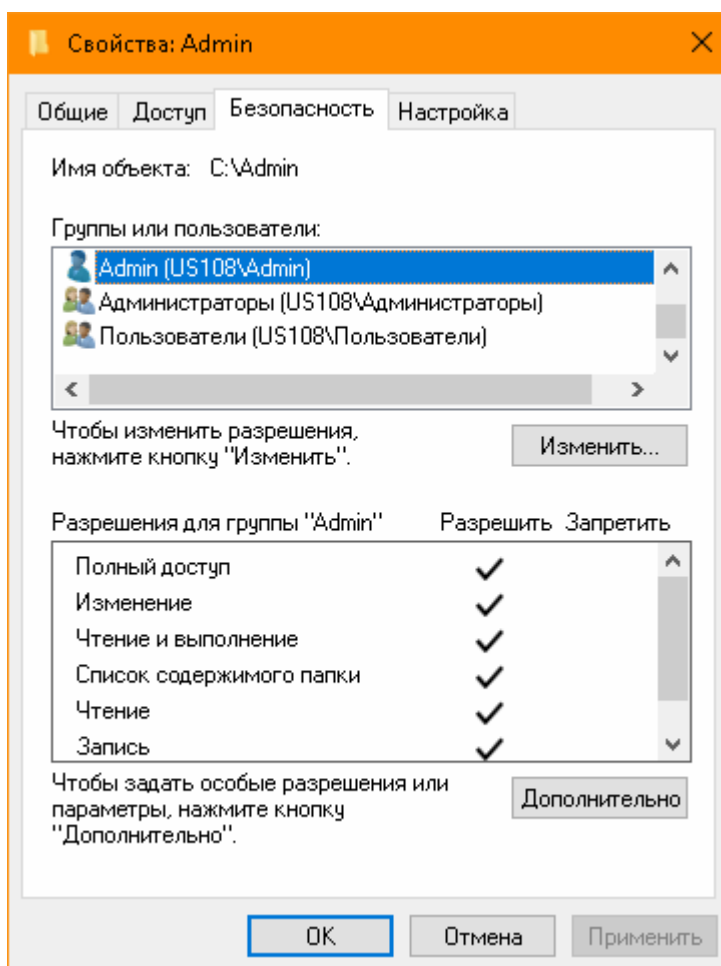


Рисунок 9 - Разрешения для Администратора

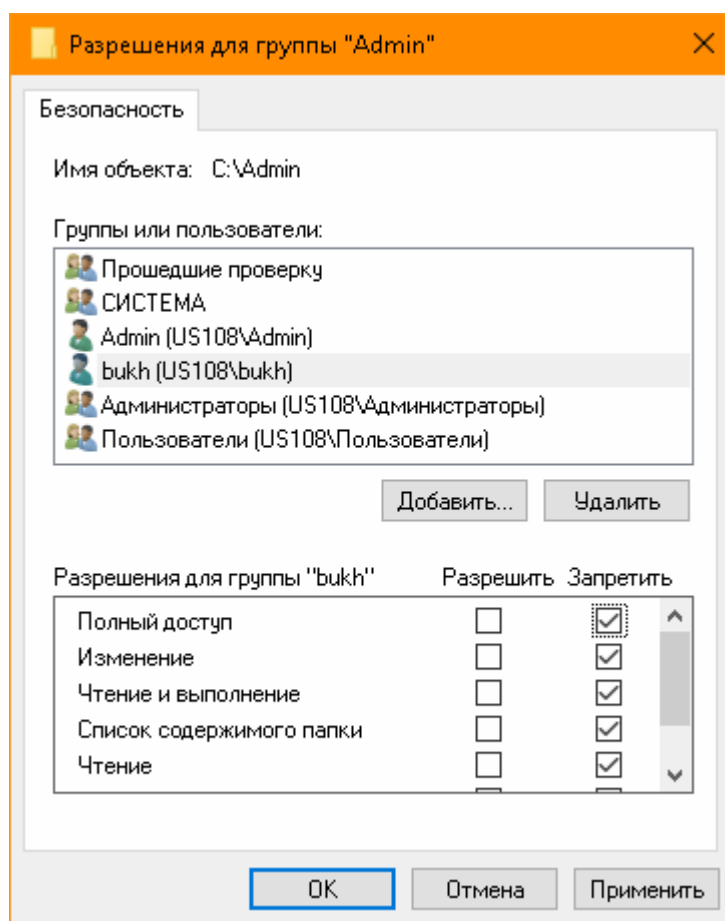


Рисунок 10 - Запрет для Бухгалтера

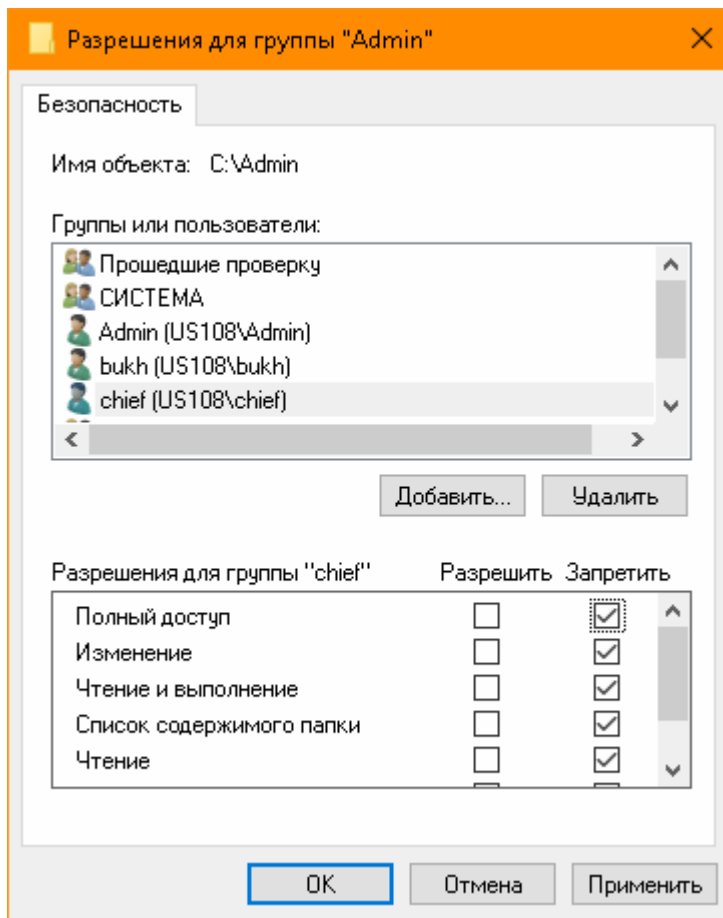


Рисунок 11 - Запрет для Начальника

Бухгалтер:

1. Для папки C:\bukh установите следующие права:
  - Полный доступ (чтение и запись) для бухгалтера.
  - Нет доступа к папке C:\Admin.
  - Доступ на запись в папке начальника (только для записи, без удаления).

Чтобы это настроить:

1. Кликните правой кнопкой на папке C:\bukh → Свойства → Безопасность.
2. Выберите Изменить:
  - Для Бухгалтера установите права Чтение и запись.
  - Для Администратора и Начальника установите доступ на Запрещено.
  - Для папки Начальника установите права Запись (позволяет добавлять файлы, но не изменять их).



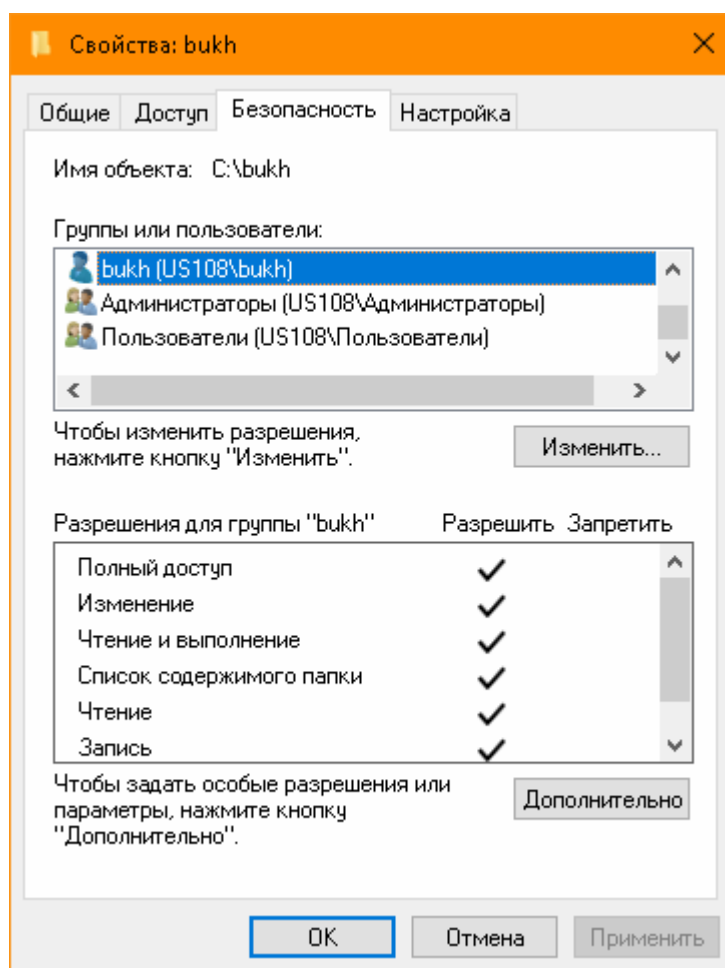


Рисунок 12 - Разрешения для Бухгалтера на папку Бухгалтера

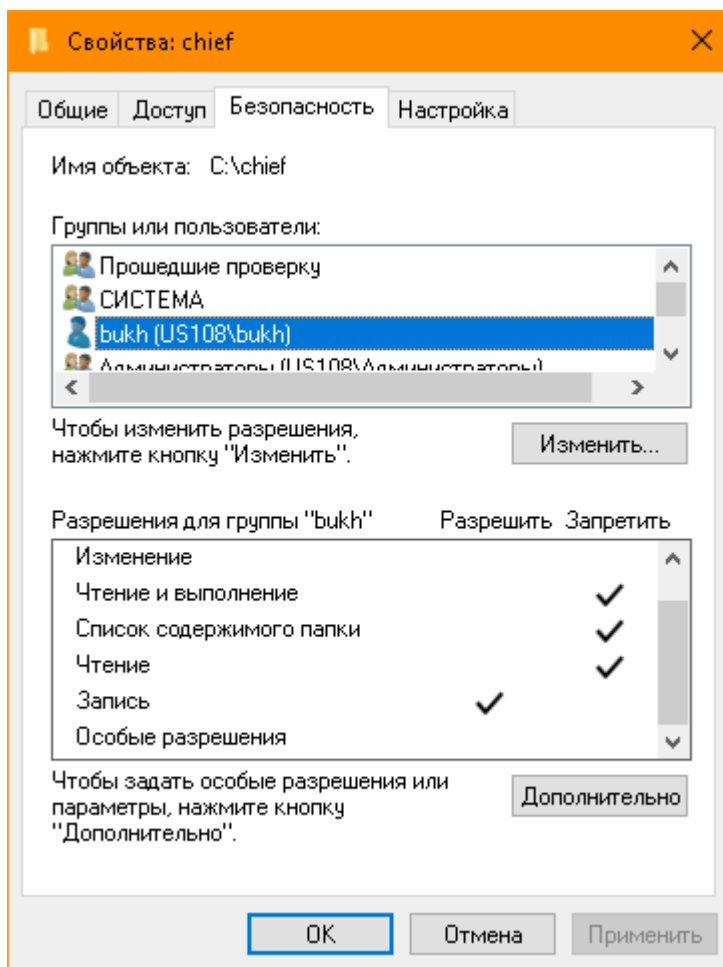


Рисунок 13 – Разрешения Бухгалтера для папки Начальника

Начальник:

- Для папки C:\chief установите следующие права:
  - Полный доступ (чтение и запись) для начальника.
  - Нет доступа к папке C:\Admin.
  - Только доступ на чтение для папки бухгалтера.

Настройка аналогична:

- Кликните правой кнопкой на папке C:\chief → Свойства → Безопасность.
  - Для Начальника установите Чтение и запись.
  - Для Бухгалтера установите Чтение.
  - Для Администратора установите Запрещено.
3. Настройка политики безопасности

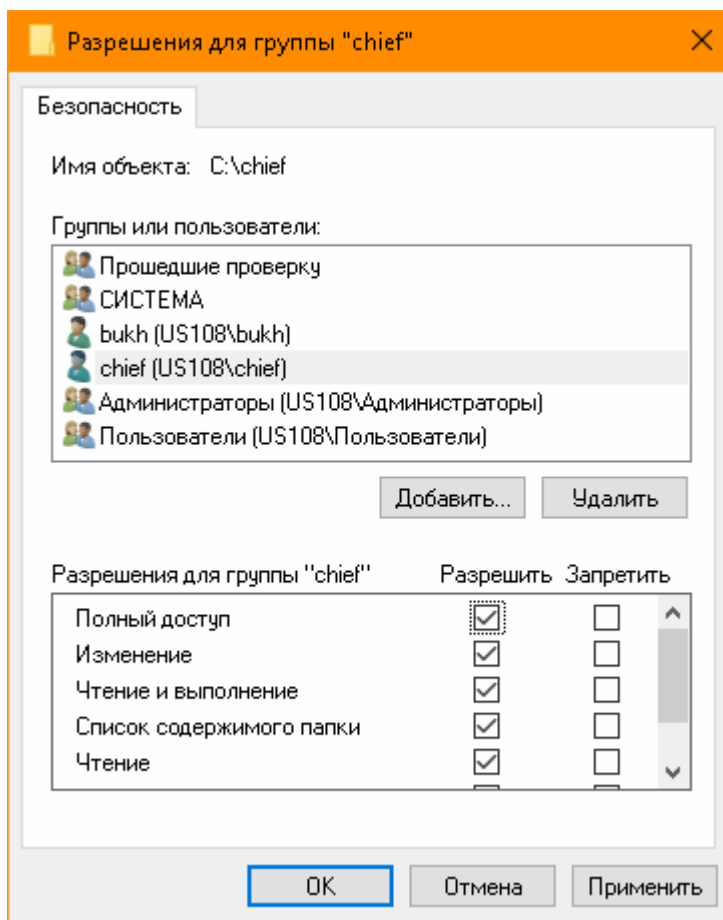


Рисунок 14 – Разрешения Начальника на папку Начальник

#### Политика пароля

1. Откройте Панель управления → Администрирование → Локальная политика безопасности.
2. Перейдите в Политика паролей:
  - Установите Минимальная длина пароля на 6 символов.
  - Включите Требования к сложности пароля (пароль должен включать как минимум три категории символов).
  - Установите Количество предыдущих паролей, которые необходимо запомнить на 3.
  - Установите Максимальный срок действия пароля на 45 дней.
3. Установите максимальное количество неудачных попыток входа:
  - Перейдите в Политика учетных записей → Политика блокировки учетных записей.
  - Установите Максимальное количество попыток входа на 5.
  - Установите Пороговое значение блокировки на 5 (то есть учетная запись будет блокироваться после 5 неудачных попыток входа).

#### Аудит событий безопасности

1. Откройте Панель управления → Администрирование → Просмотр событий.
2. В разделе Журналы Windows → Безопасность настройте аудит:

- Включите Аудит входа в систему для всех пользователей.
  - Включите Аудит изменений учетных записей для отслеживания любых изменений в учетных записях.
  - Включите Аудит использования привилегий, чтобы фиксировать любые попытки пользователей использовать привилегированные действия.
3. Все события будут записываться в журнал Безопасности.
  4. Ограничение на запуск программ из папки пользователя
    1. Откройте Панель управления → Администрирование → Локальная политика безопасности.
    2. Перейдите в Политика ограниченного использования программ.
    3. Создайте новую политику для каждого пользователя, ограничивающую запуск программ в их папке.
      - Выберите Действие → Создать новое правило.
      - Укажите путь для каждого пользователя, например, C:\bukh\\*.exe или C:\chief\\*.exe, и запретите выполнение .exe файлов из этих папок.
  5. Проверка и настройка журнала безопасности
    1. Перейдите в Просмотр событий → Журналы Windows → Безопасность.
    2. Убедитесь, что все действия, связанные с доступом, изменениями учетных записей, попытками входа, и нарушениями безопасности записываются в журнал.

### **Контрольные вопросы:**

#### **1. В чем заключается сущность принципов функционирования механизма контроля доступа?**

Механизм контроля доступа (MAC) обеспечивает определение, кто и с какими правами может получить доступ к различным объектам системы. Он регулирует как пользователи взаимодействуют с файлами, папками и другими ресурсами, основываясь на их ролях и назначенных правами доступа. Принцип работы включает в себя как методы идентификации пользователя, так и проверку полномочий на выполнение определенных операций.

#### **2. Как реализовано управление пользователями?**

Управление пользователями в операционной системе осуществляется через учетные записи пользователей, которые можно создавать, изменять или удалять в разделе Учетные записи пользователей. Каждой учетной записи назначаются права доступа, парольная защита и дополнительные параметры безопасности.

#### **3. Как выполняется блокировка и разблокировка пользователя?**

Блокировка учетной записи происходит после достижения порогового значения неудачных попыток входа в систему. Блокировка может быть

временной (с автоматическим разблокированием после установленного времени) или постоянной (до вмешательства администратора). Для разблокировки учетной записи администратор должен вручную сбросить блокировку или дождаться истечения времени блокировки.

#### **4. В чем заключаются функции персонального идентификатора?**

Персональный идентификатор (или идентификатор учетной записи) используется для уникальной идентификации пользователя в системе. Он позволяет системе связать действия пользователя с его учетной записью, фиксируя все его действия в журнале и регулируя доступ на основе прав и ролей.

#### **5. В чем заключается сущность принципов функционирования системы аудита безопасности?**

Система аудита безопасности фиксирует события, связанные с доступом к системе, файлам и приложениям. Она отслеживает как успешные, так и неудачные попытки входа, изменения учетных записей и политики безопасности, а также другие важные события, которые могут сигнализировать о нарушениях или угрозах безопасности.

#### **6. Какие существуют правила настройки и условия работы системы контроля доступа к файлам и папкам?**

Для работы системы контроля доступа необходимо наличие файловой системы NTFS и операционной системы с поддержкой профессиональных функций безопасности. Настройка прав доступа к файлам и папкам выполняется через вкладку **Безопасность** в свойствах объекта, где можно добавлять пользователей, устанавливать разрешения на чтение, запись, изменение и удаление файлов, а также на установку аудита доступа.