Цель работы – изучение принципов безопасности операционных систем и получение навыков построения политики безопасности в Windows.

Задания 1. Охарактеризовать настройки по умолчанию программного средства «Брандмауэр подключения к Интернету» в среде ОС Windows 10

Брандмауэр - это способ защиты устройства, который представляет собой барьер между самим устройством и глобальной сетью.

Основной функцией брандмауэра является защита от сетевых угроз. По принципу работы он похож на магический щит. Брандмауэр не просто отражает входящий трафик, он анализирует его и отделяет безопасный от подозрительного.

Настройки по умолчанию «Брандмауэр подключения к Интернету» представлены ниже на рисунке 1.

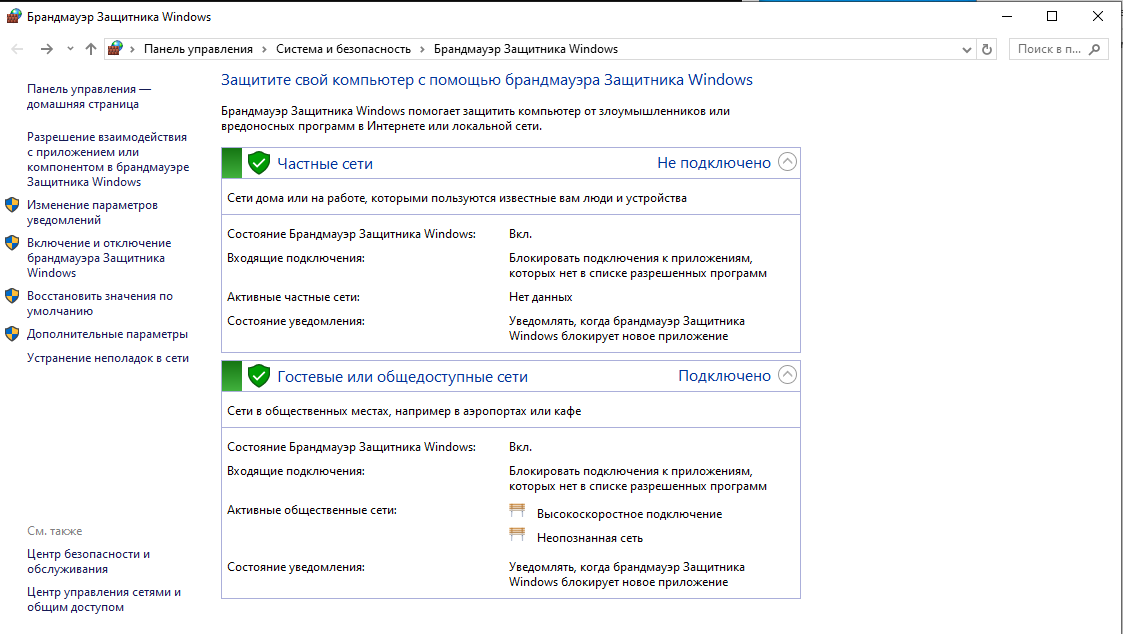


Рисунок 1 - Настройки по умолчанию «Брандмауэр подключения к Интернету»

Задание 2. Настроить параметры «Политики учетных записей» в ОС Windows 10

Политика учётных записей — это справочник, в котором можно задать сложность паролей и правила блокировки учётных записей при неудачных попытках входа в систему.

По умолчанию в справочнике автоматически уже созданы:

- политика для служебных пользователей – не рекомендуется менять;

- политика по умолчанию, которая выполняется для всех пользователей.

При необходимости администратор может изменить настройки политик по умолчанию или создать индивидуальные политики для конкретных групп пользователей.

Справочник доступен пользователям, входящим роли: «Администраторы» – полный доступ, «Аудиторы» – просмотр.

Политики учетных записей группа состоящая из 2 элементов политика паролей и политика блокировки учетной записи представлено на рисунке 2.

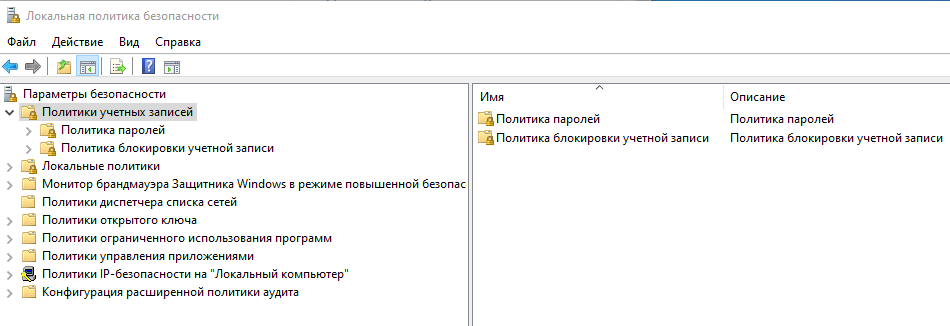


Рисунок 2 - Политики учетных записей

Свойства политики паролей представленной на рисунке 3.

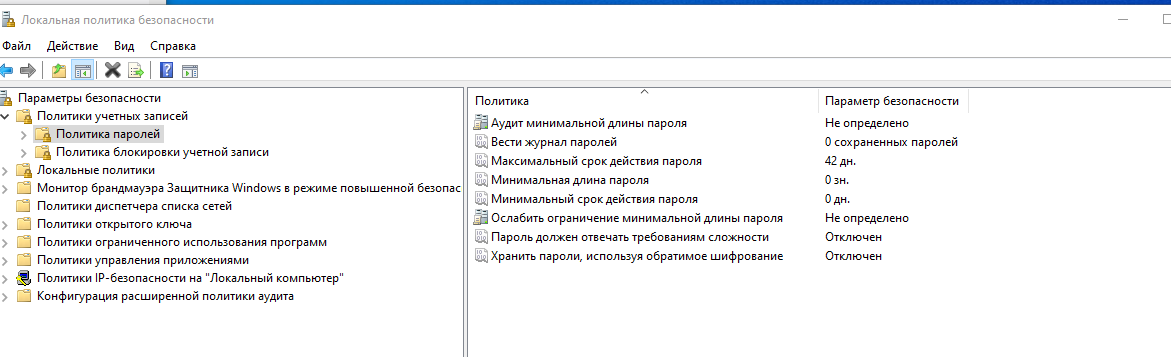


Рисунок 3 - Политика паролей

Свойства политики паролей определяют минимальной и максимальной длины пароля, минимальной и максимальной время действия пароля, флаги включения сложности пароля и шифрование паролей.

Свойства политики блокировки учетной записи, представленной на рисунке 4.

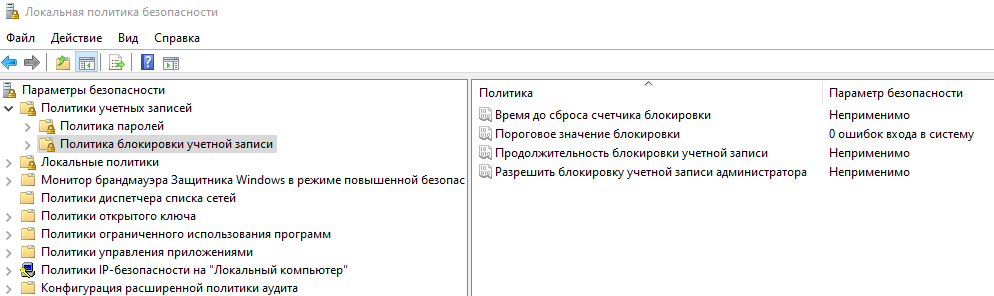


Рисунок 4 - Свойства политики блокировки учетной записи

Свойства политики блокировки учетной записи определяют количество попыток входа до блокировки, время ожидание после неудачной попытки входа, время блокировки пользователя при исчерпании всех попыток входа.

Задание 3 Настроить второй уровень доступа к объектам файловой системы NTFS в среде ОС Windows 10

Разрешения NTFS - это набор разрешений, используемых для защиты ваших файлов и папок, хранящихся на разделе с файловой системой NTFS. Эти разрешения могут определять, кто может получить доступ к определенным файлам / папкам, таким как профили пользователей. Они могут быть назначены группам или отдельным пользователям. Существуют различные типы разрешений NTFS для файлов и папок, для которых вы можете настроить.

разрешения NTFS доступны только для разделов NTFS, если вы используете файловую систему FAT32, вы не можете настроить разрешения NTFS для папки / файла в этом разделе. В этом случае вам необходимо сначала преобразовать FAT32 в NTFS.

Выбрать каталог или файл, на который требуется настроить доступ NTFS открыть свойства вкладка безопасность кнопка изменить представленная на рисунке 5.

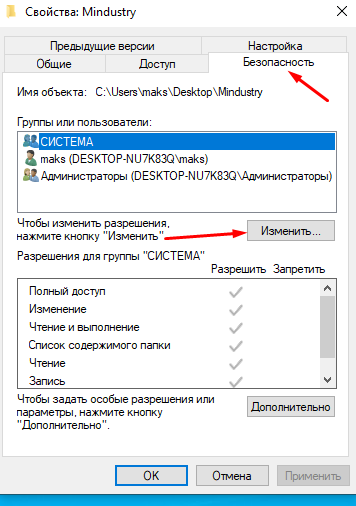


Рисунок 5 – окно с свойствами каталога или файла

На рисунке 6 представлено окно разрешения для группы.

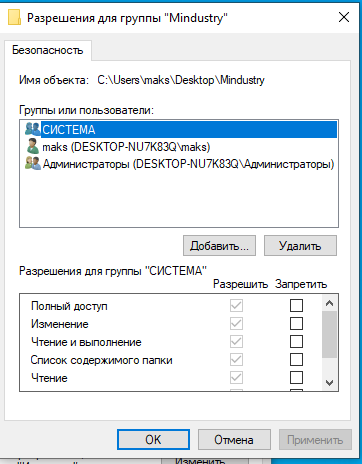


Рисунок 6 – окно разрешения для группы

В этом окне можно для определенной группы или пользователя задать доступ к папке разрешить или запретить изменение чтение запись и тд.

Вывод

Следующий задачи были выполнены:

* изучены настройки по умолчанию «Брандмауэр подключения к Интернету»;
* изучена политики учетных записей;
* изучена политика паролей;
* изучена политика блокировки учетной записи;
* изучена настройки доступа к объектам файловой системы NTFS.

Цель изучить принципы безопасности операционных систем и получение навыков построения политики безопасности в Windows была достигнута.