**ОТЧЁТ ПО ЛАБОРАТОРНОЙ РАБОТЕ №5**

**Тема: «Применение политики безопасности в ОС Windows»**

**Цель работы:** Ознакомиться с политиками безопасности в ОС Windows и процедурами создания политик безопасности.

***Задание №1:***

1. Запустить консоль «Локальная политика безопасности».
2. Перейти к пункту «Пороговое значение блокировки» в «Политике блокировки учётной записи», установить параметр равный 3 попыткам.
3. Перейти к пункту «Минимальная длина пароля» в «Политике паролей», установить значение 10.
4. Перейти к пункту «Пароль должен отвечать требованиям сложности», поставить галочку.
5. Проверить действие установленных настроек.

***Ход выполнения***

В соответствии с рекомендациями была запущена утилита «Локальная политика безопасности» (рис. 1). В политике учетных записей было установленно пошаговое значение блокировки в значение 3 (рис. 2). Минимальная длинна пароля установлена в значение 10 (рис. 3). А также к паролю включены требования сложности (рис. 4). При попытке создания пользователя система не разрешает добавлять простой пароль (рис. 5). При вводе пароля неправильно несколько раз учетная запись блокируется (рис. 6).

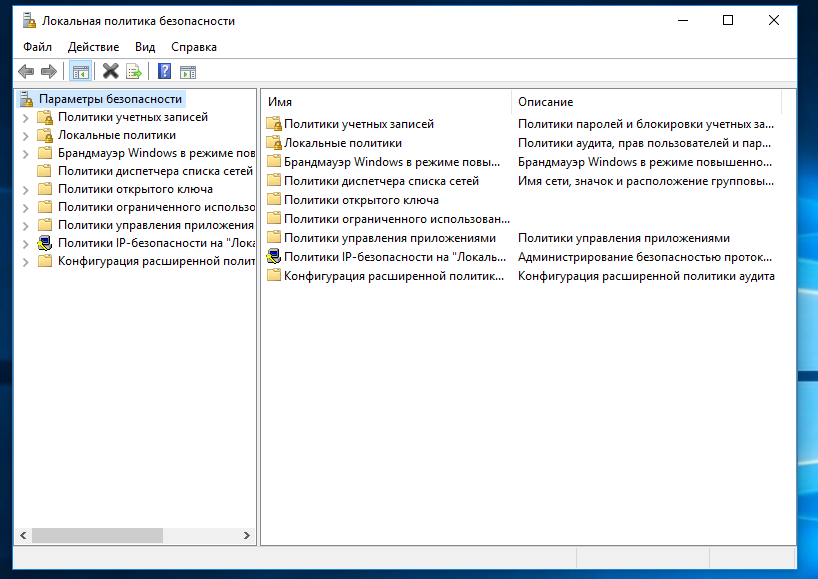


Рисунок 1 - Локальная политика безопасности

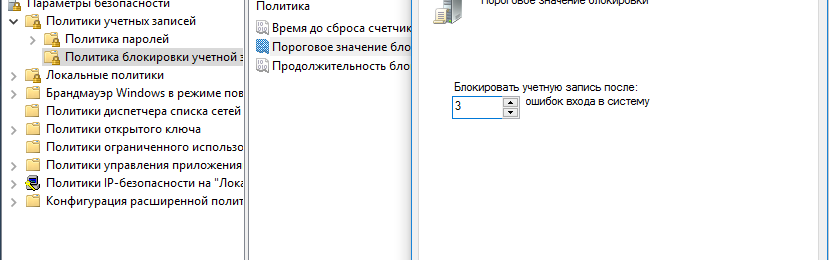


Рисунок 2 - Пошаговое значение блокировки

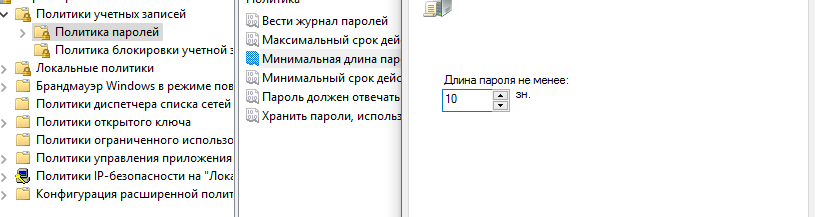


Рисунок 3 - Минимальная длинна пароля

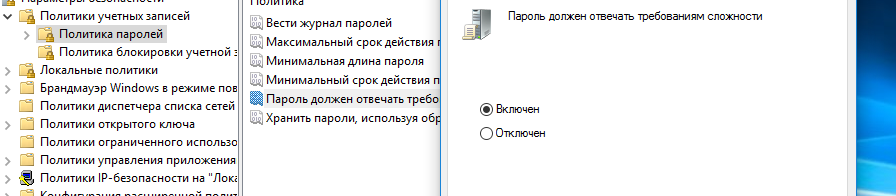


Рисунок 4 - Требования к сложности пароля

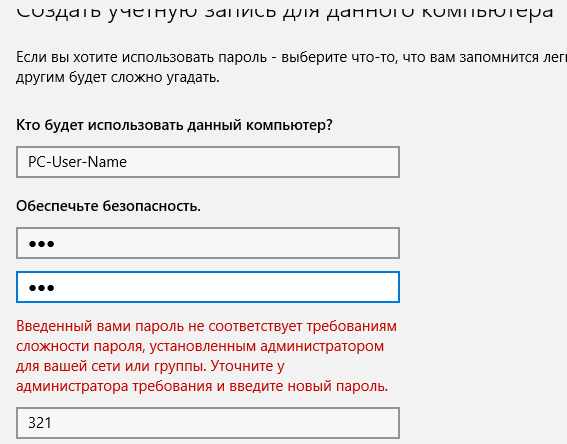


Рисунок 5 - Добавление нового пользователя

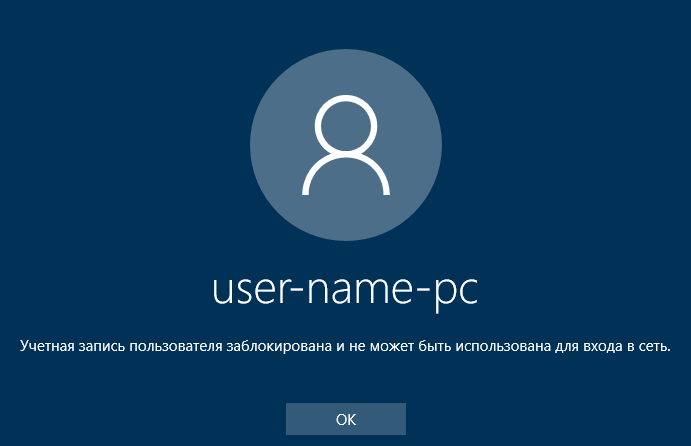


Рисунок 6 - Блокировка учетной записи

***Задание №2:***

1. Создание новой политики;
2. Редактирование свойств политики безопасности IP;
3. Создание нового фильтра;
4. Создание нового действия;
5. Установка параметров туннеля и типа подключения;
6. Установка метода проверки подлинности;

***Ход выполнения***

Была создана новая политика безопасности IP (рис. 7). Было добавлено новое правило (рис. 8). Был добавлен новый ip-фильтр (рис. 9). Также добавлено новое действие фильтра (рис. 10). Тип подключения выбран как «Локальная сеть (LAN)» (рис. 11). Также добавлен новый способ проверки подлинности (рис. 12).

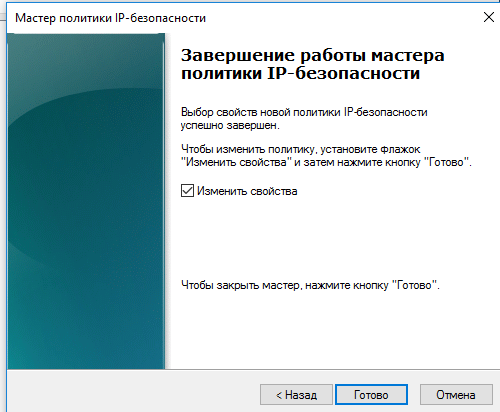


Рисунок 7 - Создание политики безопасности

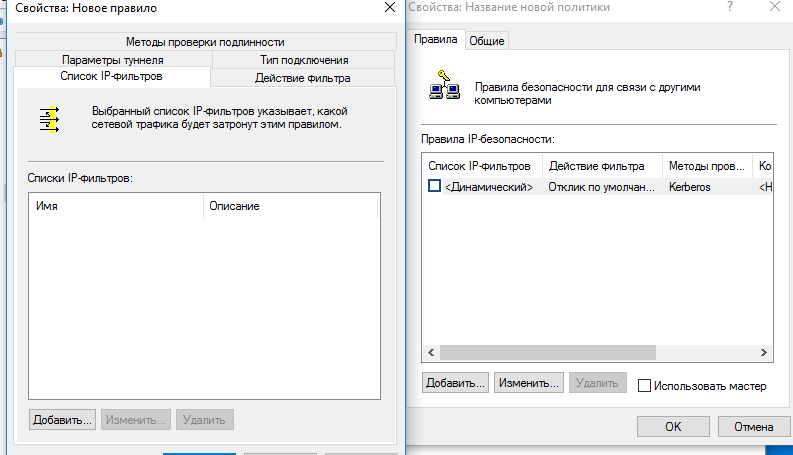


Рисунок 8 - Создание нового правила

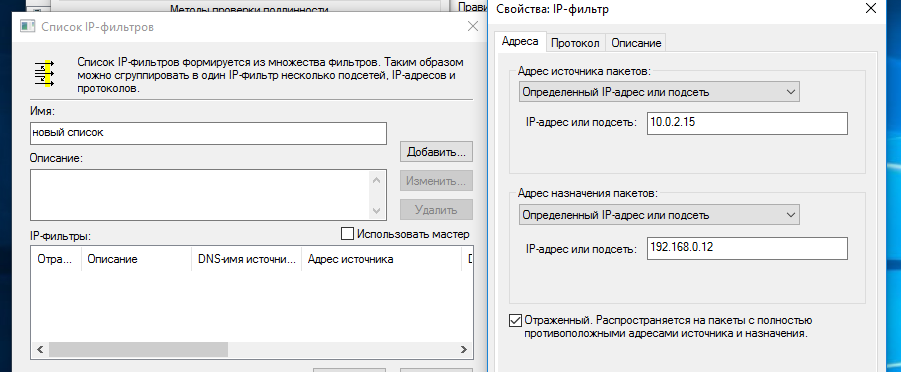


Рисунок 9 - Новый ip-фильтр

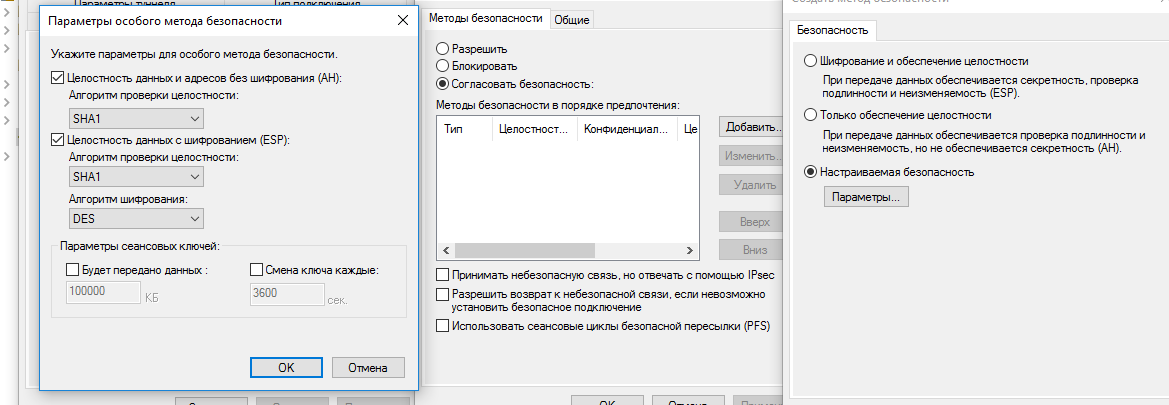


Рисунок 10 - Новое действие фильтра

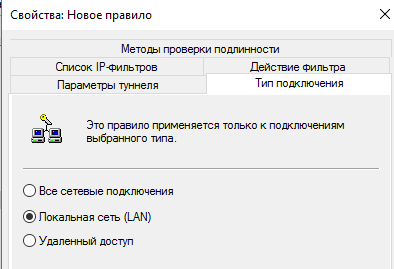


Рисунок 11 - Тип подключения

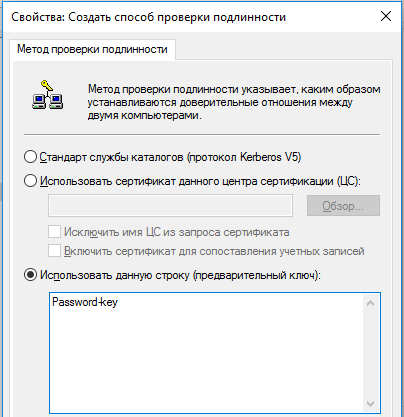


Рисунок 12 - Создание способа проверки подлинности