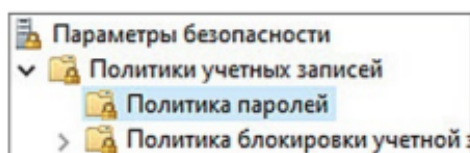


Практическая работа № 9. Политика безопасности

Необходимо запустить настройку «Локальная политика безопасности». Ввести в поиске (рядом с меню «Пуск») фразу «Локальная политика безопасности» и нажать на иконку. Запустить можно с помощью команды «Выполнить», введя команду «secpol.msc» и нажав «Ок».

Перед изменением политики нужно записать предыдущие значения к себе в тетрадь.

В окне «Локальная политика безопасности» открыть папку «Политики учётных записей» и выбрать пункт «Политика паролей».



Внести изменения в следующие настройки:

- Максимальный срок действия пароля: 60 дней.
- Минимальная длина пароля: 4.
- Пароль должен отвечать требованиям к сложности: Включён.

Прочитать описание параметра во вкладке параметра «Объяснение». Рекомендуется всегда включать в организациях данный параметр, это позволит снизить количество несанкционированного доступа к файлам пользователя.

- В окне «Локальная политика безопасности» открыть папку «Политики учётных записей» и выбрать пункт «Политика блокировки учётных записей». Данные политики позволяют повысить безопасность пользователя.
- Время до сброса счётчиков блокировки: 2 (минуты). Этот параметр безопасности определяет количество минут, которые должны пройти после неудачной попытки входа в систему до того, как счётчик неудачных попыток входа будет сброшен до 0.
- Пороговое значение блокировки: 3. После трёх попыток учётная запись будет заблокирована на 2 минуты (настройка выше).
- Продолжительность блокировки учётной записи: 3 (минуты). Этот параметр безопасности определяет количество минут, в течение которых учётная запись остаётся заблокированной до её автоматической разблокировки.

Восстановить ранее установленные политики.

Примечание

При блокировке учётной записи пользователь с правами администратора может разблокировать учётную запись с помощью утилиты «Локальные пользователи и группы» (выбрать команду «Выполнить» и ввести `lusrmgr.msc`; два раза кликнуть на нужную учётную запись и снять флажок «Заблокировать учётную запись»).