МИНИСТЕРСТВО НАУКИ И ВЫСШЕГО ОБРАЗОВАНИЯ РФ

федеральное государственное автономное образовательное учреждение высшего образования

«Санкт–Петербургский государственный университет  
аэрокосмического приборостроения»

ФАКУЛЬТЕТ СРЕДНЕГО ПРОФЕССИОНАЛЬНОГО ОБРАЗОВАНИЯ

ОТЧЕТ   
ЗАЩИЩЕН С ОЦЕНКОЙ

РУКОВОДИТЕЛЬ \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| преподаватель |  |  |  | И. В. Козлов |
| должность, уч. степень, звание |  | подпись, дата |  | инициалы, фамилия |

|  |
| --- |
| ОТЧЕТ ПО ЛАБОРАТОРНЫМ РАБОТАМ  по дисциплине МДК 02.02. Программное обеспечение компьютерных сетей |
|  |
|  |
|  |
|  |

РАБОТУ ВЫПОЛНИЛИ

|  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- |
| СТУДЕНТЫ ГР. № | С342 |  |  |  | Б. И. Глаголевский,  Е. Ю. Барабаш |
|  |  |  | подпись, дата |  | инициалы, фамилия |

# ОГЛАВЛЕНИЕ

Элементы оглавления не найдены.

# Защита учетной записи.

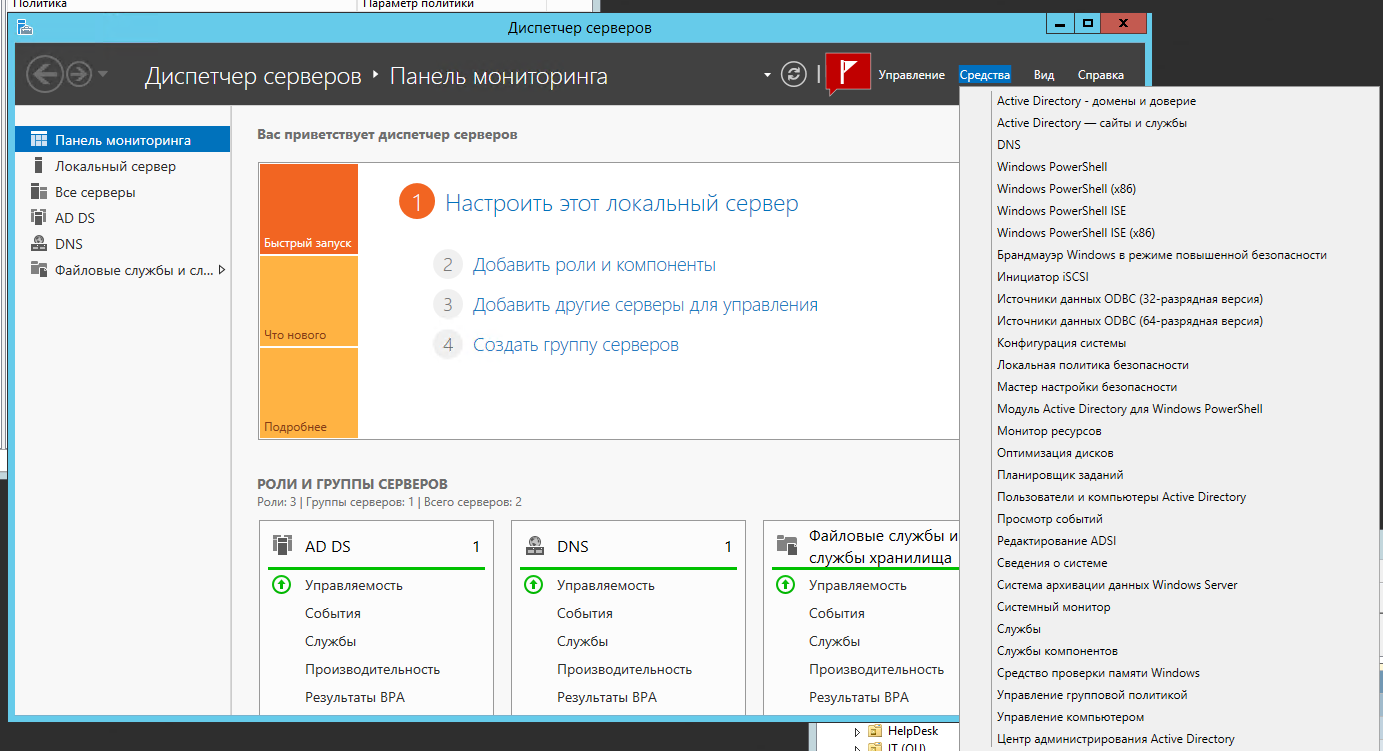


Рисунок 1. Как открыть “Управление групповой политикой” на Windows Server 2012.

Групповая политика позволяет управлять параметрами пользователя и компьютера на компьютерах под управлением операционных систем Windows Server и Windows Client. Помимо использования групповой политики для определения конфигураций для групп пользователей и клиентских компьютеров, можно также использовать групповую политику для управления серверами, настраивая множество параметров операционной и безопасности для конкретного сервера.

На “Рисунке 1” можно увидеть, как открыть данную службу.

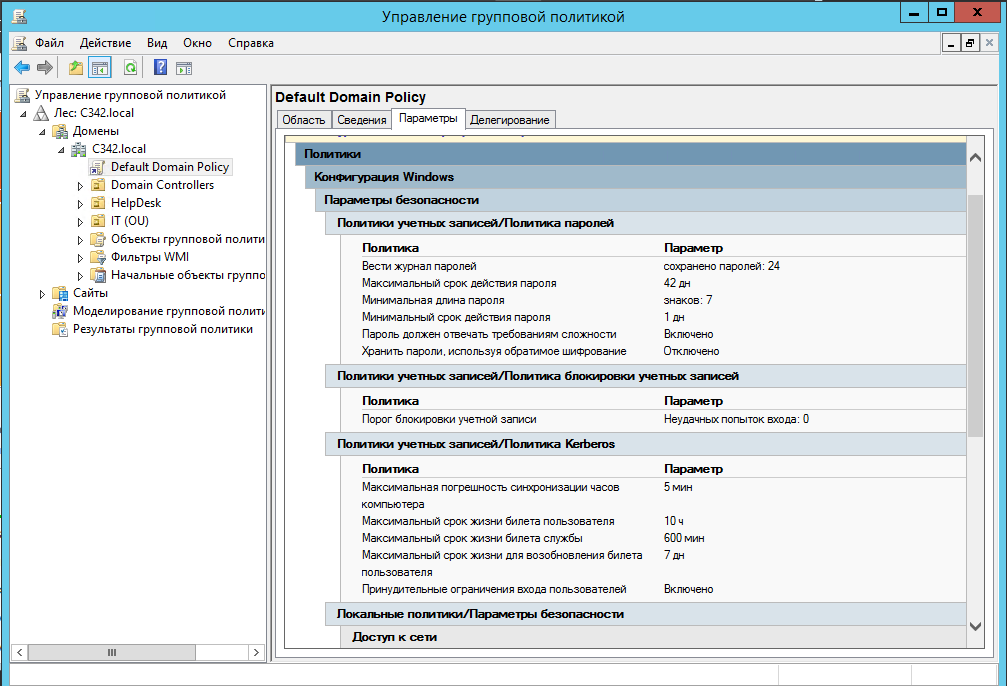


Рисунок 2 – Управление групповой политикой

На данном этапе необходимо перейти в “Default Domain Policy” по адресу “Управление групповой политикой” \” Лес C342.local” \” Домены” \” C342.local” \” Default Domain Policy”.

Это нужно, чтобы впоследствии перейти в “Редактор управления групповыми политиками”. Нажмите “Политики учетных записей/Политика паролей” правой кнопкой мыши.

**Политика паролей** — это набор правил, направленных на повышение безопасности компьютера путём поощрения пользователей к использованию надёжных паролей и их правильному использованию.

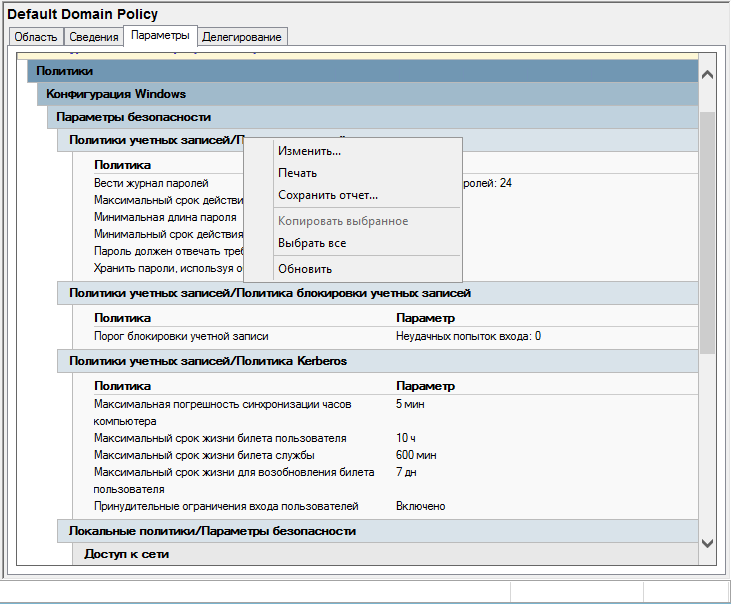


Рисунок 3 -Вход в редактор управления групповыми политиками

На этом этапе необходимо нажать кнопку “Изменить”.

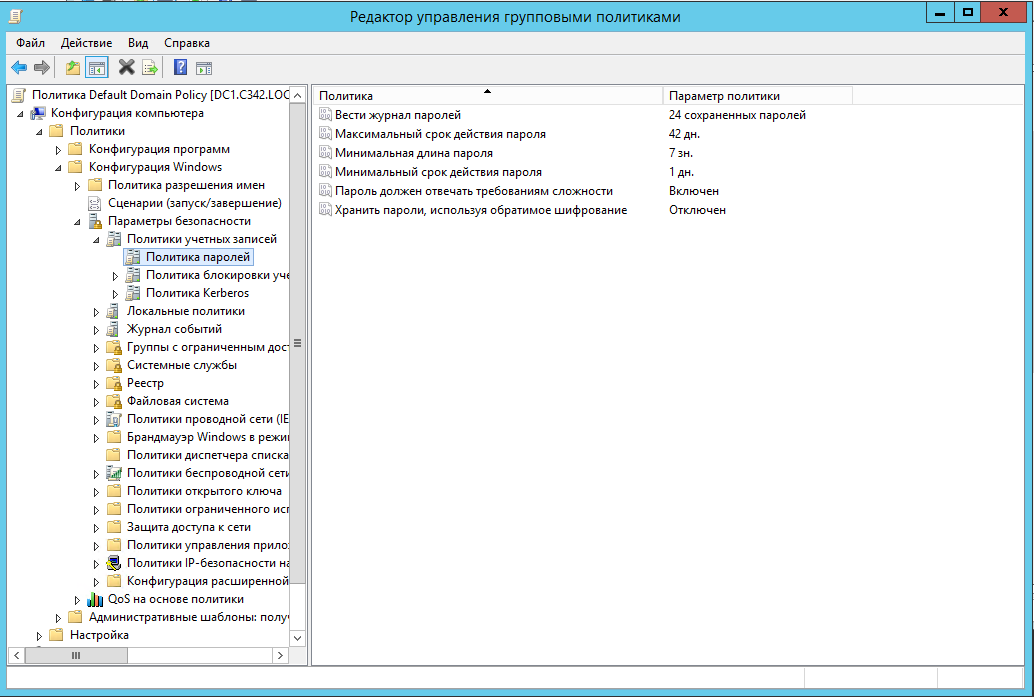


Рисунок 4 – Редактор управления групповыми политиками

На “Рисунок 4” показан путь к политике паролей домена, а также можно заметить, что политика паролей имеет следующие поля: вести журнал паролей, максимальный срок действия пароля, минимальная длина пароля, минимальный срок действия пароля, пароль должен отвечать требованиям сложности, хранить пароли, используя обратное шифрование.

Путь к политике паролей имеет следующий путь.

“Конфигурация компьютера” -> “Политики” -> “Конфигурация Windows” -> “Параметры безопасности” -> “Политики учетных записей” -> “Политики паролей”.

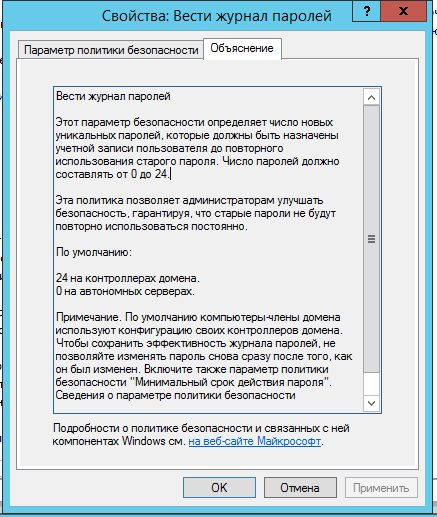


Рисунок 5 – Свойства политики “Вести журнал паролей”

На “Рисунок 5” показана справка по политике “Вести журнал паролей”. На этом окне написано, что этот параметр безопасности определяет число новых уникальных паролей, которые должны быть назначены учетной записи пользователя до повторного использования старого пароля. Число паролей должно составлять от 0 до 24. На данном этапе необходимо перейти по вкладку “Параметр политики безопасности”.

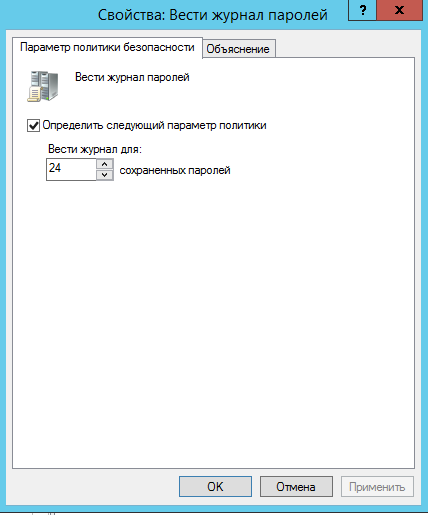


Рисунок 6 – Изменение параметра политики безопасности

На данном этапе нужно изменить 24 на 12.

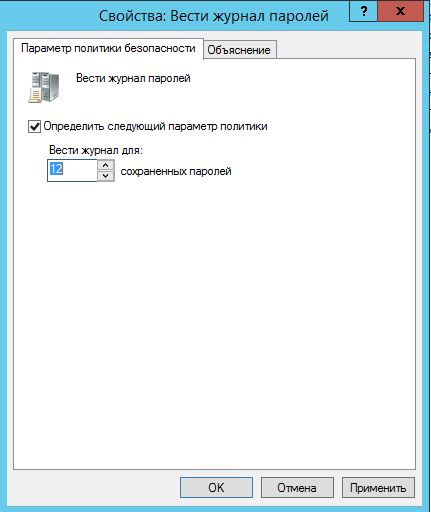


Рисунок 7 – Изменение числа сохраненных паролей

На данном этапе необходимо нажать кнопку “ОК”.

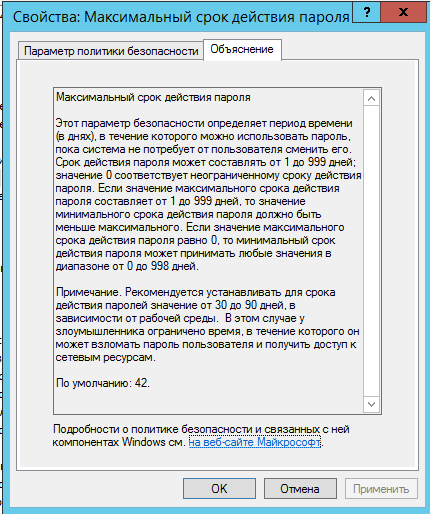


Рисунок 8 – Параметр “Максимальный срок действия пароля”

На “Рисунок 8” можно, вычитав из справочной информации, понять, что этот параметр безопасности определяет период времени в днях, в течение которого можно использовать пароль. 0 – это неограниченный срок действия, а также существует интервал от 1 до 999 дней. Рекомендуется устанавливать срок от 30 до 90 дней.

Далее необходимо нажать на вкладку “Параметр политики безопасности”

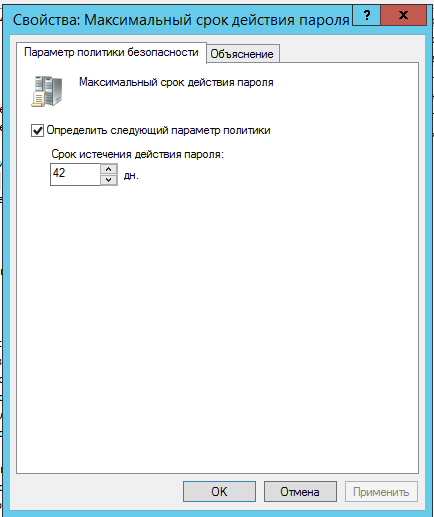


Рисунок 9 – Изменение параметра безопасности

На данном этапе необходимо изменить поле “Срок истечения действия пароля” и нажать “Применить”, а потом нажать “ОК”.

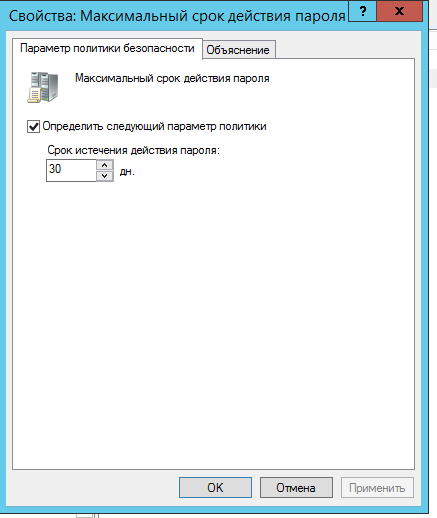


Рисунок 9.1 – Применение параметра

На данном этапе необходимо нажать кнопку “ОК”

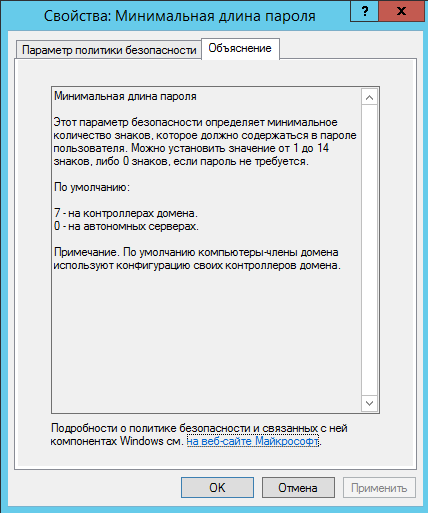


Рисунок 10 – параметр “Минимальная длина пароля”

На “Рисунок 10” можно увидеть справочную информацию по параметру “Минимальная длина пароля”. Этот параметр безопасности определяет минимальное количество знаков, которые должно содержаться в пароле пользователя. Можно устанавливать от 1 до 14 знаков, либо 0 знаков, если пароль **не требуется**.

Далее необходимо нажать на вкладку “Параметр политики безопасности”.

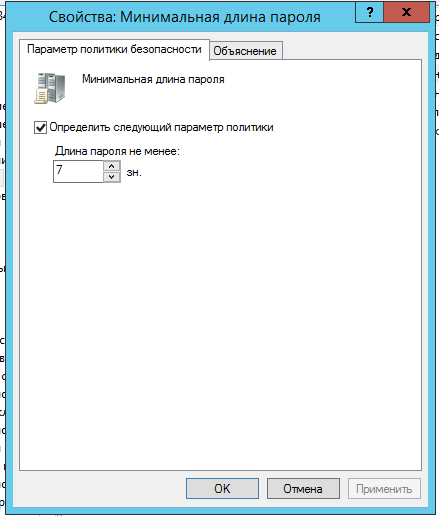


Рисунок 11 – Изменение параметра безопасности

На данном этапе нужно изменить длину пароля с 7 на 5, далее нажать на кнопку “Применить”, а в конце нажать на кнопку “ОК”.

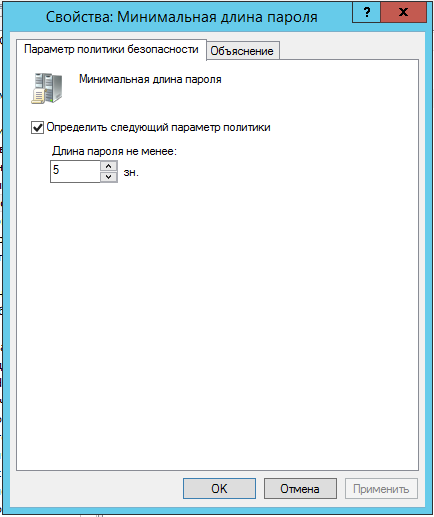


Рисунок 11.1 – применение параметра

На данном этапе необходимо нажать на кнопку “ОК”.

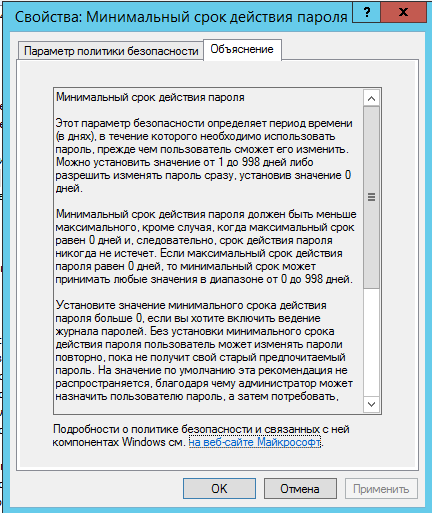


Рисунок 12 – Параметр безопасности “Минимальный срок действия пароля”

На “Рисунок 12” можно наблюдать справочную информацию по параметру безопасности “Минимальный срок действия пароля”. В этой справочной информации написано, что это параметр безопасности определяет период времени, в течение которого необходимо использовать пароль, прежде чем пользователь сможет его **изменить.** Можно установить значение от 1 до 998, либо разрешить изменять пароль сразу, установив значение 0 дней.

Далее необходимо нажать на вкладку “Параметр политики безопасности”.

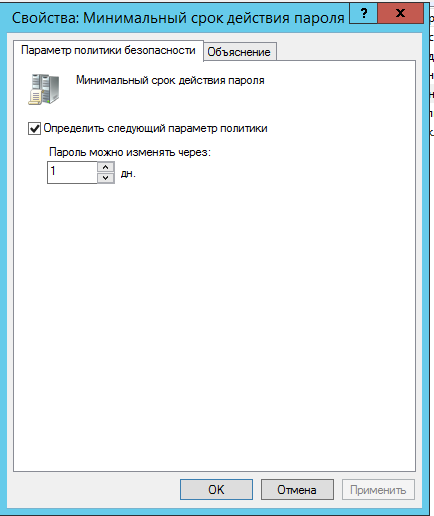


Рисунок 13 – Изменение параметра безопасности

На данном этапе необходимо изменить значение в поле “Пароль можно изменять через” с 1 на 2, затем нажать применить, а далее нажать “ОК”.

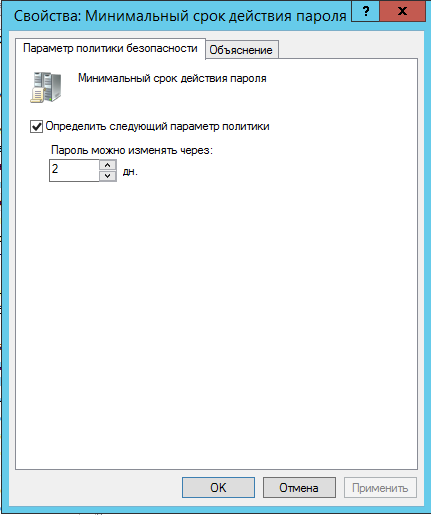


Рисунок 13.1 – Применение параметра

На данном этапе необходимо нажать на кнопку “ОК”

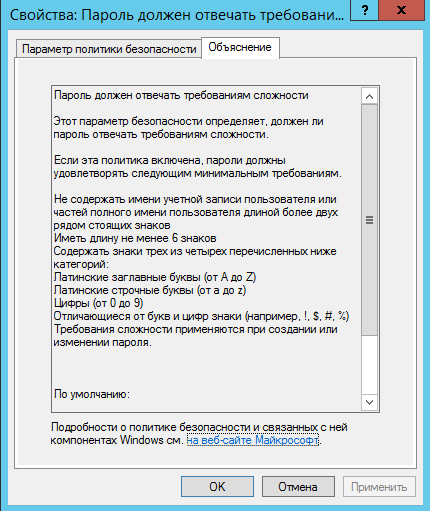


Рисунок 14 – параметр безопасности “Пароль должен отвечать требованиям сложности”

На “Рисунок 14” можно видеть справочную информацию по параметру безопасности “Пароль должен отвечать требованиям сложности”, в ней написано, что параметр определяет, должен ли пароль отвечать требованиям сложности. Если эта политика включена, пароли должны удовлетворить следующими минимальными требованиями: не содержать имени учетной записи пользователя или частей полного имени пользователя длиной более двух рядом стоящих знаков; иметь длину не более 6 знаков; содержать знаки трех из четырех перечисленных ниже категорий; Латинские буквы заглавные и строчные; цифры; специальные знаки.

Далее необходимо нажать на вкладку “Параметр политики безопасности”.

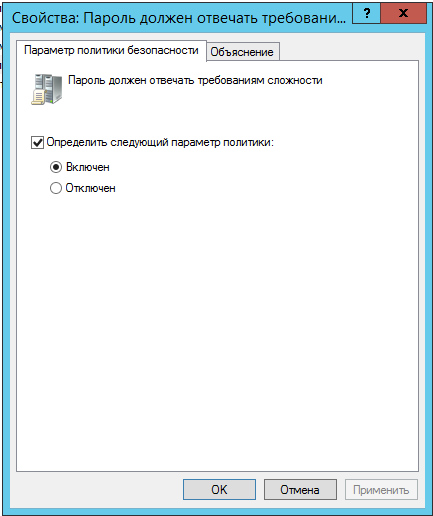


Рисунок 15 - Изменение параметра безопасности

На данном этапе можно отключить параметр безопасности, нажав на соответствующий флаг, затем необходимо нажать “Применить”, а потом нажать кнопку “ОК”.

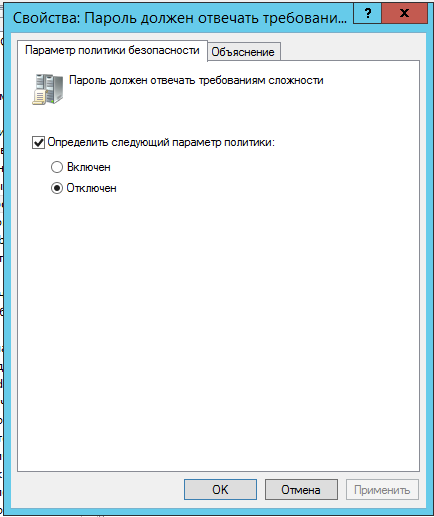


Рисунок 15.1 – Применение параметра

На данном этапе необходимо нажать на кнопку “ОК”

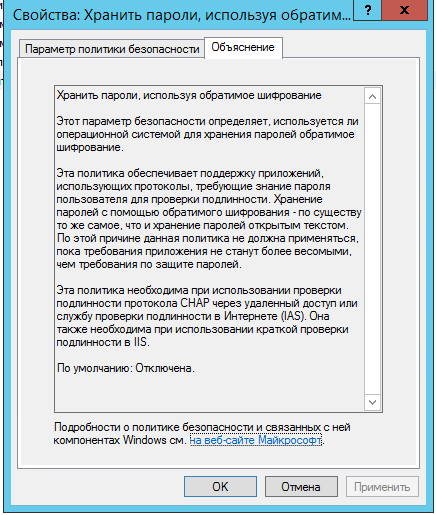


Рисунок 16 – параметр безопасности “Хранить пароли, используя обратимое шифрование”

На “Рисунок 16” можно наблюдать справочную информацию по параметру безопасности “Хранить пароли, используя обратимое шифрование”. В ней написано, что этот параметр безопасности определяет, используется ли операционной системой для хранения паролей обратимое шифрование.

Далее необходимо нажать на вкладку “Параметр политики безопасности”.

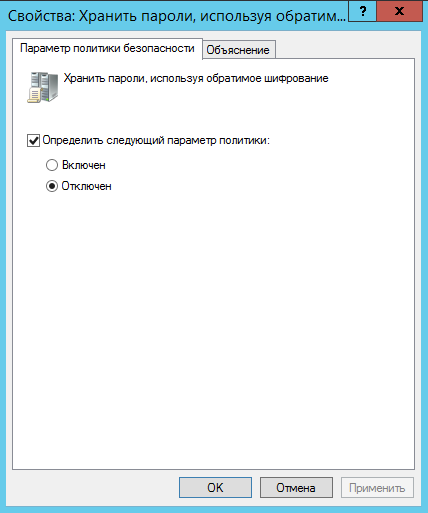


Рисунок 17 – Изменение параметра безопасности

На данном этапе необходимо выбрать флаг “Включен”, нажать кнопку “Приметь”, а далее нажать кнопку “ОК”.

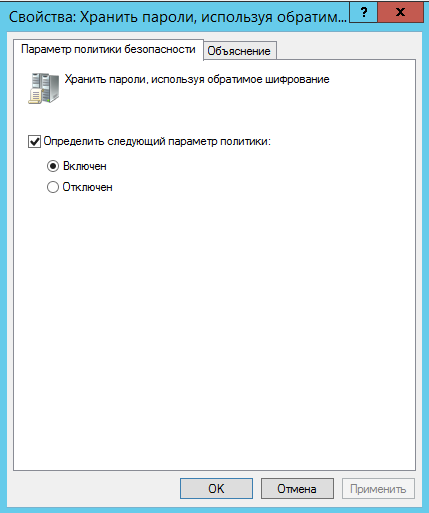


Рисунок 17.1 – Применение параметра

На данном этапе необходимо нажать кнопку “ОК”.

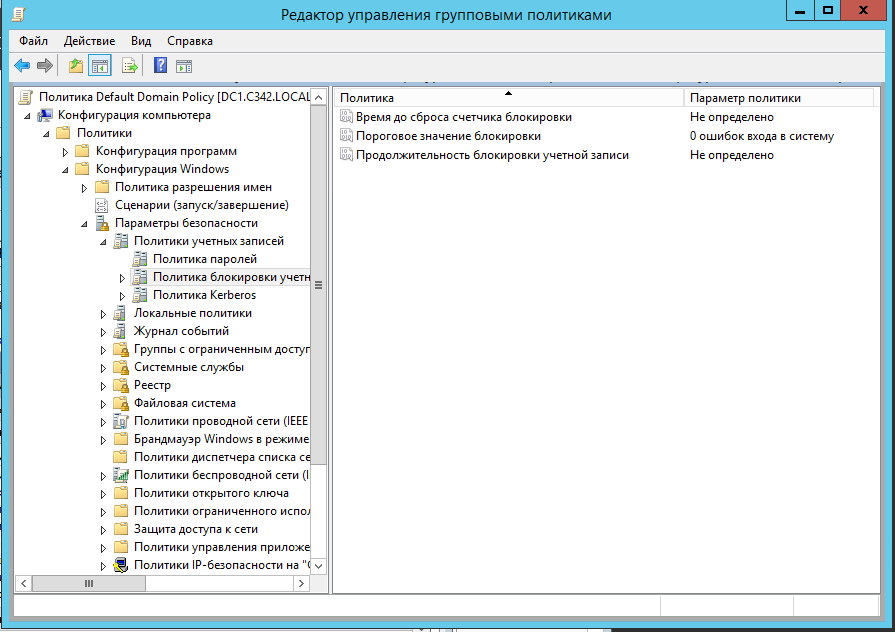


Рисунок 18 – Политика блокировки учетной записи

На данном этапе нужно перейти из “Политики паролей” в “Политику блокировки учетной записи”. В этой политике можно изменять пороговое значений неправильный попыток до блокировки учетной записи, а также продолжительность этой блокировки.

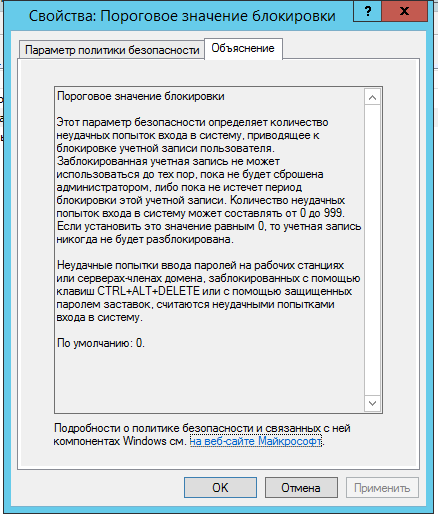


Рисунок 19 – параметр безопасности “Пороговое значение блокировки”

На “Рисунок 19” можно наблюдать справочную информацию о параметре безопасности “Пороговое значение блокировки”. Он определяет количество неудачных попыток входа в систему, приводящее к блокировке учетной записи пользователя. Заблокированная учетная запись не может использоваться до тех пор, пока не будет сброшена администратором, либо пока не истечет период блокировки учетной записи.

Далее необходимо перейти во вкладку “Параметр политики безопасности”.

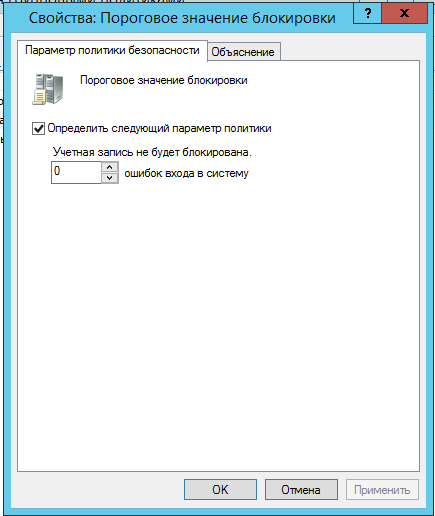


Рисунок 20 – изменение параметра безопасности

В поле “ошибок входа в систему” нужно установить 3, а затем нажать на кнопку “Применить”.

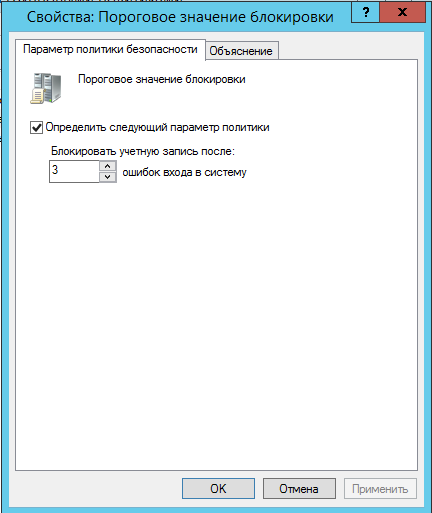


Рисунок 20.1 – Применение изменений

На данном этапе нужно нажать кнопку “ОК”.

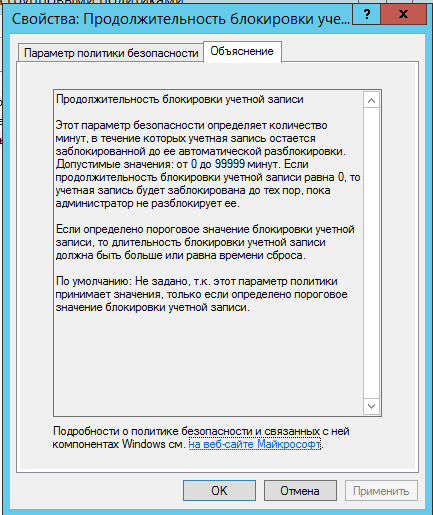


Рисунок 21 – параметр безопасности “Продолжительность блокировки учетной записи”.

На “Рисунок 21” можно наблюдать справочную информацию о параметре безопасности “Продолжительность блокировки учетной записи”. Этот параметр определяет количество минут, в течение которых учетная запись остается заблокированной до ее автоматической разблокировки. Значение от 0 до 99999 минут.

Далее необходимо перейти во вкладку “Параметр политики безопасности”.

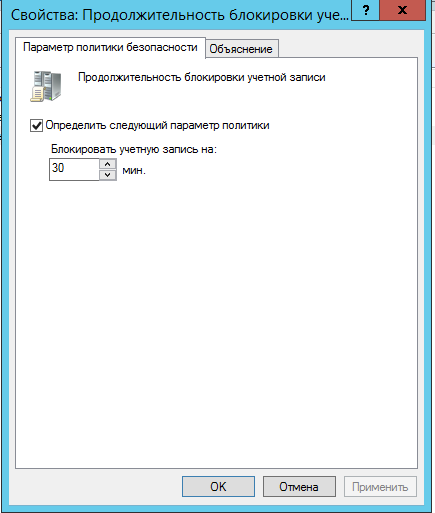


Рисунок 22 – Изменение параметра безопасности

На данном этапе необходимо изменить значение в поле “Блокировать учетную запись на” на 5 минут, а зачем нажать кнопку “Приметь”.

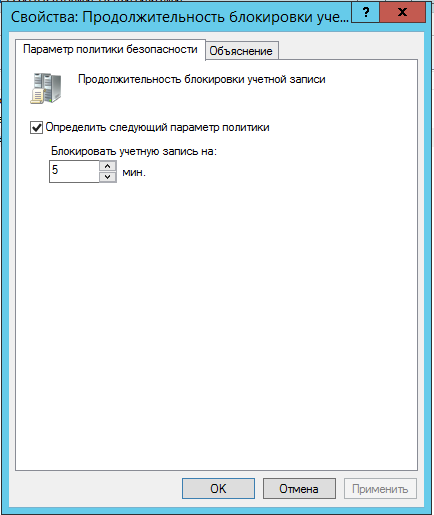


Рисунок 22.1 – Применение параметров

На данном этапе нужно нажать кнопку “ОК”.