**Практическая работа**

**«Настройка политики безопасности»**

ЦЕЛИ РАБОТЫ:

1. Научиться настраивать параметры идентификации и аутентификации.

2. Научиться настраивать параметры регистрации и аудита. Работа с журналом событий.

ОБОРУДОВАНИЕ: ПК, Windows 10.

ВРЕМЯ ВЫПОЛНЕНИЯ: 45 минут

КРАТКАЯ ТЕОРИЯ И МЕТОДИЧЕСКИЕ РЕКОМЕНДАЦИИ:

**Под политикой безопасности понимают** совокупность документированных решений, принимаемых руководством организации и направленных на защиту информации и ассоциированных с ней ресурсов.

Политика безопасности строится на основе анализа рисков, которые признаются реальными для информационной системы организации. Когда риски проанализированы и стратегия защиты определена, составляется программа обеспечения информационной безопасности. Под эту программу выделяются ресурсы, назначаются ответственные, определяется порядок контроля выполнения программы и т.п.

С практической точки зрения политику безопасности целесообразно рассматривать на трех уровнях детализации.

1. К верхнему уровню можно отнести решения, затрагивающие организацию в целом. Они носят весьма общий характер и, как правило, исходят от руководства организации.
2. К среднему уровню можно отнести вопросы, касающиеся отдельных аспектов информационной безопасности, но важные для различных эксплуатируемых организацией систем.
3. Политика безопасности нижнего уровня относится к конкретным информационным сервисам.

**Идентификация** – это присвоение субъектам и объектам доступа личного идентификатора и сравнение его с заданным.

**Аутентификация (установление подлинности)** – это проверка принадлежности субъекту доступа предъявленного им идентификатора и подтверждение его подлинности (т.е. аутентификация заключается в проверке: является ли подключающийся субъект тем, за кого он себя выдает).

Механизм идентификации и аутентификации:

* пользователь предоставляет системе свой личный идентификатор (например, вводит пароль или предоставляет палец для сканирования отпечатков);
* система сравнивает полученный идентификатор со всеми хранящимися в ее базе идентификаторами;
* если результат сравнения успешный, то пользователь получает доступ к системе в рамках установленных полномочий (совокупность прав);
* в случае отрицательного результата система сообщает об ошибке и предлагает повторно ввести идентификатор;
* Если пользователь превышает лимит возможных повторов ввода информации, система временно блокируется и выдается сообщение о несанкционированных действиях.

**Протоколирование -** сбор и накопление информации о событиях, происходящих в информационной системе. У каждого сервиса свой набор возможных событий, но в любом случае их можно разделить на:

* Внешние (вызванные действиями других сервисов),
* Внутренние (вызванные действиями самого сервиса),
* Клиентские (вызванные действиями пользователей и администраторов).

**Аудит –** это анализ накопленной информации, проводимый оперативно, в реальном времени или периодически (например, раз в день). Оперативный аудит с автоматическим реагированием на выявленные нештатные ситуации называется активным.

**Задачи протоколирования и аудита**

* Обеспечение подотчетности пользователей и администраторов
* Обеспечение возможности реконструкции последовательности событий
* Обнаружение попыток нарушений информационной безопасности
* Предоставление информации для выявления и анализа проблем

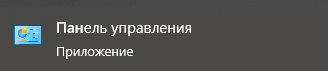
*Протоколирование осуществляется в 2 этапа.*

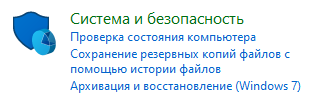
1. Регистрация событий
2. Протоколирование данных о событиях

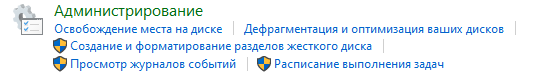
***ПОРЯДОК ВЫПОЛНЕНИЯ РАБОТЫ И ФОРМА ОТЧЕТНОСТИ:***

**Задание 1. Настройка параметров идентификации и аутентификации.**

Шаг1. Панель управления→Система и Безопасность→ Администрирование

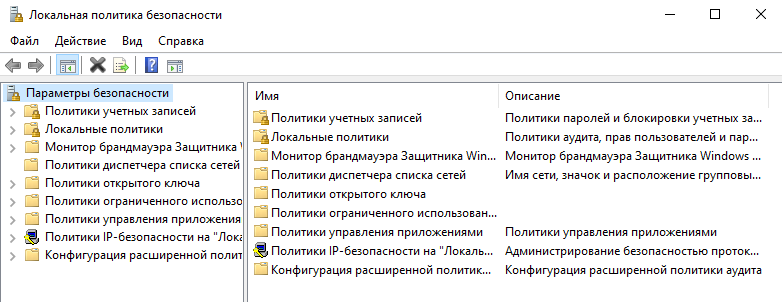




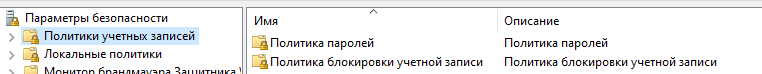


Шаг2. Следует выбрать «Локальная политика безопасности».





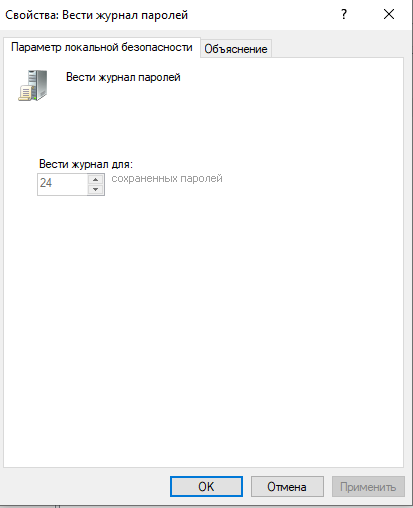
Шаг3.Выбрать «Политика учетной записи»



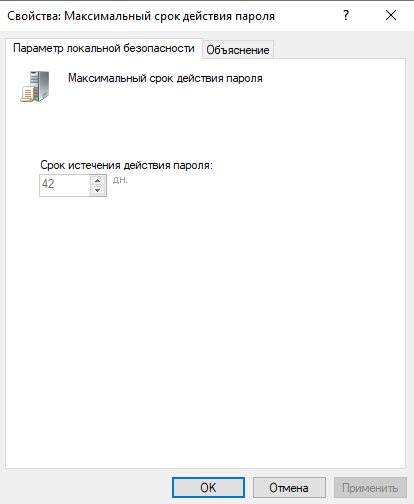
Шаг4.Следует выбрать Политику паролей(содержит настройки пароля для учетных записей)



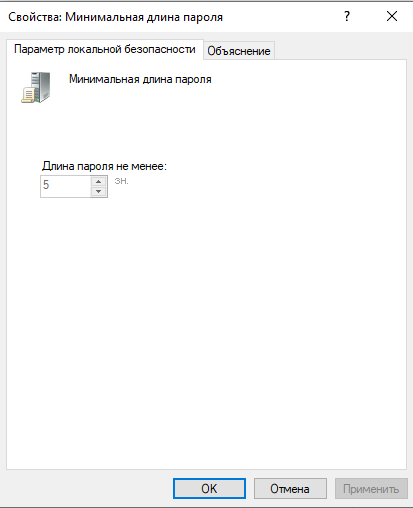
4.1. Пункт «Ввести журнал паролей»



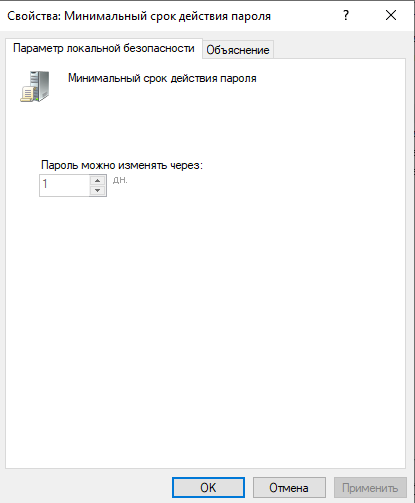
4.2. Пункт «Максимальный срок действия пароля»



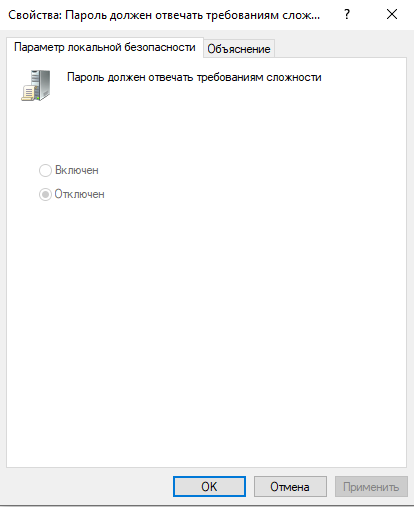
4.3. Пункт «Минимальная длина пароля»



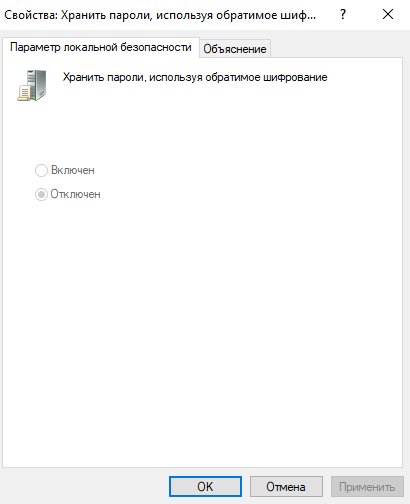
4.4. Пункт «Минимальный срок действия пароля».



4.5. Пункт «Пароль должен отвечать требованиям сложности»



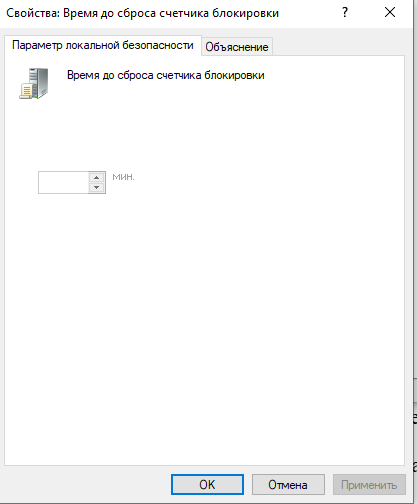
4.6. Пункт «Хранить пароли, используя обратимое шифрование»



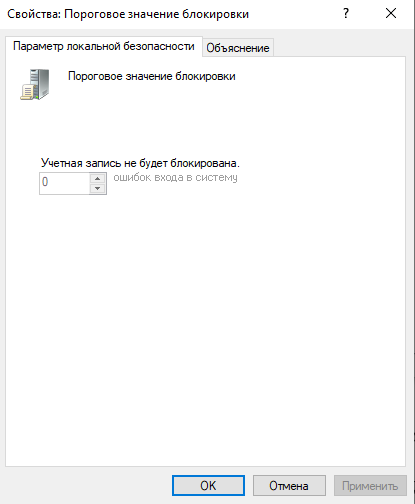
Шаг 5. Политика «Блокировка учетных записей»



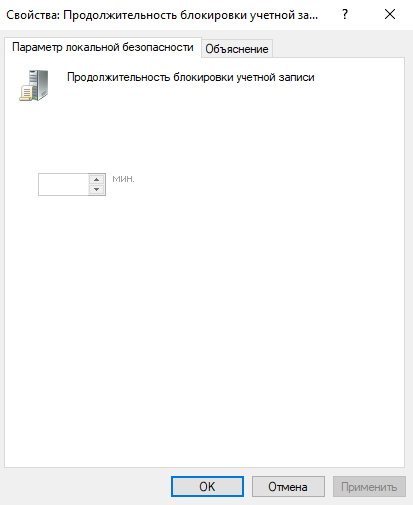
5.1. Пункт «Сброс счетчика блокировки»



5.2. Пункт «Пороговое значение блокировки»

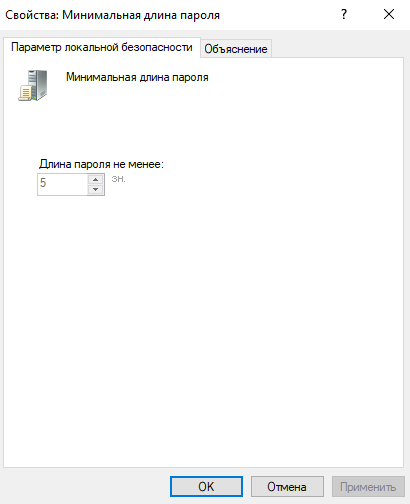


5.3. Пункт «Блокировка учетной записи»



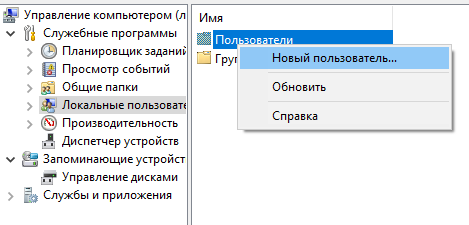
**Контрольное задание**

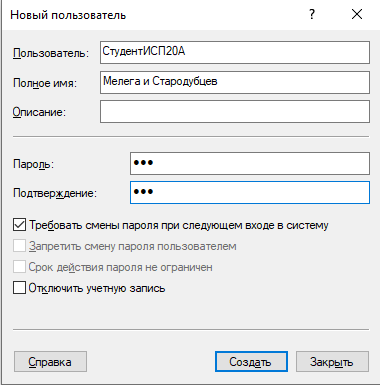
1. Установить минимальную длину пароля 8 символов.

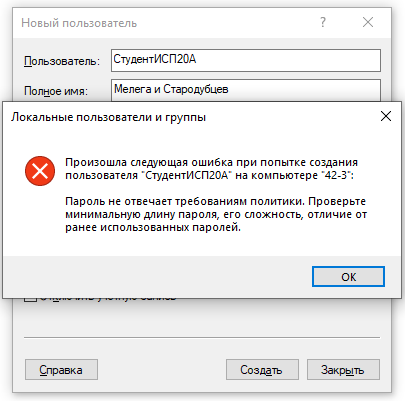


2. Создать свою учетную запись с паролем менее 4 символов. (окно об ошибке пароля зафиксировать в отчете)







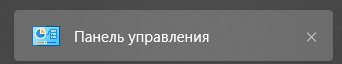


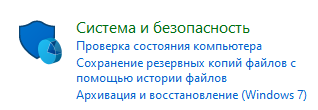
3. Удалить созданную учетную запись и установить минимальную длину пароля 0.

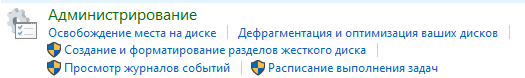
**Задание 2. Настройка параметров регистрации и аудита.**

**I. Настройка механизмов аудита.**

Шаг 1. Пуск → ‘Панель управления’→’Система и Безопасность’→ ‘Администрирование’→ ‘Локальная политика безопасности’





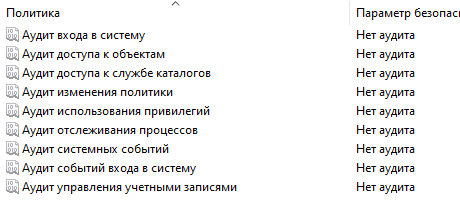




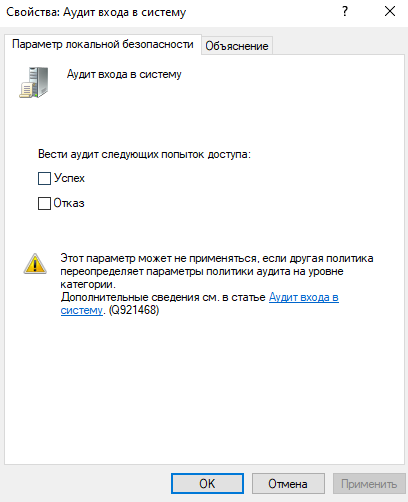
Шаг 2. ‘Локальные политики’→ ‘Политика аудита’



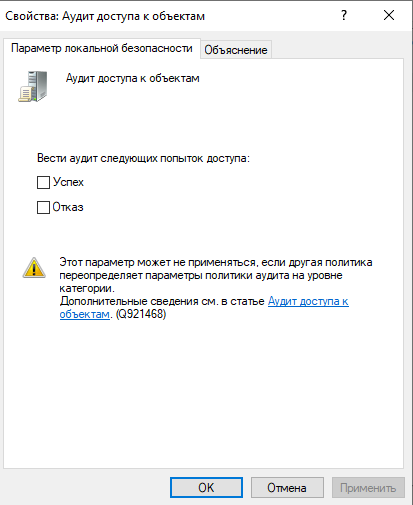
Шаг 3. Установка параметров политики аудита.



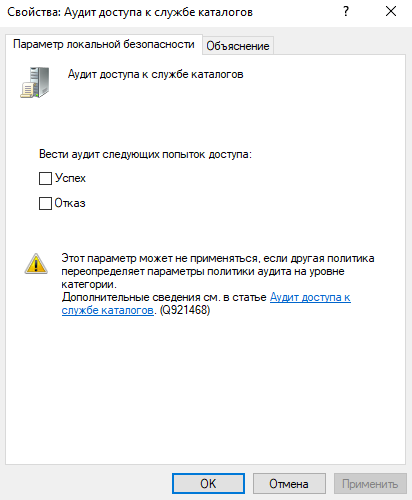
3.1. «Аудит входа в систему»



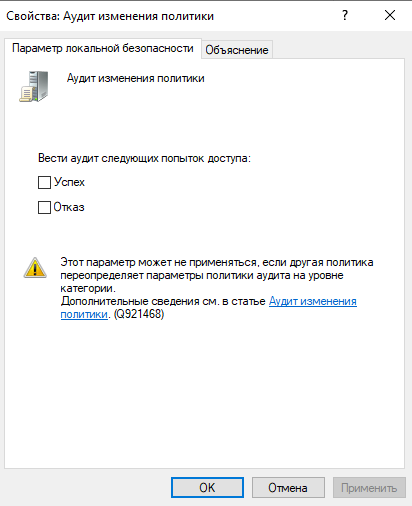
3.2. «Аудит доступа к объектам»



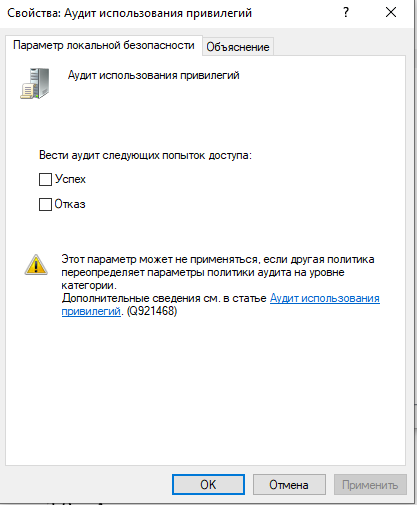
3.3. «Аудит доступа к службе каталогов»



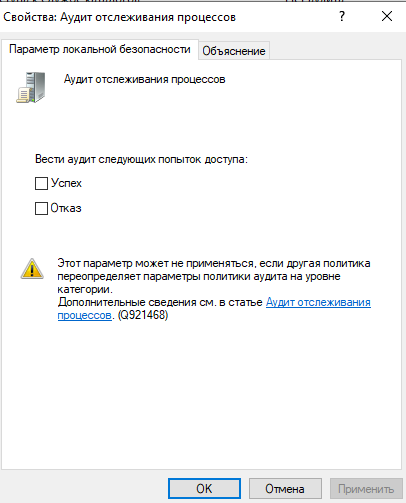
3.4. «Аудит изменения политики»



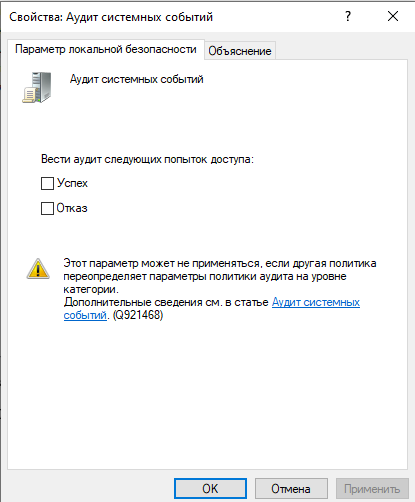
3.5. «Аудит использования привилегий»



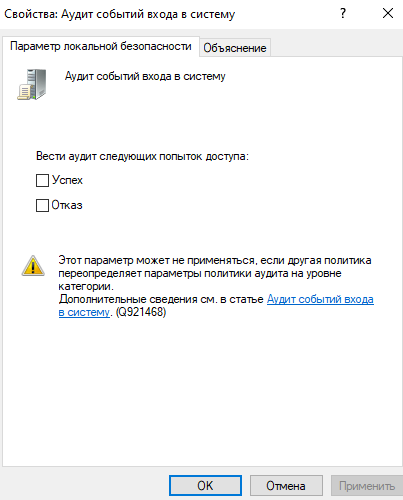
3.6. «Аудит отслеживания процессов»



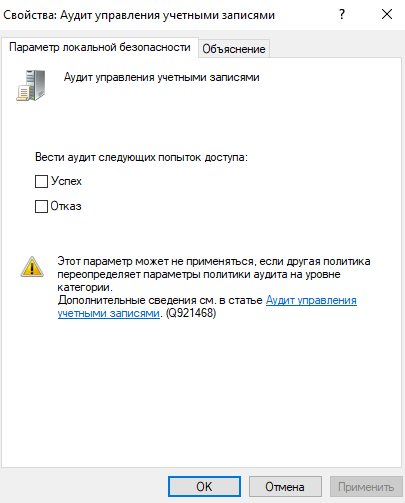
3.7. «Аудит системных событий»



3.8. «Аудит событий входа в систему»

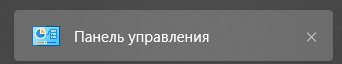


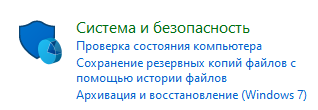
3.9. «Аудит управления учетными записями»

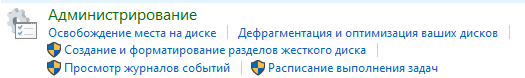


**II. Просмотр событий в журнале безопасности.**

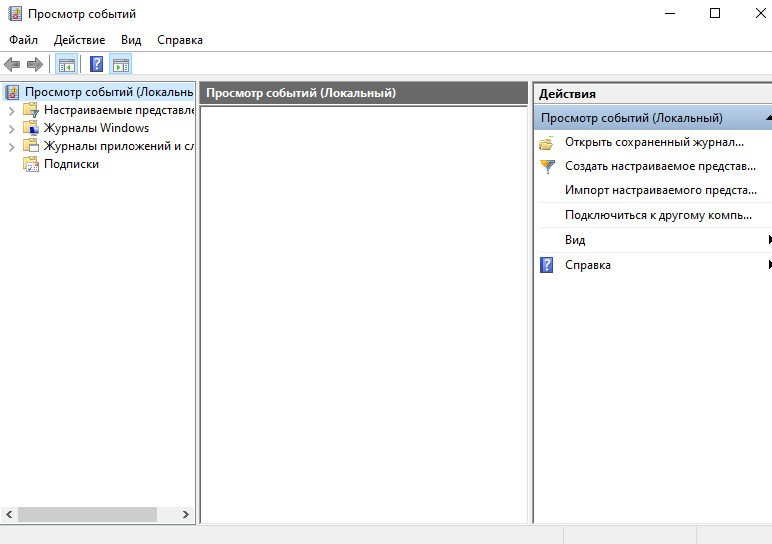
‘Пуск’→ ‘Панель управления’→’Система и Безопасность’→ ‘Администрирование’→ ‘Просмотр событий’.









****