**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

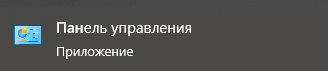
*Протоколирование осуществляется в 2 этапа.*

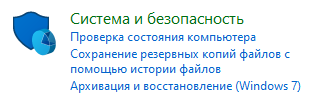
1. Регистрация событий
2. Протоколирование данных о событиях

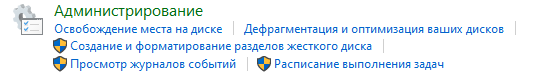
***ПОРЯДОК ВЫПОЛНЕНИЯ РАБОТЫ И ФОРМА ОТЧЕТНОСТИ:***

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

Шаг1. Панель управления→Система и Безопасность→ Администрирование

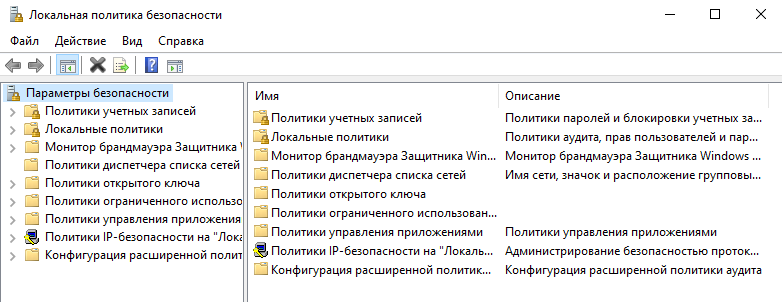




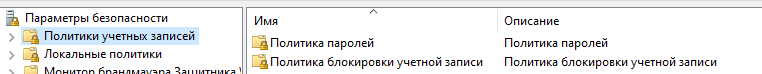


Шаг2. Следует выбрать «Локальная политика безопасности».





Шаг3.Выбрать «Политика учетной записи»

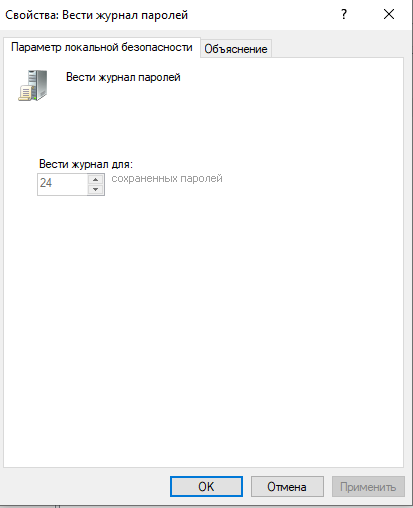


Шаг4.Следует выбрать Политику паролей(содержит настройки пароля для учетных записей)



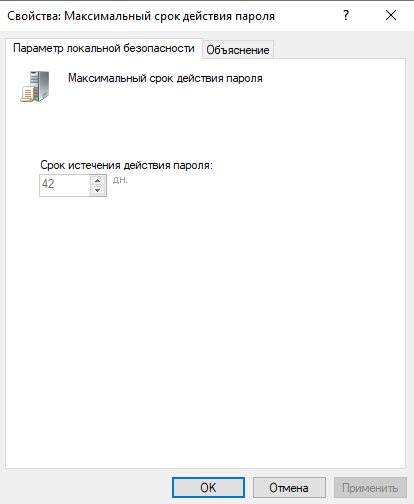
4.1. Пункт «Ввести журнал паролей»

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.



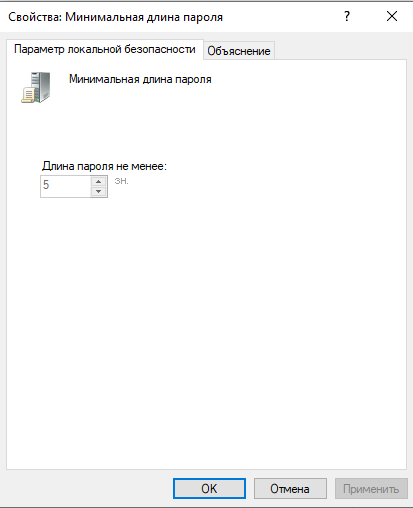
4.2. Пункт «Максимальный срок действия пароля»

Этот параметр безопасности определяет период времени (в днях), в течение которого можно использовать пароль, пока система не потребует от пользователя сменить его. Срок действия пароля может составлять от 1 до 999 дней; значение 0 соответствует неограниченному сроку действия пароля.



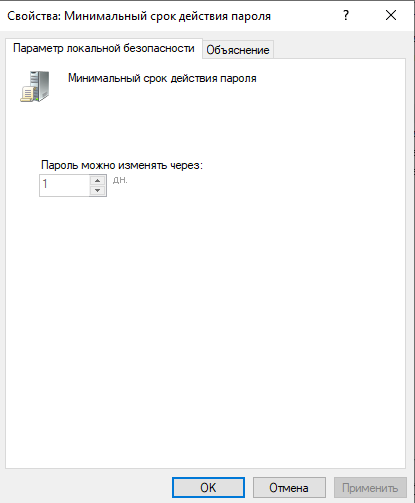
4.3. Пункт «Минимальная длина пароля»

Этот параметр безопасности определяет минимальное количество знаков, которое должно содержаться в пароле пользователя.



4.4. Пункт «Минимальный срок действия пароля».

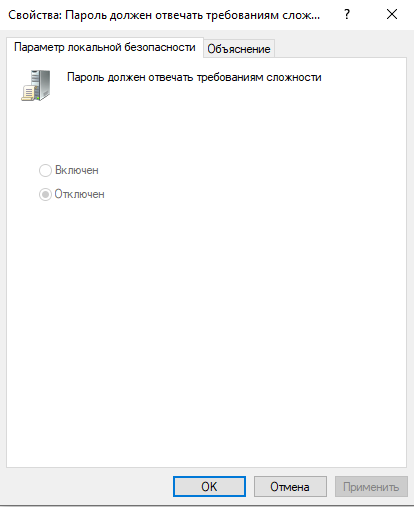
Этот параметр безопасности определяет период времени (в днях), в течение которого необходимо использовать пароль, прежде чем пользователь сможет его изменить. Можно установить значение от 1 до 998 дней либо разрешить изменять пароль сразу, установив значение 0 дней.



4.5. Пункт «Пароль должен отвечать требованиям сложности»

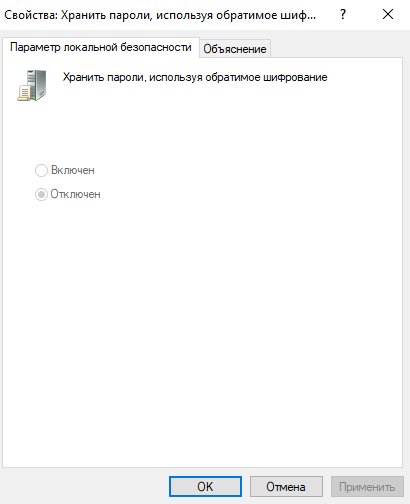
Этот параметр безопасности определяет, должен ли пароль отвечать требованиям сложности.

Если эта политика включена, пароли должны удовлетворять следующим минимальным требованиям.



4.6. Пункт «Хранить пароли, используя обратимое шифрование»

Этот параметр безопасности определяет, используется ли операционной системой для хранения паролей обратимое шифрование.

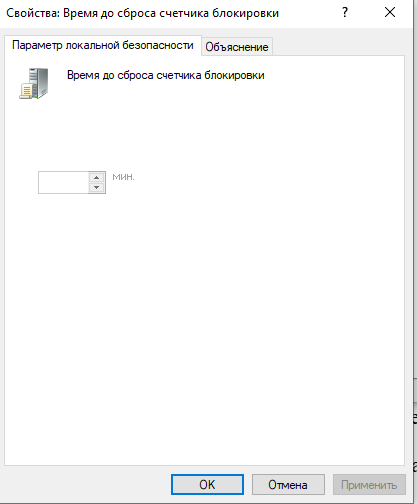


Шаг 5. Политика «Блокировка учетных записей»



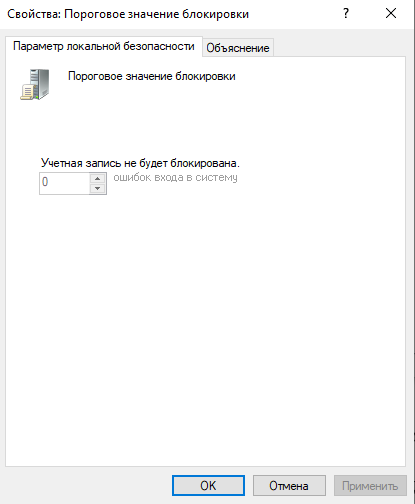
5.1. Пункт «Сброс счетчика блокировки»

Этот параметр безопасности определяет количество минут, которые должны пройти после неудачной попытки входа в систему до того, как счетчик неудачных попыток входа будет сброшен до 0. Допустимые значения: от 1 до 99999 минут.



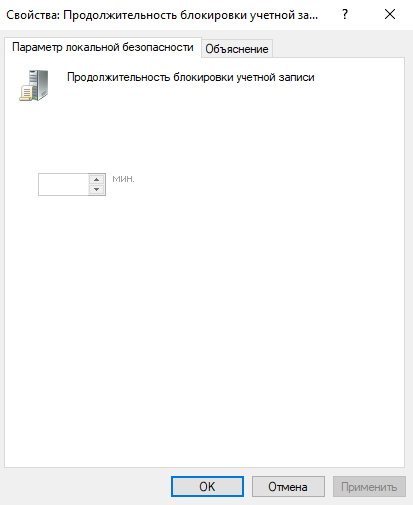
5.2. Пункт «Пороговое значение блокировки»

Этот параметр безопасности 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 этой учетной записи.



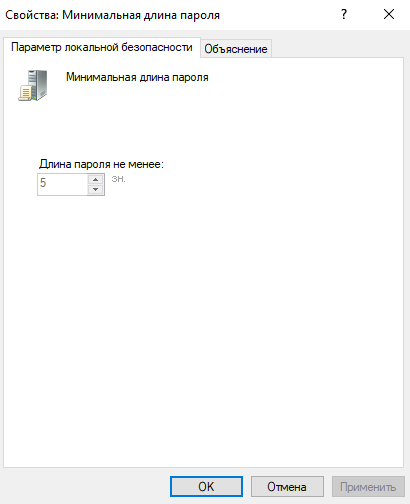
5.3. Пункт «Блокировка учетной записи»

Этот параметр безопасности определяет количество минут, в течение которых учетная запись остается заблокированной до ее автоматической разблокировки. Допустимые значения: от 0 до 99999 минут.



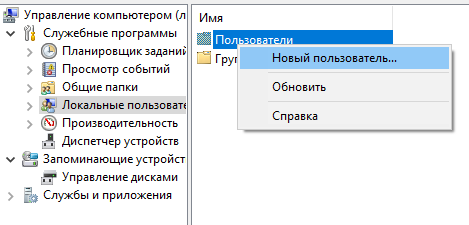
**Контрольное задание**

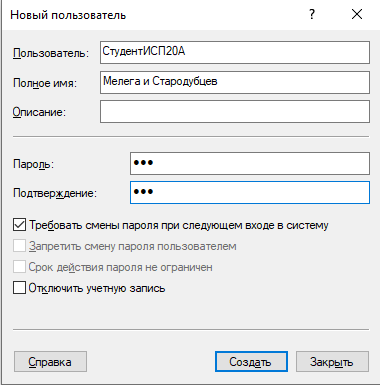
1. Установить минимальную длину пароля 8 символов.

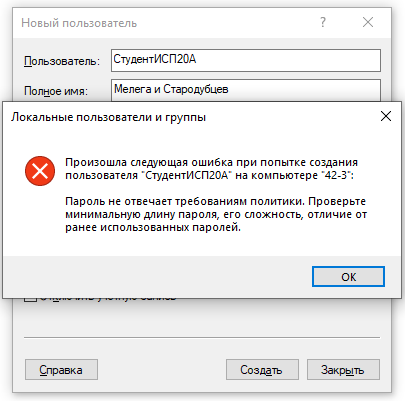


2. Создать свою учетную запись с паролем менее 4 символов. (окно об ошибке пароля зафиксировать в отчете)







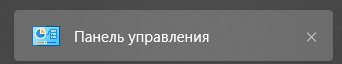


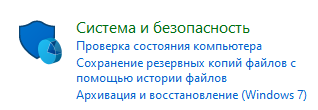
3. Удалить созданную учетную запись и установить минимальную длину пароля 0.

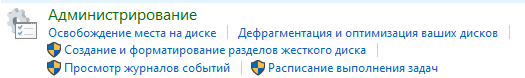
**Задание 2. Настройка параметров регистрации и аудита.**

**I. Настройка механизмов аудита.**

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





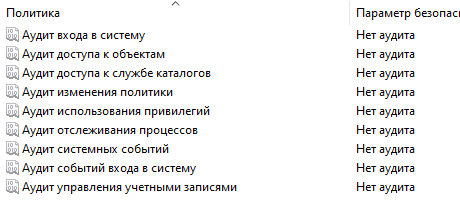




Шаг 2. ‘Локальные политики’→ ‘Политика аудита’

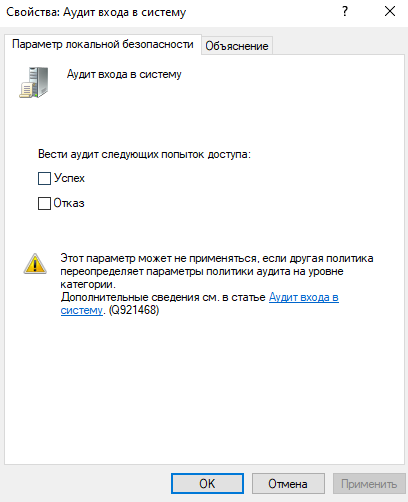


Шаг 3. Установка параметров политики аудита.



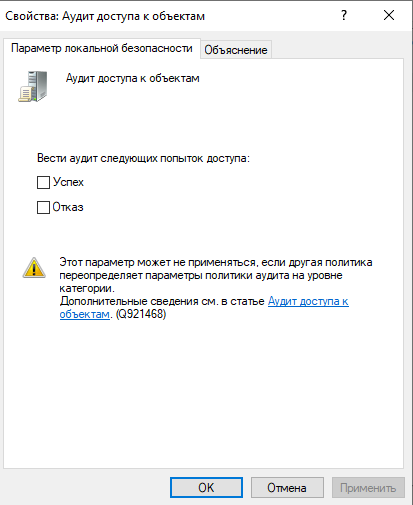
3.1. «Аудит входа в систему»

Этот параметр безопасности определяет, будет ли операционная система выполнять аудит каждой попытки входа пользователя в систему или выхода из нее на данном компьютере.



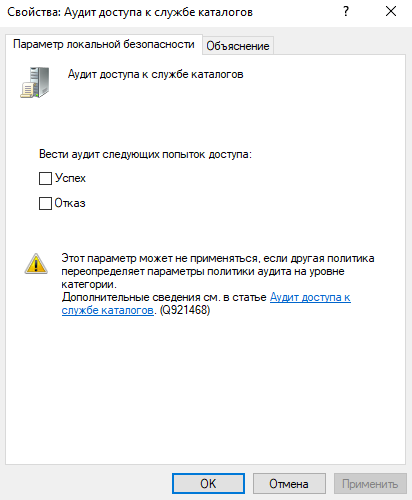
3.2. «Аудит доступа к объектам»

Этот параметр безопасности определяет, будет ли операционная система выполнять аудит попыток доступа пользователей к объектам, не относящимся к Active Directory. Аудит выполняется только для объектов, для которых указаны системные списки управления доступом, при условии, что запрашиваемый тип доступа (например, "Запись", "Чтение" и "Изменение") и учетная запись, выполняющая запрос, соответствуют параметрам в таких списках.



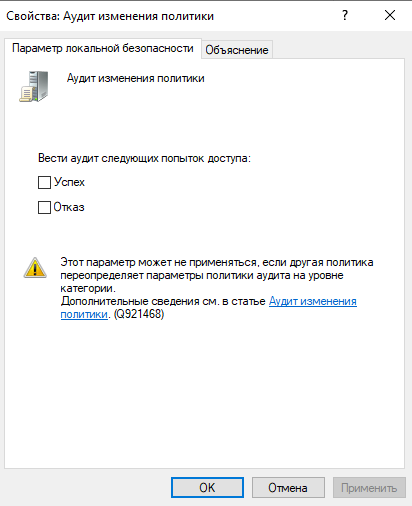
3.3. «Аудит доступа к службе каталогов»

Этот параметр безопасности определяет, будет ли операционная система выполнять аудит попыток доступа пользователей к объектам Active Directory. Аудит выполняется только для объектов, для которых указан системный список управления доступом, при условии, что запрашиваемый тип доступа (например, "Запись", "Чтение" или "Изменение") и учетная запись, выполняющая запрос, соответствуют параметрам в данном списке.



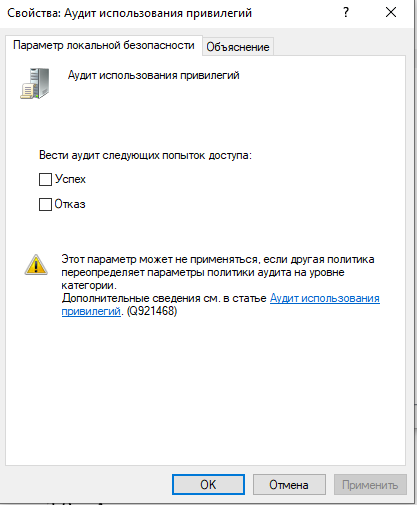
3.4. «Аудит изменения политики»

Этот параметр безопасности определяет, будет ли операционная система выполнять аудит каждой попытки изменения политики назначения прав пользователей, политики аудита, политики учетных записей или политики доверия.



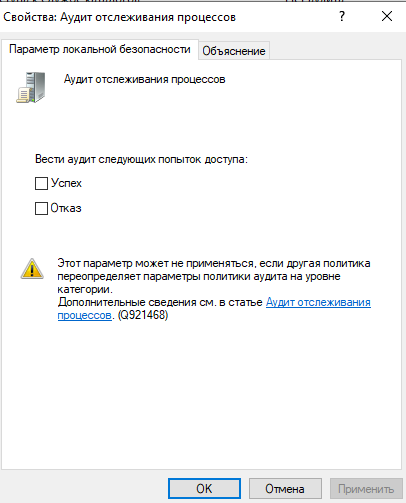
3.5. «Аудит использования привилегий»

Этот параметр безопасности определяет, будет ли выполняться аудит каждого случая применения прав пользователя.



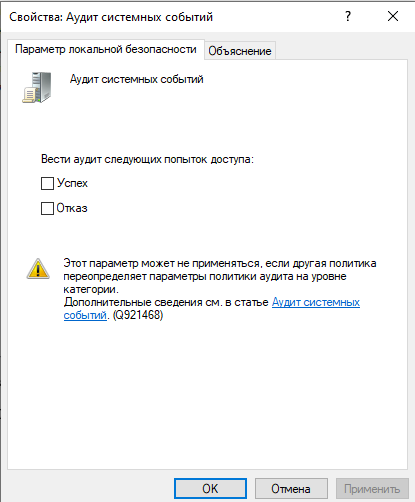
3.6. «Аудит отслеживания процессов»

Этот параметр безопасности определяет, будет ли операционная система выполнять аудит связанных с процессами событий, таких как создание процесса, завершение процесса, обработка дублирований, а также непрямой доступ к объектам.



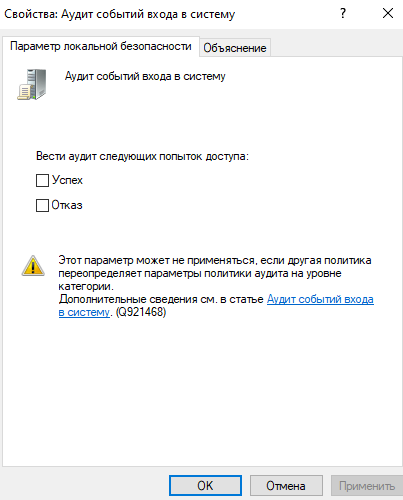
3.7. «Аудит системных событий»

Этот параметр безопасности определяет, будет ли операционная система выполнять аудит следующих событий.



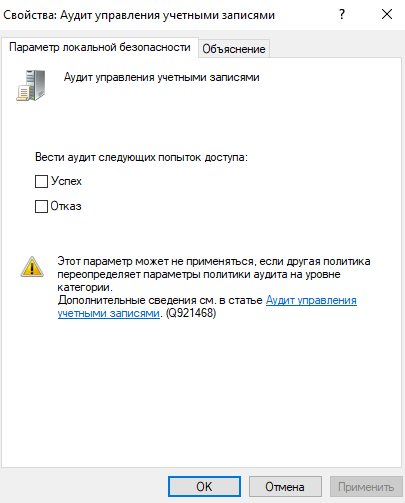
3.8. «Аудит событий входа в систему»

Этот параметр безопасности определяет, будет ли операционная система выполнять аудит каждый раз, когда на компьютере выполняется проверка учетных данных.



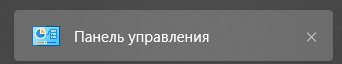
3.9. «Аудит управления учетными записями»

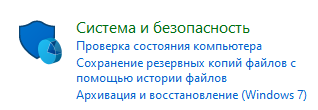
Этот параметр безопасности определяет, необходимо ли выполнять аудит каждого события управления учетными записями на компьютере. Далее указаны примеры событий управления учетными записями.

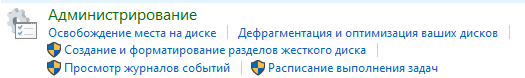


**II. Просмотр событий в журнале безопасности.**

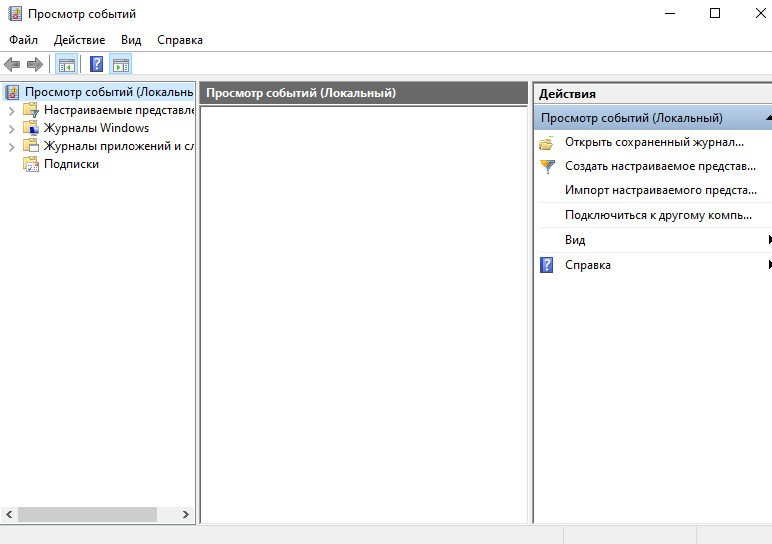
‘Пуск’→ ‘Панель управления’→’Система и Безопасность’→ ‘Администрирование’→ ‘Просмотр событий’.









****