# Лабораторная работа №4

## Настройка политики безопасности

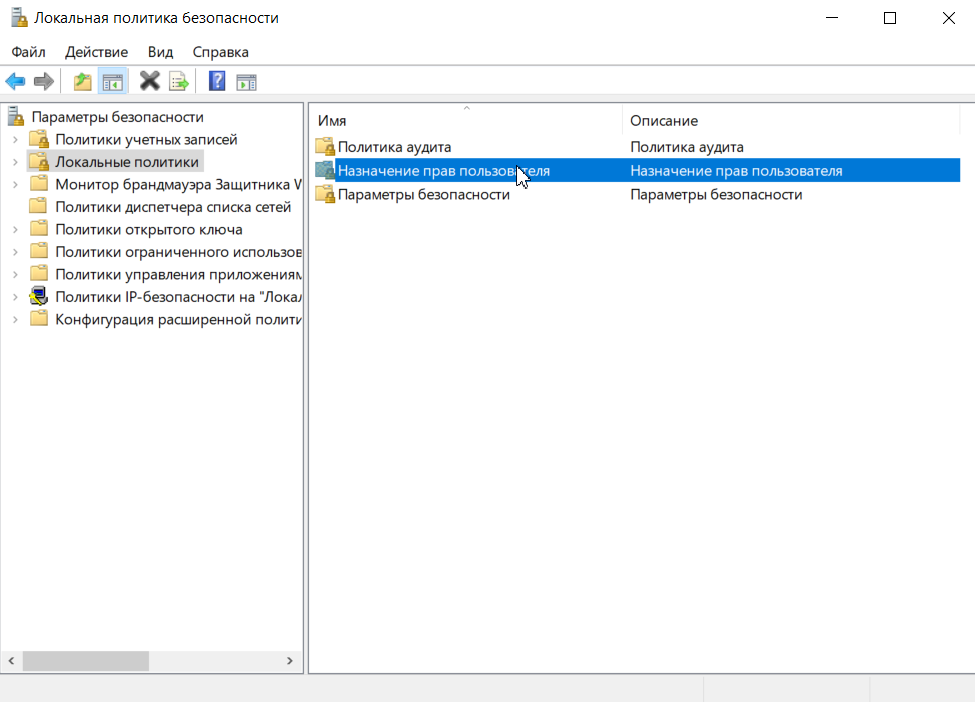
**Цель работы:**

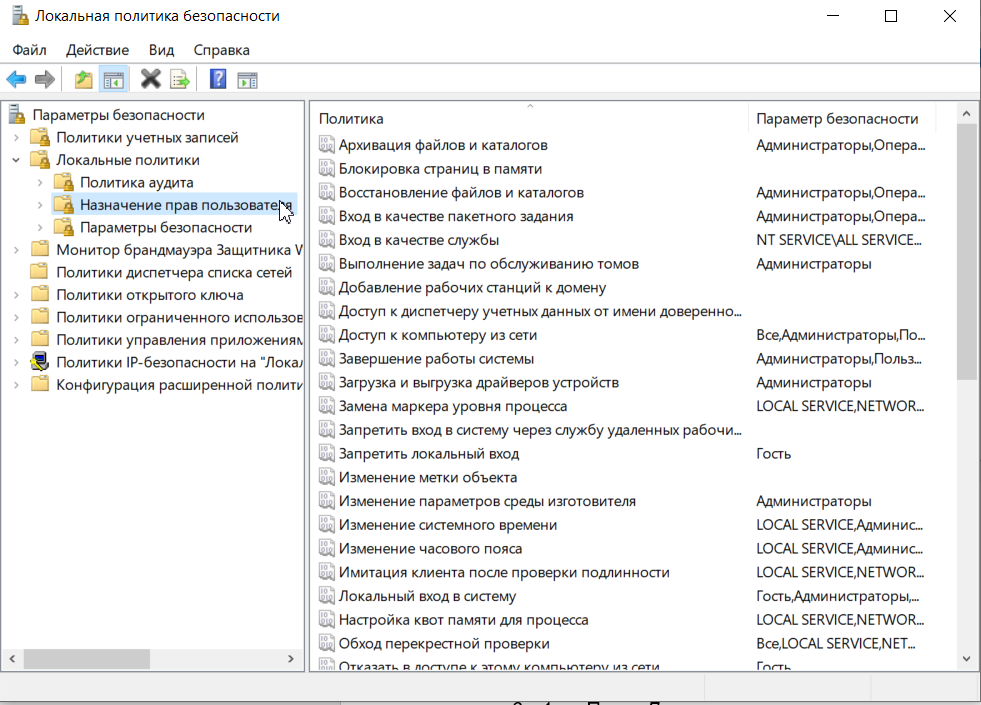
1. Приобретение необходимого объёма знаний и практических навыков в области политики безопасности

# Материал для изучения

**1)    Политика безопасности, права пользователей.**

1. Настройка политики безопасности осуществляется: *Пуск\Панель управления\Администрирование\Локальная политика безопасности\Назначение прав пользователя*





1. Основные пункты политики безопасности.

1.     Пункт *Доступ к компьютеру из сети* – определяет, какие именно пользователи и группы пользователей могут получать доступ к данному компьютеру по компьютерной сети. Если компьютер не подключен к локальной сети, рекомендуется запретить доступ пользователей извне, это позволит избежать атак взломщиков и их проникновение в систему при работе в Интернете. Для запрета доступа сетевых пользователей к компьютеру следует:

-       в окне *Политика* программы *Назначение прав пользователя* щелчком мыши выбрать политику *Доступ к компьютеру из сети*;

-       появится окно *Параметр локальной безопасности Доступ к компьютеру из сети*(рис.1.2.);

-       выделить всех пользователей (или лишних пользователей) при помощи указателя мыши и клавиши *Shift*;

-       сделать щелчок по кнопке *Удалить*;

-       нажать кнопку *ОК*.

Пользователи, которым разрешен доступ к компьютеру, должны быть отображены в данном пункте политики безопасности, иначе они не смогут войти в систему. Если пользователи в списке окна отсутствуют, то их следует добавить при помощи кнопки *Добавить пользователя или группу.* Для этого следует:

-       сделать щелчок по кнопке *Добавить пользователя или группу*;

-       в появившемся диалоговом окне сделать щелчок по кнопке *Дополнительно*;

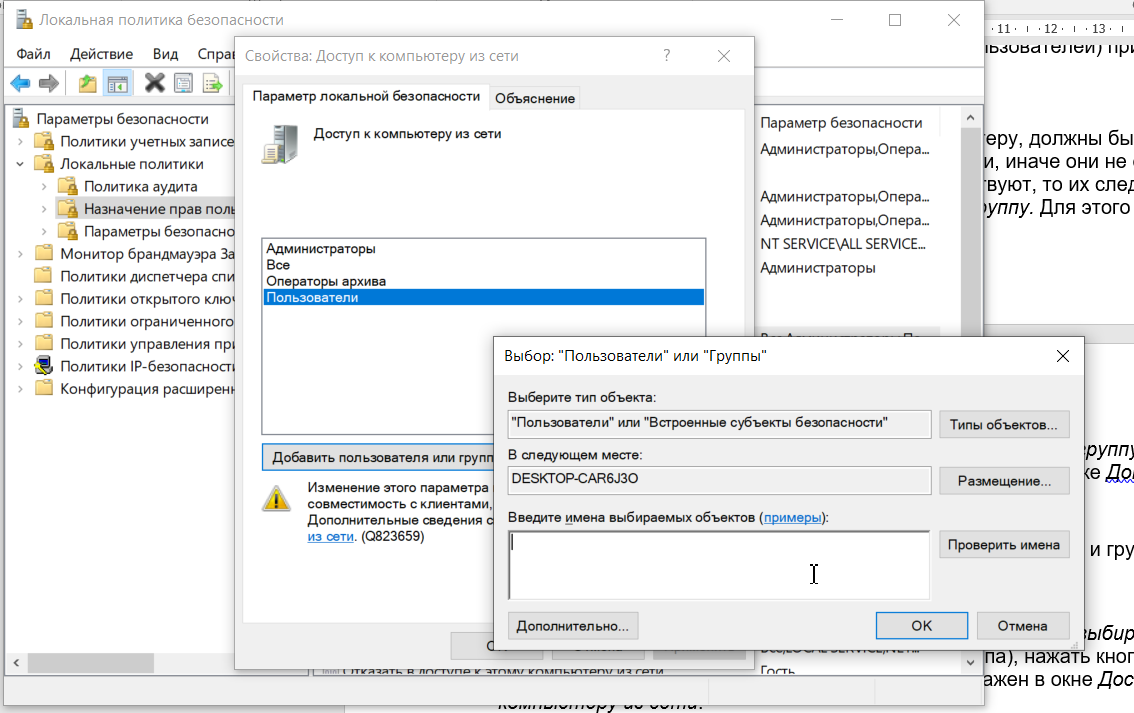
-       в окне *Пользователи* или группы нажать кнопку *Поиск*;

-       в нижней части окна появится список всех пользователей и групп;

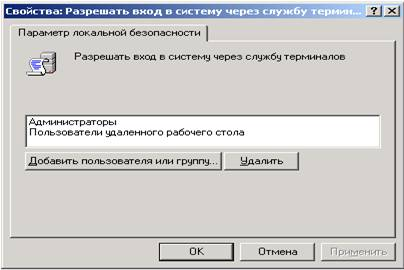
-       щелчком выбрать нужную строку нажать кнопку *ОК*;

-       в появившемся диалоговом окне в поле *Введите имена выбираемых объектов,* появится выбранный пользователь (группа), нажать кнопку *ОК*;

-       выбранный пользователь (группа) будет отображен в окне *Доступ к компьютеру из сети*.

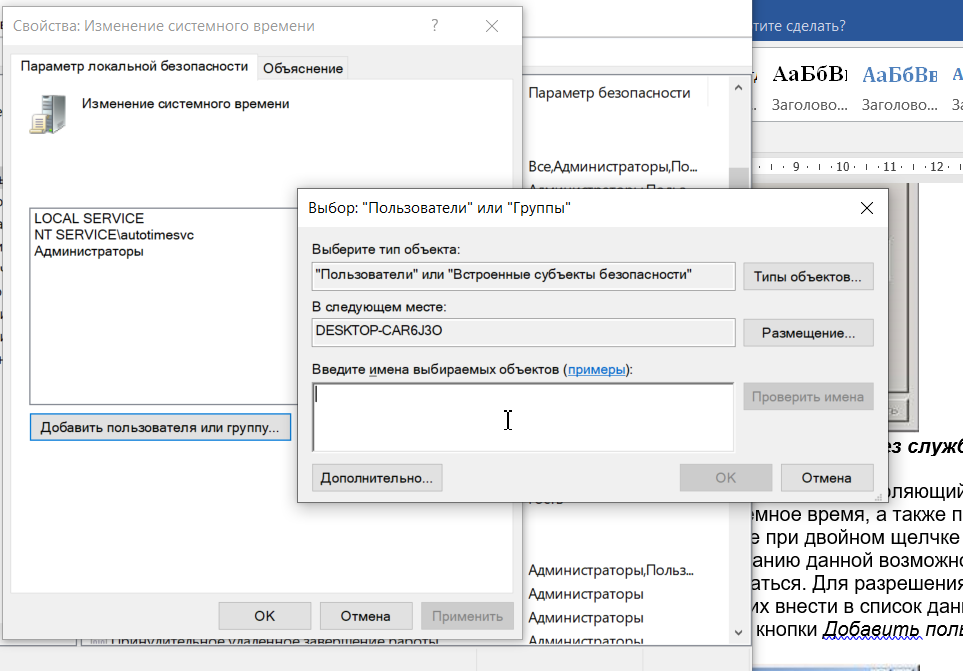


2.     Пункт *Разрешать вход в систему через службу терминалов*является аналогичным предыдущему, но вход пользователей в систему осуществляется в качестве клиентов терминал-сервера. Если данный сервис не используется, то рекомендуется аналогичным методом запретить вход в систему всех пользователей, убрав их из значения данного пункта как клиентов терминал-сервера. В случае необходимости всегда можно добавить нужных пользователей и их группы при помощи кнопки *Добавить пользователя или группу* (рис.1.4.).



**Рис. 1.4. Окно *Разрешить вход в систему через службу терминалов***

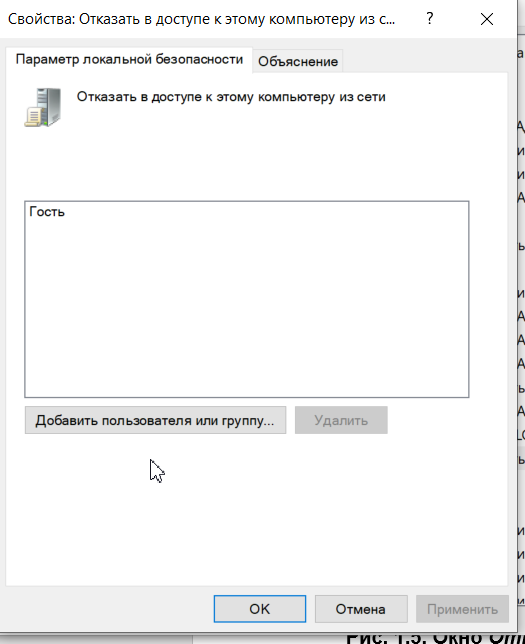
3.     Пункт *Изменение системного времени*, позволяющий пользователям, перечисленным в нем, менять системное время, а также просматривать календарь, появляющийся на экране при двойном щелчке по текущему времени на панели задач. По умолчанию данной возможностью обычные пользователи не смогут воспользоваться. Для разрешения пользователям выполнять такое действие следует их внести в список данного пункта политики безопасности при помощи кнопки *Добавить пользователя или группу* (рис.1.5.).



**Рисунок 1.5. Окно *Изменение системного времени***

4.     Пункт *Отладка программ* позволяет указать пользователей, которые смогут подсоединять свой отладчик к процессам и производить их отладку. Следует включать в этот пункт только тех пользователей, которым это действительно нужно, например, *системный администратор* и *системные программисты*. Не следует давать это право другим пользователям, так как этой возможностью могут воспользоваться [вирусы](https://pandia.ru/text/category/virus/) для заражения системы, запущенные под одной из пользовательских записей, имеющей право на отладку процессов.

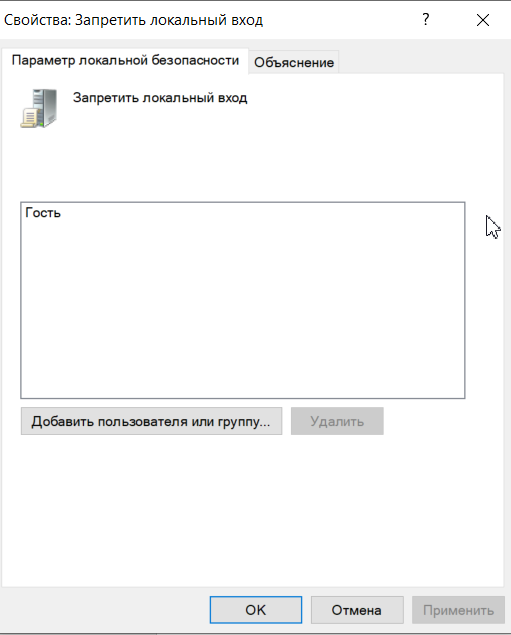
5.     Пункт *Отказ в доступе к компьютеру* *из сети* содержит пользователей и их группы, которым запрещен вход в систему по компьютерной сети. При необходимости можно добавить пользователей, которым запрещен доступ к компьютеру с помощью кнопки *Добавить пользователя или группу* (рис.1.6.).



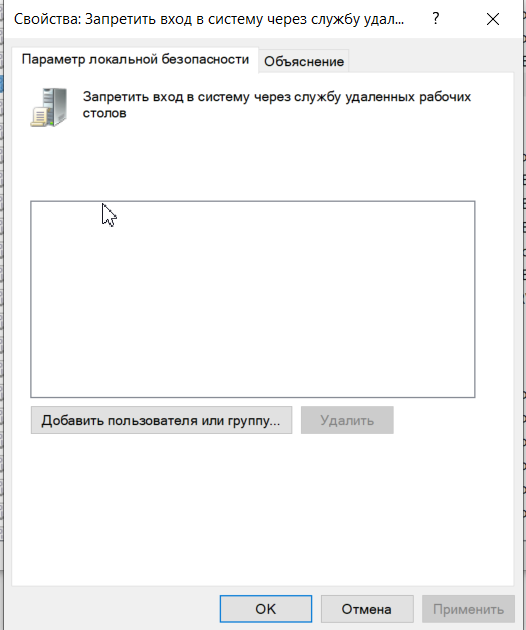
**Рис. 1.5. Окно *Отказ в доступе к компьютеру из сети***

6.     Пункт *Запретить локальный вход* содержит пользователей и их группы, которым запрещен локальный вход в систему. При необходимости можно добавить пользователей, которым запрещен доступ к компьютеру с помощью кнопки *Добавить пользователя или группу* (рис.1.7.).

7.   Пункт *Запретить вход через службу терминалов* также содержит пользователей и их группы, которым запрещен вход в систему как клиентов терминал-сервера. При необходимости можно добавить пользователей, которым запрещен доступ к компьютеру с помощью кнопки *Добавить пользователя или группу* (рис.1.8.).



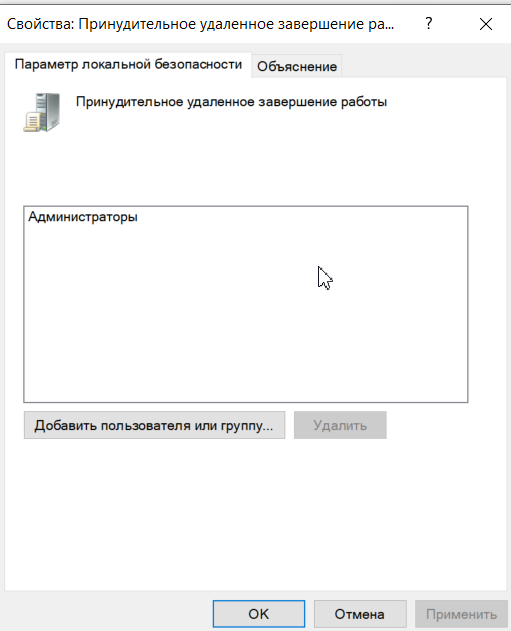
**Рис. 1.7. ОкноЗапретить *локальный вход***



**Рис. 1.8. Окно *Запретить вход в систему через службу терминалов***

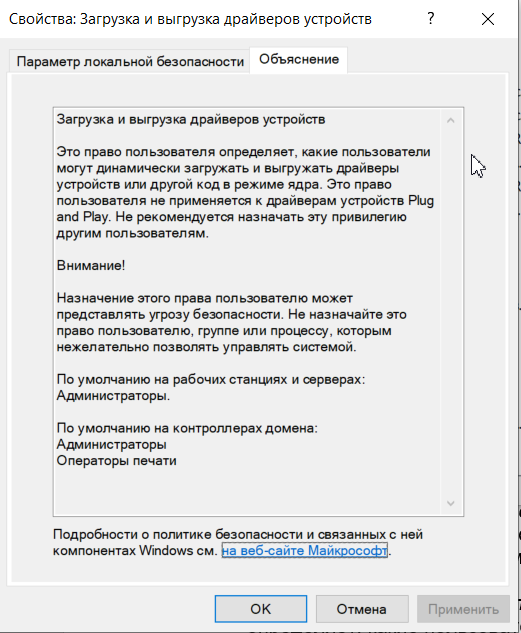
С помощью трех перечисленных выше опций локальной политики безопасности можно запретить пользователям, которые по структуре организации не должны получать доступа, вход в систему. Этим можно предотвратить внутренние [коллизии](https://pandia.ru/text/category/koll/) организации и защитить данные от их искажения или разрушения пользователями, которые удаленно пытаются ими воспользоваться.

8.     Пункт *Принудительное удаленное завершение* является очень важным в настройке локальной политики безопасности, так как если его не настроить соответствующим образом, то система может получить команду на выключение или перезагрузку от удаленно пользователя. Поэтому в данном пункте следует указывать только пользователей, которым действительно может потребоваться с машин, находящихся в локальной сети, выключить или перезапустить систему.



**Рис. 1.9. Окно *Принудительное удаленное завершение***

9.     Пункт *Загрузка и выгрузка драйверов устройств* позволяет указать, кто из пользователей может динамически устанавливать и выгружать драйвера устройств. Это право необходимо для установки драйверов устройств, имеющих спецификацию *Plug and Play*.



10. Пункт *Локальный вход в систему* является очень важным и определяет, какие пользователи и их группы могут локально входить в систему.

11. Пункт *Управление аудитом и журналом безопасности* относится к механизму аудита системы и определяет, какие пользователи и их группы могут устанавливать аудит доступа к определенным объектам, таким как файлы, ключи реестра и пр. По умолчанию в данном пункте перечислена лишь одна группа локальных системных администраторов.

12. Пункт *Изменение параметров среды оборудования* определяет пользователей, которые будут иметь право менять значения системных переменных. По умолчанию на это имеют право только пользователи, принадлежащие локальной группе администраторов.

13. Пункт *Запуск операций по обслуживанию тома* позволяет указать пользователей и их группы, которые будут иметь право выполнять задачи по поддержанию работы накопителей, такие как очистка диска или его дефрагментация. Выполнение данных задач, по умолчанию, доверяется только пользователям из группы системных администраторов.

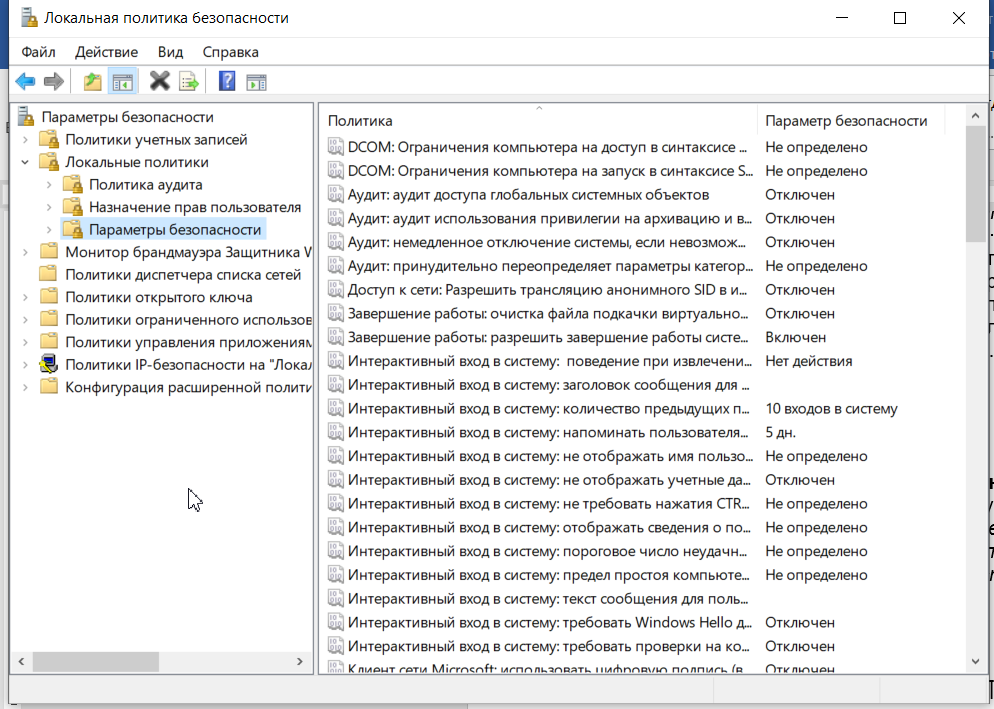
14. Пункт *Восстановление файлов и каталогов* позволяет указывать пользователей и их группы, которые могут выполнять операцию восстановления файлов и директорий из сохраненных копий, а также ставить им необходимые права доступа. По умолчанию в системе такими пользователями являются члены группы системных администраторов, а также операторы сохранения данных.

15.  Пункт *Завершение работы системы* указывает, кто из локальных пользователей, имеющих учетные записи в системе, имеет право на ее выключение или перезагрузку. По умолчанию на это имеют право все пользователи. Однако, в ряде случаев, может потребоваться запретить выполнять данные функции некоторым пользователям. Например, если нужно, чтобы компьютеры работали в то время, когда некоторые пользователи их пытаются отключить. В этом случае нужно убрать этих пользователей из данного пункта. Особенно это может быть полезно, если определенные пользователи пытаются выключить компьютер, на котором находится информация, используемая удаленно другими пользователями.

16. Пункт *Овладение файлами или иными объектами* отвечает за возможность пользователей, перечисленных в нем, брать на себя право становиться владельцами файлов и объектов. Этими объектами могут быть структуры *Active Directory*, ключи реестра, принтеры и процессы. По умолчанию на это имеют право только пользователи группы системных администраторов. Добавление к этому пункту пользователей означает предоставление им всех прав по доступу к различным объектам.

**2)    Глобальные параметры безопасности системы.**

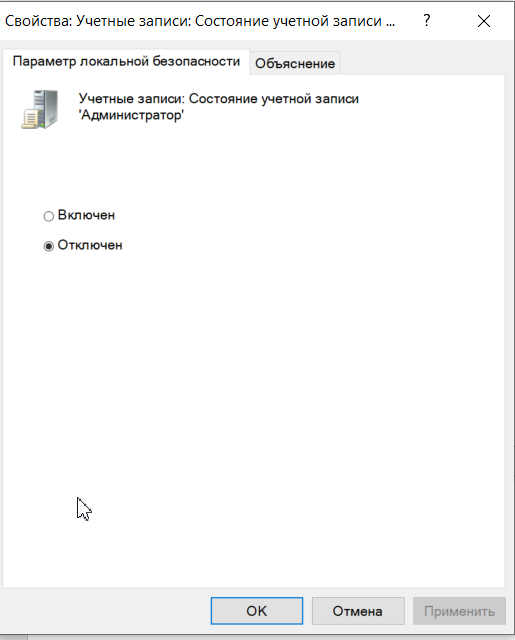
Глобальные параметры безопасности устанавливаются в разделе локальной политики безопасности *Параметры безопасности* (рис.1.10). *Пуск\Панель управления\Администрирование\Локальная политика безопасности\Параметры безопасности*



**Рис. 1.10. Окно *Параметры безопасности***

Рассмотрим наиболее важные пункты.

1.     Пункт *Учетные записи*: *Состояние учетной записи ‘Администратор’* предоставляет возможность выбора: будет ли учетная запись администратора системы включена или отключена, при нормальном функционировании системы. В случае использования системы в безопасном режиме запись администратора будет включена, независимо от значения данного пункта. Для изменения значения этого пункта следует его выбрать двойным щелчком мыши и в появившемся окне поставить флажок в соответствующем режиме (рис.1.11.)



**Рис. 1.11. Окно *Состояние учетной записи ‘Администратор’***

Отключение учетной записи системного администратора может быть полезно, т.к. это дает гарантированную защиту от атак взломщиков на эту учетную запись. Если необходимо включить учетную запись системного администратора, то это можно сделать под учетной записью другого пользователя, принадлежащего к группе системных администраторов, или в защищенном режиме работы операционной системы.

Пункт *Учетные записи: Состояние учетной записи 'Гость’* позволяет отключать учетную запись гостя, т.к. для входа под данной учетной записью не требуется пароль, что может нарушить политику прав доступа пользователями. Учетная запись *Гость* по умолчанию отключена.

**3)    Политика обновления.**

Любое программное обеспечение содержит ошибки (баги), т.к. на этапе проектирования приложений и систем невозможно все предусмотреть. Поэтому в любом приложении появляются места кода, которые работают не так, как рассчитывали разработчики, что может привести к нештатной работе [программного обеспечения](https://pandia.ru/text/category/programmnoe_obespechenie/), а также появлению новых ошибок или уязвимостей при его работе.

Для выявления ошибок все компании-разработчики стараются тестировать свое программное обеспечение, т.е. проверять работу программного обеспечения в шоковых для него условиях, когда его ограничивают в размере доступной памяти, дискового пространства, скорости работы центрального процессора и пр. На этом этапе вылавливаются ошибки и вносятся исправления в код программного обеспечения, улучшающие его стабильность (робастность) или отказоустойчивость. Однако эти меры лишь частично позволяют избавиться от наиболее явных ошибок, которые проявили себя в тестировании. В н.в. не существует аппаратных или математических методов, позволяющих избавиться от ошибок в программном обеспечении на этапе его разработки.

После долгих поисков компании-разработчики нашли простой метод, который позволяет практически со стопроцентной вероятностью избавиться от ошибок в конечных продуктах, находящихся у пользователей. Этим методом является *периодическое обновление программных продуктов*. Компании разработчики решили, что в идеале программное обеспечение должно работать двадцать четыре часа в сутки, семь дней в неделю и в его работе не должно быть никаких нештатных ситуаций, вызванных ошибками. Это можно достигнуть с помощью грамотной *политики обновления*, которая используется практически в любом современном программном продукте, т.е. система периодически выходит в Интернет и проверяет сайт компании-разработчика на появление обновлений к программному обеспечению.

Компания-разработчик для программного продукта периодически помещает на своем сайте исправления, обновления и дополнения. Исправления – это специальные заплатки для программного обеспечения, которые исправляют существующие в нем ошибки, замеченные пользователями или специалистами компании. Обновления включают различные обновления программного продукта и заплатки от обнаруженных в нем ошибок. Дополнения добавляют программному продукту определенную функциональность.

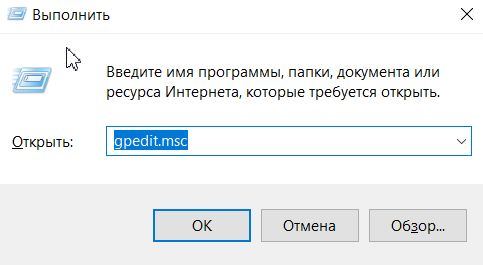
Обновления для пользователей  позволяют не только избежать ошибок ОС, проявляющихся при ее использовании, но и практически гарантированно защитить ее от взломщиков и вирусов, т.к. исправляются все замеченные ошибки в [системе безопасности](https://pandia.ru/text/category/sistemi_bezopasnosti/). Алгоритм работы системы обновления  настроен на периодическую проверку сайта компании *Microsoft* на наличие различных обновлений и скачивание или предупреждение пользователя, в зависимости от его настроек.

 Параметры центра обновления Windows 10 полностью перенесены из классической панели управления в Параметры системы. Начиная с ранних сборок Insisder Preview в параметрах центра обновления Windows 10 отсутствует возможность настройки способа получения обновлений, как и возможность отключения обновлений Windows.

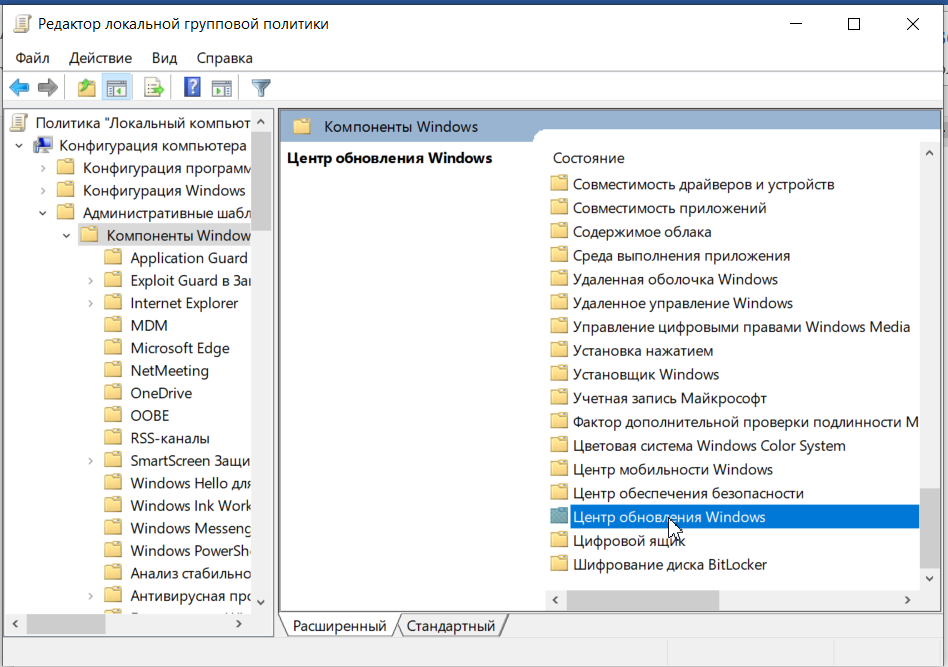
Как и в предыдущих версиях Windows вы можете управлять параметрами центра обновлений используя групповые политики, которые также регулируются путем правки параметров реестра.

## Использование редактора групповой политики

1. Откройте редактор групповой политики ( Win + R – gpedit.msc)



1. Перейдите в раздел **Конфигурация компьютера** – **Административные шаблоны** – **Компоненты Windows** – **Центр обновления Windows**



1. В правой части редактора откройте двойным щелчком параметр **Настройка автоматического обновления**

Установите состояние параметра в положение **Включено**. В блоке Параметры выберите подходящий вам вариант проверки, загрузки и установки обновлений.  
В правой части окна настройки параметра содержится подробная справка по каждому варианту настройки.

Предпочитаемым вариантом является №2 – Уведомление о загрузке и установке. В этом случае будет производиться поиск доступных обновлений, но решение о загрузке и установке обновлений принимает пользователь.

Для того, чтобы изменения вступили в силу выполните проверку обновлений в Параметрах системы:

Нажмите кнопку **Пуск**, выберите **Параметры**, перейдите в раздел **Обновление и безопасность** и нажмите кнопку **Проверка наличия обновлений**.

После применения изменений способ получения обновлений будет изменен в параметрах системы, а его настройка будет возможна только путем настройки политики.

**2.     Практическая часть.**

**1)    Вопросы по разделу:**

1.     Определите назначение *политики безопасности* системы.

2.     Где производится настройка *политики безопасности* системы?

3.     Как запретить доступ сетевых пользователей к компьютеру?

4.     Как разрешить доступ сетевым пользователям, которым разрешено работать в системе к компьютеру?

5.     Определите назначения пункта политики безопасности *Разрешать вход в систему через службу терминалов*.

6.     Как предоставить определенной группе пользователей вносить изменения в системное время?

7.     Определите назначение пункта политики безопасности *Отладка программ*.

8.     Каким образом запретить вход определенной группе пользователей в систему по локальной сети?

9.     Определите назначение пункта политики безопасности *Принудительное удаленное завершение*.

10.                        Как установить пользователей и их группы, которые могут локально входить в систему?

11.                        Как запретить определенной группе пользователей завершать работу системы, и в каких случаях это актуально?

12.                        В каком разделе производится настройка глобальных параметров безопасности?

13.                        Определите назначение *политики обновления*.

14.                        Как произвести настройку *политики обновления*?

**2)    Задание.**

1.     Произвести настройку *Политики безопасности*на своем ПК.

2.     Произвести настройку *Параметров безопасности* на своем ПК.

3.     Произвести настройку *Политики обновления* на своем ПК.

**3)    Порядок отчетности и форма контроля выполнения работы.**

Контроль выполнения задания производится по окончании занятия и на консультациях в форме защиты выполненной работы, предоставленной в электронном виде в форме «Отчет по [лабораторной работе](https://pandia.ru/text/category/laboratornie_raboti/) …».