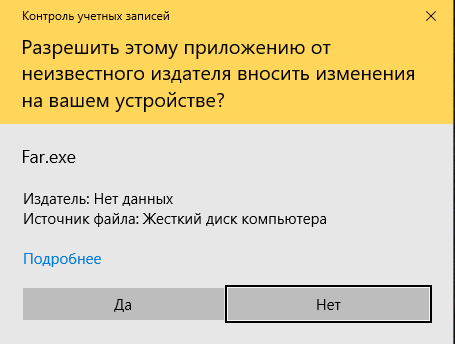
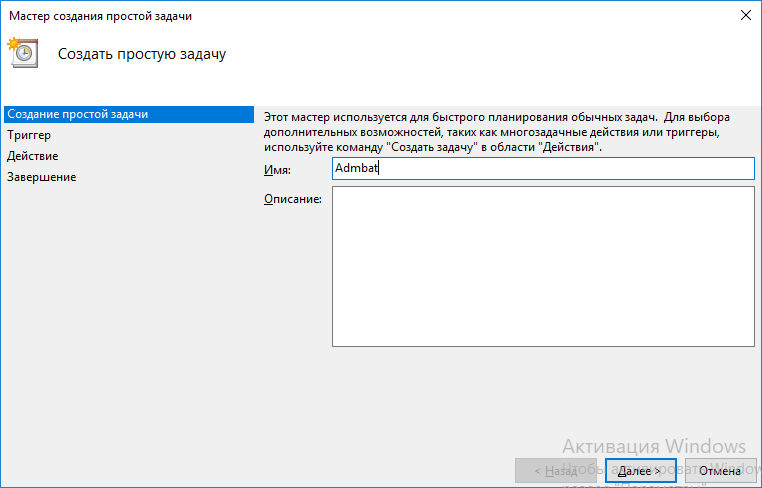
Выполнение приложений от имени Администратора без запроса UAC

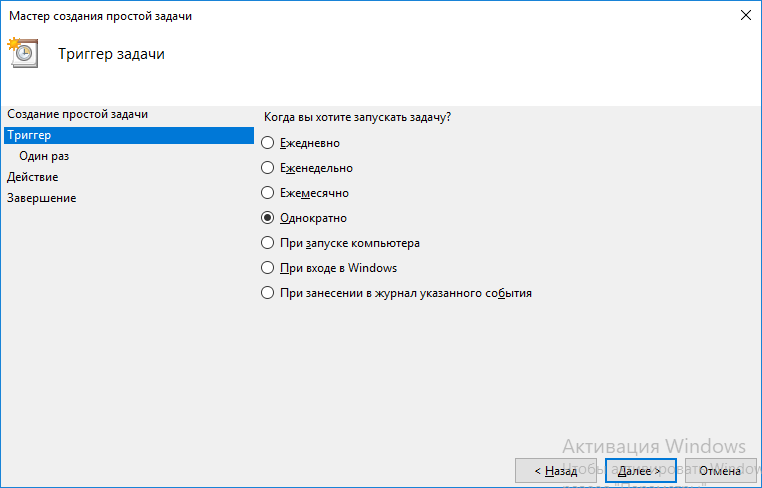
Существует множество приложений Windows, для работы которых требуются права администратора. В современных ОС для этого обычно используется режим ”Запуск от имени администратора” контекстного меню проводника. При этом выводится запрос средства контроля учетных записей пользователя UAC (User Account Control ), требующего подтверждения разрешения на запуск приложения: 



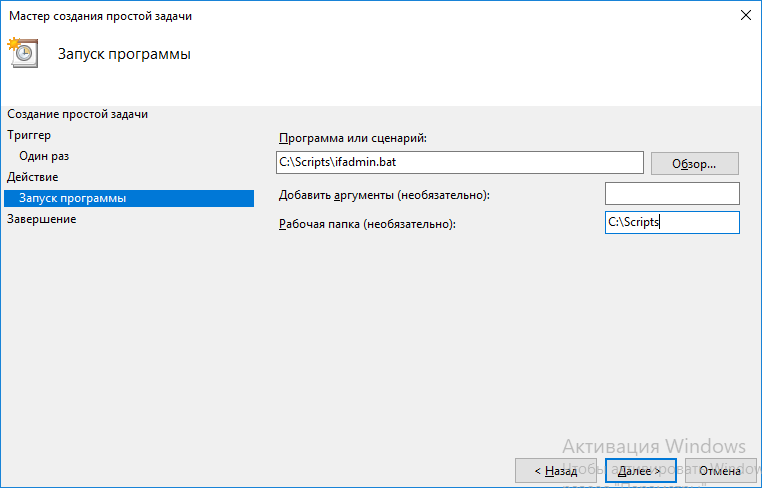
Если пользователь нажимает кнопку ”Да”, приложение выполняется с повышением привилегий в контексте учетной записи администратора. Если же пользователь нажмет ”Нет” – приложение выполнится в контексте пользовательской учетной записи. Такой же результат будет получен, если пользователь вообще не ответит на запрос UAC – по истечении времени ожидания ответа, приложение будет запущено в контексте учетной записи пользователя. Это делает проблематичным выполнение командных файлов с повышением привилегий в автоматическом режиме, поскольку требуется вмешательство пользователя. Для решения данной проблемы большинство пользователей Windows, как правило, отключают систему контроля учетных записей UAC, что нежелательно, поскольку это снижает уровень безопасности ОС. Так, например, при выключенном UAC, пользователь даже не заметит как вирус-шифровальщик удалит теневые копии томов и приступит к шифрованию файлов. В результате будут гарантировано потеряны данные без какой-либо возможности их восстановления. При включенном же UAC, попытка удаления теневых копий с помощью стандартной утилиты **vssadmin.exe** приведет к отображению на экране запроса UAC, который, как минимум, привлечет внимание пользователя и позволит отреагировать на угрозу. Подробнее о вероятности восстановления данных после вируса-шифровальщика в отдельной [статье](https://ab57.ru/recoverysh.html).  
  
Таким образом, возникает задача выполнения программ или командных файлов от имени администратора при включенном UAC, но без запроса на разрешение их запуска. Одним из способов решения подобной задачи является использование специально подготовленной задачи стандартного Планировщика заданий Windows. Необходимо создать задачу для запуска командного файлат с повышенными привилегиями. Переходим в ”Панель управления” - ”Администрирование” - ”Планировщик заданий” - ”Библиотека планировщика заданий”, выбираем в меню ”Действия” – ”Создать простую задачу”. С помощью мастера создания простой задачи, создаем задачу, например, с именем **Admbat** 



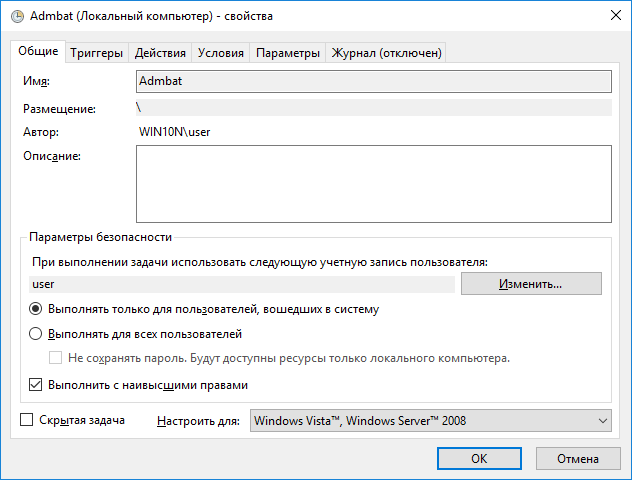
В качестве триггера запуска можно выбрать режим ”Однократно” и установить дату начала выполнения задачи уже прошедшим днем, чтобы служба планировщика не могла выполнить ее запуск в ненужное нам время. 



В качестве действия выбираем ”Запустить программу” 



В качестве программы будет запускаться командный файл, например C:\Scripts\ifadmin.bat. При необходимости можно задать рабочую папку программы.  
  
Ставим галочку на ”Открыть окно ”Свойства” для этой задачи после нажатия кнопки ”Готово” ”. В свойствах задачи включаем режим ”Выполнить с наивысшими правами”. 



Если выбрать режим ”Выполнять для все пользователей”, то задача не будет открывать никаких окон в сеансе текущего пользователя, что не очень удобно в режиме тестирования командного файла. В качестве теста можно использовать команду:  
  
**netstat –b** - отобразить список соединений с именами создавших их программ. Параметр **b**требует административных привилегий. Содержимое командного файла:  
  
**Rem Выполняем команду в контексте учетной записи пользователя  
netstat –b   
rem Пауза для просмотра результатов  
pause   
Rem Готовим содержимое командного файла Ifadmin.bat задачи планировщика Admbat  
echo netstat –b > C:\Scripts\ifadmin.bat  
echo pause >> C:\Scripts\ifadmin.bat  
Rem Выполним задачу планировщика с именем Admbat schtasks /run /tn Admbat**Таким образом, сначала будет выполнена команда **netstat –b** в контексте учетной записи пользователя, с выдачей сообщения  
  
**Запрошенная операция требует повышения.**а затем, с помощью задачи Admbat планировщика заданий – с повышенными привилегиями, т.е. под учетной записью с правами администратора – на экран будет выведен список соединений с именами программ. 

При необходимости выполнения конкретного командного файла в контексте учетной записи администратора, можно просто скопировать его содержимое в C:\Scripts\ifadmin.bat :  
  
**copy C:\MyScripts\admin1.bat C:\Scripts\ifadmin.bat**  
  
И выполнить задачу планировщика **Admbat** командой:  
  
**schtasks /run /tn Admbat**  
  
Задача планировщика будет использоваться одна и та же - **Admbat**, но содержимое командного файла **ifadmin.bat** можно менять под свои потребности.   
  
Задачу планировщика можно создать и из командной строки с помощью утилиты **schtasks.exe** и разрешить ее выполнение с правами администратора, задав параметр **/RL HIGHEST**  
  
**schtasks /create /TN "Admbat" /TR "C:\Scripts\ifadmin.bat" /SC ONCE /SD 11/12/2018 /ST 14:00 /RL HIGHEST**.  
  
Естественно, данная команда должна выполняться в контексте учетной записи с правами администратора.  
  
В заключение добавлю, что нелишней будет проверка в наличия администраторских прав в самом командном файле **ifadmin.bat**. Это легко реализуется с помощью команды:  
  
**WHOAMI /PRIV** - отобразить действующие привилегии текущего пользователя.  
  
Так, например, удаленное выключение компьютера доступно только в контексте учетной записи администратора. В этом случае, в результатах вывода WHOAMI присутствует строка "SeRemoteShutdownPrivilege". С помощью команды **find** ищем эту строку в результатах вывода команды **whoami /priv** и если она найдена (переменная ERRORLEVEL равна нулю) – командный файл выполняется с правами администратора. Например:  
  
**@echo OFF  
WHOAMI /PRIV | find /i "SeRemoteShutdownPrivilege" > nul  
if %ERRORLEVEL% == 0 goto admin  
color 8F  
echo Нет прав администратора.   
pause  
exit  
:admin  
color f0  
ECHO Есть права администратора.   
pause**  
  
Можно создать командный файл, проверяющий наличие прав администратора, и при их отсутствии, выполняющий свой перезапуск с использованием повышения привилегий за счет задачи планировщика **Admbat**.  
  
Алгоритм следующий:  
  
- выполняется проверка наличия прав администратора, так же как это происходило в предыдущем примере, и, при их отсутствии, содержимое командного файла копируется в файл, запускаемый планировщиком заданий (**ifadmin.bat**).  
  
- выполняется задача планировщика **Admbat** для запуска файла **ifadmin.bat** с правами администратора без запроса UAC.   
  
- завершается текущий командный файл (но вместо него выполняется он же, скопированный в (**ifadmin.bat**), но с правами администратора).  
  
Содержимое командного файла:   
  
**@echo OFF  
  
WHOAMI /PRIV | find /i "SeRemoteShutdownPrivilege" > nul  
  
if %ERRORLEVEL% == 0 goto admin  
  
copy /Y %~f0 C:\Scripts\ifadmin.bat  
  
schtasks /run /TN Admbat  
  
exit  
  
:admin  
  
start "notepad with admin rights" %SystemRoot%\notepad.exe C:\Scripts\ifadmin.bat  
  
exit**Несколько пояснений. Данный командный файл вначале проверяет наличие прав администратора, и если они есть – выполняется переход на метку **:admin**- запускается блокнот, открывающий файл **C:\Scripts\ifadmin.bat**. После чего работа командного файла завершается по команде **exit**. Если права администратора отсутствуют, выполняется копирование текущего командного файла, имя и путь которого принимает переменная **%~f0**, в файл **C:\Scripts\ifadmin.bat**. Для подавления запроса на перезапись существующего файла команда **copy** используется с ключом **/Y**. После копирования, выполняется запуск задачи планировщика, обеспечивающей повторный запуск этого же командного файла (скопированного в файл **C:\Scripts\ifadmin.bat**, но уже с правами администратора системы.