

## Рекомендации по настройке окружения и сети техническими специалистами для проведения квалификационного экзамена и конкурса.

При проведении квалификационного экзамена или конкурса на замещение вакантной должности нотариуса, необходимо придерживаться следующих рекомендаций, при настройке и подготовке сети, и системы:

*Все действия по настройке системы необходимо производить из-под учетной записи администратора, и непосредственно для проведения экзамена или конкурса предоставлять пользователю гостевую учетную запись.*

### Настройки окружения:

---

1. Рекомендованная версия операционной системы: **Windows 7** или выше.
2. Офисный пакет приложений **Microsoft office 2010** или выше.
3. Браузер **Google Chrome** версии **70.0** или **Mozilla Firefox** версии **51.0** или выше.
4. Во всех браузерах обязательно должна быть включена функция хранения **Cookies**.
5. Включен запрет на запуск программного обеспечения, для этого необходимо сделать следующее:
  - Запустить оснастку "Локальная политика безопасности" (открыть меню Пуск – выбрать поиск Windows - написать - **secpol.msc**).
  - Выбрать в навигации: "Политики ограниченного использования программ" - "Дополнительные правила"
  - В правой части оснастки правой кнопкой мыши вызвать контекстное меню и в нем выбрать действие "Создать правило для пути" (рис. 1):

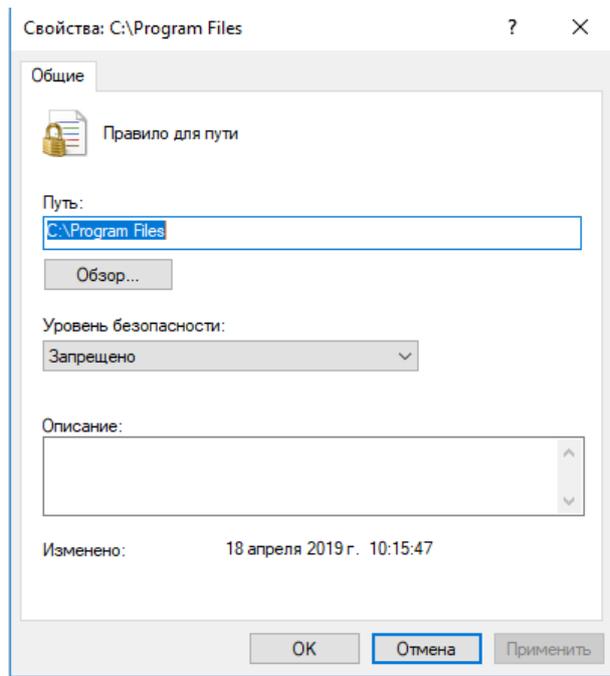


Рисунок 1

- Создать следующие запрещающие правила для (рис. 2):
- C:\Program Files
- C:\Program Files (x86)
- %windir%\system32\notepad.exe
- %systemroot%\system32\xpsrchvw.exe
- %windir%\system32\mspaint.exe

Имя	Тип	Уровень безопасности
%windir%\system32\notepad.exe	Путь	Запрещено
C:\Program Files	Путь	Запрещено
C:\Program Files (x86)	Путь	Запрещено
%systemroot%\system32\xpsrchvw.exe	Путь	Запрещено
%windir%\system32\mspaint.exe	Путь	Запрещено

Рисунок 2

В данном случае браузером по умолчанию, с которым у пользователя останется возможность работать, будет **Edge/Explorer**, для того чтобы пользователь смог запустить иной браузер (**Google Chrome / Mozilla Firefox**) необходимо создать разрешающее правило для этого браузера по аналогии с запрещающим правилом, только выбрав тип «**Неограниченный**» (рис. 3):

C:\Program Files (x86)\Google\Chrome\Application\chrome.exe	Путь	Неограниченный
---	------	----------------

Рисунок 3

# Настройки сети:

1. При настройке сети необходимо в обязательном порядке проверить подключение (корректный обмен пакетами) со следующими адресами:
  - <https://test-contest.eisnot.ru/>
  - <https://contest.eisnot.ru/>
  - <https://test-cvalexam.eisnot.ru/>
  - <https://cvalexam.eisnot.ru/>
2. Для ограничения доступа к сети необходимо сделать 2 основных действия:
  - Ограничить доступ ко всем адресам в сети интернет с помощью изменения параметров DNS.
  - Прописать доступ к определенным сайтам в файле hosts.

Для того чтобы изменить параметры DNS необходимо проделать следующие действия:

- Открыть на компьютере свойства интернет подключения.
- Выбрать в списке компонентов, которые им используются, протокол IP версии 4 и еще раз кликнуть на кнопку «Свойства» (рис. 4).

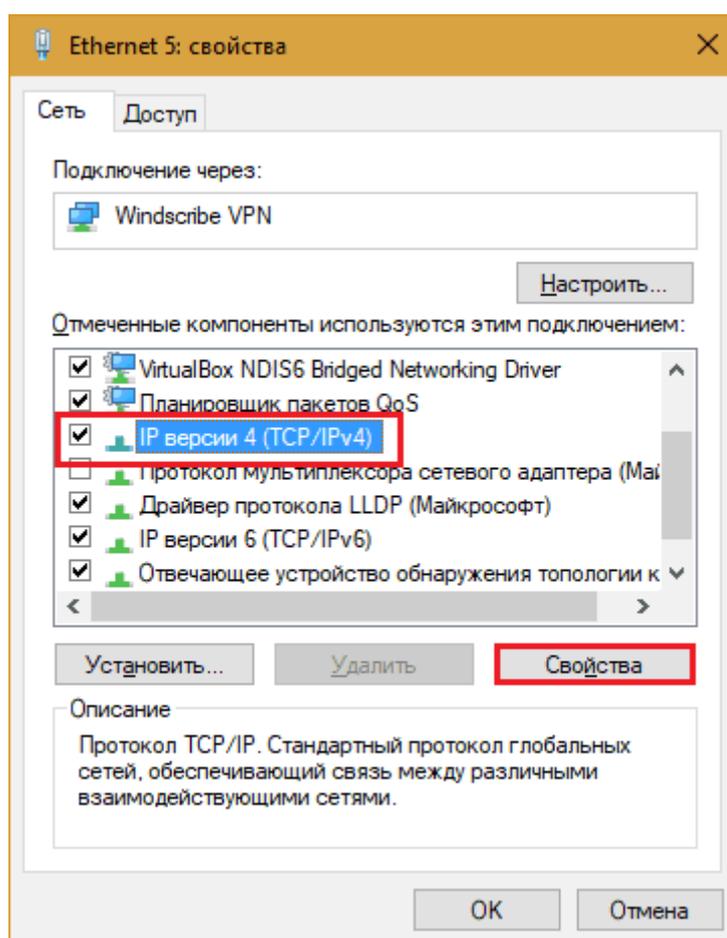


Рисунок 4

- В свойствах протокола поставить метку «**Использовать следующие адреса ДНС**» и вписать в поля цифры 127.0.0.1 (рис. 5).

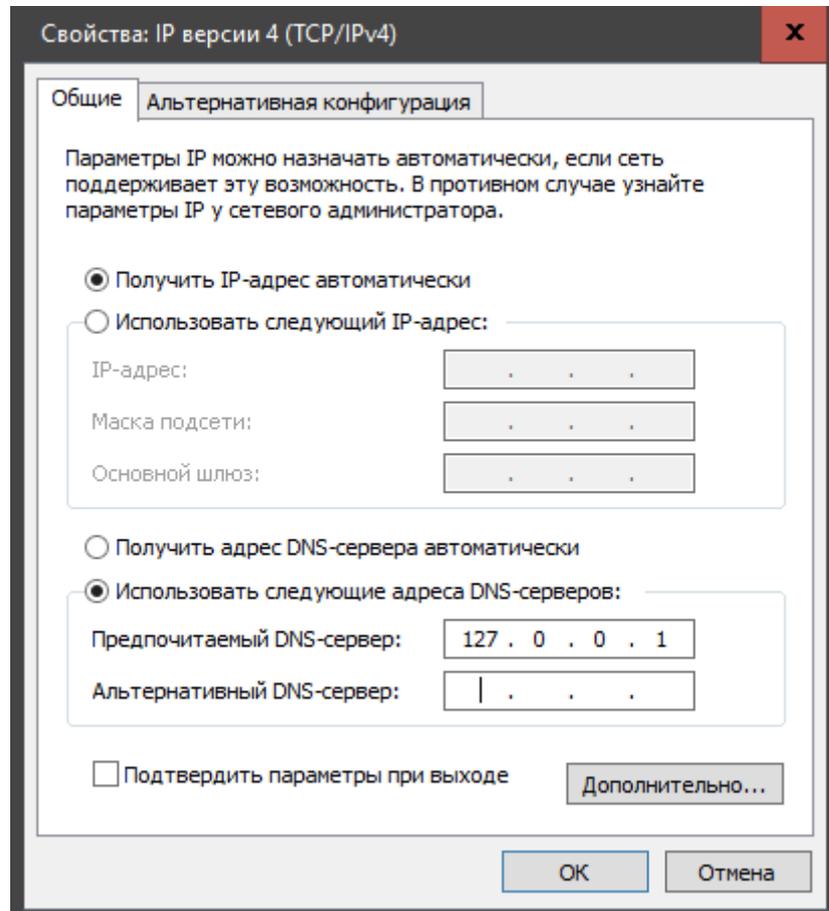


Рисунок 5

Для того чтобы прописать доступ к сайтам конкурса и квалификационного экзамена в файле hosts, необходимо сделать следующие действия:

- Открыть файл hosts по адресу **C:\Windows\System32\drivers\etc** с помощью блокнота.
- Скопировать в конец файла следующий текст:

```
193.35.100.35 test-contest.eisnot.ru
193.35.100.35 contest.eisnot.ru
193.35.100.35 test-cvalexam.eisnot.ru
193.35.100.35 cvalexam.eisnot.ru
```

# Настройки внешних носителей:

1. Для ограничения использования съемных носителей необходимо использовать групповые политики для отдельной учетной записи, для этого необходимо:

- Запустить оснастку MMC (открыть меню Пуск – выбрать поиск Windows - написать - **mmc.exe**).
- В меню «**Файл**» консоли выбрать пункт «**Добавить или удалить оснастку**» (рис. 6).

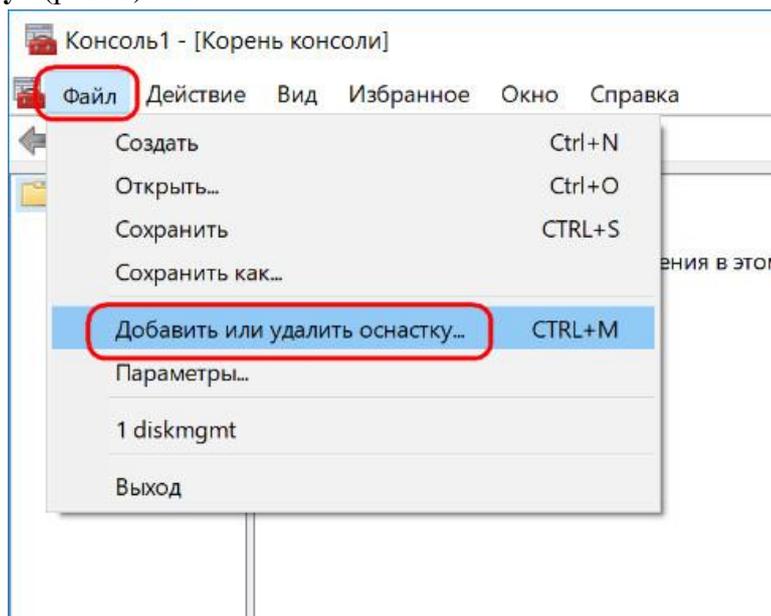


Рисунок 6

- В колонке слева выбираем «**Редактор объектов групповой политики**», и нажимаем кнопку «**Добавить**» (рис.7).

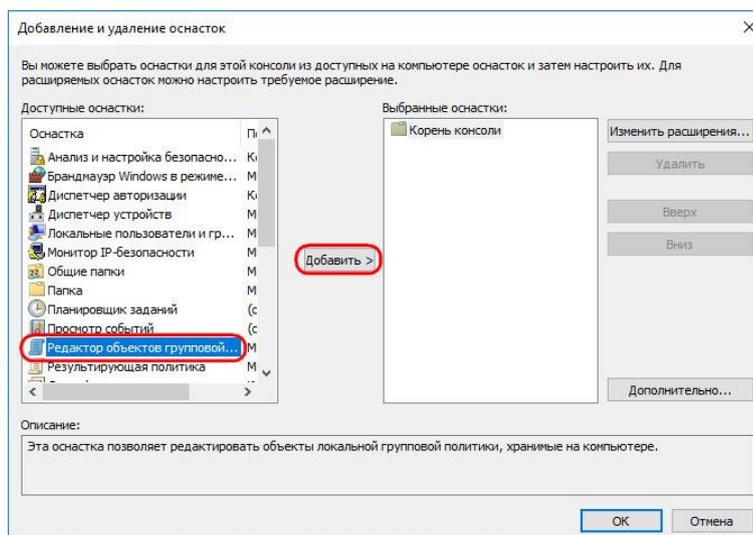


Рисунок 7



2. В целях исключения возможности внесения изменений в параметры локальной политики безопасности необходимо ограничить доступ пользователя к оснастке mmc, для этого необходимо:

- В сохраненной ранее оснастке выбрать пункт «**Консоль управления MMC**» (рис. 10)

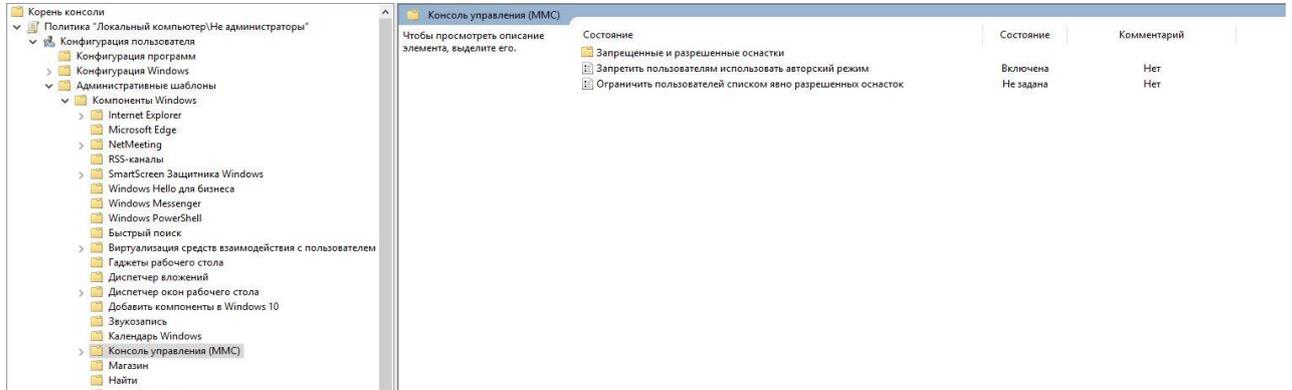


Рисунок 10

- Задать параметру «**Запретить пользователям использовать авторский режим**» состояние «**Включен**».