Кабинет информатики в домене МЭШ

Описание

Данное решение - один большой компромисс между удобством (для учащихся, учителя, админа) и безопасностью в условиях искусственных ограничений домена МЭШ, но при этом оно наиболее функциональное и наименее трудозатратное в реализации и повседневной поддержке по сравнению с альтернативными вариантами:

- **Локальные УЗ на компьютере без домена.** Такой вариант можно рассматривать, только если это ровно 1 ПК. Одна. Штука.
- **Локальные УЗ на ПК в домене.** Такой вариант можно рассматривать, только если это 1 кабинет и не более 10 ПК, и у админа очень много свободного времени на внесение каждого изменения в настройки УЗ на каждом ПК.
- **Отдельные доменные УЗ для каждого учащегося.** Это правильно, грамотно, безопасно, но тяжело реализуемо в реалиях МЭШ. Ну и еще это ад для админа с вечно забытыми логинами и паролями.
- **Доменные УЗ для каждого ПК с ручным/автоматическим входом.** Такой подход просто добавляет для админа в 5 раз больше работы по настройке, ничего не давая взамен, кроме мнимой безопасности.
- **Доменные УЗ для групп из 5 ПК с автоматическим входом.** Наш вариант.

Особенности

1. Автовход в Windows и подключение к Wi-Fi сети Study без ручного ввода учетной записи или подтверждения сертификатов. А подключение к сетям Open, Study.MOS запрещено политикой.
2. Ограничения для пользователя-школьника на изменение параметров системы, в.ч. установки мемасиков на фон рабочего стола. Ограничений на установку ПО в профиль на данный момент нет.
3. Полный контроль для системного администратора.
4. Удобство для учителя.

Зачем всё это админу

1. Единообразие конфигурации.
2. Управление через Veyon или RDP.
3. Установка/удаление ПО через KSC или GLPI или GPO.
4. Управление конфигурацией пользователей и компьютеров через GPO.
5. Контент-фильтрация через KSC.

Подробности

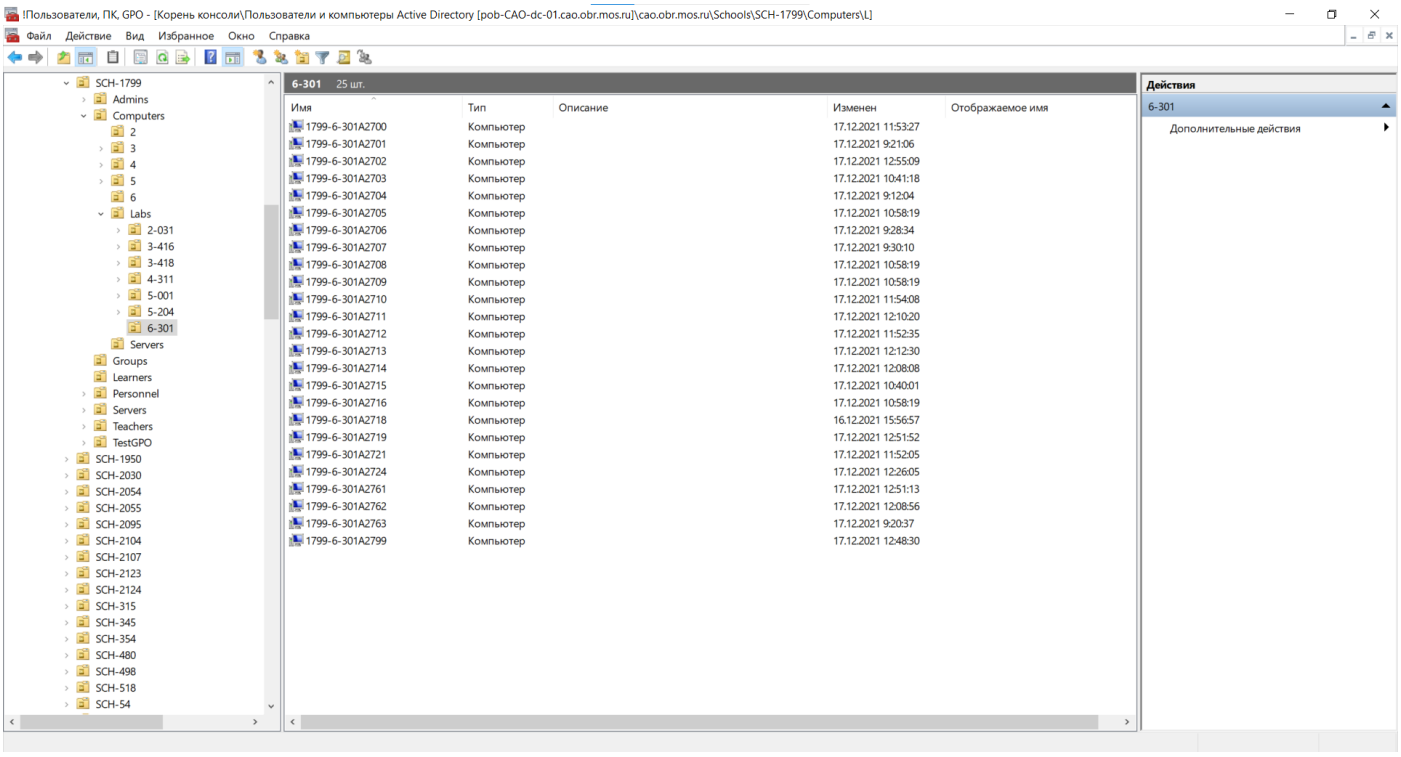
Чтобы лучше понимать, о чем здесь идет речь, можно самостоятельно изучить упоминаемые объекты. Для этого на компьютере в домене МЭШ нужно запустить оснастки “Пользователи и компьютеры Active Directory”, “Управление групповой политикой” и переключиться на домен CAO.

Если нет доступа к домену, или не установлены оснастки, то можно **скачать и открыть в браузере** отчеты объектов групповых политик:

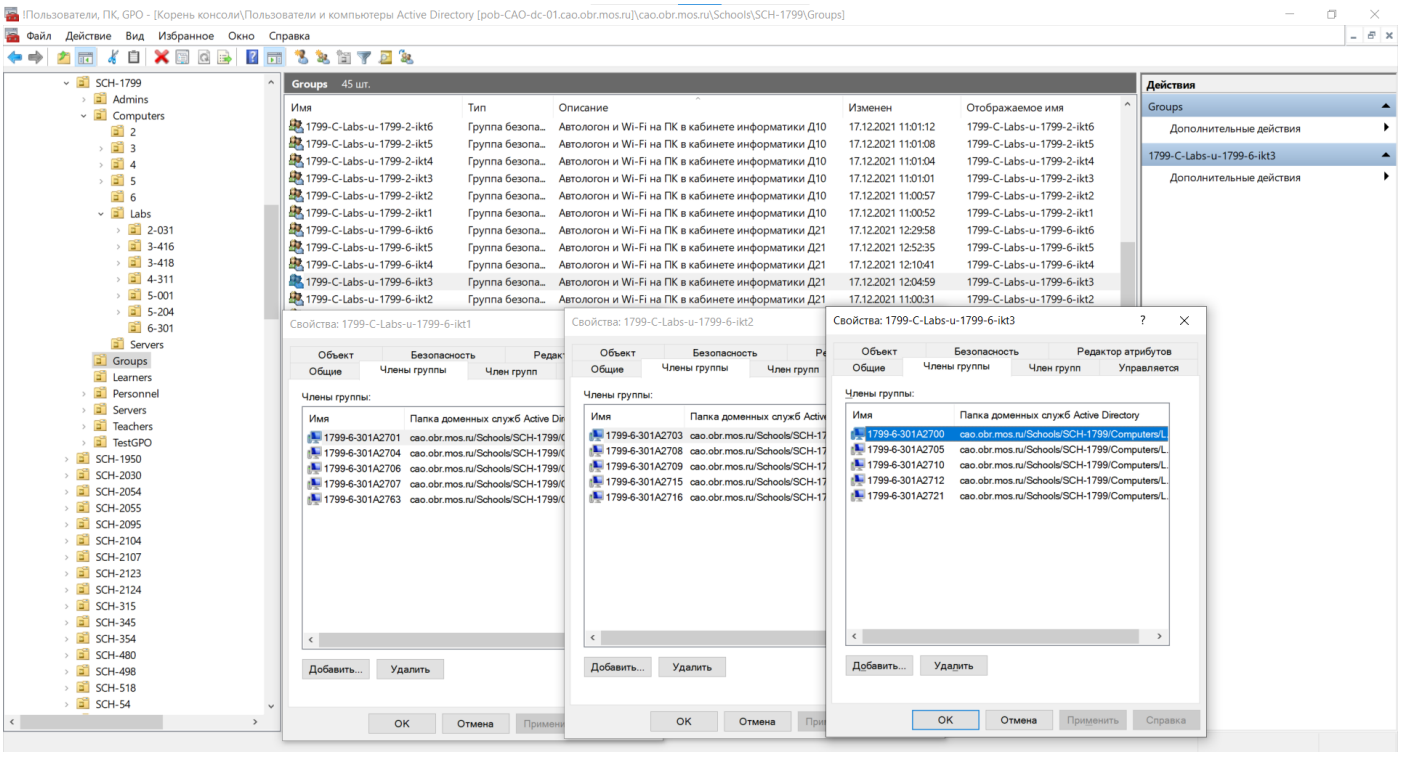
- **SCH-1799-Computers-Labs 20.12.2021.htm**
- **SCH-1799-Users-Labs 20.12.2021.htm**

1. Подключение ПК к сети - кабель и Wi-Fi Study.
2. ОС из **подготовленного образа** с набором ПО установлена по сети с помощью WDS и MDT.
3. ПК введены в **домен МЭШ**, объекты компьютеров размещены в подразделениях AD по кабинетам.
4. ПК добавлены в **группы** AD по 5 штук в каждую. Группы называются по имени учетной записи, которая используется для автологона на ПК в группе (например, **1799-C-Labs-u-1799-6-ikt1**). Каждый ПК должен состоять только в одной такой группе для автологона!
5. К подразделению **SCH-1799/Computers/Labs** применена групповая политика **SCH-1799-Computers-Labs**.
6. В политике **SCH-1799-Computers-Labs**:
   a. Переопределена сеть Study (чтобы работал автологон) и запрещены сети Open, Study.MOS.
   b. Настроен автологон с отдельными доменными обезличенными УЗ с нацеливанием по группам (1 УЗ н группу из 5 ПК для беспроблемного подключения к Study).
   c. Отключен запрос пароля при выходе системы из спящего режима / при включении монитора.
   d. Настроены другие параметры, применимые к ПК только в кабинетах информатики.
7. Полнофункциональные обезличенные УЗ, созданные специально для кабинетов информатики, добавлены в группу **1799-Users-Labs**.
8. К подразделению **SCH-1799/Teachers** применена политика **SCH-1799-Users-Labs**, ограниченная фильтром безопасности по группе обезличенных УЗ **1799-Users-Labs** (т.е. политика действует только на членов группы).
9. В политике **SCH-1799-Users-Labs** заданы параметры, ограничения и запреты для пользователей.
10. Т.к. обезличенные УЗ для полноценной работы сетевого подключения находятся в группе **1799-Teachers**, то имеют те же права на доступ к сетевым дискам **Share** и **Data**, что и сотрудники/учителя, а это плохо. Ввиду ограниченных возможностей самостоятельного администрирования инфраструктуры МЭШ, самое простое решение - не использовать для хранения файлов сотрудников/учителей корни дисков Share и Data, а создать в них вложенные папки и размещать данные уже в них, при этом запретить доступ к папке для группы **1799-Users-Labs** стандартными средствами ACL Windows.

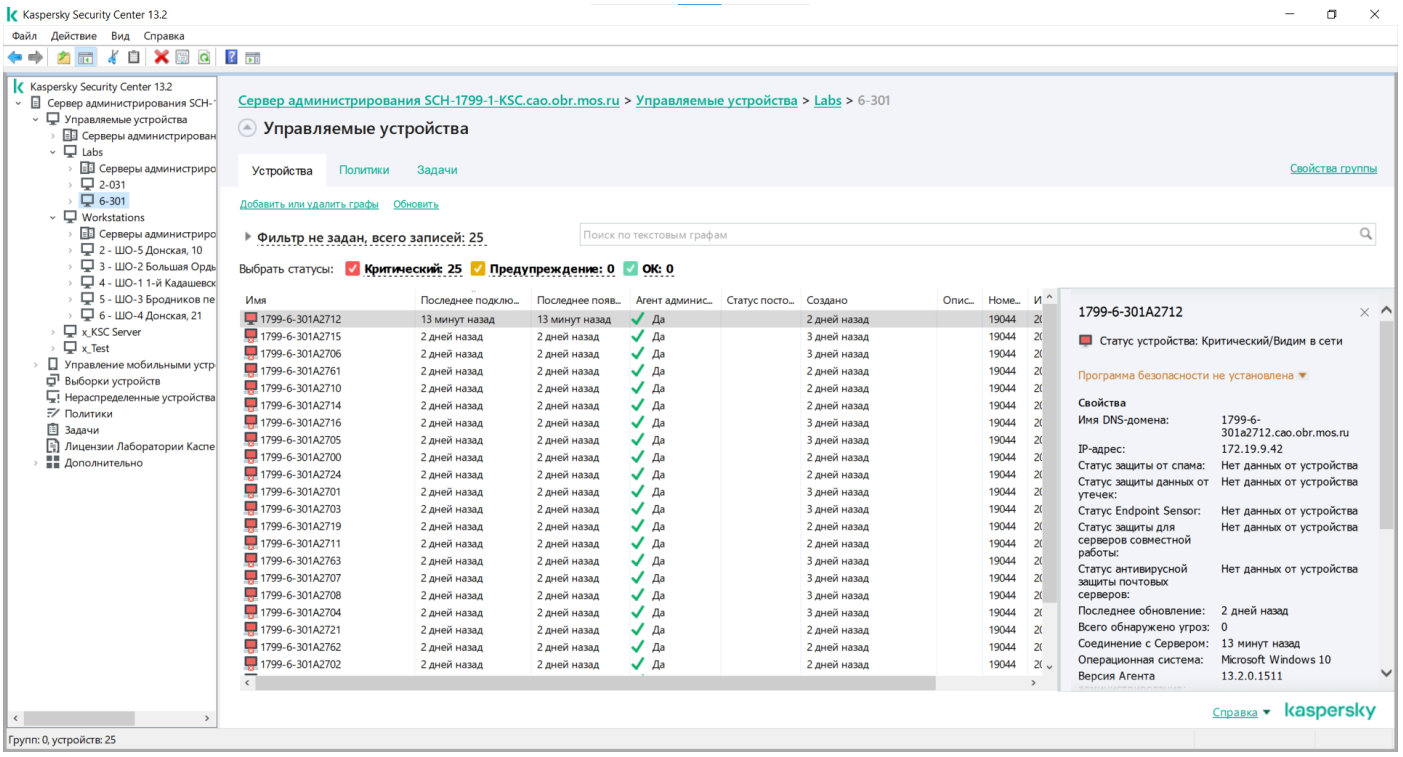
Картинки



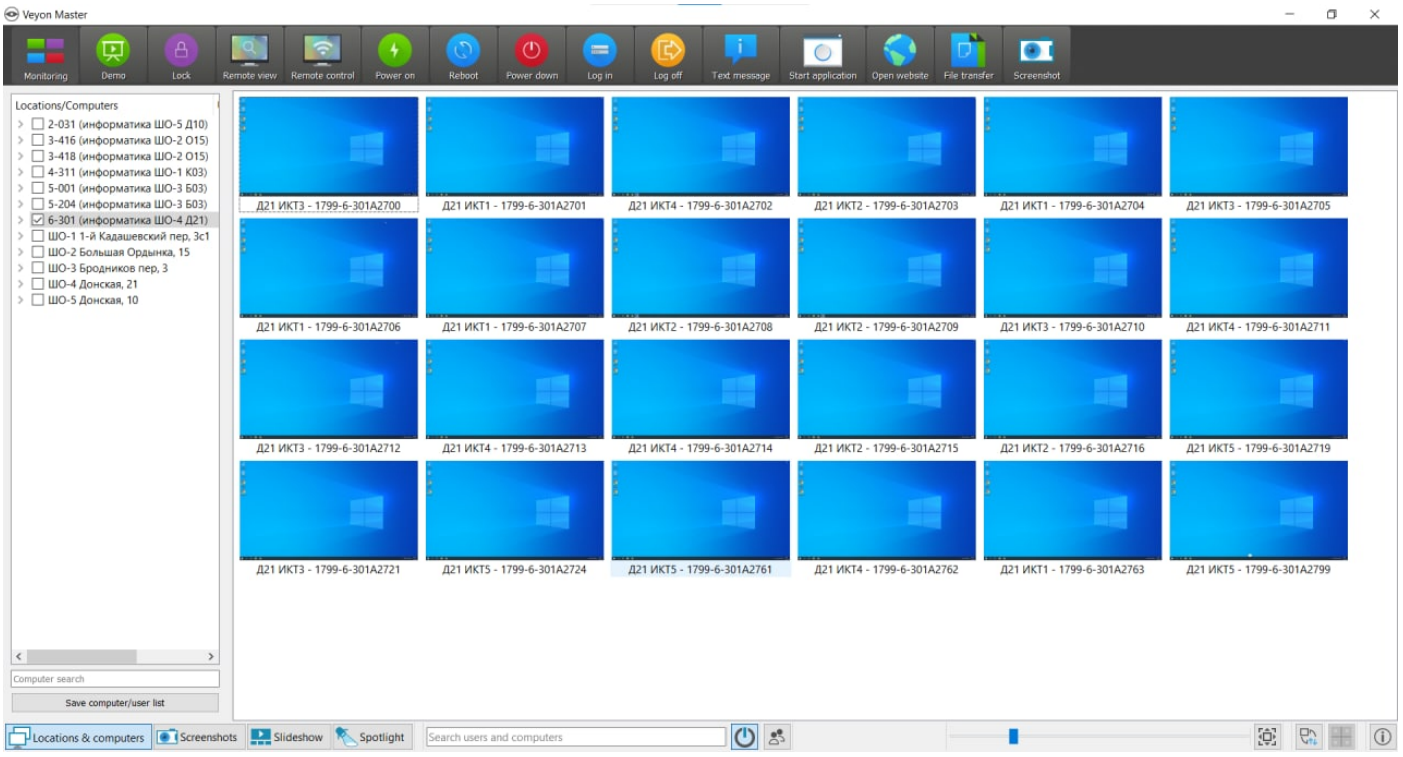
Кабинет 301 на Донской, 21 - Подразделение AD



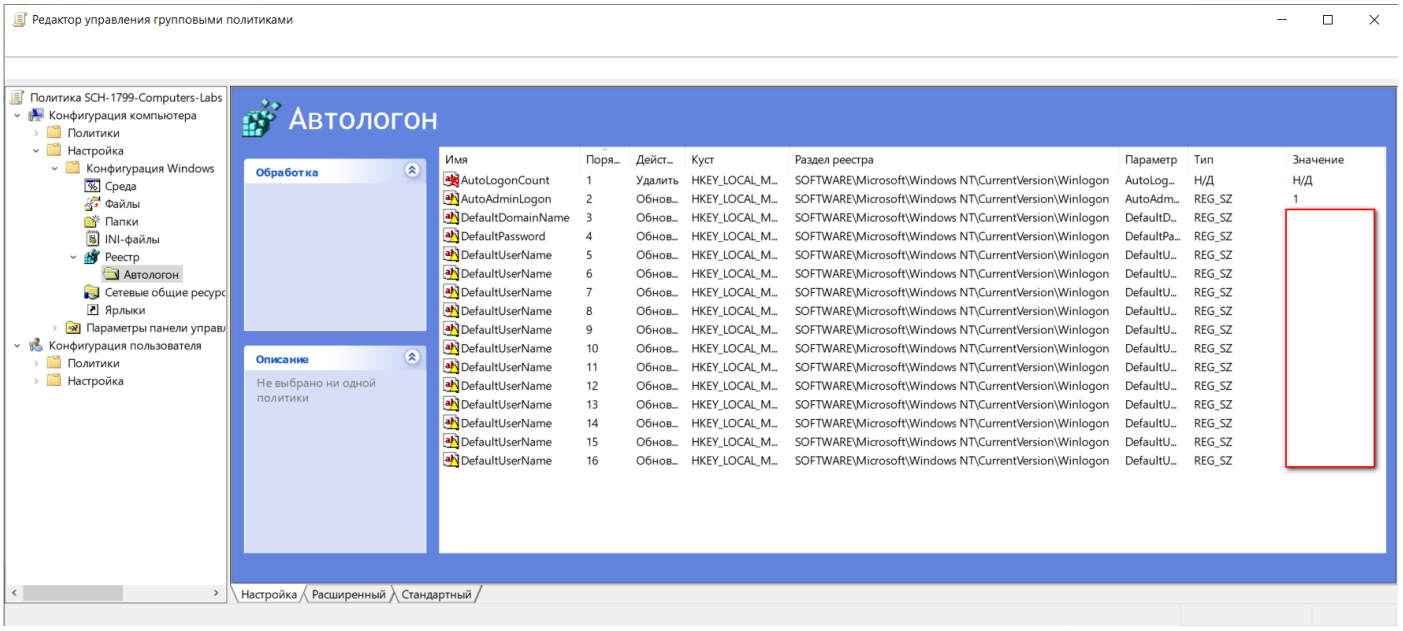
Кабинет 301 на Донской, 21 - Группы для автологона



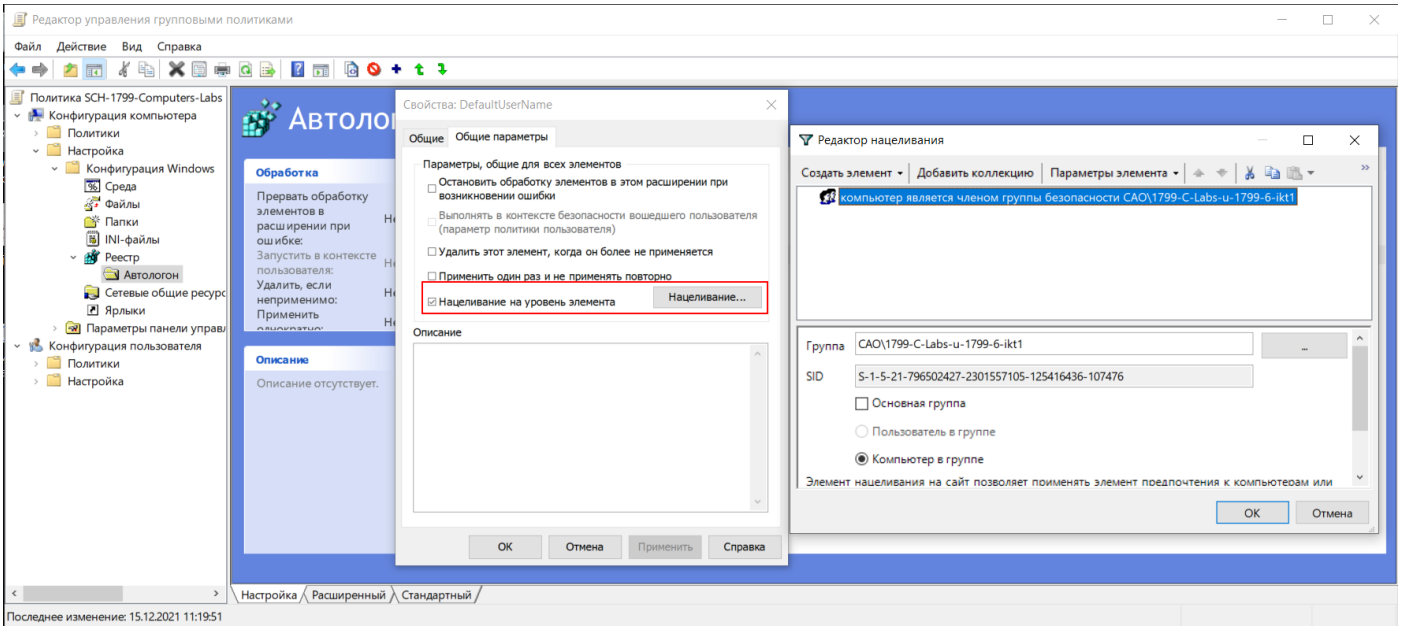
Кабинет 301 на Донской, 21 - Группа устройств KSC



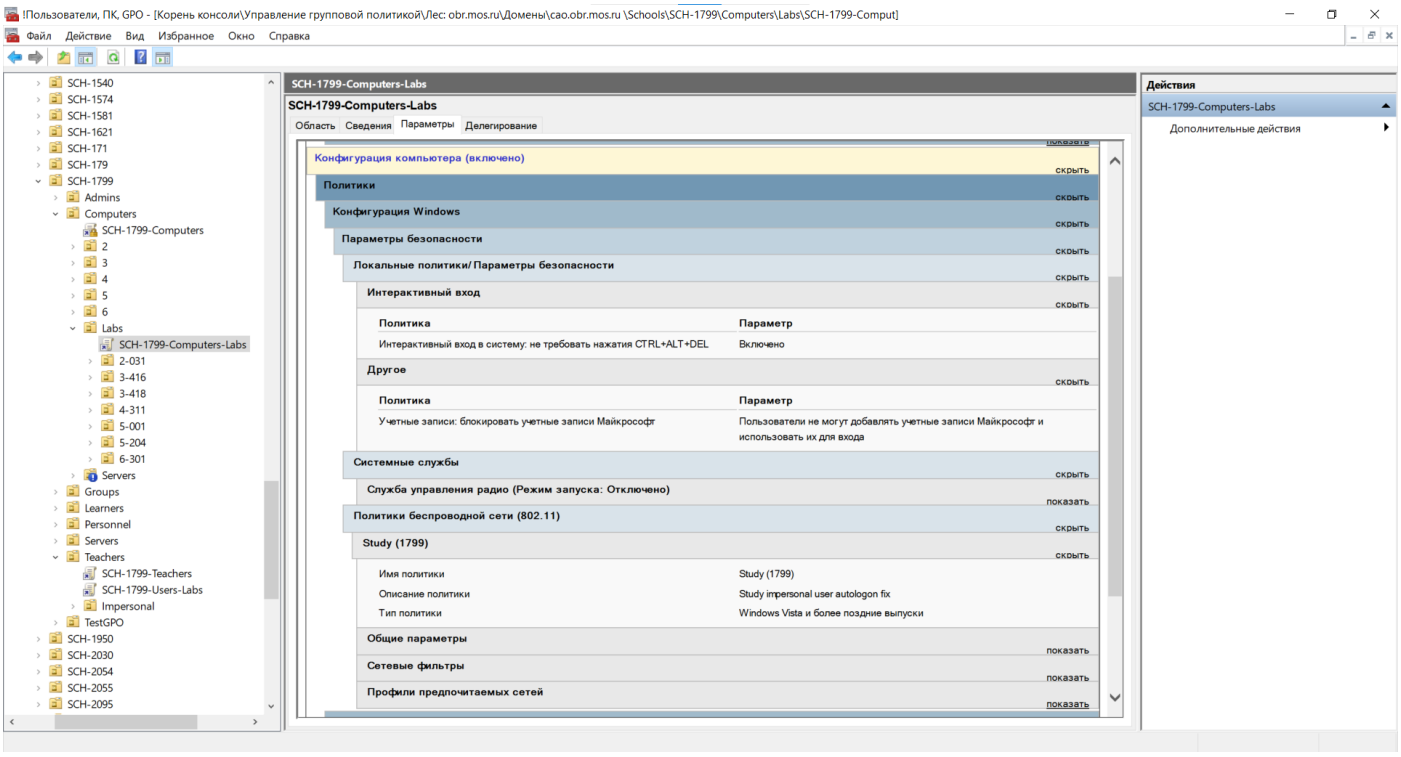
Кабинет 301 на Донской, 21 - локация Veyon на основе OU



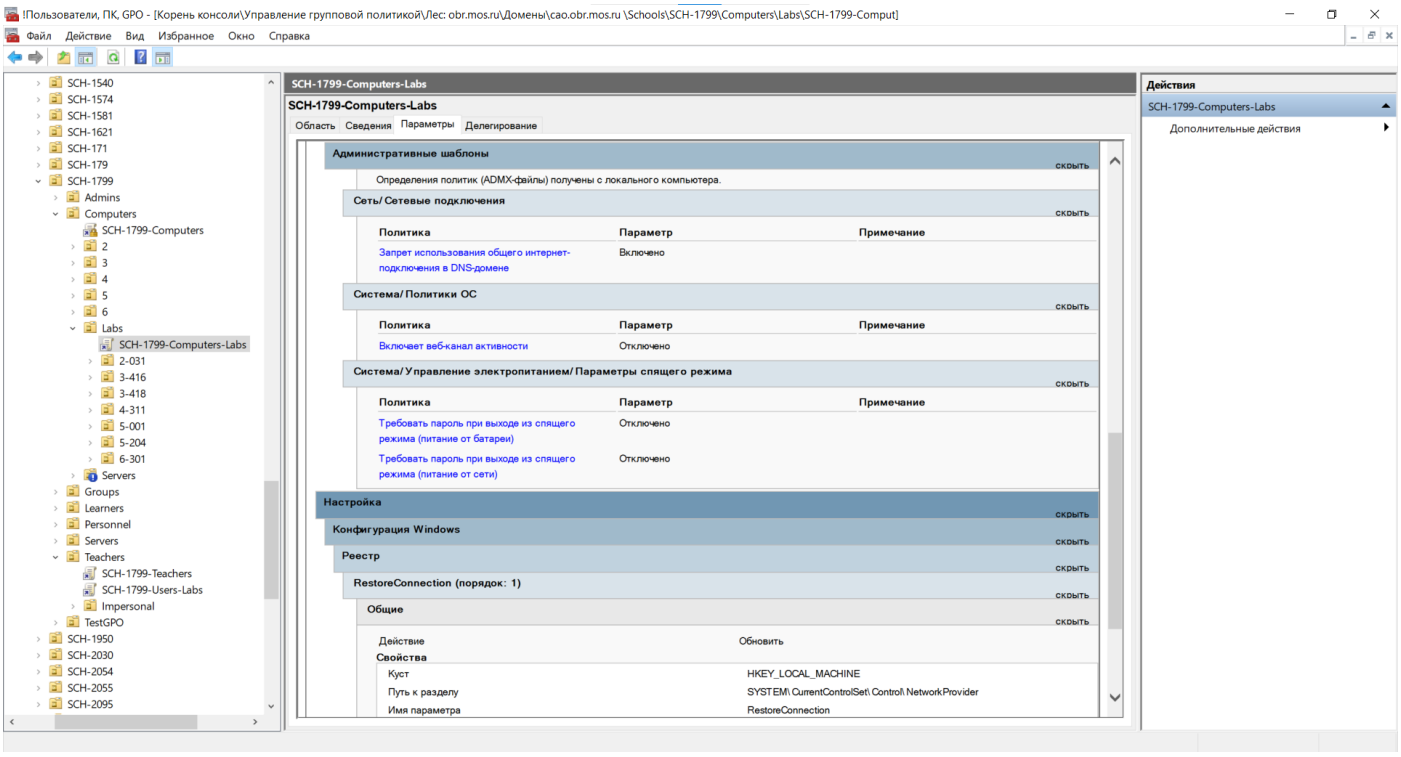
Настройки автологона с помощью Group Policy Preferences



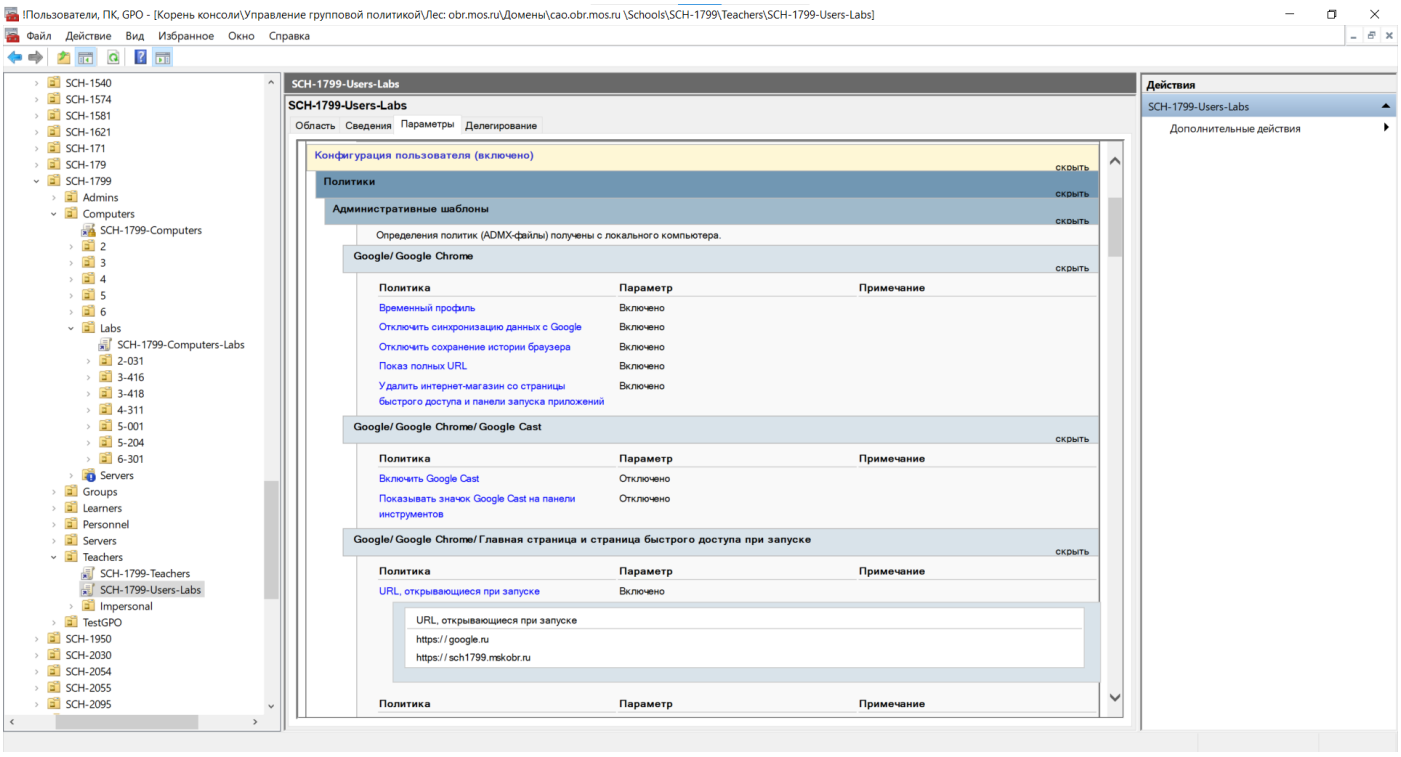
Нацеливание значения реестра DefaultUserName на группу компьютеров



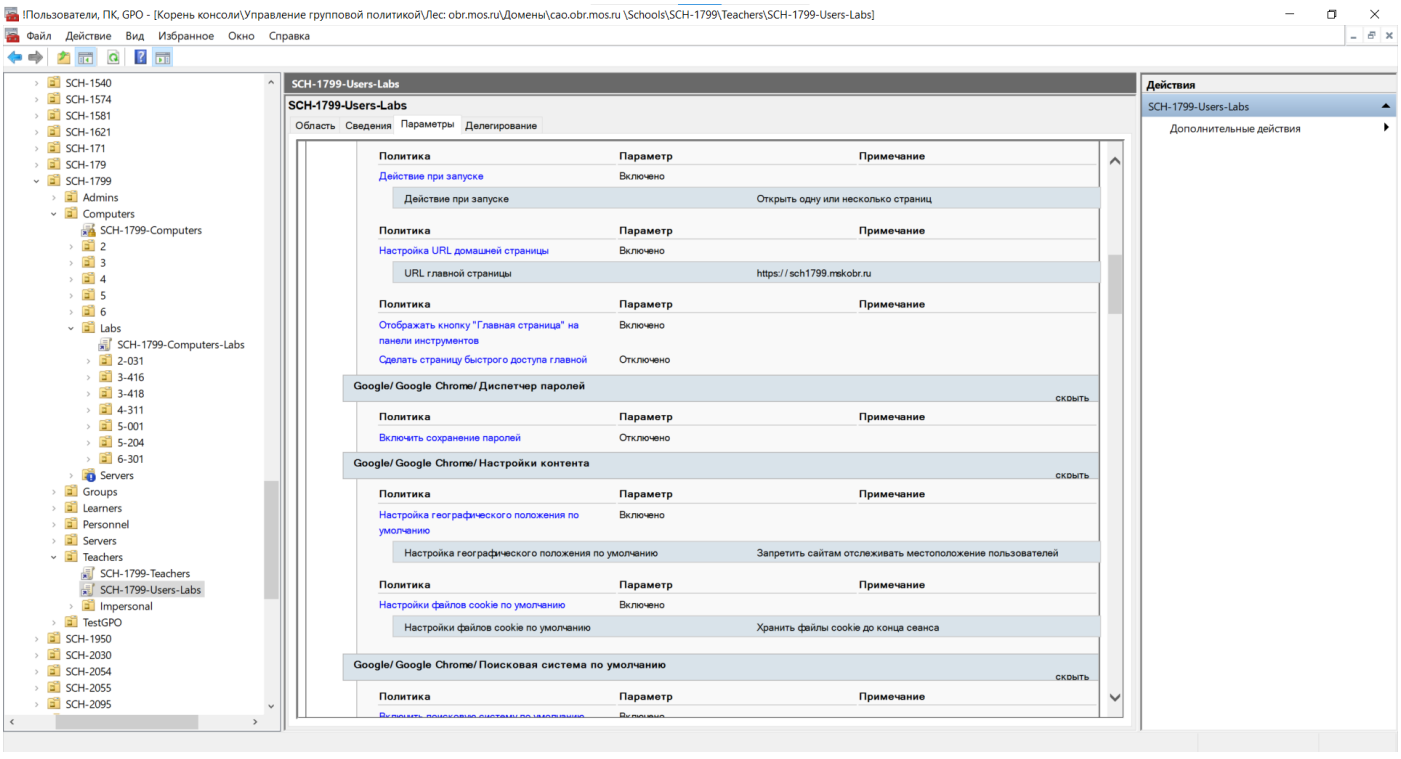
Параметры политики SCH-1799-Computers-Labs (часть 1)



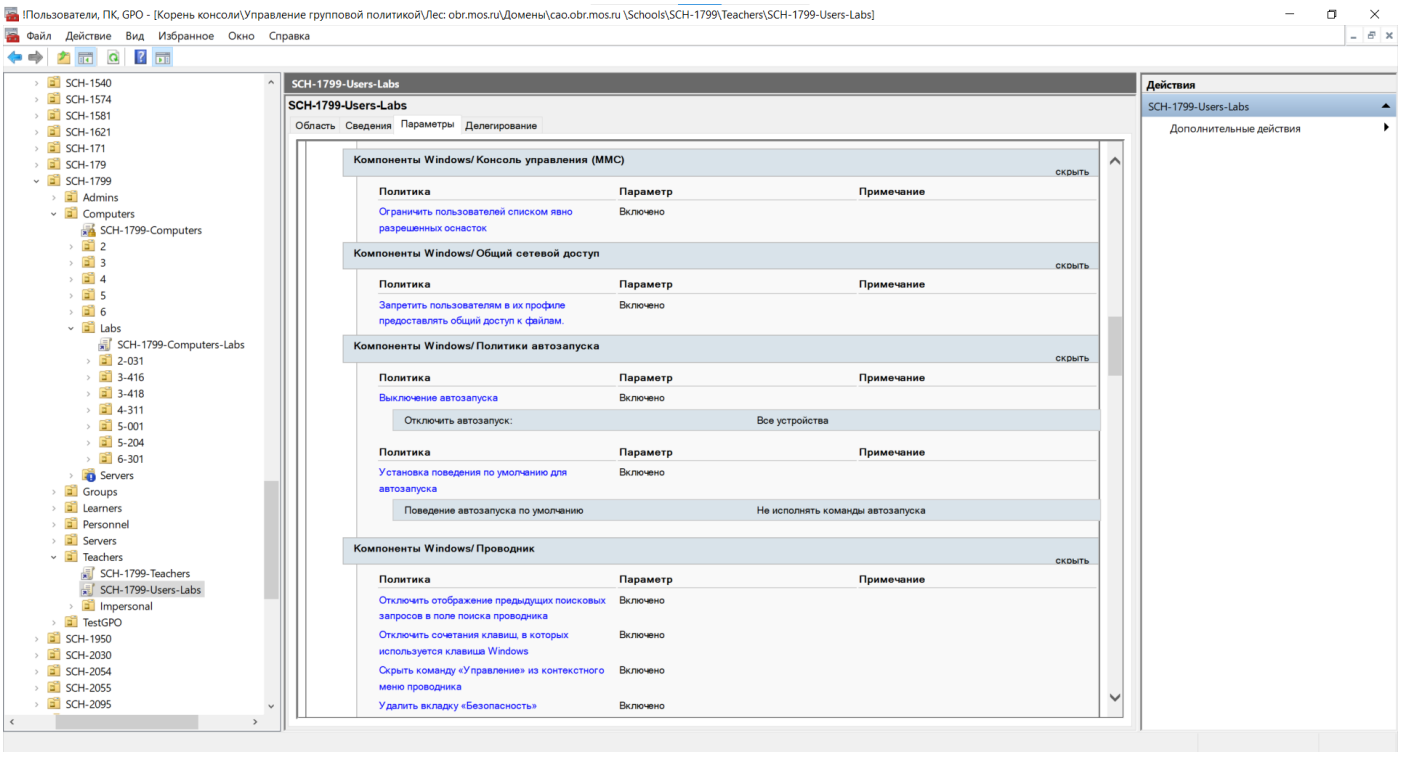
Параметры политики SCH-1799-Computers-Labs (часть 2). Настройки реестра для автологона не видны.



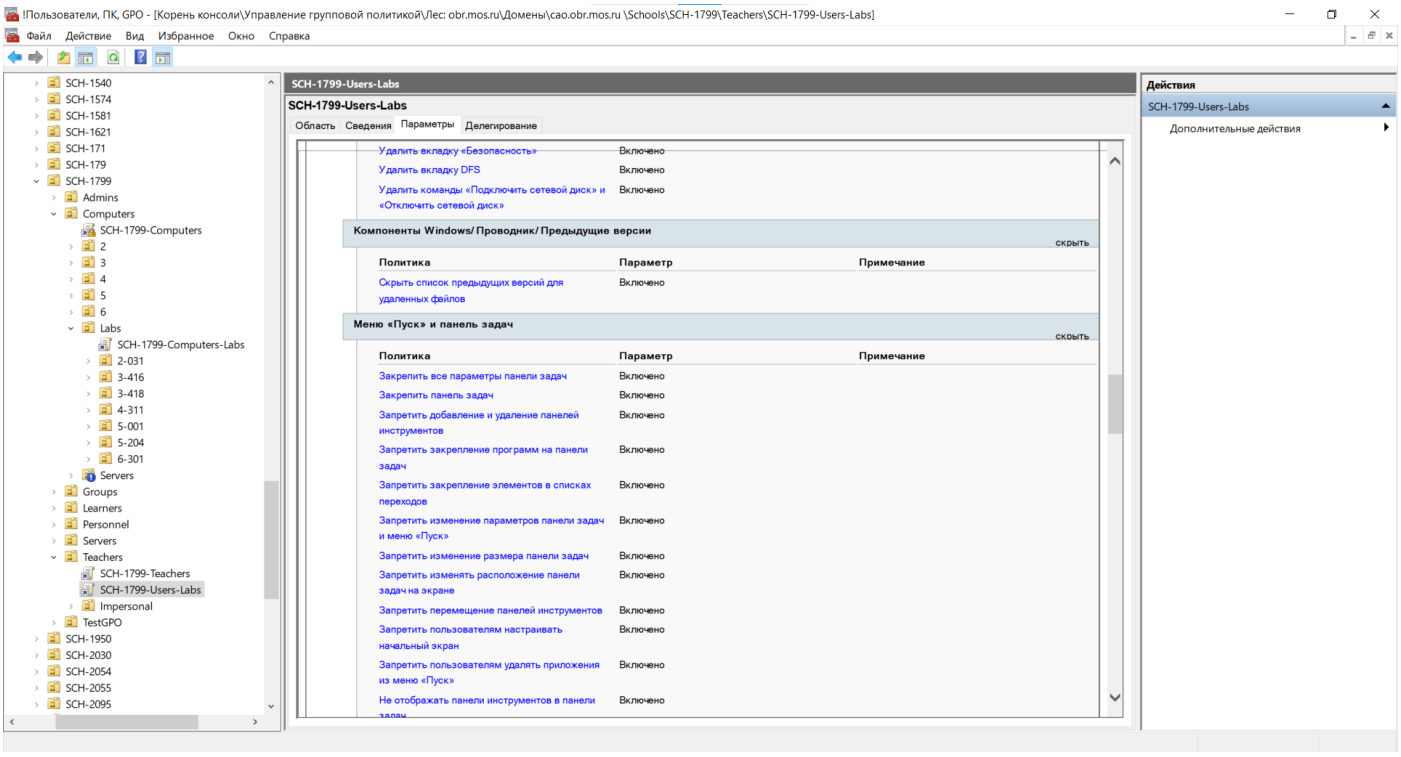
Параметры политики SCH-1799-Users-Labs (часть 1)



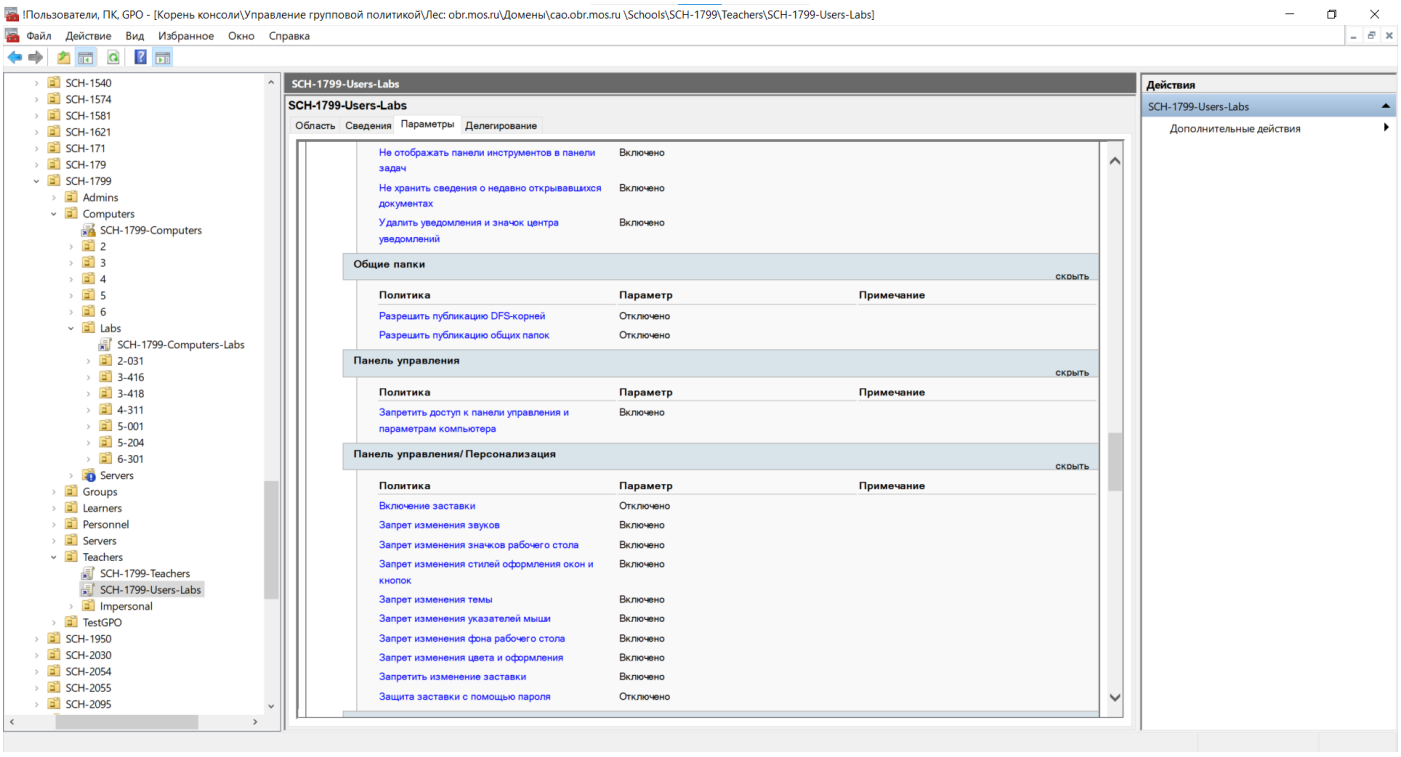
Параметры политики SCH-1799-Users-Labs (часть 2)



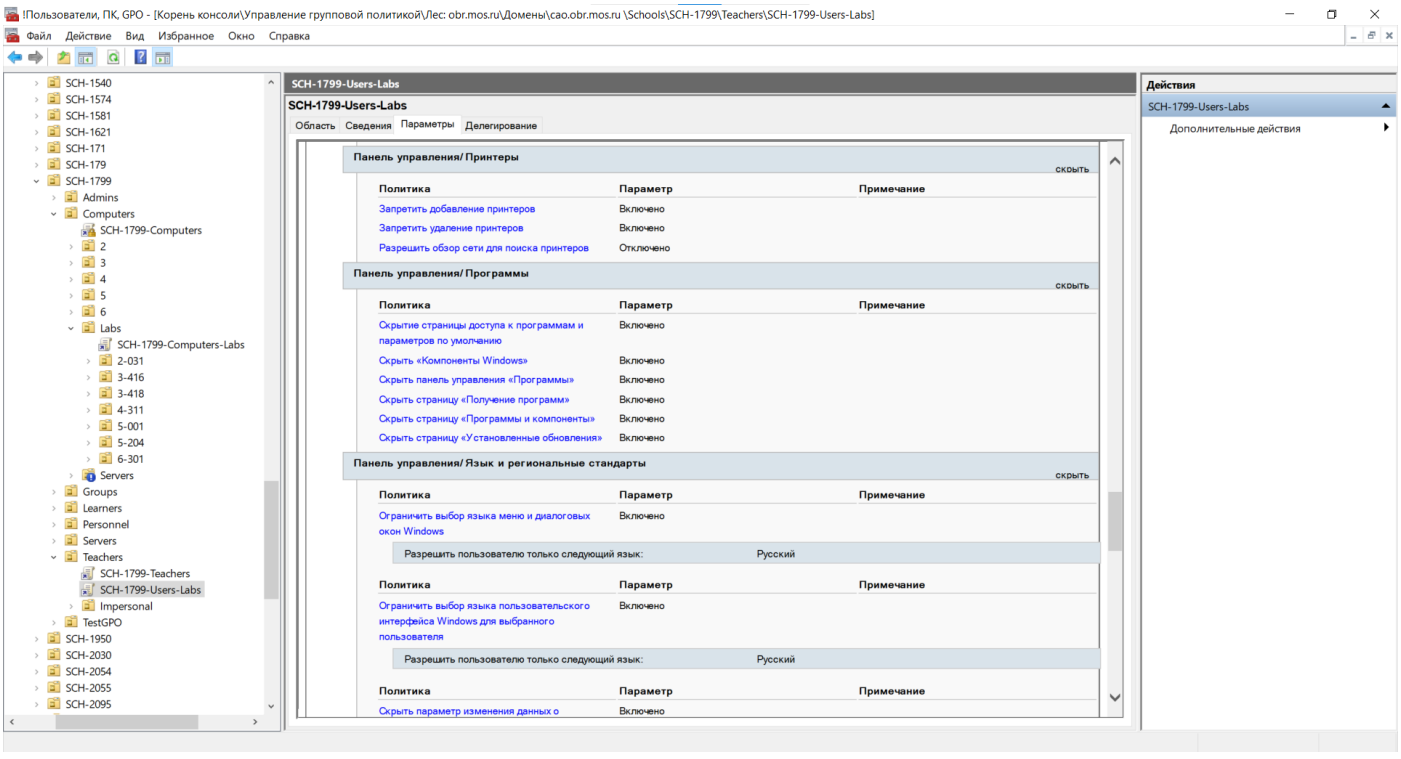
Параметры политики SCH-1799-Users-Labs (часть 3)



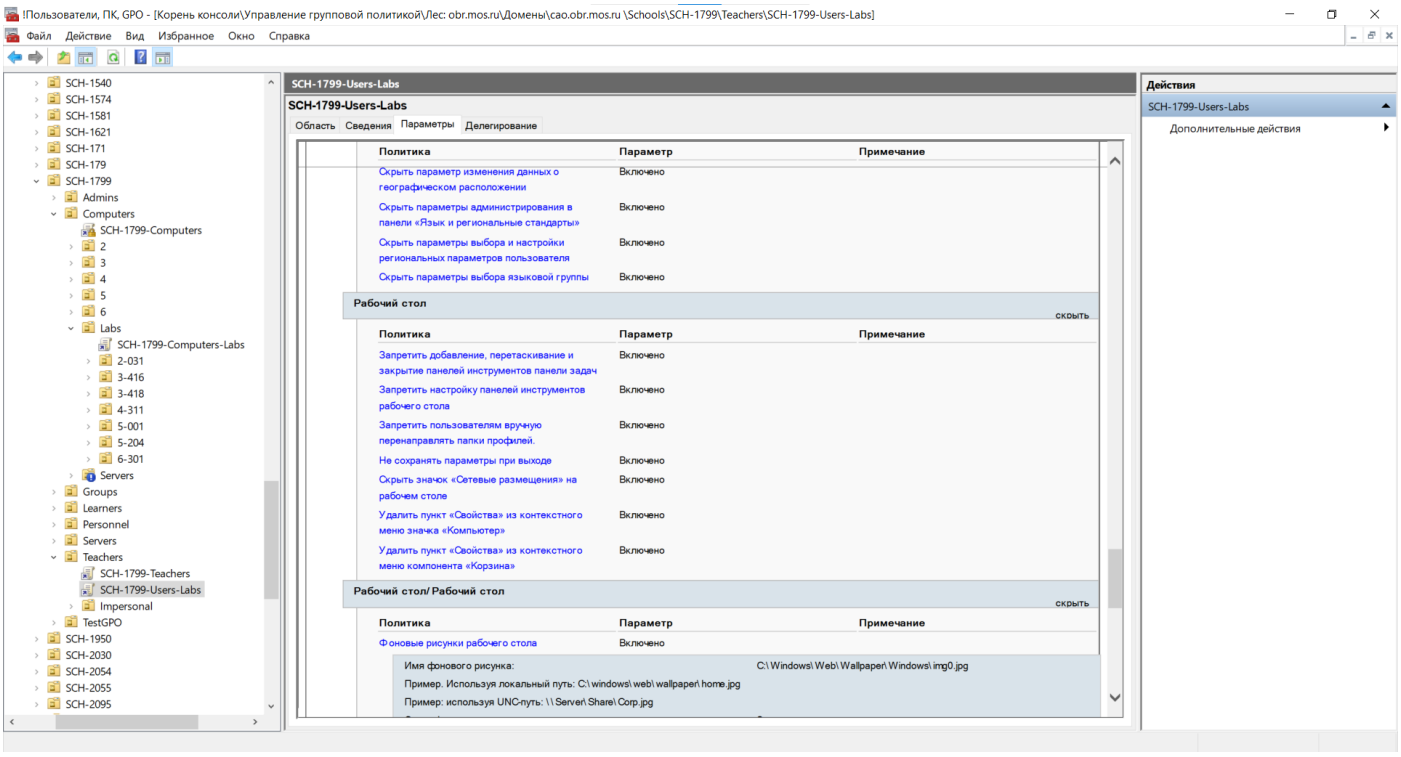
Параметры политики SCH-1799-Users-Labs (часть 4)



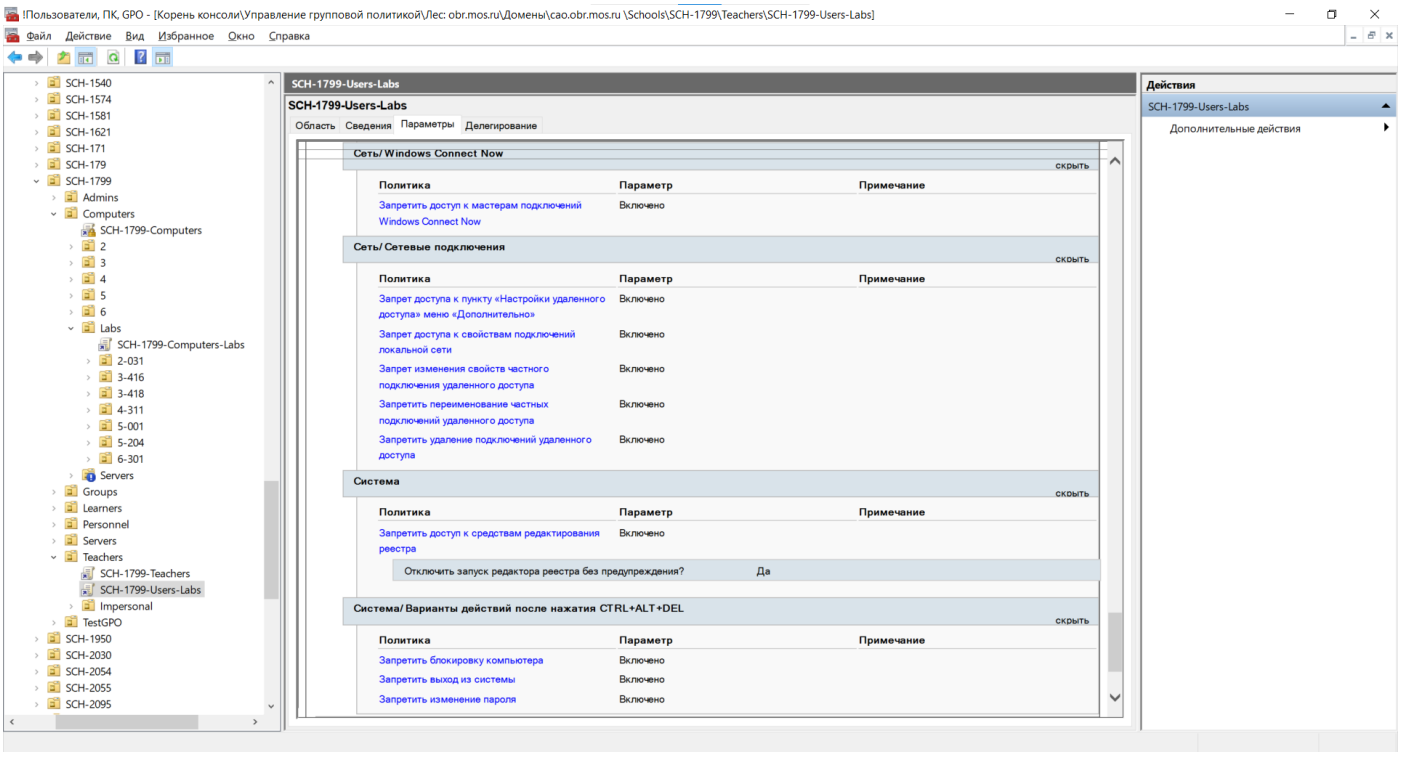
Параметры политики SCH-1799-Users-Labs (часть 5)



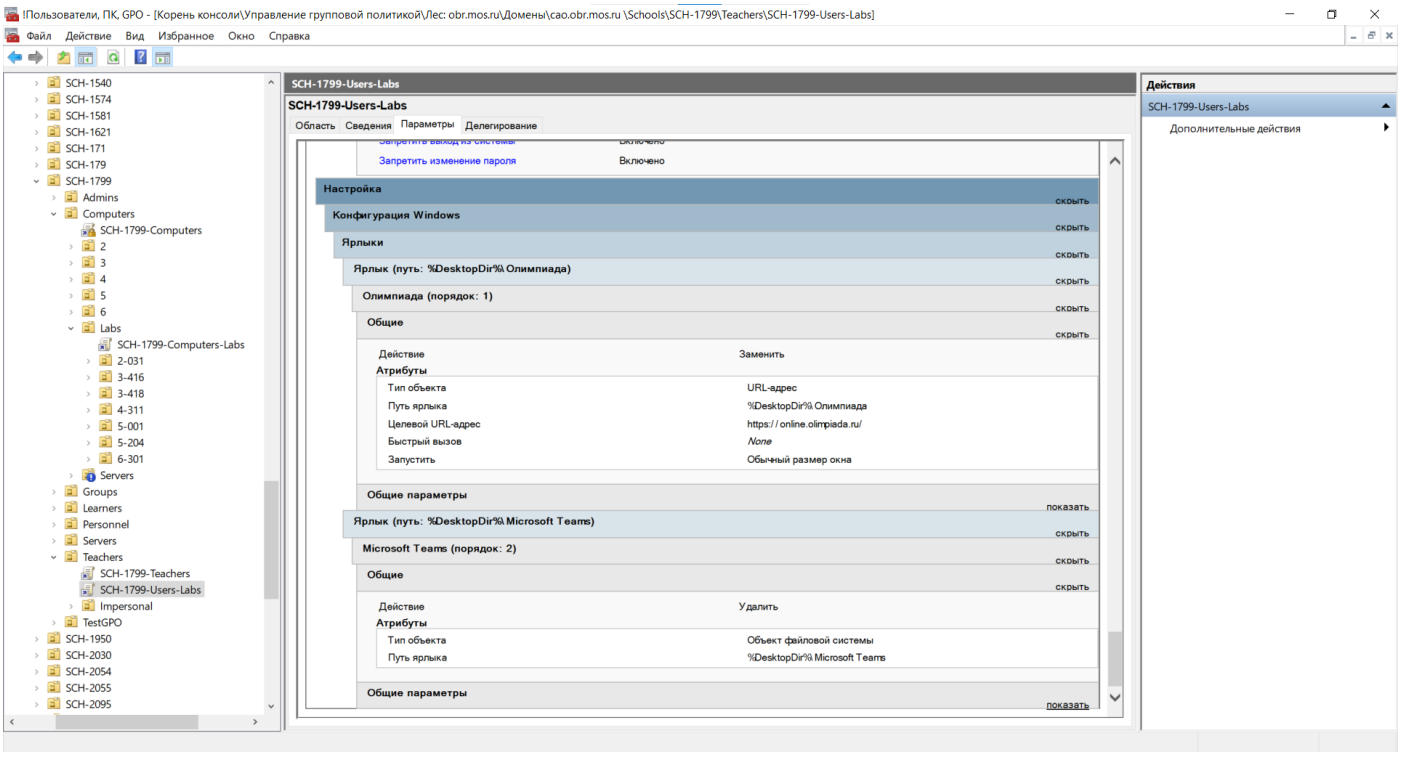
Параметры политики SCH-1799-Users-Labs (часть 6)



Параметры политики SCH-1799-Users-Labs (часть 7)



Параметры политики SCH-1799-Users-Labs (часть 8)



Параметры политики SCH-1799-Users-Labs (часть 9)