

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. Автоход 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

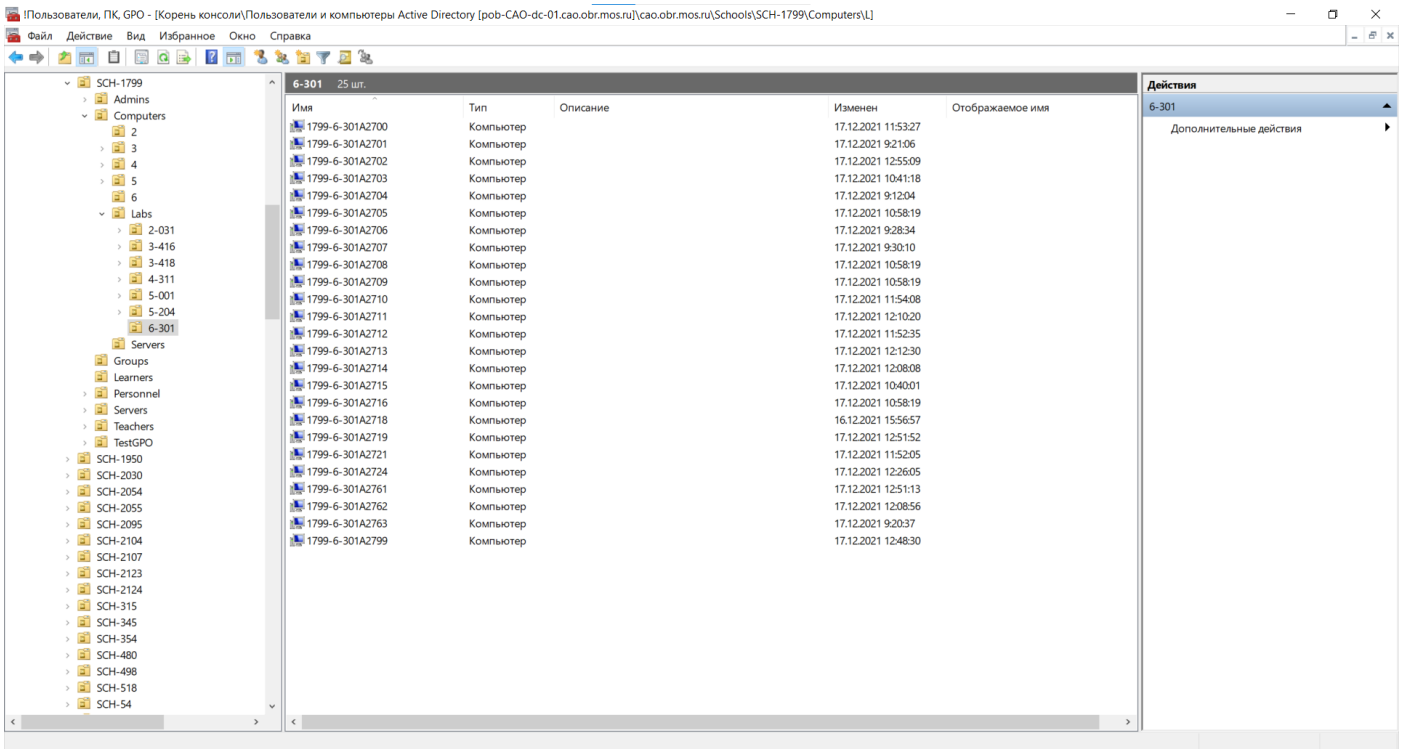
Чтобы лучше понимать, о чем здесь идет речь, можно самостоятельно изучить упоминаемые объекты. Для этого на компьютере в домене МЭШ нужно запустить оснастки "Пользователи и компьютеры Active Directory", "Управление групповой политикой" и переключиться на домен CAO.

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

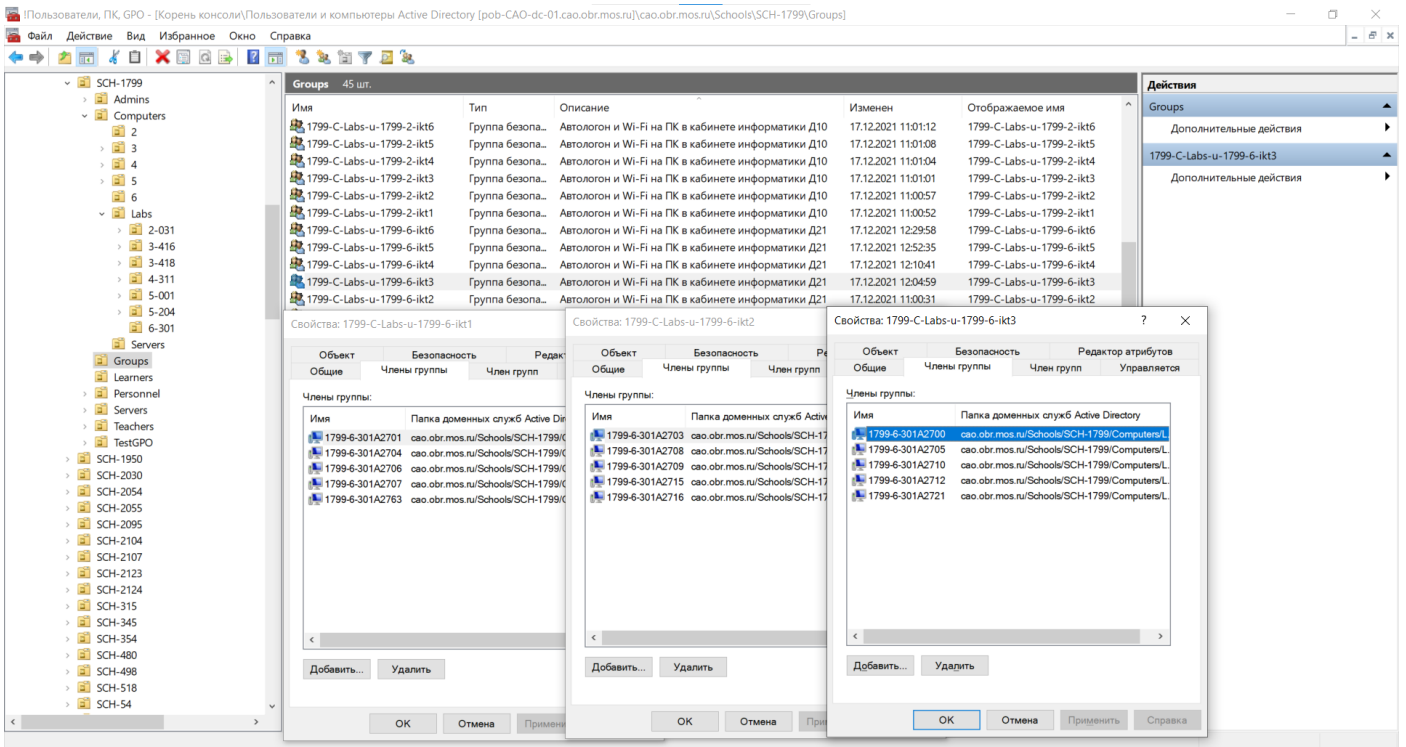
- [SCH-1799-Computers-Labs 20.12.2021.htm](#)
- [SCH-1799-Users-Labs 20.12.2021.htm](#)

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 на группу из 5 ПК для беспрепятственного 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

Kaspersky Security Center 13.2

Сервер администрирования SCH-1799-1-KSC.cao.obr.mos.ru > Управляемые устройства > Labs > 6-301

Управляемые устройства

Устройства | Политики | Задачи

Добавить или удалить графы | Обновить

Фильтр не задан, всего записей: 25

Поиск по текстовым графам

Выбор статусов: Критический: 25 Предупреждение: 0 ОК: 0

Имя	Последнее подклю...	Последнее появ...	Агент админис...	Статус посто...	Создано	Опис...	Номер...	И...
1799-6-301A2712	13 минут назад	13 минут назад	Да		2 дней назад		19044	2i
1799-6-301A2715	2 дней назад	2 дней назад	Да		19044		19044	2i
1799-6-301A2706	2 дней назад	2 дней назад	Да		3 дней назад		19044	2i
1799-6-301A2761	2 дней назад	2 дней назад	Да		2 дней назад		19044	2i
1799-6-301A2710	2 дней назад	2 дней назад	Да		2 дней назад		19044	2i
1799-6-301A2714	2 дней назад	2 дней назад	Да		3 дней назад		19044	2i
1799-6-301A2716	2 дней назад	2 дней назад	Да		3 дней назад		19044	2i
1799-6-301A2705	2 дней назад	2 дней назад	Да		2 дней назад		19044	2i
1799-6-301A2700	2 дней назад	2 дней назад	Да		2 дней назад		19044	2i
1799-6-301A2724	2 дней назад	2 дней назад	Да		2 дней назад		19044	2i
1799-6-301A2701	2 дней назад	2 дней назад	Да		2 дней назад		19044	2i
1799-6-301A2703	2 дней назад	2 дней назад	Да		3 дней назад		19044	2i
1799-6-301A2719	2 дней назад	2 дней назад	Да		2 дней назад		19044	2i
1799-6-301A2711	2 дней назад	2 дней назад	Да		2 дней назад		19044	2i
1799-6-301A2707	2 дней назад	2 дней назад	Да		3 дней назад		19044	2i
1799-6-301A2708	2 дней назад	2 дней назад	Да		2 дней назад		19044	2i
1799-6-301A2704	2 дней назад	2 дней назад	Да		3 дней назад		19044	2i
1799-6-301A2721	2 дней назад	2 дней назад	Да		2 дней назад		19044	2i
1799-6-301A2762	2 дней назад	2 дней назад	Да		2 дней назад		19044	2i
1799-6-301A2702	2 дней назад	2 дней назад	Да		2 дней назад		19044	2i

1799-6-301A2712

Статус устройства: Критический/Видим в сети

Программа безопасности не установлена

Свойства

Имя DNS-домена: 1799-6-301a2712.cao.obr.mos.ru

IP-адрес: 172.19.9.42

Статус защиты от спама: Нет данных от устройства

Статус защиты данных от утечек: Нет данных от устройства

Статус Endpoint Sensor: Нет данных от устройства

Статус защиты для серверов совместной работы: Нет данных от устройства

Статус антивирусной защиты почтовых серверов: Нет данных от устройства

Последнее обновление: 2 дней назад

Всего обнаружено угроз: 0

Соединение с Сервером: 13 минут назад

Операционная система: Microsoft Windows 10

Версия Агента: 13.2.0.1511

Справка kaspersky

Группа: 0 устройств: 25

Кабинет 301 на Донской, 21 - Группа устройств KSC

Veyon Master

Monitoring | Demo | Lock | Remote view | Remote control | Power on | Reboot | Power down | Log in | Log off | Text message | Start application | Open website | File transfer | Screenshot

Locations/Computers

- 2-031 (информатика ШО-5 Д10)
- 3-416 (информатика ШО-2 О15)
- 3-418 (информатика ШО-2 О15)
- 4-311 (информатика ШО-1 К03)
- 5-001 (информатика ШО-3 Б03)
- 5-204 (информатика ШО-3 Б03)
- 6-301 (информатика ШО-4 Д21)
 - ШО-1 1-й Кадашевский пер, 3с1
 - ШО-2 Большая Ордынка, 15
 - ШО-3 Бродников пер, 3
 - ШО-4 Донская, 21
 - ШО-5 Донская, 10

Д21 ИКТ3 - 1799-6-301A2700	Д21 ИКТ1 - 1799-6-301A2701	Д21 ИКТ4 - 1799-6-301A2702	Д21 ИКТ2 - 1799-6-301A2703	Д21 ИКТ1 - 1799-6-301A2704	Д21 ИКТ3 - 1799-6-301A2705
Д21 ИКТ1 - 1799-6-301A2706	Д21 ИКТ1 - 1799-6-301A2707	Д21 ИКТ2 - 1799-6-301A2708	Д21 ИКТ2 - 1799-6-301A2709	Д21 ИКТ3 - 1799-6-301A2710	Д21 ИКТ4 - 1799-6-301A2711
Д21 ИКТ3 - 1799-6-301A2712	Д21 ИКТ4 - 1799-6-301A2713	Д21 ИКТ4 - 1799-6-301A2714	Д21 ИКТ2 - 1799-6-301A2715	Д21 ИКТ2 - 1799-6-301A2716	Д21 ИКТ5 - 1799-6-301A2719
Д21 ИКТ3 - 1799-6-301A2721	Д21 ИКТ5 - 1799-6-301A2724	Д21 ИКТ5 - 1799-6-301A2761	Д21 ИКТ4 - 1799-6-301A2762	Д21 ИКТ1 - 1799-6-301A2763	Д21 ИКТ5 - 1799-6-301A2799

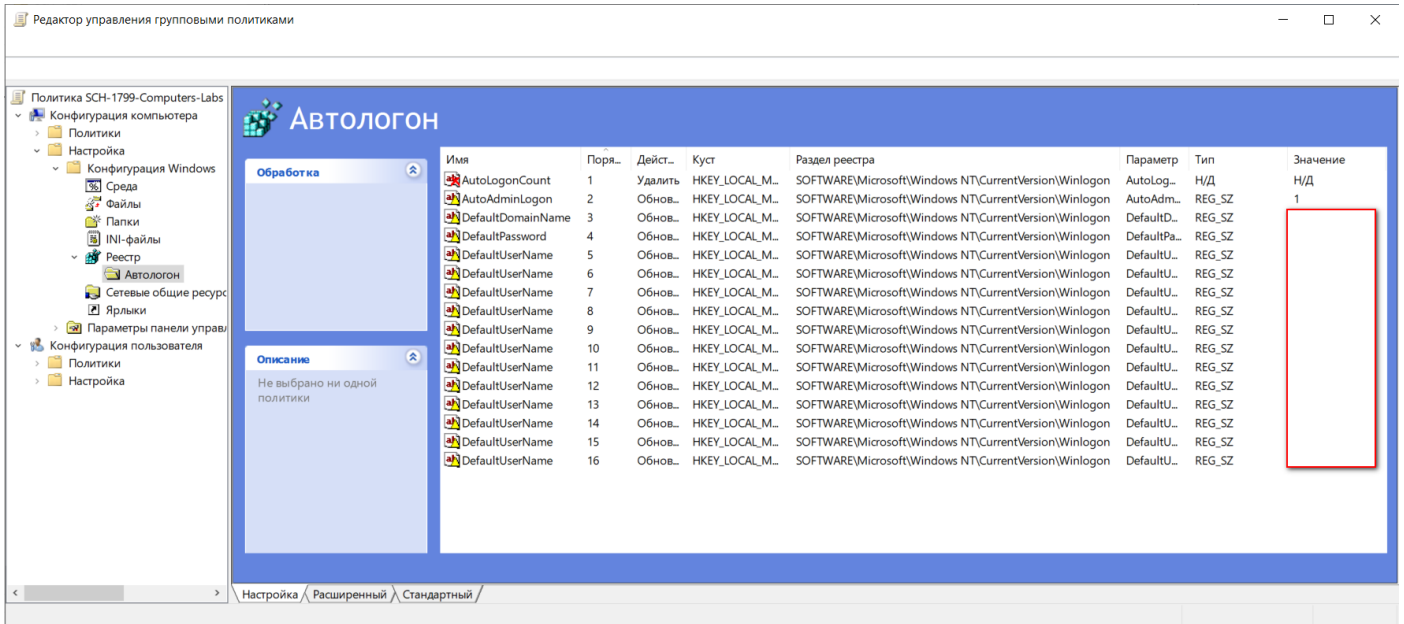
Computer search

Save computer/user list

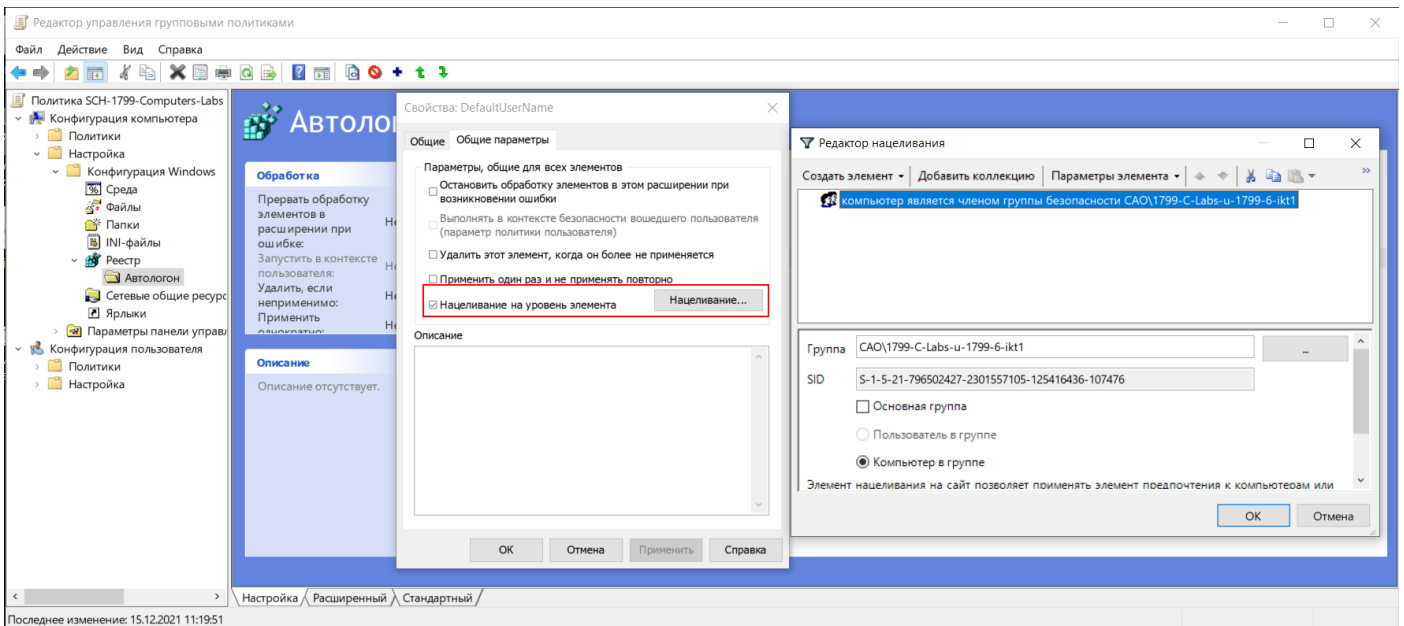
Locations & computers | Screenshots | Slideshow | Spotlight

Search users and computers

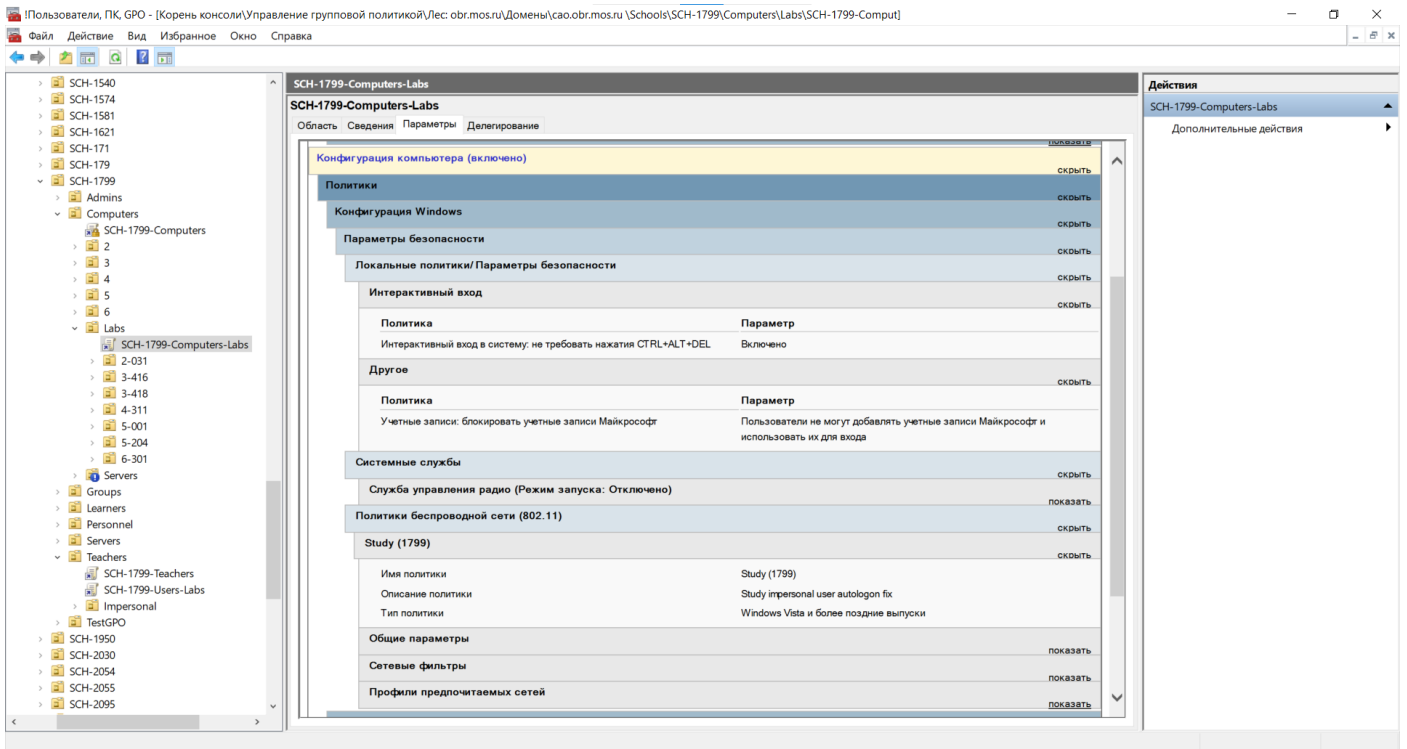
Кабинет 301 на Донской, 21 - локация Вейон на основе OU



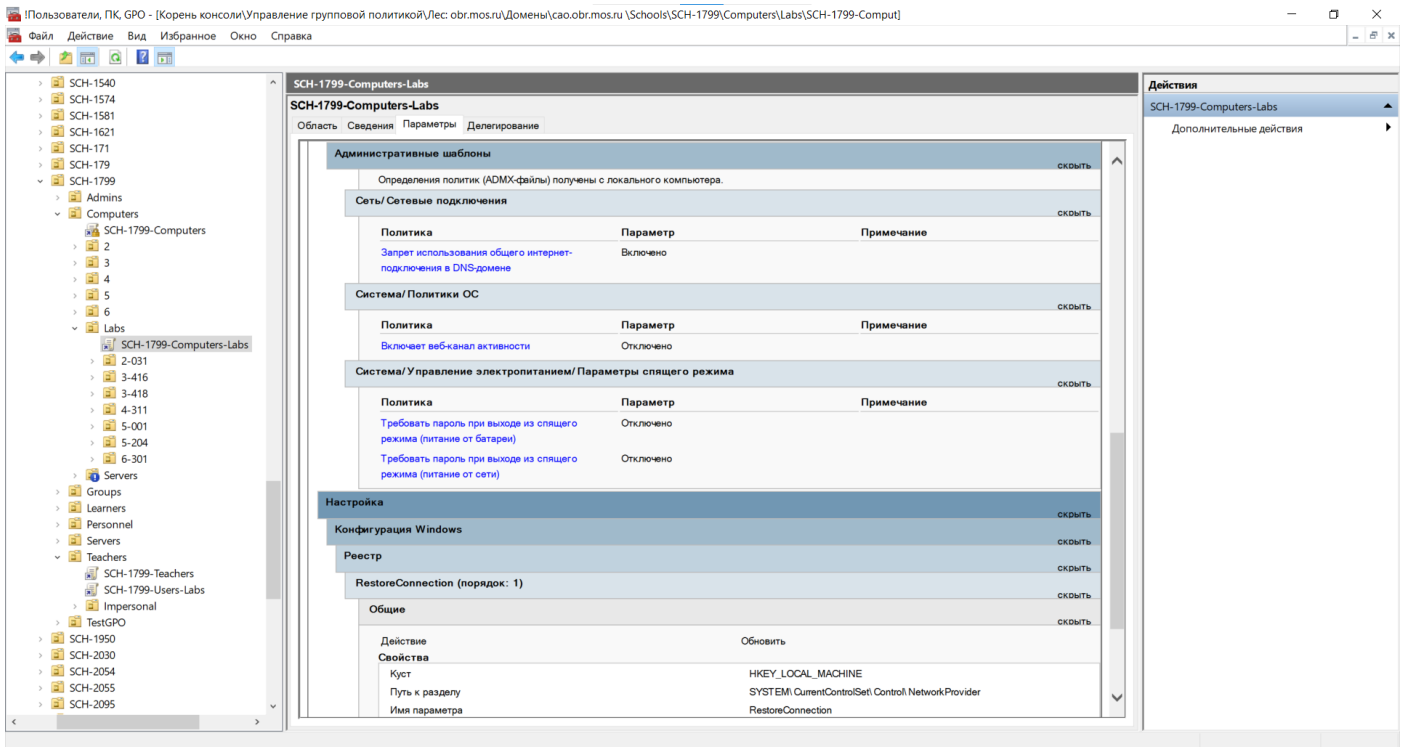
Настройки автологона с помощью Group Policy Preferences



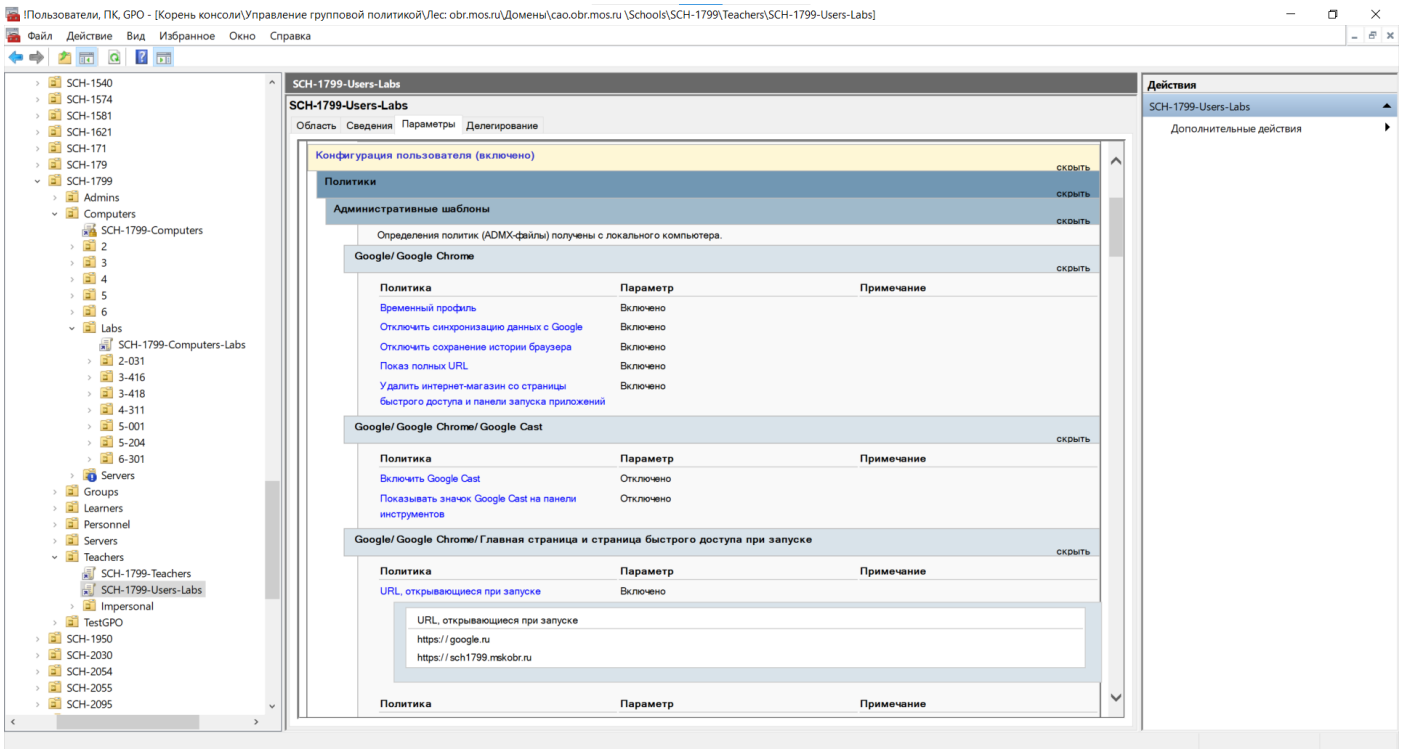
Нацеливание значения реестра DefaultUserName на группу компьютеров



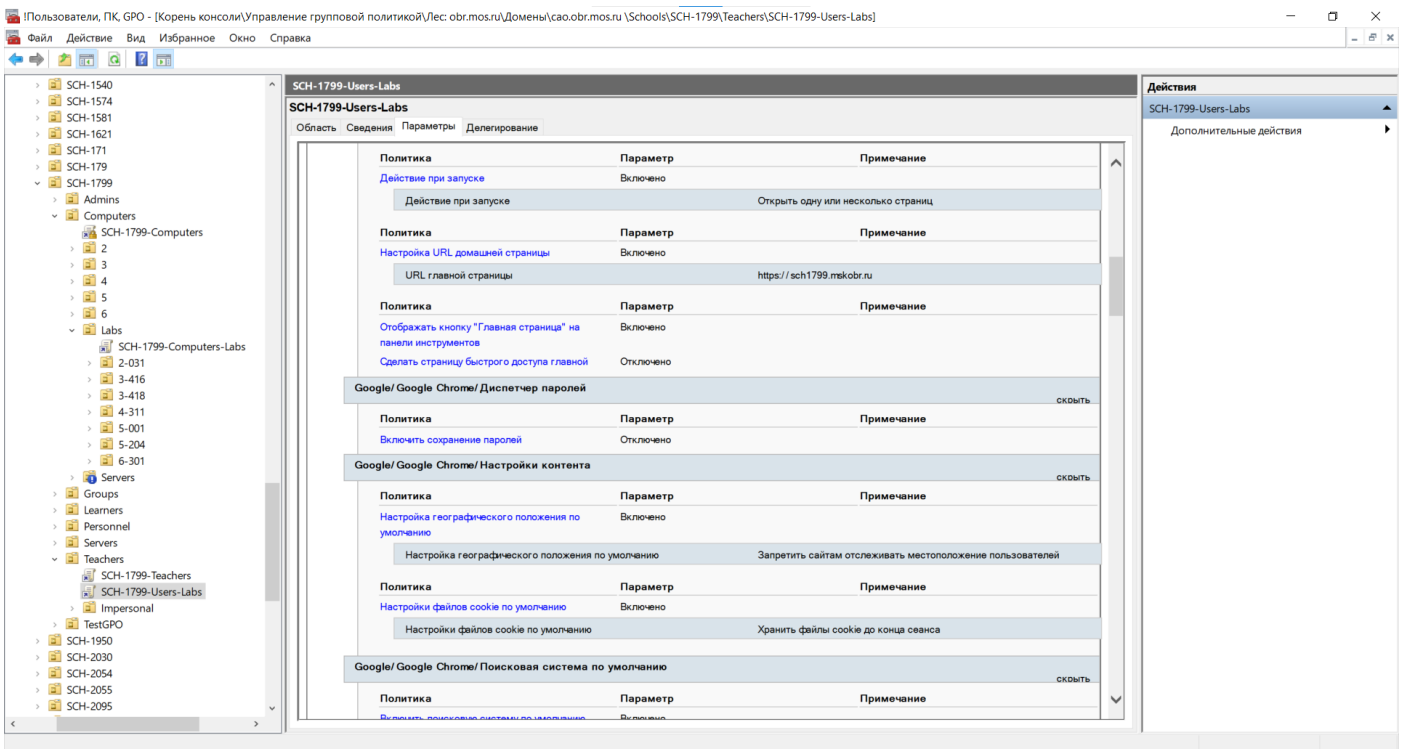
Параметры политики SCH-1799-Computers-Labs (часть 1)



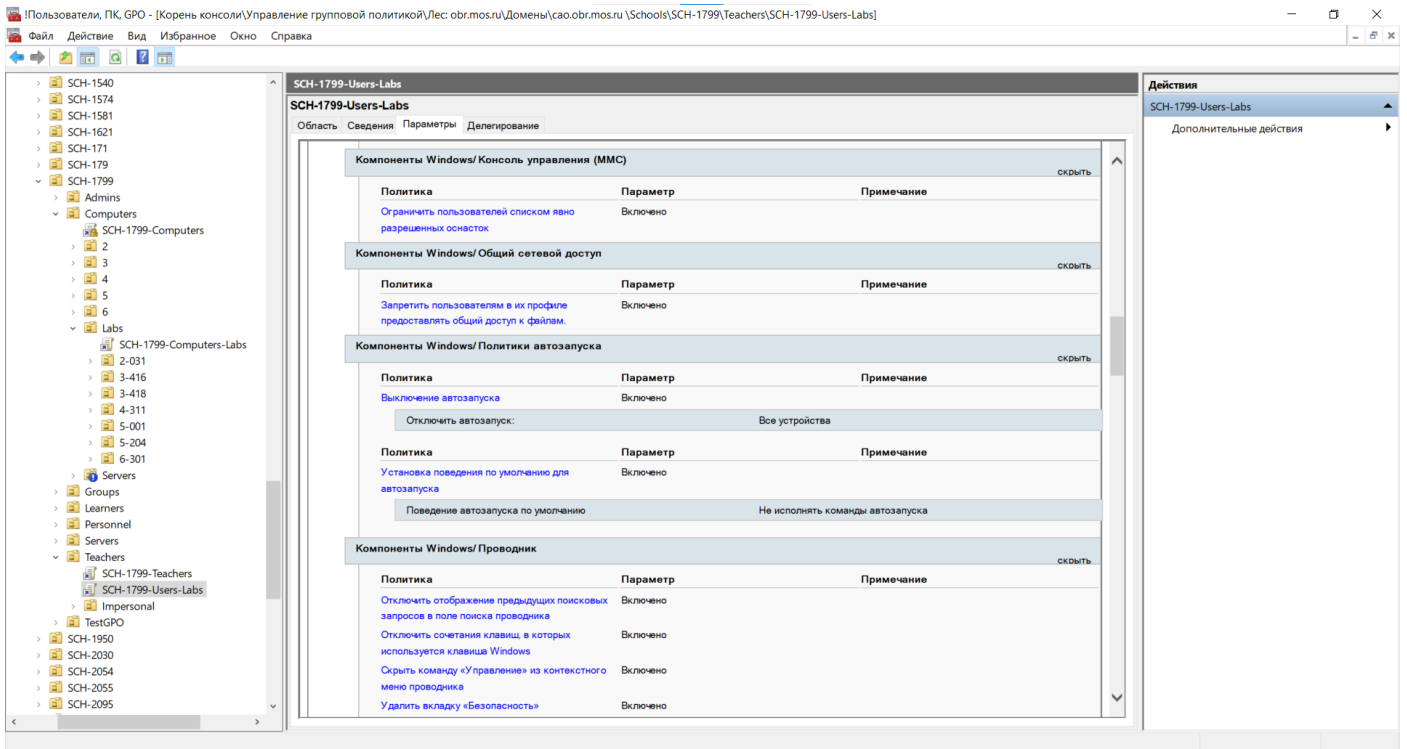
Параметры политики SCH-1799-Computers-Labs (часть 2). Настройки реестра для автологона не видны.



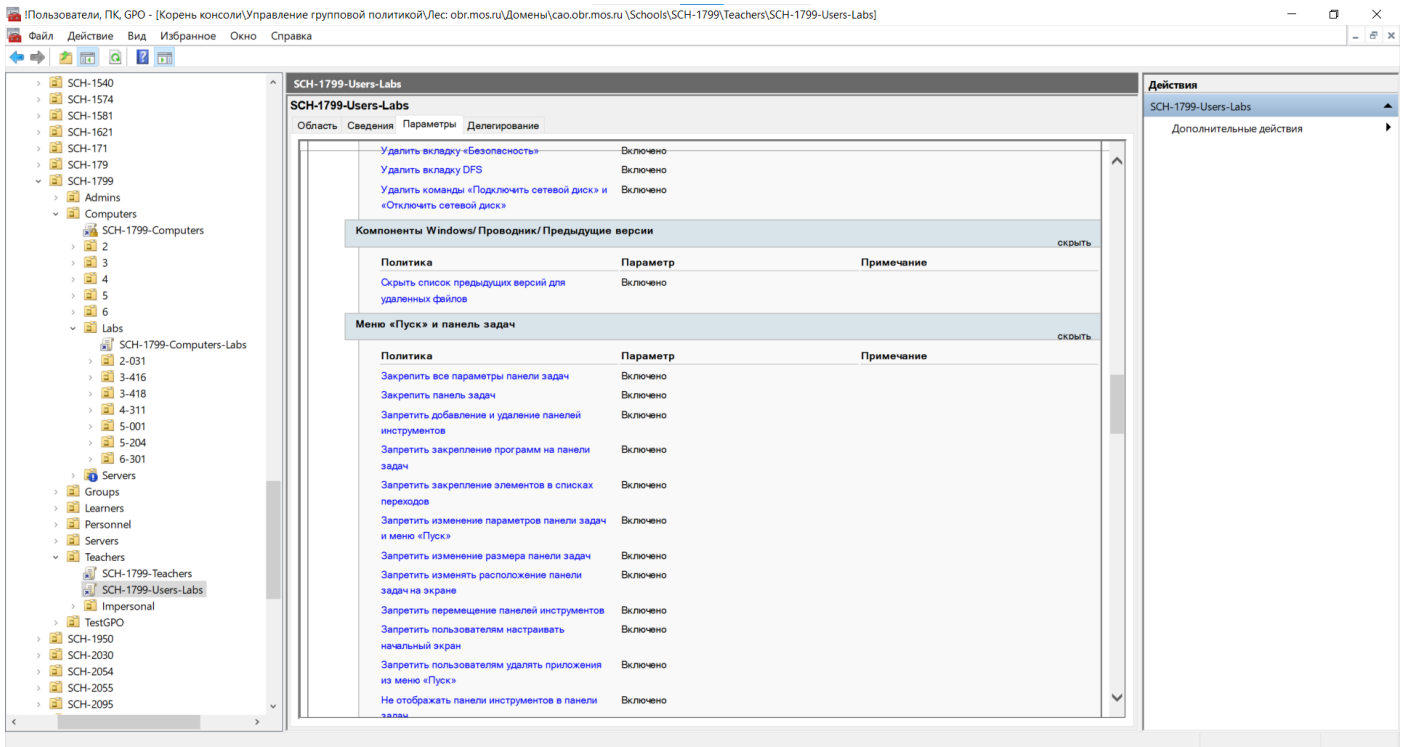
Параметры политики SCH-1799-Users-Labs (часть 1)



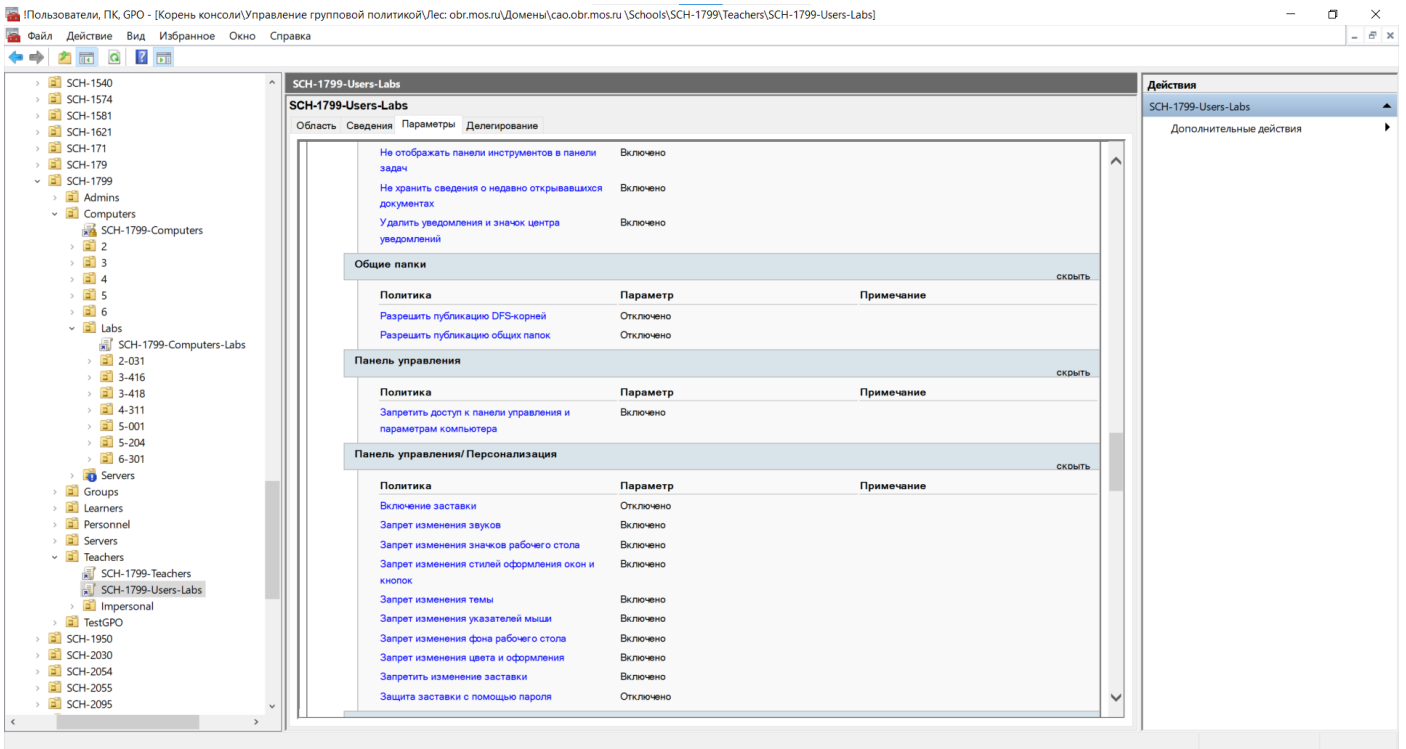
Параметры политики SCH-1799-Users-Labs (часть 2)



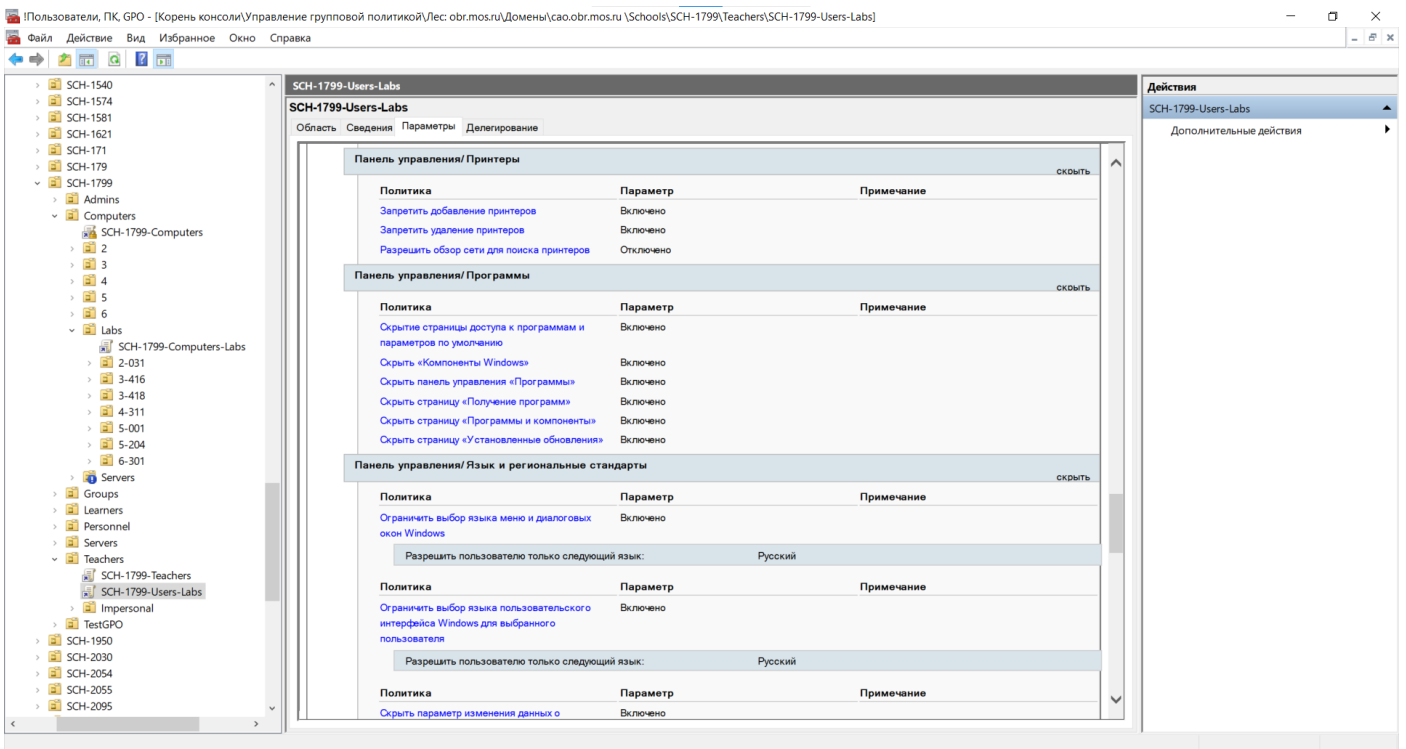
Параметры политики SCH-1799-Users-Labs (часть 3)



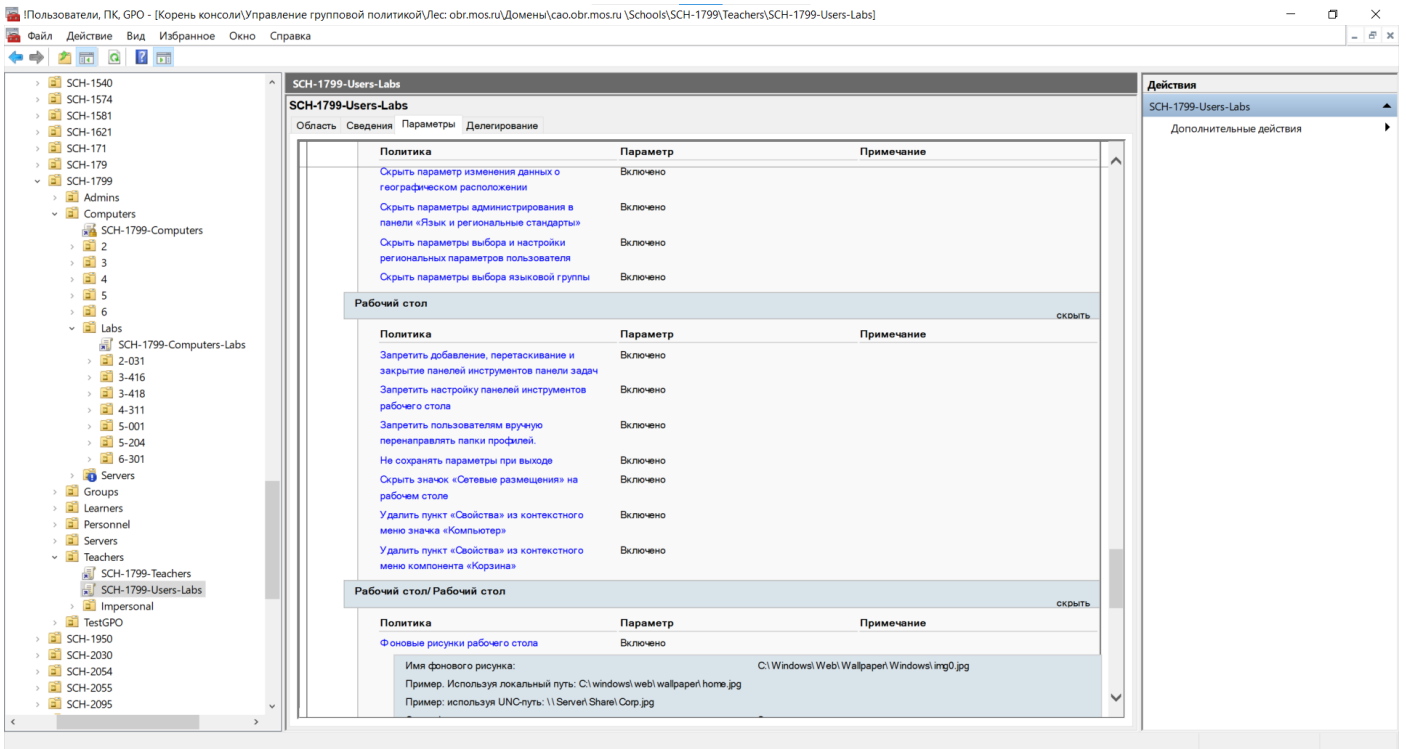
Параметры политики SCH-1799-Users-Labs (часть 4)



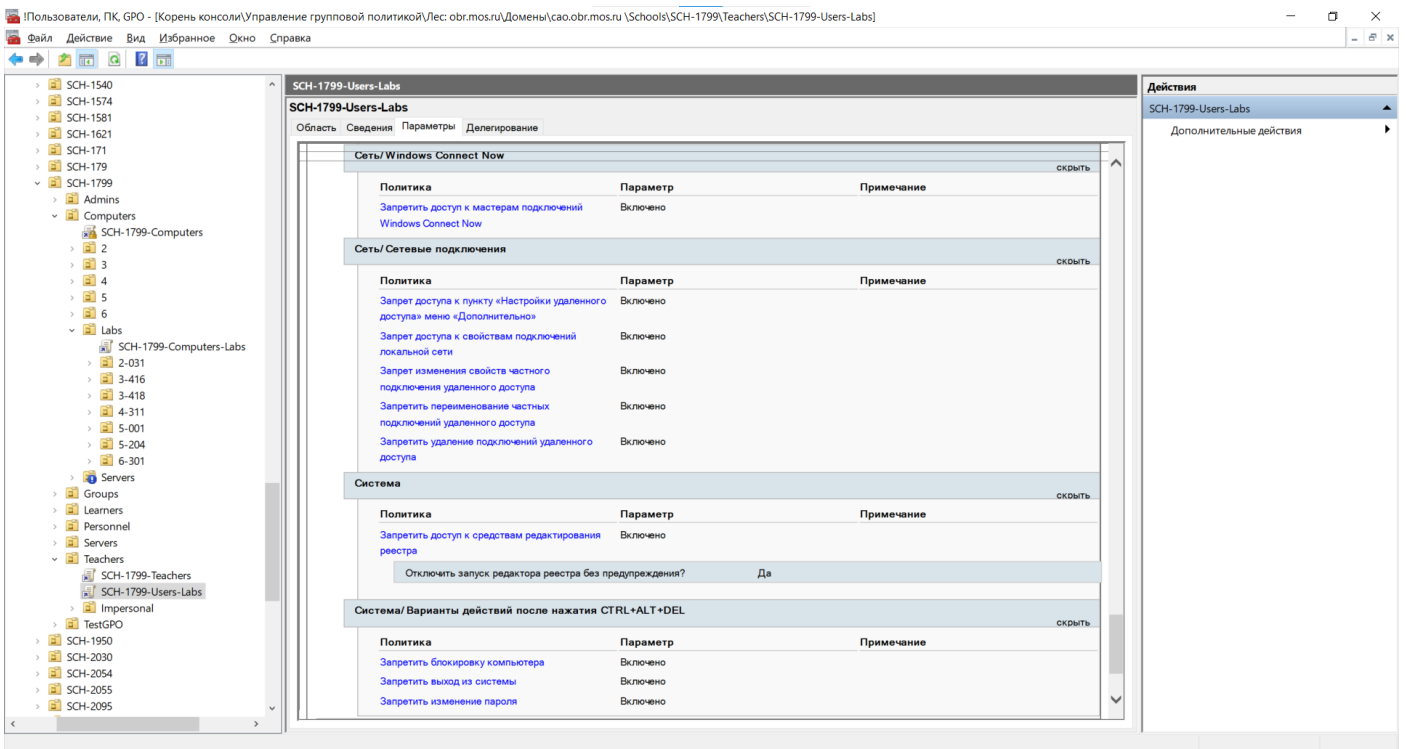
Параметры политики SCH-1799-Users-Labs (часть 5)



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



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



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

Пользователи, ПК, GPO - [Корень консоли]\Управление групповой политикой\Лес: obr.mos.ru\Домены\cao.obr.mos.ru\Schools\SCH-1799\Teachers\SCH-1799-Users-Labs

Файл Действие Вид Избранное Окно Справка

SCH-1799-Users-Labs

SCH-1799-Users-Labs

Область Сведения Параметры Делегирование

запретить ввод из системы выключено

Запретить изменение пароля Включено

Настройка

Конфигурация Windows [скрыть](#)

Ярлыки

Ярлык (путь: %DesktopDir%\Олимпиада) [скрыть](#)

Олимпиада (порядок: 1) [скрыть](#)

Общие [скрыть](#)

Действие	Заменить
Атрибуты	
Тип объекта	URL-адрес
Путь ярлыка	%DesktopDir%\Олимпиада
Целевой URL-адрес	https://online.olimpiada.ru/
Быстрый вызов	None
Запустить	Обычный размер окна

Общие параметры [показать](#)

Ярлык (путь: %DesktopDir%\Microsoft Teams) [показать](#)

Microsoft Teams (порядок: 2) [скрыть](#)

Общие [скрыть](#)

Действие	Удалить
Атрибуты	
Тип объекта	Объект файловой системы
Путь ярлыка	%DesktopDir%\Microsoft Teams

Общие параметры [показать](#)

Действия

SCH-1799-Users-Labs

Дополнительные действия

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