3.1.4.2. Настройка входа в домен по предъявлению токена

Раздел содержит инструкцию по настройке входа в домен по предъявлению токена в операционной системе **Windows Server 2022**.

Для настройки необходимы:

- компьютер с установленной операционной системой Windows 2022 Server Rus**;**
- установленные Драйверы Рутокен;
- дистрибутив ОС.

Необходимые условия:

- операционная система настроена как **Контроллер домена;**
- установлены **Службы Сертификации;**
- пользователям выданы сертификаты типа **Пользователь со смарт-картой** или **Вход со смарт-картой**.

Все описанные действия производятся с правами администратора системы.

Для примера используется учетная запись **Admin**.

Если необходимо настроить учетную запись для конкретного пользователя, то выполните процедуру, описанную в разделе.

Если необходимо выполнить настройку для группы пользователей, то выполните процедуру, описанную в разделе.

Для настройки клиентской ОС, выполните процедуру, описанную в разделе.

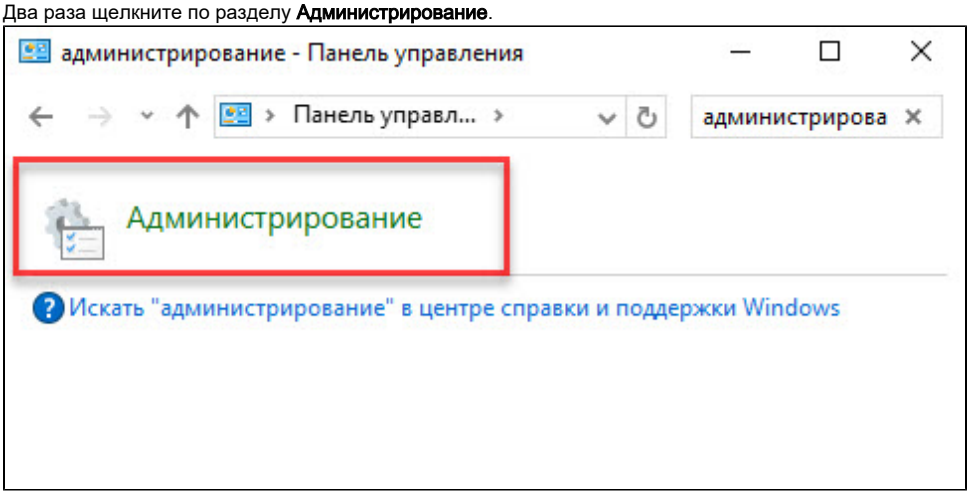
Настройка учетной записи пользователя

В первую очередь необходимо настроить учетные записи пользователей.

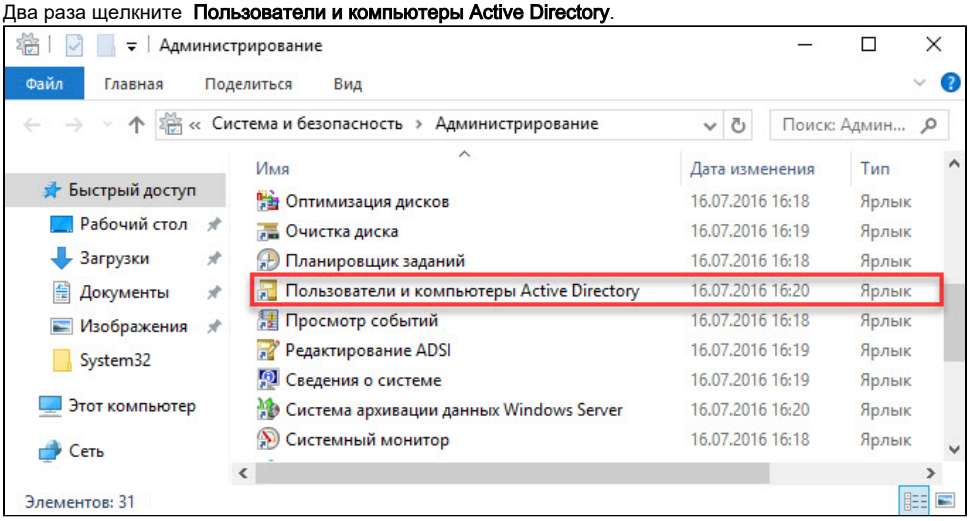
В этом примере будет настроена учетная запись **User** — пользователь домена, который включен только в группу **Пользователи домена**.

Для настройки учетной записи пользователя:

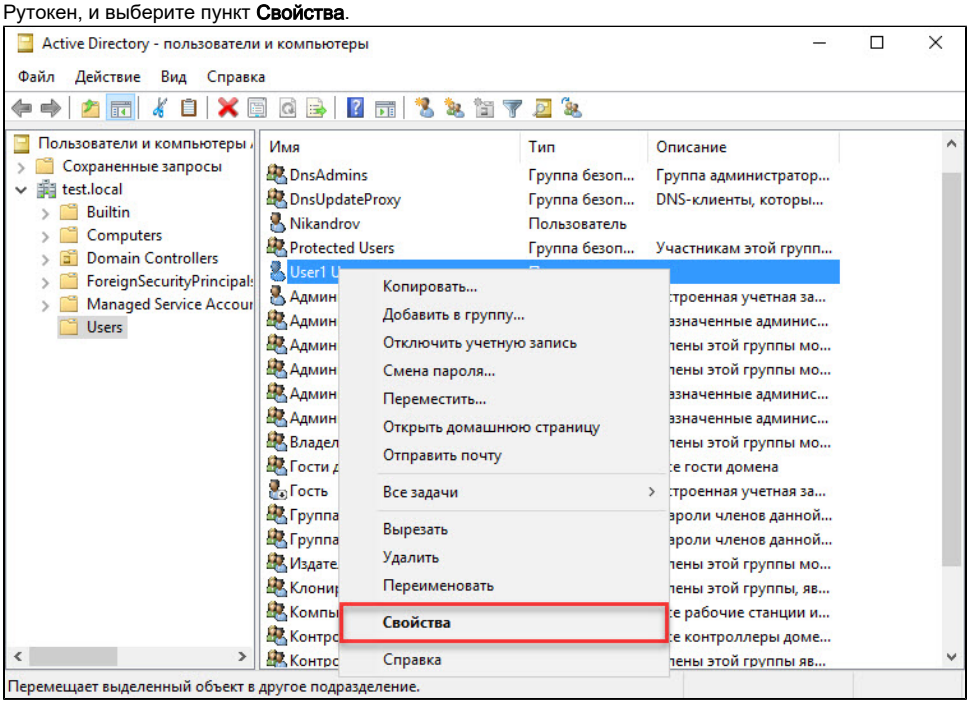
1. Откройте **Панель управления**.
2. В поле поиска введите "администрирование".
3. Два раза щелкните по разделу **Администрирование**.



4. Два раза щелкните **Пользователи и компьютеры Active Directory**.

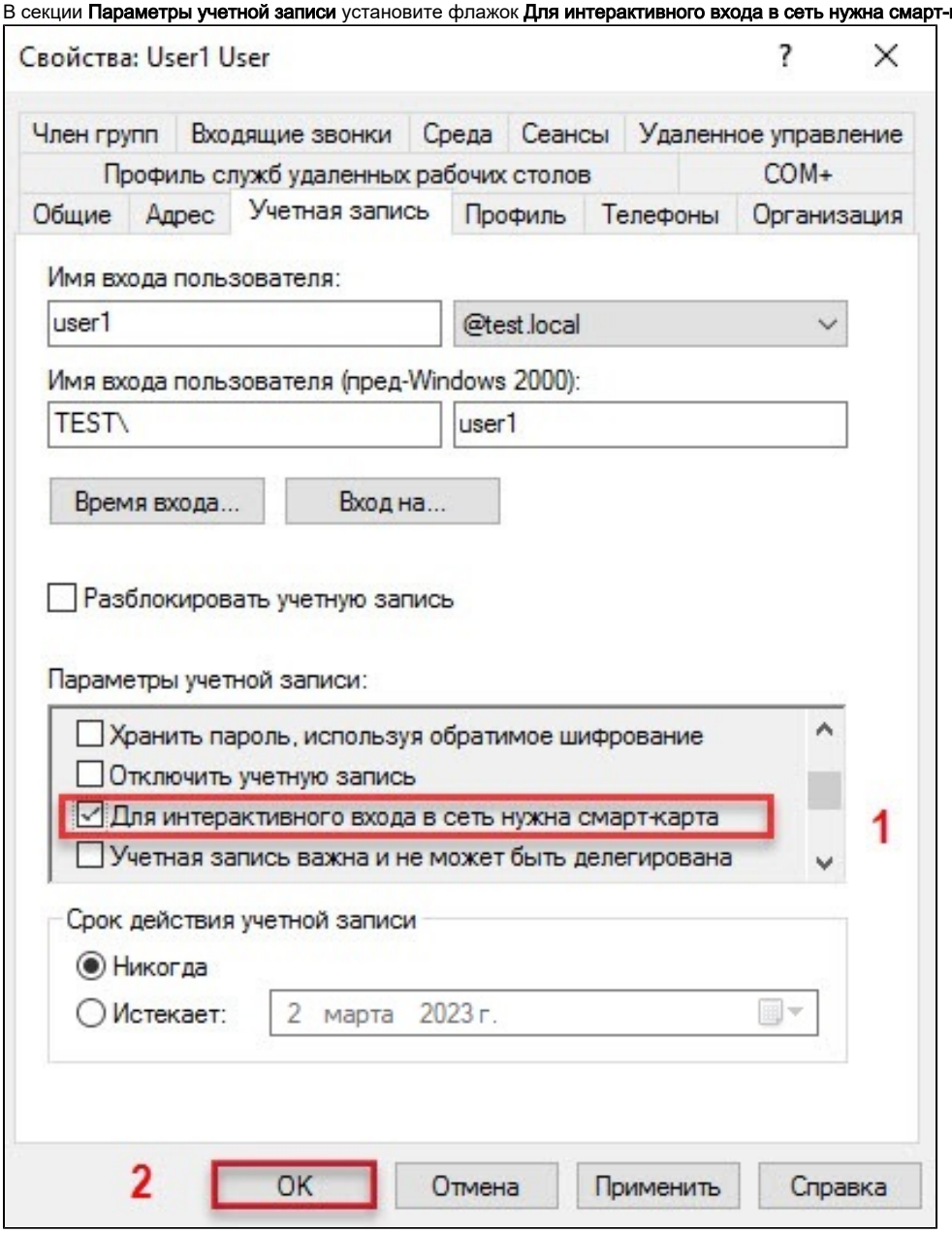


5. В левой части окна оснастки щелкните по папке **Users**.
6. Щелкните правой кнопкой мыши по имени пользователя, которому будет разрешено входить в домен только при наличии устройства Рутокен, и выберите пункт **Свойства**.



7. В окне свойств пользователя перейдите на вкладку **Учетная запись**.

8. В секции **Параметры учетной записи** установите флажок **Для интерактивного входа в сеть нужна смарт-карта**. Нажмите **ОК**.



9. Закройте окно **Active Directory - пользователи и компьютеры**.

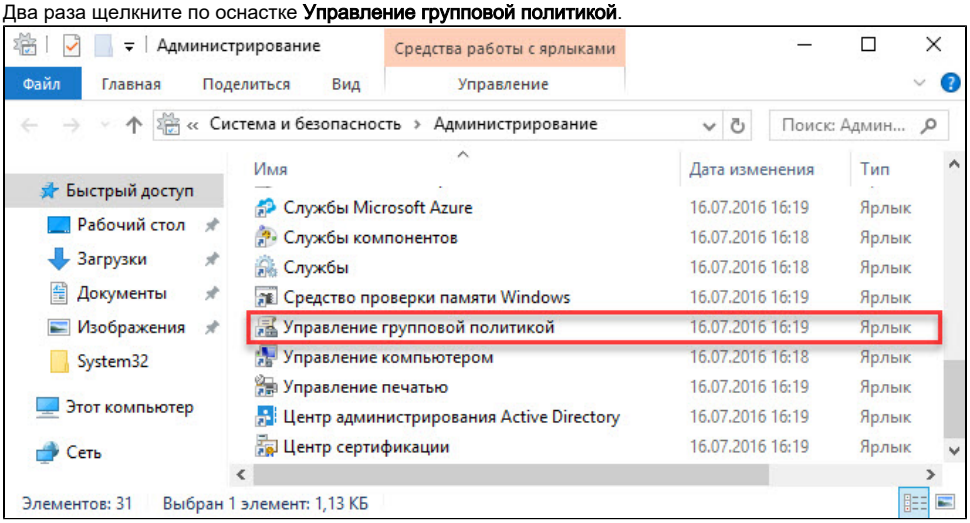
Настройка политик безопасности домена

Шаги 4-5 процедуры необходимо выполнять только в том случае, если всем пользователям будет запрещен вход в домен без устройства Рутокен с необходимым сертификатом.

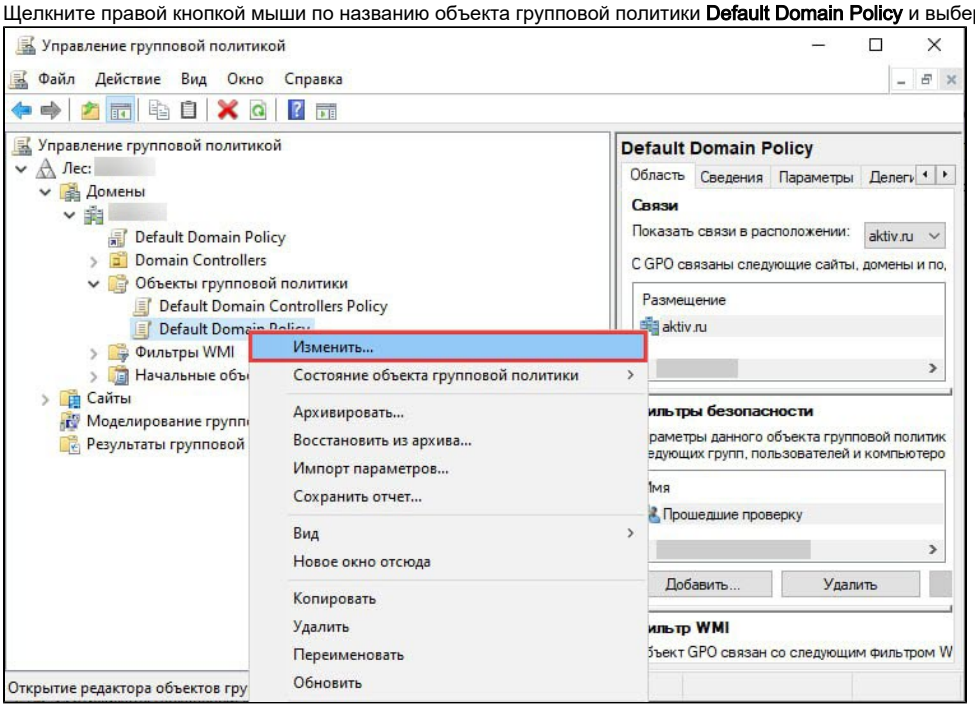
Для настройки политик безопасности:

1. Откройте **Панель управления**.
2. Два раза щелкните по разделу **Администрирование**.

3. Два раза щелкните по оснастке **Управление групповой политикой**.

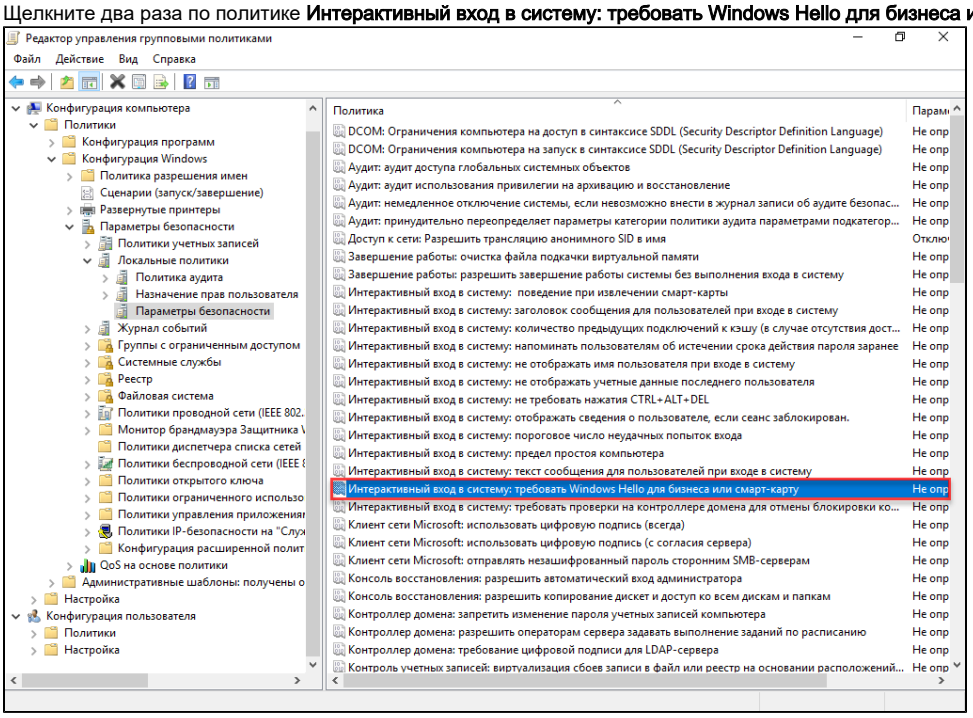


4. В окне **Управление групповой политикой** нажмите на категорию **Объекты групповой политики**.
5. Щелкните правой кнопкой мыши по названию объекта групповой политики **Default Domain Policy** и выберите пункт **Изменить...**



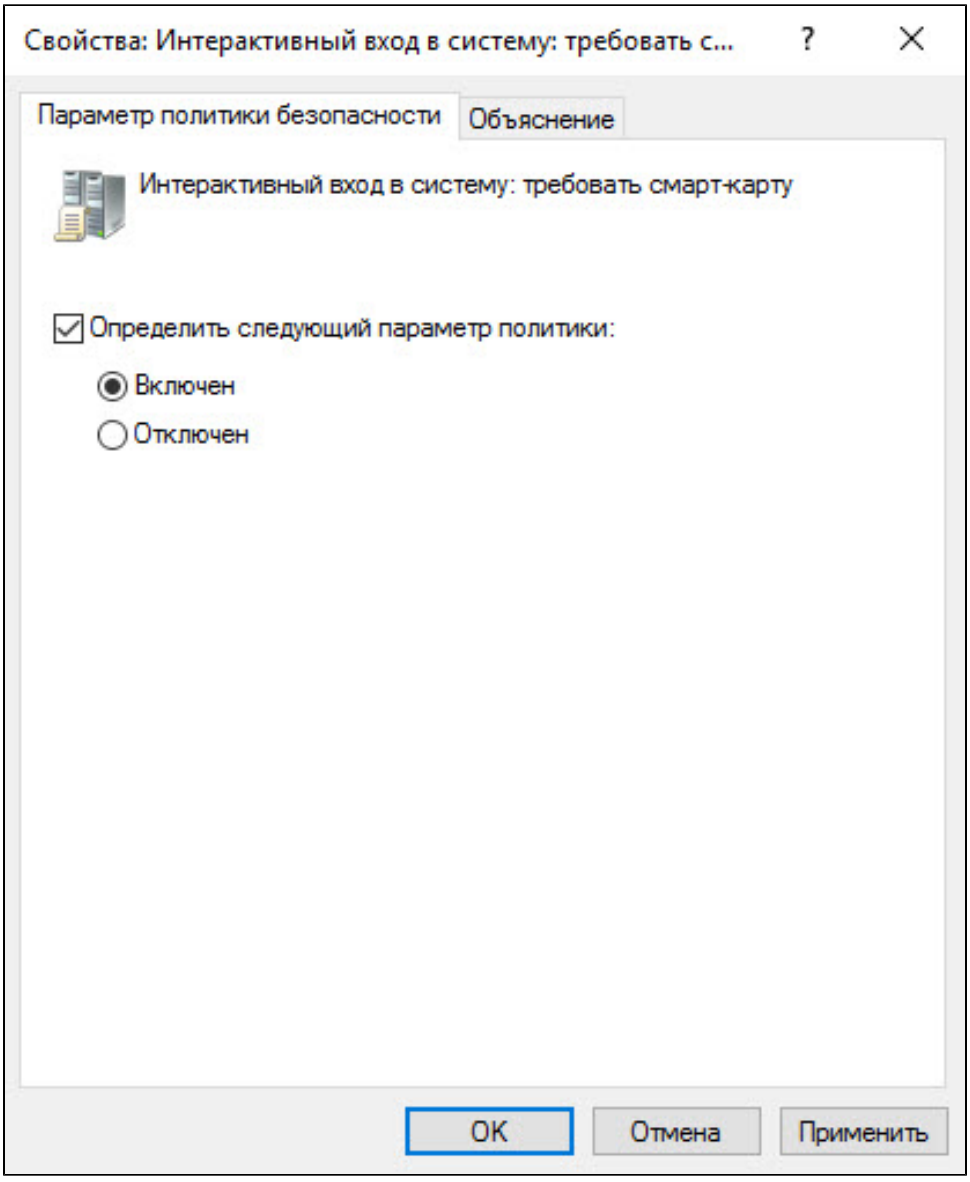
6. В окне **Редактор управления групповыми политиками** нажмите на пункт **Конфигурация Windows**.
7. Нажмите на пункт **Параметры безопасности**.
8. Нажмите на пункт **Локальные политики**.
9. Нажмите на пункт **Параметры безопасности**.

10. Щелкните два раза по политике **Интерактивный вход в систему: требовать Windows Hello для бизнеса или смарт- карту**.



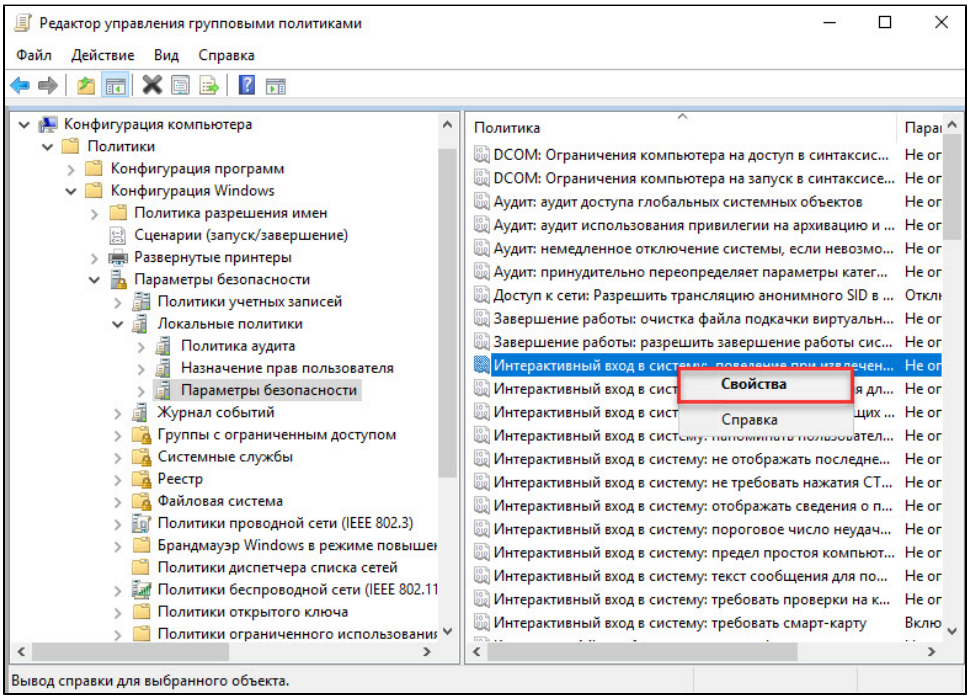
11. Установите флажок **Определить следующий параметр политики**.
12. Установите переключатель в положении **Включен**.

13. Нажмите **ОК**.



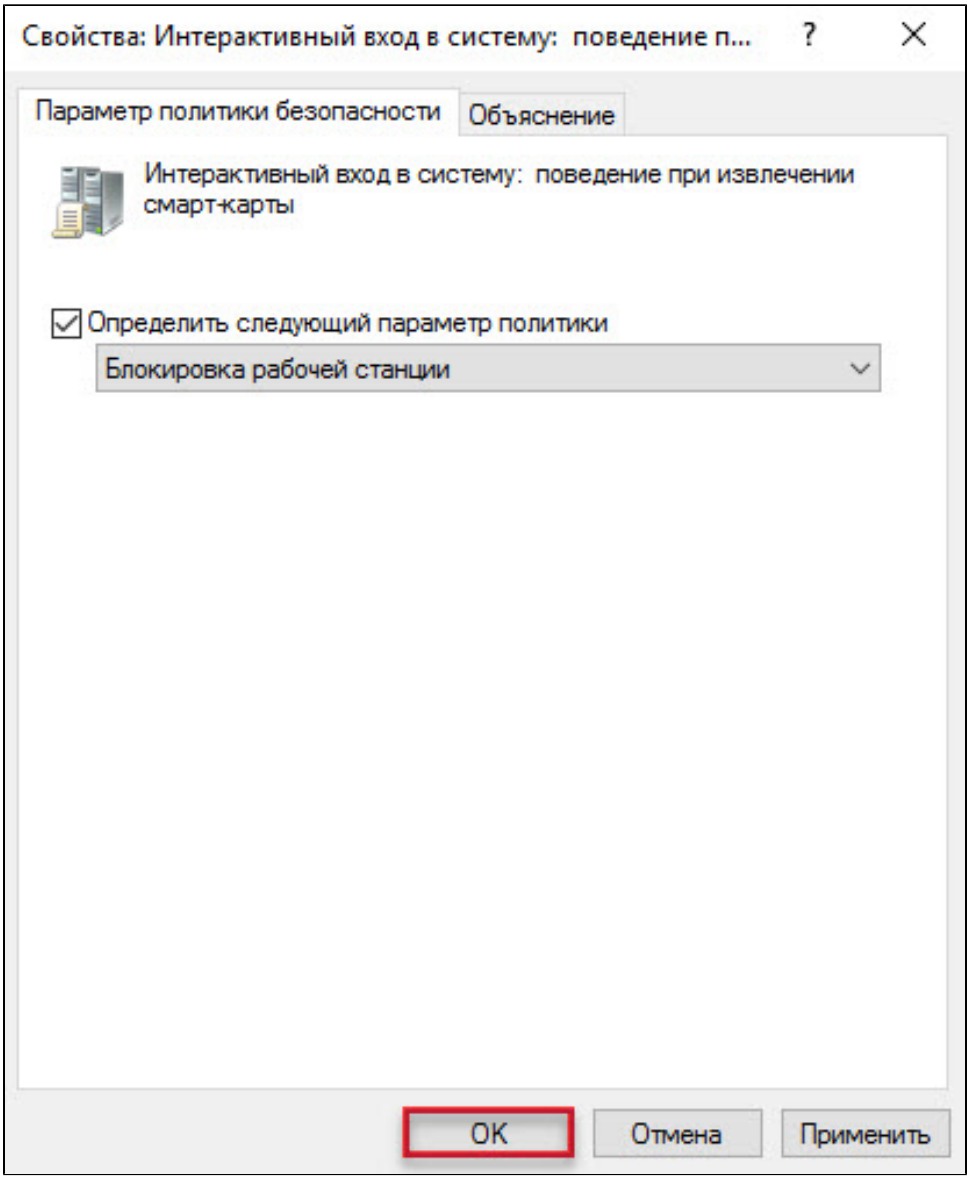
14. В окне **Редактор управления групповыми политиками** нажмите на пункт **Конфигурации Windows**.
15. Нажмите на подпункт **Параметры безопасности**.
16. Нажмите на пункт **Локальные политики**.
17. Щелкните по подпункту **Параметры безопасности**.

18. Щелкните правой кнопкой мыши по политике **Интерактивный вход в систему: поведение при извлечении смарт-карты** и выберите пункт **Свойства**.



19. Установите флажок **Определить следующий параметр политики**.
20. Из раскрывающегося списка выберите поведение клиентской ОС при отсоединении устройства Рутокен в процессе открытого пользовательского сеанса. В данном примере выбрано поведение ОС — **Блокировка рабочей станции**.

21. Нажмите **ОК**.



22. Закройте окно **Редактор управления групповыми политиками**.
23. Закройте **Панель управления**.
24. Перезагрузите компьютер.

Настройка клиентской операционной системы

Компьютеры с установленными клиентскими операционными системами **Windows 11/10/8.1/8/7/Vista/XP/2000** необходимо ввести в домен и установить на них **драйверы Рутокен**.

Редакции ОС должны включать возможность присоединения к домену.

Если клиентские компьютеры были загружены во время настройки сервера, то необходимо их перезагрузить.

Теперь пользователи, которым выдан сертификат типа **Пользователь со смарт-картой** или **Вход со смарт-картой**, смогут входить в домен только при подключении к компьютеру устройства Рутокен с этим сертификатом.
При извлечении устройства Рутокен в процессе открытого пользовательского сеанса, клиентская ОС будет автоматически заблокирована (в ОС **Windows 11/10/8.1/8/7/Vista** для блокировки рабочего стола при отключении устройства Рутокен необходимо установить автоматический запуск службы **Политика удаления смарт-карт/Smart Card Removal Policy**).