

3.1.1.2 Настройка входа в домен по предъявлению токена

Раздел содержит инструкцию по настройке входа в домен по предъявлению токена в операционной системе **Windows Server 2012 R2**.

Для настройки необходим компьютер с установленной операционной системой **Windows 2012 R2 Server Rus** и драйверами **Рутокен**, а также **дистрибутив этой ОС**.

Операционная система должна быть настроена как **Контроллер домена**, должны быть установлены **Службы Сертификации**, а 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**.

Этапы входа в домен по предъявлению токена:

1 этап: Настройка учетных записей пользователей.

2 этап: Настройка политик безопасности домена.

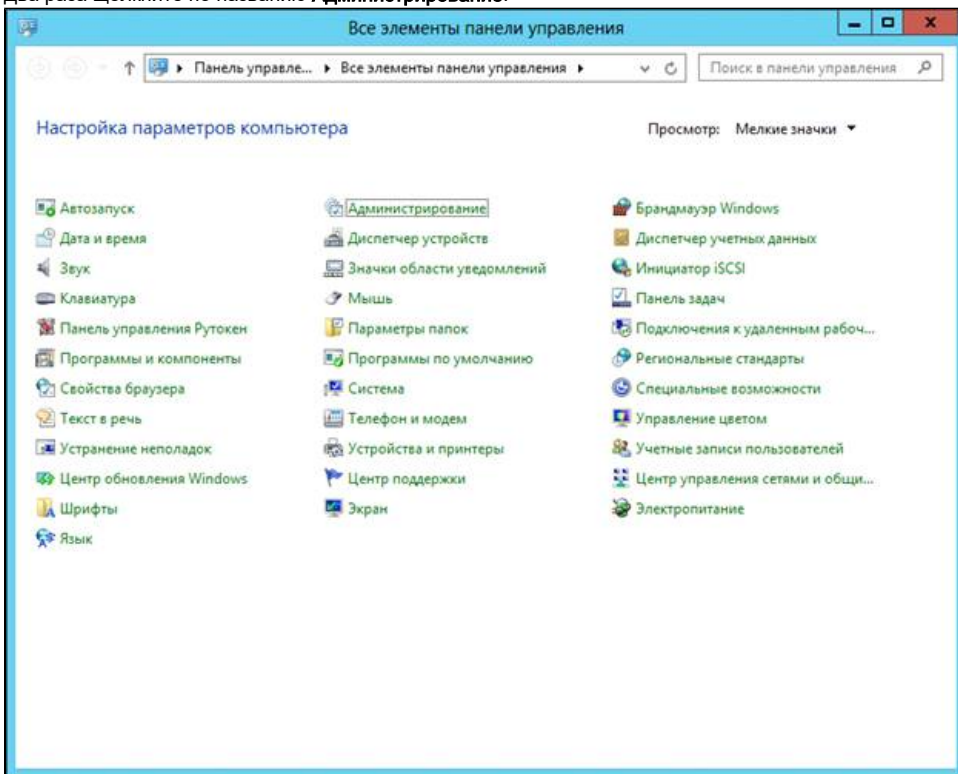
3 этап: Настройка клиентской операционной системы.

Настройка учетных записей пользователей

В первую очередь необходимо настроить учетные записи пользователей. В этом примере будет настроена учетная запись **User** — пользователь домена, включенный только в группу **Пользователи домена**.

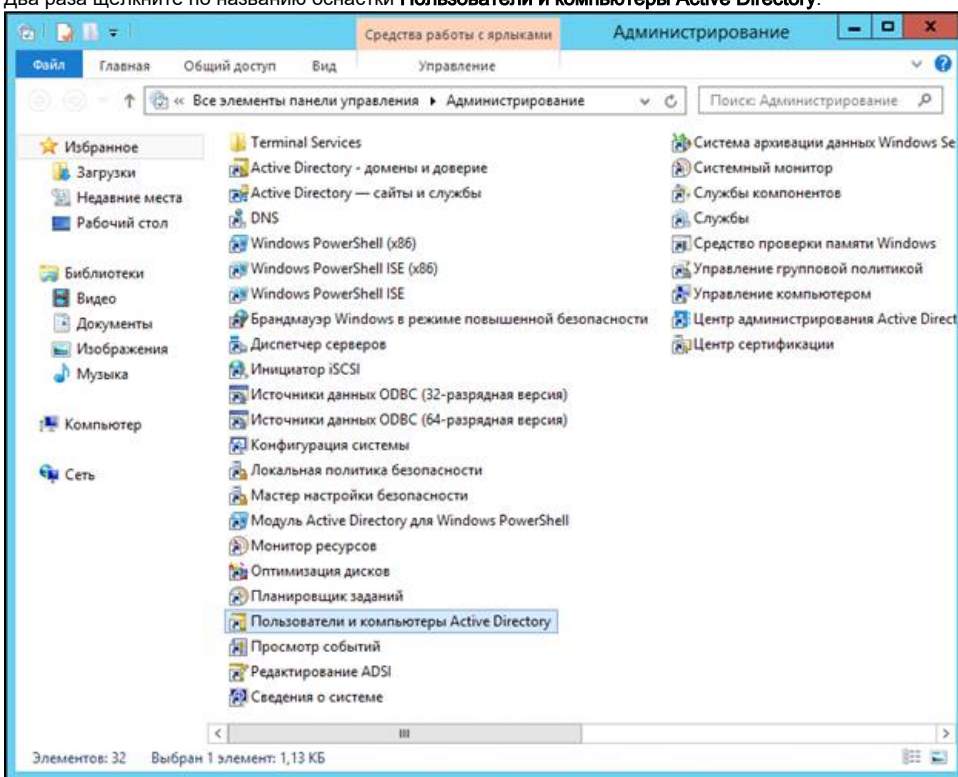
Для настройки учетной записи пользователя:

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

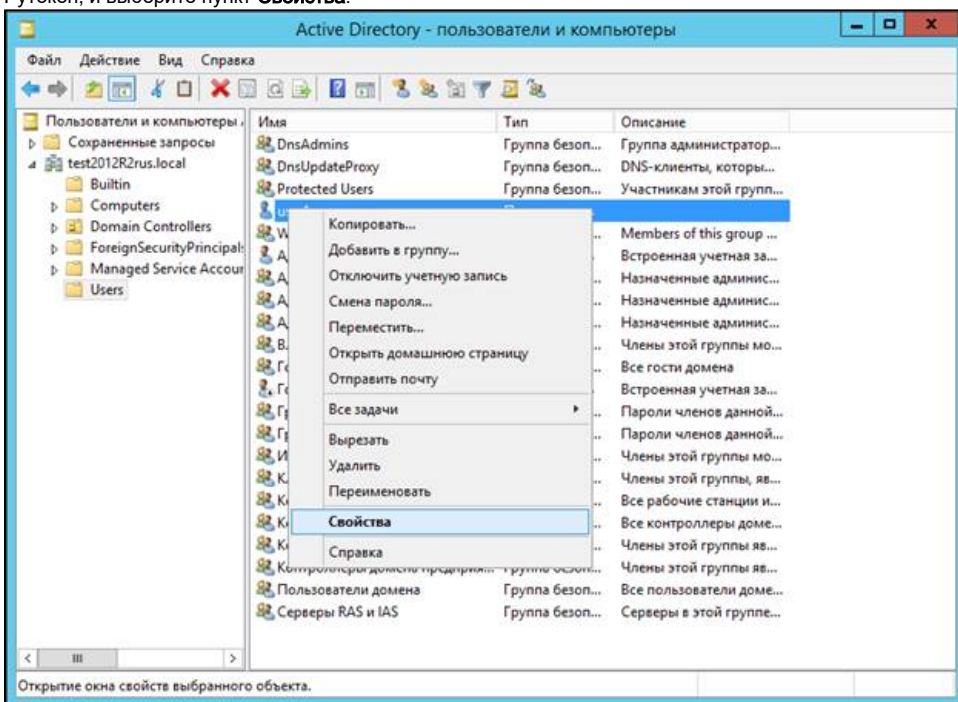


В домене под управлением **Windows Server 2012 R2** есть возможность одним действием запретить всем входить в домен без наличия устройства Рутокен с необходимым сертификатом (пользователь с учетной записью **Administrator** также не сможет войти в домен без устройства Рутокен). Шаги 2-5 данной инструкции необходимо выполнить только в том случае, если в домене будут пользователи не только с устройствами Рутокен, но и использующие альтернативные способы аутентификации (пароли, биометрические данные и т. д.). При этом шаги 9-10 надо пропустить.

3. Два раза щелкните по названию оснастки **Пользователи и компьютеры Active Directory**.



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



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

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

The screenshot shows the 'Properties: user1' dialog box with the 'Account' tab selected. The 'Interactive logon: require smart card' checkbox is checked. The 'Name of the user to log on to' field contains 'user1' and the 'Domain' dropdown shows '@test2012R2rus.local'. The 'Name of the user to log on to (pre-Windows 2000)' field contains 'TEST2012R2RUS\' and the 'Password' field contains 'user1'. The 'Time limit for logon' button is disabled. The 'Log on' button is enabled. The 'Unlock account' checkbox is unchecked. The 'Account parameters' section shows the 'Disable account' checkbox unchecked, the 'Interactive logon: require smart card' checkbox checked, the 'Account is important and cannot be delegated' checkbox unchecked, and the 'Use Kerberos DES encryption types for this' checkbox unchecked. The 'Expiration date of account' section shows the 'Never' radio button selected and the 'Expires on' date set to '15 января 2015 г.'.

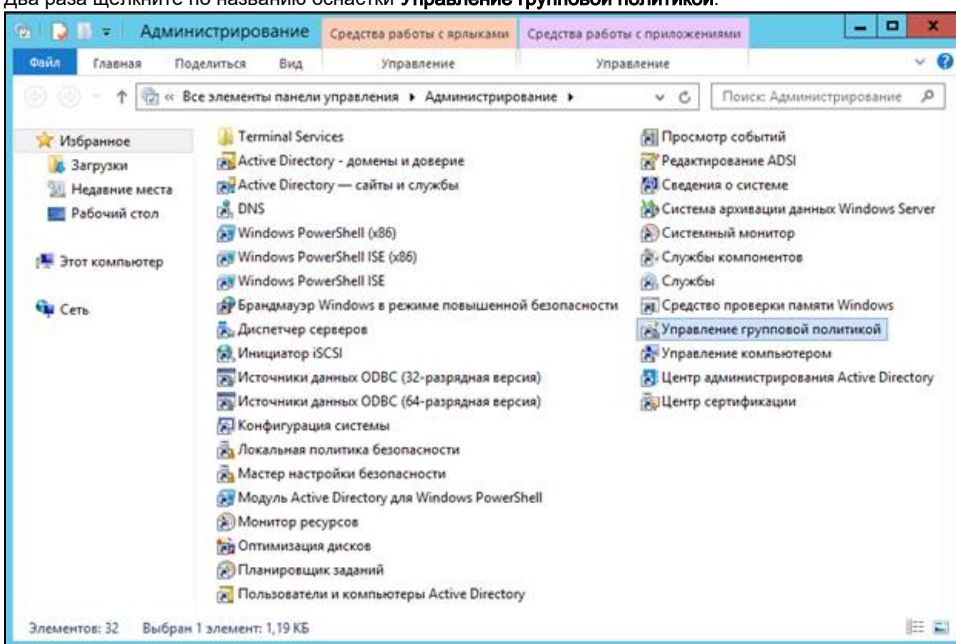
8. Закройте окно **Active Directory - пользователи и компьютеры**.
9. Аналогичным образом настройте другие учетные записи в домене. Для таких пользователей вход в домен будет доступен только при наличии устройства Рутокен с сертификатом, выданным администратором домена.

Настройка политик безопасности домена

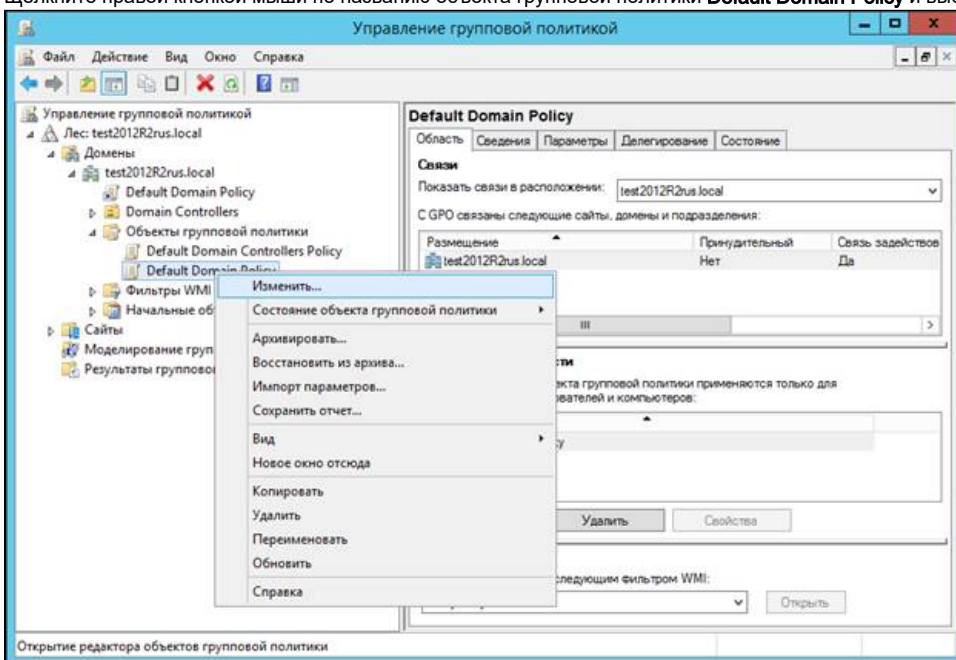
Для настройки политик безопасности:

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

3. Два раза щелкните по названию оснастки **Управление групповой политикой**.



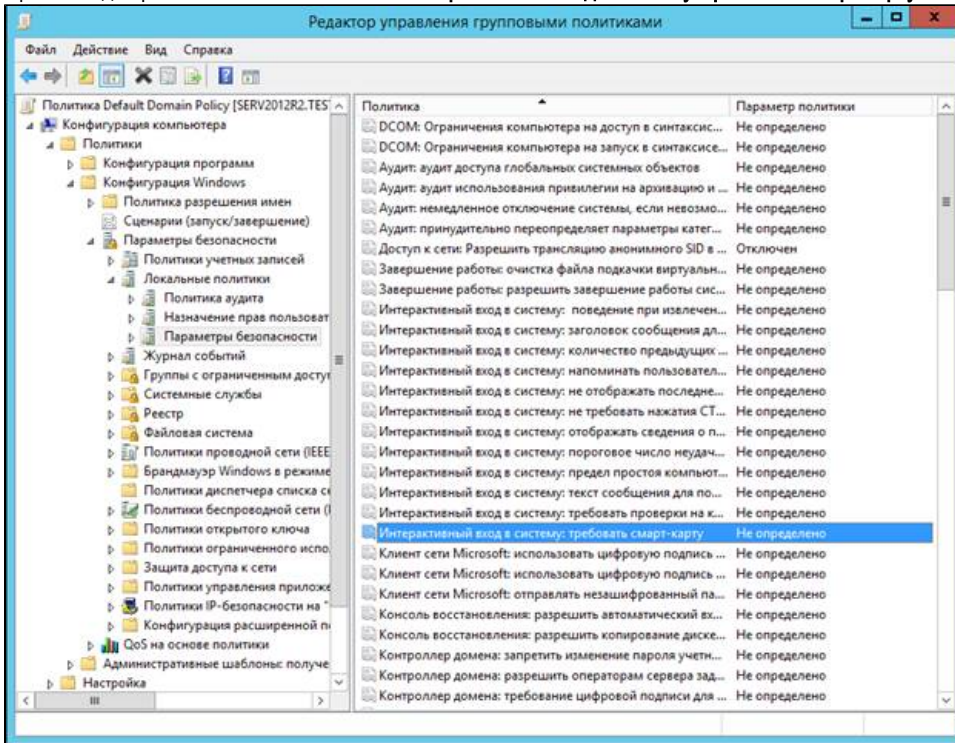
4. В окне **Управление групповой политикой** рядом с названием категории **Объекты групповой политики** щелкните по стрелочке.
5. Щелкните правой кнопкой мыши по названию объекта групповой политики **Default Domain Policy** и выберите пункт **Изменить...**



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

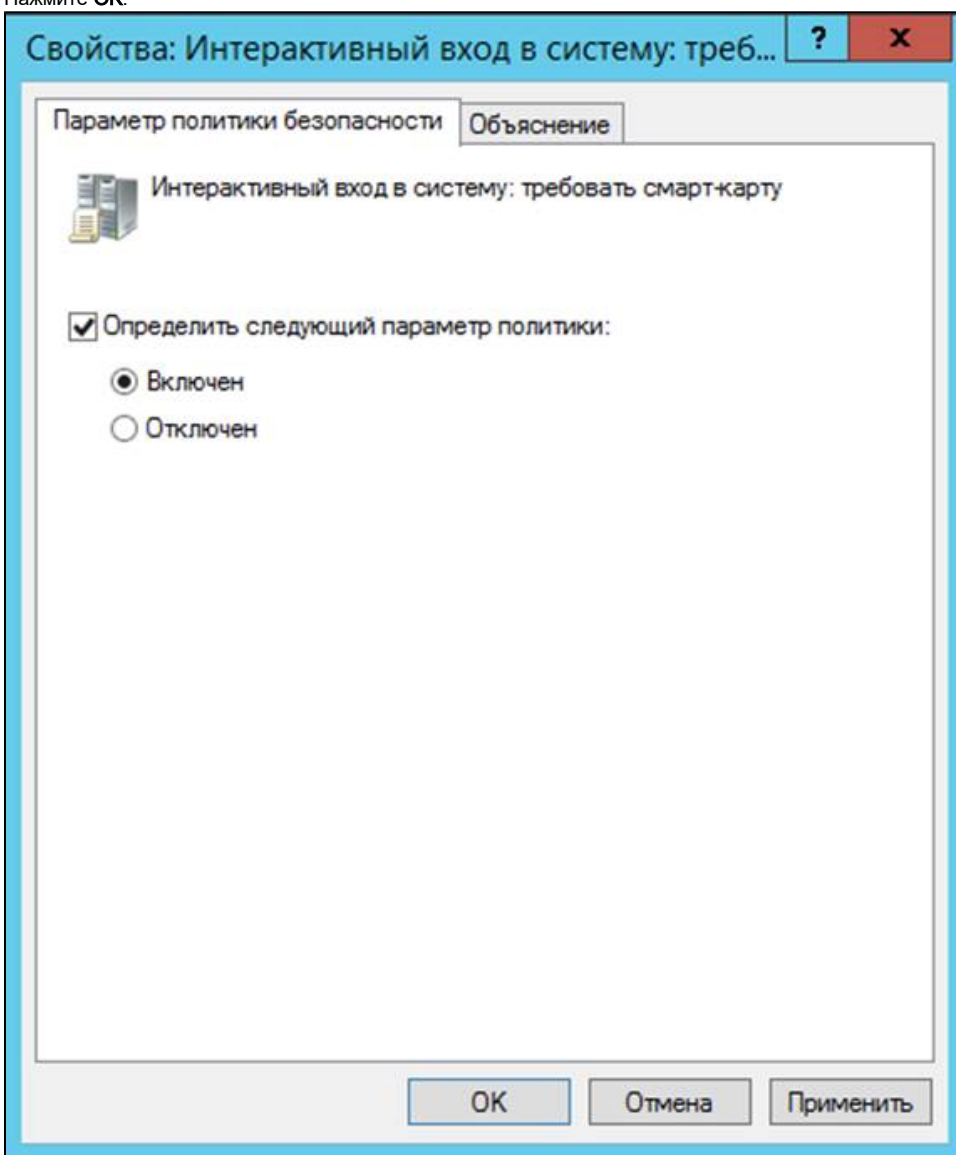
6. В окне **Редактор управления групповыми политиками** рядом с названием пункта **Конфигурация Windows** щелкните по стрелочке.
7. Рядом с названием пункта **Параметры безопасности** щелкните по стрелочке.
8. Рядом с названием пункта **Локальные политики** щелкните по стрелочке.
9. Щелкните по названию пункта **Параметры безопасности**.

10. Щелкните два раза по названию политики **Интерактивный вход в систему: требовать смарт-карту**.



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

13. Нажмите **OK**.



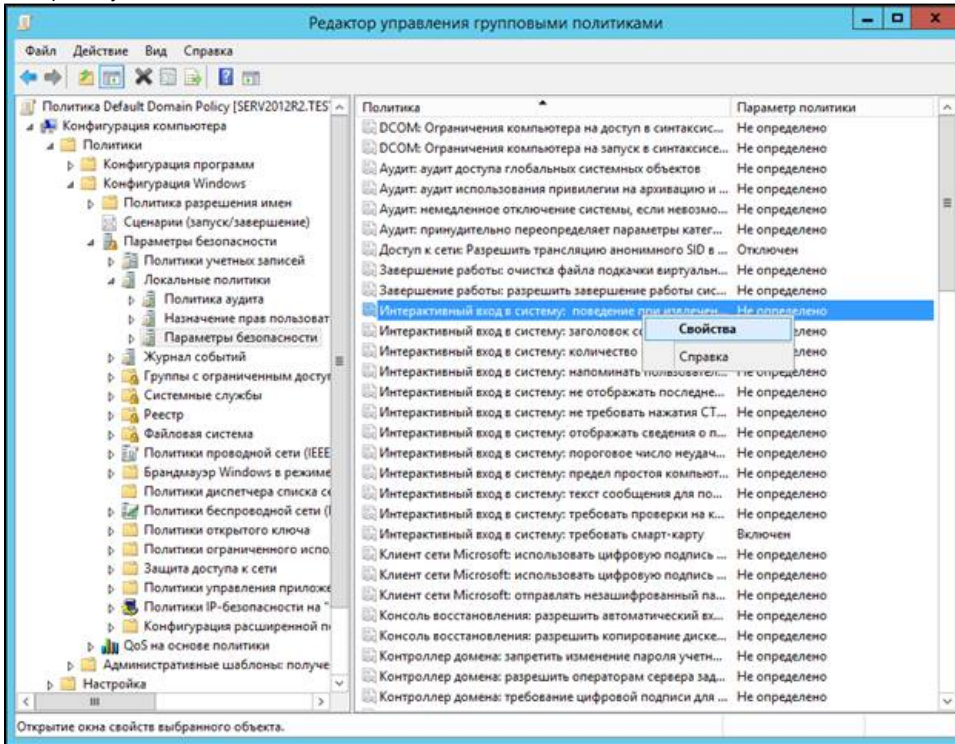
14. В окне **Редактор управления групповыми политиками** рядом с пунктом **Конфигурации Windows** щелкните по стрелочке.

15. Рядом с названием подпункта **Параметры безопасности** щелкните по стрелочке.

16. Рядом с названием **Локальные политики** щелкните по стрелочке.

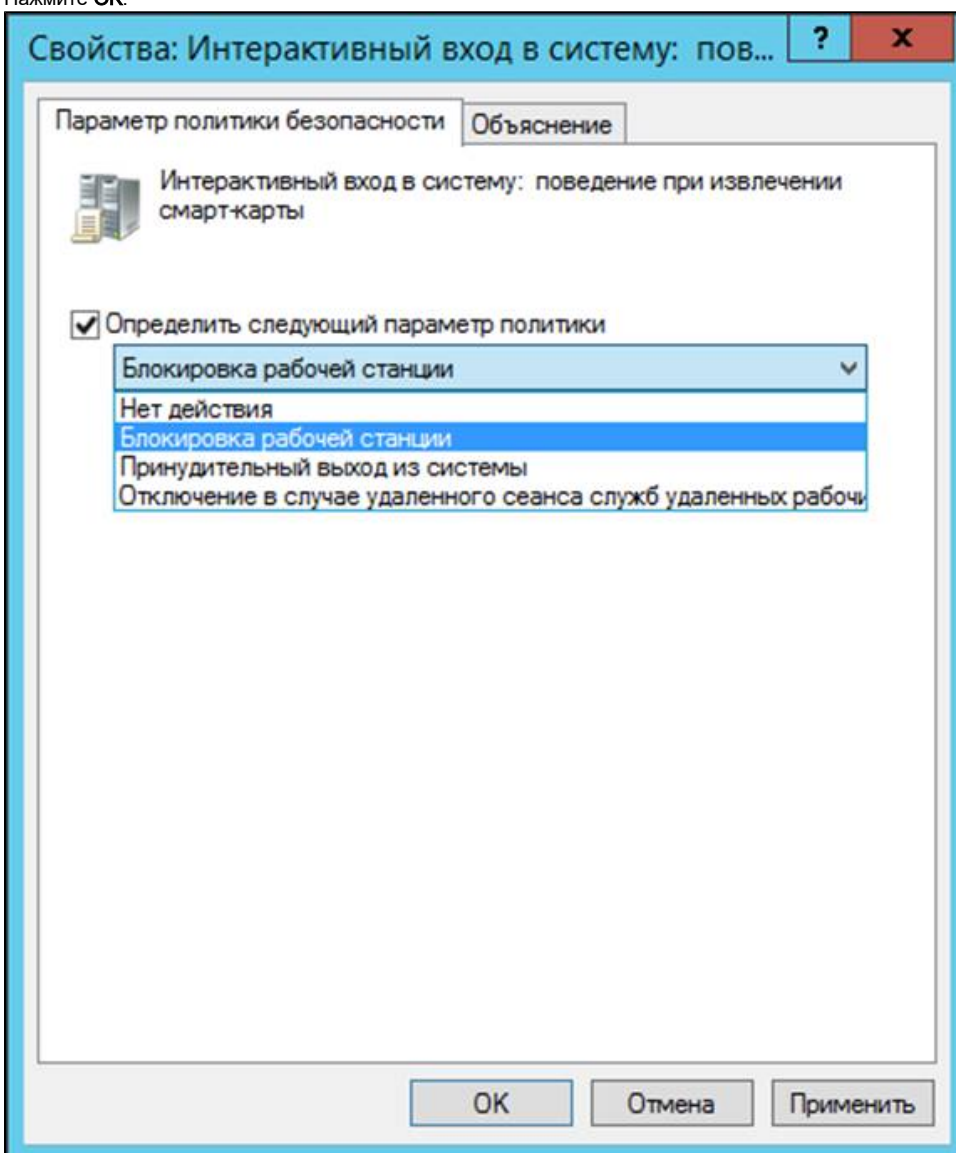
17. Щелкните по названию подпункта **Параметры безопасности**.

18. Щелкните правой кнопкой мыши по названию политики **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**.

Настройка будет доступна только после перезагрузки компьютера. Настройка серверной операционной системы после этого будет завершена.

Настройка клиентской операционной системы

Компьютеры с установленными клиентскими операционными системами **Windows 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 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**).