Средство защиты информации

«SecurePackRus»

Версия 3.0

Руководство администратора безопасности

EAPM.5090005.032-03 90 01

Листов 31

Компания «СиЭйЭн»

2016

Компания «СиЭйЭн»
Адрес 107140, г. Москва, Московско-Казанский пер., д. 11-15
Телефон +7 (495) 666-5606
e-mail info@cansec.ru
Web www.cansec.ru

Оглавление

Список сокращений

АИС	Автоматизированная информационная система
АРМ	Автоматизированное рабочее место
АС	Автоматизированная система
ЗПС	Замкнутая программная среда
ИС	Информационная система
НСД	Несанкционированный доступ
ОС	Операционная система
ПАК	Программно-аппаратный комплекс
ПКЗИ	Подсистема криптографической защиты информации
ПО	Программное обеспечение
ППО	Прикладное программное обеспечение
СЗИ	Средство или система защиты информации
СКЗИ	Средство криптографической защиты информации
СХКИ	Средство хранения конфиденциальной информации

1. Введение

Данное руководство предназначено для администраторов средства защиты информации «SecurePackRus» версия 3.0 (сокращенные названия изделия – SecurePackRus 3.0 или SPR 3.0).В руководстве содержатся сведения, необходимые администраторам для настройки и управления основными механизмами защиты.

2. Политики защиты критических ресурсов

2.1. Защита объектов файловой системы

После первоначальной установки SPR 3.0 политика защиты объектов файловой системы включена в режиме Аудит. Контроль доступа пользователей ккритическим объектам файловой системы не производится!

При первоначальной установке SPR3.0 список правил доступа к съемным носителям пуст, поэтому активация политики приведет к полной блокировке всех классов съемных носителей. После установки SPR3.0 и создания базового набора правил доступа необходимо включить контроль за подключением съемных носителей.

При первоначальной установке SPR3.0 список правил защиты объектов файловой системы пуст, поэтому активация политики не приводит к блокировке модификации каких либо областей файловой системы.

Для изменения режима работы политики необходимо:

- раскрыть в консоли управления политиками следующий путь: *Конфигурация компьютера →Политики →Конфигурация Windows→Параметры безопасности →Политики SecurePackRus→Защита критических ресурсов→Файловая системаи*, вызвав меню, выбрать радел «Свойства»и в открывшемся окне отметить пункт «Активировать действие правил» (рис.1)

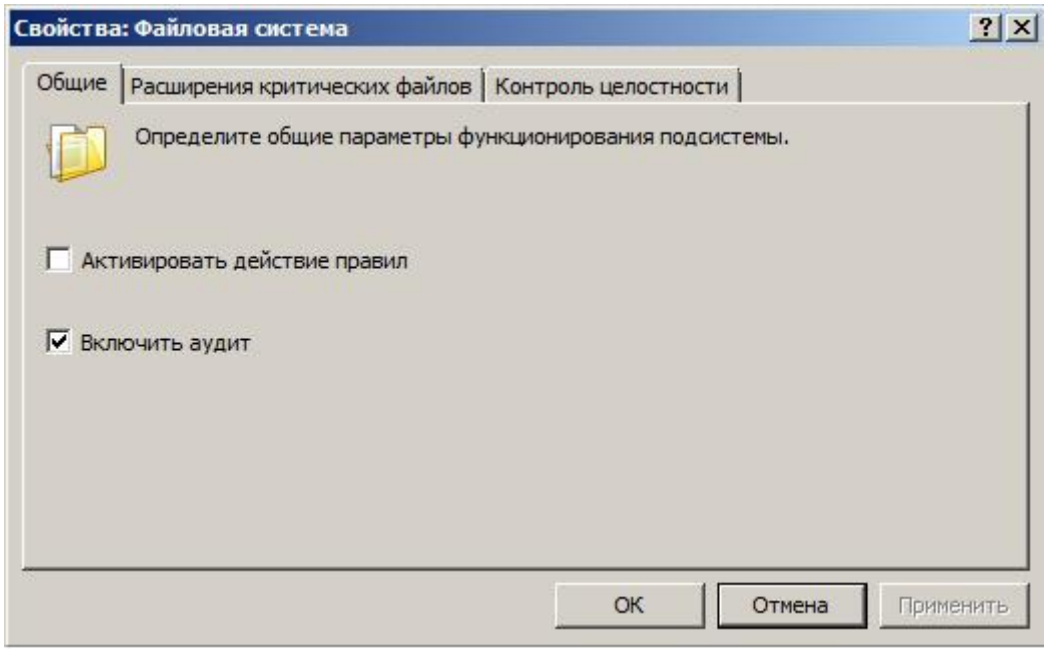


Рис.1

Для изменения набора расширений критических файлов необходимо:

- раскрыть в консоли управления политиками следующий путь:*Конфигурация компьютера →Политики →Конфигурация Windows→Параметры безопасности →Политики SecurePackRus→Защита критических ресурсов→Файловая системаи*, вызвав меню, выбрать радел «Свойства», в открывшемся выбрать закладку «Расширения критических файлов» (рис. 2)

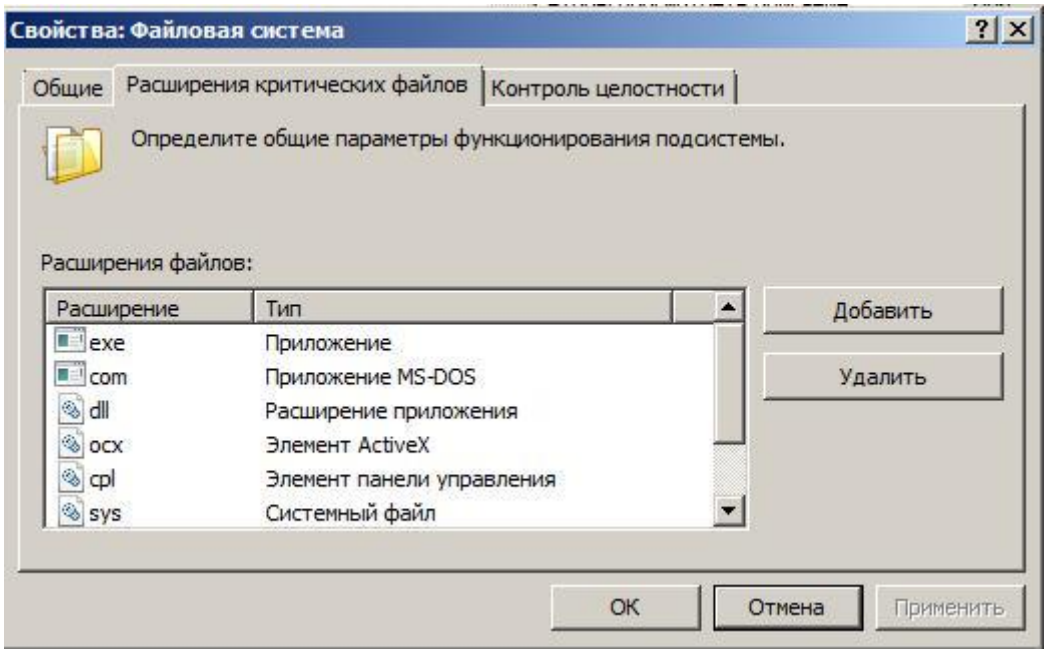


Рис.2

Для изменения параметров контроля целостности критических файлов необходимо:

- раскрыть в консоли управления политиками следующий путь:*Конфигурация компьютера →Политики →Конфигурация Windows→Параметры безопасности →Политики SecurePackRus→Защита критических ресурсов→Файловая системаи*, вызвав меню, выбрать радел «Свойства», в открывшемся выбрать закладку «Контроль целостности» (рис. 3)

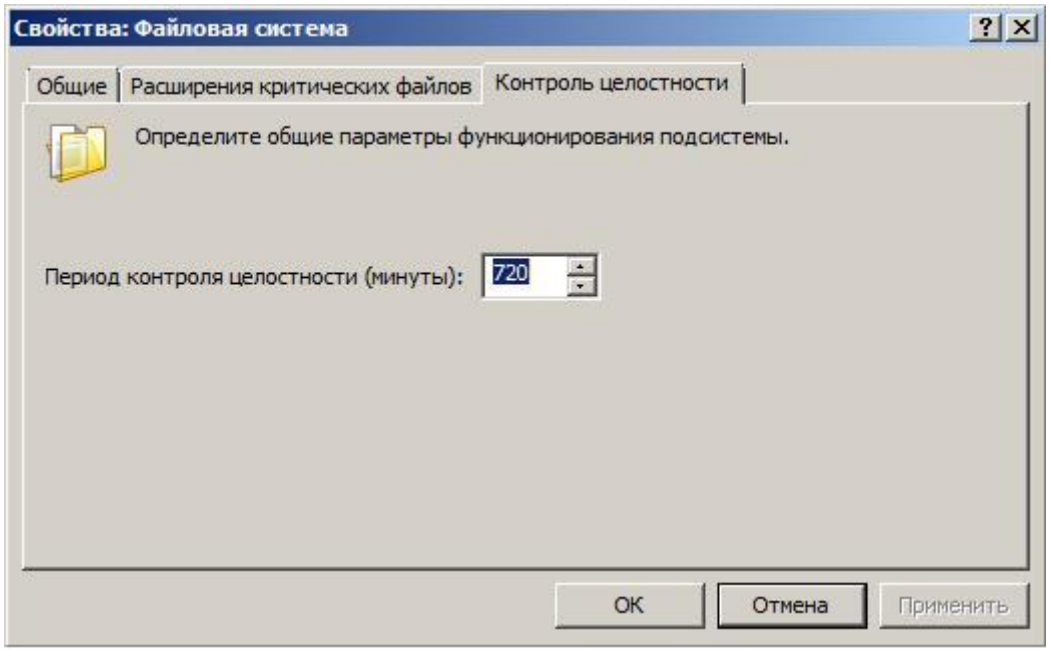


Рис. 3

2.1.1. Создание правил защиты объектов файловой системы

Правила защиты критических объектов файловой системы позволяют администраторам задавать директории, содержимое которых будет защищено от модификации и контролироваться на целостность.

Для настройки правила защиты критических объектов файловой системы необходимо:

- раскрыть в консоли управления политиками следующий путь: *Конфигурация компьютера →Политики →Конфигурация Windows→Параметры безопасности →Политики SecurePackRus→ Защита критических ресурсов→Файловая системаи*, вызвав меню, выбрать радел «Создать новое правило»(Рис. 4);
- Выбрать тип действия правила «Блокировать модификацию и контролировать целостность файлов»;
- Ввести необязательное описание правила;
- Перейти на следующую страницу (Рис.5)
- Ввести путь, который будет являть областью действия данного правила. Путь может быть введен как в явном виде, так и виде переменной среды.
- Нажать кнопку «Готово»

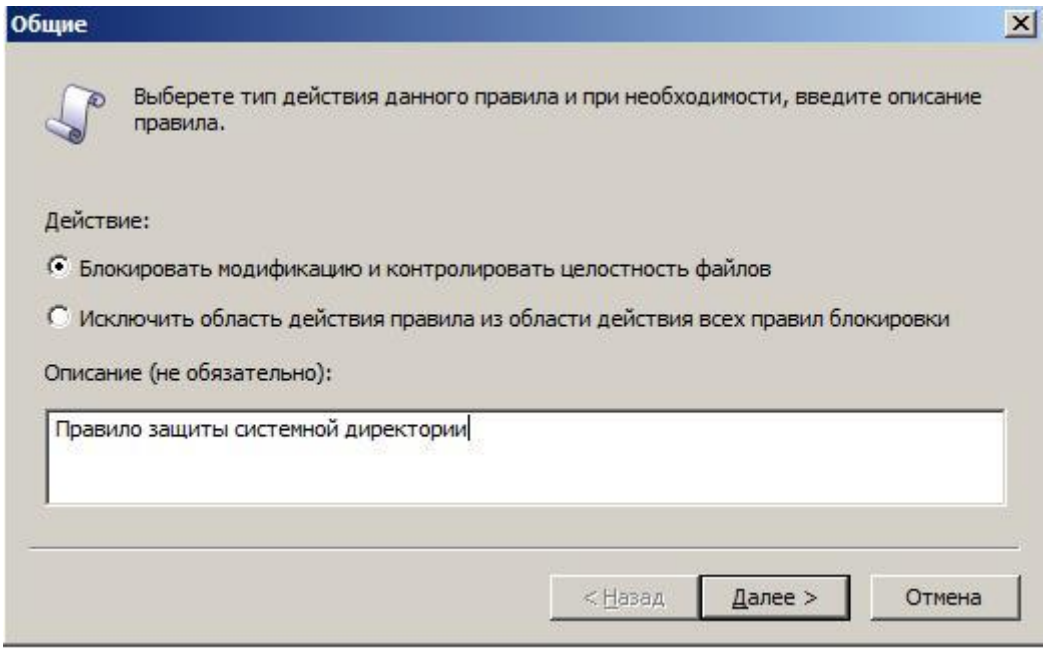


Рис 4

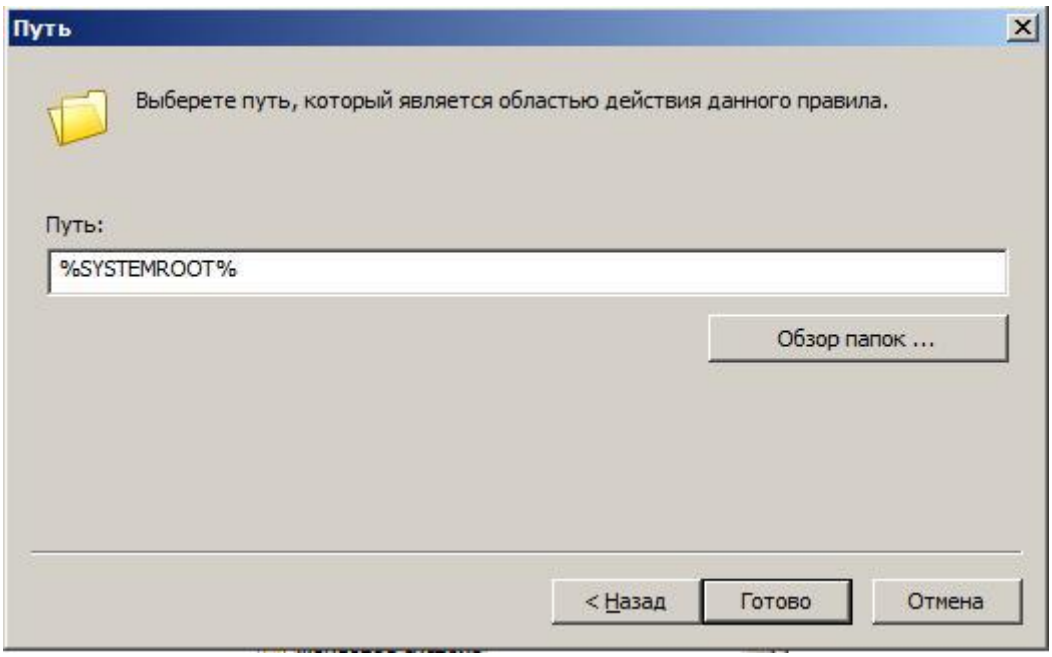


Рис 5

При возвращении в ММСконсоль для обновления визуализации списка правил нажмите кнопку F5.

Для настройки исключения из правил защиты критических объектов файловой системы необходимо:

- раскрыть в консоли управления политиками следующий путь: *Конфигурация компьютера →Политики →Конфигурация Windows→Параметры безопасности*

→*Политики SecurePackRus*→ *Защита критических ресурсов*→*Файловая системаи*, вызвав меню, выбрать радел «Создать новое правило»(Рис. 6);

- Выбрать тип действия правила «Исключить область действия правила из области действия всех правил блокировки»;
- Ввести необязательное описание правила;
- Перейти на следующую страницу (Рис.7)
- Ввести путь, который будет являть областью действия данного правила. Путь может быть введен как в явном виде, так и виде переменной среды.
- Нажать кнопку «Готово»

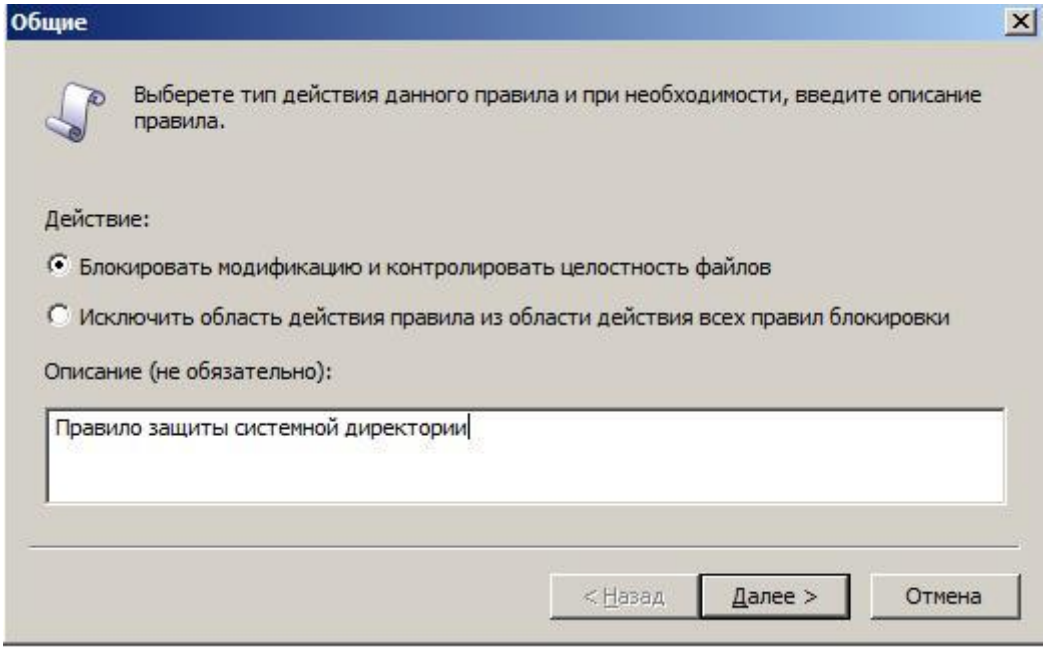


Рис 6

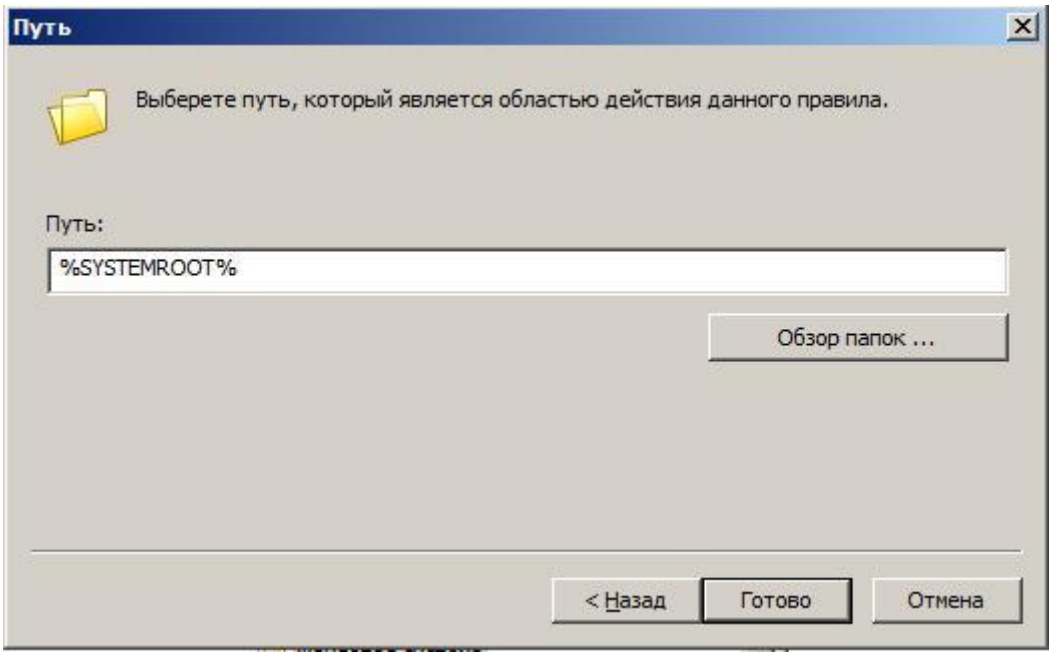


Рис 7

При возвращении в ММСконсоль для обновления визуализации списка правил нажмите кнопку F5 (рис. 8).

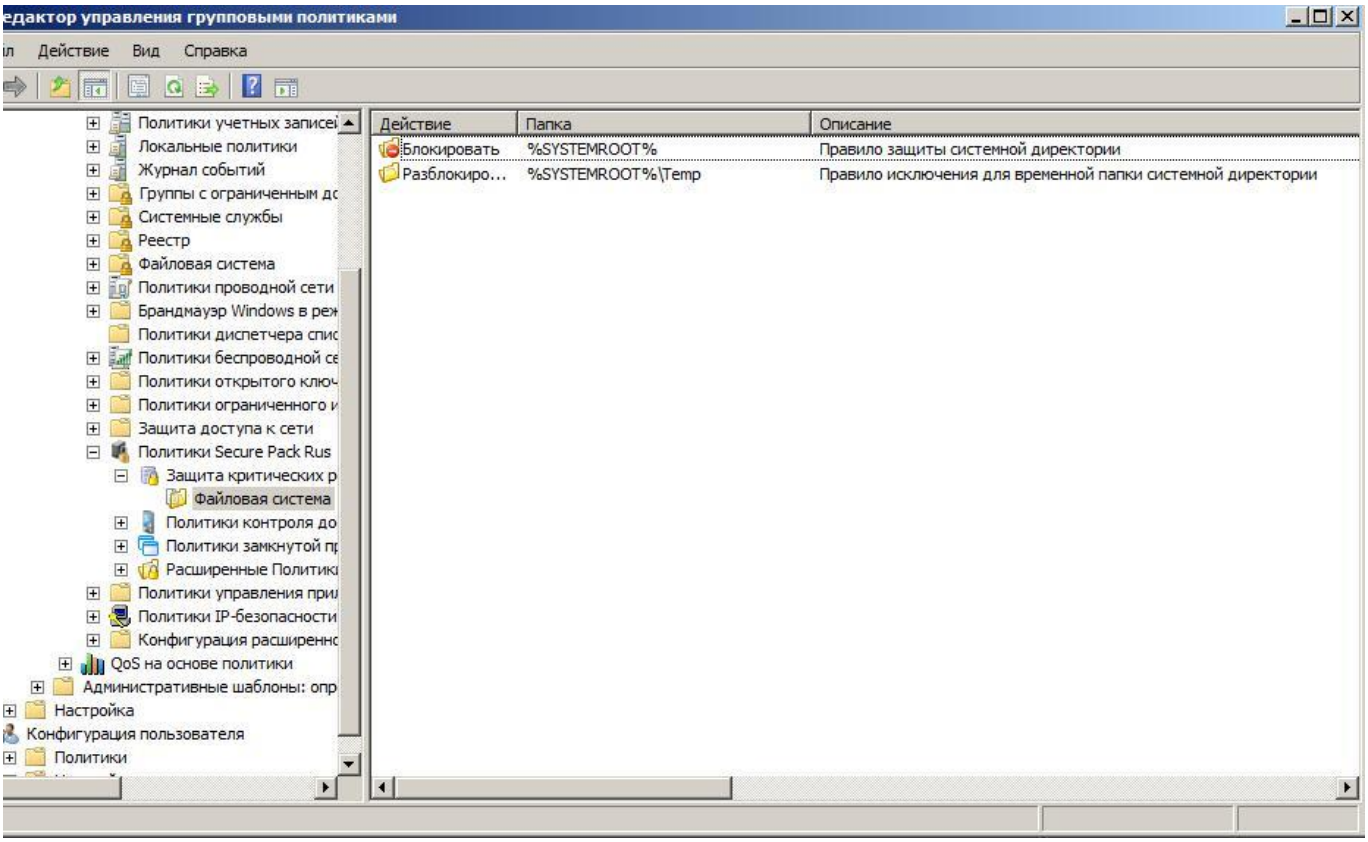


Рис. 8

3. Политики контроля доступа к устройствам

3.1. Управление доступом к съемным хранилищам данных

После первоначальной установки SPR 3.0 политика доступа к съемным носителям включена в режиме Аудит. Контроль доступа пользователей кинформации на съемных носителях в данном режиме не производится!

При первоначальной установке SPR3.0 список правил доступа к съемным носителям пуст, поэтому активация политики приведет к полной блокировке всех классов съемных носителей. После установки SPR3.0 и создания базового набора правил доступа необходимо включить контроль за подключением съемных носителей.

Для изменения режима работы политики доступа необходимо:

- раскрыть в консоли управления политиками следующий путь: *Конфигурация компьютера →Политики →Конфигурация Windows→Параметры безопасности →Политики SecurePackRus→Политика контроля доступа к устройствам →Съемные устройства* и, вызвав меню, выбрать радел «Свойства» (Рис. 9)

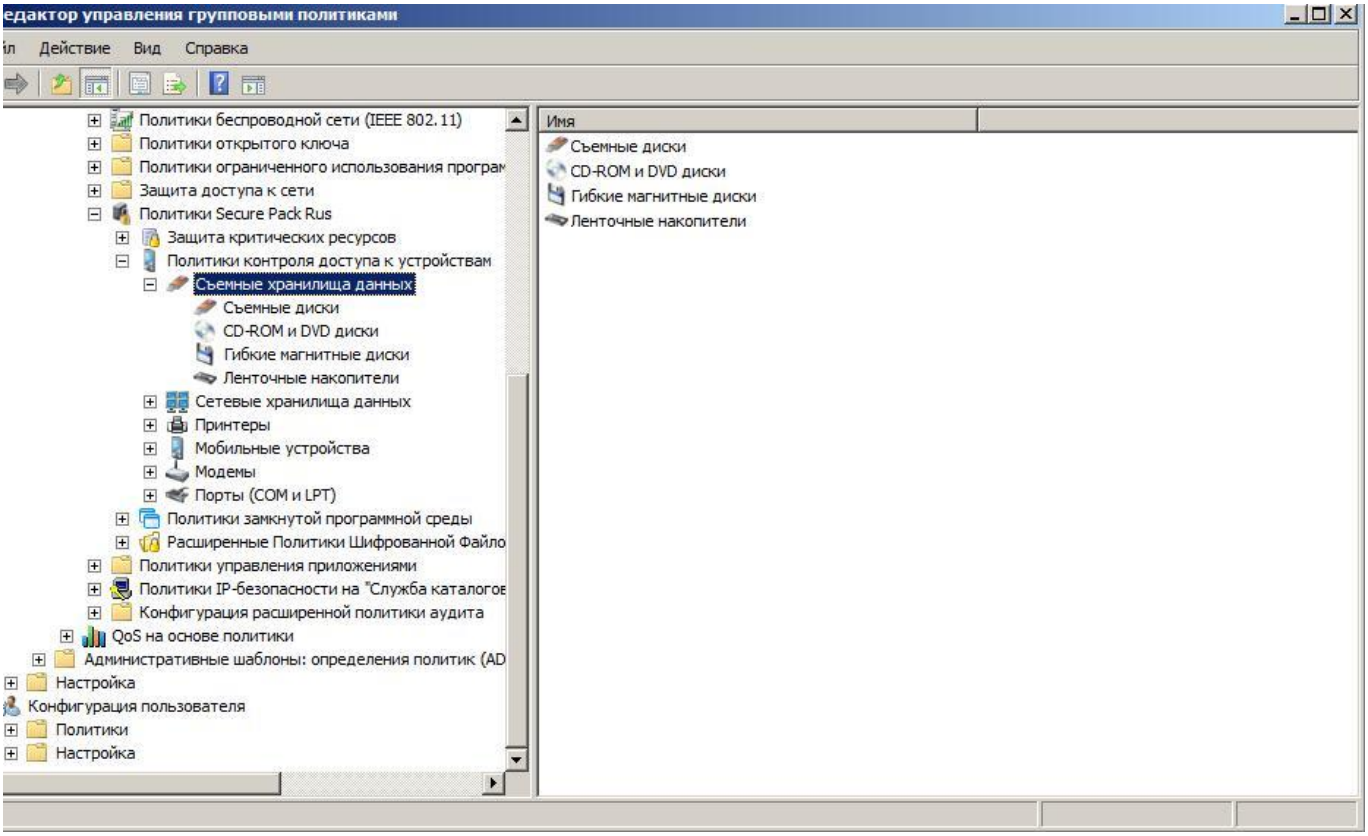


Рисунок 9 - Изменение режима работы политики

- в открывшемся окне отметить пункт «Активировать проверку разрешений» (Рис. 10)

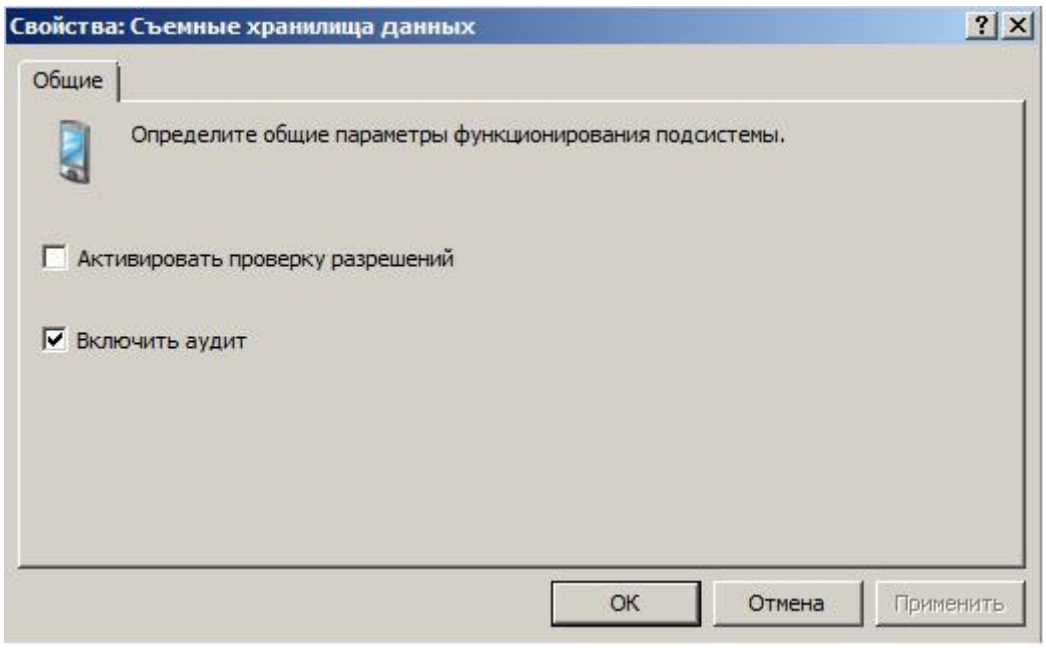


Рисунок 10 - Активация политики

Активация проверки разрешений при доступе пользователей к съемным носителям запретит любое действие, не разрешенное администратором правилами доступа к съемным носителям.

3.1.1. Создание правил доступа к съемным хранилищам данных

Правила доступа к съемным носителям позволяют администраторам задавать различные разрешения для пользователей и групп безопасности при работе с различными классами съемных носителей информации.

Для настройки правил доступа к съемным носителям необходимо раскрыть в консоли управления политиками следующий путь: *Конфигурация компьютера →Политики →Конфигурация Windows→Параметры безопасности →Политики SecurePackRus→Политика контроля доступа к устройствам→Съемные устройства* (Рис. 11).

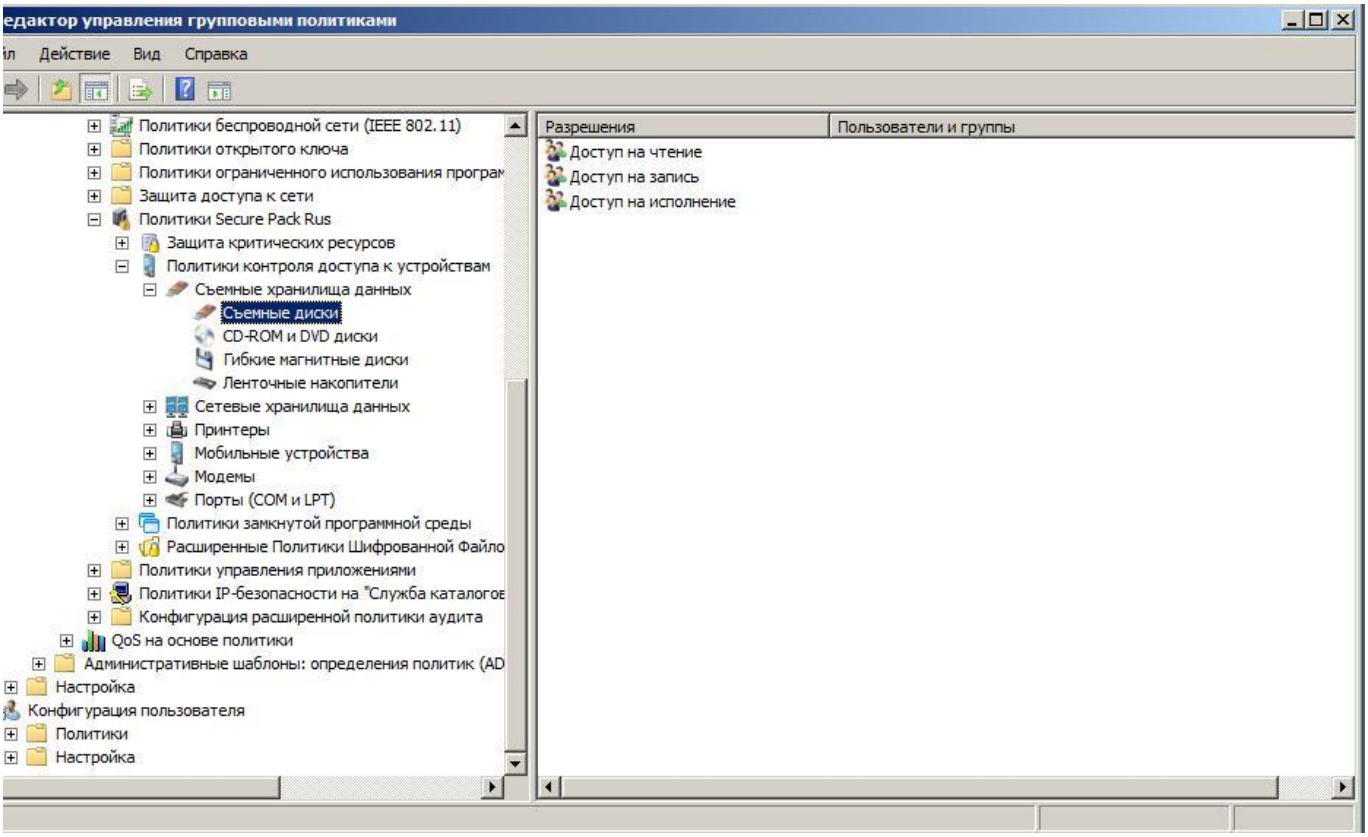


Рисунок 11 - Типы разрешений доступа

SPR3.0 различает следующие классы съемных хранилищ данных:

- съемные диски
- CD-ROMиDVDдиски
- Гибкие магнитные диски
- Ленточные накопители

Кроме того, для данных на каждом классе устройств можно указать разрешенный тип доступа к ним:

- Чтение
- Запись
- Исполнение

Для того, что бы дать разрешение пользователю или группе безопасности на определенный тип доступа к данным на определенном классе съемных устройств необходимо добавить этого пользователя или группу в соответствующий пункт групповой политики. Для этого необходимо выделить пункт групповой политики, вызвать меню и выбрать пункт «Свойства».

В открывшемся окне выполнить действие «Добавить» и выбрать пользователя или группу безопасности (Рис. 12).

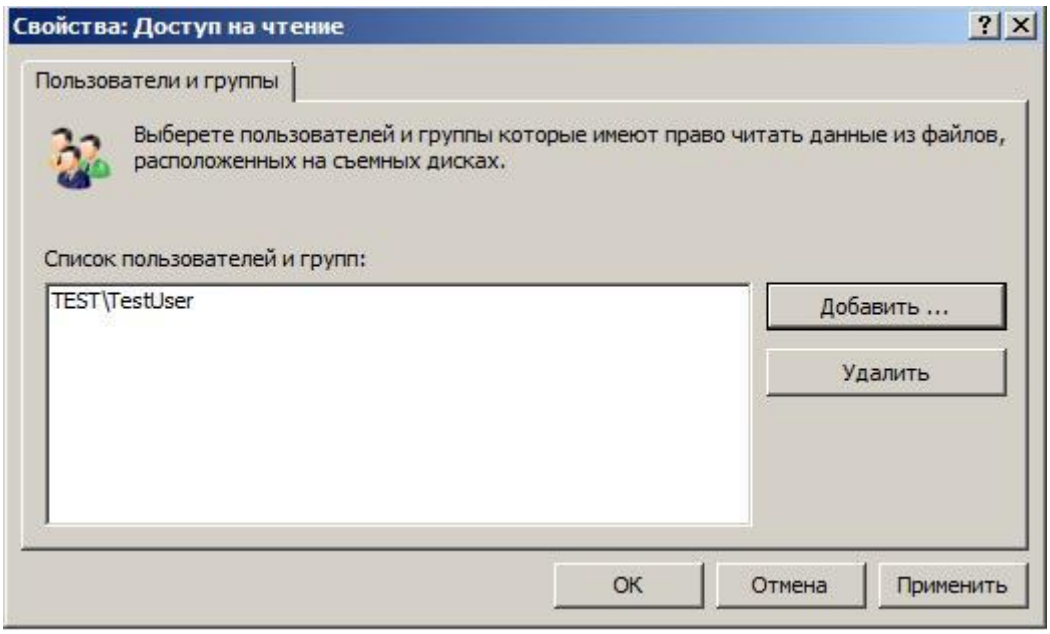


Рисунок 12 - Список членов правила

После применения политики, указанные изменения вступят в силу.

4. Настройка правил мандатного шифрования данных на съемных носителях

4.1. Установка режима работы политики мандатного шифрования

После первоначальной установки SPR 3.0 политика мандатного шифрования включена в режиме Аудит. Мандатное шифрование данных на съемных носителях информации в данном режиме не производится!

При первоначальной установке SPR3.0 список правил политики мандатного шифрования пуст, поэтому активация политики приведет к блокировке доступа к незашифрованным файлам на съемных носителях для всех пользователей. После установки SPR3.0 и создания базового набора правил мандатного шифрования необходимо активировать политику разрешений.

Для изменения режима работы политики мандатного шифрования необходимо:

- раскрыть в консоли управления политиками следующий путь: *Конфигурация компьютера →Политики →Конфигурация Windows→Параметры безопасности →Политики SecurePackRus→Расширенные политики шифрованной файловой системы (EFS) →Мандатное шифрование→Съемные устройства* и, вызвав меню, выбрать радел «Свойства»
- в открывшемся окне отметить пункт «Активировать проверку разрешений» (Рис. 13)

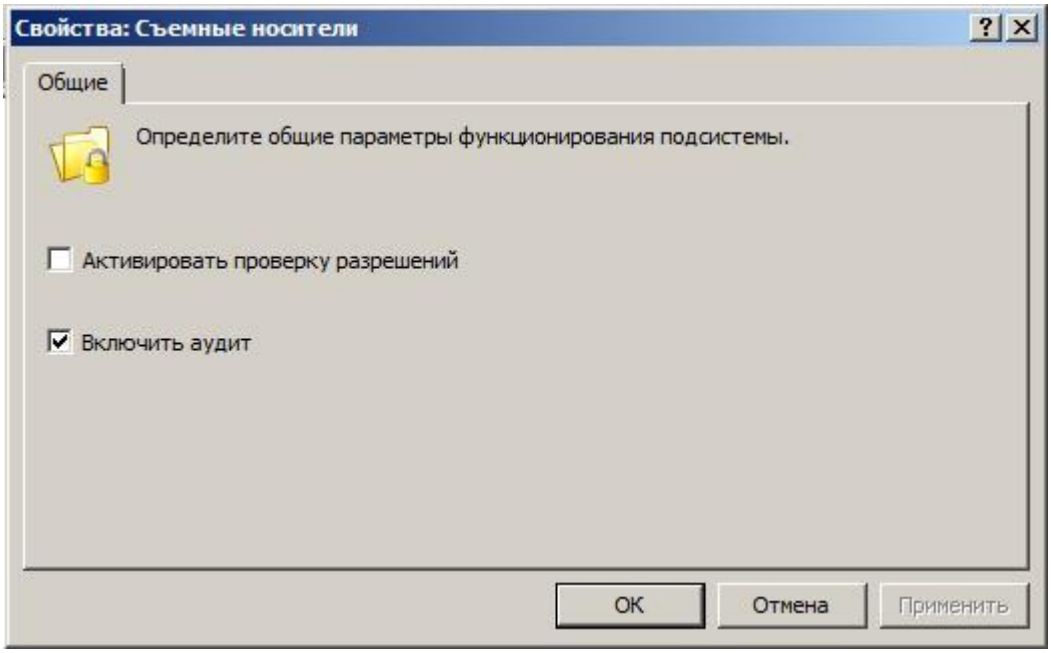


Рисунок 13 - Активация политики

Активация проверки разрешений при доступе пользователей к файлам на съемных носителях запретит любое действие, не разрешенное администратором правилами политики мандатного шифрования.

4.2. Создание правил политики мандатного шифрования

Правила политики мандатного шифрования позволяют администраторам задавать различные разрешения для пользователей и групп безопасности при работе с незашифрованными данными на съемных носителях информации.

Для настройки правил доступа к съемным носителям необходимо раскрыть в консоли управления политиками следующий путь: *Конфигурация компьютера →Политики →Конфигурация Windows→Параметры безопасности →Политики SecurePackRus→Расширенные политики шифрованной файловой системы (EFS) →Мандатное шифрование →Съемные устройства(Рис. 14)*

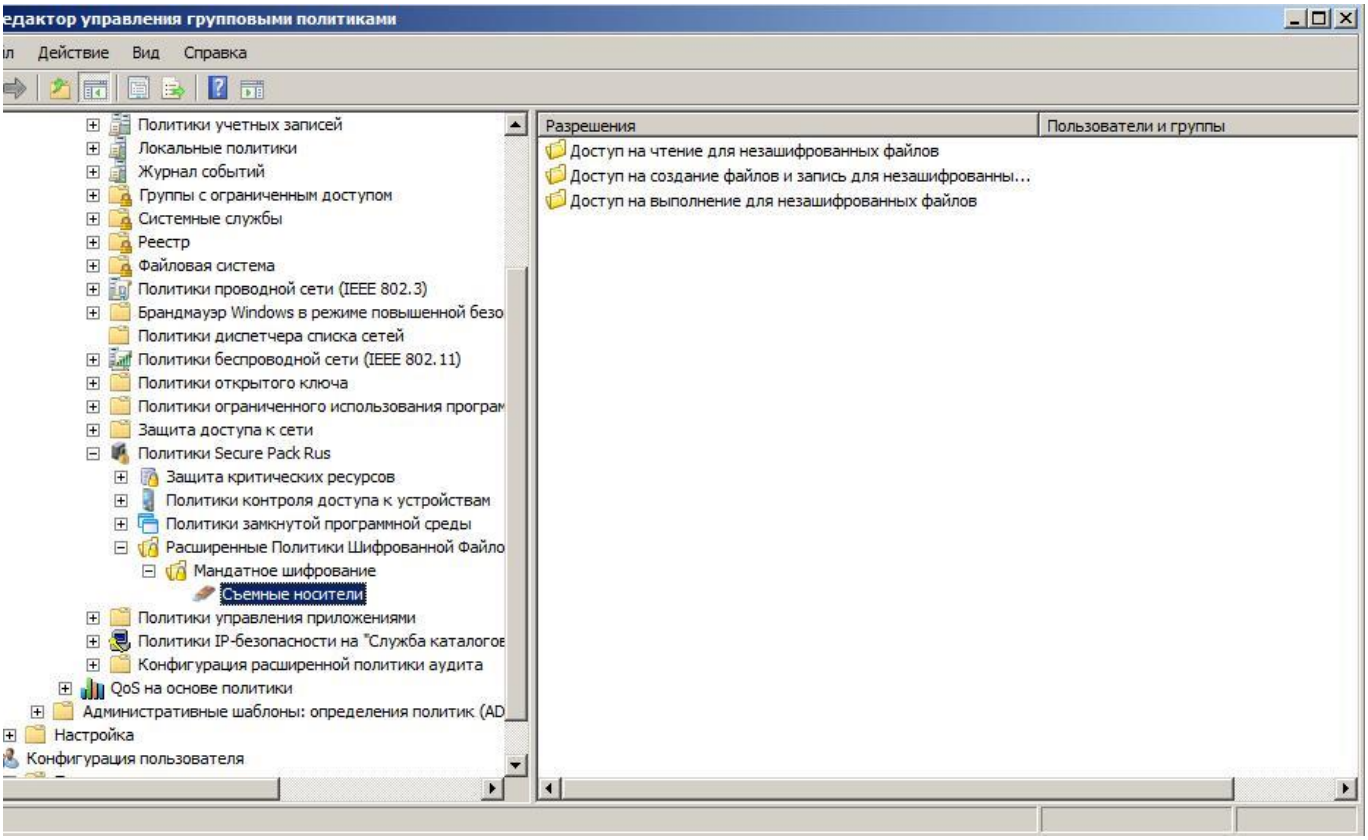


Рисунок 14 - Типы разрешений доступа

SPR3.0 различает три типа доступа с незашифрованным файлам на съемных носителях:

- чтение
- чтение и запись
- исполнение

Для того, что бы дать разрешение пользователю или группе безопасности на определенный тип доступа к незашифрованным данным на съемных устройствах необходимо добавить этого пользователя или группу в соответствующий пункт групповой политики. Для этого

необходимо выделить пункт групповой политики, вызвать меню и выбрать пункт «Свойства» (**Ошибка! Источник ссылки не найден.**).

В открывшемся окне выполнить действие «Добавить» и выбрать пользователя или группу безопасности (Рис. 15).

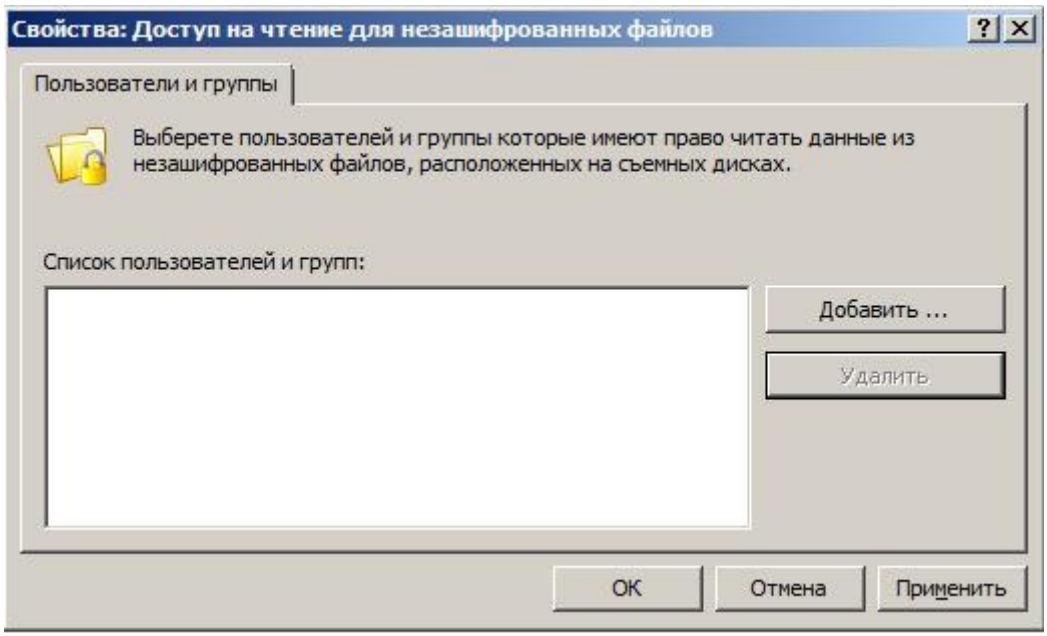


Рисунок 15 - Добавление пользователя или группы

После выполнения описанных выше действий в списке политики должен появиться указанный элемент (Рис. 16).

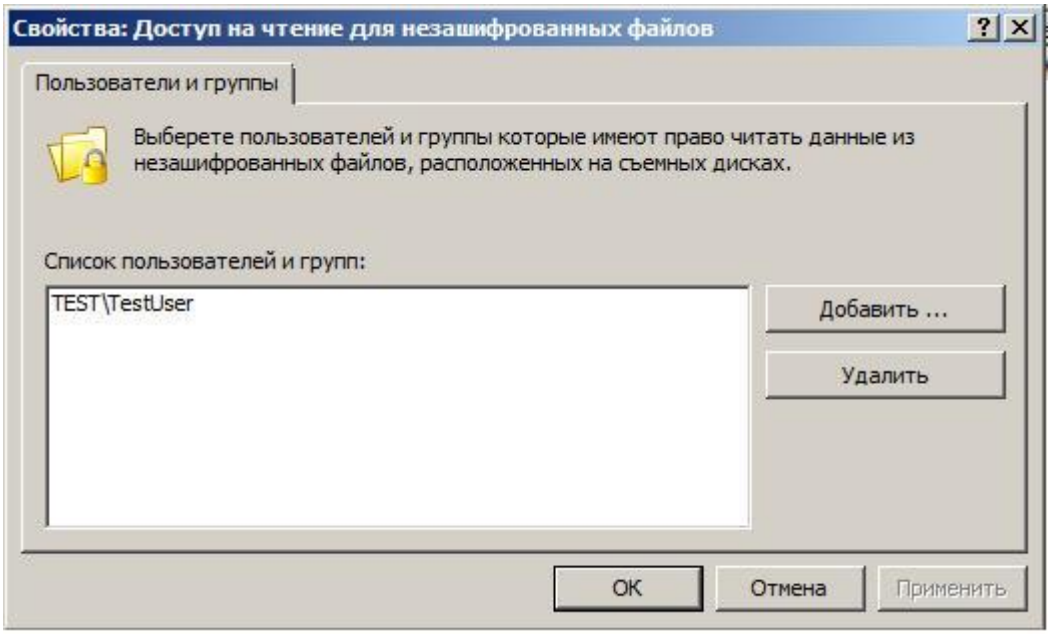


Рисунок 16 - Список членов правила

После применения политики, указанные изменения вступят в силу

5. Настройка правил контроля запуска сценариев

5.1. Установка режима работы политики контроля выполнения сценариев

После первоначальной установки SPR 3.0 политика контроля выполнения сценариев включена в режиме Аудит. Проверка выполняемых сценариев в данном режиме не производится!

При первоначальной установке SPR3.0 список разрешенных к выполнению сценариев пуст, поэтому активация политики приведет к блокировке выполнения всех сценариев для всех пользователей. После установки SPR3.0необходимо определенное время на обучение подсистемы контроля выполнения сценариев. После чегонеобходимо импортировать список выполненныхза время обучения сценариев и включить режим Блокировки.

Для изменения режима работы политики контроля выполнения сценариев необходимо:

- раскрыть в консоли управления политиками следующий путь: *Конфигурация компьютера →Политики →Конфигурация Windows→Параметры безопасности →Политики SecurePackRus→Политики замкнутой программной среды→Контроль выполнения сценариев* и, вызвав меню, выбрать радел «Свойства» (Рисунок 17)

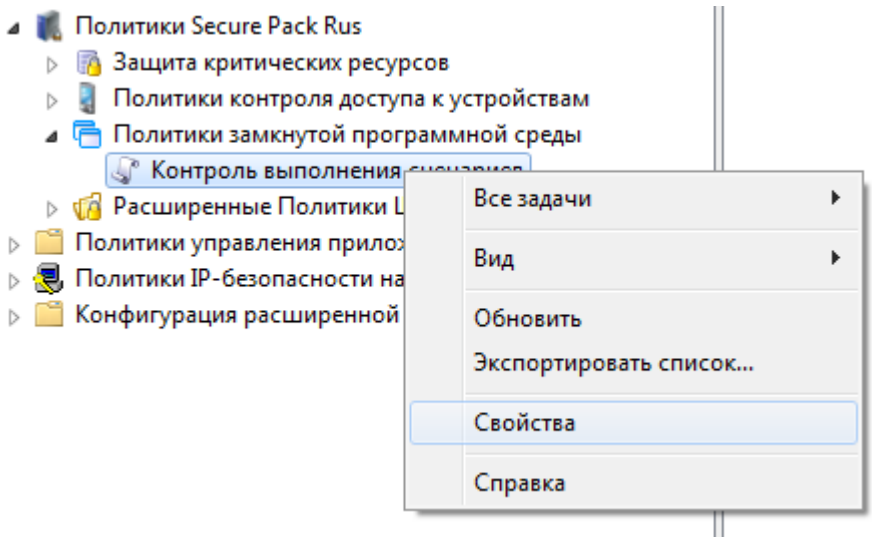


Рисунок 17 - Изменение режима работы политики

- в открывшемся окне отметить пункт «Активировать режим блокировки сценариев» и, при необходимости, отметить пункт «Режим добавления политик» (Рисунок 18)

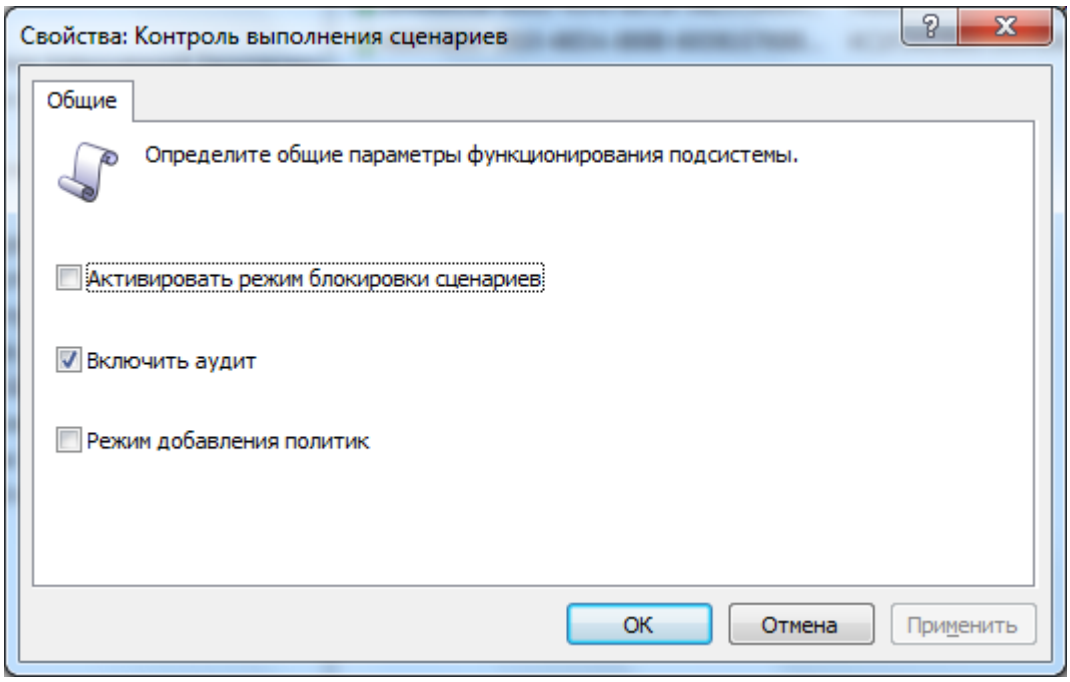


Рисунок 181 - Активация политики

Активация блокировкисценариев запретит выполнение любых сценариев, которых нет в списке разрешенных.

Активация режима добавления политик приведет к тому, что при импорте правил запущенных сценариев они будут добавляться к уже существующим правилам (если режим не активирован, то все правила будут замещены новыми).

5.2. Импорт и удаление правил политики контроля выполнения сценариев

Для импорта правил с компьютеров домена необходимо, чтобы на этих компьютерах в параметрах рабочего подключения был установлен компонент «Служба доступа к файлам и принтерам сетей Microsoft». Кроме того, компьютеры домена должны быть доступны для подключения администратора.Поэтому, настройки безопасности «Доступ к компьютеру из сети» и «Отказ в доступе к компьютеру из сети» должны быть установлены таким образом, чтобы не ограничивать доступ администратора к компьютеру.

Правила политики контроля выполнения сценариев позволяют администраторам импортироватьразрешенные для выполнения сценарии, как с локального компьютера, так и с компьютеров домена. Правила политики применяются для всех пользователей компьютера.

Для импорта правил политики контроля выполнения сценариев необходимо раскрыть в консоли управления политиками следующий путь: *Конфигурация компьютера →Политики →Конфигурация Windows→Параметры безопасности →Политики SecurePackRus→Политики*

замкнутой программной среды→Контроль выполнения сценариеви, вызвав меню, выбрать радел «Все задачи→*Импортировать правила …*» *(*Рисунок *)*

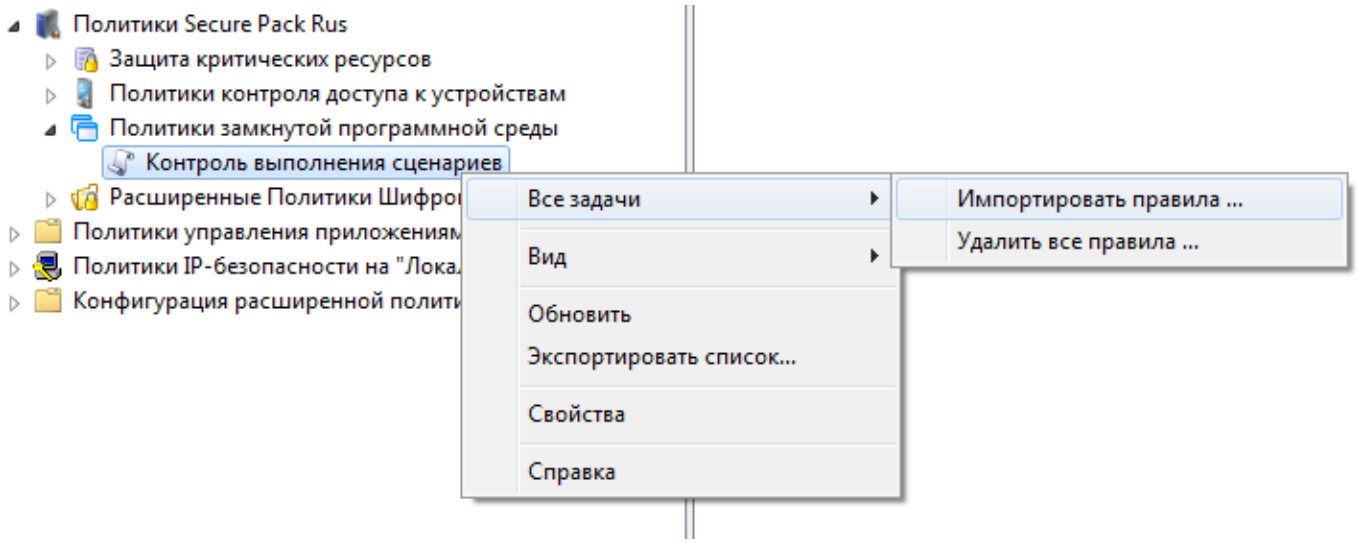


Рисунок 19 – Пункт меню «Импортировать правила»

- в открывшемся окне, в списке компьютеров для импорта по умолчанию находится локальный компьютер. Для добавления компьютеров из домена необходимо выполнить действие «Добавить» и выбрать компьютеры в домене, с которых будет произведен импорт информации о запущенных сценариях (Рисунок).

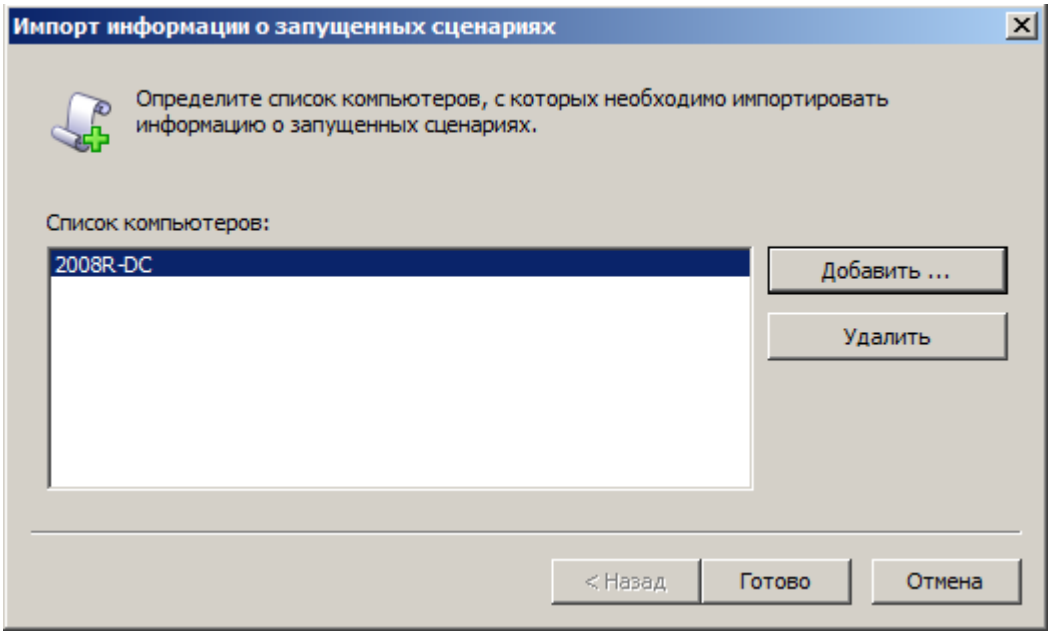


Рисунок 20 - Добавление компьютеров из домена

- после выполнения описанных выше действий в списке политики должны появиться компьютеры, с которых будет произведен импорт информации о запущенных сценариях.

- после добавления компьютеров, с них будет произведен импорт правил разрешенных сценариев, и эти правила будут применены (Рисунок).

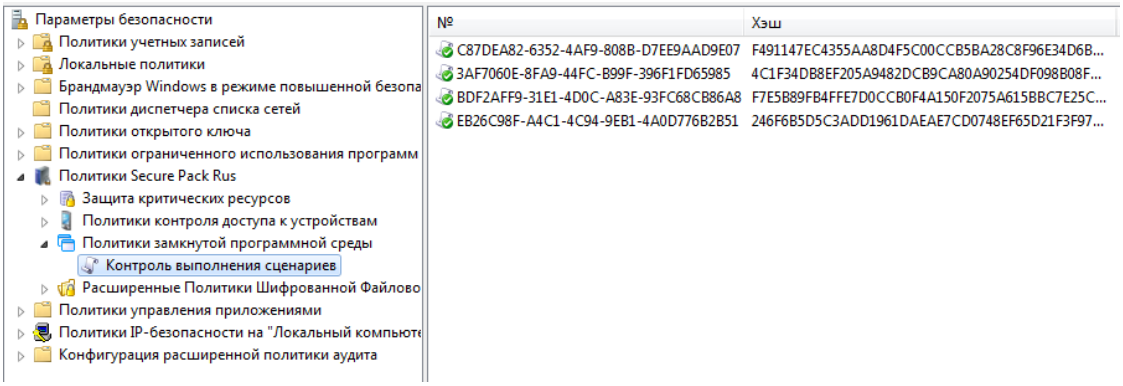


Рисунок 21 - Правила разрешенных к выполнению сценариев

Для удаления правил политики контроля выполнения сценариев необходимо раскрыть в консоли управления политиками следующий путь: *Конфигурация компьютера →Политики →Конфигурация Windows→Параметры безопасности →Политики SecurePackRus→Политики замкнутой программной среды→Контроль выполнения сценариеви*, вызвав меню, выбрать радел «Все задачи→*Удалить все правила …*» *(*Рисунок *).*

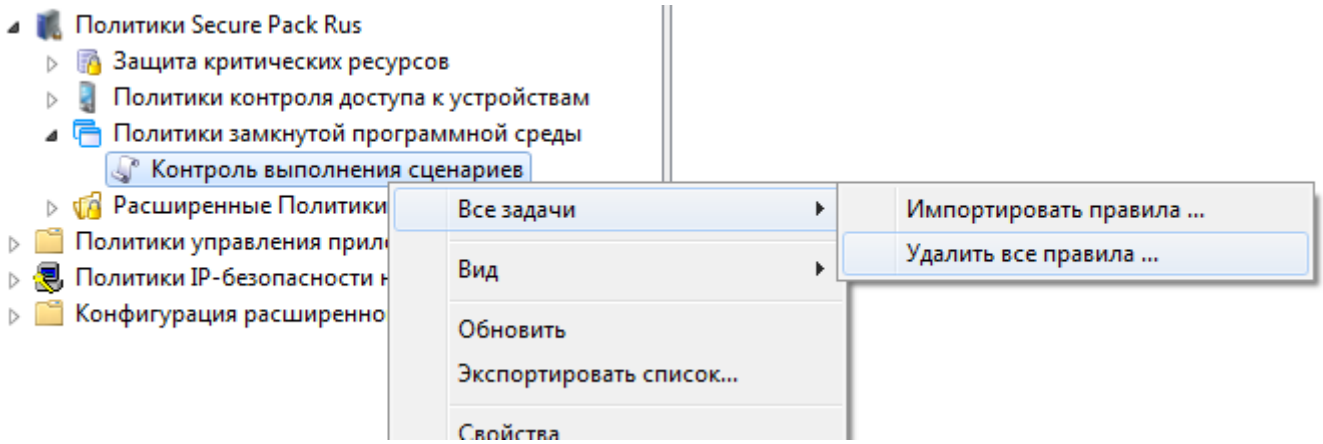


Рисунок 22 - Удаление всех правил

6. Вывод графических окон сервисом Крипто-Про CSP КС3

В процессе работы сервис CSP Крипто-Про может выводить графические окна для взаимодействия с пользователем: информацию о ключевых носителях, приглашение на генерацию последовательностей случайных чисел для формирования ключевого материала и т.д.

В связи с изменениями в подсистеме защиты пользовательских ОС семейства Windows 7 / 8 и серверных ОС семейства Windows Server 2008 / 2012 для вывода графических окон CSP Крипто-Про использует новый сервис ОС, в связи с чем возможны ошибочные действия пользователя при работе с этими окнами. Ниже описана процедура работы пользователя с окнами CSP Крипто-Про и условия, необходимые для их корректного отображения в серверных ОС семейства Windows Server 2008 / 2012.

6.1. Настройка серверных ОС Windows Server 2008 / 2012

Для корректного отображения окон информации сервисом CSP Крипто-Про в ОС должны быть активированы необходимые компоненты, которые реализуют вывод информации с уровня сервиса на уровень пользователя. В пользовательских ОС семейства Windows 7 / 8 все необходимые компоненты активированы по умолчанию, но для серверных ОС семейства Windows Server 2008 / 2012 требуется дополнительная настройка.

Для корректного отображения окон CSP Крипто-Про в ОС семейства Windows Server 2008 / 2012 необходимо активировать «Службы рукописного ввода»: Пуск → Администрирование → Диспетчер сервера → Компоненты → Добавить компоненты (рис. 23)

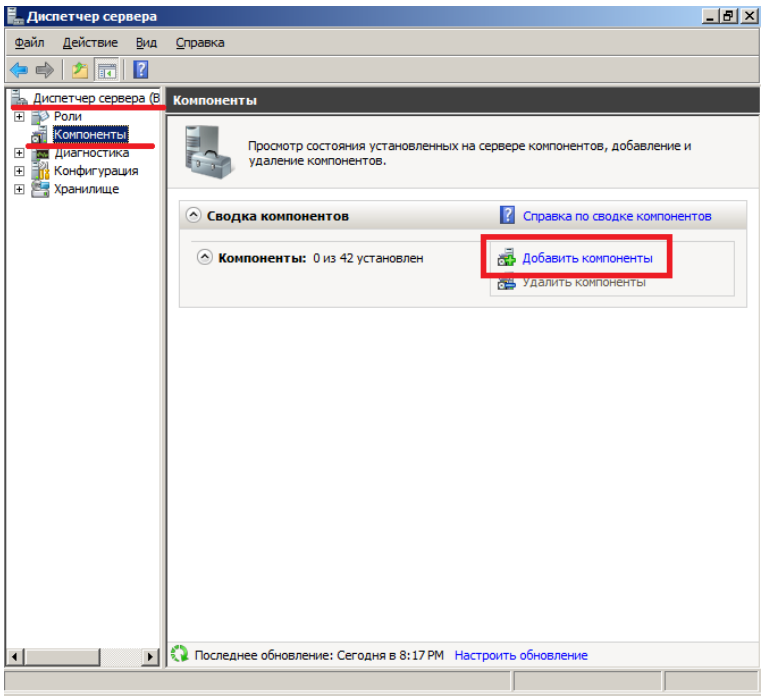
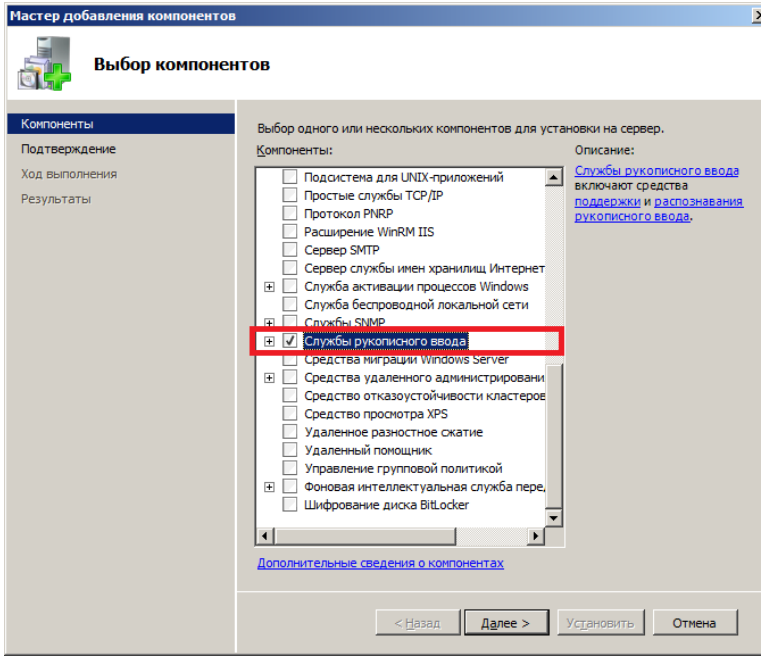
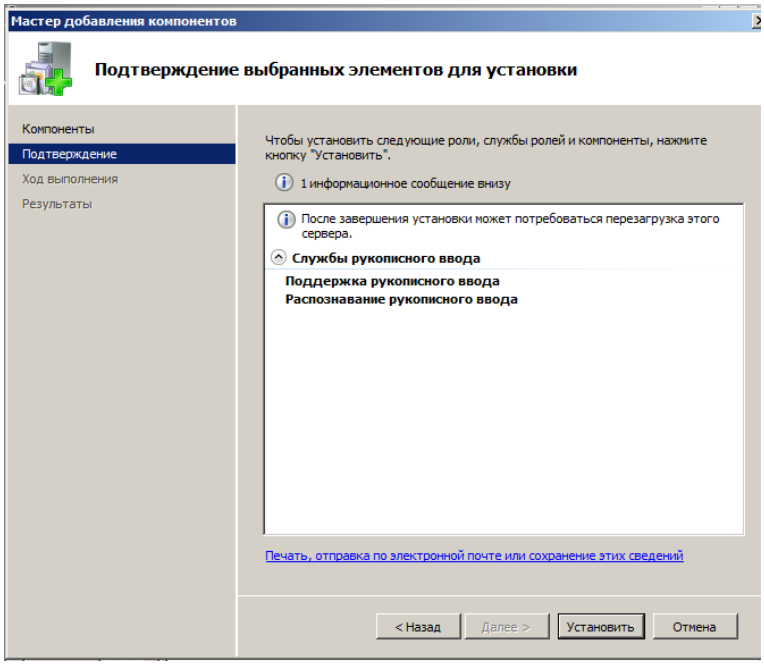
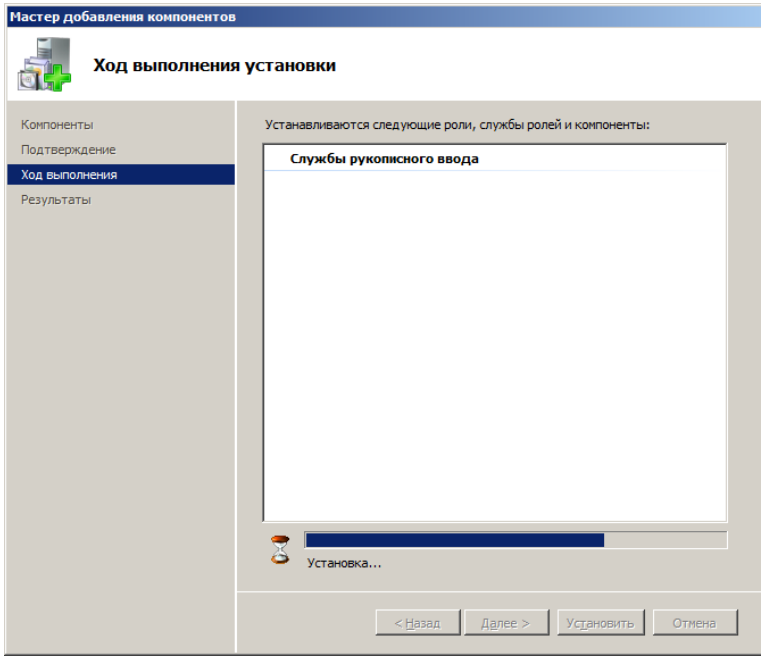


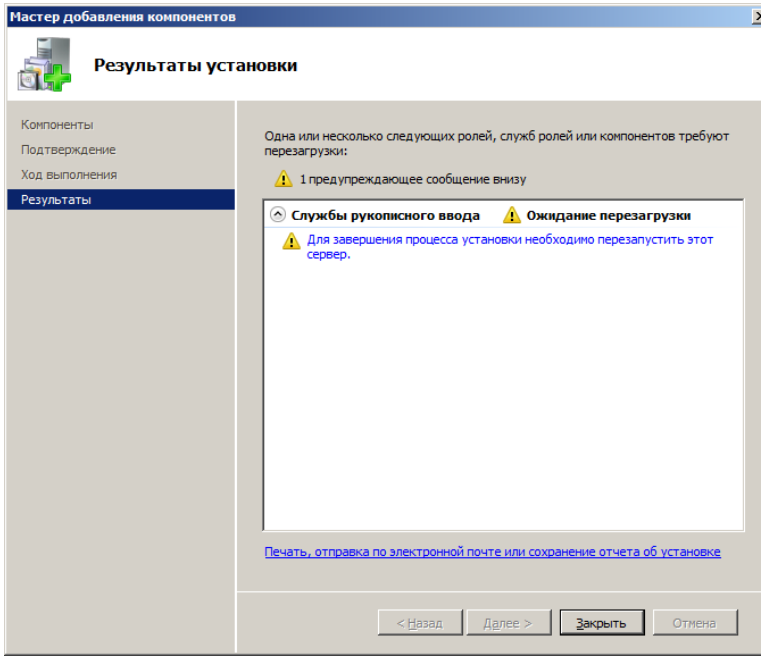
Рис.23 – Добавление компоненты

В списке доступных компонент выбрать «Службы рукописного ввода» и завершить установку (рис. 24 – 27).









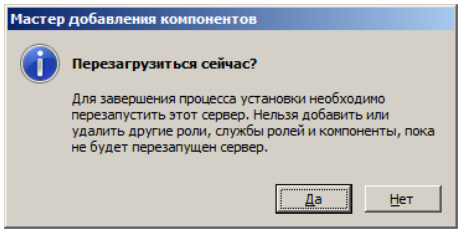


Рис.24 – 27 – Установка службы

После перезагрузки ОС будет продолжена установка службы (рис. 28).

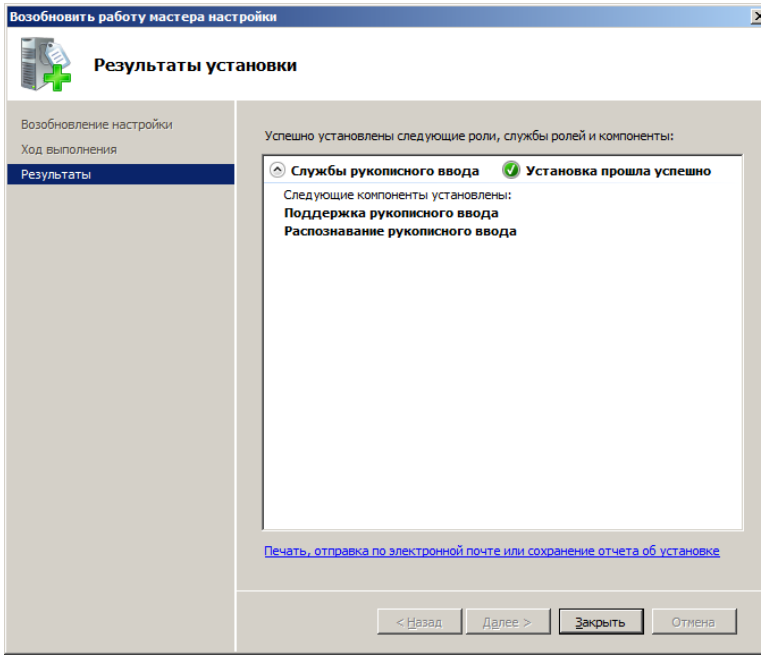


Рис.28 – Установка службы

6.2. Работа с окнами сервиса Крипто-Про CSP КС3

При работе пользователя сервис CSP Крипто-Про может выводить сообщения для взаимодействия с пользователем – пример такого сообщения представлен на рис. 29 - 30.

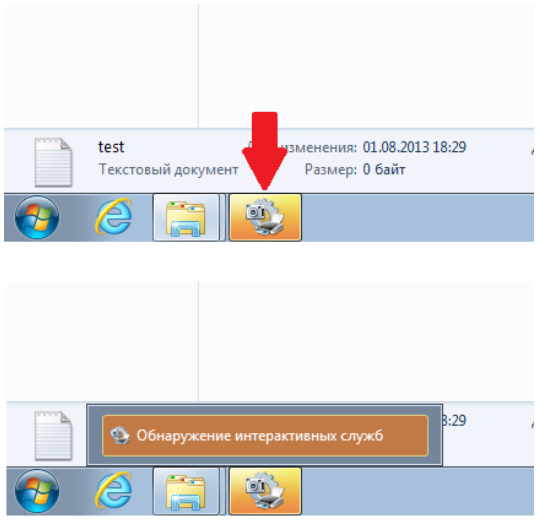


Рис. 29 - 30 – Сообщение сервиса CSP Крипто-Про

Возникновении такого сообщения означает, что криптографической подсистеме необходимо взаимодействие с пользователем. Пользователь должен перейти в окно приглашения (рис. 31 - 32) и выбрать действие «Посмотреть сообщение», после чего выполнить необходимые действия (например, генерацию последовательности случайных чисел – рис. 33).

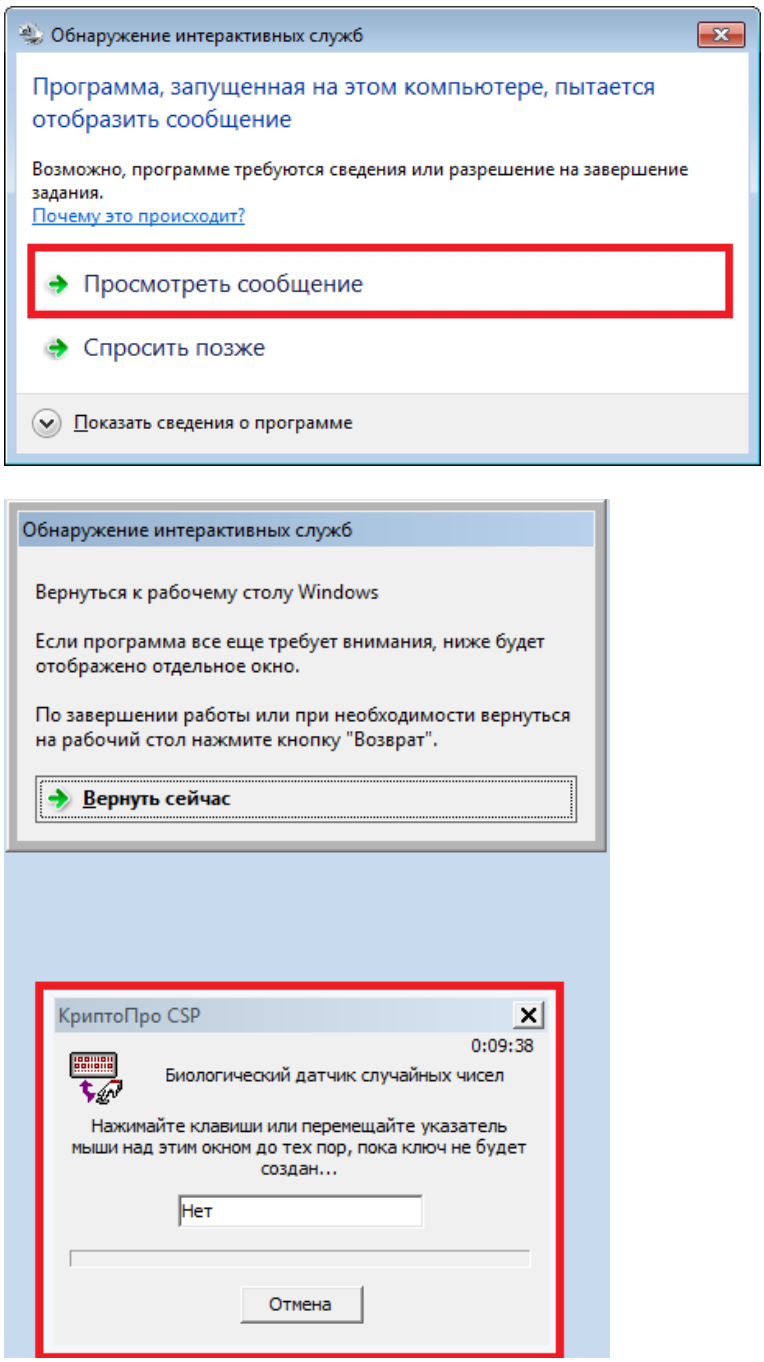


Рис. 31 - 32 – Окно взаимодействия с сервисом CSP Крипто-Про

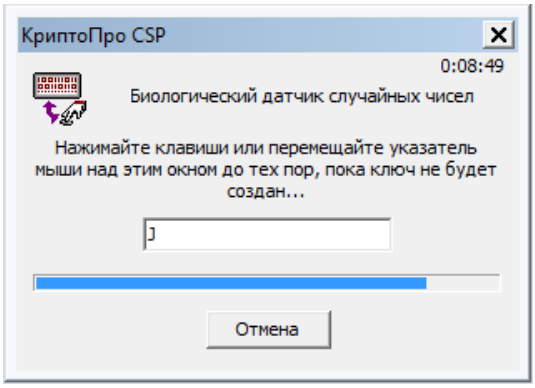


Рис. 33 – Выполнение действий в окне сервиса

После выполнения действия в окне сервиса для возврата в режим работы с рабочим столом Windows пользователь должен выбрать действие «Вернуть сейчас» (рис 12).

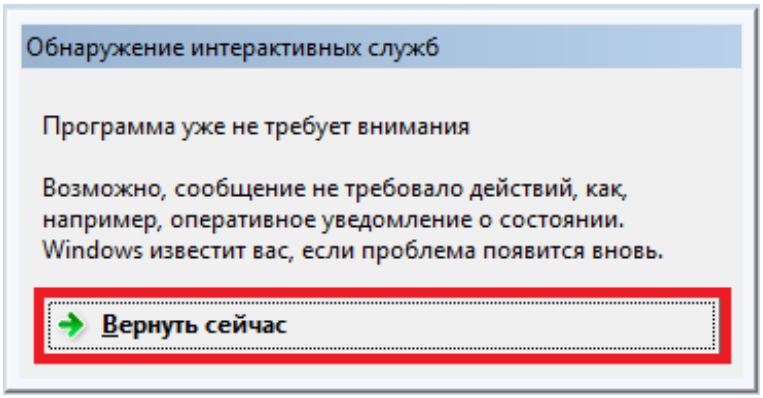


Рис.34 – Завершение взаимодействия с сервисом CSP Крипто-Про

Взаимодействие с сервисом CSP Крипто-Про можно отложить, не переходя в окно приглашения. Тем не менее, если пользователь перешел в окно приглашения, но выбрал действие «Спросить позже», запрос сервиса CSP Крипто-Про будет завершен с ошибкой. Для повторного взаимодействия с сервисом CSP Крипто-Про может потребоваться перезагрузка АРМ.

7. Дополнительные требования к эксплуатации SPR 3.0 исполнения 1 и 2.

К АИС, использующим SPR 3.0 исполнения 1 и 2 предъявляются ряд дополнительных требований технического и организационного характера:

- Запрещается создавать (открывать) системные объекты с именами, совпадающими с предопределенными именами служебных объектов ОС;
- Запрещается выполнять сценарии, напрямую вызывая подсистему Windows ScriptHost;
- При эксплуатации АИС должна быть исключена возможность подключения к ПЭВМ USB накопителей, реализующих интерфейс составного съемного устройства.

Список литературы

1. **Компания "СиЭйЭн".** Формуляр. *Средство защиты информации «Secure Pack Rus» версия 3.0.* ЕАРМ.5090005.032-03 30 01.

2. —. Описание применения. *Средство защиты информации «Secure Pack Rus» версия 3.0.* ЕАРМ.5090005.032-03 31 01.