Средство защиты информации

«КриптоПро SPR»

Версия 4.0

Руководство администратора безопасности

ЖТЯИ.00112-01 90 01

Листов 33

Компания «КРИПТО-ПРО»

2021

ООО «КРИПТО-ПРО»
Адрес 127018, г. Москва, ул. Сущевский Вал, дом 18
Телефон +7 (495) 995-4820
e-mail info@cryptopro.ru
Web www.cryptopro.ru

Оглавление

Список сокращений 4
1. Введение 5
2. Основные подсистемы 6
3. Политики защиты критических ресурсов 7
3.1. Защита объектов файловой системы 7
3.2. Управление правилами защиты объектов файловой системы 9
3.3. Формирование политики защиты объектов файловой системы 14
4. Политики контроля доступа к устройствам 15
4.1. Контроль доступа к съемным хранилищам данных 15
4.2. Управление правилами доступа к съемным хранилищам данных 17
4.3. Формирование политики доступа к съемным хранилищам данных 18
5. Настройка правил мандатного шифрования данных на съемных носителях 20
5.1. Установка режима работы политики мандатного шифрования 20
5.2. Управление правил политики мандатного шифрования 21
5.3. Формирование политики мандатного шифрования 23
6. Вывод графических окон сервисом КриптоПро CSP КС3 25
6.1. Настройка серверных ОС Windows Server 2008 / 2012 25
6.2. Настройка серверных ОС Windows Server 2016 28
6.3. Работа с окнами сервиса КриптоПро CSP КС3 28
7. Использование дополнительных средств защиты загрузки 32
Список литературы 33

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 «КриптоПро SPR» версия 4.0 (сокращенное названия изделия – SPR 4.0). В руководстве содержатся сведения, необходимые администраторам для настройки и управления основными механизмами защиты.

2. Основные подсистемы

Функционирование СЗИ SPR 4.0 опирается на следующие подсистемы:

- Подсистема управления политиками;
- Подсистема доверенной аутентификации;
- Подсистема дискреционного разграничения доступа;
- Подсистема защиты критических ресурсов;
- Подсистема контроля доступа к устройствам;
- Подсистема мандатного шифрования;
- Подсистема замкнутой программной среды;
- Подсистема контроля запуска сценариев;
- Подсистема аудита безопасности.

Данное Руководство описывает порядок настройки следующих политик безопасности основных подсистем, реализуемых СЗИ SPR 4.0:

- Подсистема защиты критических ресурсов;
- Подсистема контроля доступа к устройствам;
- Подсистема мандатного шифрования.

Описание порядка настройки политик безопасности, не входящих в данное Руководство, содержится в соответствующих документах в составе документации [1], [2], [3] и [4].

3. Политики защиты критических ресурсов

3.1. Защита объектов файловой системы

Внимание

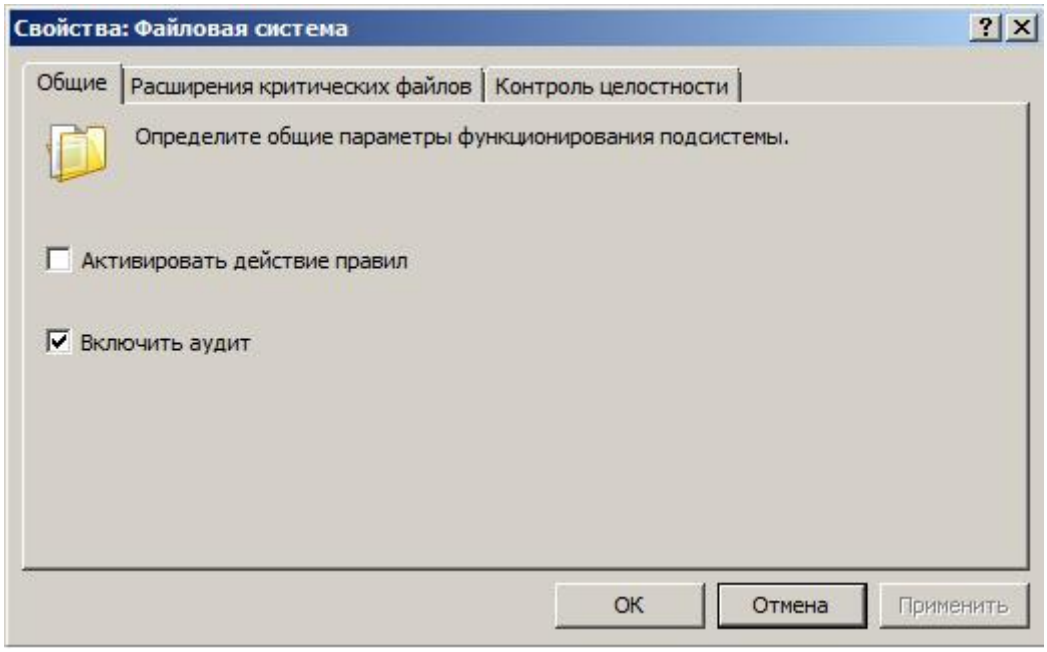
После первоначальной установки SPR 4.0 политика защиты объектов файловой системы включена в режиме Аудит. Контроль доступа пользователей к критическим объектам файловой системы не производится!

При первоначальной установке SPR 4.0 список правил доступа к съемным носителям пуст, поэтому активация политики приведет к полной блокировке всех классов съемных носителей. После установки SPR 4.0 и создания базового набора правил доступа необходимо включить контроль за подключением съемных носителей.

При первоначальной установке SPR 4.0 список правил защиты объектов файловой системы пуст, поэтому активация политики не приводит к блокировке модификации каких-либо областей файловой системы.

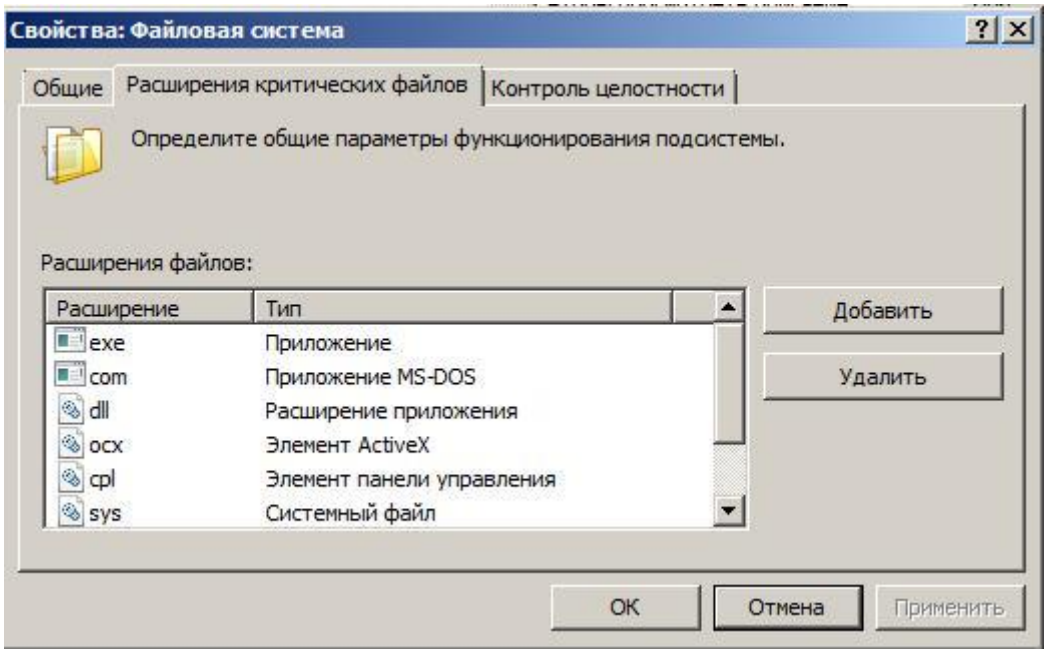
Для изменения режима работы политики необходимо раскрыть в консоли управления политиками следующий путь «Конфигурация компьютера → Политики → Конфигурация Windows → Параметры безопасности → Политики КриптоПро SPR → Защита критических ресурсов → Файловая система» и, вызвав меню, выбрать радел «Свойства» 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 КриптоПро SPR → Защита критических ресурсов → Файловая система» и, вызвав меню, выбрать радел «Свойства», в открывшемся выбрать закладку «Расширения критических файлов» (Рис. 2)

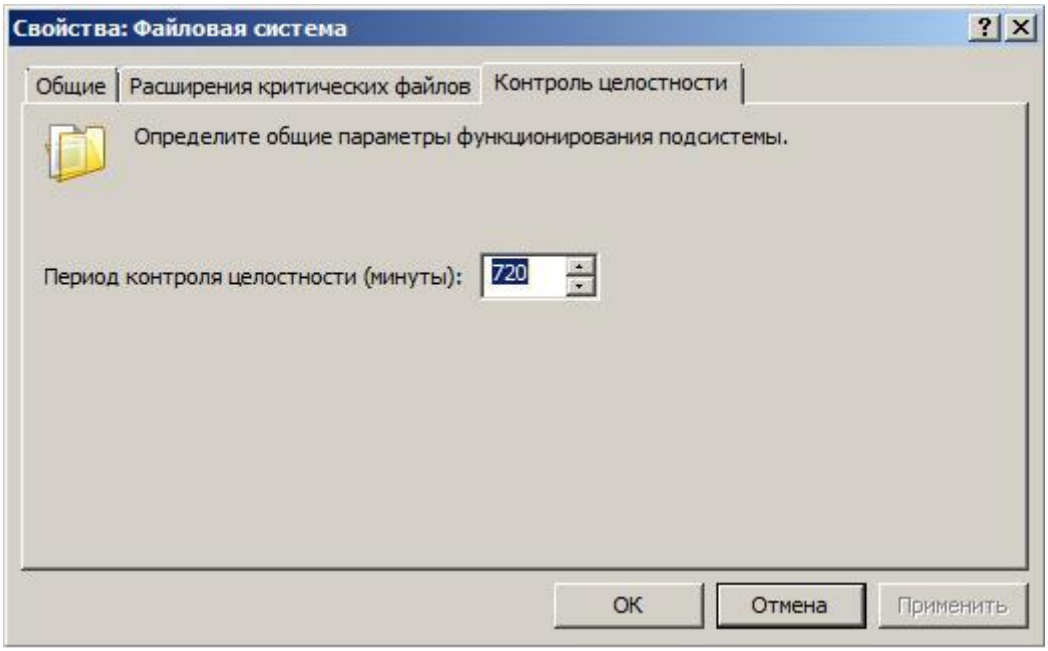
Рис. 2.



Для изменения параметров контроля целостности критических файлов необходимо раскрыть в консоли управления политиками следующий путь «Конфигурация компьютера → Политики → Конфигурация Windows → Параметры безопасности → Политики КриптоПро SPR →

Защита критических ресурсов → Файловая система» и, вызвав меню, выбрать радел «Свойства», в открывшемся выбрать закладку «Контроль целостности» (Рис. 3)

Рис. 3.



3.2. Управление правилами 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 КриптоПро SPR → Защита критических ресурсов → Файловая система» и, 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.

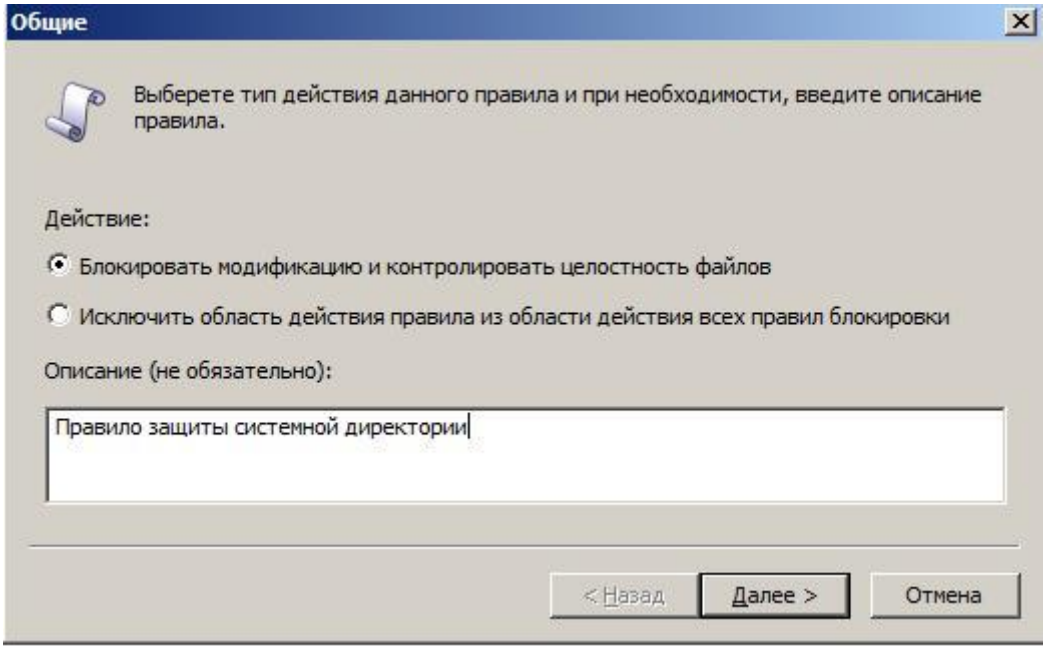
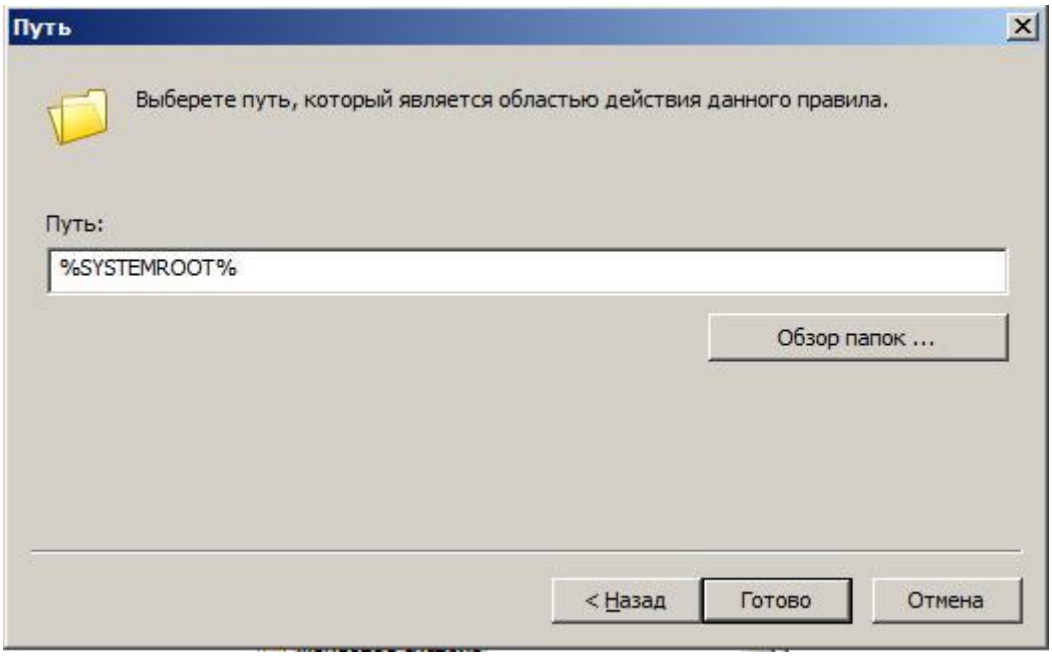


Рис. 5.



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 КриптоПро SPR → Защита критических ресурсов → Файловая система» и, 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.

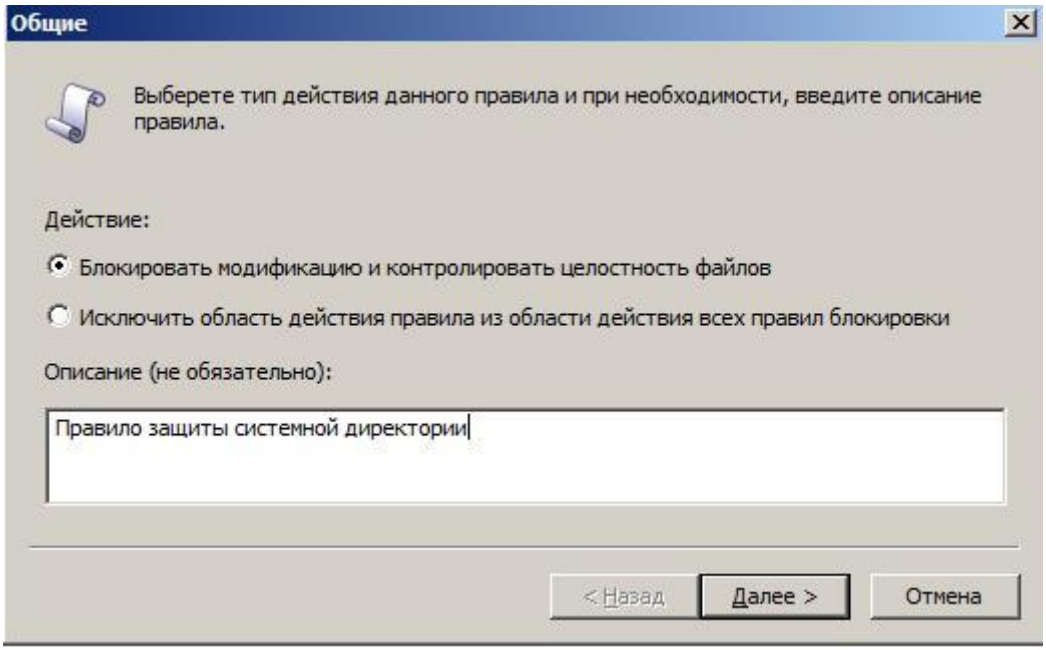
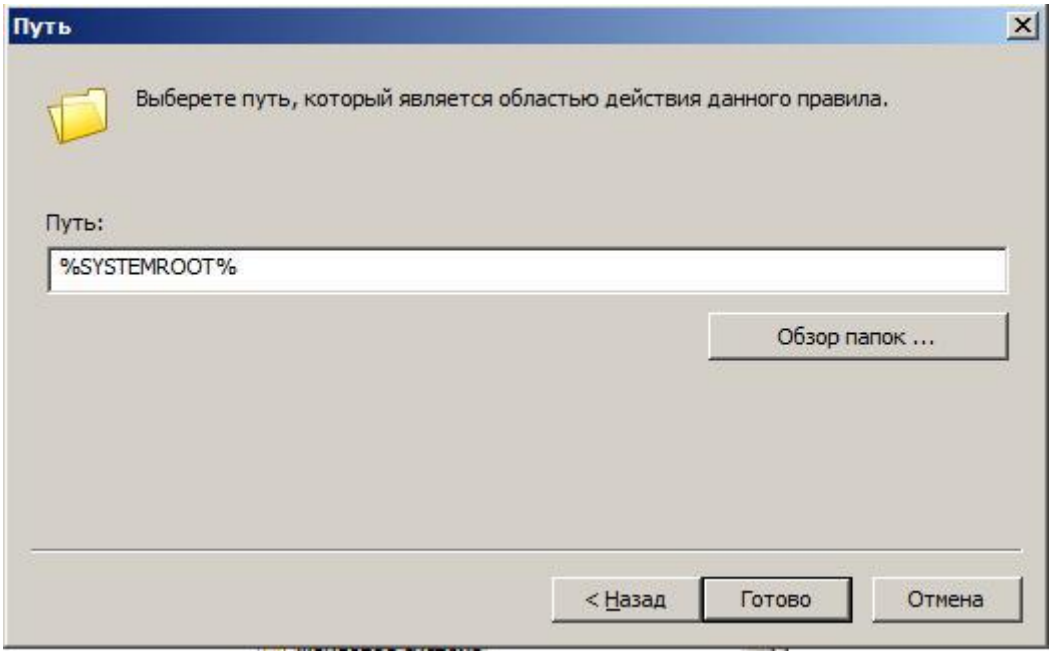
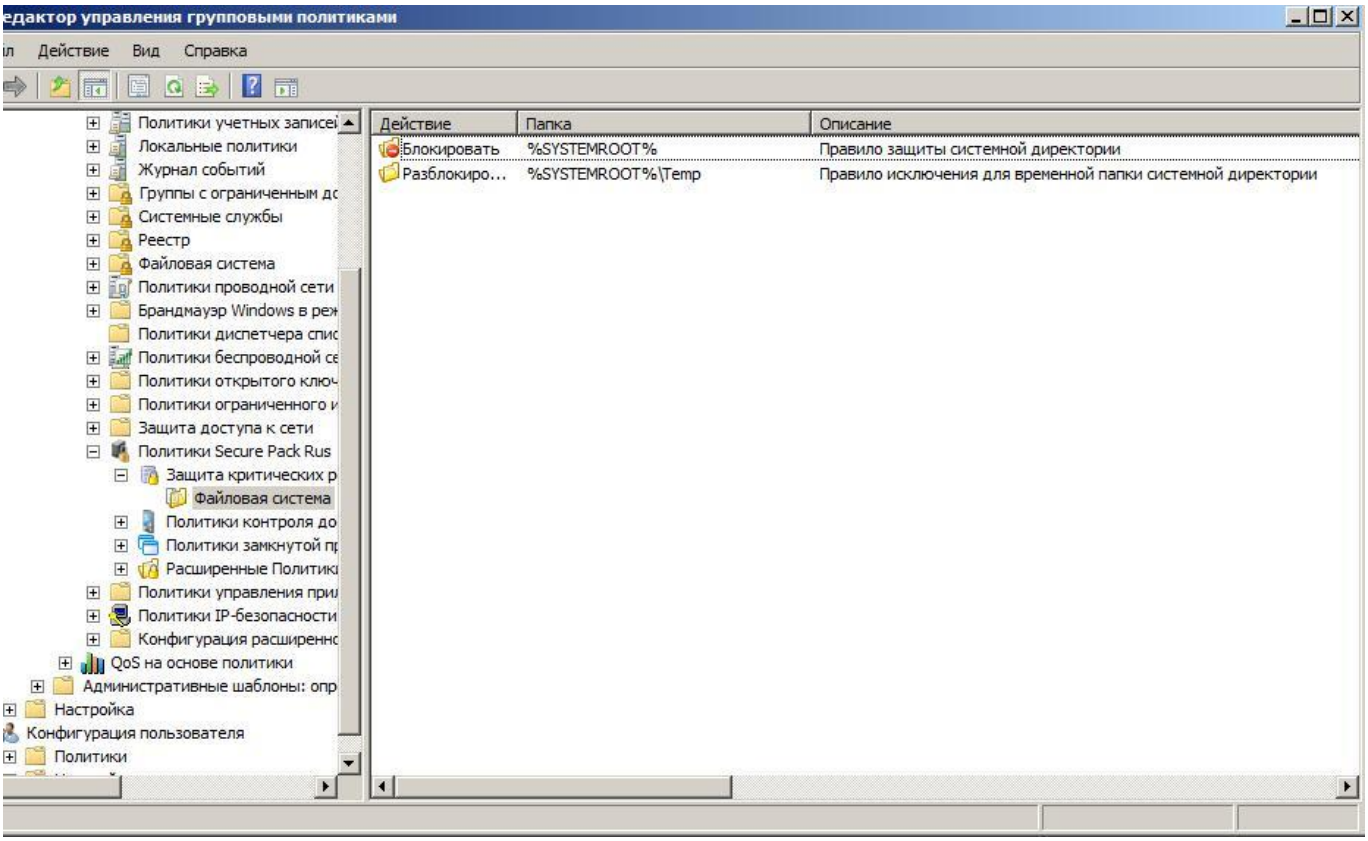


Рис. 7.



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

Рис. 8.



3.3. Формирование политики защиты объектов файловой системы

Политика защиты объектов файловой системы SPR 4.0 реализует контроль целостности объектов файловой системы (ФС) в соответствии с заданными списками абсолютных путей ФС. Обеспечивается контроль целостности файлов в соответствии с заданным набором расширений критических файлов.

Для формирования политики защиты объектов файловой системы необходимо определить перечень путей ФС, по которым расположены критичные объекты и добавить их в список контроля. В список контроля следует включать объекты из состава файлов ОС, общесистемного ПО (ОПО), специального ПО (СПО), установленного на данном АРМ.

В состав СЗИ включен базовый набор расширений критических файлов – в случае, если критичные объекты ФС имеют расширение, отсутствующее в базовом наборе, его необходимо расширить и добавить требуемые типы файлов для поставки их на контроль.

Примечание

Необходимо учитывать, что в штатном режиме работы подсистема защиты критических ресурсов SPR 4.0 обеспечивает запрет на модификацию объектов ФС, стоящих на контроле. При постановке на контроль объектов, которые требуют доступа на запись в процессе работы, возможно нарушение работоспособности.

При формировании политики защиты объектов файловой системы необходимо добавить в список для контроля следующие пути ФС:

- C:\Windows;
- C:\Program Files;
- C:\Program Files (x86) (При использовании 64-разрядных ОС).

Данные правила обеспечат контроль целостности объектов ФС в составе ОС и ОПО при установке ОС по умолчанию (на системный диск «C»). При установке ОС/ОПО/СПО по нестандартным путям, следует выполнить соответствующую модификацию указанных путей ФС.

4. Политики контроля доступа к устройствам

4.1. Контроль доступа к съемным хранилищам данных

Внимание

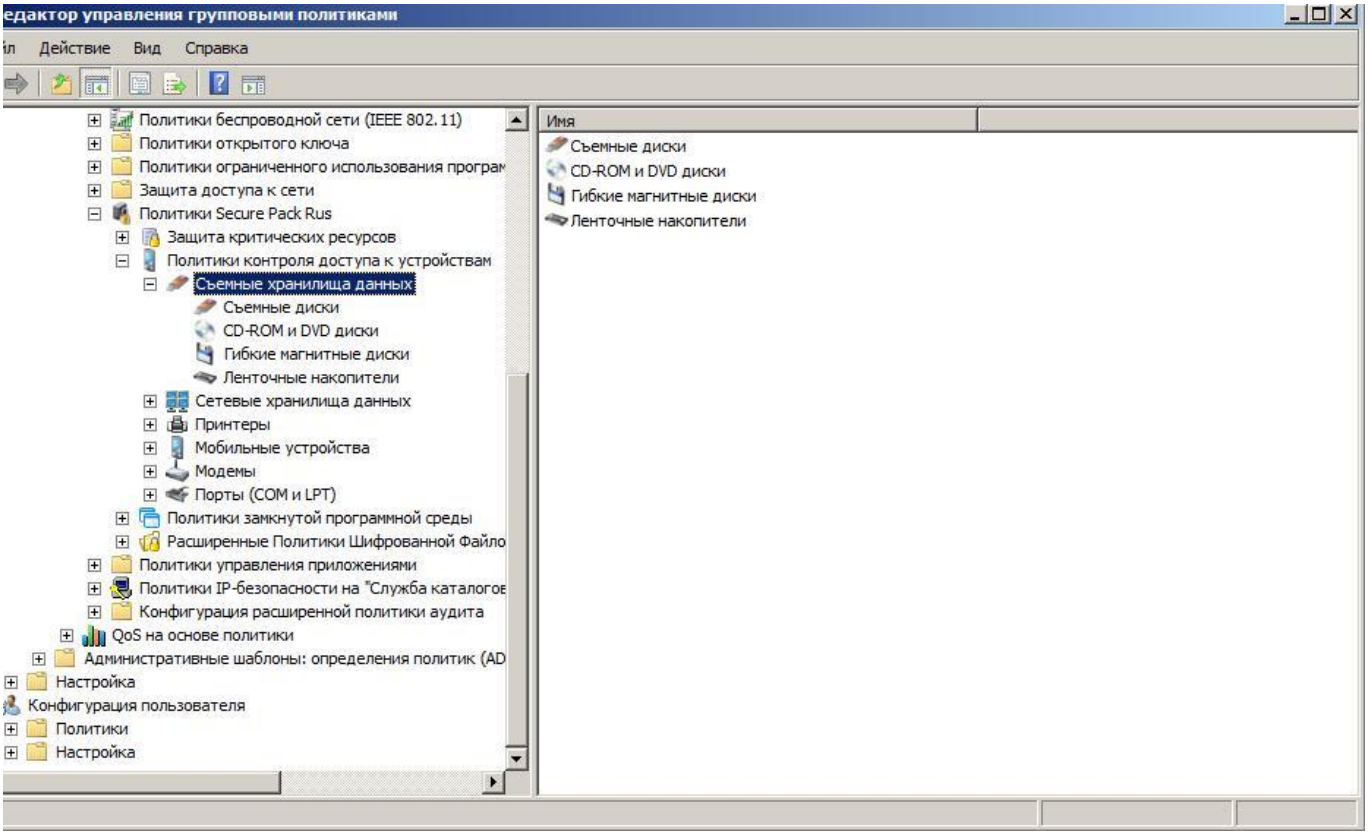
После первоначальной установки SPR 4.0 политика доступа к съемным носителям включена в режиме Аудит. Контроль доступа пользователей к информации на съемных носителях в данном режиме не производится!

При первоначальной установке SPR 4.0 список правил доступа к съемным носителям пуст, поэтому активация политики приведет к полной блокировке всех классов съемных носителей. После установки SPR 4.0 и создания базового набора правил доступа необходимо включить контроль за подключением съемных носителей.

Для изменения режима работы политики доступа необходимо:

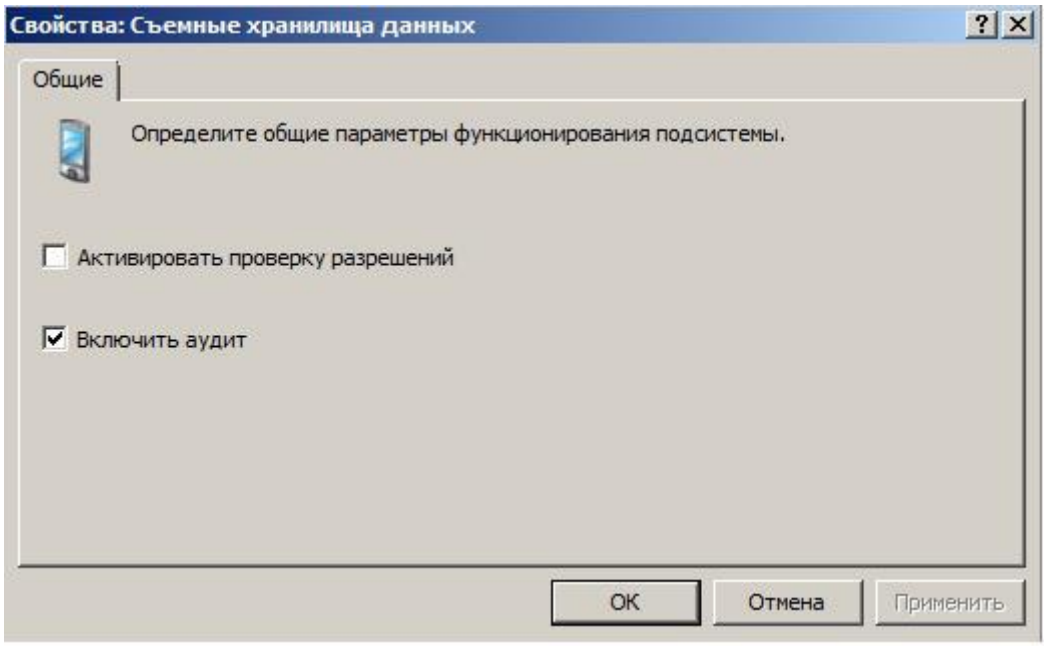
- раскрыть в консоли управления политиками следующий путь «Конфигурация компьютера → Политики → Конфигурация Windows → Параметры безопасности → Политики КриптоПро SPR → Политика контроля доступа к устройствам → Съемные устройства» и, вызвав меню, выбрать радел «Свойства» (Рис. 9)

Рис. 9. Изменение режима работы политики



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

Рис. 10. Активация политики



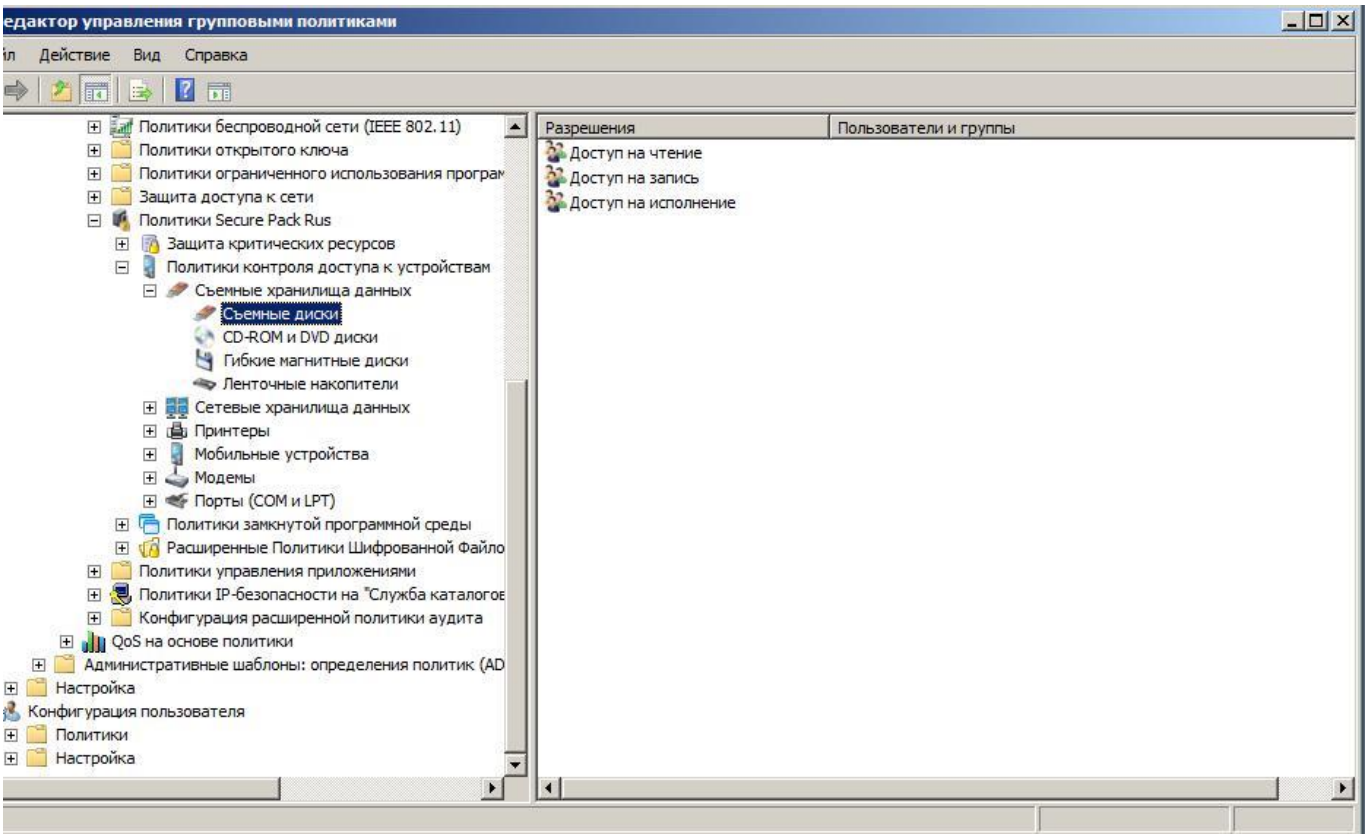
Активация проверки разрешений при доступе пользователей к съемным носителям запретит любое действие, не разрешенное администратором правилами доступа к съемным носителям.

4.2. Управление правилами 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 КриптоПро SPR → Политика контроля доступа к устройствам → Съемные устройства» (Рис. 11).

Рис. 11. Типы разрешений доступа



SPR 4.0 различает следующие классы съемных хранилищ данных:

- съемные диски
- CD-ROM/DVDдиски
- Гибкие магнитные диски
- Ленточные накопители

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

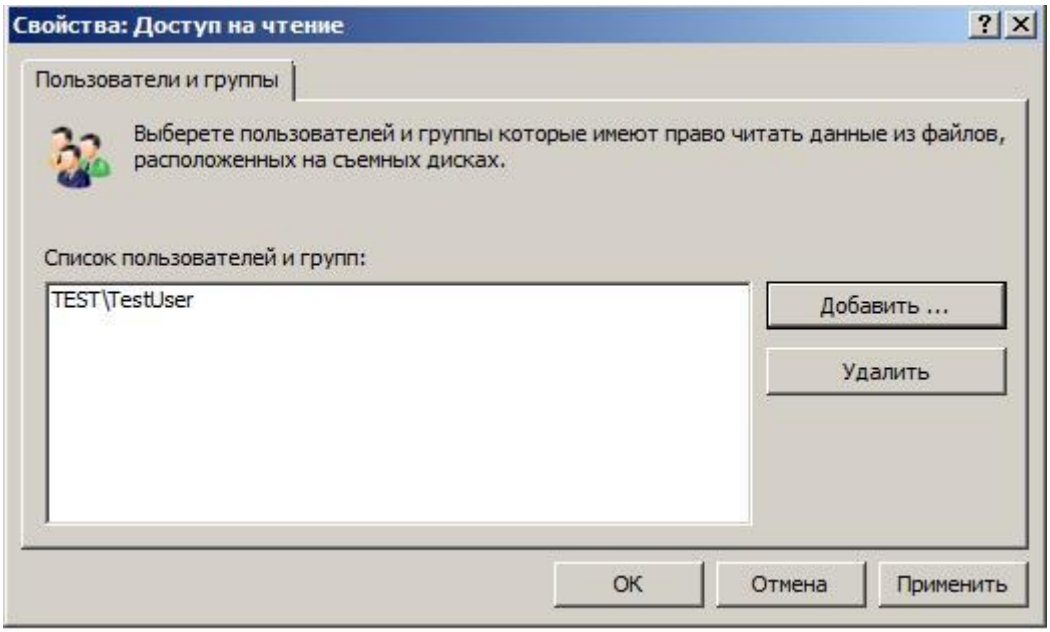
- Чтение
- Запись

- 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).

Рис. 12. Список членов правила



После применения политики, указанные изменения вступят в силу.

4.3. Формирование политики доступа к съемным хранилищам данных

Политика доступа к съемным хранилищам данных SPR 4.0 реализует функции разграничения доступа пользователей к различным устройствам (съемные диски, CD-ROM и DVD диски, дискеты, переносные (WPD) устройства, порты, принтеры и т.д.). Доступ регулируется по типу доступа: чтение, запись и исполнение.

Для формирования политики защиты объектов файловой системы необходимо определить перечень устройств и тип разрешенного доступа. Политика доступа к съемным хранилищам позволяет определить устройства на уровне экземпляра или класса целиком. Определение на уровне экземпляра учитывает уникальный идентификатор устройства, в то время как определение на уровне класса устройств учитывает тип устройства.

Примечание

Определение на уровне экземпляра учитывает идентификатор, полученный от устройства, в связи с чем есть вероятность совпадения идентификаторов различных устройств. При формировании политики защиты рекомендуется использовать более широкие правила на уровне класса устройств.

При установке СЗИ SPR 4.0 создается правило по умолчанию политики доступа к съемным устройствам для экземпляра системного диска ОС и всех найденных экземпляров сетевых устройств передачи данных (сетевые карты). Данные правила обеспечивают корректную работоспособность АРМ и обеспечивают возможность сетевого взаимодействия после установки СЗИ. При необходимости уточнения параметров или в случае физической замены зарегистрированных компонентов, следует изменить соответствующие правила политики.

Рекомендуемой политикой, при разрешенном использовании пользователями съемных носителей информации, является запрет типа доступа «Исполнение». При назначении прав доступа к съемным устройствам следует использовать ролевую модель доступа и назначать права доступа для групп безопасности. Такой подход обеспечивает более простой контроль прав доступа путем контроля членства пользователя в соответствующей группе безопасности и снижает количество в списке контроля доступа политики.

При активации политики мандатного шифрования данных, соответствующие правила будут применяться только для данных на съемных носителях информации и при доступе пользователей, указанных в списке контроля доступа политики доступа к съемным хранилищам данных. Следует учитывать взаимосвязь настроек этих параметров при планировании настроек политики безопасности.

5. Настройка правил мандатного шифрования данных на съемных носителях

5.1. Установка режима работы политики мандатного шифрования

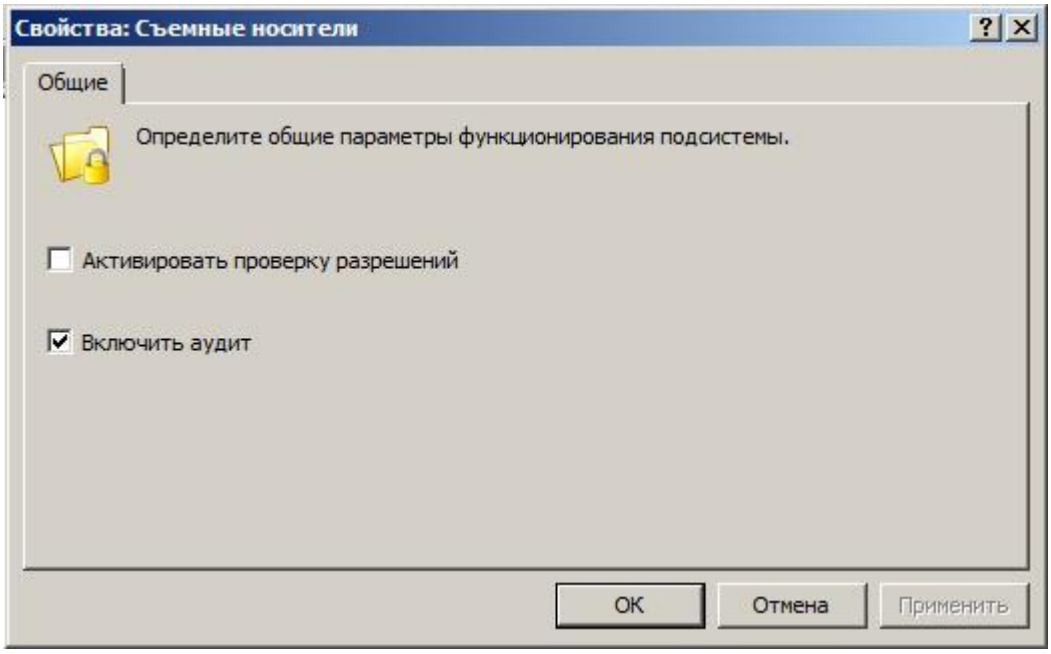
Внимание
На рабочих местах где планируется применение политик мандатного шифрования для защиты конфиденциальных данных необходимо установить средство хранения конфиденциальной информации КриптоПро EFS.
После первоначальной установки SPR 4.0 политика мандатного шифрования включена в режиме Аудит. Мандатное шифрование данных на съемных носителях информации в данном режиме не производится.

При первоначальной установке SPR 4.0 список правил политики мандатного шифрования пуст, поэтому активация политики приведет к блокировке доступа к незашифрованным файлам на съемных носителях для всех пользователей. После установки SPR 4.0 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 КриптоПро SPR → 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).

Рис. 13. Активация политики



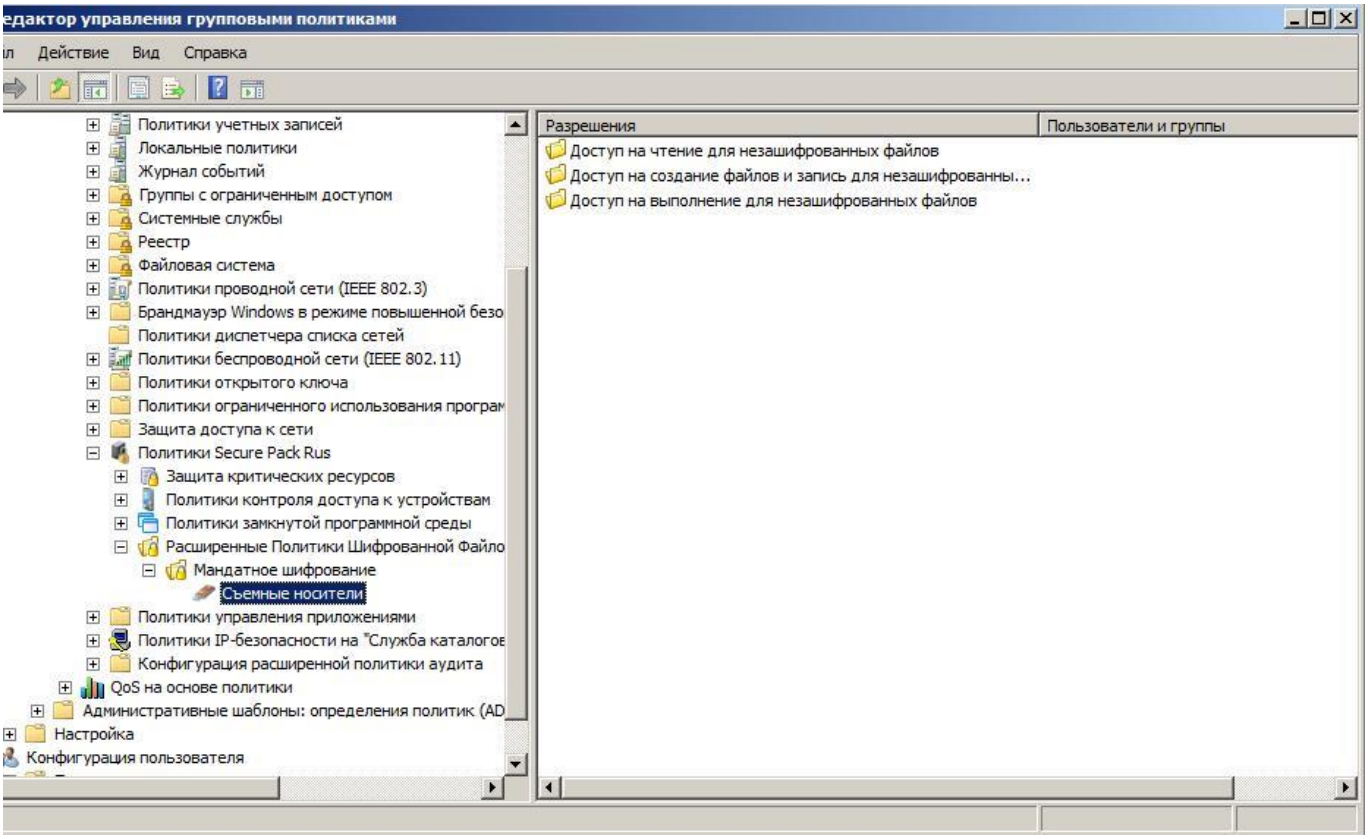
Активация проверки разрешений при доступе пользователей к файлам на съемных носителях запретит любое действие, не разрешенное администратором правилами политики мандатного шифрования.

5.2. Управление 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 КриптоПро SPR → Расширенные политики шифрованной файловой системы (EFS) → Мандатное шифрование → Съемные устройства» (Рис. 14)

Рис. 14. Типы разрешений доступа

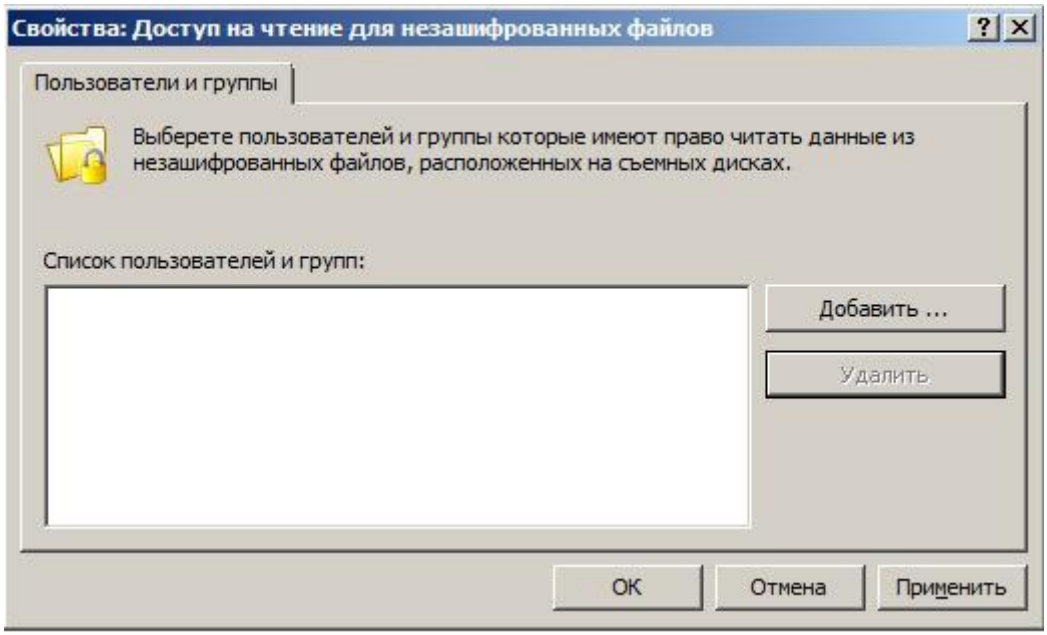


SPR 4.0 различает три типа доступа с незашифрованным файлам на съемных носителях:

- чтение
- чтение и запись
- исполнение

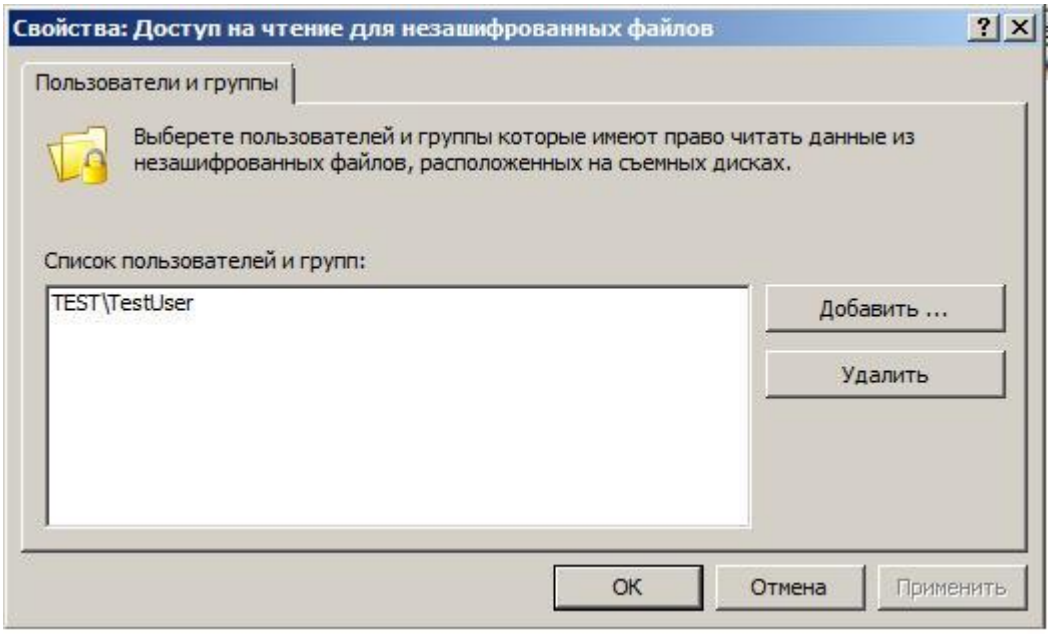
Для того что бы дать разрешение пользователю или группе безопасности на определенный тип доступа к незашифрованным данным на съемных устройствах необходимо добавить этого пользователя или группу в соответствующий пункт групповой политики. Для этого необходимо выделить пункт групповой политики, вызвать меню и выбрать пункт «Свойства». В открывшемся окне выполнить действие «Добавить» и выбрать пользователя или группу безопасности (Рис. 15).

Рис. 15. Добавление пользователя или группы



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

Рис. 16. Список членов правила



После применения политики, указанные изменения вступят в силу.

5.3. Формирование политики мандатного шифрования

Подсистема мандатного шифрования реализует возможность административного управления шифрованием данных, сохраняемых пользователем на съемные носители информации или считываемых пользователем со съемных носителей информации. Подробное описание возможных режимов настройки политики мандатного шифрования описано в (6).

Примечание

При активации политики мандатного шифрования данных, соответствующие правила будут применяться только для данных на съемных носителях информации и при доступе пользователей, указанных в списке контроля доступа политики доступа к съемным хранилищам данных.

Настройка правил мандатного шифрование предполагает разрешение доступа определенной политикой группы пользователей с съемных носителей информации. Тип доступа при обработке незашифрованной информации («чтение незашифрованной информации» / «запись незашифрованной информации» / «запрет обработки незашифрованной информации») определяется администратором на основе режимов обработки информации.

Примечание

Подсистема мандатного шифрования опирается на механизм шифрованной файловой системы ОС Windows – EFS. Для корректной работы механизма EFS, разделы диска съемного устройства хранения должны быть предварительно отформатированы для использования файловой системы NTFS.

Поддержка использование отечественных криптоалгоритмов ГОСТ реализована с использованием СКЗИ Крипто Про CSP и Крипто Про EFS. Для корректной работы механизмов EFS необходимо выполнить ряд предварительных настроек (выпуски установка сертификатов правильного формата для пользователей из состава групп, указанных в правилах политики мандатного шифрования). Информацию требуемых настройках можно получить в документации на ОС Windows и СКЗИ Крипто Про EFS.

6. Вывод графических окон сервисом КриптоПро CSP КС3

В процессе работы сервис CSP КриптоПро 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.

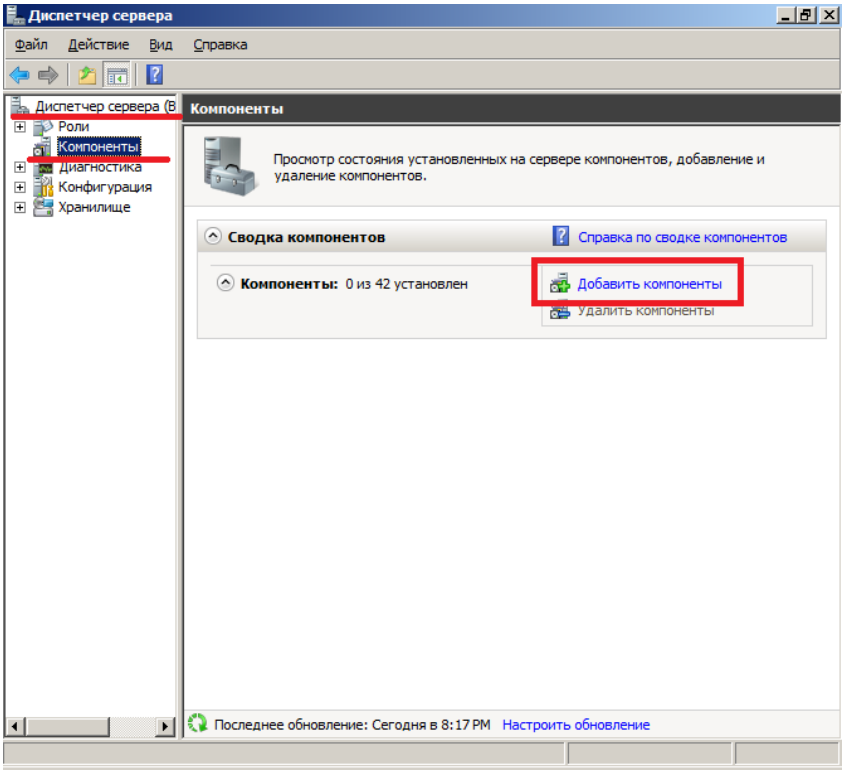
В связи с изменениями в подсистеме защиты пользовательских ОС семейства Windows 7 / 8 и серверных ОС семейства Windows Server 2008 / 2012 для вывода графических окон CSP КриптоПро использует новый сервис ОС, в связи с чем возможны ошибочные действия пользователя при работе с этими окнами. Ниже описана процедура работы пользователя с окнами CSP КриптоПро 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 КриптоПро 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 КриптоПро в ОС семейства Windows Server 2008 / 2012 необходимо активировать «Службы рукописного ввода» «Пуск → Администрирование → Диспетчер сервера → Компоненты → Добавить компоненты» (Рис. 17)

Рис. 17. Добавление компоненты



В списке доступных компонент выбрать «Службы рукописного ввода» и завершить установку (Рис. 18 - Рис. 22).

Рис. 18.

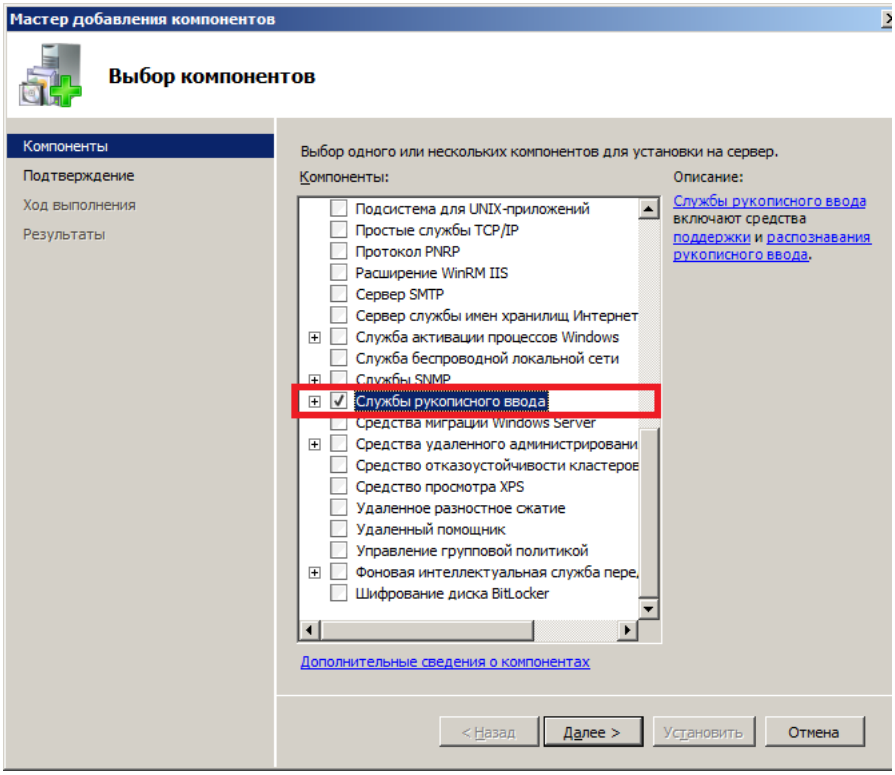


Рис. 19.

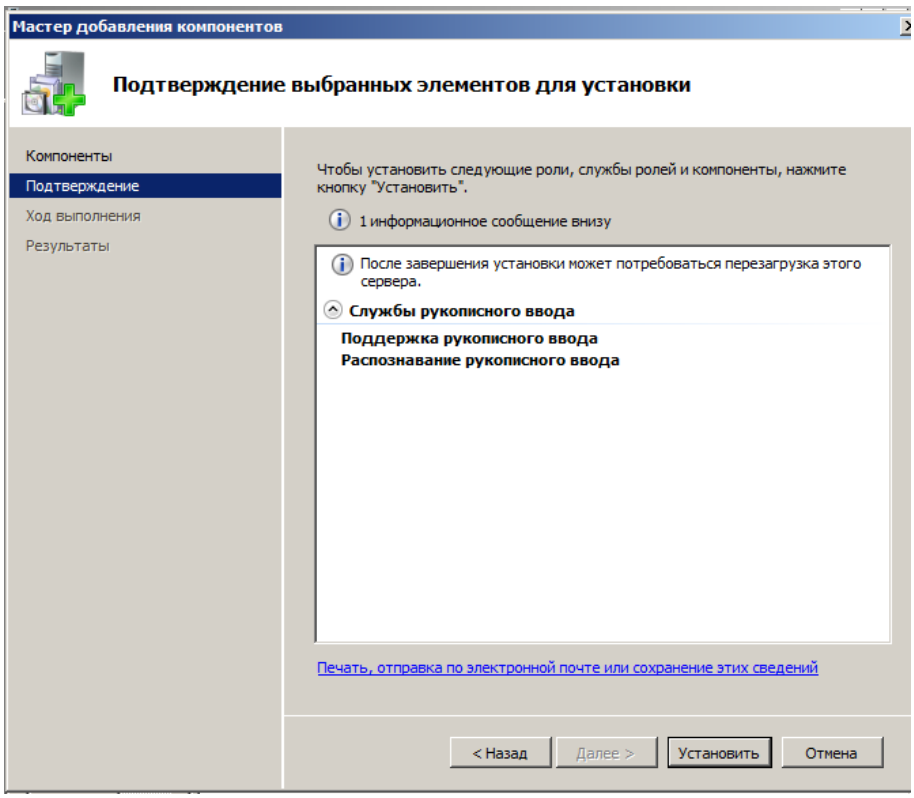


Рис. 20.

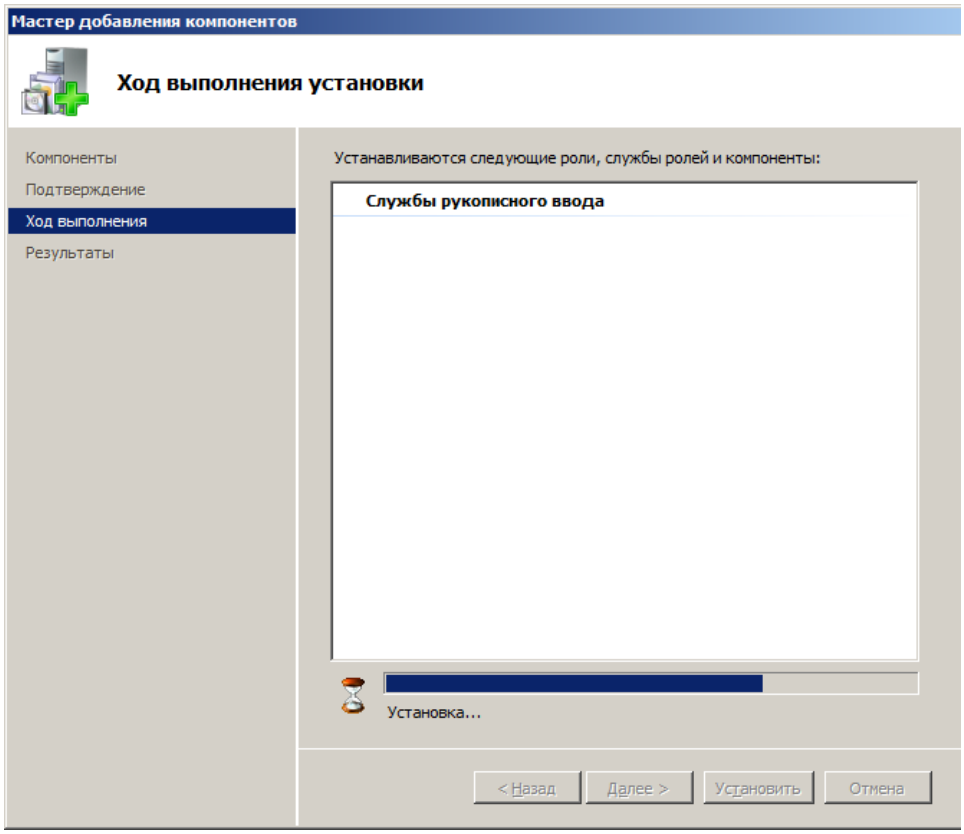

Мастер добавления компонентов
Ход выполнения установки
Компоненты
Подтверждение
Ход выполнения
Результаты
Устанавливаются следующие роли, службы ролей и компоненты:
Службы рукописного ввода
Установка...
< Назад
Далее >
Установить
Отмена

Рис. 21.

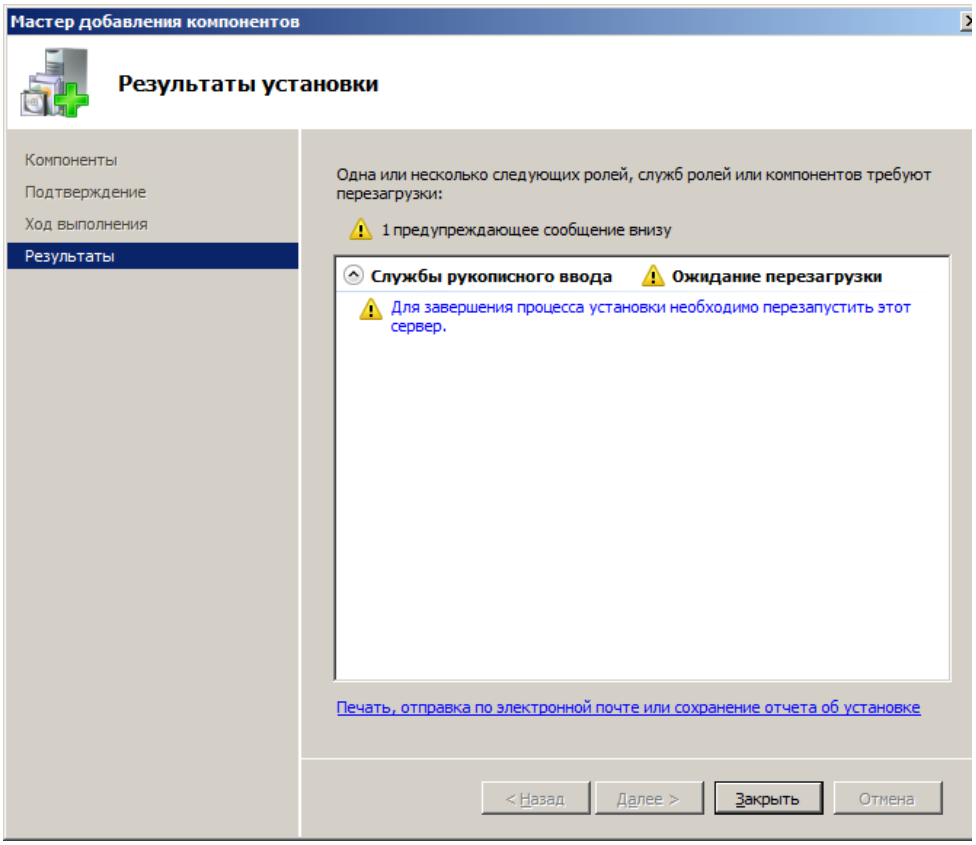
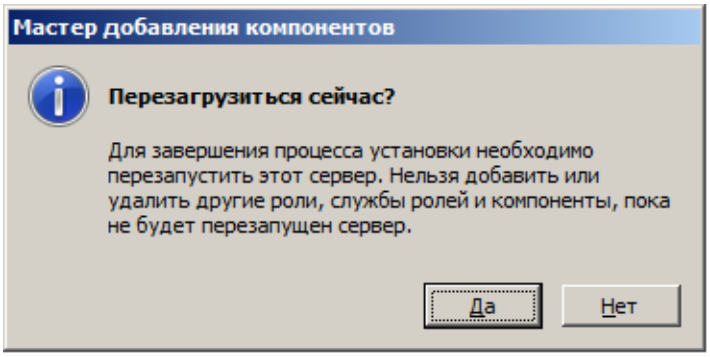
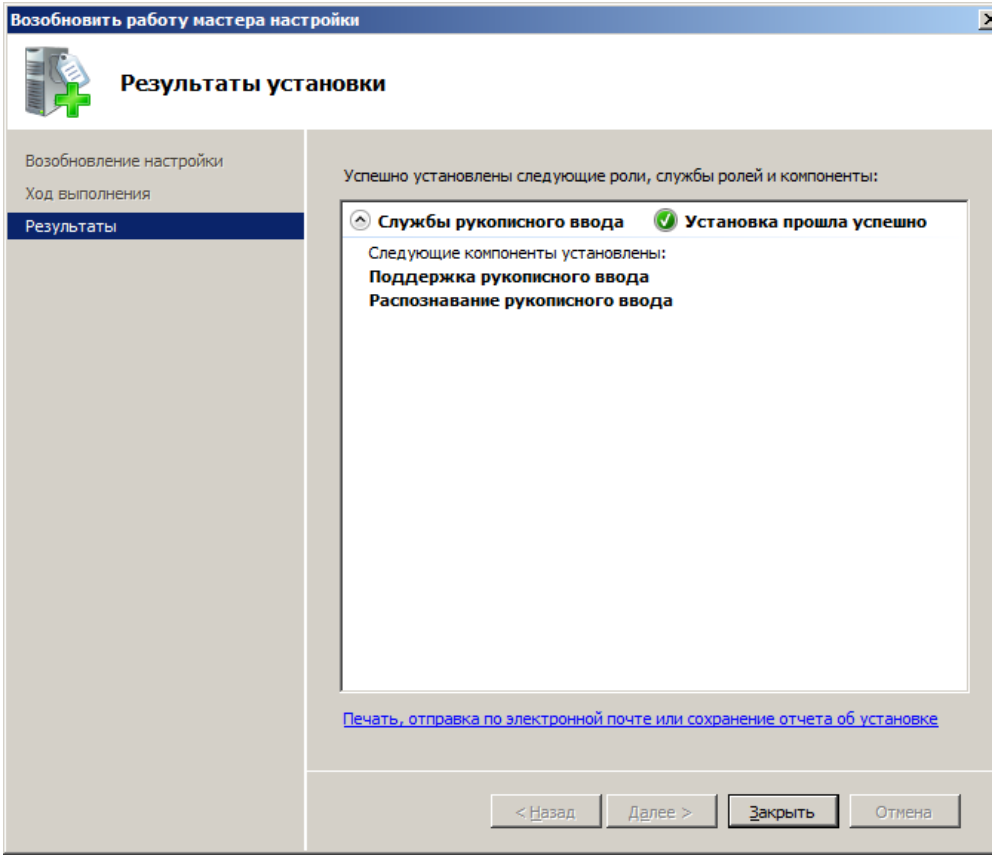

Мастер добавления компонентов
Результаты установки
Компоненты
Подтверждение
Ход выполнения
Результаты
Одна или несколько следующих ролей, служб ролей или компонентов требуют перезагрузки:
1 предупреждающее сообщение внизу
Службы рукописного ввода
Ожидание перезагрузки
Для завершения процесса установки необходимо перезапустить этот сервер.
Печать, отправка по электронной почте или сохранение отчета об установке
< Назад
Далее >
Закрыть
Отмена

Рис. 22.



После перезагрузки ОС будет продолжена установка службы (Рис. 23).

Рис. 23. Установка службы



6.2. Настройка серверных ОС Windows Server 2016

Для корректного отображения окон информации сервисом CSP КриптоПро для серверных ОС семейства Windows Server 2016 дополнительных настроек не требуется.

6.3. Работа с окнами сервиса КриптоПро CSP КС3

При работе пользователя сервис CSP КриптоПро может выводить сообщения для взаимодействия с пользователем – пример такого сообщения представлен на Рис. 24 и Рис. 25.

Рис. 24. Сообщение сервиса КриптоПро CSP

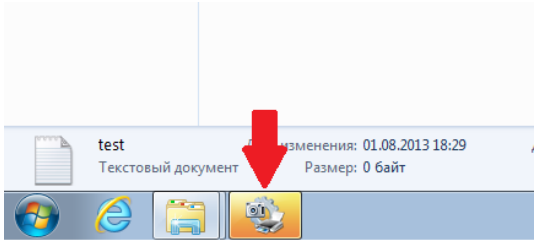
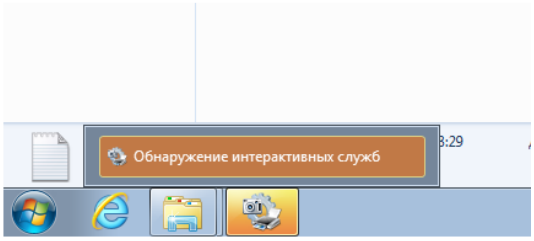


Рис. 25. Сообщение сервиса КриптоПро CSP



Возникновении такого сообщения означает, что криптографической подсистеме необходимо взаимодействие с пользователем. Пользователь должен перейти в окно приглашения (Рис. 26 и

Рис. 27) и выбрать действие «Посмотреть сообщение», после чего выполнить необходимые действия (например, генерацию последовательности случайных чисел – Рис. 28).

Рис. 26. Окно взаимодействия с сервисом КриптоПро CSP

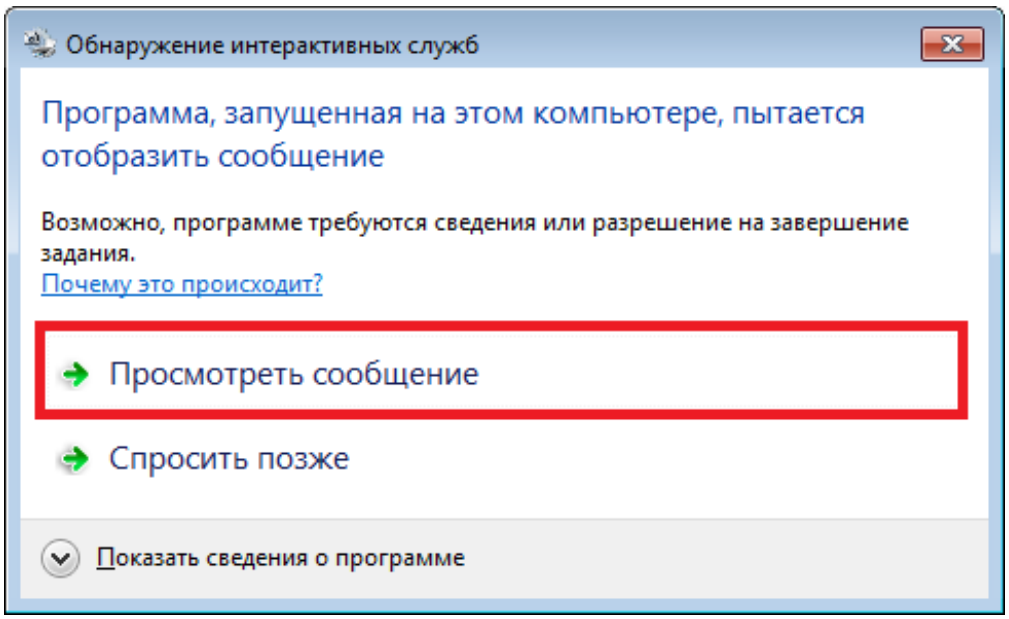


Рис. 27. Окно взаимодействия с сервисом КриптоПро CSP

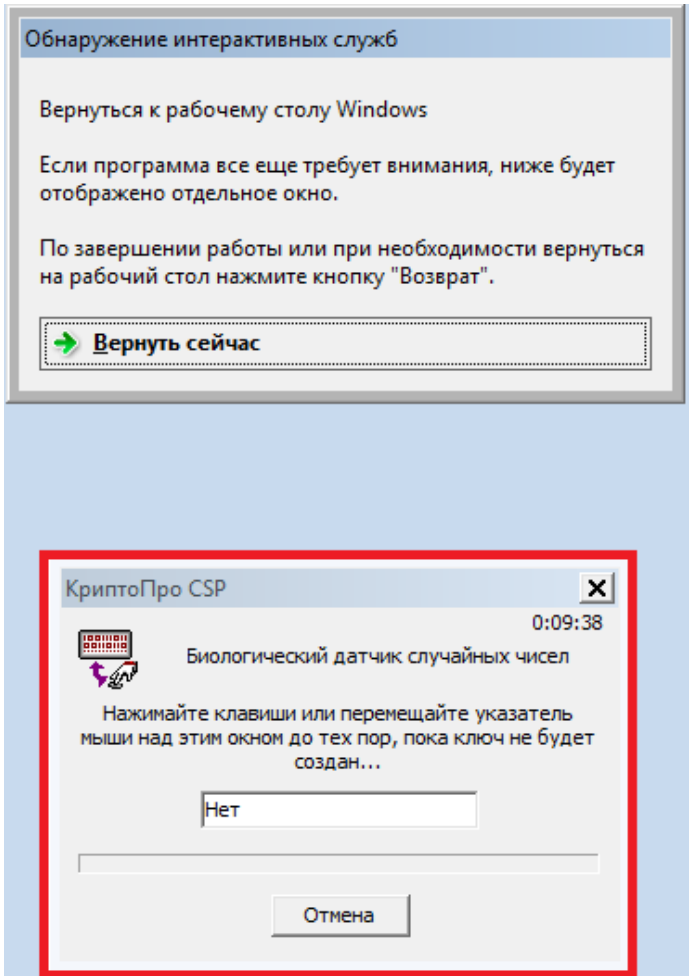
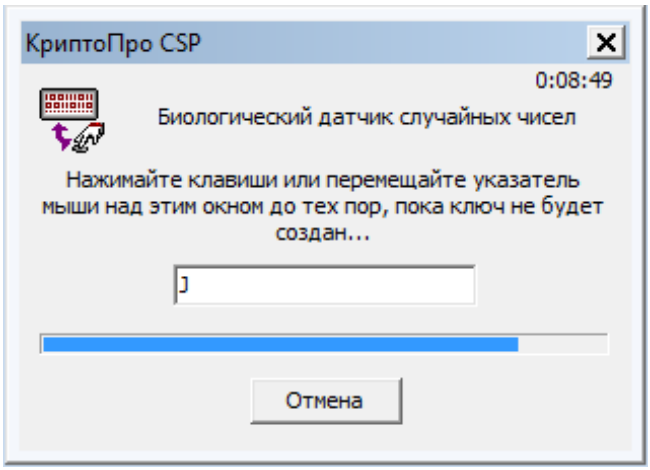
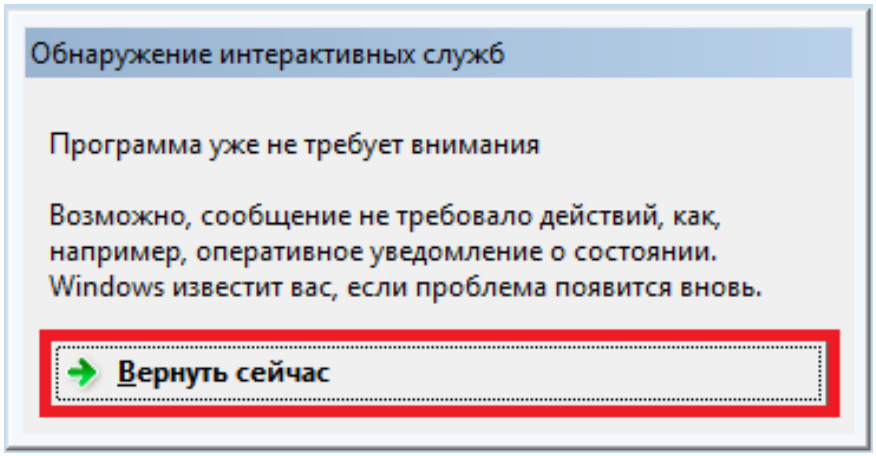


Рис. 28. Выполнение действий в окне сервиса



После выполнения действия в окне сервиса для возврата в режим работы с рабочим столом Windows пользователь должен выбрать действие «Вернуть сейчас» (Рис. 29).

Рис. 29. Завершение взаимодействия с сервисом КриптоПро CSP



Примечание

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

7. Использование дополнительных средств защиты загрузки

Использование программного СЗИ SPR 4.0 для защиты АРМ не обеспечивает запрет доступа пользователей к ресурсам компьютера в обход механизмов системы защиты. Для обеспечения контроля загружаемой ОС на АРМ могут использоваться технические средства доверенной загрузки (АПМДЗ), либо внедряться комплексные организационно-технических мероприятия, обеспечивающие невозможность доступа пользователей к информации на АРМ в обход механизмов защиты.

При использовании решений АПМДЗ необходимо обеспечить контроль целостности файлов СЗИ SPR 4.0 на этапе загрузки ОС. По умолчанию установка СЗИ SPR 4.0 производиться по стандартному пути ФС «C:\Program Files». Необходимо убедиться в постановке пути установки СЗИ SPR 4.0 на контроль модуля АПМДЗ.

Список литературы

1. **Компания "КРИПТО-ПРО".** Руководство администратора безопасности. Установка. *Средство защиты информации «КриптоПро SPR» версия 4.0.* ЖТЯИ.00112-01 90 02.

2. —. Руководство администратора безопасности. Аутентификация. *Средство защиты информации «КриптоПро SPR» версия 4.0.* ЖТЯИ.00112-01 90 03.

3. —. Руководство администратора безопасности. Аудит. *Средство защиты информации «КриптоПро SPR» версия 4.0.* ЖТЯИ.00112-01 90 05.

4. —. Руководство администратора безопасности. Политики управления приложениями. *Средство защиты информации «КриптоПро SPR» версия 4.0.* ЖТЯИ.00112-01 90 04.

5. —. Формуляр. *Средство защиты информации «КриптоПро SPR» версия 4.0.* ЖТЯИ.00112-01 30 01.