

**Средство защиты информации
«SecurePackRus»**

Версия 3.0

Руководство администратора безопасности

ЖТЯИ.00106-01 90 01

Листов 34



Компания «КРИПТО-ПРО»

2019

Компания «КРИПТО-ПРО», 2019. Все права защищены.

Этот документ входит в комплект поставки изделия. На него распространяются все условия лицензионного соглашения. Без специального письменного разрешения компании «КРИПТО-ПРО» этот документ или его часть в печатном или электронном виде не могут быть подвергнуты копированию и передаче третьим лицам с коммерческой целью.

Информация, содержащаяся в этом документе, может быть изменена разработчиком без специального уведомления, что не является нарушением обязательств по отношению к пользователю со стороны компании «КРИПТО-ПРО».

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	12
4. Политики контроля доступа к устройствам	14
4.1. Контроль доступа к съемным хранилищам данных	14
4.2. Управление правилами доступа к съемным хранилищам данных	15
4.3. Формирование политики доступа к съемным хранилищам данных	17
5. Настройка правил мандатного шифрования данных на съемных носителях	19
5.1. Установка режима работы политики мандатного шифрования	19
5.2. Управление правил политики мандатного шифрования.....	20
5.3. Формирование политики мандатного шифрования	22
6. Настройка правил контроля запуска сценариев	23
6.1. Установка режима работы политики контроля выполнения сценариев	23
6.2. Импорт и удаление правил политики контроля выполнения сценариев.....	24
7. Вывод графических окон сервисом КриптоПро CSP КСЗ	27
7.1. Настройка серверных ОС Windows Server 2008 / 2012	27
7.2. Настройка серверных ОС Windows Server 2016.....	30
7.3. Работа с окнами сервиса КриптоПро CSP КСЗ.....	30
8. Использование дополнительных средств защиты загрузки	32
9. Дополнительные требования к эксплуатации SPR 3.0 исполнения 1 и 2.	33
Список литературы	34

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. Основные подсистемы

Функционирование СЗИ SPR 3.0 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 3.0:

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

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



После первоначальной установки SPR 3.0 политика защиты объектов файловой системы включена в режиме Аудит. Контроль доступа пользователей к критическим 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 система*, вызвав меню, выбрать раздел «Свойства» и в открывшемся окне отметить пункт «Активировать действие правил» (рис.1)

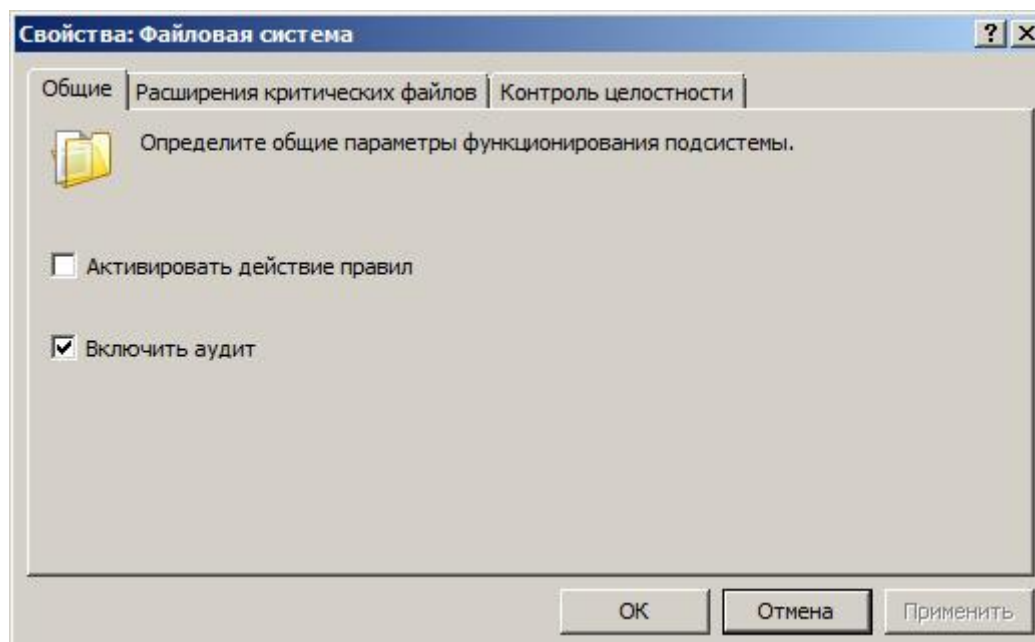


Рис.1

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 система* и, вызвав меню, выбрать раздел «Свойства», в открывшемся выбрать закладку «Расширения критических файлов» (рис. 2)

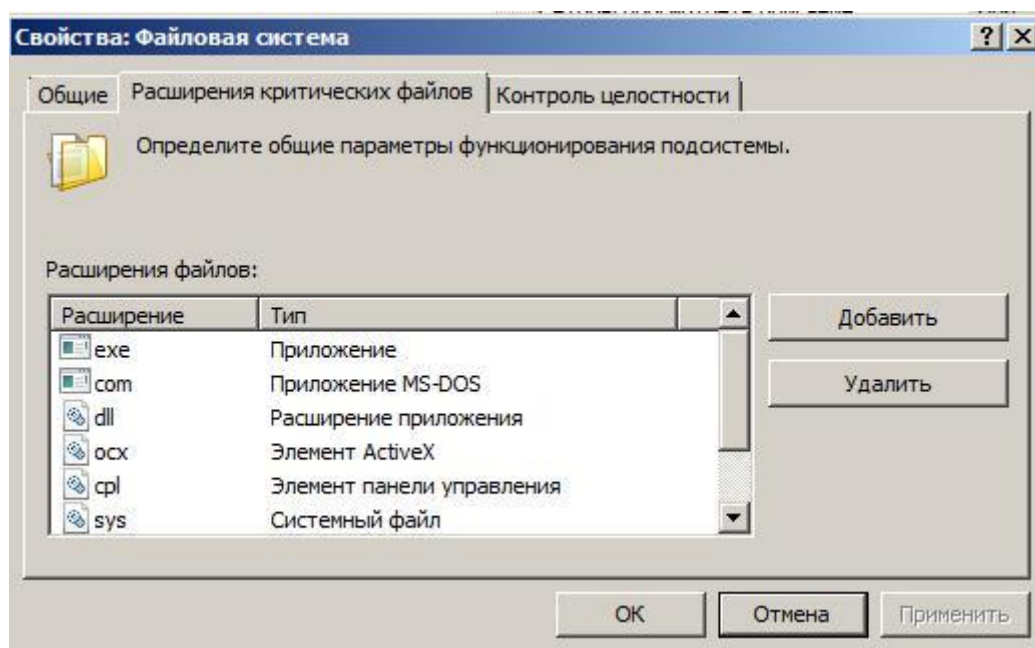


Рис.2

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 система* и, вызвав меню, выбрать раздел «Свойства», в открывшемся выбрать закладку «Контроль целостности» (рис. 3)

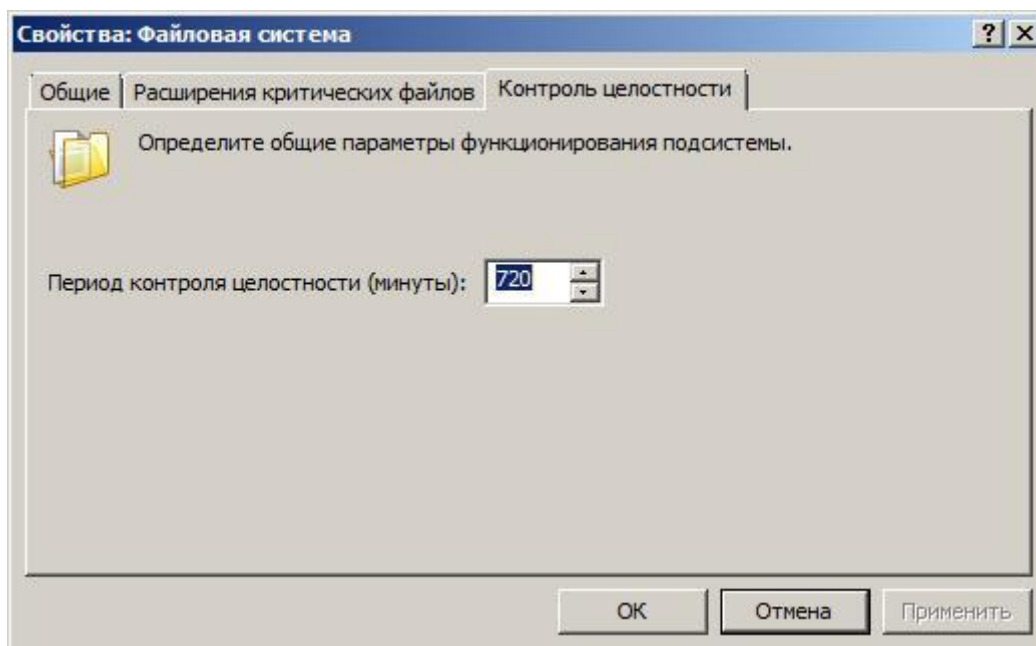


Рис. 3

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 SecurePackRus → Защита критических ресурсов → Файловая система* и, вызвав меню, выбрать раздел «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 в виде переменной среды.
- Нажать кнопку «Готово»

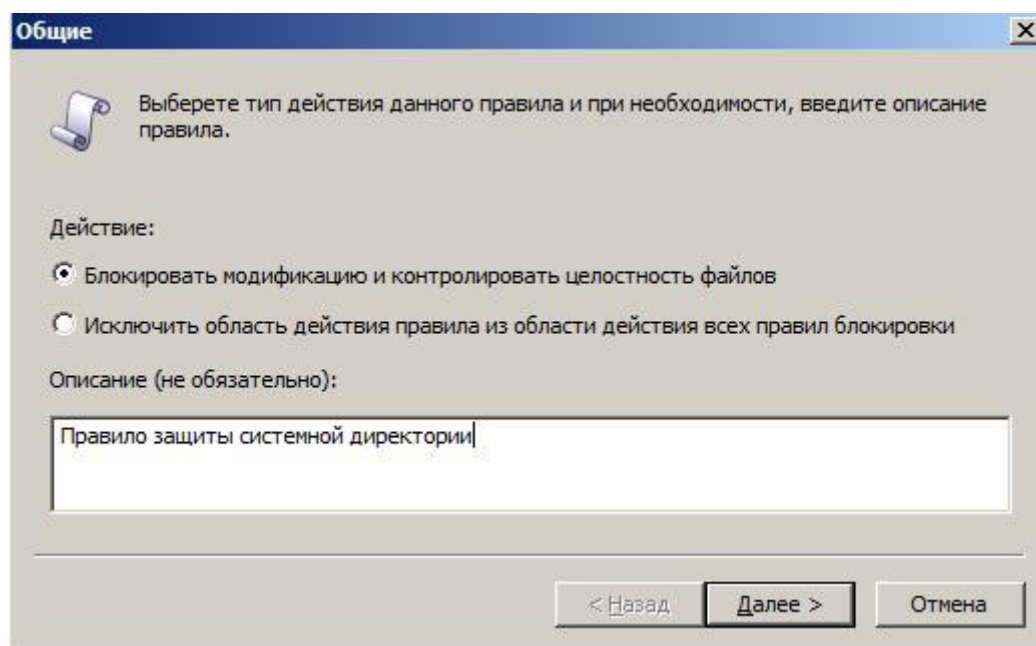


Рис 4

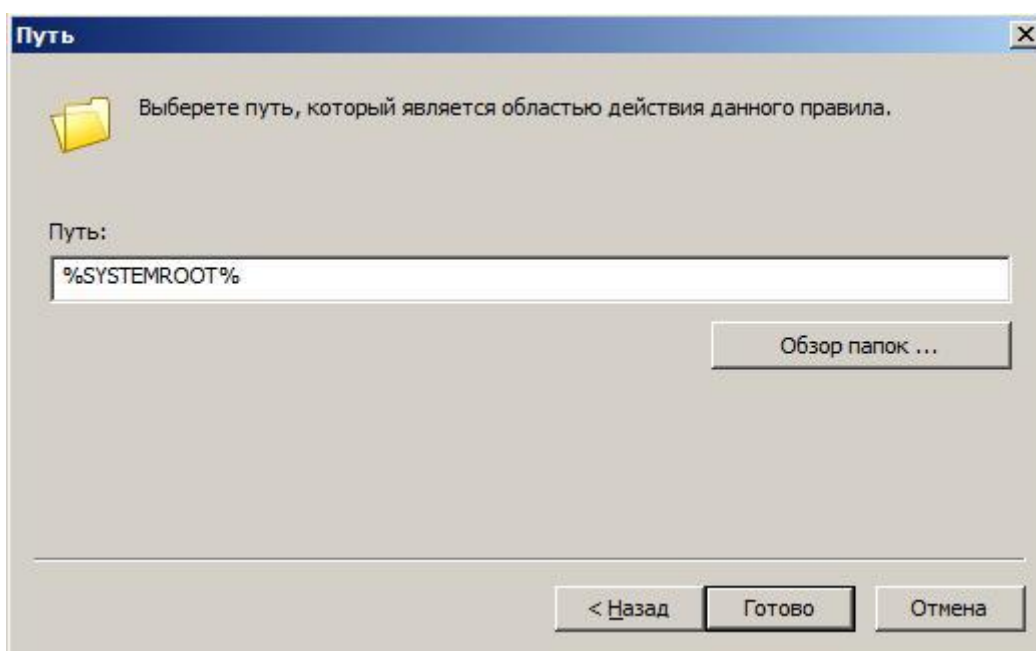


Рис 5

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 система и, вызвав меню, выбрать раздел «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 в виде переменной среды.
- Нажать кнопку «Готово»

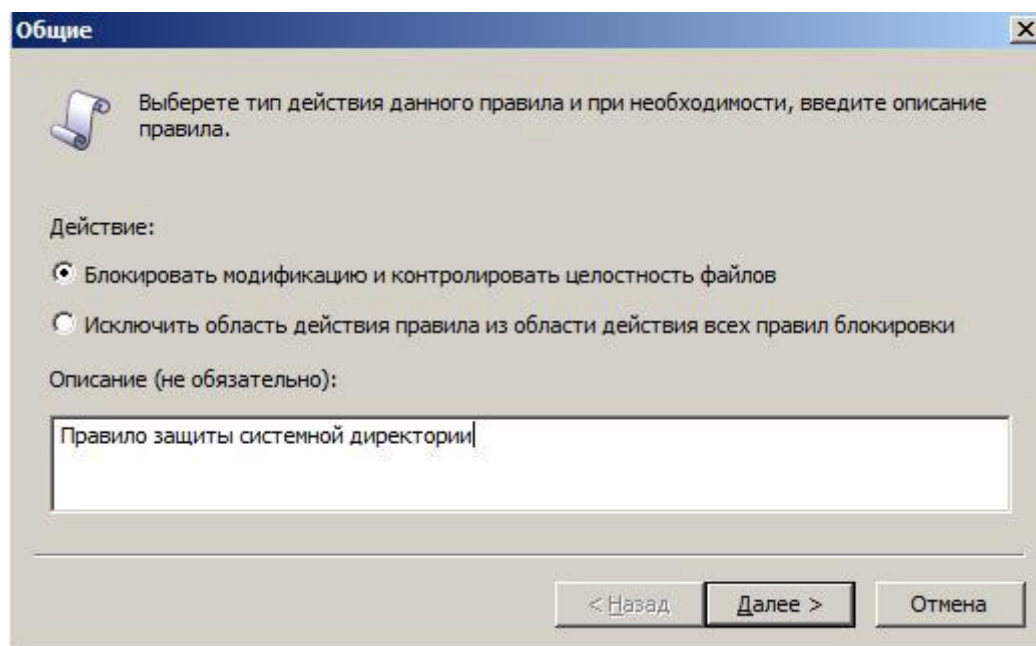


Рис 6

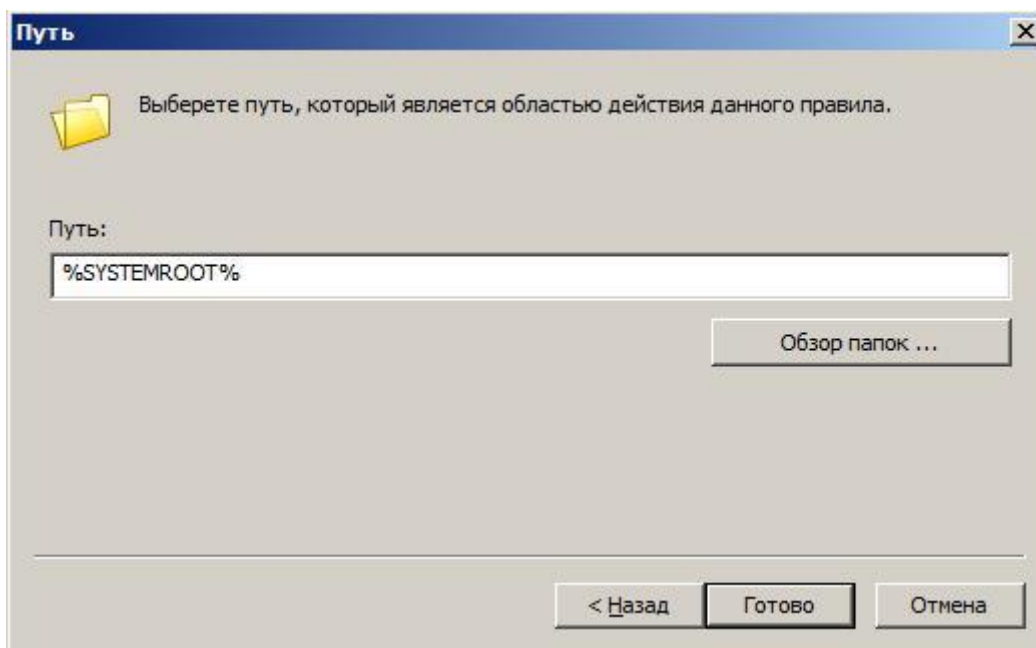


Рис 7

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

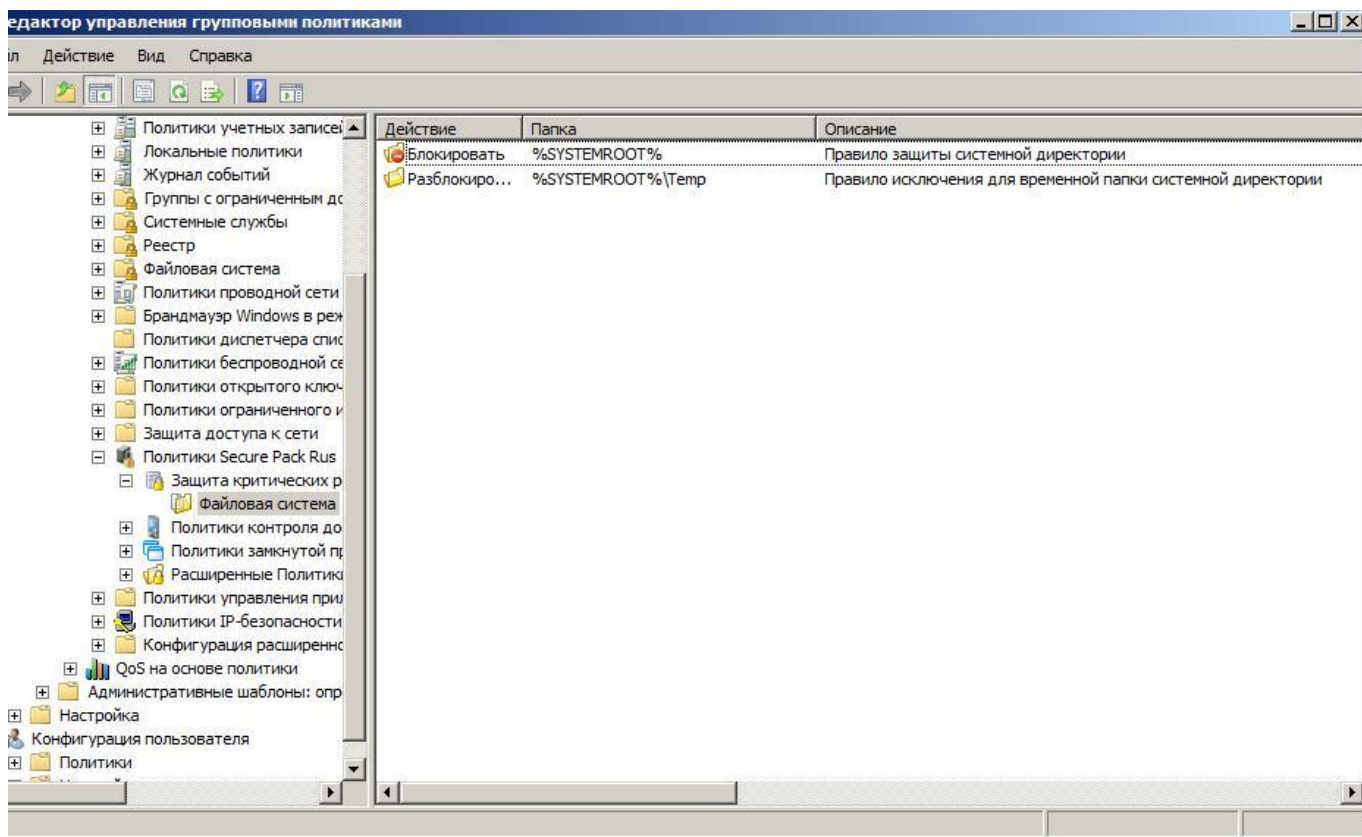


Рис. 8

3.3. Формирование политики защиты объектов файловой системы

Политика защиты объектов файловой системы SPR 3.0 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.



Необходимо учитывать, что в штатном режиме работы подсистема защиты критических ресурсов SPR 3.0 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 «С»). 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



После первоначальной установки SPR 3.0 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 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 раздел «Свойства» (Рис. 9)

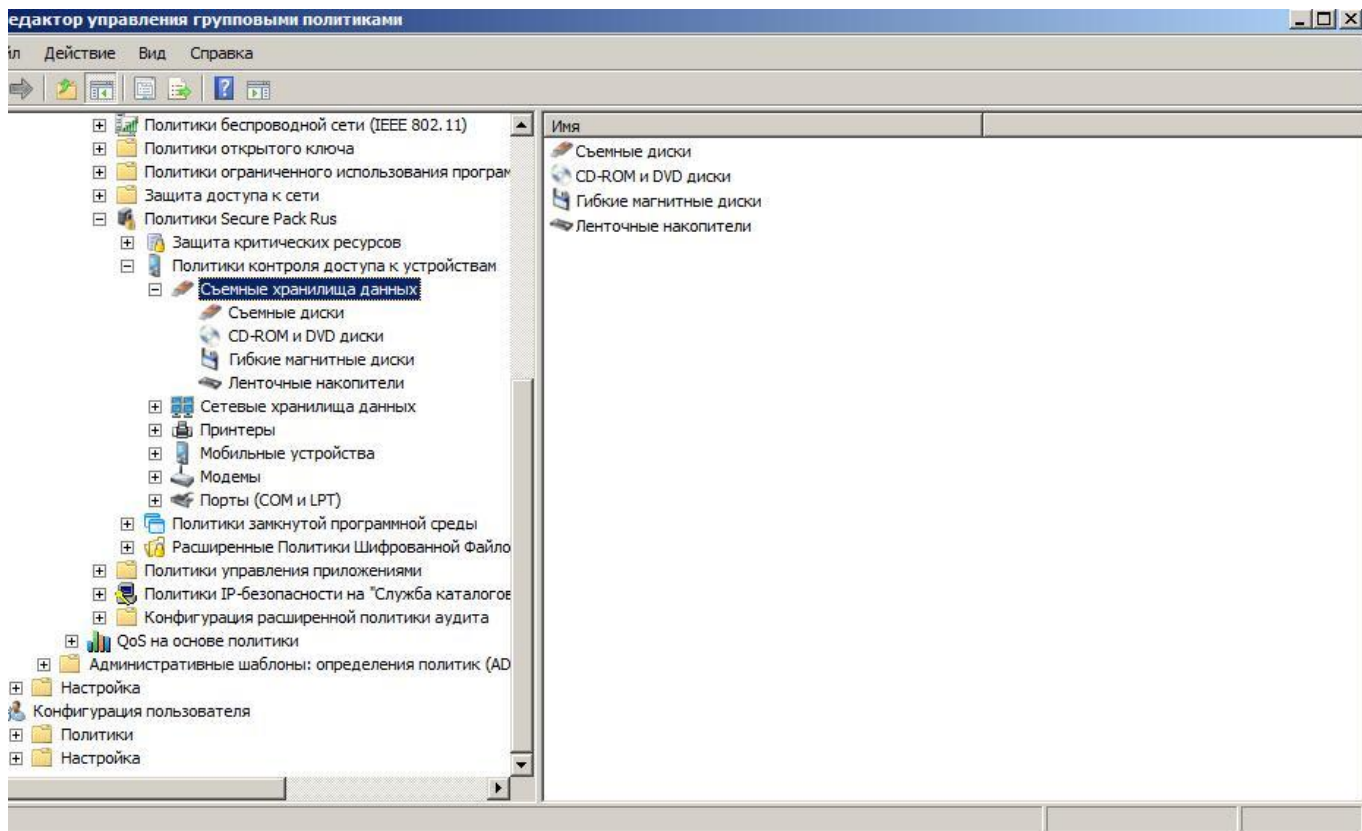


Рисунок 9 - Изменение режима работы политики

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

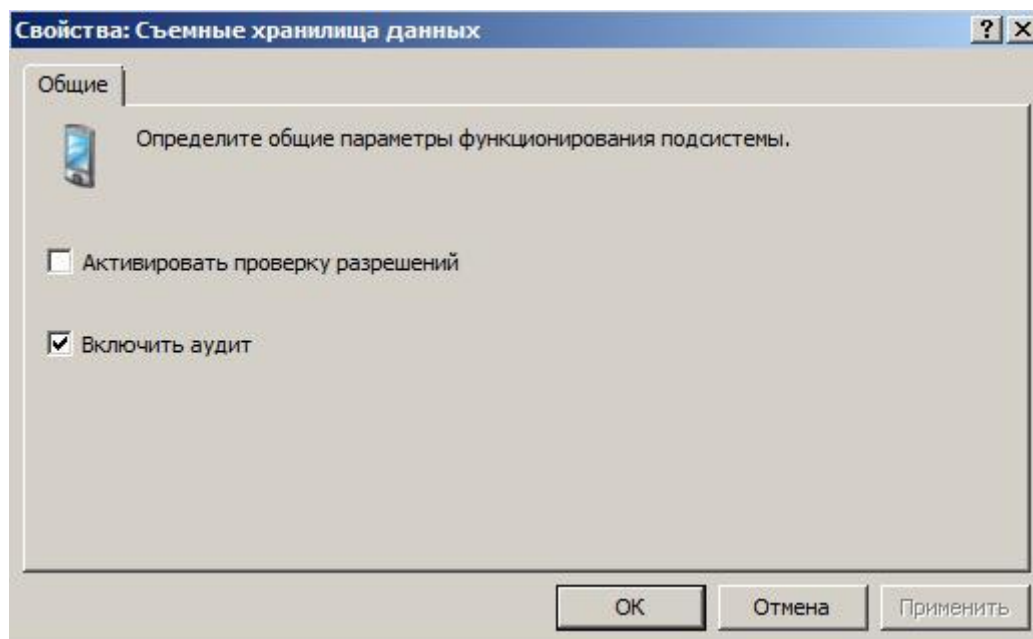


Рисунок 10 - Активация политики

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

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 SecurePackRus → Политика контроля доступа к устройствам → Съемные устройства* (Рис. 11).

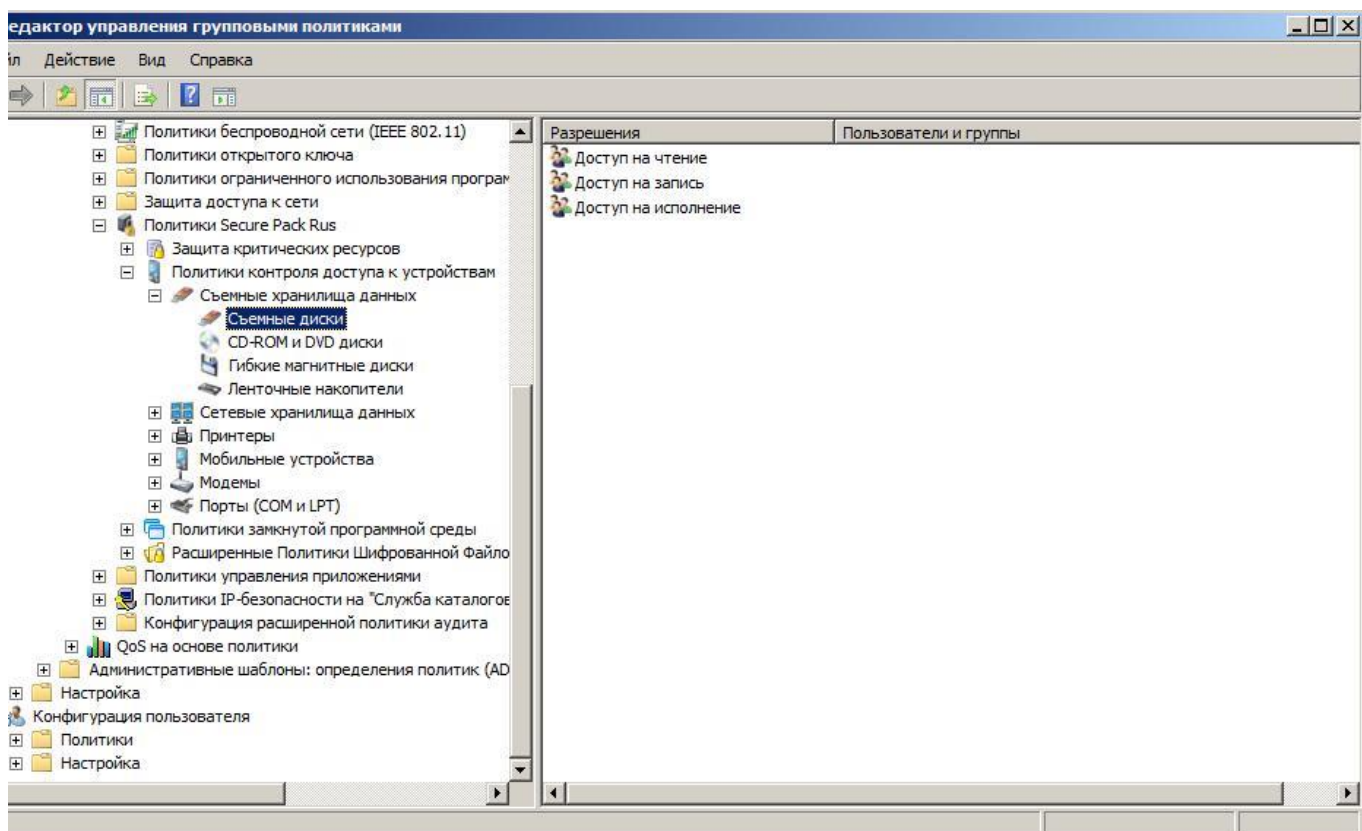


Рисунок 11 - Типы разрешений доступа

SPR3.0 различает следующие классы съемных хранилищ данных:

- съемные диски
- CD-ROM/DVD диски
- 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).

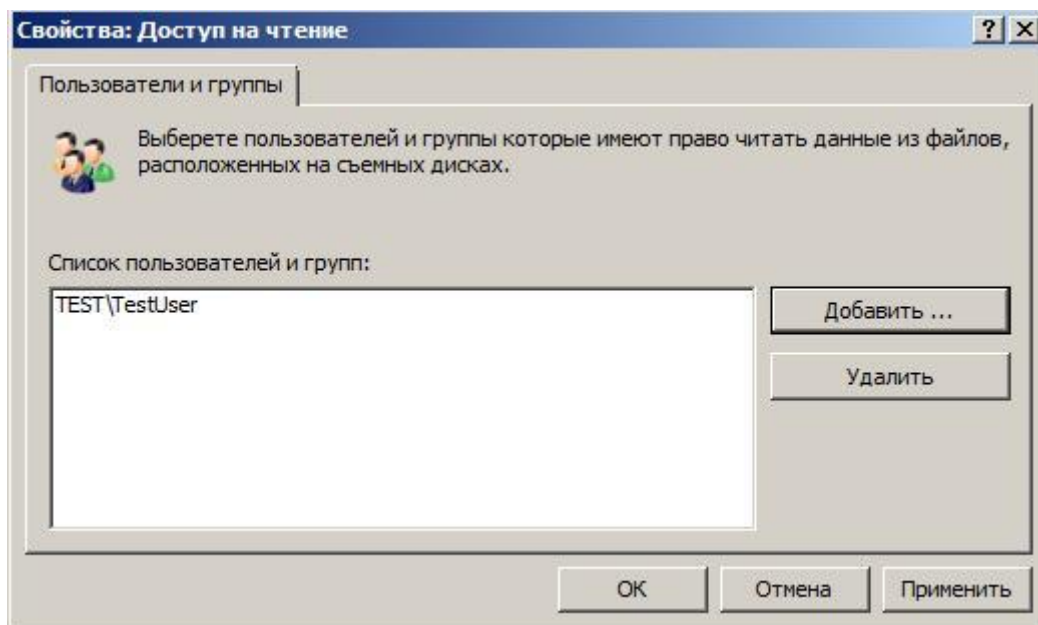


Рисунок 12 - Список членов правила

После применения политики, указанные изменения вступят в силу.

4.3. Формирование политики доступа к съемным хранилищам данных

Политика доступа к съемным хранилищам данных SPR 3.0 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.



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 3.0 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



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 раздел «Свойства»
- в открывшемся окне отметить пункт «Активировать проверку разрешений» (Рис. 13)

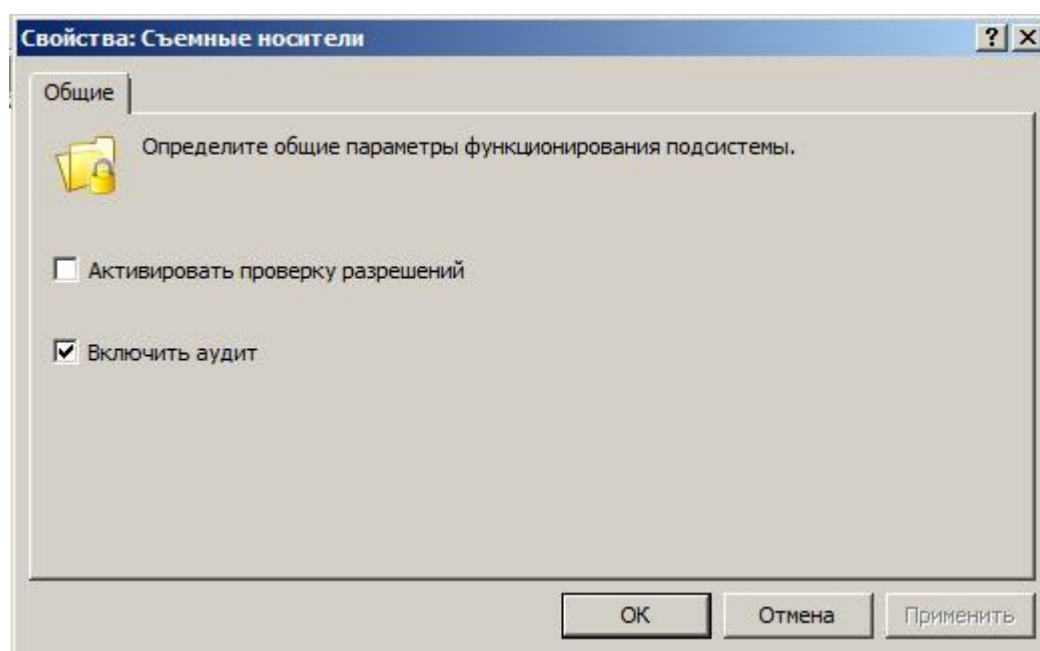


Рисунок 13 - Активация политики

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

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 SecurePackRus → Расширенные политики шифрованной файловой системы (EFS) → Мандатное шифрование → Съемные устройства (Рис. 14)*

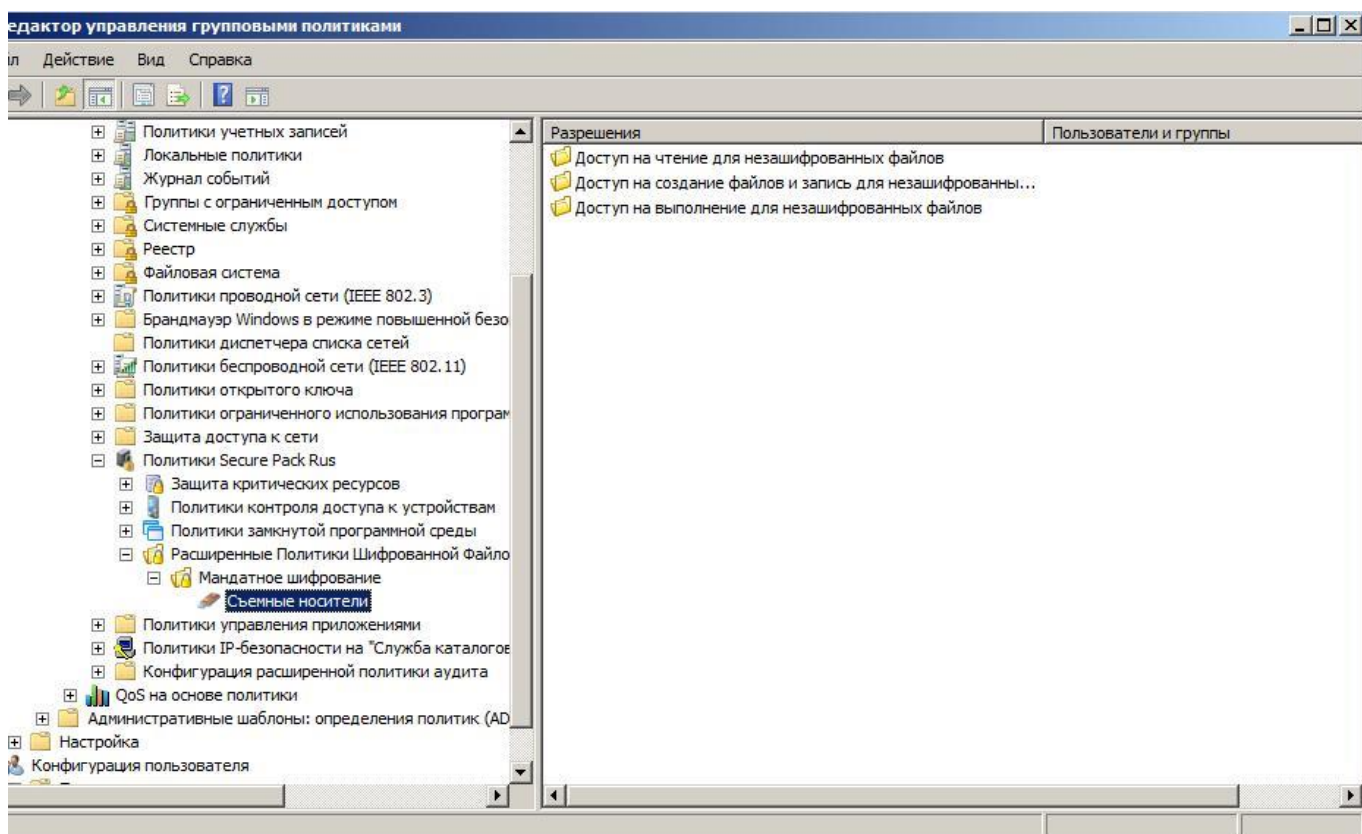


Рисунок 14 - Типы разрешений доступа

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

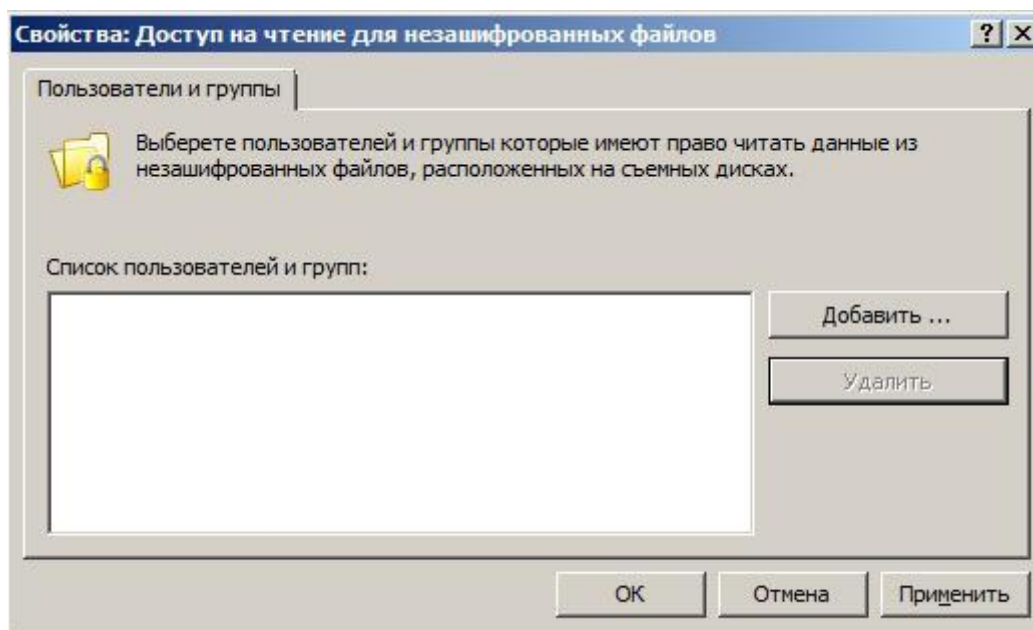


Рисунок 15 - Добавление пользователя или группы

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

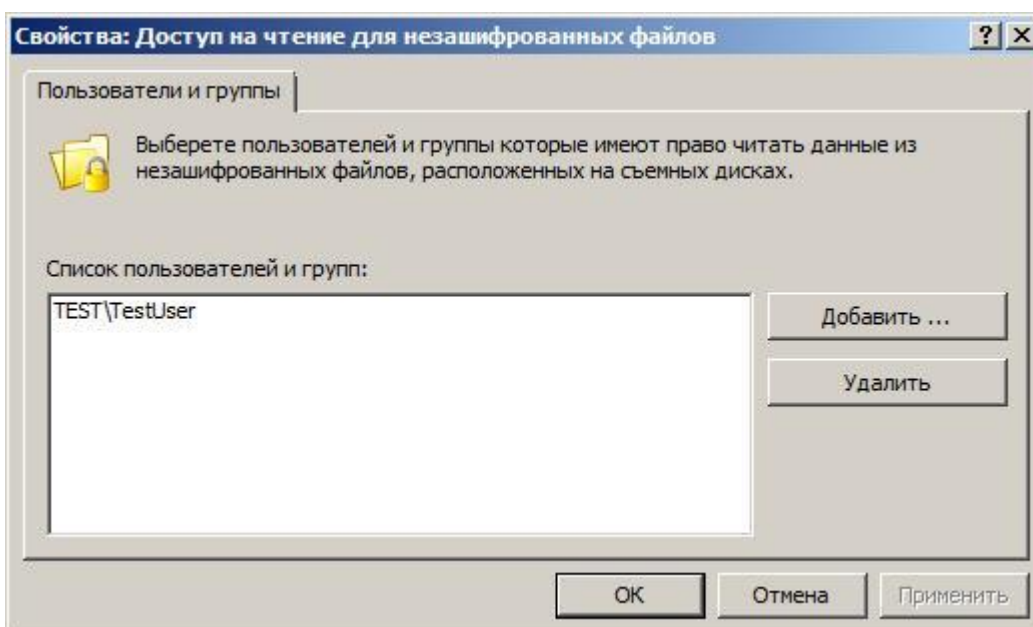


Рисунок 16 - Список членов правила

После применения политики, указанные изменения вступят в силу.

5.3. 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).



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 шифрования 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.



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 использования 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 настроек можно получить в документации на ОС Windows и СКЗИ Крипто Про EFS.

6. Настройка правил контроля запуска сценариев

6.1. 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 SPR3.0 необходимо определенное время на обучение подсистемы контроля выполнения сценариев. После чего необходимо импортировать список выполненных за 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 раздел «Свойства» (Рисунок 17)

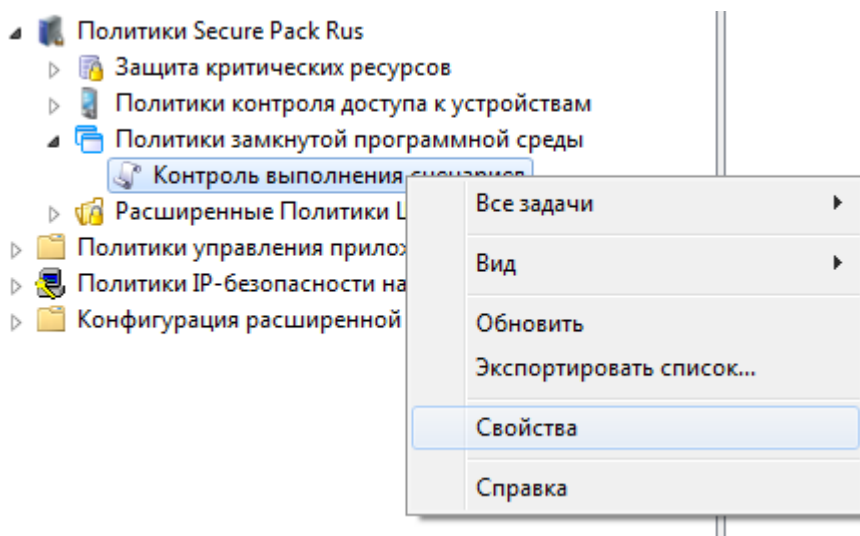


Рисунок 17 - Изменение режима работы политики

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

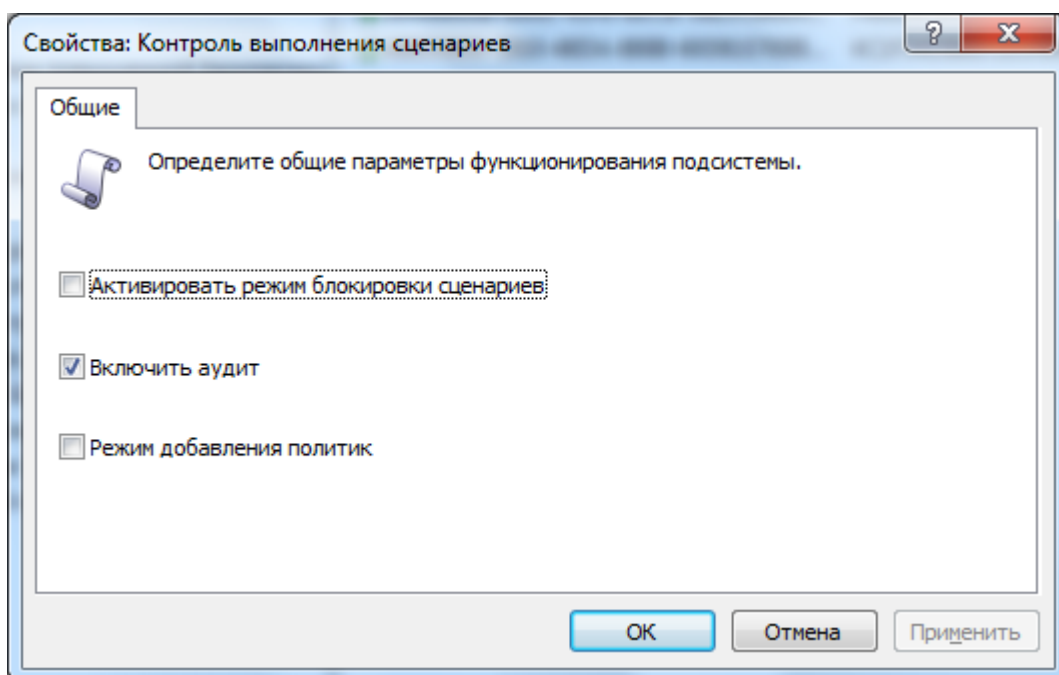


Рисунок 181 - Активация политики

Активация блокировки сценариев 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).

6.2. 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 импортировать разрешенные 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 сценариев, вызвав меню, выбрать раздел «Все задачи→Импортировать правила ...» (Рисунок)

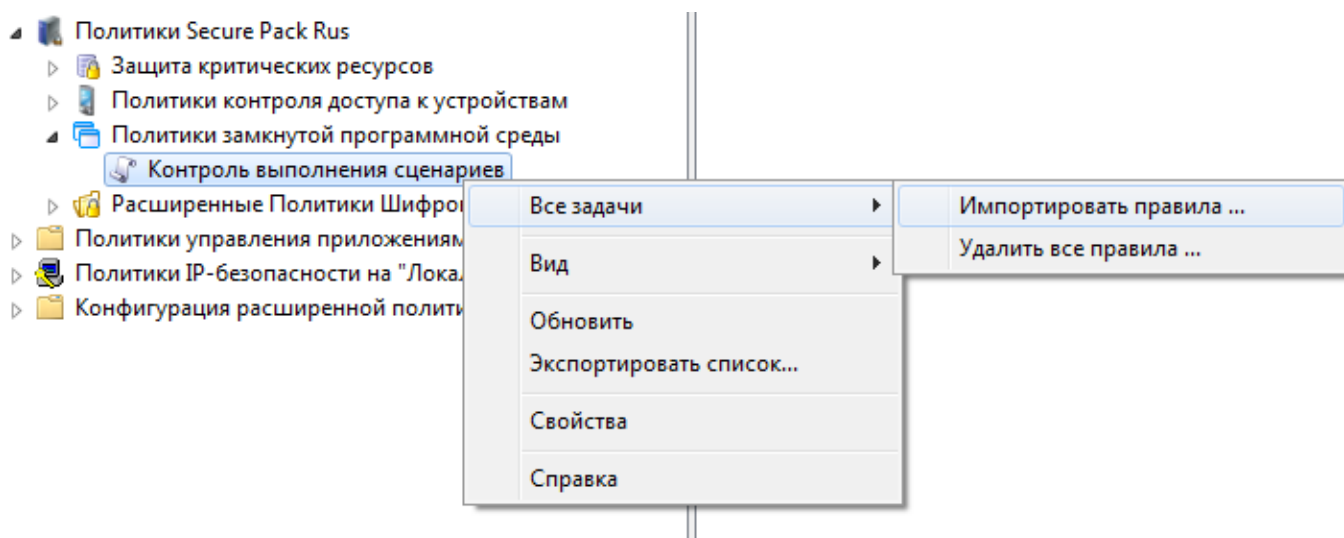


Рисунок 19 – Пункт меню «Импортировать правила»

- 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).

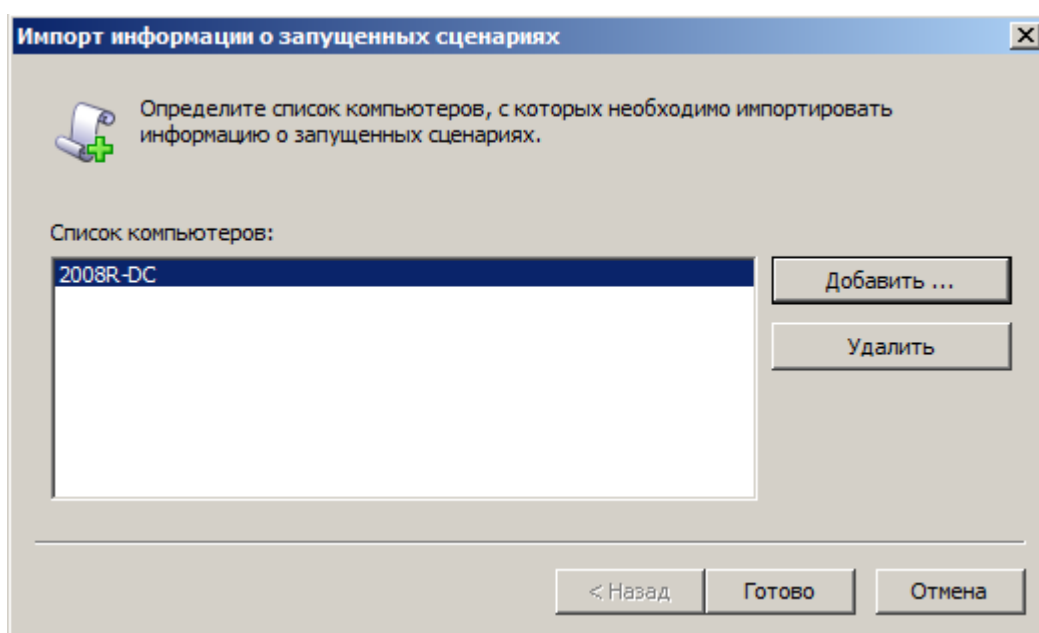


Рисунок 20 - Добавление компьютеров из домена

- 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).

№	Хэш
C87DEA82-6352-4AF9-808B-D7EE9AAD9E07	F491147EC4355AA8D4F5C00CCB5BA28C8F96E34D6B...
3AF7060E-8FA9-44FC-B99F-396F1FD65985	4C1F34DB8EF205A9482DCB9CA80A90254DF098B08F...
BDF2AFF9-31E1-4D0C-A83E-93FC68CB86A8	F7E5B89FB4FFE7D0CCB0F4A150F2075A615BBC7E25C...
EB26C98F-A4C1-4C94-9EB1-4A0D776B2B51	246F6B5D5C3ADD1961DAEAE7CD0748EF65D21F3F97...

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 сценариев* и, вызвав меню, выбрать раздел «Все задачи → Удалить все правила ...» (Рисунок).

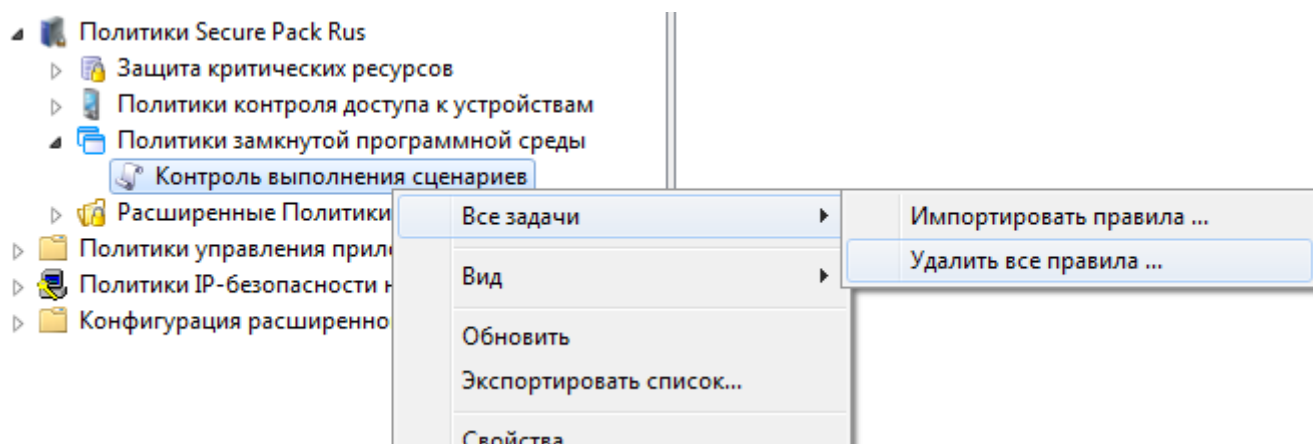


Рисунок 22 - Удаление всех правил

7. Вывод графических окон сервисом КriptoПро CSP KC3

В процессе работы сервис CSP КriptoПро 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 КriptoПро 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 КriptoПро и условия, необходимые для их корректного отображения в серверных ОС семейства Windows Server 2008 / 2012.

7.1. Настройка серверных ОС Windows Server 2008 / 2012

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

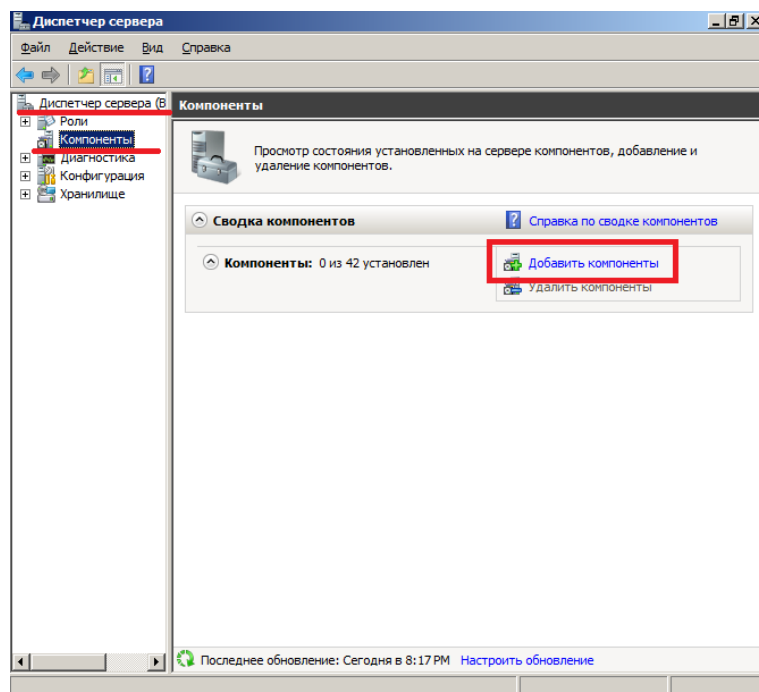
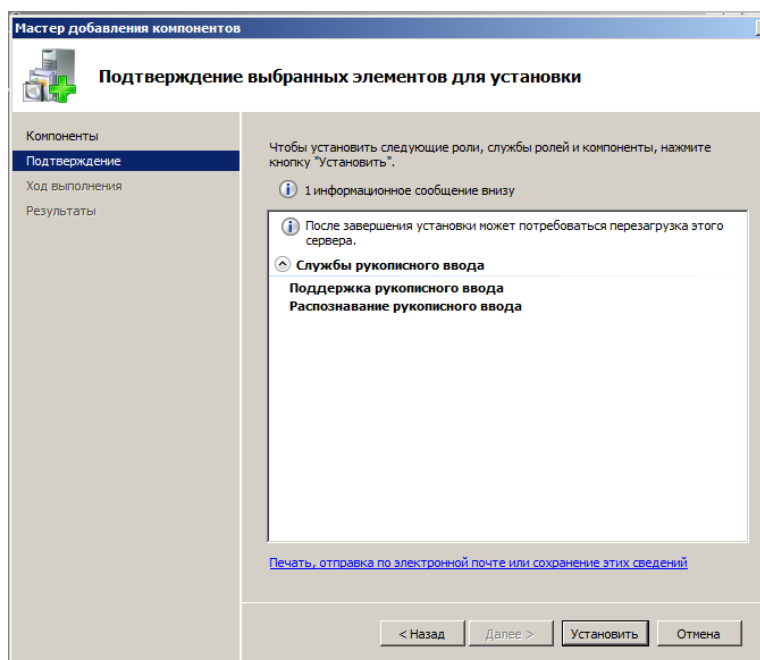
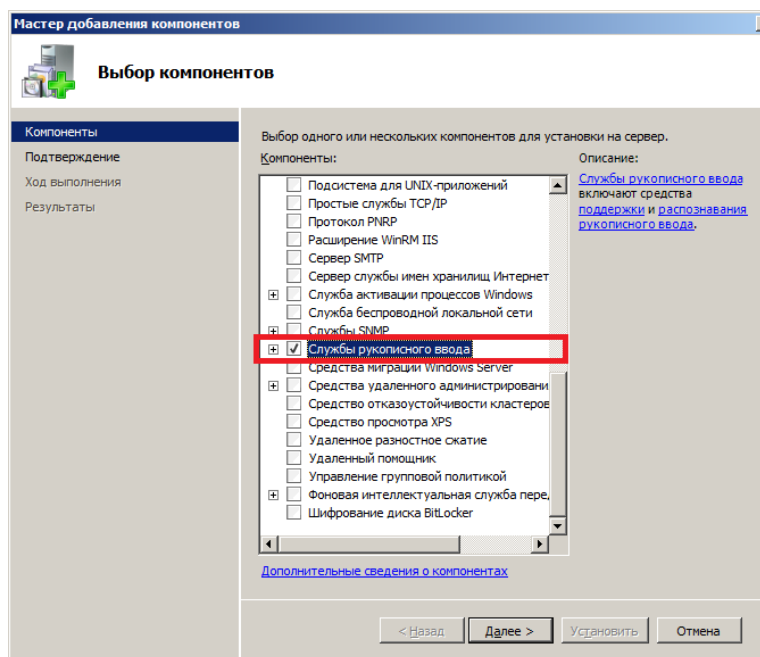


Рис.23 – Добавление компоненты

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



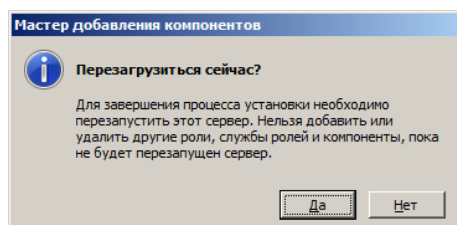
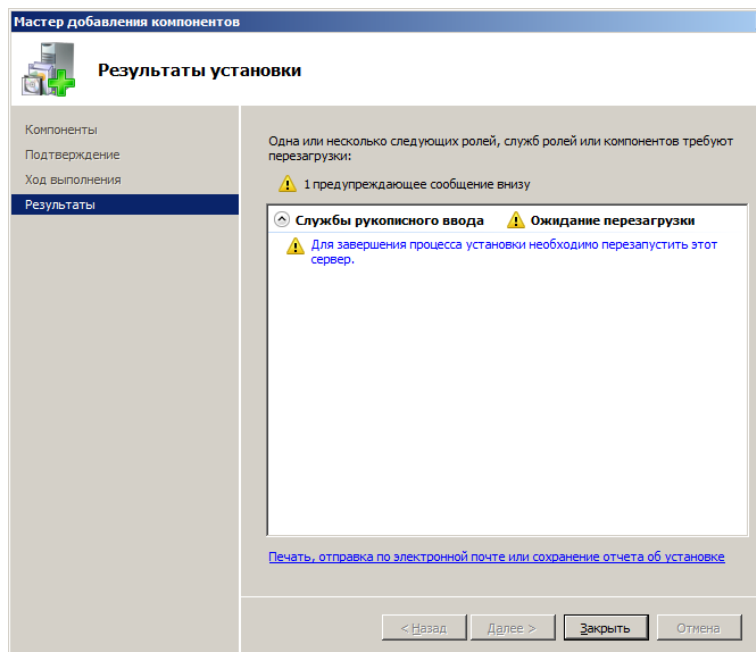
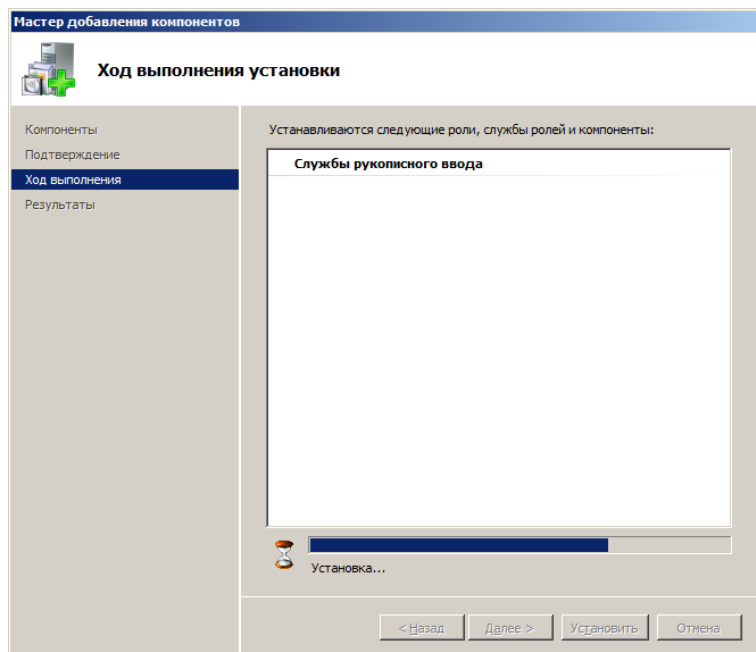


Рис.24 – 27 – Установка службы

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

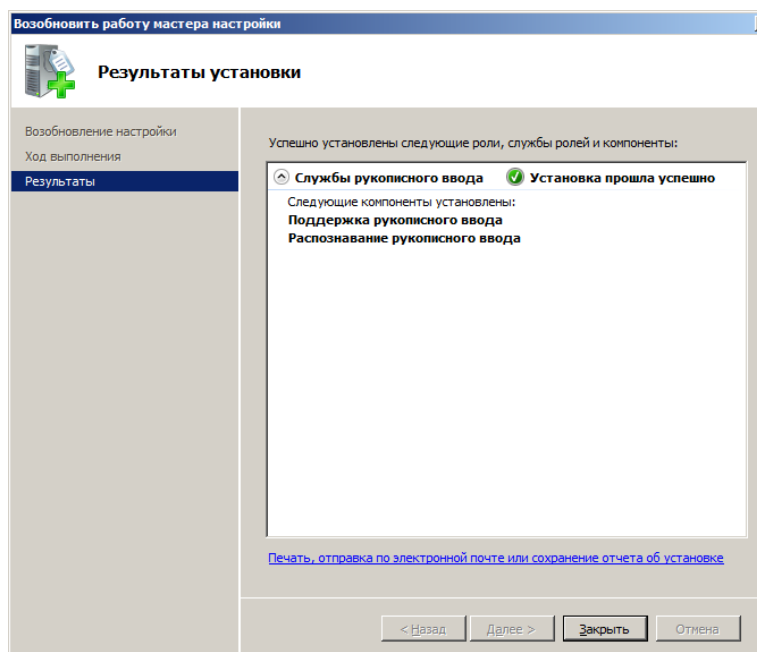


Рис.28 – Установка службы

7.2. Настройка серверных ОС Windows Server 2016

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

7.3. Работа с окнами сервиса КriptoПро CSP KC3

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

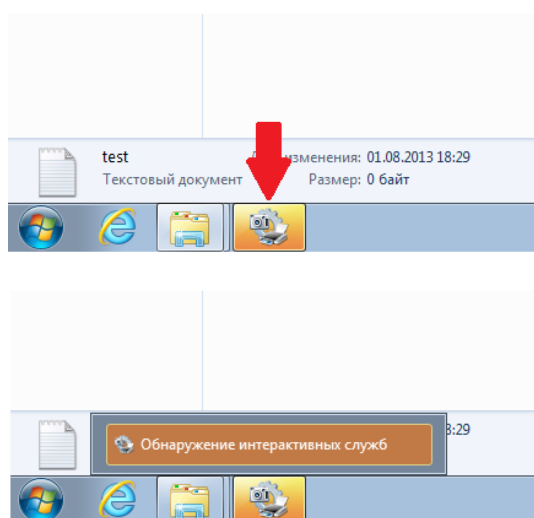


Рис. 29 - 30 – Сообщение сервиса CSP Кripto-Про

Возникновению 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).

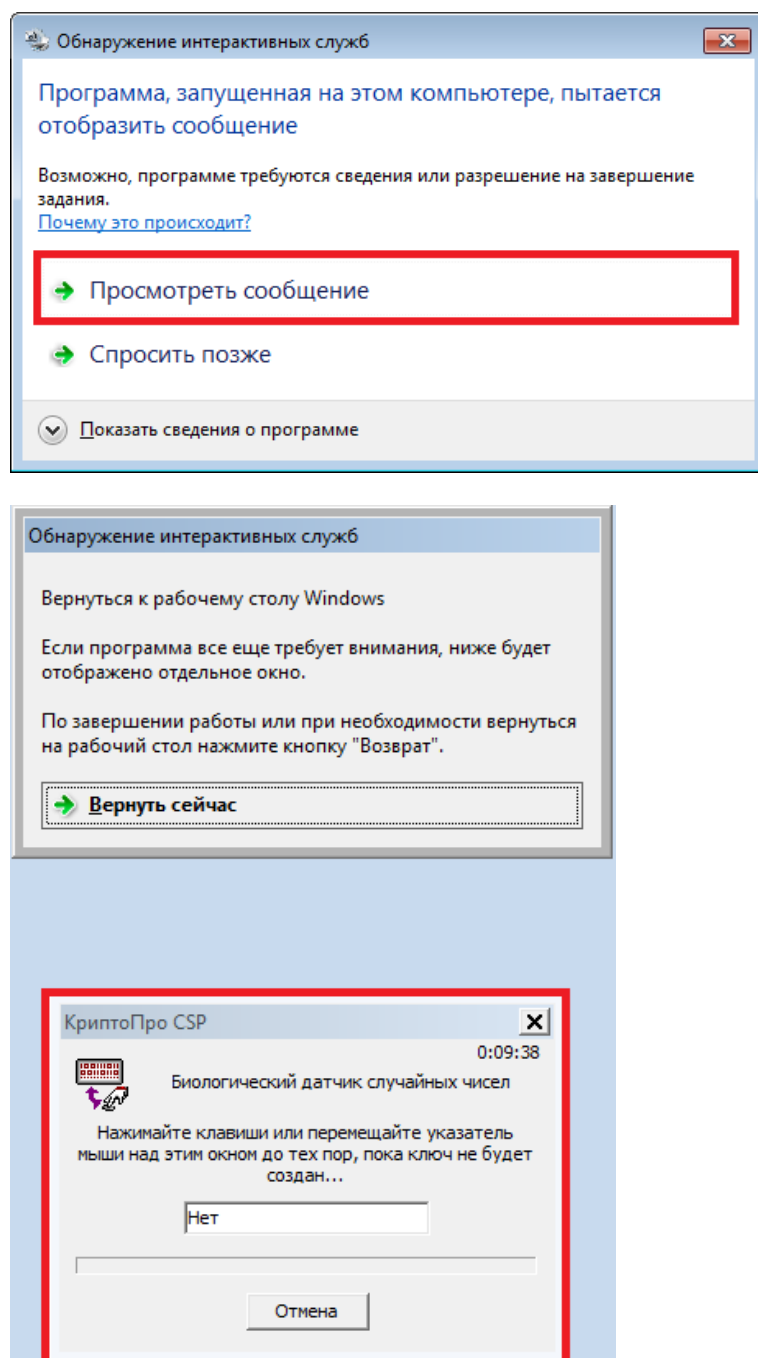


Рис. 31 - 32 – Окно взаимодействия с сервисом CSP Крипто-Про

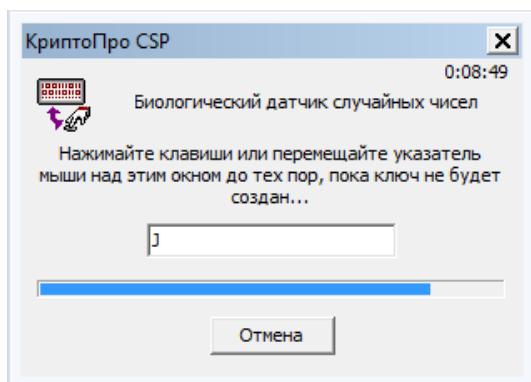


Рис. 33 – Выполнение действий в окне сервиса

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

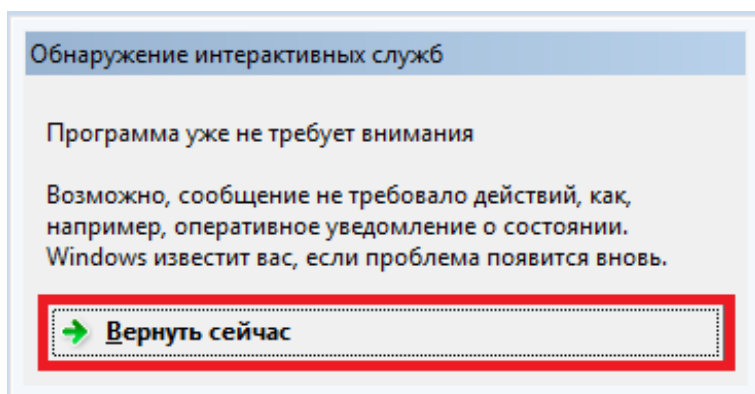


Рис.34 – Завершение взаимодействия с сервисом CSP Крипто-Про



Взаимодействие с сервисом CSP 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.

8. Использование дополнительных средств защиты загрузки

Использование программного СЗИ SPR 3.0 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 3.0 на этапе загрузки ОС. По умолчанию установка СЗИ SPR 3.0 производится по стандартному пути ФС «C:\Program Files». Необходимо убедиться в постановке пути установки СЗИ SPR 3.0 на контроль модуля АПМДЗ.

9. 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 "КРИПТО-ПРО". Руководство администратора безопасности. Установка. *Средство защиты информации «Secure Pack Rus» версия 3.0.* ЖТЯИ.00106-01 90 02.
2. —. Руководство администратора безопасности. Аутентификация. *Средство защиты информации «Secure Pack Rus» версия 3.0.* ЖТЯИ.00106-01 90 03.
3. —. Руководство администратора безопасности. Аудит. *Средство защиты информации «Secure Pack Rus» версия 3.0.* ЖТЯИ.00106-01 90 05.
4. —. Руководство администратора безопасности. Политики управления приложениями. *Средство защиты информации «Secure Pack Rus» версия 3.0.* ЖТЯИ.00106-01 90 04.
5. —. Формуляр. *Средство защиты информации «Secure Pack Rus» версия 3.0.* ЖТЯИ.00106-01 30 01.