Средство защиты информации

«SecurePackRus»

Версия 3.0

Руководство администратора безопасности

Аудит

EAPM.5090005.032-03 90 05

Листов 24

Компания «СиЭйЭн»

2016

Компания «СиЭйЭн», 2011-2016. Все права защищены.

Этот документ входит в комплект поставки изделия. На него распространяются все условия лицензионного соглашения. Без специального письменного разрешения компании «СиЭйЭн» 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 «СиЭйЭн».

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	Автоматизированнаяинформационная 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. События подсистемы защиты критических ресурсов

Имя источника: SPR-CriticalResourceProtection

ID	Уровень события	Текст
100	Информация	Запущен цикл расчета контрольных сумм защищаемых файлов.
101	Информация	Завершен цикл расчета контрольных сумм защищаемых файлов. Информация о цикле: Обработанные файлы:%1 Ошибки:%2
102	Информация	Запущен цикл проверки контрольных сумм защищаемых файлов.
103	Информация	Завершен цикл проверки контрольных сумм защищаемых файлов. Информация о цикле: Проверенные файлы:%1 Нарушение целостности:%2 Ошибки:%3
104	Информация	Выполнена попытка получения доступа к защищаемому объекту. Сведения об объекте: Тип:%1 Имя:%2 Сведения о процессе: Идентификатор:%3 Имя файла:%4 Сведения о запросе на доступ: Маска доступа:%5 Доступ:%6

2. События подсистемы управления доступа к устройствам

Имя источника: SPR-DeviceAccessControl

ID	Уровень события	Текст
200	Информация	Выполнена попытка активации контролируемого устройства. Сведения об устройстве: Класс:%1 Тип шины:%2 Описание:%3 Экземпляр:%4
201	Информация	Контролируемое устройство было удалено. Сведения об устройстве: Класс:%1 Описание:%2 Экземпляр:%3
202	Информация	Смонтирован том на контролируемом съемном носителе. Сведения о томе: Имя:%1 Метка:%2 Файловая система:%3 Экземпляр:%4
204	Информация	Выполнена попытка получения доступа к контролируемому устройству. Сведения об устройстве: Класс:%1 Описание%2 Экземпляр:%3 Сведения о процессе: Идентификатор:%4 Имя файла:%5 Сведения о запросе на доступ: Маска доступа:%6 Доступ:%7
205	Информация	Выполнена попытка получения доступа к объекту файловой системы на

	контролируемом съемном носителе. Сведения об объекте: Тип:%1 Имя:%2 Сведения о процессе: Идентификатор:%3 Имя файла:%4 Сведения о запросе на доступ: Маска доступа%5 Доступ:%6

3. События подсистемы контроля запуска сценариев

Имя источника: SPR-ScriptControl

№	Идентификатор	Тип	Источник	Описание
1	1	Предупреждение	SPR-ScriptsControl	Событие запуска сценария. Параметр: Хэш выполненного сценария.
2	2	Предупреждение	SPR-ScriptsControl	Событие блокировки сценария. Параметр: Хэшзаблокированного сценария.
3	3	Предупреждение	SPR-ScriptsControl	Событие разрешенного к запуску сценария. Параметр: Хэш разрешенного к запускусценария.

4. Настройка автоматизированного сбора событий журналов аудита

Для удобства администрирования программных продуктов SecurePackRUS и своевременного обнаружения фактов нарушения политик ИБ рекомендуется настроить автоматизированный сбор событий журналов аудита с рабочих станций в сети предприятия. Автоматизированный сбор событий аудита позволяет администратору группировать информацию обо всех инцидентах ИБ в сети на одной точке (АРМ администратора), что дает ему возможность анализировать процессы в зависимостях, а так же упрощает процесс управления собранным материалом (отчеты, резервное копирование).

Данная инструкция описывает способы настройки автоматизированного сбора событий журналов аудита для ОС семейства WindowsXP/2003 и Windows 7/2008, учитывая различия по доступному функционалу.

4.1. Ограничения на использование службы сбора ошибок

Служба сбора ошибок использует клиент-серверную модель взаимодействия: в сети предприятия располагается компьютер - сборщик ошибок (collector) и остальные рабочие станции – источники (source) отсылают ему сообщения в соответствии с описанными на сборщике правилами. На компьютере-сборщике можно создать несколько наборов правил-подписок (subscriptions), определив группы станций-источников, которые подчиняются этим правилам.

В Таблица **1** приведены возможные роли для различных версий ОС семействаWindows XP/Server2003 и Windows 7/Server2008 R2

Таблица 1 - Роли службы сборщика ошибок в различных версиях ОС

Тип ОС	Источник (source)	Сборщик (collector)
Windows Server 2003 SP1	✓	✗
Windows Server 2003 SP2	✓	✗
Windows Server 2003 R2	✓	✓
Windows Server 2008	✓	✓
Windows XP SP2	✓	✗
Windows Vista	✓	✗
Windows Vista SP1	✓	✓
Windows 7	✓	✓

4.2. Настройка службы сбора ошибок (eventcollector)

При настройке службы сбора ошибок (eventcollector) возможно использование двух схем, отличающихся по способу взаимодействия компьютера-сборщика (eventcollector) и компьютера-источника (eventsource): соединение инициировано компьютером-сборщиком либо исходным компьютером (источником). В данном документе рассмотрен первый вариант настройки службы сбора ошибок, т.к. он предпочтителен при работе в сети предприятия, позволяет автоматизировать процесс настройки используя групповые политики домена. Рассматриваемый ниже сценарий развертывания служб сбора ошибок предусматривает наличие контроллера домена, развернутой доменной сети, рабочей станции под управлением ОС Windows 7, введенной в домен, для использования ее в качестве компьютера – сборщика ошибок журналов аудита, а так же рабочих станций-источников ошибок журналов аудита так же являющихся членами домена, работающих под управлением ОС семейств Windows XP/Server 2003 и Windows 7/Server 2008 R2.

Возможен вариант настройки служб сбора ошибок для среды рабочей группы предприятия, а так же при использовании в качестве компьютера-сборщика рабочую станцию с ОС Windows Server 2003. Этот сценарий требует ручной настройки параметров аутентификации и создания, текстовых файлов-конфигурации для описания параметров конкретной подписки. За дополнительной информацией следует обращаться на сайт компании Microsoft.

4.2.1. Настройка службы сбора ошибок на компьютерах, работающих под управлением ОС Windows 7

Для настройки службы сбора ошибок необходимо выполнить следующие действия:

- На компьютере - сборщике (collector)выполнить активацию службы WinRM, выполнив команду **winrmqc –q.** Удостовериться что служба запущена (см. рис. 1).
- На компьютере - сборщике (collector)выполнить активацию службы подписки EventCollector, выполнив команду **wecutilqc**(см. рис. 1).

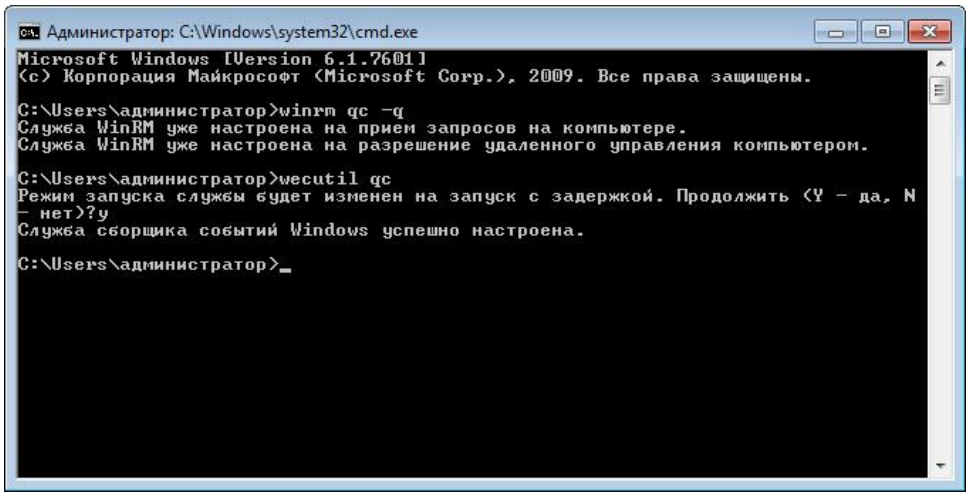

Рисунок 1 – Активация службы удаленного управления

- Настроить правила сбора ошибок из журналов аудита удаленных компьютеров: Пуск-> *Администрирование -> Просмотр событий -> Подписки* (см. рис. 2-3).

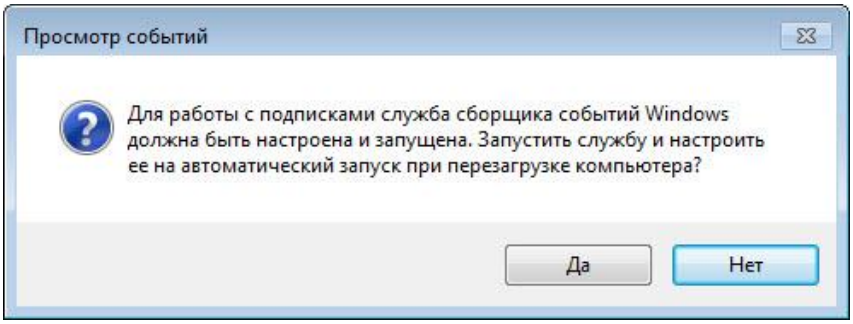

Рисунок 2 – Создание новой подписки

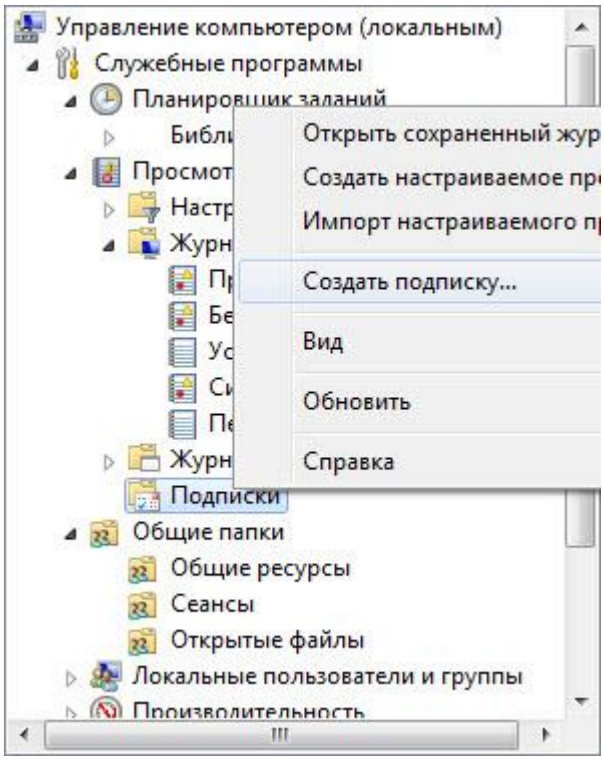

Рисунок 3 – Создание новой подписки

- Выбрать ***Создать подписку*** и задать требуемые параметры: имя, тип и собираемые в рамках подписки события, согласившись с запуском службы сбора пересылки (см. рис. 4)

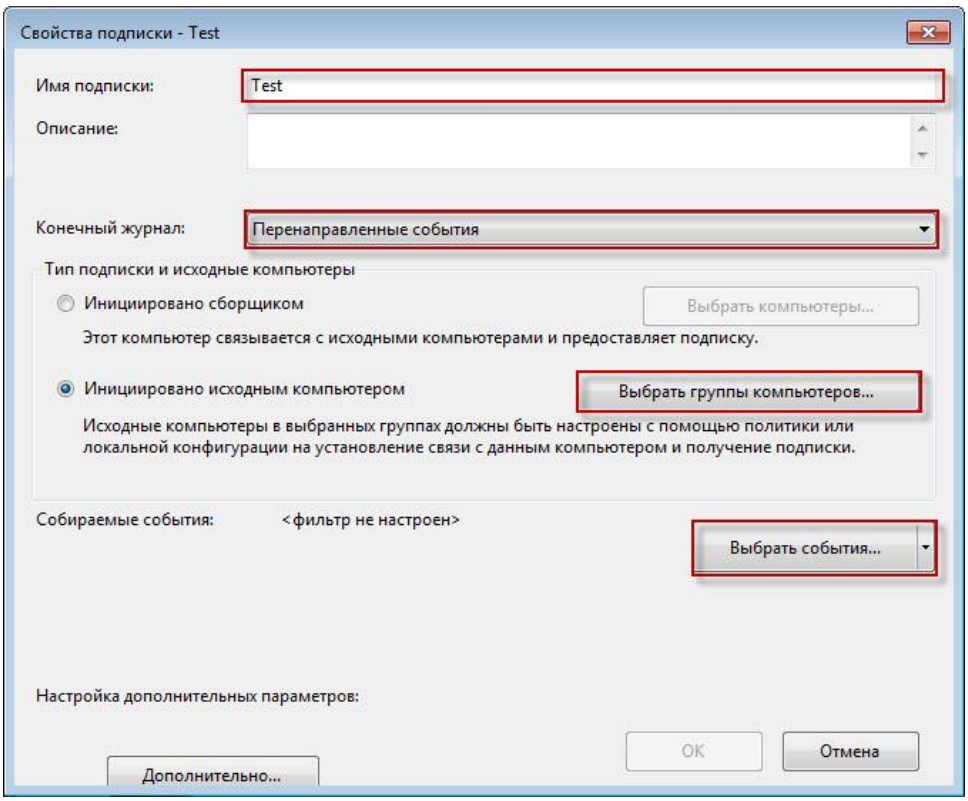

Рисунок 4 – Типы собираемых событий

- После указания параметров подписка появляется в списке с указанием текущего количества подключенных станций-источников (см. рис. 5).

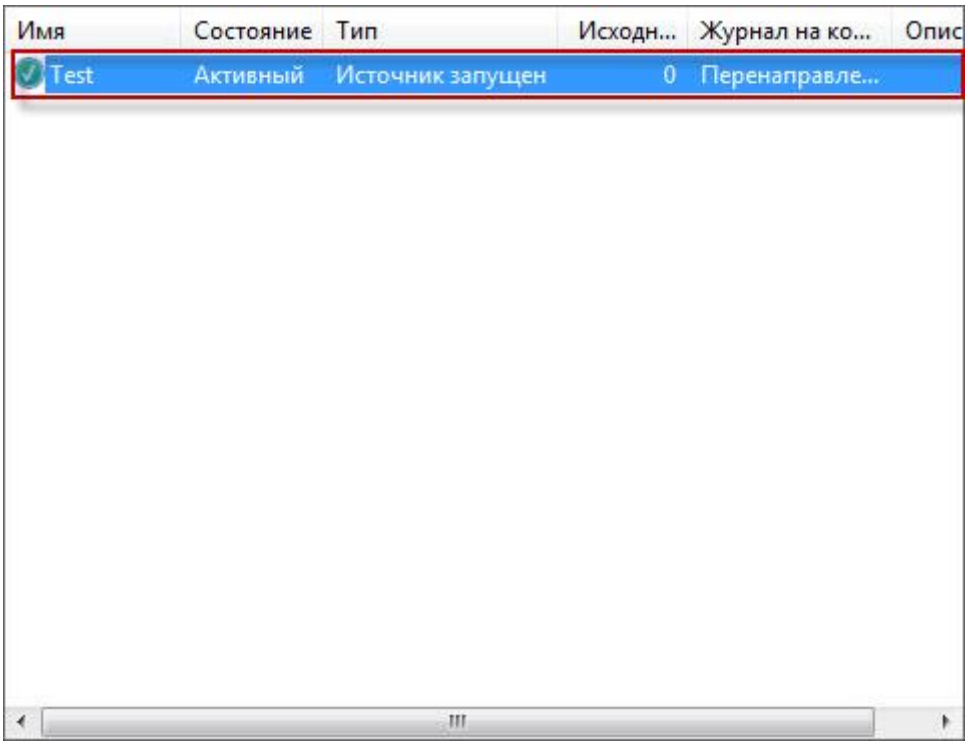

Рисунок 5 – Список текущих подписок

Для корректной работы службы сбора ошибок при создании подписки для компьютеров-источников под управлением ОС WindowsXP / Server 2003 необходимо отмечать пункт Изменить запрос вручную во вкладке *XML,* созданной подписки (см. рис 6).

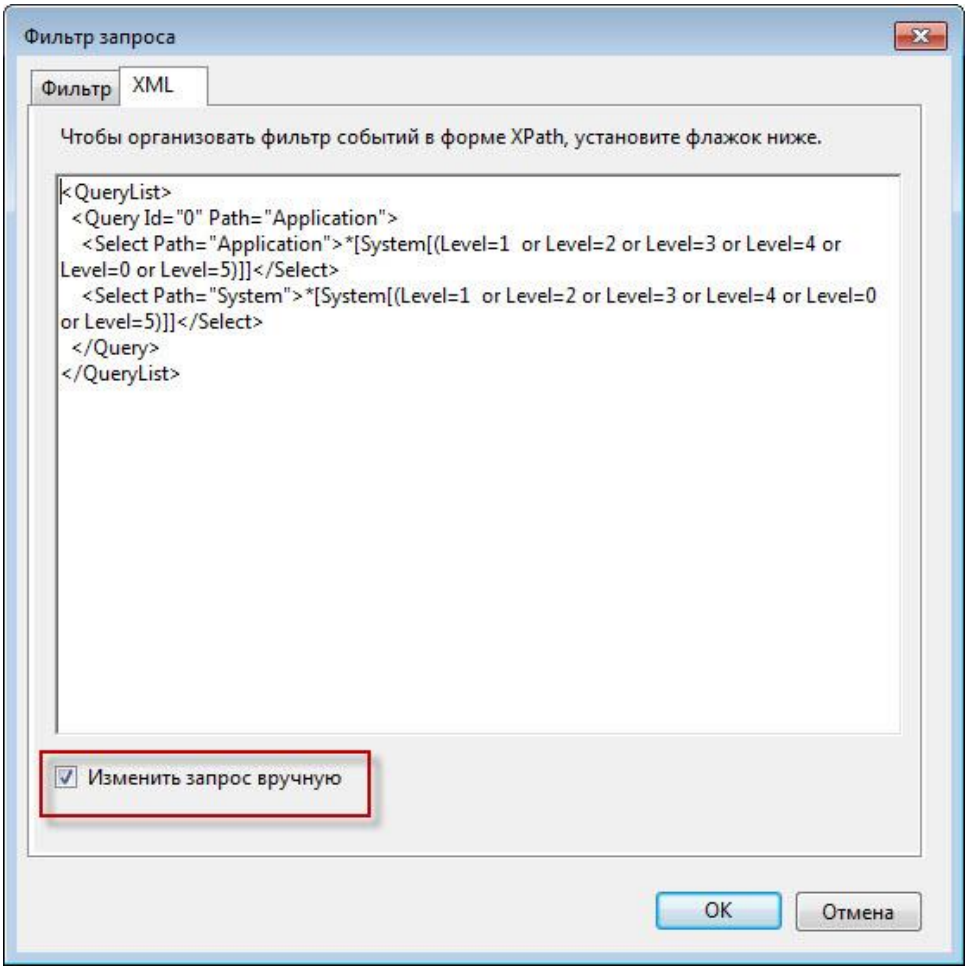

Рисунок 6 – Формирование текста запроса подписки вручную

При выборе типа событий журнала *Безопасность* при необходимости его передачи на компьютер-сборщик требуется дополнительная настройка на компьютере-источнике. Необходимые шаги по настройке компьютера-источника представлены в соответствующем разделе пункта 2.3. Более подробно об особенностях процедуры сбора ошибок журнала *Безопасность* можно узнать на сайте компании Microsoft: http://blogs.technet.com/b/otto/archive/2009/06/22/forwarding-security-events-from-windows-xp-server-2003-and-vista-server-2008.aspx

4.2.2.Настройка групповых политик для работы службы сбора ошибок

После создания новой подписки на компьютере-сборщике необходимо обозначить его как сервер-сборщик событий аудита в локальной сети домена:

- На контроллере домена **з**апустить редактор групповой политики, выполнив команду**gpedit.msc.** В ветке *Конфигурация компьютера -> Административные шаблоны -> Компоненты Windows ->Пересылка событий (см. рис. 7)* задать параметр *SubscriptionManagers,* указав в качестве параметра имя компьютера-сборщика (collector) в формате “*server=FQDN:5985” (см. рис. 8)*

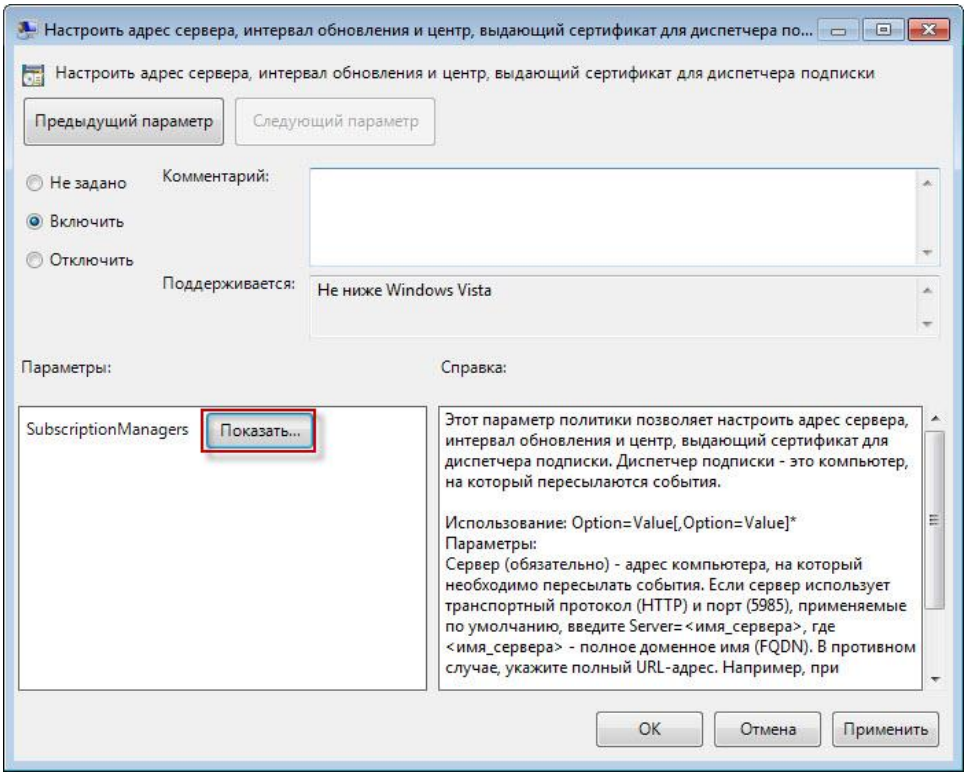

Рисунок 7 – Определение доменной политики

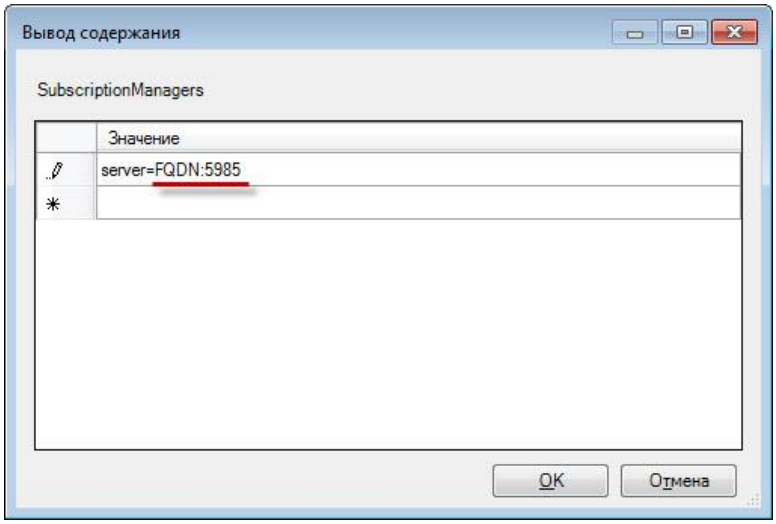

Рисунок 8 – Задание адреса компьютера-сборщика

Настройки сервера сборщика ошибок задаются для домена, таким образом, обеспечивая администратора удобной точкой распространения настроек в случае смены адреса компьютера сборщика.

Указание порта после FQDN-имени сервера сборщика необходимо для корректной работы службы сбора событий аудита с рабочих станций, работающих под ОС Windows XP / Server 2003. Это связано с различием в версиях протокола WinRM, используемых в этих ОС. Значение порта по умолчанию для службы WinRM в ОС Windows XP/Server 2003 установлено 80, хотя порт по умолчанию для сервера сборщика под управлением ОС Windows 7/Server 2008 R2 установлен 5985. Таким образом, без указания порта в настройках доменной политики, службы сбора ошибок с рабочих станций под управлением ОС Windows XP/Server 2003 работать не будут.

В случае использования контроллера домена под управлением ОС Windows Server 2003 возможно отсутствие раздела Пересылка событий. В данной ситуации необходимо воспользоваться средством удаленного управления сервером для управления доменной политикой с рабочей станции-сборщика под управлением ОС Windows 7. Более подробно про Средства удаленного администрирования (RSAT) можно прочитать на сайте компании Microsoft:http://www.microsoft.com/download/en/details.aspx?id=7887

4.3. Настройка службы отправки ошибок (eventsource)

4.3.1. Настройка службы отправки ошибок на компьютерах, работающих под управлением ОС Windows XP/Server2003

Для настройки службы автоматизированного сбора ошибок в ОС семейства Windows XP / Server 2003 необходимо предварительно установить компоненты WS-Management v1.1 (не входит в комплект поставки ОС). Скачать эти компоненты можно с сайта компании Microsoft: http://www.microsoft.com/downloads/en/details.aspx?FamilyID=845289ca-16cc-4c73-8934-dd46b5ed1d33&displaylang=en.

После установки компонент RemoteManagement необходима их настройка:

- На компьютере - источнике (source) выполнить активацию службы WinRM, выполнив команду **winrmqc –q.** Удостовериться что служба запущена (см. рис. 8).
- На компьютере - источнике (source) выполнить активацию службы подписки EventCollector, выполнив команду **wecutilqc** (см. рис. 9).

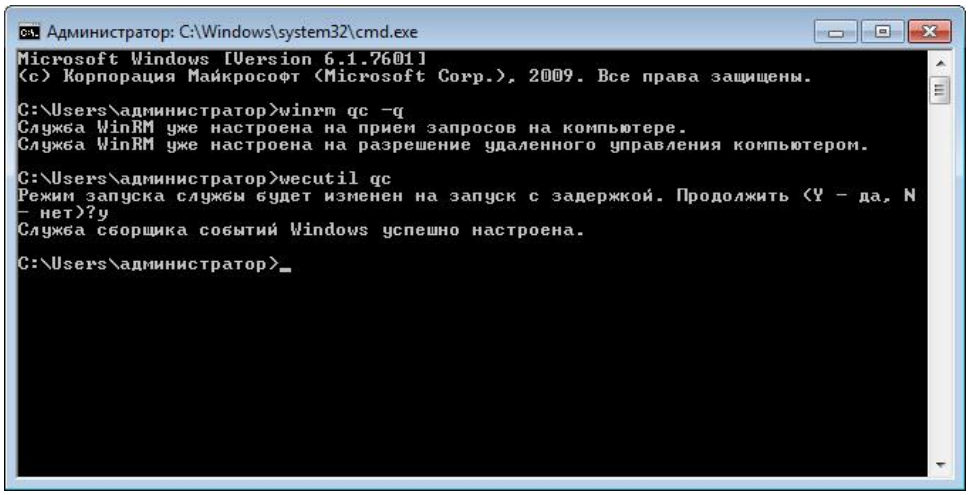

Рисунок 9 – Активация службы удаленного управления

После выполнения описанных действий в списке журналов на компьютере-источнике появиться журнал **Microsoft-Windows-Forwarding** (Рисунок 10), в котором будут фиксироваться события работы службы подписки, а в журнале на компьютере-сборщике (collector) будут фиксироваться события, определенные в файле конфигурации.

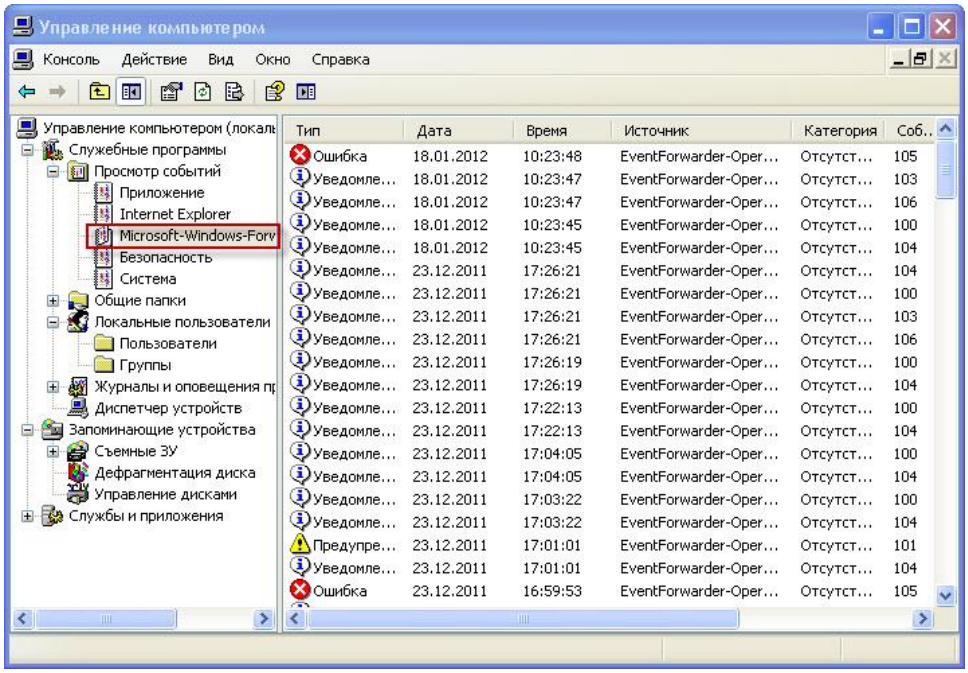

Рисунок 10 – Журнал Microsoft-Windows-Forwarding

Для корректной работы службы сбора ошибок при создании подписки для компьютеров-источников под управлением ОС Windows XP/Server 2003 необходимо отмечать пункт Изменить запрос вручную во вкладке *XML*созданной подписки (см. п. 2.2.1).

4.3.2. Настройка сбора ошибок журнала безопасность на компьютерах, работающих под управлением ОС Windows XP/Server 2003

Настройки по умолчанию не позволяют настроить сбор ошибок из журнала **Безопасность**. Это обусловлено более высокими требованиями безопасности и соответственно более высоким уровнем доступа, требуемым для чтения содержимого файла журнала.

Что бы получить возможность пересылать события из журнала **Безопасность** на рабочих станциях под управлением ОС Windows XP следует изменить порядок запуска службы **WindowsRemoteManagement** (рис. 11) от имени Локального администратора. Для этого необходимо выполнить:

1. *Пуск -> Администрирование -> Службы*
2. Служба **Windows Remote Services** -> *Свойства*
3. В свойства *Запуск от имени* указать **Локальный администратор.**

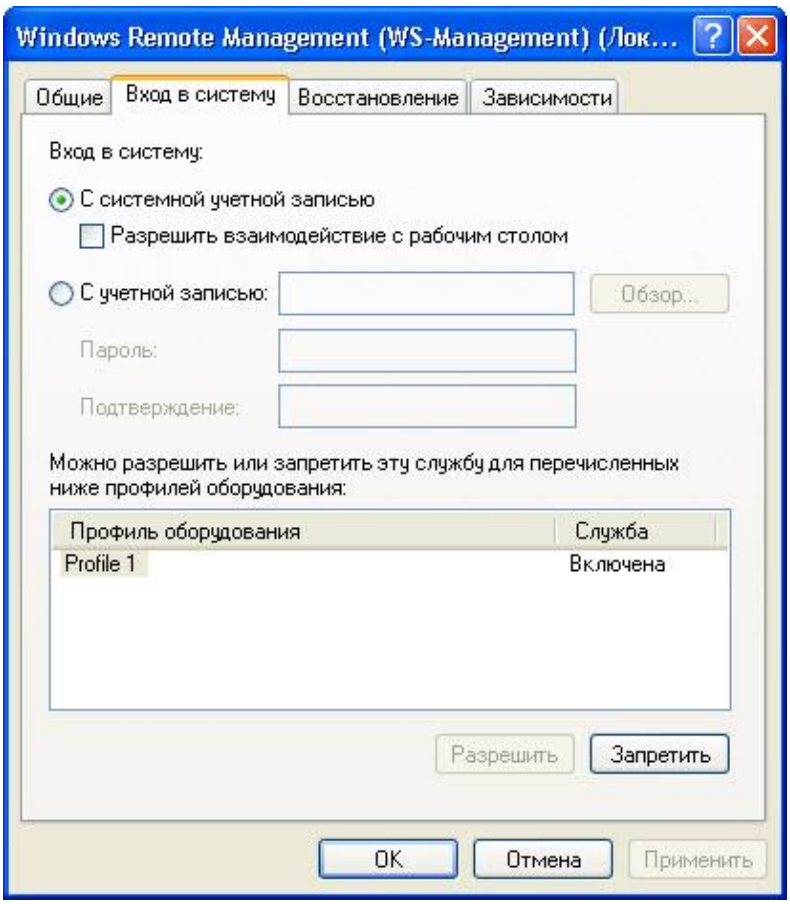

Рисунок 11 – Настройка запуска службы

Данная настройка является потенциально небезопасной. Следует особенно внимательно относиться к описанной выше возможности, т.к. она влечет существенные риски информационной безопасности.

Что бы получить возможность пересылать события из журнала **Безопасность** на серверах под управлением ОС Windows Server 2003 необходимо добавить ключ реестра *CustomerSD*со значением *”O:BAG:SYD:(A;;CC;;;NS)”*по адресу **HKLM/SYSTEM/CurrentControlSet/Services/EventLog/Security,** выполнив команду *regedit (рис. 12)*.

Имя	Тип	Значение
(По умолчанию)	REG_SZ	(значение не присвоено)
AutoBackupLogFiles	REG_DWORD	0x00000000 (0)
CustomSD	REG_SZ	O:BAG:SYD:(D;;0xf0007;;;AN)(D;;0xf0007;;;BG)(A;;0...
DisplayNameFile	REG_EXPAND_SZ	%SystemRoot%\System32\els.dll
DisplayNameID	REG_DWORD	0x00000101 (257)
File	REG_EXPAND_SZ	%SystemRoot%\System32\config\SecEvent.Evt
MaxSize	REG_DWORD	0x08000000 (134217728)
PrimaryModule	REG_SZ	Security
RestrictGuestAcc...	REG_DWORD	0x00000001 (1)
Retention	REG_DWORD	0x00000000 (0)

Рисунок 12 – Создание записи реестра

4.3.3. Настройка службы отправки ошибок на компьютерах, работающих под управлением ОС Windows 7/Server 2008 R2

Для настройки службы отправки ошибок необходимо выполнить следующие действия:

- На компьютере - источнике (source) выполнить активацию службы WinRM, выполнив команду **winrmqc –q.** Удостовериться что служба запущена (см. рис. 13).
- На компьютере - источнике (source) выполнить активацию службы подписки EventCollector, выполнив команду **wecutilqc**(рис. 13).

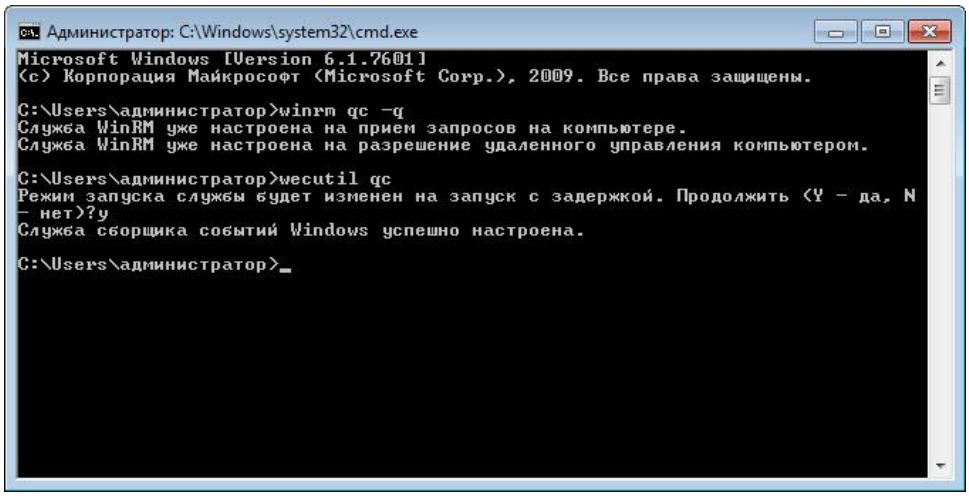

Рисунок 13 – Активация службы удаленного управления

После выполнения описанных действий в списке журналов на компьютере-источнике появиться журнал **Microsoft-Windows-Forwarding**в котором будут фиксироваться события работы службы подписки, а в журнале на компьютере-сборщике (collector) будут фиксироваться события, определенные в файле конфигурации.

4.3.4. Настройка сбора ошибок журнала безопасность на компьютерах, работающих под управлением ОС Windows 7/Server 2008 R2

Настройки по умолчанию не позволяют настроить сбор ошибок из журнала **Безопасность**. Это обусловлено более высокими требованиями безопасности и соответственно более высоким уровнем доступа, требуемым для чтения содержимого файла журнала.

Что бы получить возможность пересылать события из журнала **Безопасность** на рабочих станциях под управлением ОС Windows 7/Server 2008 R2 необходимо:

1. Открыть консоль **Управление компьютером**
2. В разделе пользователи и группы выбрать Группы -> Чтение журналов аудита -> Свойства
3. Добавить субъект доступа “Сетевой сервис” в группу доступа (рис. 14)

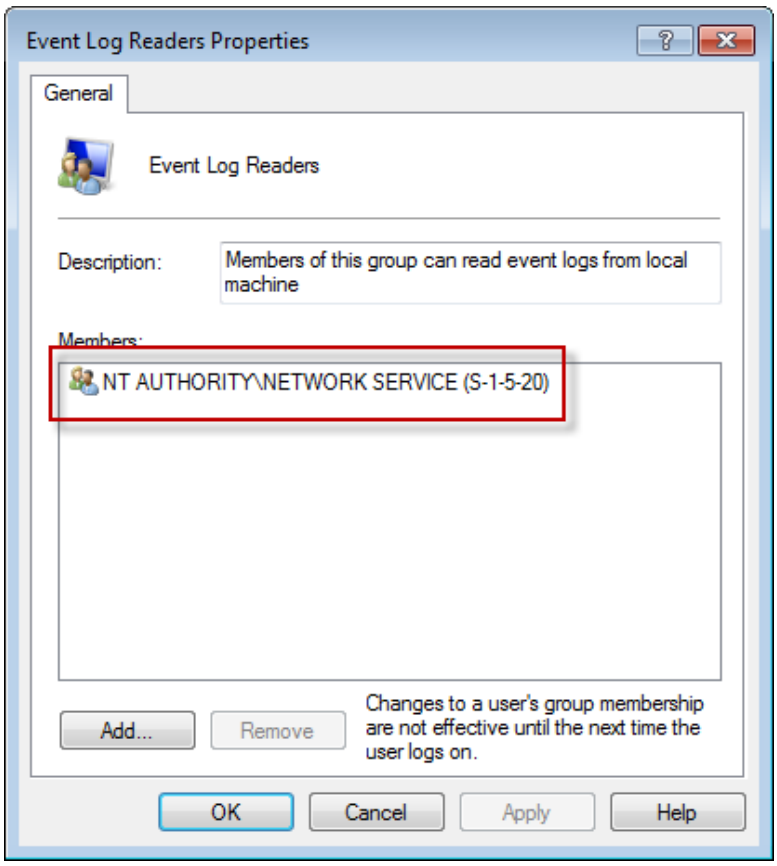

Рисунок 14 – Настройка группы безопасности доступа к журналам аудита.

2.4 Проверка работы службы сбора ошибок

Для контроля за работой службы сбора событий аудита на конечных рабочих местах администратору следует обратиться к событиям журнала Microsoft-Windows-Forwarding.

При отсутствии на компьютере-сборщике данных о событиях с компьютера источника, работающего под управлением ОС Windows XP / Server 2003, следует проверить настройку Ручного управления запросом в разделе XML в свойстве подписки.

При появлении ошибок, связанных с правами доступа, при попытке получить доступ к журналу **Безопасность,** необходимо проверить выполнение требований, описанных в п.п. 2.3.2, 2.3.4.

В случае ошибок связи с компьютером-сборщиком необходимо проверить настройки Подписки (см. п. 2.2.1) и параметры, определяющие способ взаимодействия с ним (см. п. 2.2.2).

После смены настроек следует выполнять команду *gpupdate /force* для получения новых значений политики с контроллера домена.

В случае штатной работы службы сбора событий аудита возникают следующие записи (рис. 15-18) в журнале Microsoft-Windows-Forwarding:

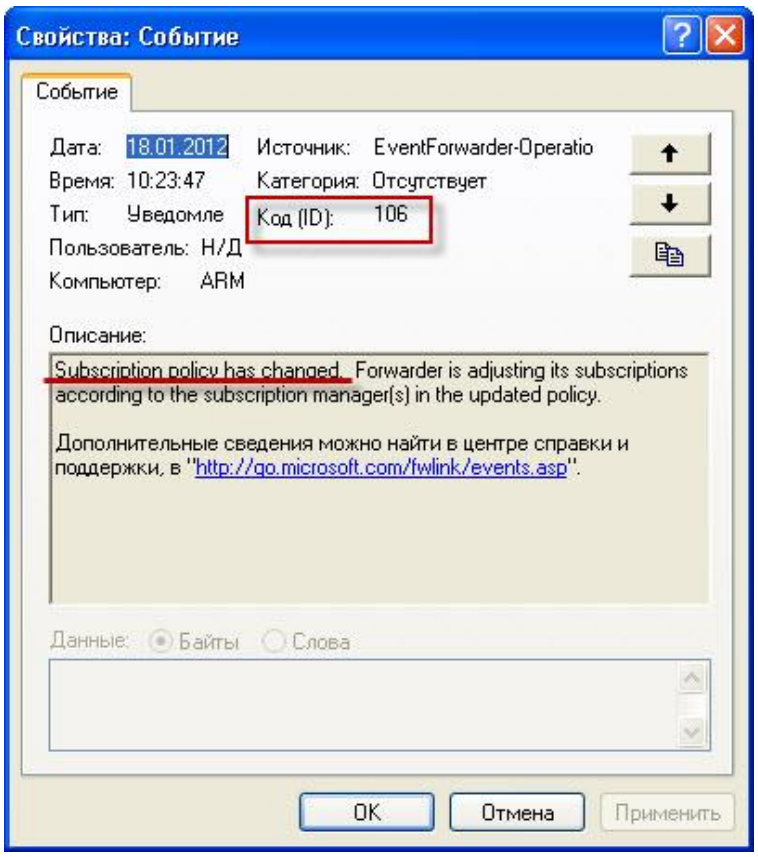

Рисунок 15 – Политика успешно обновлена (код 106)

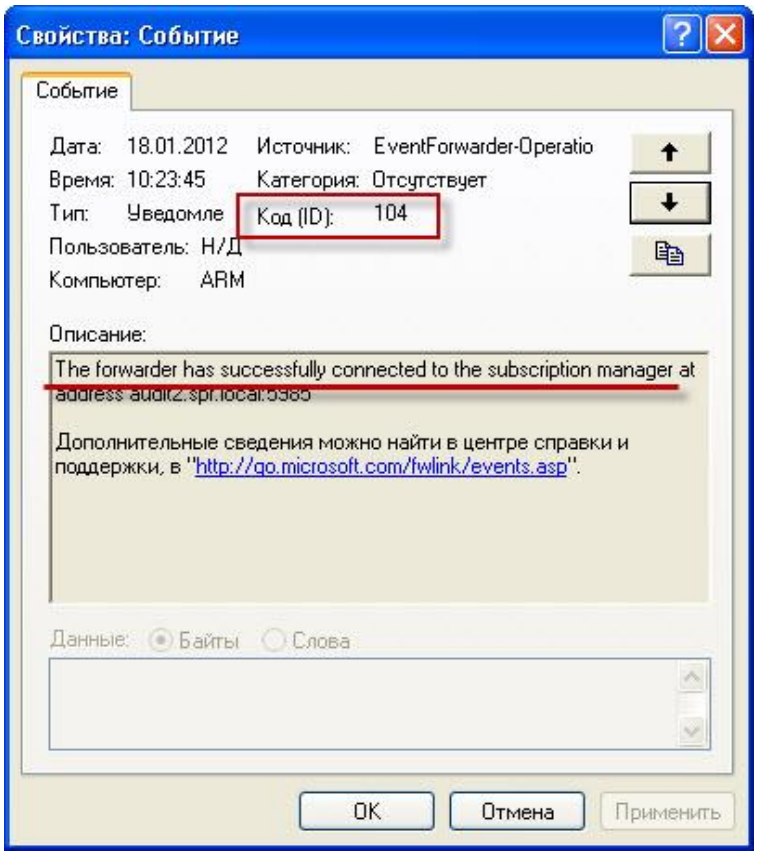

Рисунок 16 – Соединение с компьютером-сборщиком успешно установлено (код 104)

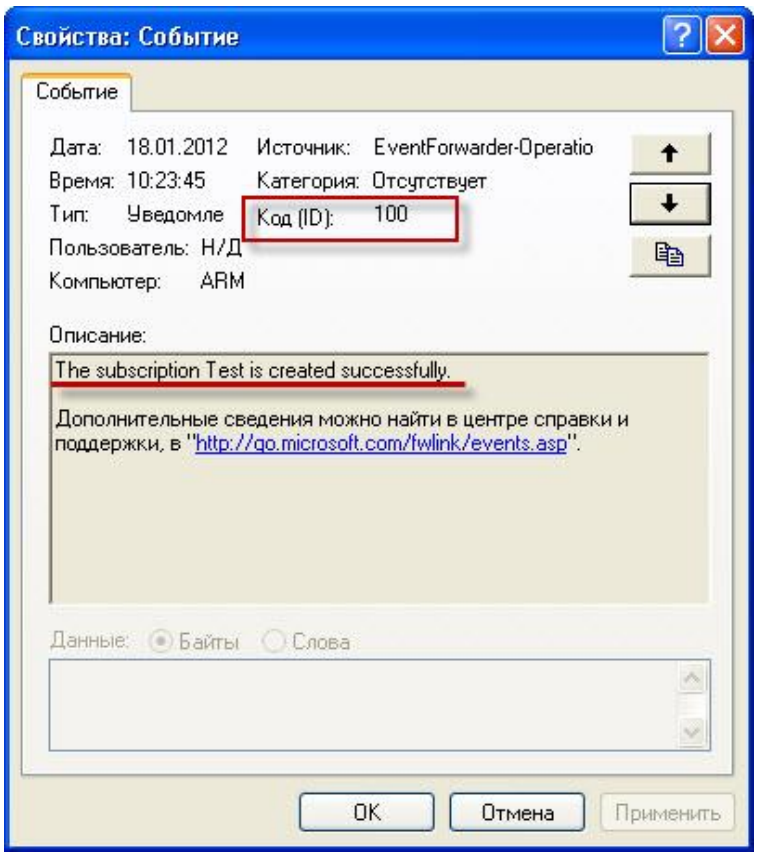

Рисунок 17 – Подписка успешно применена (код 100)

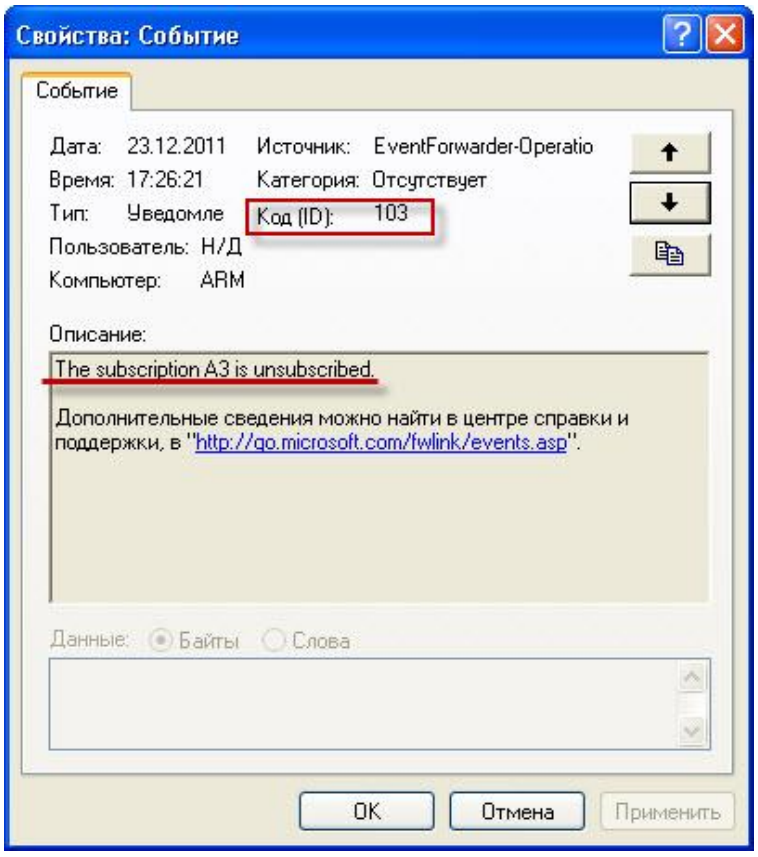

Рисунок 18 – Подписка успешно отключена (код103)

5. Приложение 1

XML-файл для формирования запроса к журналу аудита и автоматизации сбора ошибок (следует использовать на этапе настойки политики подписки на компьютере-сборщике п.п. 4.2.1).

Данная конфигурация подписки позволяет собирать события следующих политик:

- ✓ Secure Pack (в .т.ч.
  - SPR-CriticalResourceProtection
  - SPR-DeviceAccessControl
  - SPR-ScriptControl
- ✓ Software RestrictionPolicy
  - Windows-Software-Restriction-Policy
- ✓ CryproPro(вт.ч. CryptoPro EFS)

<QueryList>

<Query Id="0" Path="Secure Pack Rus">

<Select Path="Secure Pack Rus">[System[(Level=1 or Level=2 or Level=3 or Level=4 or Level=0 or Level=5)]]</Select>*

</Query>

<Query Id="1" Path="Application">

<Select Path="Application">[System[Provider[@Name='Microsoft-Windows-SoftwareRestrictionPolicies'] and (Level=1 or Level=2 or Level=3 or Level=4 or Level=0 or Level=5)]]</Select>*

</Query>

<Query Id="2" Path="Application">

<Select Path="Application">[System[Provider[@Name='Software Restriction Policies'] and (Level=1 or Level=2 or Level=3 or Level=4 or Level=0 or Level=5)]]</Select>*

</Query>

<Query Id="3" Path="Application">

<Select Path="Application">[System[Provider[@Name='cpcsp'] and (Level=1 or Level=2 or Level=3 or Level=4 or Level=0 or Level=5)]]</Select>*

</Query>

</QueryList>

Список литературы

1. **Компания "СиЭйЭн".** Описание применения. *Средство защиты информации «Secure Pack Rus» версия 3.0.* ЕАРМ.5090005.032-03 31 01.

2. —. Формуляр. *Средство защиты информации «Secure Pack Rus» версия 3.0.* ЕАРМ.5090005.032-03 30 01.