NTechnology | SIEM

Руководство по настройке источников

НЦОТ

Содержание

1. Общая информация о системе ... 3

1.1 О документе ... 3

1.2 О NT SIEM ... 3

1.3 Краткое описание возможностей системы ... 3

2. Microsoft Windows Vista—11; Windows Server 2008—2022: настройка источника ... 5

2.1 Настройка дескриптора безопасности журнала ... 8

2.2 Настройка включения командной строки в события создания процессов с помощью групповой политики ... 8

2.3 Настройка расширенной политики аудита с помощью групповой политики ... 9

2.4 Настройка политики аудита утилитой auditpol ... 11

3. Microsoft Windows XP: настройка источника ... 13

3.1 Настройка локальных политик аудита событий ... 14

3.2 Отключение гостевой учетной записи ... 15

3.3 Создание учетной записи ОС ... 15

3.4 Настройка локальной групповой политики для учетной записи ... 17

3.5 Настройка разрешений на имя в пространстве имен WMI ... 17

3.6 Настройка разрешений на COM-приложения ... 19

4. Microsoft Windows Server 2003, 2003 R2: настройка источника ... 23

4.1 Настройка локальной политики безопасности для группы Distributed COM Users ... 26

4.2 Настройка разрешений на COM-приложения для группы COM-пользователей ... 28

4.3 Настройка разрешений на имя в пространстве имен WMI ... 31

4.4 Получение идентификатора безопасности (SID) учетной записи ... 33

4.5 Настройка доступа к журналу ... 34

4.6 Отключение контроля учетных записей (UAC) ... 35

1. Общая информация о системе

1.1 О документе

Этот документ содержит информацию для планирования и выполнения развертывания компьютерной программы, предназначенной для сбора и анализа событий информационной безопасности (Security Information and Event Management system) «NTechnology SIEM» (далее – NT SIEM), а также о работе со службами сбора событий с машин Windows.

Комплект документации NT SIEM включает в себя следующие документы:

- Этот документ;
- Руководство по созданию запросов – содержит описание наборов запросов и результаты применения этих запросов;
- Руководство пользователя – содержит справочную информацию и инструкции по настройке и администрированию продукта. Содержит сценарии использования продукта для управления информационными активами организации и событиями информационной безопасности;
- Руководство по написанию правил – содержит рекомендации по созданию правил нормализации, агрегации, корреляции и обогащения событий.
- Руководство по установке – содержит информацию для внедрения продукта в инфраструктуре организации: инструкции по установке, первоначальной настройке и удалению продукта.

1.2 О NT SIEM

NT SIEM – это система, которая осуществляет сбор, хранение и анализ событий, исходящих от сетевых устройств, средств защиты информации, баз данных, ключевых корпоративных ресурсов, инфраструктуры систем и приложений.

1.3 Краткое описание возможностей системы

Система NT SIEM предоставляет следующие основные функциональные возможности:

- Сбор журналов событий с различных источников;
- Визуализация данных в виде графиков, диаграмм в форме дашбордов;
- Анализ журналов событий в соответствии с правилами нормализации, корреляции, агрегации и обогащения;
- Формирование инцидентов на основе процессов агрегации, обогащения и корреляции;
- Управление инцидентами информационной безопасности;

- Хранение событий и инцидентов информационной безопасности;
- Фильтрация по различным параметрам событий и инцидентов, в том числе с использованием избранных запросов для быстрого доступа к фильтрам по событиям;
- Использование готовой базы правил, а также возможность создания собственных правил и табличных списков;
- Мониторинг состояния системы;
- Отправка уведомлений пользователям в рамках веб-приложения и по электронной почте;
- Формирование и выгрузка отчетов за определенный период времени;
- Осуществление интеграций, в том числе и с SOAR-системами;
- Мониторинг активов.

2. Microsoft Windows Vista—11; Windows Server 2008—2022: настройка источника

Настройку источника нужно выполнять от имени учетной записи, имеющей права локального администратора Windows.

При использовании в IT-инфраструктуре организации межсетевого экрана или других средств для контроля сетевого трафика требуется настроить в них правила, разрешающие трафик в обоих направлениях между узлом источника и узлом NT Collector. Используются стандартный TCP-порт 135 и динамические TCP-порты 49152—65535.

При использовании на узле источника межсетевого экрана Windows в нем нужно включить правила для входящих подключений «Удаленное управление журналом событий (именованные каналы — входящий)» (Remote Event Log Management (NP-In)), «Удаленное управление журналом событий (RPC)» (Remote Event Log Management (RPC)), «Удаленное управление журналом событий (RPC-EPMAP)» (Remote Event Log Management (RPC-EPMAP)).

Чтобы **включить правило межсетевого экрана Windows** необходимо:

a) Открыть панель управления Windows.
b) Запустить брандмауэр Windows.
c) В левой части окна выбрать узел Монитор брандмауэра Защитника Windows в режиме повышенной безопасности → <Категория правила>.
d) Выбрать правило.
e) В главном меню выбрать Действия → Включить правило.

События сохраняются в журнале событий Windows.

Для доступа NT Collector на источник следует создать и настроить доменную учетную запись.

Для сбора событий из журналов Windows на рабочих станциях нужно на контроллере домена:

a) Создать доменную группу учетных записей для сбора событий.
b) Создать доменную учетную запись для доступа NT Collector на рабочие станции.
c) Добавить учетную запись в доменную группу.
d) Создать групповую политику учетных записей для сбора событий.
e) Настроить групповую политику для группы Event Log Readers.
f) Настроить групповую политику для удаленного доступа.

Следует отметить, что можно не настраивать групповую политику для удаленного доступа, если на контроллере домена и на всех рабочих станциях, к которым применяется групповая политика, в группу Users добавлен пользователь

Authenticated Users и в политику безопасности «Доступ к компьютеру из сети» добавлена группа Users или Everyone.

g) Если нужно, настроить групповую политику для раздела реестра `HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\WINEVT`.

   Можно не настраивать групповую политику для раздела реестра, если на контроллере домена и на всех рабочих станциях, к которым применяется групповая политика, в группу Users добавлен пользователь Authenticated Users.

h) Назначить групповую политику рабочим станциям, с которых нужно собирать события.

Чтобы **создать доменную группу пользователей** необходимо:

a) Открыть панель управления Windows.
b) Выбрать Администрирование → Пользователи и компьютеры Active Directory.
c) Запустить оснастка «Active Directory — пользователи и компьютеры».

Также можно запустить оснастку «Active Directory — пользователи и компьютеры» выполнив команду dsa.msc.

d) В левой части окна выберите объект Пользователи и компьютеры Active Directory → <Имя домена> → Users.
e) В главном меню выбрать Действие → Создать → Группа. Откроется окно Новый объект — Группа.
f) В поле Имя группы ввести название группы.
g) Нажать кнопку ОК.

В результате доменная группа пользователей будет создана.

Для сбора событий из журнала Windows на источнике нужно:

1. Средствами ОС создать учетную запись локального пользователя ОС для доступа NT Collector.

Чтобы **создать учетную запись пользователя ОС** необходимо:

a) Открыть панель управления Windows.
b) Выбрать Администрирование → Управление компьютером.
c) В левой части окна выбрать узел Управление компьютером → Локальные пользователи и группы → Пользователи.
d) В главном меню выбрать Действие → Новый пользователь.
e) В поле Пользователь ввести логин учетной записи.
f) Установить флажок Запретить смену пароля пользователем.
g) Установить флажок Срок действия пароля не ограничен.
h) Ввести пароль и подтвердить его.
i) Нажать Создать.

Данные этой учетной записи нужно указать при добавлении учетной записи в NT SIEM.

2. Добавить учетную запись в локальную (групповую) политику безопасности «Доступ к компьютеру из сети» (Access this computer from the network).

Чтобы **добавить учетную запись в локальную политику безопасности** необходимо:

a) Открыть панель управления Windows.
b) Выбрать Администрирование → Локальная политика безопасности.
c) В левой части окна выбрать узел Параметры безопасности → Локальные политики → Назначение прав пользователя.
d) Выбрать политику, к которой нужно добавить учетную запись.
e) В главном меню выбрать Действие → Свойства.
f) В открывшемся окне нажать кнопку Добавить пользователя или группу.
g) В открывшемся окне нажать кнопку Размещение.
h) В открывшемся окне выбрать:

если используется локальная учетная запись — имя узла;
если используется доменная учетная запись — имя домена.

i) Нажать кнопку ОК.
j) В поле Введите имена выбираемых объектов ввести логин учетной записи и нажать ОК.
k) В окне Свойства <Имя политики> нажать ОК.

3. Добавить учетную запись в локальную группу пользователей Event Log Readers или изменить дескрипторы безопасности журналов ОС для доступа учетной записи.

Чтобы **добавить учетную запись в локальную группу пользователей** необходимо:

a) Открыть панель управления Windows.
b) Выбрать Администрирование → Управление компьютером.
c) В левой части окна выбрать узел Локальные пользователи и группы → Группы.
d) Выбрать группу, в которую нужно добавить учетную запись.
e) В главном меню выбрать Действие → Добавить в группу.
f) Нажать Добавить.
g) Нажать Размещение.
h) В открывшемся окне выбрать:
   если используется локальная учетная запись — имя узла;
   если используется доменная учетная запись — имя домена.
i) Нажать ОК.
j) В поле Введите имена выбираемых объектов ввести логин учетной записи и нажать ОК
k) В окне Свойства <Имя группы> нажать ОК

4. Настроить включение командной строки Windows в события создания процессов.

5. Настроить групповую политику расширенной политики аудита с помощью утилиты auditpol или из консоли управления групповыми политиками.

Консоль управления групповыми политиками (Group Policy Management Console) по умолчанию устанавливается на серверных ОС вместе с ролью Active Directory Domain Services, для клиентских ОС нужно дополнительно установить средства удаленного администрирования сервера (Remote Server Administration Tools).

2.1 Настройка дескриптора безопасности журнала

Права доступа к журналу указаны в его дескрипторе безопасности в формате языка определения дескрипторов безопасности (SDDL). Для получения дескриптора журнала используется утилита wevtutil. Утилита расположена в папке `C:\Windows\System32`.

Чтобы настроить дескриптор безопасности журнала необходимо:

1. Нажать Пуск → Выполнить.
2. В поле Открыть ввести cmd и нажать ОК. Откроется интерфейс командной строки.
3. Получить идентификатор безопасности (SID) учетной записи NT Collector:
   `wmic useraccount where name='<Имя учетной записи>' get sid`
4. Получить дескриптор журнала:
   `wevtutil gl <Имя журнала>`
5. Обновите дескриптор безопасности, добавив в конец строки элемент управления доступом (ACE) для учетной записи NT Collector с разрешением на чтение журнала (A — Access; 0x1 — Read):
   `wevtutil sl <Имя журнала> /ca:<Дескриптор безопасности журнала>(A;;0x1;;;<SID учетной записи>)`

В результате В реестре Windows для журнала создан строковый параметр CustomSD, в него занесен настроенный дескриптор безопасности.

2.2 Настройка включения командной строки в события создания процессов с помощью групповой политики

Чтобы настроить включение командной строки Windows в события создания процессов с помощью групповой политики необходимо:

1. Открыть панель управления Windows.

2. Выбрать Администрирование → Управление групповой политикой. Также есть возможность запустить консоль управления групповыми политиками, выполнив команду gpmc.msc.
3. Выбрать узел используемой политики Управление групповой политикой → Лес: <Имя леса> → Домены → <Имя домена> → <Имя групповой политики серверов или рабочих станций>.
4. В главном меню выбрать Действие → Изменить.
5. В левой части окна выбрать узел Политика <Имя политики> → Конфигурация компьютера → Политики → Административные шаблоны → Система → Аудит создания процессов.
6. Выбрать Включать командную строку в события создания процессов.

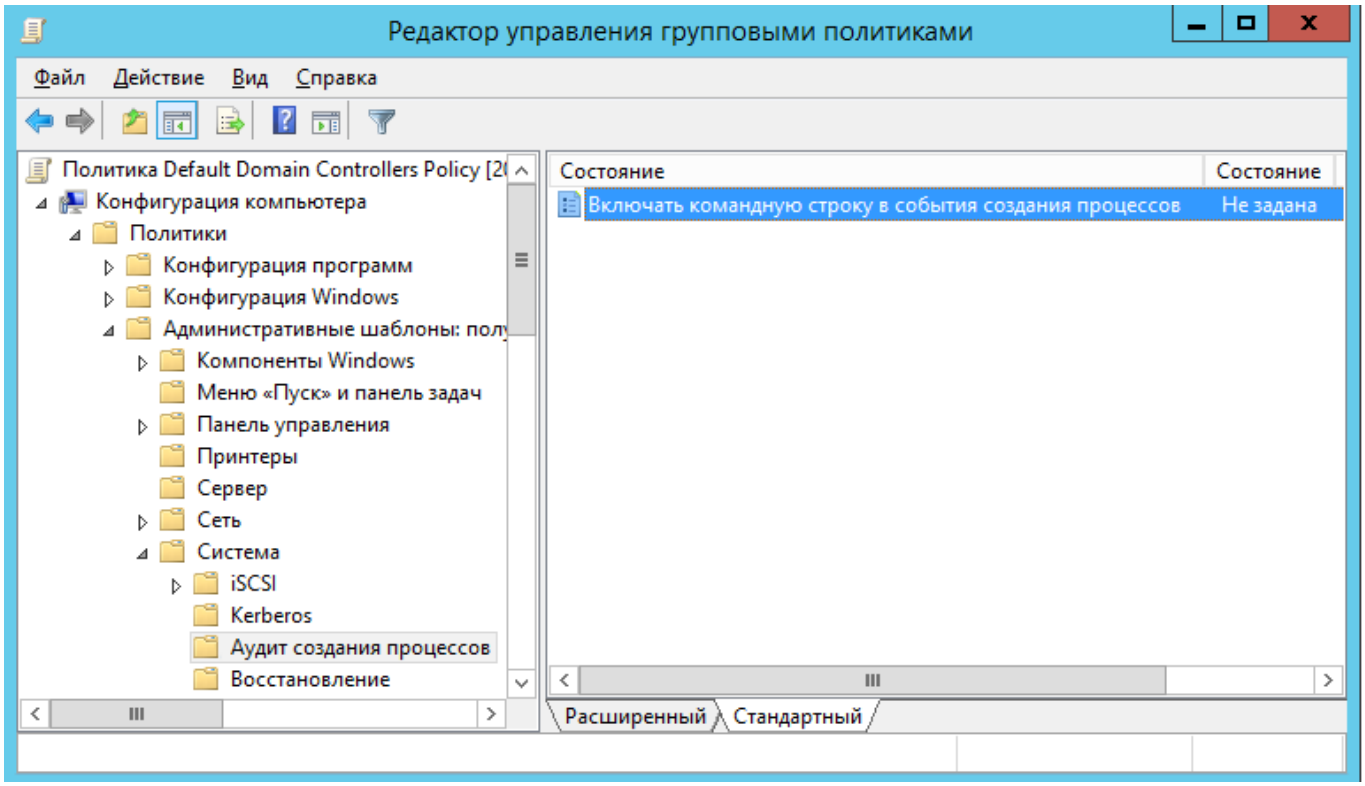


Рисунок 1 - Выбор параметра **Включать командную строку в события создания процессов**

7. В главном меню выбрать Действие → Изменить.
8. Выбрать вариант Включено.
9. Нажать ОК.

2.3 Настройка расширенной политики аудита с помощью групповой политики

Чтобы настроить расширенную политику аудита с помощью групповой политики необходимо:

1. Открыть панель управления Windows.

2. Выбрать Администрирование → Управление групповой политикой. Есть возможность запустить консоль управления групповыми политиками, выполнив команду `gpmc.msc`.
3. В левой части окна выберите:
   если нужно настроить групповую политику для контроллеров домена — Управление групповой политикой → Лес: <Имя леса> → Домены → <Имя домена> → Domain Controllers → <Имя групповой политики контроллеров домена>;
   если нужно настроить групповую политику для серверов или рабочих станций — Управление групповой политикой → Лес: <Имя леса> → Домены → <Имя домена> → <Имя групповой политики серверов или рабочих станций>.

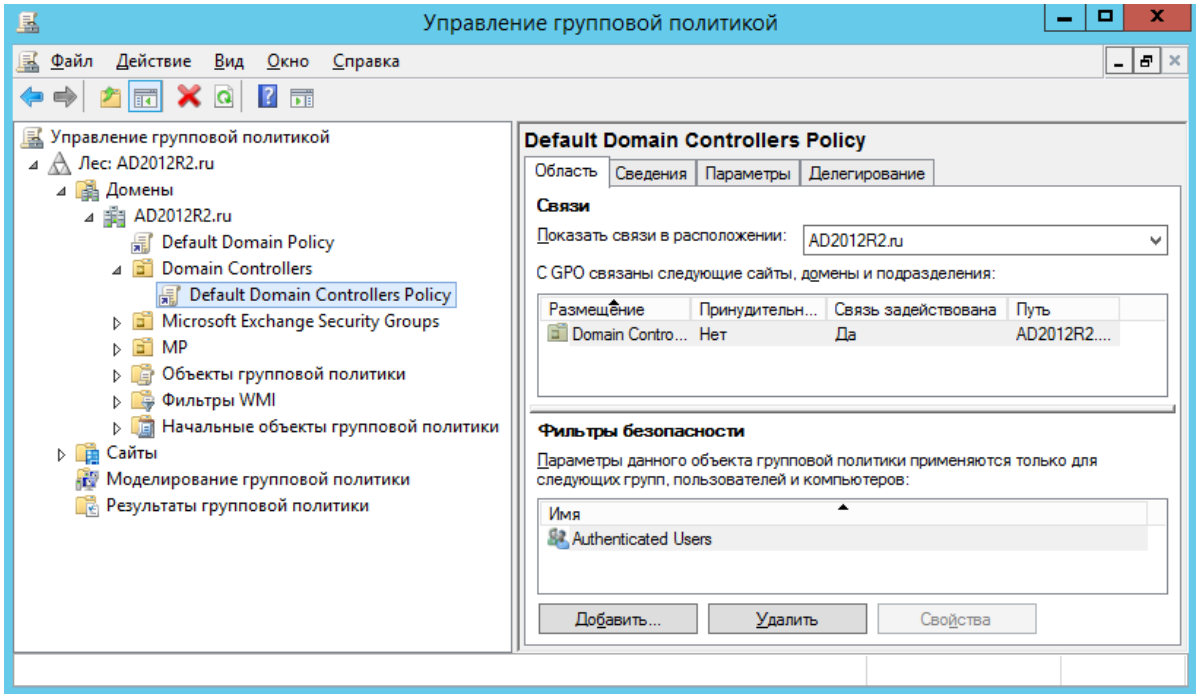


Рисунок 2 - Выбор объекта групповой политики

4. В главном меню выбрать Действие → Изменить. Откроется окно Редактор управления групповыми политиками.
5. Выберите узел Конфигурация компьютера → Политики → Конфигурация Windows → Параметры безопасности → Конфигурация расширенной политики аудита → Политики аудита → <Название категории>.
6. Выберите подкатегорию политики аудита.

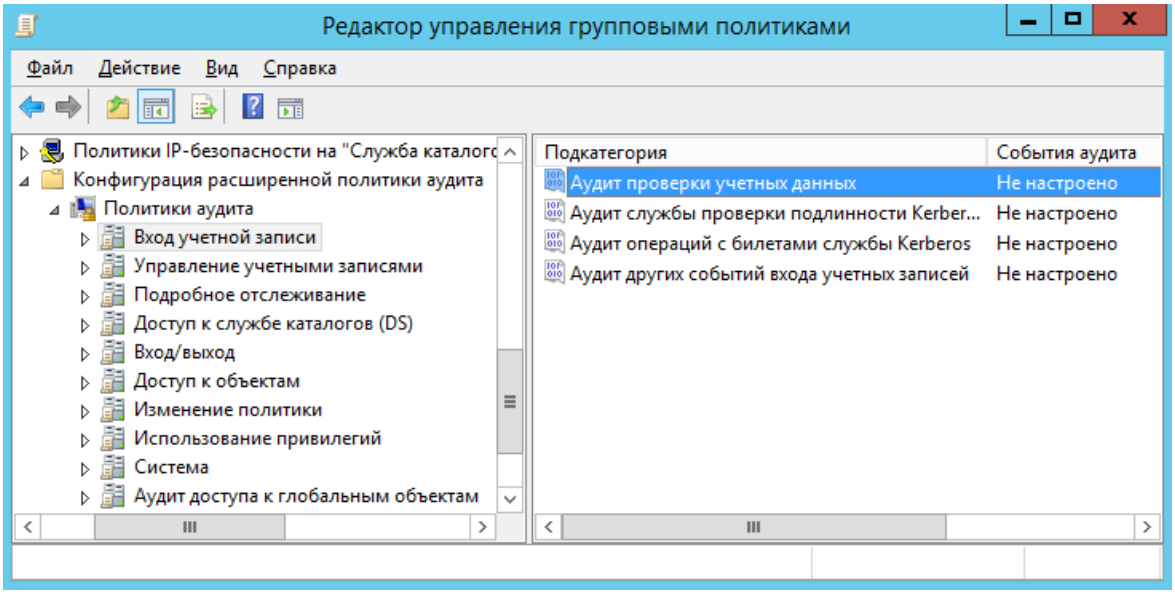


Рисунок 3 - Выбор подкатегории политики аудита

7. В главном меню выбрать Действие → Свойства.
8. Установить флажок Настроить следующие события аудита.
9. Если требуется включить аудит успехов, установить флажок Успех.
10. Если требуется включить аудит отказов, установить флажок Отказ.

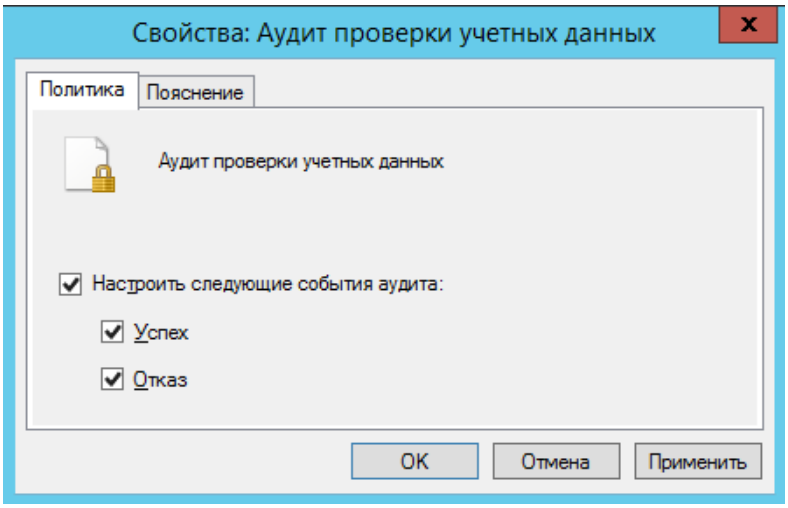


Рисунок 4 - Настройка подкатегории политики аудита

11. Нажать кнопку ОК

Расширенная политика аудита настроена.

2.4 Настройка политики аудита утилитой auditpol

Для настройки политики аудита можно использовать утилиту auditpol, входящую в состав ОС.

Чтобы настроить политику аудита необходимо:

1. Нажать Пуск → Выполнить.
2. В поле Открыть ввести cmd и нажать ОК. Откроется интерфейс командной строки.
3. Получить статус категорий политик аудита:
   `auditpol /get /category:*`
   На экране появится список категорий и подкатегорий политик аудита с указанием статуса.
4. Настроить категории политики аудита:

- Если требуется включить аудит успехов:
  `auditpol /set /category:<Название категории> /success:enable`
- Если требуется отключить аудит успехов:
  `auditpol /set /category:<Название категории> /success:disable`
- Если требуется включить аудит отказов:
  `auditpol /set /category:<Название категории> /failure:enable`
- Если требуется отключить аудит отказов:
  `auditpol /set /category:<Название категории> /failure:disable`

5. Настройть подкатегории политики аудита:

- Если требуется включить аудит успехов:
  `auditpol /set /subcategory:<Название подкатегории> /success:enable`
- Если требуется включить аудит отказов:
  `auditpol /set /subcategory:<Название подкатегории> /failure:enable`

В результате политика аудита настроена.

3. Microsoft Windows XP: настройка источника

Настройку источника нужно выполнять от имени учетной записи, имеющей права локального администратора Windows.

При использовании в IT-инфраструктуре организации межсетевого экрана или других средств для контроля сетевого трафика требуется настроить в них правила, разрешающие трафик в обоих направлениях между узлом источника и узлом NT Collector. Используются системный TCP-порт 135 и динамические TCP-порты 1024—5000.

При использовании на узле источника межсетевого экрана Windows в нем нужно включить правила для входящих подключений «Инструментарий управления Windows (асинхронный — входящий трафик)» (Windows Management Instrumentation (ASync-In)), «Инструментарий управления Windows (DCOM — входящий трафик)» (Windows Management Instrumentation (DCOM-In)), «Инструментарий управления Windows (WMI — входящий трафик)» (Windows Management Instrumentation (WMI-In)).

Для того, чтобы **включить правило межсетевого экрана Windows** необходимо выполнить следующие действия:

a) Открыть панель управления Windows.
b) Запустить брандмауэр Windows.
c) В левой части окна выбрать узел Монитор брандмауэра Защитника Windows в режиме повышенной безопасности → <Категория правила>.
d) Выбрать правило.
e) В главном меню выбрать Действия → Включить правило.

Для настройки журналирования событий на источнике требуется настроить локальную групповую политики аудита событий. События сохраняются в журнале событий Windows.

Для сбора событий из журнала Windows на источнике нужно:

1. Отключить гостевую учетную запись.
2. Создать локальную учетную запись для доступа NT Collector и удалить эту запись из группы «Пользователи».

Данные этой учетной записи нужно указать при добавлении учетной записи в NT SIEM.

3. Настроить локальную групповую политику, чтобы добавить учетную запись в политики безопасности «Доступ к компьютеру из сети» и «Управление аудитом и журналом безопасности».

4. Настроить для учетной записи разрешения на имя CIMV2 в пространстве имен WMI.
5. Настроить для учетной записи разрешения на COM-приложения.

3.1 Настройка локальных политик аудита событий

С помощью локальной групповой политики нужно настроить политики аудита событий в соответствии с таблицей Параметры политик аудита.

Политика	**Тип аудита**
Аудит входа в систему	Успех, Отказ
Аудит доступа к объектам	Успех, Отказ
Аудит доступа к службе каталогов	Успех, Отказ
Аудит изменения политики	Успех, Отказ
Аудит использования привилегий	Успех, Отказ
Аудит отслеживания процессов	Успех, Отказ
Аудит системных событий	Успех, Отказ
Аудит событий входа в систему	Успех, Отказ
Аудит управления учетными записями	Успех, Отказ

Чтобы настроить локальную политику аудита событий необходимо:

1. Нажать Пуск → Выполнить.
2. В поле Открыть ввести gpedit.msc и нажать кнопку ОК. Откроется редактор локальной групповой политики.
3. В иерархическом списке выбать узел Политика "Локальный компьютер" → Конфигурация компьютера → Конфигурация Windows → Параметры безопасности → Локальные политики → Политика аудита.
4. Выбрать политику.
5. В главном меню выбрать Действие → Свойства. Откроется окно Свойства: <Название политики>.
6. Если требуется включить аудит успехов, установить флажок Успех.
7. Если требуется включить аудит отказов, установить флажок Отказ.
8. Нажать кнопку ОК.
9. Нажать Пуск → Выполнить.
10. В поле Открыть ввести gpupdate /force и нажать кнопку ОК.

В результате локальная политика аудита событий настроена.

3.2 Отключение гостевой учетной записи

Если на узле есть службы, которые запускаются от имени гостевой учетной записи, отключение этой записи может привести к неработоспособности таких служб.

Чтобы отключить гостевую учетную запись необходимо:

1. Нажать Пуск → Выполнить.
2. В поле Открыть ввести regedit и нажать ОК. Откроется окно Редактор реестра.
3. В иерархическом списке выбрать узел Мой компьютер → HKEY_LOCAL_MACHINE → SYSTEM → CurrentControlSet → Control → Lsa.
4. Выбрать параметр forceguest.
5. В главном меню выбрать Правка → Изменить. Откроется окно Изменение параметра DWORD.
6. В поле Значение ввести 0.

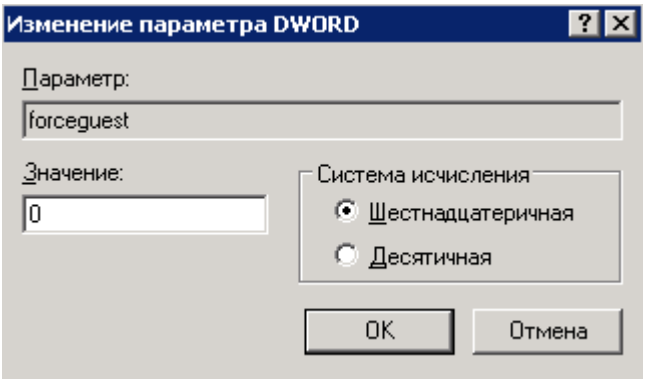


Рисунок 5 - Настройка параметра forceguest

7. Нажать кнопку ОК.

В результате гостевая учетная запись будет отключена.

3.3 Создание учетной записи ОС

Чтобы создать учетную запись пользователя ОС необходимо:

1. Открыть панель управления Windows.
2. Выбрать Администрирование → Управление компьютером. Откроется консоль управления компьютером.

Также есть возможность открыть консоль управления компьютером, выполнив команду `compmgmt.msc`.

3. В левой части окна выберать узел Управление компьютером → Локальные пользователи и группы → Пользователи.
4. В главном меню выбрать Действие → Новый пользователь.
5. В открывшемся окне в поле Новый пользователь ввести логин учетной записи.
6. В поле Пароль ввести пароль и подтвердить его в поле Подтверждение.
7. Снять флажок Потребовать смену пароля при следующем входе в систему.

8. Установить флажок Запретить смену пароля пользователем.
9. Установить флажок Срок действия пароля не ограничен.

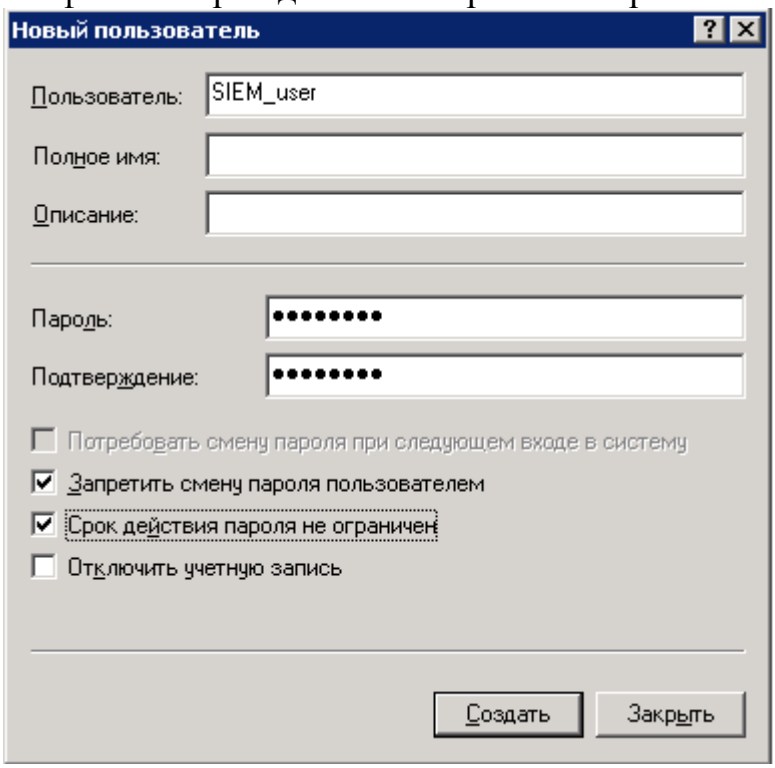


Рисунок 6 - Настройка параметров учетной записи

10. Нажать кнопку Создать.
11. Нажать кнопку Закрыть.

В результате учетная запись будет создана.

Чтобы удалить учетную запись из группы «Пользователи» необходимо:

1. Открыть панель управления Windows.
2. Выбрать Администрирование → Управление компьютером.

Откроется консоль управления компьютером.

Также можно открыть консоль управления компьютером, выполнив команду compmgmt.msc.

3. В левой части окна выбрать узел Управление компьютером → Локальные пользователи и группы → Пользователи.
4. Выбрать учетную запись.
5. В главном меню выбрать Действие → Свойства.

Откроется окно Свойства:<Имя пользователя>.

6. Выбрать вкладку Членство в группах.
7. Выбрать группу Пользователи.
8. Нажать кнопку Удалить.
9. Нажать кнопку ОК.

В результате учетная запись будет удалена из группы.

3.4 Настройка локальной групповой политики для учетной записи

Чтобы настроить локальную групповую политику необходимо:

1. Нажать Пуск → Выполнить.
2. В поле Открыть ввести gpedit.msc и нажать кнопку ОК. Откроется редактор локальной групповой политики.
3. В левой части окна выбрать Политика "Локальный компьютер" → Конфигурация компьютера → Конфигурация Windows → Параметры безопасности → Локальные политики → Назначение прав пользователя.
4. Выбрать Доступ к компьютеру из сети.
5. В главном меню выбрать Действие → Свойства. Откроется окно Свойства: Доступ к компьютеру из сети.
6. Нажать кнопку Добавить пользователя или группу. Откроется окно Выбор: Пользователи или Группы.
7. В поле Введите имена выбираемых объектов введсти логин учетной записи и нажать кнопку ОК.
8. Нажать кнопку ОК.
9. Выбрать Управление аудитом и журналом безопасности.
10. В главном меню выбрать Действие → Свойства. Откроется окно Свойства: Управление аудитом и журналом безопасности.
11. Нажать кнопку Добавить пользователя или группу. Откроется окно Выбор: Пользователи или Группы.
12. В поле Введите имена выбираемых объектов ввести логин учетной записи и нажать кнопку ОК.
13. Нажать кнопку ОК.
14. Нажать Пуск → Выполнить.
15. В поле Открыть ввести gpupdate /force и нажать кнопку ОК.

В результате локальная групповая политика будет настроена.

3.5 Настройка разрешений на имя в пространстве имен WMI

Чтобы настроить разрешения учетной записи на имя в пространстве имен WMI необходимо:

1. Открыть панель управления Windows.
2. Выбрать Администрирование → Управление компьютером.

Также можно открыть консоль инфраструктуры управления Windows (WMI) выполнив команду wmimgmt.msc.

3. В левой части окна выбрать узел Управление компьютером → Службы и приложения → Управляющий элемент WMI.
4. В главном меню выбрать Действие → Свойства. Откроется окно Свойства: Управляющий элемент WMI.
5. Выбрать вкладку Безопасность.
6. В иерархическом списке выбрать узел Root → CIMV2.
7. Нажать кнопку Безопасность. Откроется окно Безопасность для ROOT\CIMV2.
8. Нажать кнопку Дополнительно. Откроется окно Дополнительные параметры безопасности для CIMV2.
9. Нажать кнопку Добавить. Откроется окно Выбор: Пользователи или Группы.
10. В поле Введите имена выбираемых объектов ввести логин учетной записи и нажать кнопку ОК. Откроется окно Элемент разрешения для CIMV2.
11. В раскрывающемся списке Применять выбрать Данное пространство и подпространство имен.
12. В колонке Разрешить установить флажки Выполнение методов, Включить учетную запись, Включить удаленно, Прочесть безопасность и нажать кнопку ОК.

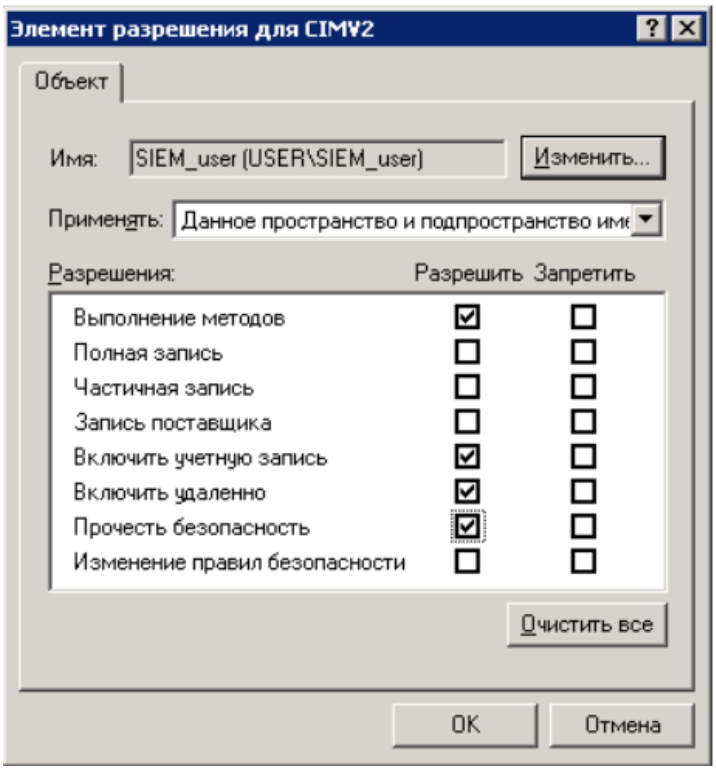


Рисунок 7 - Настройка разрешений учетной записи

13. В окне Дополнительные параметры безопасности для CIMV2 нажать кнопку ОК.
14. В окне Безопасность для ROOT\CIMV2 нажать кнопку ОК.
15. В окне Свойства: Управляющий элемент WMI нажать кнопку ОК.

В результате разрешения учетной записи будут настроены.

3.6 Настройка разрешений на COM-приложения

Чтобы настроить разрешения на COM-приложения для группы COM-пользователей необходимо:

1. Открыть панель управления Windows.
2. Выбрать Администрирование → Службы компонентов. Откроется консоль службы компонентов.

   Также можно открыть консоль службы компонентов выполнив команду dcomcnfg.exe.
3. В левой части окна выбрать узел Корень консоли → Службы компонентов → Компьютеры → Мой компьютер.
4. В главном меню выбрать Действие → Свойства. Откроется окно Свойства: Мой компьютер.
5. Выбрать вкладку Безопасность COM.
6. В блоке параметров Права доступа нажать кнопку Изменить настройки по умолчанию. Откроется окно Разрешение на доступ.
7. Нажать кнопку Добавить. Откроется окно Выбор: Пользователи или Группы.
8. В поле Введите имена выбираемых объектов ввести логин учетной записи и нажать кнопку ОК.
9. В окне Разрешение на доступ в колонке Разрешить установить флажки Локальный доступ и Удаленный доступ.

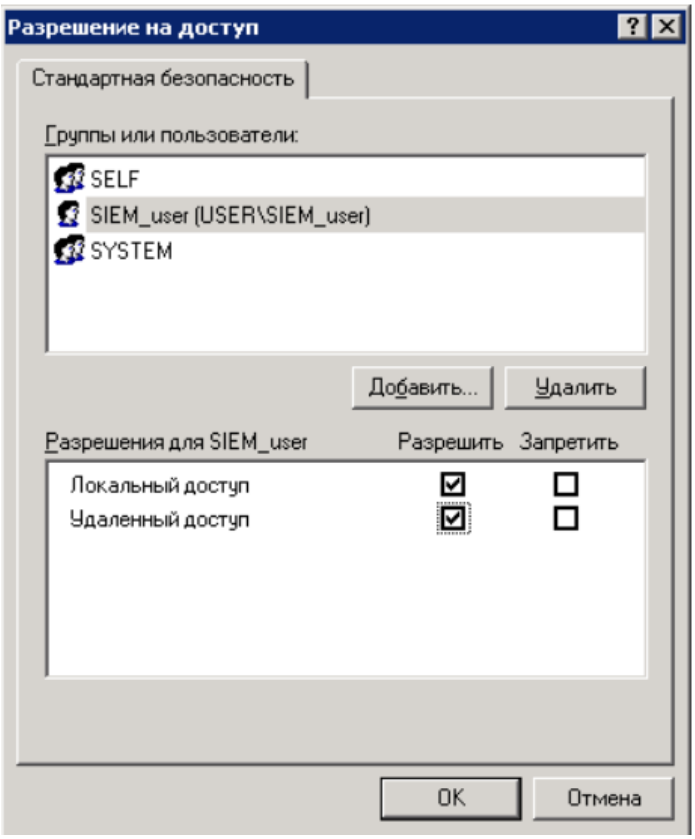


Рисунок 8 - Настройка для учетной записи разрешений на доступ по умолчанию

10. Нажать кнопку ОК.
11. В блоке параметров панели Разрешения на запуск и активацию нажать кнопку Изменить настройки по умолчанию. Откроется окно Разрешение на запуск.
12. Нажать кнопку Добавить. Откроется окно Выбор: Пользователи или Группы.
13. В поле Введите имена выбираемых объектов ввести логин учетной записи и нажать кнопку ОК.
14. В окне Разрешение на запуск в колонке Разрешить установить флажки Локальный запуск, Удаленный запуск, Локальная активация, Удаленная активация.

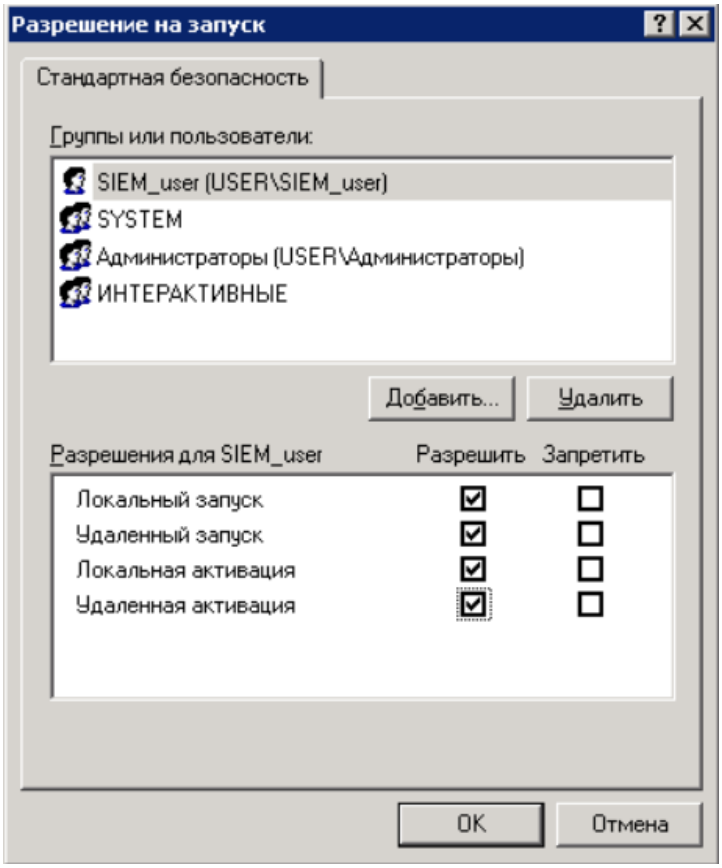


Рисунок 9 - Настройка для учетной записи разрешений на запуск и активацию по умолчанию

15. Нажать кнопку ОК.
16. В блоке параметров панели Разрешения на запуск нажать кнопку Изменить ограничения.
17. Нажать кнопку Добавить. Откроется окно Выбор: Пользователи или Группы.
18. В поле Введите имена выбираемых объектов ввести логин учетной записи и нажать кнопку ОК.
19. В окне Разрешение на запуск в колонке Разрешить установить флажки Локальный запуск, Удаленный запуск, Локальная активация, Удаленная активация.

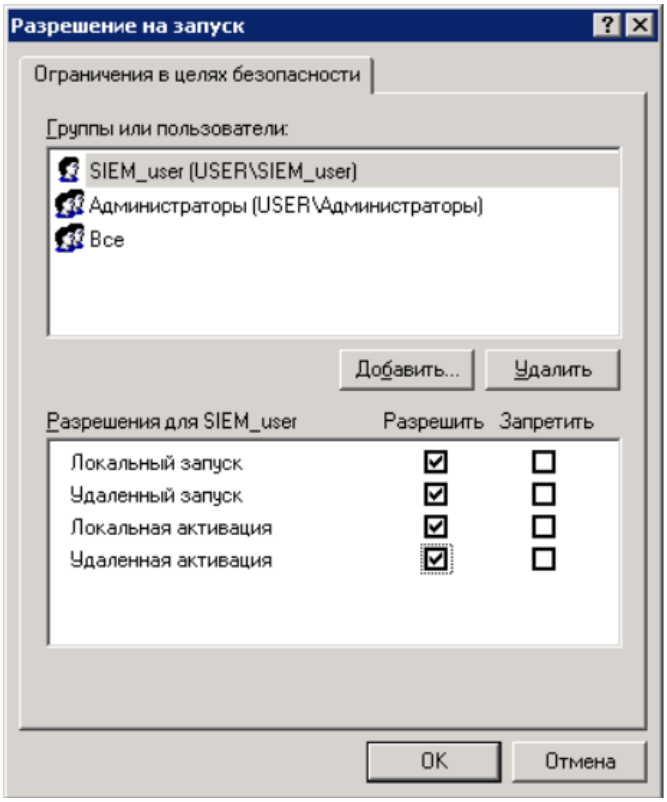


Рисунок 10 - Настройка для учетной записи разрешений на запуск и активацию

20. Нажать кнопку ОК.

21. В окне Свойства: Мой компьютер нажать кнопку ОК.

В результате разрешения будут настроены.

4. Microsoft Windows Server 2003, 2003 R2: настройка источника

Настройку источника нужно выполнять от имени учетной записи, имеющей права локального администратора Windows.

При использовании в IT-инфраструктуре организации межсетевого экрана или других средств для контроля сетевого трафика требуется настроить в них правила, разрешающие трафик в обоих направлениях между узлом источника и узлом NT Collector. Используются системный TCP-порт 135 и динамические TCP-порты 1024-5000.

При использовании на узле источника межсетевого экрана Windows в нем нужно включить правила для входящих подключений «Инструментарий управления Windows (асинхронный — входящий трафик)» (Windows Management Instrumentation (ASync-In)), «Инструментарий управления Windows (DCOM — входящий трафик)» (Windows Management Instrumentation (DCOM-In)), «Инструментарий управления Windows (WMI — входящий трафик)» (Windows Management Instrumentation (WMI-In)).

Чтобы включить правило межсетевого экрана Windows необходимо:

a) Открыть панель управления Windows.
b) Запустить брандмауэр Windows.
c) В левой части окна выбрать узел Монитор брандмауэра Защитника Windows в режиме повышенной безопасности → <Категория правила>.
d) Выбрать правило.
e) В главном меню выберите Действия → Включить правило.

События сохраняются в журнале событий Windows.

Для сбора событий из журнала Windows на источнике нужно:

1. Средствами ОС создать учетную запись локального пользователя ОС для доступа NT Collector.

   Чтобы создать учетную запись пользователя ОС необходимо:

   a) Открыть панель управления Windows.
   b) Выбрать Администрирование → Управление компьютером.
   c) В левой части окна выбрать узел Управление компьютером → Локальные пользователи и группы → Пользователи.
   d) В главном меню выбрать Действие → Новый пользователь.
   e) В поле Пользователь ввести логин учетной записи.
   f) Установить флажок Запретить смену пароля пользователем.

g) Установить флажок Срок действия пароля не ограничен.
h) Ввести пароль и подтвердить его.

Следует отметить, что данные этой учетной записи нужно указать при добавлении учетной записи в NT SIEM.

2. Добавить учетную запись в локальную группу пользователей Distributed COM Users.

Чтобы добавить учетную запись в локальную группу пользователей необходимо:

a) Открыть панель управления Windows.
b) Выбрать Администрирование → Управление компьютером.
c) В левой части окна выбрать узел Локальные пользователи и группы → Группы.
d) Выбрать группу, в которую нужно добавить учетную запись.
e) В главном меню выбрать Действие → Добавить в группу.
f) Нажать Добавить.
g) Нажать Размещение.
h) В открывшемся окне выбрать:
если используется локальная учетная запись — имя узла;
если используется доменная учетная запись — имя домена.
i) Нажать ОК.
j) В поле Введите имена выбираемых объектов ввести логин учетной записи и нажать ОК.
k) В окне Свойства <Имя группы> нажать ОК.

Группа Distributed COM Users должна быть добавлена в локальные политики безопасности «DCOM: Ограничения компьютера на доступ в синтаксисе SDDL» с разрешением «Удаленный доступ» и «DCOM: Ограничения компьютера на запуск в синтаксисе SDDL» с разрешением «Удаленная активация». Группе должны быть предоставлены права на приложения COM: право доступа с разрешением «Удаленный доступ» и право на запуск и активацию с разрешением «Удаленная активация».

3. Добавить учетную запись в локальную (групповую) политику безопасности «Доступ к компьютеру из сети» (Access this computer from the network).

Чтобы добавить учетную запись в локальную политику безопасности необходимо:

a) Открыть панель управления Windows.
b) Выбрать Администрирование → Локальная политика безопасности.

c) В левой части окна выбрать узел Параметры безопасности → Локальные политики → Назначение прав пользователя.
d) Выбрать политику, к которой нужно добавить учетную запись.
e) В главном меню выбрать Действие → Свойства.
f) В открывшемся окне нажать кнопку Добавить пользователя или группу.
g) В открывшемся окне нажать кнопку Размещение.
h) В открывшемся окне выбрать:
если используется локальная учетная запись — имя узла;
если используется доменная учетная запись — имя домена.
i) Нажать кнопку ОК.
j) В поле Введите имена выбираемых объектов ввестие логин учетной записи и нажать ОК.
k) В окне Свойства <Имя политики> нажать ОК.

4. Выдать учетной записи в пространстве имен WMI разрешения «Включить учетную запись», «Включить удаленно», «Прочесть безопасность» на имя cimv2.
5. Добавить учетную запись в локальную группу пользователей Administrators или получить идентификатор безопасности учетной записи и настроить доступ к журналам ОС.

   Чтобы добавить учетную запись в локальную группу пользователей необходимо:

   a) Открыть панель управления Windows.
   b) Выбрать Администрирование → Управление компьютером.
   c) В левой части окна выбрать узел Локальные пользователи и группы → Группы.
   d) Выбрать группу, в которую нужно добавить учетную запись.
   e) В главном меню выбрать Действие → Добавить в группу.
   f) Нажать Добавить.
   g) Нажать Размещение.
   h) В открывшемся окне выбрать:
   если используется локальная учетная запись — имя узла;
   если используется доменная учетная запись — имя домена.
   i) Нажать ОК.
   j) В поле Введите имена выбираемых объектов ввести логин учетной записи и нажать ОК.
   k) В окне Свойства <Имя группы> нажать ОК.

6. Отключить контроль учетных записей (UAC).

4.1 Настройка локальной политики безопасности для группы Distributed COM Users

Чтобы настроить локальную политику безопасности для группы Distributed COM Users необходимо:

1. Открыть панель управления Windows.
2. Выбрать Администрирование → Локальная политика безопасности.
   Также можно запустить оснастку для настройки локальных параметров безопасности, выполнив команду secpol.msc.
3. В левой части окна выбрать узел Локальные политики → Параметры безопасности.
4. Выбрать политику DCOM: Ограничения компьютера на доступ в синтаксисе SDDL (DCOM: Machine Access Restrictions in Security Descriptor Definition Language (SDDL) syntax).
5. В главном меню выбрать Действие → Свойства.

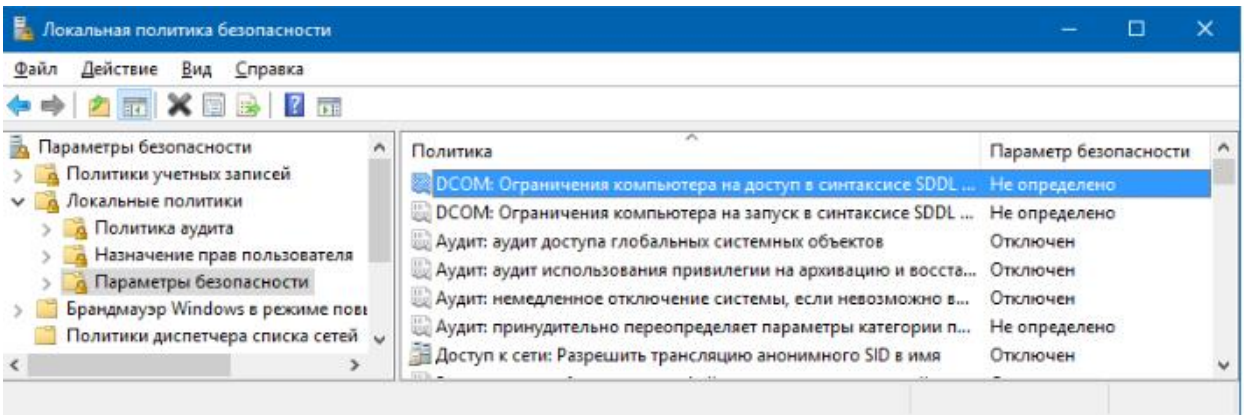


Рисунок 11 - Выбор локальной политики безопасности

6. В открывшемся окне нажать кнопку Изменить.
7. В открывшемся окне выбрать группу пользователей Distributed COM Users.
8. В нижней части окна в столбце Разрешить установить флажок Удаленный доступ.

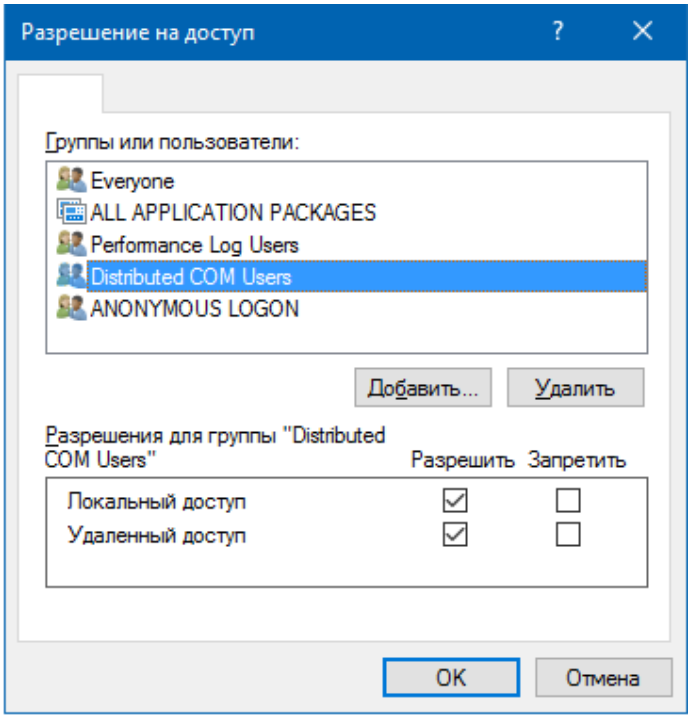


Рисунок 12 - Настройка разрешений политики в «DCOM: Ограничения компьютера на доступ в синтаксисе SDDL» для группы Distributed COM Users

9. Нажать кнопку ОК.
10. В окне Свойства <Имя политики> нажать кнопку ОК.
11. Выбрать политику DCOM: Ограничения компьютера на запуск в синтаксисе SDDL (DCOM: Machine Launch Restrictions in Security Descriptor Definition Language (SDDL) syntax).
12. В главном меню выбрать Действие → Свойства.
13. В открывшемся окне нажать кнопку Изменить.
14. В открывшемся окне выбрать группу пользователей Distributed COM Users.
15. В нижней части окна в столбце Разрешить установить флажок Удаленная активация.

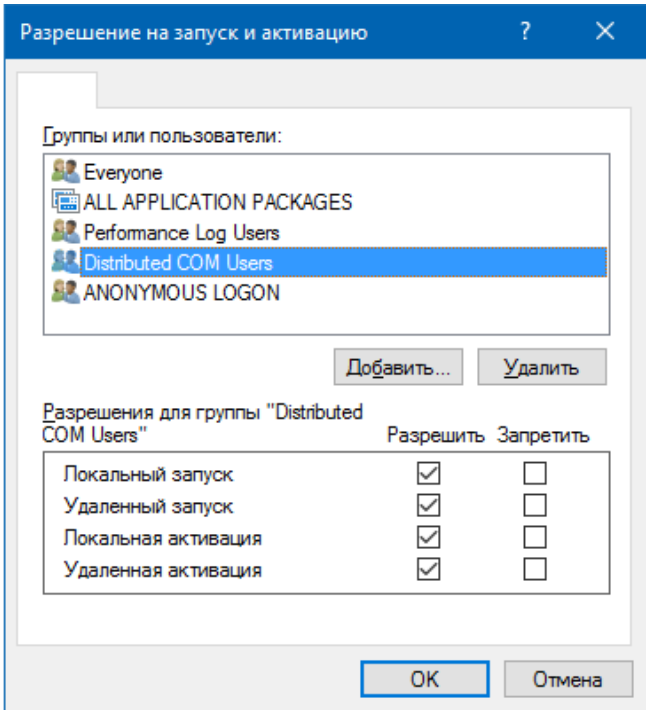


Рисунок 13 - Настройка разрешений политики в «DCOM: Ограничения компьютера на запуск в синтаксисе SDDL» для группы Distributed COM Users

16. Нажать кнопку ОК.
17. В окне Свойства <Имя политики> нажать кнопку ОК.

В результате локальная политика безопасности будет настроена.

4.2 Настройка разрешений на COM-приложения для группы COM-пользователей

Чтобы настроить разрешения на COM-приложения для группы COM-пользователей необходимо:

1. Открыть панель управления Windows.
2. Выбрать Администрирование → Службы компонентов.
3. В левой части окна выбрать узел Корень консоли → Службы компонентов → Компьютеры → Мой компьютер.

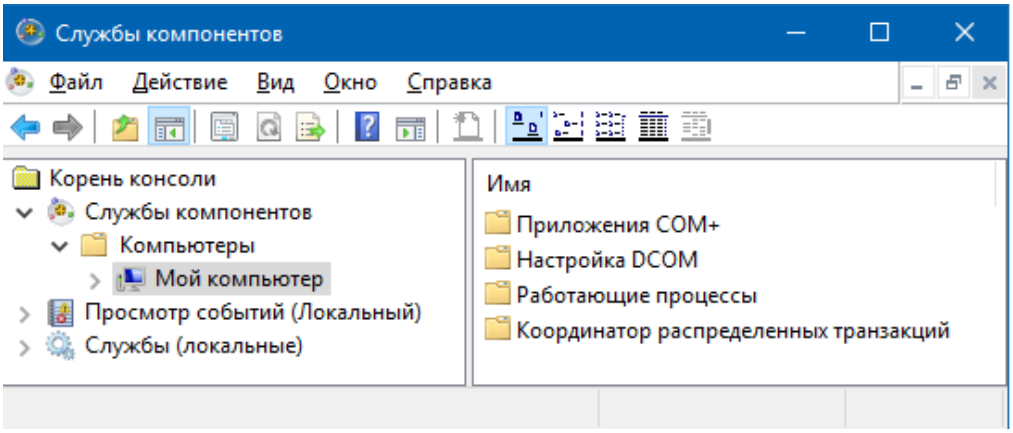


Рисунок 14 - Выбор узла Мой компьютер

4. В главном меню выбрать Действие → Свойства.
5. В открывшемся окне выбрать вкладку Безопасность COM.

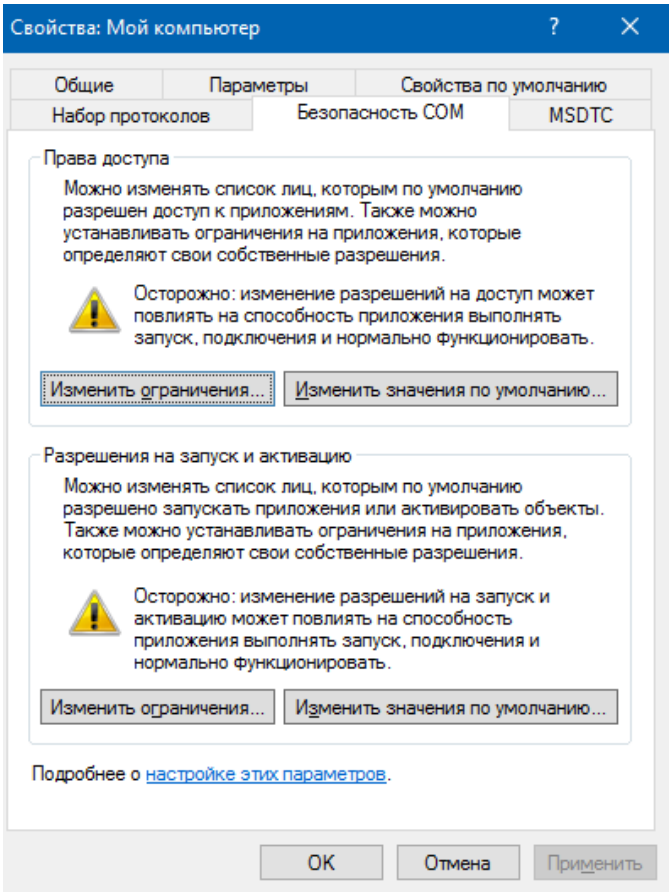


Рисунок 15 - Вкладка Безопасность COM

6. В панели Права доступа нажать кнопку Изменить ограничения.
7. В открывшемся окне нажать кнопку Добавить.
8. В открывшемся окне нажать кнопку Размещение.
9. В открывшемся окне выбрать имя узла и нажать кнопку ОК.
10. В поле Введите имена выбираемых объектов ввести Distributed COM Users и нажать кнопку Проверить имена.
11. Нажать кнопку ОК.
12. В поле Разрешения для группы "Distributed COM Users" в столбце Разрешить установить флажок Удаленный доступ.

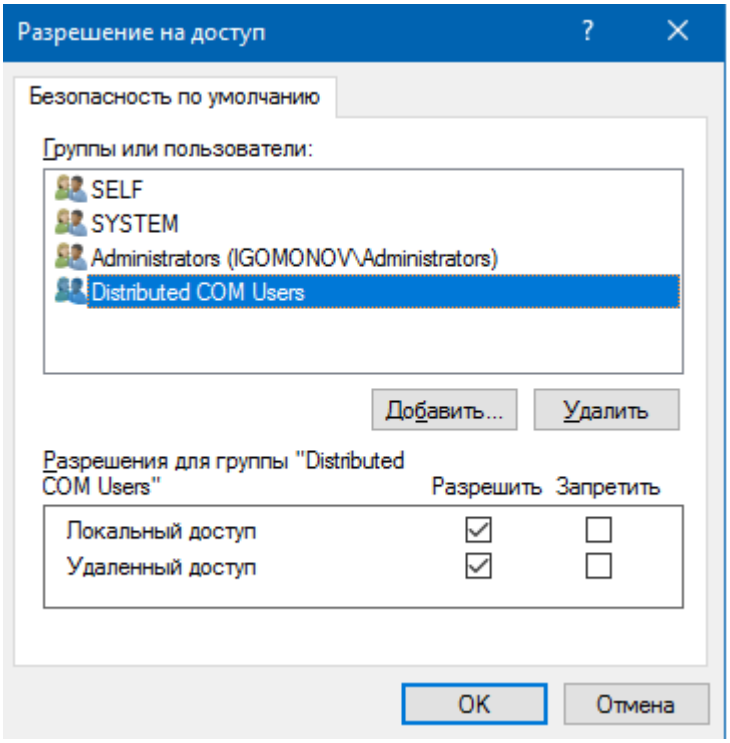


Рисунок 16 - Настройка разрешений на доступ для группы Distributed COM Users

13. Нажать кнопку ОК.
14. В панели Разрешения на запуск и активацию нажать кнопку Изменить ограничения.
15. В открывшемся окне нажать кнопку Добавить.
16. В открывшемся окне нажать кнопку Размещение.
17. В открывшемся окне выбрать имя узла и нажать кнопку ОК.
18. В поле Введите имена выбираемых объектов ввести Distributed COM Users и нажать кнопку Проверить имена.
19. Нажать кнопку ОК.
20. В поле Разрешения для группы "Distributed COM Users" в столбце Разрешить установить флажки Удаленный запуск, Удаленная активация.

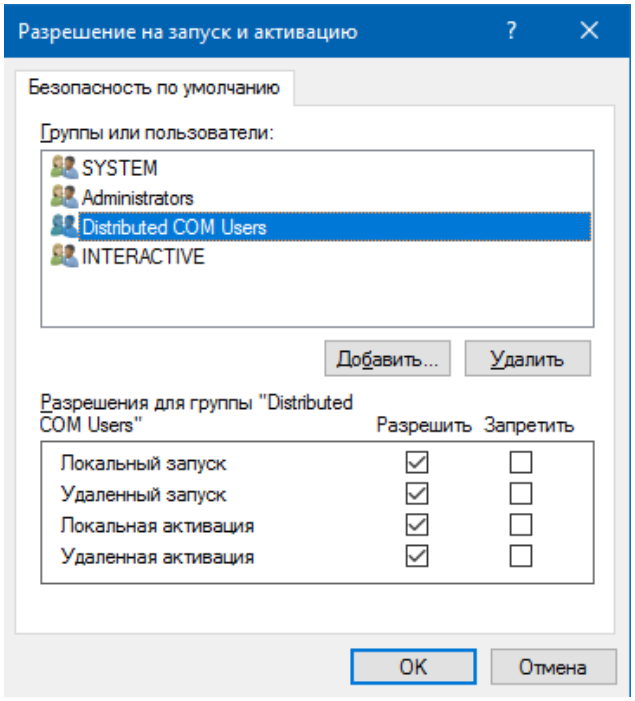


Рисунок 17 - Настройка разрешений на запуск и активацию для группы Distributed COM Users

21. Нажать кнопку ОК.
22. В окне Свойства: Мой компьютер нажать кнопку ОК.

В результате разрешения будут настроены.

4.3 Настройка разрешений на имя в пространстве имен WMI

Чтобы настроить разрешения учетной записи на имя в пространстве имен WMI необходимо:

1. Открыть панель управления Windows.
2. Выбрать Администрирование → Управление компьютером.
3. В левой части окна выбрать узел Управление компьютером → Службы и приложения → Управляющий элемент WMI.

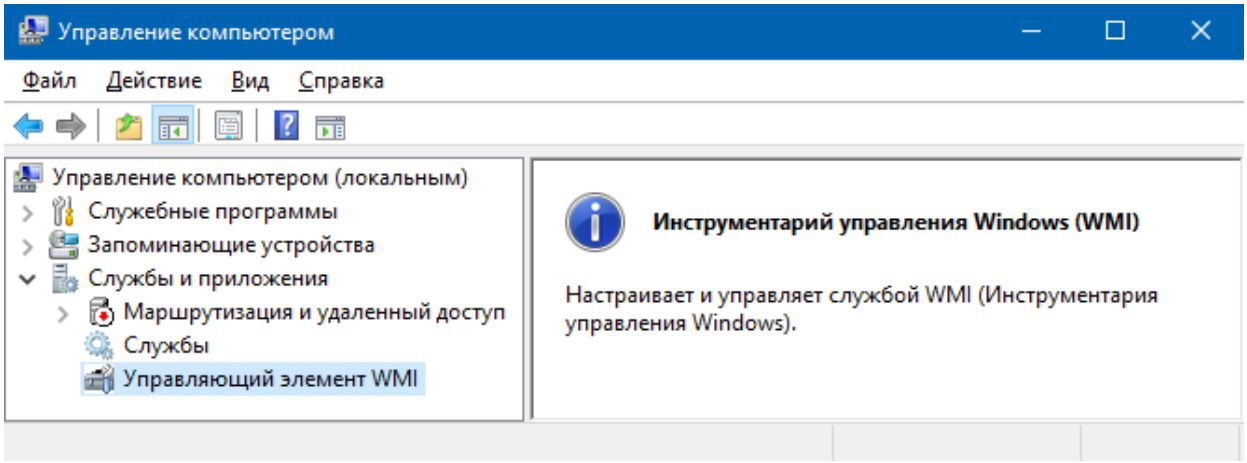


Рисунок 18 - Выбор узла Управляющий элемент WMI

4. В главном меню выбрать Действие → Свойства.
5. В открывшемся окне выбрать вкладку Безопасность.
6. Выбрать узел Root → cimv2.

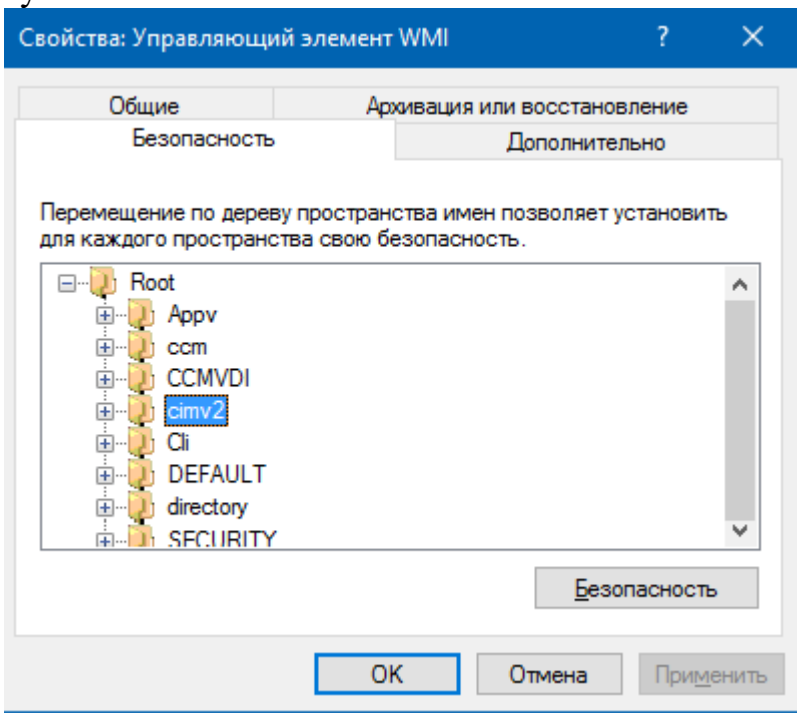
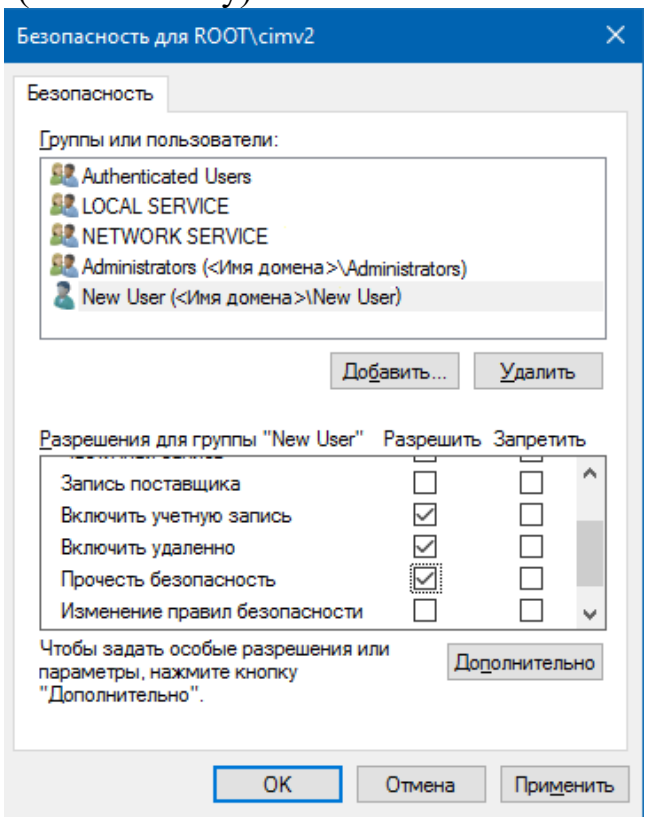


Рисунок 19 - Выбор имени в пространстве имен WMI

7. Нажать кнопку Безопасность.
8. В открывшемся окне нажать кнопку Добавить.
9. В открывшемся окне нажать кнопку Размещение.
10. В открывшемся окне выбрать:
    если используется локальная учетная запись — имя узла;
    если используется доменная учетная запись — имя домена.
11. Нажать кнопку ОК.
12. В поле Введите имена выбираемых объектов ввести логин учетной записи и нажать кнопку Проверить имена.
13. Нажать кнопку ОК.

14. В окне Безопасность для <Имя WMI> в поле Разрешения для группы <Логин> в столбце Разрешить установить флажки Включить учетную запись (Enable Account), Включить удаленно (Remote Enable), Прочесть безопасность (Read Security).



15. Нажать кнопку ОК.
16. В окне Свойства: Управляющий элемент WMI нажать кнопку ОК.

В результате разрешения на имя будут настроены.

4.4 Получение идентификатора безопасности (SID) учетной записи

Чтобы получить идентификатор безопасности учетной записи необходимо:

1. Нажать Пуск → Выполнить.
2. В поле Открыть ввести cmd и нажать ОК. Откроется интерфейс командной строки.
3. Выполнить команду:

```
wmic useraccount where name='<Логин>' get sid
```

На экране появится идентификатор безопасности указанной учетной записи.

4.5 Настройка доступа к журналу

Чтобы настроить доступ к журналу необходимо:

1. Нажать Пуск → Выполнить.
2. В поле Открыть ввести regedit и нажать ОК. Откроется окно Редактор реестра.
3. В левой части окна выбрать узел `KEY_LOCAL_MACHINE\System\CurrentControlSet\Services\Eventlog\<Имя журнала>`.
4. В правой части окна выбрать CustomSD.

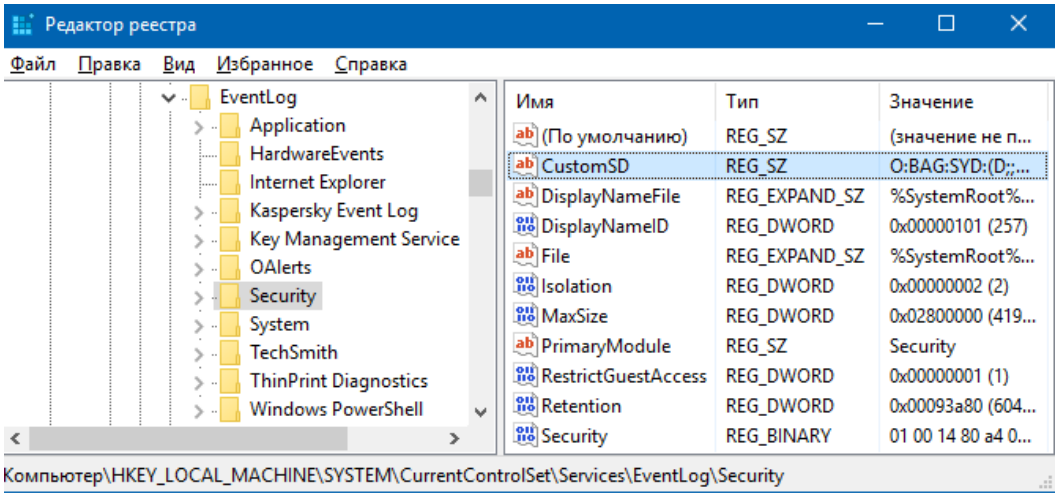


Рисунок 20 - Выбор параметра CustomSD

5. В главном меню выбрать Правка → Изменить.

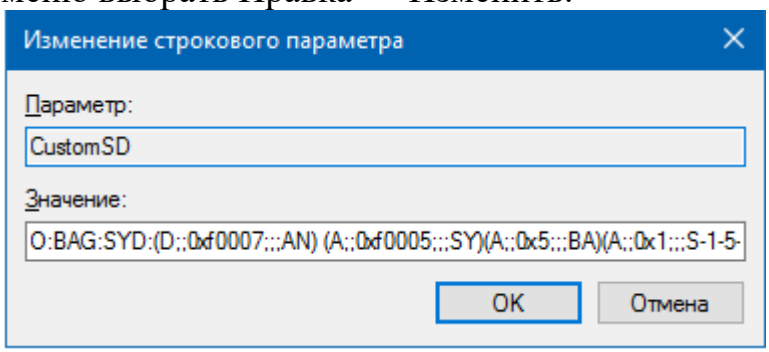


Рисунок 21 - Настройка параметра CustomSD

6. В поле Значение в конец строки дескриптора безопасности журнала добить элемент управления доступом (ACE) для учетной записи NT Collector с разрешением на чтение журнала (A — Access; 0x1 — Read).

`<Дескриптор безопасности журнала>(A;;0x1;;;<SID учетной записи>)`

7. Нажать кнопку ОК.

В результате Доступ к журналу будет настроен.

4.6 Отключение контроля учетных записей (UAC)

Чтобы отключить контроль учетных записей (UAC) необходимо:

1. Нажать Пуск → Выполнить.
2. В поле Открыть ввести regedit и нажать ОК. Откроется окно Редактор реестра.
3. В левой части окна выбрать узел `HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Policies\System`.
4. В главном меню в разделе Правка выбрать пункт Создать → Параметр DWORD (32 бита) и ввести имя параметра `LocalAccountTokenFilterPolicy`.

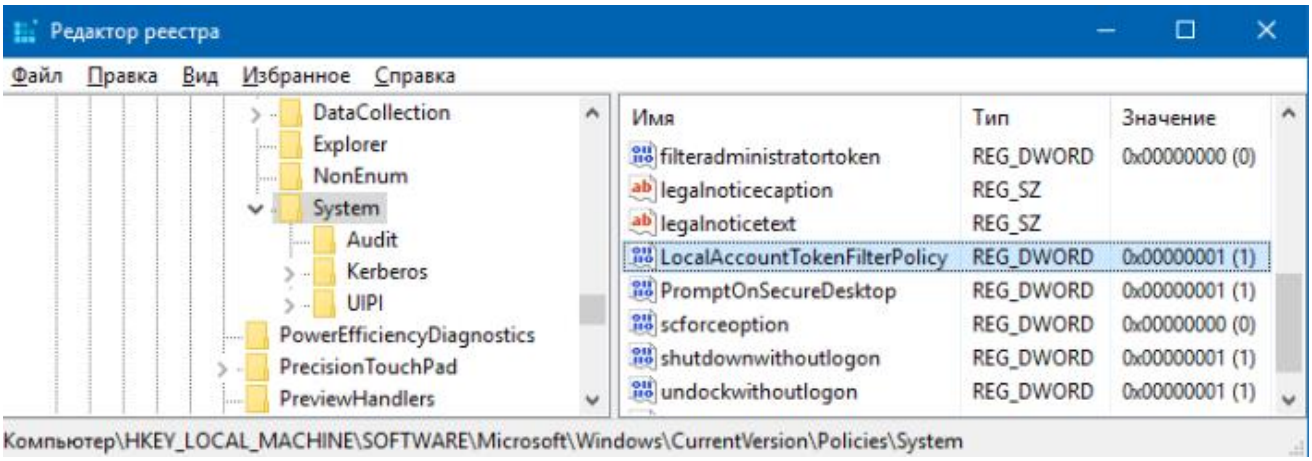


Рисунок 22 - Создание параметра LocalAccountTokenFilterPolicy

5. В главном меню выбрать Правка → Изменить.
6. В блоке параметров Система исчисления выбрать вариант Десятичная.
7. В поле Значение ввести 1 и нажать кнопку ОК.

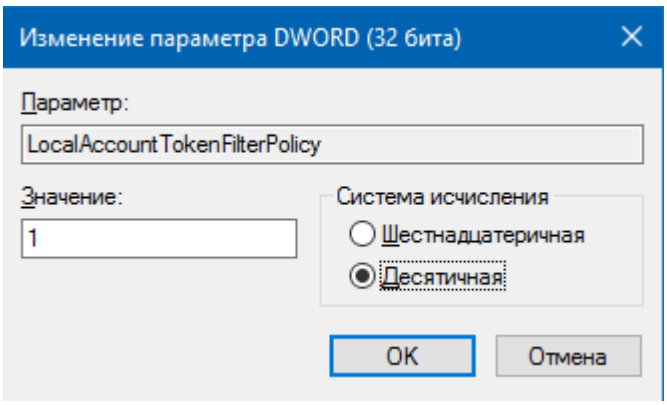


Рисунок 23 - Настройка параметра LocalAccountTokenFilterPolicy

В результате контроль учетных записей будет отключен.