ГАЗИНФОРМ СЕРВИС

# Средство защиты информации от несанкционированного доступа «Блокхост-Сеть 3»

## Руководство администратора безопасности. Приложение 5

Санкт-Петербург, 2019

# Содержание

# Введение

Настоящее приложение предназначено для администраторов средства защиты информации от несанкционированного доступа «Блокхост-Сеть 3» и содержит описание списка событий, фиксируемых в консоли «Система развертывания и аудита».

# Дискреционное управление доступом

| Код события | Тип события | Уровень важности | Формат Windows-события | CEF-формат | Условие воспроизведения |
|---|---|---|---|---|---|
| 257 (0x101) | Доступ к файловому объекту | Сведения | Событие: доступ к файловому объекту<br>Пользователь: domain/login<br>SID пользователя:<br>Метка пользователя:<br>Имя объекта:<br>Метка объекта:<br>Имя процесса:<br>Тип доступа:<br>Привилегии:<br>[запись]][чтение]][исполнение]<br>Режим работы СЗИ: мягкий режим \| полный функционал | Mon DD hh:mm:ss hostname<br>CEF:0\|GIS\|Blockhost-Net\|3.0<br>\|BH-Access-257\| Доступ к файловому объекту \|Low\|<br>cat=Дискреционное управление доступом<br>dhost=имя хоста источника события<br>rt=дата возникновения события на клиенте<br>cs1=содержимое поля ‘Режим работы СЗИ’<br>cs1Label=Режим работы СЗИ<br>cs2=содержимое поля ‘Привилегии’<br>cs2Label=Привилегии доступа<br>cs4=содержимое поля ‘Метка пользователя’<br>cs4Label=Метка пользователя<br>cs5=содержимое поля ‘Метка объекта’<br>cs51Label=Метка объекта<br>filepath=содержимое поля ‘Имя Объекта’<br>sproc=содержимое поля ‘Имя процесса’<br>suser=содержимое поля ‘Пользователь’<br>suid=содержимое поля ‘SID пользователя’<br>externalId=257<br>categorySignificance=/Informational<br>categoryBehavior=/Access/Start<br>categoryDeviceGroup=/Identity Management<br>catdt=Access and Identity Management<br>categoryOutcome=/Success<br>categoryObject=/Host/Resource/File | Необходимо настроить аудит для пользователя или группы пользователей на какой-либо файловый ресурс (с помощью дискреционного механизма СЗИ). Далее необходимо осуществить успешную попытку доступа к этому ресурс (под успехом подразумевается успешное получение доступа с запрашиваемыми правами чтения или записи). |
| 258 (0x102) | Отказ на доступ к файловому объекту | Предупреждение | Событие: отказ на доступ к файловому объекту<br>Пользователь:<br>SID пользователя:<br>Метка пользователя:<br>Имя объекта:<br>Метка объекта:<br>Имя процесса:<br>Тип доступа:<br>Привилегии:<br>[запись]][чтение]][исполнение]<br>Режим работы СЗИ: мягкий режим \| полный функционал | Mon DD hh:mm:ss hostname<br>CEF:0\|GIS\|Blockhost-Net\|3.0<br>\|BH-Access-258\| Отказ на доступ к файловому объекту \|Medium\|<br>cat=Дискреционное управление доступом<br>dhost=имя хоста источника события<br>rt=дата возникновения события на клиенте<br>cs1=содержимое поля ‘Режим работы СЗИ’<br>cs1Label=Режим работы СЗИ<br>cs2=содержимое поля ‘Привилегии’<br>cs2Label=Привилегии доступа<br>cs3=содержимое поля ‘Тип доступа’<br>cs3Label=Тип доступа<br>cs4=содержимое поля ‘Метка пользователя’ cs4Label=Метка | Необходимо настроить аудит для пользователя или группы пользователей на какой-либо файловый ресурс (с помощью дискреционного механизма СЗИ). Далее необходимо осуществить неудачную попытку доступа к этому ресурсу (под неудачей подразумевается получение отказа доступа с запрашиваемыми правами чтения или |

| | | | | | |
|---|---|---|---|---|---|
| | | | | пользователя<br>cs5=содержимое поля ‘Метка объекта’<br>cs51Label=Метка объекта<br>filepath=содержимое поля ‘Имя Объекта’<br>sproc=содержимое поля ‘Имя процесса’<br>suser=содержимое поля ‘Пользователь’<br>suid=содержимое поля ‘SID пользователя’<br>externalId=258<br>categorySignificance=/Informational/Warning<br>categoryBehavior=/Access<br>categoryDeviceGroup=/Identity Management<br>catdt=Access and Identity Management<br>categoryOutcome=/Failure<br>categoryObject=/Host/Resource/File | записи). |

# Контроль процессов

| Код события | Тип события | Уровень важности | Формат Windows-события | CEF-формат | Условия воспроизведения |
|---|---|---|---|---|---|
| 259<br>(0x103) | Запуск процесса | Сведения | Событие: запуск процесса<br>Процесс:<br>Пользователь: domain/login<br>SID пользователя:<br>Режим работы СЗИ: мягкий режим \| полный функционал | Mon DD hh:mm:ss hostname<br>CEF:0\|GIS\|Blockhost-Net\|3.0<br>\|BH-AppControl-259\|Запуск процесса\|Low\|<br>cat=Контроль процессов<br>dhost=имя хоста источника события<br>rt=дата возникновения события на клиенте<br>cs1=содержимое поля ‘Режим работы СЗИ’<br>cs1Label=Режим работы СЗИ<br>suser=содержимое поля ‘Пользователь’<br>suid=содержимое поля ‘SID пользователя’<br>sproc=содержимое поля ‘Процесс’<br>externalId=259<br>categorySignificance=/Informational<br>categoryBehavior=/Access/Start<br>categoryDeviceGroup=/Identity Management<br>catdt=Access and Identity Management<br>categoryOutcome=/Success<br>categoryObject=/Host/Resource/File | Необходимо в механизме контроля процессов (ЗПС) настроить аудит запуска разрешенных настройками ЗПС процессов. Далее необходимо осуществить запуск процессов при входе с выполненными настройками.<br>При успешном запуске процесса в рамках ЗПС или аудита процессов должно появиться данное сообщение. |
| 260<br>(0x104) | Завершение процесса | Сведения | Событие: завершение процесса<br>Процесс:<br>Пользователь: domain/login<br>SID пользователя:<br>Режим работы СЗИ: мягкий режим \| полный функционал | Mon DD hh:mm:ss hostname<br>CEF:0\|GIS\|Blockhost-Net\|3.0<br>\|BH-AppControl-260\|Завершение процесса\|Low\|<br>cat=Контроль процессов<br>dhost=имя хоста источника события<br>rt=дата возникновения события на клиенте<br>cs1=содержимое поля ‘Режим работы СЗИ’ | Необходимо в механизме контроля процессов (ЗПС) настроить аудит запуска разрешенных процессов. Далее необходимо осуществить запуск процессов при входе с выполненными настройками. После запуска процесс |

| | | | | | |
|---|---|---|---|---|---|
| | | | | cs1Label=Режим работы СЗИ<br>suser=содержимое поля ‘Пользователь’<br>suid=содержимое поля ‘SID пользователя’<br>sproc=содержимое поля ‘Процесс’<br>externalId=260<br>categorySignificance=/Informational<br>categoryBehavior=/Access/Stop<br>categoryDeviceGroup=/Identity Management<br>catdt=Access and Identity Management<br>categoryOutcome=/Success<br>categoryObject=/Host/Resource/File | необходимо завершить. При успешном запуске процесса и последующем завершении должно появляется данное сообщение. |
| 3876<br>(0xF24) | Отказ на запуск процесса | Предупреждение | Событие: отказ за запуск процесса<br>Причина: отказ по политике замкнутой среды \| отказ по политике разрешенных процессов<br>Процесс:<br>Пользователь: domain/login<br>SID пользователя:<br>Режим работы СЗИ: мягкий режим \| полный функционал | Mon DD hh:mm:ss bhhostname<br>CEF:0\|GIS\|Blockhost-Net\|3.0<br>\|BH-AppControl-3876\|Отказ на запуск процесса \|Medium\|<br>cat=Контроль процессов<br>dhost=имя хоста источника события<br>rt=дата возникновения события на клиенте<br>cs1=содержимое поля ‘Режим работы СЗИ’<br>cs1Label=Режим работы СЗИ<br>reason=содержимое поля ‘Причина’<br>suser=содержимое поля ‘Пользователь’<br>suid=содержимое поля ‘SID пользователя’<br>sproc=содержимое поля ‘Процесс’<br>externalId=3876<br>categorySignificance=/Informational/Warning<br>categoryBehavior=/Access/Stop<br>categoryDeviceGroup=/Identity Management<br>catdt=Access and Identity Management<br>categoryOutcome=/Failure<br>categoryObject=/Host/Resource/File | Два варианта воспроизведения:<br>1. Необходимо в механизме контроля процессов (ЗПС) настроить запрет запуска процессов с галочкой «аудит». Далее необходимо осуществить попытку запуска запрещенных процессов при входе с выполненными настройками. При отказе запуске процесса появится данное сообщение.<br>2. При попытке запустить не разрешенный в рамках ЗПС процесс должно появиться данное сообщение. |

# Контроль запуска

| Код события | Тип события | Уровень важности | Формат Windows-события | CEF-формат | Условия воспроизведения |
|---|---|---|---|---|---|
| 3877<br>(0xF25) | Запуск процесса | Сведения | Событие: запуск процесса<br>Процесс:<br>Пользователь: domain/login<br>SID пользователя:<br>Режим работы СЗИ: мягкий режим \| полный функционал | Mon DD hh:mm:ss hostname<br>CEF:0\|GIS\|Blockhost-Net\|3.0<br>\|BH-AppControl-3877\|Запуск процесса\|Low\|<br>cat=Контроль запуска<br>dhost=имя хоста источника события<br>rt=дата возникновения события на клиенте<br>cs1=содержимое поля ‘Режим работы СЗИ’<br>cs1Label=Режим работы СЗИ | Выполнение запуска одного из процессов, контролируемого СЗИ. |

| | | | | | |
|---|---|---|---|---|---|
| | | | | suser=содержимое поля ‘Пользователь’<br>suid=содержимое поля ‘SID пользователя’<br>sproc=содержимое поля ‘Процесс’<br>externalId=3877<br>categorySignificance=/Informational<br>categoryBehavior=/Access/Start<br>categoryDeviceGroup=/Identity Management<br>catdt=Access and Identity Management<br>categoryOutcome=/Success<br>categoryObject=/Host/Resource/File | |
| 3878 (0xF26) | Завершение процесса | Сведения | Событие: завершение процесса<br>Процесс:<br>Пользователь: domain/login<br>SID пользователя:<br>Режим работы СЗИ: мягкий режим \| полный функционал | Mon DD hh:mm:ss hostname<br>CEF:0\|GIS\|Blockhost-Net\|3.0<br>\|BH-AppControl-3878\|Завершение процесса\|Low\|<br>cat=Контроль запуска<br>dhost=имя хоста источника события<br>rt=дата возникновения события на клиенте<br>cs1=содержимое поля ‘Режим работы СЗИ’<br>cs1Label=Режим работы СЗИ<br>suser=содержимое поля ‘Пользователь’<br>suid=содержимое поля ‘SID пользователя’<br>sproc=содержимое поля ‘Процесс’<br>externalId=3878<br>categorySignificance=/Informational<br>categoryBehavior=/Access/Stop<br>categoryDeviceGroup=/Identity Management<br>catdt=Access and Identity Management<br>categoryOutcome=/Success<br>categoryObject=/Host/Resource/File | Завершение работы одного из процессов, контролируемого СЗИ. |
| 3879 (0xF27) | Доступ к файлу | Предупреждение | Событие: доступ к файлу<br>Процесс:<br>Файл:<br>Пользователь: domain/login<br>SID пользователя:<br>Режим работы СЗИ: мягкий режим \| полный функционал | Mon DD hh:mm:ss hostname<br>CEF:0\|GIS\|Blockhost-Net\|3.0<br>\|BH-AppControl-3879\|Доступ к файлу\|Low\|<br>cat=Контроль запуска<br>dhost=имя хоста источника события<br>rt=дата возникновения события на клиенте<br>cs1=содержимое поля ‘Режим работы СЗИ’<br>cs1Label=Режим работы СЗИ<br>suser=содержимое поля ‘Пользователь’<br>suid=содержимое поля ‘SID пользователя’<br>sproc=содержимое поля ‘Процесс’<br>filename=содержимое поля Файл | Получение доступа к файлу определенного типа (аудио, видео или изображение). Аудит ведется для всех файлов типа. |

| | | | | | |
|---|---|---|---|---|---|
| | | | | externalId=3879<br>categorySignificance=/Informational<br>categoryBehavior=/Access/Start<br>categoryDeviceGroup=/Identity Management<br>catdt=Access and Identity Management<br>categoryOutcome=/Success<br>categoryObject=/Host/Resource/File | |

# Аутентификация

| Код события | Тип события | Уровень важности | Формат Windows-события | CEF-формат | Условия воспроизведения |
|---|---|---|---|---|---|
| 1029 (0x405) | Выход пользователя из системы | Сведения | Событие: выход пользователя из системы<br>Пользователь: domain/login<br>SID пользователя:<br>Мандатная метка:<br>Режим работы СЗИ: мягкий режим \| полный функционал | Mon DD hh:mm:ss hostname<br>CEF:0\|GIS\|Blockhost-Net\|3.0<br>\|BH-Auth-1029\|Выход пользователя из системы\|Low\|<br>cat=Аутентификация<br>dhost=имя хоста источника события<br>rt=дата возникновения события на клиенте<br>cs4=содержимое поля ‘Мандатная метка’<br>cs4Label=Мандатная метка<br>cs1=содержимое поля ‘Режим работы СЗИ’<br>cs1Label=Режим работы СЗИ<br>suser=содержимое поля ‘Пользователь’<br>suid=содержимое поля ‘SID пользователя’<br>externalId=1029<br>categorySignificance=/Informational<br>categoryBehavior=/Access/Stop<br>categoryDeviceGroup=/Identity Management<br>catdt=Access and Identity Management<br>categoryOutcome=/Success<br>categoryObject=/Host/Operating System | Выход пользователя из ОС (завершение сеанса пользователя). |
| 3880 (0xF28 | Локальный вход в систему | Сведения | Событие: локальный вход в систему<br>Пользователь: domain/login<br>SID пользователя:<br>Мандатная метка:<br>Тип аутентификации: по токену \| аутентификация Windows \| по паролю (механизм Блокхост-Сеть)<br>Идентификатор токена: [идентификатор токена]<br>Режим работы СЗИ: мягкий режим \| полный функционал | Mon DD hh:mm:ss hostname<br>CEF:0\|GIS\|Blockhost-Net\|3.0<br>\|BH-Auth-3880\|Локальный вход в систему\|Low\|<br>cat=Аутентификация<br>dhost=имя хоста источника события<br>rt=дата возникновения события на клиенте<br>cs4=содержимое поля ‘Мандатная метка’<br>cs4Label=Мандатная метка | Успешный интерактивный вход пользователя в ОС.<br><br>Поле ‘Идентификатор токена’ имеет значение только в случае, если вход выполняется по токену. |

| | | | | | |
|---|---|---|---|---|---|
| | | | | cs1=содержимое поля ‘Режим работы СЗИ’<br>cs1Label=Режим работы СЗИ<br>cs2= содержимое поля ‘Тип аутентификации’<br>cs2Label=Тип аутентификации<br>cs3=содержимое поля ‘Идентификатор токена’<br>cs3Label=Идентификатор токена<br>suser=содержимое поля ‘Пользователь’<br>suid=содержимое поля ‘SID пользователя’<br>externalId=3880<br>categorySignificance=/Informational<br>categoryBehavior=/Access/Start<br>categoryDeviceGroup=/Identity Management<br>catdt=Access and Identity Management<br>categoryOutcome=/Success<br>categoryObject=/Host/Operating System | |
| 3881 (0xF29) | Отказ на локальный вход в систему | Предупреждение | Событие: отказ на локальный вход в систему<br>Причина: пароль не соответствует политике аутентификации СЗИ \| <другие причины><br>Пользователь: domain/login<br>SID пользователя:<br>Мандатная метка:<br>Тип аутентификации: по токену \| аутентификация Windows \| по паролю (механизм Блокхост-Сеть)<br>Идентификатор токена: [идентификатор токена]<br>Режим работы СЗИ: мягкий режим \| полный функционал | Mon DD hh:mm:ss hostname<br>CEF:0\|GIS\|Blockhost-Net\|3.0<br>\|BH-Auth-3881\|Отказ на локальный вход в систему\|Medium\|<br>cat=Аутентификация<br>dhost=имя хоста источника события<br>rt=дата возникновения события на клиенте<br>cs4=содержимое поля ‘Мандатная метка’<br>cs4Label=Мандатная метка<br>cs1=содержимое поля ‘Режим работы СЗИ’<br>cs1Label=Режим работы СЗИ<br>cs2= содержимое поля ‘Тип аутентификации’<br>cs2Label=Тип аутентификации<br>cs3=содержимое поля ‘Идентификатор’<br>токена cs3Label=Идентификатор токена<br>reason=содержимое поля ‘Причина’<br>suser=содержимое поля ‘Пользователь’<br>suid=содержимое поля ‘SID пользователя’<br>externalId=3881<br>categorySignificance=/Informational/Warning<br>categoryBehavior=/Authorization/Verify<br>categoryDeviceGroup=/Identity Management<br>catdt=Access and Identity Management<br>categoryOutcome=/Failure<br>categoryObject=/Host/Operating System | Блокировка интерактивного входа пользователя в ОС по следующим причинам:<br>• неправильный пароль, токен или пинкод;<br>• несоответствие политикам ОС или БХС;<br>• отсутствие пользователя или его группы в консоли БХС;<br>• блокировка пользователя администратором.<br><br>Поле ‘Идентификатор токена’ имеет значение только в случае, если вход выполняется по токену. |

| | | | | | |
|---|---|---|---|---|---|
| 3888 (0xF30) | Вход в систему по RDP | Сведения | Событие: вход в систему по RDP<br>Пользователь: domain/login<br>SID пользователя:<br>Мандатная метка:<br>Тип аутентификации: по токену \| аутентификация Windows \| по паролю (механизм Блокхост-Сеть)<br>Идентификатор токена: [идентификатор токена]<br>Режим работы СЗИ: мягкий режим \| полный функционал | Mon DD hh:mm:ss hostname<br>CEF:0\|GIS\|Blockhost-Net\|3.0<br>\|BH-Auth-3888\|Вход в систему по RDP\|Low\|<br>cat=Аутентификация<br>dhost=имя хоста источника события<br>rt=дата возникновения события на клиенте<br>cs4=содержимое поля Мандатная метка<br>cs4Label=Мандатная метка<br>cs1=содержимое поля ‘Режим работы СЗИ’<br>cs1Label=Режим работы СЗИ<br>cs2= содержимое поля ‘Тип аутентификации’<br>cs2Label=Тип аутентификации<br>cs3=содержимое поля ‘Идентификатор’ токена cs3Label=Идентификатор токена<br>suser=содержимое поля ‘Пользователь’<br>suid=содержимое поля ‘SID пользователя’<br>externalId=3888<br>categorySignificance=/Informational<br>categoryBehavior=/Access/Start<br>categoryDeviceGroup=/Identity Management<br>catdt=Access and Identity Management<br>categoryOutcome=/Success<br>categoryObject=/Host/Operating System | Успешный вход пользователя в систему с помощью RDP-сессии. Поле ‘Идентификатор токена’ имеет значение только в случае, если вход выполняется по токену. |
| 3889 (0xF31) | Отказ на вход в систему по RDP | Предупреждение | Событие: отказ на вход в систему по RDP<br>Причина: пароль не соответствует политике аутентификации СЗИ \| <другие причины><br>Пользователь: domain/login<br>SID пользователя:<br>Мандатная метка:<br>Тип аутентификации: по токену \| аутентификация Windows \| по паролю (механизм Блокхост-Сеть)<br>Идентификатор токена: [идентификатор токена]<br>Режим работы СЗИ: мягкий режим \| полный функционал | Mon DD hh:mm:ss hostname<br>CEF:0\|GIS\|Blockhost-Net\|3.0<br>\|BH-Auth-3889\|Отказ на вход в систему по RDP\|Medium\|<br>cat=Аутентификация<br>dhost=имя хоста источника события<br>rt=дата возникновения события на клиенте<br>cs4=содержимое поля ‘Мандатная метка’<br>cs4Label=Мандатная метка<br>cs1=содержимое поля ‘Режим работы СЗИ’ cs1Label=Режим работы СЗИ<br>cs2= содержимое поля ‘Тип аутентификации’<br>cs2Label=Тип аутентификации<br>cs3=содержимое поля ‘Идентификатор токена‘<br>cs3Label=Идентификатор токена | Блокировка входа пользователя в ОС по RDP по любой из следующих причин:<br>• неправильный пароль, токен или пинкод;<br>• несоответствие политикам ОС или БХС;<br>• отсутствие пользователя или его группы в консоли БХС;<br>• блокировка пользователя администратором.<br><br>Поле ‘Идентификатор токена’ имеет значение только в случае, если вход выполняется по токену. |

| | | | | | |
|---|---|---|---|---|---|
| | | | | reason=значение из поля ‘Причина’<br>suser=значение из поля ‘Пользователь’<br>suid=значение из поля ‘SID пользователя’<br>externalId=3889<br>categorySignificance=/Informational/Warning<br>categoryBehavior=/Authentication/Verify<br>categoryDeviceGroup=/Identity Management<br>catdt=Access and Identity Management<br>categoryOutcome=/Failure<br>categoryObject=/Host/Operating System | |
| 3890<br>(0xF32) | Доступ к ресурсу с совместным доступом по сети | Сведения | Событие: доступ к ресурсу с совместным доступом по сети<br>Пользователь: domain/login<br>SID пользователя:<br>Мандатная метка:<br>Режим работы СЗИ: мягкий режим \| полный функционал | Mon DD hh:mm:ss hostname<br>CEF:0\|GIS\|Blockhost-Net\|3.0<br>\|BH-Auth-3890\|Доступ к ресурсу с совместным доступом по сети\|Low\|<br>cat=Аутентификация<br>dhost=имя хоста источника события<br>rt=дата возникновения события на клиенте<br>cs4=содержимое поля ‘Мандатная метка’<br>cs4Label=Мандатная метка<br>cs1=содержимое поля ‘Режим работы СЗИ’<br>cs1Label=Режим работы СЗИ<br>suser=содержимое поля ‘Пользователь’<br>suid=содержимое поля ‘SID пользователя’<br>externalId=3890<br>categorySignificance=/Informational<br>categoryBehavior=/Access<br>categoryDeviceGroup=/Identity Management<br>catdt=Access and Identity Management<br>categoryOutcome=/Success<br>categoryObject=/Host/Operating System | Доступ к ресурсам с совместным доступом (принтеры, сканеры и т.д.) по сети с других узлов сети. Событие формируется на узле, на котором находится ресурс общего доступа. |
| 3891<br>(0xF33) | Отказ на доступ к ресурсу с совместным доступом по сети | Предупреждение | Событие: отказ на доступ к ресурсу с совместным доступом по сети<br>Причина: пароль не соответствует политике аутентификации СЗИ \| <другие причины><br>Пользователь: domain/login<br>SID пользователя:<br>Мандатная метка:<br>Режим работы СЗИ: мягкий режим \| полный функционал | Mon DD hh:mm:ss hostname<br>CEF:0\|GIS\|Blockhost-Net\|3.0<br>\|BH-Auth-3891\| Отказ на доступ к ресурсу с совместным доступом по сети\|Medium\|<br>cat=Аутентификация<br>dhost=имя хоста источника события<br>rt=дата возникновения события на клиенте<br>cs4=содержимое поля ‘Мандатная метка’<br>cs4Label=Мандатная метка<br>cs1=содержимое поля ‘Режим работы СЗИ’ cs1Label=Режим работы СЗИ<br>reason=содержимое поля ‘Причина’ | Отказ на доступ к ресурсам с совместным доступом (принтеры, сканеры и т.д.) по сети с других узлов сети. Событие формируется на узле, на котором находится ресурс общего доступа. |

| | | | | | |
|---|---|---|---|---|---|
| | | | | suser=содержимое поля ‘Пользователь’<br>suid=содержимое поля ‘SID пользователя’<br>externalId=3891<br>categorySignificance=/Informational/Warning<br>categoryBehavior=/Authentication/Verify<br>categoryDeviceGroup=/Identity Management<br>catdt=Access and Identity Management<br>categoryOutcome=/Failure<br>categoryObject=/Host/Operating System | |
| 3892<br>(0xF34) | Аутентификация через RunAs или открытие сессии | Сведения | Событие: аутентификация через RunAs<br>Пользователь: domain/login<br>SID пользователя:<br>Мандатная метка:<br>Режим работы СЗИ: мягкий режим \| полный функционал | Mon DD hh:mm:ss hostname<br>CEF:0\|GIS\|Blockhost-Net\|3.0<br>\|BH-Auth-3892\|Аутентификация через RunAs или открытие сессии\|Low\|<br>cat=Аутентификация<br>dhost=имя хоста источника события<br>rt=дата возникновения события на клиенте<br>cs4=содержимое поля ‘Мандатная метка’<br>cs4Label=’Мандатная метка’<br>cs1=содержимое поля ‘Режим работы СЗИ’ cs1Label=Режим работы СЗИ<br>suser=содержимое поля ‘Пользователь’<br>suid=содержимое поля ‘SID пользователя’<br>externalId=3892<br>categorySignificance=/Informational<br>categoryBehavior=/Access/Start<br>categoryDeviceGroup=/Identity Management<br>catdt=Access and Identity Management<br>categoryOutcome=/Success<br>categoryObject=/Host/Operating System | Успешный запуск приложения от имени другого пользователя («Запуск от имени…»). |
| 3893<br>(0xF35) | Отказ на аутентификацию через RunAs или открытие сессии | Предупреждение | Событие: отказ на аутентификацию через RunAs<br>Причина:<br>Пользователь: domain/login<br>SID пользователя:<br>Мандатная метка:<br>Режим работы СЗИ: мягкий режим \| полный функционал | Mon DD hh:mm:ss hostname<br>CEF:0\|GIS\|Blockhost-Net\|3.0<br>\|BH-Auth-3893\|Отказ на аутентификацию через RunAs или открытие сессии\|Medium\|<br>cat=Аутентификация<br>dhost=имя хоста источника события<br>rt=дата возникновения события на клиенте<br>cs4=содержимое поля ‘Мандатная метка’<br>cs4Label=Мандатная метка<br>cs1=содержимое поля ‘Режим работы СЗИ’<br>cs1Label=Режим работы СЗИ | Отказ на запуск приложения от имени другого пользователя («Запуск от имени…»). |

| | | | | | |
|---|---|---|---|---|---|
| | | | | suser=содержимое поля ‘Пользователь’<br>suid=содержимое поля SID пользователя<br>externalId=3893<br>categorySignificance=/Informational/Warning<br>categoryBehavior=/Authentication/Verify<br>categoryDeviceGroup=/Identity Management<br>catdt=Access and Identity Management<br>categoryOutcome=/Failure<br>categoryObject=/Host/Operating System | |
| 3894<br>(0xF36) | Пользователь приостановил сеанс работы на компьютере | Сведения | Событие: пользователь приостановил сеанс работы на компьютере<br>Пользователь: domain/login<br>SID пользователя:<br>Мандатная метка:<br>Режим работы СЗИ: мягкий режим \| полный функционал | Mon DD hh:mm:ss hostname<br>CEF:0\|GIS\|Blockhost-Net\|3.0<br>\|BH-Auth-3894\|Пользователь приостановил сеанс работы на компьютере\|Low\|<br>cat=Аутентификация<br>dhost=имя хоста источника события<br>rt=дата возникновения события на клиенте<br>cs4=содержимое поля ‘Мандатная метка’<br>cs4Label=Мандатная метка<br>cs1=содержимое поля ‘Режим работы СЗИ’<br>cs1Label=Режим работы СЗИ<br>suser=содержимое поля ‘Пользователь’<br>suid=содержимое поля ‘SID пользователя’<br>externalId=3894<br>categorySignificance=/Informational<br>categoryBehavior=/Access/Stop<br>categoryDeviceGroup=/Identity Management<br>catdt=Access and Identity Management<br>categoryOutcome=/Success<br>categoryObject=/Host/Operating System | Блокировка сессии пользователя по требованию пользователя или средствами СЗИ. |
| 3895<br>(0xF37) | Пользователь возобновил сеанс работы на компьютере | Сведения | Событие: пользователь возобновил сеанс работы на компьютере<br>Пользователь: domain/login<br>SID пользователя:<br>Мандатная метка:<br>Тип аутентификации: по токену \| аутентификация Windows \| по паролю (механизм Блокхост-Сеть)<br>Идентификатор токена: [идентификатор токена]<br>Режим работы СЗИ: мягкий режим \| полный функционал | Mon DD hh:mm:ss hostname<br>CEF:0\|GIS\|Blockhost-Net\|3.0<br>\|BH-Auth-3895\|Пользователь возобновил сеанс работы на компьютере\|Low\|<br>cat=Аутентификация<br>dhost=имя хоста источника события<br>rt=дата возникновения события на клиенте<br>cs4=содержимое поля ‘Мандатная метка’<br>cs4Label=Мандатная метка<br>cs1=содержимое поля ‘Режим работы СЗИ’ | Возобновление заблокированной сессии пользователя.<br><br>Поле ‘Идентификатор токена’ имеет значение только в случае, если вход выполняется по токену. |

| | | | | | |
|---|---|---|---|---|---|
| | | | | cs1Label=Режим работы СЗИ<br>cs2=содержимое поля ‘Тип аутентификации’<br>cs2Label=Тип аутентификации<br>cs3=содержимое поля ‘Идентификатор токена’<br>cs3Label=Идентификатор токена<br>suser=содержимое поля ‘Пользователь’<br>suid=содержимое поля ‘SID пользователя’<br>externalId=3895<br>categorySignificance=/Informational/Warning<br>categoryBehavior=/Access/Start<br>categoryDeviceGroup=/Identity Management<br>catdt=Access and Identity Management<br>categoryOutcome=/Success | |
| 3896<br>(0xF38) | Отказ возобновления сеанса работы пользователем | Ошибка | Событие: отказ возобновления сеанса работы пользователем<br>Причина: пароль не соответствует требованиям безопасности \| <другие причины><br>Пользователь: domain/login<br>SID пользователя:<br>Мандатная метка:<br>Тип аутентификации: по токену \| аутентификация Windows \| по паролю (механизм Блокхост-Сеть)<br>Идентификатор токена: [идентификатор токена]<br>Режим работы СЗИ: мягкий режим \| полный функционал | Mon DD hh:mm:ss  hostname<br>CEF:0\|GIS\|Blockhost-Net\|3.0<br>\|BH-Auth-3896\|Отказ возобновления сеанса работы пользователя \|High\|<br>cat=Аутентификация<br>dhost=имя хоста источника события<br>rt=дата возникновения события на клиенте<br>cs4=содержимое поля ‘Мандатная метка’<br>cs4Label=Мандатная метка<br>cs1=содержимое поля ‘Режим работы СЗИ’<br>cs1Label=Режим работы СЗИ<br>cs2=содержимое поля ‘Тип аутентификации’<br>cs2Label=Тип аутентификации<br>cs3=содержимое поля ‘Идентификатор токена’<br>cs3Label=Идентификатор токена<br>reason=содержимое поля ‘Причина’<br>suser=содержимое поля ‘Пользователь’<br>suid=содержимое поля ‘SID пользователя’<br>externalId=3896<br>categorySignificance=/Informational/Error<br>categoryBehavior=/Authorization/Verify<br>categoryDeviceGroup=/Identity Management<br>catdt=Access and Identity Management<br>categoryOutcome=/Failure<br>categoryObject=/Host/Operating System | Отказ в возобновлении заблокированной сессии пользователя.<br>Возможные причины отказа:<br>• пароль/пинкод токена не отвечают требованием политики СЗИ;<br>• пароль/пинкод токена некорректен, пользователь предоставил неверный токен;<br>• пользователь не предоставил токен.<br><br>Поле ‘Идентификатор токена’ имеет значение только в случае, если вход выполняется по токену. |
| 3897 | Смена пароля | Сведения | Событие: смена пароля пользователя | Mon DD hh:mm:ss  hostname | Смена пароля |

| | | | | | |
|---|---|---|---|---|---|
| (0xF39) | пользователя | | Пользователь: domain/login<br>SID пользователя:<br>Тип аутентификации: по токену \| аутентификация Windows \| по паролю (механизм Блокхост-Сеть)<br>Идентификатор токена: [идентификатор токена]<br>Режим работы СЗИ: мягкий режим \| полный функционал | CEF:0\|GIS\|Blockhost-Net\|3.0 \|BH-Auth-3897\|Смена пароля пользователя\|Low\| cat=Аутентификация dhost=имя хоста источника события rt=дата возникновения события на клиенте cs1=содержимое поля ‘Режим работы СЗИ’ cs1Label=Режим работы СЗИ suser=содержимое поля ‘Пользователь’ suid=содержимое поля ‘SID пользователя’ externalId=3897 categorySignificance=/Informational categoryBehavior=/Authentication/Modify categoryDeviceGroup=/Identity Management catdt=Access and Identity Management categoryOutcome=/Success categoryObject=/Host/Operating System | пользователя на клиентском компьютере. Смена пароля может быть выполнена в следующих случаях:<br>• при входе пользователя в ОС;<br>• по требованию пользователя (ctrl+alt+del) ;<br>• администратором СЗИ через клиентскую или серверную консоль СЗИ. |
| 3904 (0xF40) | Отказ при смене пароля пользователя | Ошибка | Событие: отказ при смене пароля пользователя<br>Причина: пароль не соответствует политике аутентификации СЗИ \| <другие причины><br>Пользователь: domain/login<br>SID пользователя:<br>Тип аутентификации: по токену \| аутентификация Windows \| по паролю (механизм Блокхост-Сеть)<br>Идентификатор токена: [идентификатор токена]<br>Режим работы СЗИ: мягкий режим \| полный функционал | Mon DD hh:mm:ss hostname CEF:0\|GIS\|Blockhost-Net\|3.0 \|BH-Auth-3904\|Отказ при смене пароля пользователем \|High\| cat=Аутентификация dhost=имя хоста источника события rt=дата возникновения события на клиенте cs1=содержимое поля ‘Режим работы СЗИ’ cs1Label=Режим работы СЗИ cs2=содержимое поля ‘Тип аутентификации’ cs2Label=Тип аутентификации cs3=содержимое поля ‘Идентификатор токена’ cs3Label=Идентификатор токена reason=содержимое поля ‘Причина’ suser=содержимое поля ‘Пользователь’ suid=содержимое поля ‘SID пользователя’ externalId=3904 categorySignificance=/Informational/Error categoryBehavior=/Authentication/Modify categoryDeviceGroup=/Identity Management catdt=Access and Identity Management categoryOutcome=/Failure categoryObject=/Host/Operating System | Отказ на смену пароля пользователя на клиентском компьютере. Смена пароля может быть выполнена в следующих случаях:<br>• при входе пользователя в ОС;<br>• по требованию пользователя (ctrl+alt+del) ;<br>• администратором СЗИ через клиентскую или серверную консоль СЗИ. |

| | | | | | |
|---|---|---|---|---|---|
| 3905 (0xF41) | Смена пин-кода токена | Сведения | Событие: смена пин-кода токена<br>Пользователь: domain/login<br>Идентификатор токена:<br>Режим работы СЗИ: мягкий режим \| полный функционал | Mon DD hh:mm:ss hostname<br>CEF:0\|GIS\|Blockhost-Net\|3.0<br>\|BH-Auth-3905\|Смена пин-кода токена\|Low\|<br>cat=Аутентификация<br>dhost=имя хоста источника события<br>rt=дата возникновения события на клиенте<br>cs1=содержимое поля ‘Режим работы СЗИ’<br>cs1Label=Режим работы СЗИ<br>cs3=содержимое поля ‘Идентификатор токена‘<br>cs3Label=Идентификатор токена<br>suser=содержимое поля ‘Пользователь’<br>externalId=3905<br>categorySignificance=/Informational<br>categoryBehavior=/Authentication/Modify<br>categoryDeviceGroup=/Identity Management<br>catdt=Access and Identity Management<br>categoryOutcome=/Success<br>categoryObject==/Host/Resource | Смена пин-кода токена на клиентском компьютере. Смена пароля может быть выполнена в следующих случаях:<br>• при входе пользователя в ОС;<br>• по требованию пользователя (ctrl+alt+del) ;<br>• администратором СЗИ через клиентскую или серверную консоль СЗИ. |
| 3906 (0xF42) | Отказ при смене пин-кода токена | Ошибка | Событие: отказ при смене пин-кода токена<br>Причина:<br>Пользователь: domain/login<br>Идентификатор токена:<br>Режим работы СЗИ: мягкий режим \| полный функционал | Mon DD hh:mm:ss hostname<br>CEF:0\|GIS\|Blockhost-Net\|3.0<br>\|BH-Auth-3906\|Отказ при смена пин-кода токена\|High\|<br>cat=Аутентификация<br>dhost=имя хоста источника события<br>rt=дата возникновения события на клиенте<br>cs1=содержимое поля ‘Режим работы СЗИ’<br>cs1Label=Режим работы СЗИ<br>cs3=содержимое поля ‘Идентификатор токена‘<br>cs3Label=Идентификатор токена<br>reason=значение из поля ‘Причина’<br>suser=значение из поля ‘Пользователь’<br>suid=значение из поля ‘SID пользователя’<br>externalId=3906<br>categorySignificance=/Informational/Error<br>categoryBehavior=/Authentication/Modify<br>categoryDeviceGroup=/Identity Management<br>catdt=Access and Identity Management | Отказ на смену пин-кода токена на клиентском компьютере. Смена пароля может быть выполнена в следующих случаях:<br>• при входе пользователя в ОС;<br>• по требованию пользователя (ctrl+alt+del) ;<br>• администратором СЗИ через клиентскую или серверную консоль СЗИ. |

| | | | | | |
|---|---|---|---|---|---|
| | | | | categoryOutcome=/Failure<br>categoryObject==/Host/Resource | |

# Контроль портов

| Код события | Тип события | Уровень важности | Формат Windows-события | CEF-формат | Условия воспроизведения |
|---|---|---|---|---|---|
| 1028 (0x404) | Предоставление доступа к USB устройству | Сведения | Событие: предоставление доступа к USB устройству<br>Пользователь: domain/login<br>SID пользователя:<br>Имя порта:<br>Режим работы СЗИ: мягкий режим \| полный функционал | Mon DD hh:mm:ss hostname<br>CEF:0\|GIS\|Blockhost-Net\|3.0<br>\|BH-PortControl-1028\|Предоставление доступа к USB устройству\|Low\|<br>cat=Контроль портов<br>dhost=имя хоста источника события<br>rt=дата возникновения события на клиенте<br>cs1=содержимое поля ‘Режим работы СЗИ’<br>cs1Label=Режим работы СЗИ<br>cs2=содержимое поля ‘Имя порта’<br>cs2Label=Имя порта<br>suser=содержимое поля ‘Пользователь’<br>suid=содержимое поля ‘SID пользователя’<br>externalId=1028<br>categorySignificance=/Informational<br>categoryBehavior=/Access/Start<br>categoryDeviceGroup=/Identity Management<br>catdt=Access and Identity Management<br>categoryOutcome=/Success<br>categoryObject=/Host/Resource | Выдача разрешения пользователю на использование USB-устройства.<br>Событие может формироваться в следующих случаях:<br>• вход пользователя в ОС (создание сессии пользователя) ;<br>• подключение USB-устройства пользователем, ранее осуществившим вход в ОС. |
| 1027 (0x403) | Отказ в предоставлении доступа к USB устройству | Предупреждение | Событие: отказ в предоставлении доступа к USB устройству<br>Пользователь: domain/login<br>SID пользователя:<br>Имя порта:<br>Режим работы СЗИ: мягкий режим \| полный функционал | Mon DD hh:mm:ss hostname<br>CEF:0\|GIS\|Blockhost-Net\|3.0<br>\|BH-PortControl-1027\|Отказ в предоставлении доступа к USB устройству \|Medium\|<br>cat=Контроль портов<br>dhost=имя хоста источника события<br>rt=дата возникновения события на клиенте<br>cs1=содержимое поля ‘Режим работы СЗИ’<br>cs1Label=Режим работы СЗИ<br>cs2=содержимое поля ‘Имя порта’<br>cs2Label=Имя порта<br>suser=содержимое поля ‘Пользователь’<br>suid=содержимое поля ‘SID пользователя’<br>externalId=1027<br>categorySignificance=/Informational/Warning<br>categoryBehavior=/Access | Отказ на выдачу разрешения (запрет) пользователю на использование USB-устройства.<br>Событие может формироваться в следующих случаях:<br>• вход пользователя в ОС (создание сессии пользователя) ;<br>• подключение USB-устройства пользователем, ранее осуществившим вход в ОС. |

| | | | | | |
|---|---|---|---|---|---|
| | | | | categoryDeviceGroup=/Identity Management<br>catdt=Access and Identity Management<br>categoryOutcome=/Failure<br>categoryObject=/Host/Resource | |
| 1030<br>(0x406) | USB устройство извлечено | Сведения | Событие: USB устройство извлечено<br>Пользователь: domain/login<br>SID пользователя:<br>Имя порта:<br>Режим работы СЗИ: мягкий режим \| полный функционал | Mon DD hh:mm:ss hostname<br>CEF:0\|GIS\|Blockhost-Net\|3.0<br>\|BH-PortControl-1030\|USB устройство извлечено \|Low\|<br>cat=Контроль портов<br>dhost=имя хоста источника события<br>rt=дата возникновения события на клиенте<br>cs1=содержимое поля ‘Режим работы СЗИ’<br>cs1Label=Режим работы СЗИ<br>cs2=содержимое поля ‘Имя порта’<br>cs2Label=Имя порта<br>suser=содержимое поля ‘Пользователь’<br>suid=содержимое поля ‘SID пользователя’<br>externalId=1030<br>categorySignificance=/Informational<br>categoryBehavior=/Access/Stop<br>categoryDeviceGroup=/Identity Management<br>catdt=Access and Identity Management<br>categoryOutcome=/Success<br>categoryObject=/Host/Resource | Физическое отключение разрешенного для использования устройства в процессе работы пользователя |
| 1031<br>(0x407) | Предоставление доступа к устройству (COM, LPT, CDROM) | Сведения | Событие: предоставление доступа к устройству (COM, LPT, CDROM)<br>Пользователь: domain/login<br>SID пользователя:<br>Имя порта:<br>Режим работы СЗИ: мягкий режим \| полный функционал | Mon DD hh:mm:ss hostname<br>CEF:0\|GIS\|Blockhost-Net\|3.0<br>\|BH-PortControl-1031\| Предоставление доступа к устройству (COM, LPT, CDROM)\|Low\|<br>cat=Контроль портов<br>dhost=имя хоста источника события<br>rt=дата возникновения события на клиенте<br>cs1=содержимое поля ‘Режим работы СЗИ’<br>cs1Label=Режим работы СЗИ<br>cs2=содержимое поля ‘Имя порта’<br>cs2Label=Имя порта<br>suser=содержимое поля ‘Пользователь’<br>suid=содержимое поля ‘SID пользователя’<br>externalId=1031<br>categorySignificance=/Informational<br>categoryBehavior=/Access/Start<br>categoryDeviceGroup=/Identity Management<br>catdt=Access and Identity Management<br>categoryOutcome=/Success<br>categoryObject=/Host/Resource | Выдача разрешения пользователю на использование COM, LPT – устройств, либо CDROM.<br>Событие может формироваться в следующих случаях:<br>• вход пользователя в ОС (создание сессии пользователя) ;<br>• подключение устройства пользователем, ранее осуществившим вход в ОС. |

| | | | | | |
|---|---|---|---|---|---|
| 1032 (0x408) | Отказ в предоставлении доступа к устройству (COM, LPT, CDROM) | Сведения | Событие: отказ в предоставлении доступа к устройству (COM, LPT, CDROM)<br>Пользователь: domain/login<br>SID пользователя:<br>Имя порта:<br>Режим работы СЗИ: мягкий режим \| полный функционал | Mon DD hh:mm:ss bhhostname<br>CEF:0\|GIS\|Blockhost-Net\|3.0<br>\|BH-PortControl-1032\|Отказ в предоставлении доступа к устройству (COM, LPT, CDROM)\|Low\|<br>cat=Контроль портов<br>dhost=имя хоста источника события<br>rt=дата возникновения события на клиенте<br>cs1=содержимое поля ‘Режим работы СЗИ’<br>cs1Label=Режим работы СЗИ<br>cs2=содержимое поля ‘Имя порта’<br>cs2Label=Имя порта<br>suser=содержимое поля ‘Пользователь’<br>suid=содержимое поля ‘SID пользователя’<br>externalId=1032<br>categorySignificance=/Informational<br>categoryBehavior=/Access<br>categoryDeviceGroup=/Identity Management<br>catdt=Access and Identity Management<br>categoryOutcome=/Failure<br>categoryObject=/Host/Resource | Отказ на выдачу разрешения (запрет) пользователю на использование COM, LPT – устройств, либо CDROM.<br>Событие может формироваться в следующих случаях:<br>• вход пользователя в ОС (создание сессии пользователя) ;<br>• подключение устройства пользователем, ранее осуществившим вход в ОС. |

# Очистка остаточной информации

| Код события | Тип события | Уровень важности | Формат Windows-события | CEF-формат | Условия воспроизведения |
|---|---|---|---|---|---|
| 1537 (0x601) | Очистка памяти процесса | Сведения | Событие: очистка памяти процесса<br>Имя процесса:<br>Режим работы СЗИ: мягкий режим \| полный функционал | Mon DD hh:mm:ss hostname<br>CEF:0\|GIS\|Blockhost-Net\|3.0<br>\|BH-InformClean-1537\|Очистка памяти процесса\|Low\|<br>cat=очистка остаточной информации<br>dhost=имя хоста источника события<br>rt=дата возникновения события на клиенте<br>cs1=содержимое поля ‘Режим работы СЗИ’<br>cs1Label=Режим работы СЗИ<br>sproc=содержимое поля ‘Имя процесса’<br>externalId=1537<br>categorySignificance=/Informational<br>categoryBehavior=/Delete<br>categoryDeviceGroup=/Data Security<br>catdt=Access and Identity Management<br>categoryOutcome=/Success<br>categoryObject=/Host/Application | Очистка памяти процесса после завершения работы процесса, указанного в перечне обрабатываемых файлов подсистемы очистки остаточной информации. |
| 769 | Гарантированное | Сведения | Событие: гарантированное удаление | Mon DD hh:mm:ss hostname | Выполнение |

| | | | | | |
|---|---|---|---|---|---|
| (0x301) | удаление файлового объекта | | файлового объекта<br>Пользователь: domain/login<br>SID пользователя:<br>Имя объекта:<br>Режим работы СЗИ: мягкий режим \| полный функционал | CEF:0\|GIS\|Blockhost-Net\|3.0 \|BH-InformClean-769\|гарантированное удаление файлового объекта\|Low\| cat=очистка остаточной информации dhost=имя хоста источника события rt=дата возникновения события на клиенте cs1=содержимое поля ‘Режим работы СЗИ’ cs1Label=Режим работы СЗИ filepath=содержимое поля ‘Имя Объекта’ suser=содержимое поля ‘Пользователь’ suid=содержимое поля ‘SID пользователя’ externalId=769 categorySignificance=/Informational categoryBehavior=/Delete categoryDeviceGroup=/Data Security catdt=Access and Identity Management categoryOutcome=/Success categoryObject=/Host/File | гарантированного удаления файлового объекта с диска. |
| 771 (0x303) | Невозможно завершить операцию гарантированного удаления | Ошибка | Событие: невозможно завершить операцию гарантированного удаления<br>Пользователь: domain/login<br>SID пользователя:<br>Имя объекта:<br>Режим работы СЗИ: мягкий режим \| полный функционал | Mon DD hh:mm:ss hostname CEF:0\|GIS\|Blockhost-Net\|3.0 \|BH-InformClean-771\|Невозможно завершить операцию гарантированного удаления\|High\| cat=очистка остаточной информации dhost=имя хоста источника события rt=дата возникновения события на клиенте cs1=содержимое поля ‘Режим работы СЗИ’ cs1Label=Режим работы СЗИ filepath=содержимое поля ‘Имя Объекта’ suser=содержимое поля ‘Пользователь’ suid=содержимое поля ‘SID пользователя’ externalId=771 categorySignificance=/Informational/Error categoryBehavior=/Delete categoryDeviceGroup=/Data Security catdt=Access and Identity Management categoryOutcome=/Failure categoryObject=/Host/File | Выполнение гарантированного удаления файлового объекта с диска не было выполнено из-за возникшей ошибки. |

# Контроль целостности файлов

| Код события | Тип события | Уровень важности | Формат Windows-события | CEF-формат | Условия воспроизведения |
|---|---|---|---|---|---|
| 3968 (0xF80) | Нарушена целостность файла | Предупреждение | Событие: нарушена целостность файла<br>Имя файла:<br>Путь:<br>Режим работы СЗИ: мягкий режим \| полный функционал | Mon DD hh:mm:ss hostname CEF:0\|GIS\|Blockhost-Net\|3.0 \|BH-IntegrityControl-3968\|Нарушена целостность файла\|Medium\| cat=контроль целостности файлов dhost=имя хоста источника события rt=дата возникновения события на клиенте cs1=содержимое поля ‘Режим работы СЗИ’ cs1Label=Режим работы СЗИ filepath=содержимое поля ‘Путь’ filename=содержимое поля ‘Имя файла’ externalId=3968 categorySignificance=/Informational/Warning categoryBehavior=/Modify categoryDeviceGroup=/Data Security catdt=Access and Identity Management categoryOutcome=/Attempt categoryObject=/Host/File | Обнаружено нарушение целостности файлового объекта. |
| 3969 (0xF81) | Файл восстановлен из резервной копии | Предупреждение | Событие: файл восстановлен из резервной копии<br>Имя файла:<br>Путь:<br>Режим работы СЗИ: мягкий режим \| полный функционал | Mon DD hh:mm:ss hostname CEF:0\|GIS\|Blockhost-Net\|3.0 \|BH-IntegrityControl-3969\|Файл восстановлен из резервной копии\|Medium\| cat=контроль целостности файлов dhost=имя хоста источника события rt=дата возникновения события на клиенте cs1=содержимое поля ‘Режим работы СЗИ’ cs1Label=Режим работы СЗИ filepath=содержимое поля ‘Путь’ filename=содержимое поля ‘Имя файла’ externalId=3969 categorySignificance=/Informational/Warning categoryBehavior=/Modify categoryDeviceGroup=/Data Security catdt=Access and Identity Management categoryOutcome=/Success categoryObject=/Host/File | Выполнено восстановление измененного файла из резервной копии. |
| 3970 (0xF82) | Не удалось восстановить файл из резервной копии | Ошибка | Событие: не удалось восстановить файл из резервной копии<br>Причина: нет доступа к файлу | Mon DD hh:mm:ss hostname CEF:0\|GIS\|Blockhost-Net\|3.0 \|BH-IntegrityControl-3970\|Не удалось | В процессе восстановления файла из резервной копии |

| | | | | | |
|---|---|---|---|---|---|
| | | | Имя файла:<br>Путь:<br>Режим работы СЗИ: мягкий режим \| полный функционал | восстановить файл из резервной копии\|High\|<br>cat=контроль целостности файлов<br>dhost=имя хоста источника события<br>rt=дата возникновения события на клиенте<br>cs1=содержимое поля ‘Режим работы СЗИ’<br>cs1Label=Режим работы СЗИ<br>filepath=содержимое поля ‘Путь’<br>filename=содержимое поля ‘Имя файла’<br>externalId=3970<br>categorySignificance=/Informational/Error<br>categoryBehavior=/Modify<br>categoryDeviceGroup=/Data Security<br>catdt=Access and Identity Management<br>categoryOutcome=/Failure<br>categoryObject=/Host/File | произошла ошибка. Восстановление файла не было выполнено. |
| 3971 (0xF83) | Отказ на вход пользователя из-за нарушения контроля целостности | Предупреждение | Событие: отказ на вход пользователя из-за нарушения контроля целостности<br>Пользователь: domain\login<br>SID пользователя:<br>Мандатная метка:<br>Режим работы СЗИ: мягкий режим \| полный функционал | Mon DD hh:mm:ss hostname CEF:0\|GIS\|Blockhost-Net\|3.0 \|BH—IntegrityControl-3971\|Отказ на вход пользователя из-за нарушения контроля целостности\|Medium\|<br>cat=Контроль целостности<br>dhost=имя хоста источника события<br>rt=дата возникновения события на клиенте<br>cs1=содержимое поля ‘Режим работы СЗИ’<br>cs1Label=Режим работы СЗИ<br>suser=содержимое поля ‘Пользователь’<br>suid=содержимое поля ‘SID пользователя’<br>externalId=3971<br>categorySignificance=/Informational/Warning<br>categoryBehavior=/Access/Stop<br>categoryDeviceGroup=/Data Security<br>catdt=Access and Identity Management<br>categoryOutcome=/Success<br>categoryObject=/Actor/User | Отказ на вход пользователя в ОС из-за нарушения целостности одного из контролируемых файлов. Происходит в случае, если в параметрах работы СЗИ задана соответствующая настройка. |
| 3907 (0xF43) | Блокировка сессии пользователя из-за нарушения контроля целостности файлов | Предупреждение | Событие: блокировка сессии пользователя из-за нарушения контроля целостности файлов<br>Пользователь: domain/login<br>SID пользователя:<br>Режим работы СЗИ: мягкий режим \| полный функционал | Mon DD hh:mm:ss hostname CEF:0\|GIS\|Blockhost-Net\|3.0 \|BH—IntegrityControl-3907\|Система заблокировала сессию пользователя из-за нарушения контроля целостности \|Medium\|<br>cat=Контроль целостности<br>dhost=имя хоста источника события<br>rt=дата возникновения события на клиенте<br>cs1=содержимое поля ‘Режим работы | Блокировка сессии пользователя из-за нарушения целостности одного из контролируемых файлов. Происходит в случае, если в параметрах работы СЗИ задана соответствующая настройка. |

| | | | | | |
|---|---|---|---|---|---|
| | | | | СЗИ'<br>cs1Label=Режим работы СЗИ<br>suser=содержимое поля 'Пользователь'<br>suid=содержимое поля 'SID пользователя'<br>externalId=3907<br>categorySignificance=/Informational/Warning<br>categoryBehavior=/Access/Stop<br>categoryDeviceGroup=/Data Security<br>catdt=Access and Identity Management<br>categoryOutcome=/Success<br>categoryObject=/Actor/User | |

# Контроль печати

| Код события | Тип события | Уровень важности | Формат Windows-события | CEF-формат | Условия воспроизведения |
|---|---|---|---|---|---|
| 1334 (0x536) | Печать документа | Сведения | Событие: печать документа<br>Пользователь: domain/login<br>SID пользователя:<br>Мандатная метка пользователя:<br>Имя процесса:<br>Имя принтера:<br>Имя документа:<br>Мандатная метка документа:<br>Размер документа:<br>Количество страниц для печати:<br>Режим работы СЗИ: мягкий режим \| полный функционал | Mon DD hh:mm:ss hostname<br>CEF:0\|GIS\|Blockhost-Net\|3.0<br>\|BH—PrintControl-1334\| Печать документа\|Low\|<br>cat=Контроль печати<br>dhost=имя хоста источника события<br>rt=дата возникновения события на клиенте<br>cs1=содержимое поля 'Режим работы СЗИ'<br>cs1Label=Режим работы СЗИ<br>cs2=содержимое поля 'Имя принтера'<br>cs2Label=Имя принтера<br>cs4=содержимое поля 'Мандатная метка пользователя'<br>cs4Label=Мандатная метка пользователя<br>cs5=содержимое поля 'Мандатная метка документа'<br>cs5Label=Мандатная метка документа<br>cn1=содержимое поля 'Количество страниц для печати'<br>cn1Label=Количество страниц<br>fname=содержимое поля 'Имя документа'<br>fsize=содержимое поля 'Размер документа'<br>sproc=содержимое поля 'Имя процесса'<br>suser=содержимое поля 'Пользователь'<br>suid=содержимое поля 'SID пользователя'<br>externalId=1334<br>categorySignificance=/Informational<br>categoryBehavior=/Print<br>categoryDeviceGroup=/Application<br>catdt=Access and Identity Management | Успешная печать документа. Событие формируется в случае, если на клиенте СЗИ включен контроль печати. |

| | | | | | |
|---|---|---|---|---|---|
| | | | | categoryOutcome=/Success<br>categoryObject=/Host/Application | |
| 1333<br>(0x535) | Отказ в печати документа | Предупреждение | Событие: отказ в печати документа<br>Пользователь: domain/login<br>SID пользователя:<br>Мандатная метка пользователя:<br>Имя процесса:<br>Имя принтера:<br>Имя документа:<br>Мандатная метка документа:<br>Размер документа:<br>Количество страниц для печати:<br>Режим работы СЗИ: мягкий режим \| полный функционал | Mon DD hh:mm:ss hostname<br>CEF:0\|GIS\|Blockhost-Net\|3.0<br>\|BH—PrintControl-1333\| Отказ в печати документа\|Medium\|<br>cat=Контроль печати<br>dhost=имя хоста источника события<br>rt=дата возникновения события на клиенте<br>cs1=содержимое поля ‘Режим работы СЗИ’<br>cs1Label=Режим работы СЗИ<br>cs2=содержимое поля ‘Имя принтера‘<br>cs2Label=Имя принтера<br>cs4=содержимое поля ‘Мандатная метка пользователя’<br>cs4Label=Мандатная метка пользователя<br>cs5=содержимое поля ‘Мандатная метка документа’<br>cs5Label=Мандатная метка документа<br>cn1=содержимое поля ‘Количество страниц для печати’<br>cn1Label=Количество страниц<br>fname=содержимое поля ‘Имя документа’<br>fsize=содержимое поля ‘Размер документа’<br>sproc=содержимое поля ‘Имя процесса’<br>suser=содержимое поля ‘Пользователь’<br>suid=содержимое поля ‘SID пользователя’<br>externalId=1333<br>categorySignificance=/Informational/Warning<br>categoryBehavior=/Print<br>categoryDeviceGroup=/Application<br>catdt=Access and Identity Management<br>categoryOutcome=/Failure<br>categoryObject=/Host/Application | Необходимо сконфигурировать контроль печати таким образом, чтобы печать документа (приложения, которое его печатает) была запрещена. При попытке печати документа будет сформировано данное событие. |

# События сервера СЗИ

| **Код события** | **Тип события** | **Уровень важности** | **Формат Windows-события** | **CEF-формат** | **Условия воспроизведения** |
|---|---|---|---|---|---|
| 3961<br>(0xF79) | Подключение клиента к серверу | Сведения | Событие: подключение клиента<br>Имя клиента: domain/host<br>IP клиента: | Mon DD hh:mm:ss hostname<br>CEF:0\|GIS\|Blockhost-Net\|3.0<br>\|BH-ServerSZI-3961\|Подключение клиента\|Low\|<br>cat=События сервера СЗИ | Подключение клиента к серверу СЗИ. |

| | | | | | |
|---|---|---|---|---|---|
| | | | | dhost=имя хоста источника события<br>rt=дата возникновения события на клиенте<br>sourceAddress=содержимое поля ‘IP клиента’<br>sourceHostName=содержимое поля ‘Имя клиента’<br>externalId=3961<br>categorySignificance=/Informational<br>categoryBehavior=/Communicate<br>categoryDeviceGroup=/Application<br>catdt=Access and Identity Management<br>categoryOutcome=/Success<br>categoryObject=/Host/Application | |
| 3960 (0xF78) | Отключение клиента от сервера | Сведения | Событие: отключение клиента<br>Имя клиента: domain/host<br>IP клиента: | Mon DD hh:mm:ss hostname<br>CEF:0\|GIS\|Blockhost-Net\|3.0<br>\|BH-ServerSZI-3960\|Отключение клиента\|Low\|<br>cat=События сервера СЗИ<br>dhost=имя хоста источника события<br>rt=дата возникновения события на клиенте<br>sourceAddress=содержимое поля ‘IP клиента’<br>sourceHostName=содержимое поля ‘Имя клиента’<br>externalId=3960<br>categorySignificance=/Informational<br>categoryBehavior=/Communicate<br>categoryDeviceGroup=/Application<br>catdt=Access and Identity Management<br>categoryOutcome=/Success<br>categoryObject=/Host/Application | Отключение клиента от сервера СЗИ. |
| 3908 (0xF44) | Отказ в подключении клиента к серверу | Ошибка | Событие: отказ в подключении клиента<br>Причина:<br>Имя клиента: domain/host<br>IP клиента: | Mon DD hh:mm:ss hostname<br>CEF:0\|GIS\|Blockhost-Net\|3.0<br>\|BH-ServerSZI-3908\|Отказ в подключении клиента\|High\|<br>cat=События сервера СЗИ<br>dhost=имя хоста источника события<br>rt=дата возникновения события на клиенте<br>sourceAddress=содержимое поля ‘IP клиента’<br>sourceHostName=содержимое поля ‘Имя клиента’<br>reason=содержимое поля ‘Причина’<br>externalId=3908<br>categorySignificance=/Informational/Error<br>categoryBehavior=/Communicate<br>categoryDeviceGroup=/Application<br>catdt=Access and Identity Management | Отказ в подключении клиента к серверу СЗИ. Возможные причины отказа - клиент с таким именем уже есть на сервере. |

| | | | | | |
|---|---|---|---|---|---|
| | | | | categoryOutcome=/Failure<br>categoryObject=/Host/Application | |
| 3074<br>(0xC02) | Отказ в подключении клиента к серверу из-за ошибки аутентификации | Ошибка | Событие: отказ в подключении клиента к серверу из-за ошибки аутентификации<br>Причина:<br>Имя клиента: domain/host<br>IP клиента: | Mon DD hh:mm:ss hostname<br>CEF:0\|GIS\|Blockhost-Net\|3.0<br>\|BH-ServerSZI-3074\| Отказ в подключении клиента к серверу из-за ошибки аутентификации \|High\|<br>cat=События сервера СЗИ<br>dhost=имя хоста источника события<br>rt=дата возникновения события на клиенте<br>sourceAddress=содержимое поля ‘IP клиента’<br>sourceHostName=содержимое поля ‘Имя клиента’<br>reason=содержимое поля ‘Причина’<br>externalId=3074<br>categorySignificance=/Informational/Error<br>categoryBehavior=/Communicate<br>categoryDeviceGroup=/Application<br>catdt=Access and Identity Management<br>categoryOutcome=/Failure<br>categoryObject=/Host/Application | Ошибка при подключении клиента к серверу. Возможная причина ошибки - некорректный ключ клиента СЗИ |
| 3333<br>(0xD05) | Нарушено лицензионное соглашение | Ошибка | Событие: нарушено лицензионное соглашение<br>Причина: превышено допустимое количество клиентов на сервере \|<br>Используется такая же лицензия на сервере<br>Имя компьютера: domain/host<br>IP компьютера: | Mon DD hh:mm:ss hostname<br>CEF:0\|GIS\|Blockhost-Net\|3.0<br>\|BH-ServerSZI-3333\|нарушено лицензионное соглашение\|High\|<br>cat=События сервера СЗИ<br>dhost=имя хоста источника события<br>rt=дата возникновения события на клиенте<br>sourceAddress=содержимое поля ‘IP компьютера’<br>sourceHostName=содержимое поля ‘Имя компьютера’<br>reason=содержимое поля ‘Причина’<br>externalId=3333<br>categorySignificance=/Informational/Error<br>categoryBehavior=/Communicate<br>categoryDeviceGroup=/Application<br>catdt=Access and Identity Management<br>categoryOutcome=/Failure<br>categoryObject=/Host/Application | На сервере СЗИ нет достаточного количества лицензий для подключения клиентов. |
| 3909<br>(0xF45) | Подключение к головному серверу | Сведения | Событие: подключение к головному серверу<br>Имя сервера: domain/host<br>IP сервера: | Mon DD hh:mm:ss hostname<br>CEF:0\|GIS\|Blockhost-Net\|3.0<br>\|BH-ServerSZI-3909\|Подключение к головному серверу \|Low\|<br>cat=События сервера СЗИ<br>dhost=имя хоста источника события<br>rt=дата возникновения события на | Восстановление связи с головным (родительским) сервером СЗИ. Событие формируется на подчиненном сервере. |

| | | | | | |
|---|---|---|---|---|---|
| | | | | клиенте<br>sourceAddress=содержимое поля ‘IP сервера’<br>sourceHostName=содержимое поля ‘Имя сервера’<br>externalId=3909<br>categorySignificance=/Informational<br>categoryBehavior=/Communicate<br>categoryDeviceGroup=/Application<br>catdt=Access and Identity Management<br>categoryOutcome=/Success<br>categoryObject=/Host/Application | |
| 3910 (0xF46) | Отключение от головного сервера | Сведения | Событие: отключение от головного сервера<br>Имя сервера: domain/host<br>IP сервера: | Mon DD hh:mm:ss hostname<br>CEF:0\|GIS\|Blockhost-Net\|3.0<br>\|BH-ServerSZI-3910\|Отключение от головного сервера\|Low\|<br>cat=События сервера СЗИ<br>dhost=имя хоста источника события<br>rt=дата возникновения события на клиенте<br>sourceAddress=содержимое поля ‘IP сервера’<br>sourceHostName=содержимое поля ‘Имя сервера’<br>externalId=3910<br>categorySignificance=/Informational<br>categoryBehavior=/Communicate<br>categoryDeviceGroup=/Application<br>catdt=Access and Identity Management<br>categoryOutcome=/Success<br>categoryObject=/Host/Application | Потеря связи с головным (родительским) сервером СЗИ.<br>Событие формируется на подчиненном сервере. |
| 3911 (0xF47) | Отказ в подключении к головному серверу | Ошибка | Событие: отказ в подключении к головному серверу<br>Причина:<br>Имя сервера: domain/host<br>IP сервера: | Mon DD hh:mm:ss hostname<br>CEF:0\|GIS\|Blockhost-Net\|3.0<br>\|BH-ServerSZI-3911\|Отключение головного сервера\|High\|<br>cat=События сервера СЗИ<br>dhost=имя хоста источника события<br>rt=дата возникновения события на клиенте<br>sourceAddress=содержимое поля ‘IP сервера’<br>sourceHostName=содержимое поля ‘Имя сервера’<br>reason=содержимое поля ‘Причина’<br>externalId=3911<br>categorySignificance=/Informational/Error<br>categoryBehavior=/Communicate<br>categoryDeviceGroup=/Application<br>catdt=Access and Identity Management<br>categoryOutcome=/Failure<br>categoryObject=/Host/Application | Нижележащему (подчиненному) серверу отказано в подключении к головному (родительскому) серверу СЗИ.<br>Событие формируется на подчиненном сервере. |

| | | | | | |
|---|---|---|---|---|---|
| 3912 (0xF48) | Подключение к дочернему серверу | Сведения | Событие: подключение дочернего сервера<br>Имя сервера: domain/host<br>IP сервера: | Mon DD hh:mm:ss hostname CEF:0\|GIS\|Blockhost-Net\|3.0 \|BH-ServerSZI-3912\|Подключение дочернего сервера\|Low\| cat=События сервера СЗИ dhost=имя хоста источника события rt=дата возникновения события на клиенте sourceAddress=содержимое поля ‘IP сервера’ sourceHostName=содержимое поля ‘Имя сервера’ externalId=3912 categorySignificance=/Informational categoryBehavior=/Communicate categoryDeviceGroup=/Application catdt=Access and Identity Management categoryOutcome=/Success categoryObject=/Host/Application | Восстановление связи с дочерним (подчиненным) сервером СЗИ.<br>Событие формируется на родительском сервере. |
| 3913 (0xF49) | Отключение от дочернего сервера | Сведения | Событие: отключение дочернего сервера<br>Имя сервера: domain/host<br>IP сервера: | Mon DD hh:mm:ss hostname CEF:0\|GIS\|Blockhost-Net\|3.0 \|BH-ServerSZI-3913\|Отключение дочернего сервера\|Low\| cat=События сервера СЗИ dhost=имя хоста источника события rt=дата возникновения события на клиенте sourceAddress=содержимое поля ‘IP сервера’ sourceHostName=содержимое поля ‘Имя сервера’ externalId=3913 categorySignificance=/Informational categoryBehavior=/Communicate categoryDeviceGroup=/Application catdt=Access and Identity Management categoryOutcome=/Success categoryObject=/Host/Application | Потеря связи с нижележащим (подчиненным) сервером СЗИ.<br>Событие формируется на родительском сервере. |
| 3920 (0xF50) | Отказ в подключении к дочернему серверу | Ошибка | Событие: отказ в подключении дочернего сервера<br>Причина:<br>Имя сервера: domain/host<br>IP сервера: | Mon DD hh:mm:ss hostname CEF:0\|GIS\|Blockhost-Net\|3.0 \|BH-ServerSZI-3920\|Отказ в подключении дочернего сервера\|High\| cat=События сервера СЗИ dhost=имя хоста источника события rt=дата возникновения события на клиенте sourceAddress=содержимое поля ‘IP сервера’ sourceHostName=содержимое поля ‘Имя сервера’ | Головному (родительскому) серверу отказано в подключении к нижележащему (подчиненному) серверу СЗИ.<br>Событие формируется на родительском сервере. |

| | | | | | |
|---|---|---|---|---|---|
| | | | | reason=содержимое поля ‘Причина’<br>externalId=3920<br>categorySignificance=/Informational/Error<br>categoryBehavior=/Communicate<br>categoryDeviceGroup=/Application<br>catdt=Access and Identity Management<br>categoryOutcome=/Failure<br>categoryObject=/Host/Application | |
| 3921 (0xF51) | Подключение консоли к серверу по иерархии | Сведения | Событие: открытие сессии управления по иерархии<br>Имя родит. сервера: domain/host<br>Пользователь: | Mon DD hh:mm:ss hostname<br>CEF:0\|GIS\|Blockhost-Net\|3.0<br>\|BH-ServerSZI-3921\|Открытие сессии управление по иерархии \|Low\|<br>cat=События сервера СЗИ<br>dhost=имя хоста источника события<br>rt=дата возникновения события на клиенте<br>sourceHostName=содержимое поля ‘Имя родительского сервера’<br>suser=содержимое поля ‘Пользователь’<br>externalId=3921<br>categorySignificance=/Informational<br>categoryBehavior=/Communicate<br>categoryDeviceGroup=/Application<br>catdt=Access and Identity Management<br>categoryOutcome=/Success | Подключение консоли управления СЗИ к серверу, находящемуся ниже по уровню иерархии. Событие формируется на сервере СЗИ, к которому было выполнено подключение. |
| 3922 (0xF52) | Сервер администрирования запущен | Сведения | Событие: сервер администрирования запущен | Mon DD hh:mm:ss hostname<br>CEF:0\|GIS\|Blockhost-Net\|3.0<br>\|BH-ServerSZI-3922\|Сервер администрирования запущен\|Low\|<br>cat=События сервера СЗИ<br>dhost=имя хоста источника события<br>rt=дата возникновения события на клиенте<br>externalId=3922<br>categorySignificance=/Informational<br>categoryBehavior= Execute/Start<br>categoryDeviceGroup=/Application<br>catdt=Access and Identity Management<br>categoryOutcome=/Success | Запуск и инициализация служб сервера СЗИ. |
| 3923 (0xF53) | Сервер администрирования остановлен | Предупреждение | События: сервер администрирования остановлен | Mon DD hh:mm:ss hostname<br>CEF:0\|GIS\|Blockhost-Net\|3.0<br>\|BH-ServerSZI-3923\|Сервер администрирования остановлен\|Medium\|<br>cat=События сервера СЗИ<br>dhost=имя хоста источника события<br>rt=дата возникновения события на клиенте<br>externalId=3923<br>categorySignificance=/Informational/Warning | Остановка служб сервера СЗИ. |

| | | | | | |
|---|---|---|---|---|---|
| | | | | categoryBehavior= Execute/Stop<br>categoryDeviceGroup=/Application<br>catdt=Access and Identity Management<br>categoryOutcome=/Success | |
| 3924 (0xF54) | Ошибка при запуске сервера администрирования | Ошибка | Событие: ошибка при запуске сервера администрирования<br>Причина: не удалось запустить службы <список служб> \| <другие причины> | Mon DD hh:mm:ss hostname<br>CEF:0\|GIS\|Blockhost-Net\|3.0<br>\|BH-ServerSZI-3924\|Ошибка при запуске сервера администрирования\|High\|<br>cat=События сервера СЗИ<br>dhost=имя хоста источника события<br>rt=дата возникновения события на клиенте<br>reason=содержимое поля ‘Причина’<br>externalId=3924<br>categorySignificance=/Informational/Error<br>categoryBehavior= Execute<br>categoryDeviceGroup=/Application<br>catdt=Access and Identity Management<br>categoryOutcome=/Failure | В процессе запуска и инициализации служб сервера СЗИ произошла ошибка. |
| 3972 (0xF84) | Запуск цикла опроса подчиненных серверов (по расписанию) | Сведения | Событие: запуск цикла опроса подчиненных серверов (по расписанию) | Конвертация в CEF отсутствует (событие не передается в SIEM-систему) | Запущен процесс сбора событий аудита с подчиненных серверов (в соответствие с расписанием, определенным администратором сервера, выполняющего сбор) |
| 3973 (0xF85) | Завершение цикла опроса подчиненных серверов (по расписанию) | Сведения | Событие: завершение цикла опроса подчиненных серверов (по расписанию) | Конвертация в CEF отсутствует (событие не передается в SIEM-систему) | Завершен процесс сбора событий аудита с подчиненных серверов (в соответствие с расписанием, определенным администратором сервера, выполняющего сбор) |
| 3974 (0xF86) | Запуск цикла опроса клиентских компьютеров (по расписанию) | Сведения | Событие: запуск цикла опроса клиентских компьютеров (по расписанию) | Конвертация в CEF отсутствует (событие не передается в SIEM-систему) | Запущен процесс сбора событий аудита с клиентских компьютеров, подключенных к серверу (в соответствие с расписанием, определенным администратором сервера, выполняющего сбор) |
| 3975 (0xF87) | Завершение цикла опроса клиентских компьютеров (по расписанию) | Сведения | Событие завершение цикла опроса клиентских компьютеров (по расписанию) | Конвертация в CEF отсутствует (событие не передается в SIEM-систему) | Завершен процесс сбора событий аудита с подчиненных серверов (в соответствие с |

| | | | | | |
|---|---|---|---|---|---|
| | | | | | расписанием сбора, определенным администратором сервера, выполняющего сбор) |
| 3976 (0xF88) | Запуск цикла опроса подчиненных серверов (по требованию пользователя) | Сведения | Событие: запуск цикла опроса подчиненных серверов (по требованию пользователя) | Конвертация в CEF отсутствует (событие не передается в SIEM-систему) | Запущен внеплановый процесс сбора событий аудита с подчиненных серверов. Инициатором процесса является администратор сервера, выполняющего сбор. |
| 3977 (0xF89) | Завершение цикла опроса подчиненных серверов (по требованию пользователя) | Сведения | Событие: завершение цикла опроса подчиненных серверов (по требованию пользователя) | Конвертация в CEF отсутствует (событие не передается в SIEM-систему) | Завершен внеплановый процесс сбора событий аудита с подчиненных серверов. Инициатором процесса является администратор сервера, выполняющего сбор. |
| 3978 (0xF8A) | Запуск цикла опроса клиентских компьютеров (по требованию пользователя) | Сведения | Событие: запуск цикла опроса клиентских компьютеров (по требованию пользователя) | Конвертация в CEF отсутствует (событие не передается в SIEM-систему) | Запущен внеплановый процесс сбора событий аудита с клиентских компьютеров, подключенных к серверу. Инициатором процесса является администратор сервера, выполняющего сбор. |
| 3979 (0xF8B) | Завершение цикла опроса клиентских компьютеров (по требованию пользователя) | Сведения | Событие: завершение цикла опроса клиентских компьютеров (по требованию пользователя) | Конвертация в CEF отсутствует (событие не передается в SIEM-систему) | Завершен внеплановый процесс сбора событий аудита с клиентских компьютеров, подключенных к серверу. Инициатором процесса является администратор сервера, выполняющего сбор. |
| 3989 (0xF95) | Прерывание цикла опроса клиентов из-за наступления исключающего интервала | Сведения | Событие: прерывание цикла опроса клиентов из-за наступления исключающего интервала | Конвертация в CEF отсутствует (событие не передается в SIEM-систему) | Процесс сбора событий аудита с клиентских компьютеров был прерван из-за наступления интервала времени, в рамках которого сетевой канал между сервером и клиентскими компьютерами не должен быть утилизирован. Исключающие интервалы определяются |

| | | | | | |
|---|---|---|---|---|---|
| | | | | | администратором сервера, осуществляющего сбор. |
| 3990 (0xF96) | Прерывание цикла опроса подсерверов из-за наступления исключающего интервала | Сведения | Событие: прерывание цикла опроса подсерверов из-за наступления исключающего интервала | Конвертация в CEF отсутствует (событие не передается в SIEM-систему) | Процесс сбора событий аудита с подчиненных серверов был прерван из-за наступления интервала времени, в рамках которого сетевой канал между сервером и подчиненными серверами не должен быть утилизирован. Исключающие интервалы определяются администратором сервера, осуществляющего сбор. |
| 3980 (0xF8C) | Ошибка при попытке сбора аудита с клиентских компьютеров | Ошибка | Событие: ошибка при попытке сбора аудита с клиентских компьютеров Возможные причины: устаревшая версия клиента БХ-Сеть; клиентский компьютер не в сети Имена клиентских компьютеров: | Конвертация в CEF отсутствует (событие не передается в SIEM-систему) | Не удалось выполнить сбор событий аудита с части клиентских компьютеров, подключенных к серверу СЗИ. Возможные причины: • на клиентском компьютере установлено СЗИ старой версии; • не удалось установить соединение с клиентским компьютером; (выключен, перезагружается, сбой в сети и т.д.). |
| 3981 (0xF8D) | Ошибка при попытке сбора аудита с подчиненных серверов | Ошибка | Событие: ошибка при попытке сбора аудита с подчиненных серверов Возможные причины: устаревшая версия сервера БХ-Сеть; подчиненный сервер не в сети Имена подчиненных серверов: | Конвертация в CEF отсутствует (событие не передается в SIEM-систему) | Не удалось выполнить сбор событий аудита с части подчиненных серверов, подключенных к серверу СЗИ. Возможные причины: • на подчиненном сервере установлено СЗИ старой версии; • не удалось установить соединение с подчиненным сервером; (выключен, перезагружается, сбой в сети и т.д.). |
| 3983 | Недостаточно места на | Ошибка | Событие: недостаточно места на | Конвертация в CEF отсутствует | На компьютере с сервером |

| | | | | | |
|---|---|---|---|---|---|
| (0xF8F) | сервере для сохранения событий аудита | | сервере для сохранения событий аудита<br>Рекомендация: произведите очистку хранилища событий методом автоархивации | (событие не передается в SIEM-систему) | СЗИ недостаточно дискового пространства для сохранения событий аудита в хранилище для долгосрочного хранения событий. |
| 3984 (0xF90) | Ошибка при записи событий аудита в кэш событий | Ошибка | Событие: ошибка при записи событий аудита в кэш событий<br>Причина: превышен максимальный размер кэша событий | Конвертация в CEF отсутствует (событие не передается в SIEM-систему) | Размер временного хранилища событий аудита на сервере СЗИ превысил допустимый размер. Максимальный допустимый размер хранилища определяется администратором в настройках сервера СЗИ. |
| 3985 (0xF91) | Запуск создания архива событий аудита по расписанию | Сведения | Событие: запуск создания архива событий аудита по расписанию<br>Тип архивации: перемещение событий в файл архива \| удаление событий<br>Имя файла: <имя файла><br>Начиная с:<br>Заканчивая по: | Конвертация в CEF отсутствует (событие не передается в SIEM-систему) | Запущен процесс создания архива событий аудита. |
| 3986 (0xF92) | Успешное создание архива событий аудита | Сведения | Событие: успешное создание архива событий аудита | Конвертация в CEF отсутствует (событие не передается в SIEM-систему) | Завершен процесс создания архива событий аудита. |
| 3987 (0xF93) | Ошибка при создании архива событий аудита | Ошибка | Событие: ошибка при создании архива событий аудита<br>Причина: | Конвертация в CEF отсутствует (событие не передается в SIEM-систему) | В процесс создания архива событий аудита произошла ошибка. |
| 3988 (0xF94) | Ошибка при попытке экспорта событий аудита в SIEM-систему | Ошибка | Событие: ошибка при попытке экспорта событий аудита в SIEM-систему<br>Причина: | Конвертация в CEF отсутствует (событие не передается в SIEM-систему) | Не удалось экспортировать события аудита, собранные сервером с его клиентских компьютеров и подчиненных серверов, в SIEM-систему из-за невозможности установки соединения. |

# Событие клиента СЗИ

| Код события | Тип события | Уровень важности | Формат Windows-события | CEF-формат | Условия воспроизведения |
|---|---|---|---|---|---|
| 3089 | Подключение клиента | Сведения | Событие: подключение клиента к | Mon DD hh:mm:ss  hostname | Подключение клиента к |

| | | | | | |
|---|---|---|---|---|---|
| (0xC11) | к серверу | | серверу<br>IP сервера: | CEF:0\|GIS\|Blockhost-Net\|3.0<br>\|BH-ClientSZI-3089\|Подключение клиента к серверу\|Low\|<br>cat=События клиента СЗИ<br>dhost=имя хоста источника события<br>rt=дата возникновения события на клиенте<br>sourceAddress=содержимое поля ‘IP сервера’<br>externalId=3089<br>categorySignificance=/Informational<br>categoryBehavior=/Communicate<br>categoryDeviceGroup=/Application<br>catdt=Access and Identity Management<br>categoryOutcome=/Success<br>categoryObject=/Host/Application | серверу СЗИ. |
| 3925<br>(0xF55) | Отключение клиента от сервера | Сведения | Событие: отключение клиента от сервера<br>IP сервера: | Mon DD hh:mm:ss hostname<br>CEF:0\|GIS\|Blockhost-Net\|3.0<br>\|BH-ClientSZI-3925\|Отключение клиента от сервера\|Low\|<br>cat=События клиента СЗИ<br>dhost=имя хоста источника события<br>rt=дата возникновения события на клиенте<br>sourceAddress=содержимое поля ‘IP сервера’<br>externalId=3925<br>categorySignificance=/Informational<br>categoryBehavior=/Communicate<br>categoryDeviceGroup=/Application<br>catdt=Access and Identity Management<br>categoryOutcome=/Success<br>categoryObject=/Host/Application | Отключение клиента от сервера СЗИ. |
| 3090<br>(0xC12) | Отказ в подключении клиента к серверу | Ошибка | Событие: отказ в подключении клиента к серверу<br>Причина:<br>IP сервера: | Mon DD hh:mm:ss hostname<br>CEF:0\|GIS\|Blockhost-Net\|3.0<br>\|BH-ClientSZI-3090\|Отказ от подключения клиента к серверу\|High\|<br>cat=События клиента СЗИ<br>dhost=имя хоста источника события<br>rt=дата возникновения события на клиенте<br>reason=содержимое поля ‘Причина’<br>sourceAddress=содержимое поля ‘IP сервера’<br>externalId=3090<br>categorySignificance=/Informational/Error<br>categoryBehavior=/Communicate<br>categoryDeviceGroup=/Application<br>catdt=Access and Identity Management<br>categoryOutcome=/Failure<br>categoryObject=/Host/Application | Отказ в подключении клиента к серверу СЗИ. Возможные причины отказа - клиент с таким именем уже есть на сервере. |

| | | | | | |
|---|---|---|---|---|---|
| 3091 (0xC13) | Сервер не найден | Ошибка | Событие: сервер не найден<br>IP сервера: | Mon DD hh:mm:ss hostname<br>CEF:0\|GIS\|Blockhost-Net\|3.0<br>\|BH-ClientSZI-3091\|Сервер не найден\|High\|<br>cat=События клиента СЗИ<br>dhost=имя хоста источника события<br>rt=дата возникновения события на клиенте<br>sourceAddress=содержимое поля ‘IP сервера’<br>externalId=3091<br>categorySignificance=/Informational/Error<br>categoryBehavior=/Communicate<br>categoryDeviceGroup=/Application<br>catdt=Access and Identity Management<br>categoryOutcome=/Failure<br>categoryObject=/Host/Application | Клиенту не удалось установить соединение с сервером СЗИ по имеющемуся адресу. |
| 3926 (0xF56) | Клиент запущен | Информация | Событие: клиент запущен | Mon DD hh:mm:ss hostname<br>CEF:0\|GIS\|Blockhost-Net\|3.0<br>\|BH-ClientSZI-3926\|Клиент запущен\|Low\|<br>cat=События клиента СЗИ<br>dhost=имя хоста источника события<br>rt=дата возникновения события на клиенте<br>externalId=3926<br>categorySignificance=/Informational<br>categoryBehavior=/Access/Start<br>categoryDeviceGroup=/Application<br>catdt=Access and Identity Management<br>categoryOutcome=/Success<br>categoryObject=/Host/Application | Завершение запуска и инициализации всех служб клиента СЗИ. |
| 3927 (0xF57) | Клиент остановлен | Информация | Событие: клиент остановлен | Mon DD hh:mm:ss hostname<br>CEF:0\|GIS\|Blockhost-Net\|3.0<br>\|BH-ClientSZI-3927\|Клиент остановлен\|Low\|<br>cat=События клиента СЗИ<br>dhost=имя хоста источника события<br>rt=дата возникновения события на клиенте<br>externalId=3927<br>categorySignificance=/Informational<br>categoryBehavior=/Access/Stop<br>categoryDeviceGroup=/Application<br>catdt=Access and Identity Management<br>categoryOutcome=/Success<br>categoryObject=/Host/Application | Остановка всех служб клиента СЗИ. |
| 3928 (0xF58) | Ошибка при запуске клиента | Ошибка | Событие: ошибка при запуске клиента<br>Причина: не удалось запустить службы <список служб> | Mon DD hh:mm:ss hostname<br>CEF:0\|GIS\|Blockhost-Net\|3.0<br>\|BH-ClientSZI-3928\|Ошибка при запуске | В процессе запуска и инициализации служб клиента СЗИ произошла |

| | | | | | |
|---|---|---|---|---|---|
| | | | | клиента\|High\|<br>cat=События клиента СЗИ<br>dhost=имя хоста источника события<br>rt=дата возникновения события на клиенте<br>reason=содержимое поля ‘Причина’<br>externalId=3928<br>categorySignificance=/Informational/Error<br>categoryBehavior=/Access<br>categoryDeviceGroup=/Application<br>catdt=Access and Identity Management<br>categoryOutcome=/Failure<br>categoryObject=/Host/Application | ошибка. |
| 3929 (0xF59) | Включение мягкого режима | Предупреждение | Событие: включение мягкого режима<br>Источник: локальная консоль \| серверная консоль \| групповые политики<br>Изменения внес: domain\login | Mon DD hh:mm:ss hostname<br>CEF:0\|GIS\|Blockhost-Net\|3.0\|BH-ClientSZI-3929\|Включение мягкого режима\|Medium\|<br>cat=События клиента СЗИ<br>dhost=имя хоста источника события<br>rt=дата возникновения события на клиенте<br>cs1=содержимое поля ‘Источник’<br>cs1Label=Тип консоли<br>suser=содержимое поля ‘Изменения внес’<br>externalId=3929<br>categorySignificance=/Informational/Warning<br>categoryBehavior= /Modify/Configuration<br>categoryDeviceGroup=/Application<br>catdt=Access and Identity Management<br>categoryOutcome=/Success<br>categoryObject=/Host/Application | На клиенте СЗИ включен «мягкий» режим работы. Возможные источники (способы) включения режима:<br>• включение через серверную консоль;<br>• включение через локальную консоль (установленную на том же компьютере, что и клиент) ;<br>• включение через групповые политики СЗИ. |
| 3936 (0xF60) | Отключение мягкого режима | Предупреждение | Событие: отключение мягкого режима<br>Источник: локальная консоль \| серверная консоль \| групповые политики<br>Изменения внес: domain\login | Mon DD hh:mm:ss hostname<br>CEF:0\|GIS\|Blockhost-Net\|3.0\|BH-ClientSZI-3936\|Отключение мягкого режима\|Medium\|<br>cat=События клиента СЗИ<br>dhost=имя хоста источника события<br>rt=дата возникновения события на клиенте<br>cs1=содержимое поля ‘Источник’<br>cs1Label=Тип консоли<br>suser=содержимое поля ‘Изменения внес’<br>externalId=3936<br>categorySignificance=/Informational/Warning<br>categoryBehavior= /Modify/Configuration<br>categoryDeviceGroup=/Application<br>catdt=Access and Identity Management | На клиенте СЗИ выключен «мягкий» режим работы. Возможные источники (способы) включения режима:<br>• включение через серверную консоль;<br>• включение через локальную консоль (установленную на том же компьютере, что и клиент);<br>• включение через групповые политики. |

| | | | | | |
|---|---|---|---|---|---|
| | | | | categoryOutcome=/Success<br>categoryObject=/Host/Application | |
| 3937<br>(0xF61) | Изменение параметров роботы клиента СЗИ | Предупреждение | Список изменений:<br>Пользователи:<br><Имя пользователя> (Добавление / Удаление / Изменение)<br>Временные папки<br>Монопольный доступ<br>Дискреционный<br>Ограничение по времени<br>Контроль процессов<br>Контроль печати<br>Полномочия<br>Аутентификация<br>Список токенов<br>Свойства пользователя<br>Контроль портов и CD<br>Группы пользователей:<br><Имя группы пользователей> (Добавление / Удаление / Изменение)<br>Временные папки<br>Монопольный доступ<br>Дискреционный<br>Ограничение по времени<br>Контроль процессов<br>Контроль печати<br>Полномочия<br>Аутентификация<br>Свойства пользователя<br>Контроль портов и CD<br>Список токенов<br>Механизмы:<br>Мандатное разграничение<br>Контроль целостности файлов<br>Очистка остаточной информации<br>Общие настройки<br>Политика аутентификации<br>Сбор аудита<br>Контроль запуска<br>Контроль целостности среды | Конвертация в CEF отсутствует (событие не передается в SIEM-систему) | Выполнено изменение параметров работы (настроек безопасности) клиента СЗИ.<br>Данное событие будет сформировано в журнале клиента СЗИ, если на нем будут любым доступным способом (с помощью серверной или локальной консолей, групповых настроек) изменены настройки механизмов безопасности или общие параметры работы СЗИ.<br>Стоит обратить внимание, что для следующих изменений настроек формируются отдельные события аудита:<br>• добавление токена;<br>• добавление / удаление пользователя;<br>• включение и отключение мягкого режима. |
| 3938<br>(0xF62) | Добавлен пользователь на клиенте СЗИ | Сведения | Событие: добавлен пользователь на клиенте СЗИ<br>Источник: локальная консоль \| серверная консоль<br>Изменения внес: domain\login<br>Пользователь: domain\login | Mon DD hh:mm:ss hostname<br>CEF:0\|GIS\|Blockhost-Net\|3.0<br>\|BH-ClientSZI-3938\|Добавлен пользователь на клиенте СЗИ\|Low\|<br>cat=События клиента СЗИ<br>dhost=имя хоста источника события<br>rt=дата возникновения события на клиенте<br>cs1=содержимое поля ‘Источник’<br>cs1Label=Тип консоли<br>suser=содержимое поля ‘Изменения | В настройки безопасности клиента СЗИ был добавлен пользователь.<br>Возможные источники (способы) добавления пользователя:<br>• через серверную консоль;<br>• через локальную консоль (установленную на том же компьютере, что и |

| | | | | | |
|---|---|---|---|---|---|
| | | | | внес'<br>duser=содержимое поля 'Пользователь'<br>externalId=3938<br>categorySignificance=/Informational<br>categoryBehavior= /Modify/Configuration<br>categoryDeviceGroup=/Application<br>catdt=Access and Identity Management<br>categoryOutcome=/Success<br>categoryObject=/Host/Application | клиент) ;<br>• через групповые политики. |
| 3939 (0xF63) | Добавлена группа на клиенте СЗИ | Сведения | Событие: добавлена группа на клиенте СЗИ<br>Источник: локальная консоль \| серверная консоль<br>Изменения внес: domain\login<br>Группа: <имя группы> | Mon DD hh:mm:ss hostname<br>CEF:0\|GIS\|Blockhost-Net\|3.0<br>\|BH-ClientSZI-3939\|Добавлена группа на клиенте СЗИ\|Low\|<br>cat=События клиента СЗИ<br>dhost=имя хоста источника события<br>rt=дата возникновения события на клиенте<br>cs1=содержимое поля 'Источник'<br>cs1Label=Тип консоли<br>suser=содержимое поля 'Изменения внес'<br>duser=содержимое поля 'Группа'<br>externalId=3939<br>categorySignificance=/Informational<br>categoryBehavior= /Modify/Configuration<br>categoryDeviceGroup=/Application<br>catdt=Access and Identity Management<br>categoryOutcome=/Success<br>categoryObject=/Host/Application | В настройки безопасности клиента СЗИ была добавлена группа.<br>Возможные источники (способы) добавления группы:<br>• через серверную консоль;<br>• через локальную консоль (установленную на том же компьютере, что и клиент) ;<br>• через групповые политики. |
| 3940 (0xF64) | Удален пользователь на клиенте СЗИ | Сведения | Событие: удален пользователь на клиенте СЗИ<br>Источник: локальная консоль \| серверная консоль<br>Изменения внес: domain\login<br>Пользователь: domain\login | Mon DD hh:mm:ss hostname<br>CEF:0\|GIS\|Blockhost-Net\|3.0<br>\|BH-ClientSZI-3940\|Удален пользователь на клиенте СЗИ\|Low\|<br>cat=События клиента СЗИ<br>dhost=имя хоста источника события<br>rt=дата возникновения события на клиенте<br>cs1=содержимое поля 'Источник'<br>cs1Label=Тип консоли<br>suser=содержимое поля 'Изменения внес'<br>duser=содержимое поля 'Пользователь'<br>externalId=3940<br>categorySignificance=/Informational<br>categoryBehavior= /Modify/Configuration<br>categoryDeviceGroup=/Application<br>catdt=Access and Identity Management<br>categoryOutcome=/Success<br>categoryObject=/Host/Application | Из настроек безопасности клиента СЗИ был удален пользователь.<br>Возможные источники (способы) удаления пользователя:<br>• через серверную консоль;<br>• через локальную консоль (установленную на том же компьютере, что и клиент) ;<br>• через групповые политики. |
| 3941 | Удалена группа на клиенте | Сведения | Событие: удалена группа на клиенте | Mon DD hh:mm:ss hostname | Из настроек безопасности |

| | | | | | |
|---|---|---|---|---|---|
| (0xF65) | СЗИ | | СЗИ<br>Источник: локальная консоль \| серверная консоль<br>Изменения внес: domain\login<br>Группа: <имя группы> | CEF:0\|GIS\|Blockhost-Net\|3.0 \|BH-ClientSZI-3941\|Удалена группа на клиенте СЗИ\|Low\|<br>cat=События клиента СЗИ<br>dhost=имя хоста источника события<br>rt=дата возникновения события на клиенте<br>cs1=содержимое поля ‘Источник’<br>cs1Label=Тип консоли<br>suser=содержимое поля ‘Изменения внес’<br>duser=содержимое поля ‘Группа’<br>externalId=3941<br>categorySignificance=/Informational<br>categoryBehavior= /Modify/Configuration<br>categoryDeviceGroup=/Application<br>catdt=Access and Identity Management<br>categoryOutcome=/Success<br>categoryObject=/Host/Application | клиента СЗИ была удалена группа.<br>Возможные источники (способы) удаления группы:<br>• через серверную консоль;<br>• через локальную консоль (установленную на том же компьютере, что и клиент) ;<br>• через групповые политики. |
| 3942 (0xF66) | Добавлен токен на клиенте СЗИ | Сведения | Событие: добавлен токен на клиенте СЗИ<br>Источник: локальная консоль \| серверная консоль<br>Изменения внес : domain\login<br>Пользователь:<br>Имя токена:<br>Идентификатор токена: | Mon DD hh:mm:ss hostname<br>CEF:0\|GIS\|Blockhost-Net\|3.0 \|BH-ClientSZI-3042\|Добавление токена на клиенте СЗИ\|Low\|<br>cat=События клиента СЗИ<br>dhost=имя хоста источника события<br>rt=дата возникновения события на клиенте<br>cs1=содержимое поля ‘Источник'<br>cs1Label=Тип консоли<br>cs3=содержимое поля ‘Идентификатор токена’<br>cs3Label=Идентификатор токена<br>cs6=содержимое поля ‘Имя токена‘<br>cs6Label=Имя токена<br>suser=содержимое ‘Изменения внес’<br>duser=содержимое поля ‘Пользователь’<br>externalId=3942<br>categorySignificance=/Informational<br>categoryBehavior=/Modify/Configuration<br>categoryDeviceGroup=/Database<br>catdt=Access and Identity Management<br>categoryOutcome=/Success<br>categoryObject=/Host/Application | В настройках безопасности клиента СЗИ выполнена привязка токена к пользователю.<br>Возможные источники (способы) привязки токена к пользователю:<br>• через серверную консоль;<br>• через локальную консоль (установленную на том же компьютере, что и клиент) ;<br>• через групповые политики. |

# Действия администратора СЗИ

| Код событ | Тип события | Уровень важности | Формат Windows-события | CEF-формат | Условия воспроизведения |
|---|---|---|---|---|---|

| ия | | | | | |
|---|---|---|---|---|---|
| 3943 (0xF67) | Запуск консоли СЗИ | Сведения | Событие: запуск консоли СЗИ<br>Пользователь: domain\login<br>SID пользователя:<br>Полномочия: администратор \| аудитор | Mon DD hh:mm:ss hostname<br>CEF:0\|GIS\|Blockhost-Net\|3.0<br>\|BH-adminAction-3943\|Запуск консоли СЗИ\|Low\|<br>cat=Действия администратора СЗИ<br>dhost=имя хоста источника события<br>rt=дата возникновения события на клиенте<br>cs1=содержимое поля ‘Полномочия’<br>cs1Label=Привилегии администратора<br>suser=содержимое поля ‘Пользователь’<br>suid=содержимое поля ‘SID пользователя’<br>externalId=3943<br>categorySignificance=/Informational<br>categoryBehavior=/Access/Start<br>categoryDeviceGroup=/Application<br>catdt=Access and Identity Management<br>categoryOutcome=/Success<br>categoryObject=/Host/Application | Администратор выполнил запуск консоли управления политиками СЗИ. |
| 3944 (0xF68) | Отказ на запуск консоли СЗИ | Ошибка | Событие: отказ на запуск консоли СЗИ<br>Причина:<br>Пользователь: domain\login<br>SID пользователя:<br>Полномочия: администратор \| аудитор | Mon DD hh:mm:ss hostname<br>CEF:0\|GIS\|Blockhost-Net\|3.0<br>\|BH-adminAction-3944\|Отказ на запуск консоли СЗИ\|Low\|<br>cat=Действия администратора СЗИ<br>dhost=имя хоста источника события<br>rt=дата возникновения события на клиенте<br>cs1=содержимое поля ‘Полномочия‘<br>cs1Label=Привилегии администратора<br>suser=содержимое поля ‘Пользователь’<br>suid=содержимое поля ‘SID пользователя’<br>reason=содержимое поля ‘Причина’<br>externalId=3944<br>categorySignificance=/Informational<br>categoryBehavior=/Access<br>categoryDeviceGroup=/Application<br>catdt=Access and Identity Management<br>categoryOutcome=/Failure<br>categoryObject=/Host/Application | Не удалось выполнить запуск консоли управления политиками СЗИ.<br>Возможные причины:<br>• запуск консоли выполнялся из-под учетной записи пользователя, не обладающей административными правами;<br>• учетная запись не добавлена в список пользователей. |
| 3945 (0xF69) | Изменение параметров работы СЗИ | Предупреждение | Список изменений:<br>Лицензии<br><Имя лицензии><br>(Удаление / Добавление)<br>Передача в SIEM (Включение / Выключение)<br>Настройки сервера<br>Настройки подключения к родительскому серверу | Конвертация в CEF отсутствует (событие не передается в SIEM-систему) | Были изменены параметры работы сервера СЗИ, указанные в событии. |

| | | | | | |
|---|---|---|---|---|---|
| | | | Пароль подключения клиентов<br>Пароль подключения подчиненных серверов<br>Машины:<br><Имя машины> (Удаление / Добавление / При изменении операция не указывается)<br>Группы машин:<br><Имя группы> (Удаление из <ИМЯ> /<br>Изменение /<br>Перемещение из <ИМЯ> в <ИМЯ> /<br>Добавление в <ИМЯ>)<br>Пользователи:<br><Имя пользователя> (Добавление /<br>Удаление / Изменение)<br>Временные папки<br>Монопольный доступ<br>Дискреционный<br>Ограничение по времени<br>Контроль процессов<br>Контроль печати<br>Полномочия<br>Аутентификация<br>Список токенов<br>Свойства пользователя<br>Контроль портов и CD<br>Механизмы: (В списке перечисляются только измененные механизмы)<br>Мандатное разграничение<br>Контроль целостности файлов<br>Очистка остаточной информации<br>Общие настройки<br>Сбор аудита<br>Контроль запуска<br>Политика аутентификации<br>Контроль целостности среды<br>Группы пользователей: (В списке перечисляются только измененные механизмы)<br><Имя группы пользователей> (Добавление / Удаление / Изменение)<br>Временные папки<br>Монопольный доступ<br>Дискреционный<br>Ограничение по времени<br>Контроль процессов<br>Контроль печати<br>Полномочия | | |

| | | | | | |
|---|---|---|---|---|---|
| | | | Аутентификация<br>Список токенов<br>Свойства пользователя<br>Контроль портов и CD<br>Механизмы: (В списке перечисляются только измененные механизмы)<br>Мандатное разграничение<br>Контроль целостности файлов<br>Очистка остаточной информации<br>Общие настройки<br>Сбор аудита<br>Контроль запуска<br>Политика аутентификации<br>Контроль целостности среды<br>Список машин:<br><Имя машины> (Удаление / Добавление) | | |

# Ограничение по времени

| Код события | Тип события | Уровень важности | Формат Windows-события | CEF-формат | Условие воспроизведения |
|---|---|---|---|---|---|
| 3332 (0xD04) | Отказ на вход пользователя из-за ограничений по времени | Предупреждение | Событие: отказ на вход пользователя из-за ограничений по времени<br>Пользователь: domain\login<br>SID пользователя:<br>Мандатная метка:<br>Режим работы СЗИ: мягкий режим \| полный функционал | Mon DD hh:mm:ss hostname<br>CEF:0\|GIS\|Blockhost-Net\|3.0<br>\|BH-TimeRestriction-3332\|Отказ на вход пользователя из-за ограничений по времени\|Medium\|<br>cat=Ограничения по времени<br>dhost=имя хоста источника события<br>rt=дата возникновения события на клиенте<br>cs4=содержимое поля ‘Мандатная метка’<br>cs4Label=Мандатная метка<br>cs1=содержимое поля ‘Режим работы СЗИ’<br>cs1Label=Режим работы СЗИ<br>suser=содержимое поля ‘Пользователь’<br>suid=содержимое поля ‘SID пользователя’<br>externalId=3332<br>categorySignificance=/Informational/Warning<br>categoryBehavior=/Access<br>categoryDeviceGroup=/Identity Management<br>catdt=Access and Identity Management<br>categoryOutcome=/Failure<br>categoryObject=/Host/Operating System | Событие формируется при входе пользователя в ОС в случае, если работа пользователя в ОС в этот момент времени не предусмотрена настройками механизма «Ограничение по времени». |
| 3957 (0xF75) | Блокировка сессии пользователя из-за | Предупреждение | Событие: блокировка сессии пользователя из-за нарушения | Mon DD hh:mm:ss hostname<br>CEF:0\|GIS\|Blockhost-Net\|3.0 | Событие формируется в случае, если во время |

| | | | | | |
|---|---|---|---|---|---|
| | нарушения ограничений по времени | | ограничений по времени<br>пользователя<br>Пользователь: domain\login<br>SID пользователя:<br>Мандатная метка:<br>Режим работы СЗИ: мягкий режим \| полный функционал | \|BH-TimeRestriction-3957\|Блокировка сессии пользователя из-за нарушения ограничений по времени\|Medium\|<br>cat=Ограничения по времени<br>dhost=имя хоста источника события<br>rt=дата возникновения события на клиенте<br>cs4=содержимое поля ‘Мандатная метка'<br>cs4Label=Мандатная метка<br>cs1=содержимое поля ‘Режим работы СЗИ’<br>cs1Label=Режим работы СЗИ<br>suser=содержимое поля ‘Пользователь’<br>suid=содержимое поля ‘SID пользователя’<br>externalId=3957<br>categorySignificance=/Informational/Warning<br>categoryBehavior=/Access/Stop<br>categoryDeviceGroup=/Identity Management<br>catdt=Access and Identity Management<br>categoryOutcome=/Success<br>categoryObject=/Host/Operating System | работы пользователя истек интервал времени, в течение которого пользователю разрешено работать в ОС. |

# Контроль целостности среды

## Контроль установки/удаления драйверов

| Код события | Тип события | Уровень важности | Формат Windows-события | CEF-формат | Условия воспроизведения |
|---|---|---|---|---|---|
| 3841 (0xF01) | Установка драйвера | Сведения | Событие: установка драйвера<br>Имя драйвера:<br>Путь к файлу:<br>Тип запуска: SERVICE_BOOT_START \| SERVICE_SYSTEM_START \| SERVICE_AUTO_START \| SERVICE_DEMAND_START \| SERVICE_DISABLED | Mon DD hh:mm:ss hostname<br>CEF:0\|GIS\|Blockhost-Net\|3.0\|BH-DriversControl-3841\|Установка драйвера\|Low\|<br>cat=Контроль целостности среды<br>dhost=имя хоста источника события<br>rt=дата возникновения события на клиенте<br>cs1=содержимое поля ‘Тип запуска’<br>cs1Label=Тип запуска драйвера<br>cs2=содержимое поля ‘Имя драйвера’<br>cs2Label=Имя драйвера<br>filepath=содержимое поля ‘Имя Объекта’<br>externalId=3841<br>categorySignificance=/Informational<br>categoryBehavior=/Modify/Configuration<br>categoryDeviceGroup=/Assessment Tools<br>catdt=Access and Identity Management | Регистрация (установка) нового драйвера в ОС |

| | | | | | |
|---|---|---|---|---|---|
| | | | | categoryOutcome=/Success<br>categoryObject=/Host/Operating System | |
| 3842<br>(0xF02) | Удаление драйвера | Сведения | Событие: удаление драйвера<br>Имя драйвера: | Mon DD hh:mm:ss hostname<br>CEF:0\|GIS\|Blockhost-Net\|3.0<br>\|BH-DriversControl-3842\|Удаление драйвера\|Low\|<br>cat=Контроль целостности среды<br>dhost=имя хоста источника события<br>rt=дата возникновения события на клиенте<br>cs2=содержимое поля ‘Имя драйвера’<br>cs2Label=Имя драйвера<br>externalId=3842<br>categorySignificance=/Informational<br>categoryBehavior=/Modify/Configuration<br>categoryDeviceGroup=/Assessment Tools<br>catdt=Access and Identity Management<br>categoryOutcome=/Success<br>categoryObject=/Host/Operating System | Разрегистрация (удаление) драйвера из ОС |
| 3843<br>(0xF03) | Изменение параметров драйвера | Сведения | Событие: изменение параметров драйвера<br>Имя драйвера:<br>Старый тип запуска:<br>SERVICE_BOOT_START \|<br>SERVICE_SYSTEM_START \|<br>SERVICE_AUTO_START \|<br>SERVICE_DEMAND_START \|<br>SERVICE_DISABLED<br>Новый тип запуска: <ключ запуска> \|<br>без изменений<br>Старый путь: <старый путь к драйверу><br>Новый путь: <новый путь к драйверу> \|<br>без изменений | Mon DD hh:mm:ss hostname<br>CEF:0\|GIS\|Blockhost-Net\|3.0<br>\|BH-DriversControl-3843\|Установка драйвера\|Low\|<br>cat=Контроль целостности среды<br>dhost=имя хоста источника события<br>rt=дата возникновения события на клиенте<br>cs1=содержимое поля ‘Старый тип запуска’<br>cs1Label=Тип запуска драйвера<br>cs2= содержимое поля ‘Имя драйвера’<br>cs2Label=Имя драйвера<br>cs3= содержимое поля ‘Новый тип запуска’<br>cs3Label=Новый тип запуска драйвера<br>oldFilePath=содержимое поля ‘Старый путь’<br>filepath=содержимое поля ‘Новый путь’<br>externalId=3843<br>categorySignificance=/Informational<br>categoryBehavior=/Modify/Configuration<br>categoryDeviceGroup=/Assessment Tools<br>catdt=Access and Identity Management<br>categoryOutcome=/Success<br>categoryObject=/Host/Operating System | Изменение одного или нескольких параметров одного из драйверов в ОС |

## Контроль установки/удаления служб

| Код | Тип события | Уровень | Формат Windows-события | CEF-формат | Условия |
|---|---|---|---|---|---|

| события | | важности | | | воспроизведения |
|---|---|---|---|---|---|
| 3846 (0xF06) | Установка службы | Сведения | Событие: установка службы<br>Имя службы:<br>Путь к файлу:<br>Тип запуска: SERVICE_BOOT_START \| SERVICE_SYSTEM_START \| Автоматически \| Вручную \| Отключено | Mon DD hh:mm:ss hostname CEF:0\|GIS\|Blockhost-Net\|3.0 \|BH-ServiceControl-3846\|Установка службы\|Low\| cat=Контроль целостности среды dhost=имя хоста источника события rt=дата возникновения события на клиенте cs2=содержимое поля ‘Тип запуска’ cs2Label=Тип запуска службы filepath=содержимое поля ‘Путь к файлу’ destinationServiceName=содержимое поля ‘Имя службы’ externalId=3846 categorySignificance=/Informational categoryBehavior=/Modify/Configuration categoryDeviceGroup=/Assessment Tools catdt=Access and Identity Management categoryOutcome=/Success categoryObject=/Host/Operating System | Регистрация (установка) новой службы в ОС |
| 3847 (0xF07) | Удаление службы | Сведения | Событие: удаление службы<br>Имя службы: | Mon DD hh:mm:ss hostname CEF:0\|GIS\|Blockhost-Net\|3.0 \|BH-ServiceControl-3847\|Удаление службы\|Low\| cat=Контроль целостности среды dhost=имя хоста источника события rt=дата возникновения события на клиенте destinationServiceName=содержимое поля ‘Имя службы’ externalId=3847 categorySignificance=/Informational categoryBehavior=/Modify/Configuration categoryDeviceGroup=/Assessment Tools catdt=Access and Identity Management categoryOutcome=/Success categoryObject=/Host/Operating System | Разрегистрация (удаление) службы из ОС |
| 3848 (0xF08) | Изменение параметров службы | Сведения | Событие: изменение параметров службы<br>Имя службы:<br>Старый тип запуска: SERVICE_BOOT_START \| SERVICE_SYSTEM_START \| Автоматически \| Вручную \| Отключено<br>Новый тип запуска: <ключ запуска> \| без изменений<br>Старый путь: <старый путь к службе><br>Новый путь: <новый путь к службе> \| без изменений | Mon DD hh:mm:ss hostname CEF:0\|GIS\|Blockhost-Net\|3.0 \|BH-ServiceControl-3848\|Изменение параметров службы\|Low\| cat=Контроль целостности среды dhost=имя хоста источника события rt=дата возникновения события на клиенте cs2=содержимое поля ‘Старый тип Запуска’ cs2Label=Тип запуска службы cs3=содержимое поля ‘Новый тип запуска’ cs3Label=Новый тип запуска службы | Изменение одного или нескольких параметров одной из служб в ОС |

| | | | | | |
|---|---|---|---|---|---|
| | | | | oldFilePath=содержимое поля ‘Старый путь’<br>filepath=содержимое поля ‘Новый путь’<br>destinationServiceName=содержимое поля ‘Имя службы’<br>externalId=3848<br>categorySignificance=/Informational<br>categoryBehavior=/Modify/Configuration<br>categoryDeviceGroup=/Assessment Tools<br>catdt=Access and Identity Management<br>categoryOutcome=/Success<br>categoryObject=/Host/Operating System | |

## Контроль установки/удаления приложений

| Код события | Тип события | Уровень важности | Формат Windows-события | CEF-формат | Условия воспроизведения |
|---|---|---|---|---|---|
| 3846 (0xF06) | Установка службы | Сведения | Событие: установка службы<br>Имя службы:<br>Путь к файлу:<br>Тип запуска: SERVICE_BOOT_START \| SERVICE_SYSTEM_START \| Автоматически \| Вручную \| Отключено | Mon DD hh:mm:ss hostname<br>CEF:0\|GIS\|Blockhost-Net\|3.0<br>\|BH-ServiceControl-3846\|Установка службы\|Low\|<br>cat=Контроль целостности среды<br>dhost=имя хоста источника события<br>rt=дата возникновения события на клиенте<br>cs2=содержимое поля ‘Тип запуска’<br>cs2Label=Тип запуска службы<br>filepath=содержимое поля ‘Путь к файлу’<br>destinationServiceName=содержимое поля ‘Имя службы’<br>externalId=3846<br>categorySignificance=/Informational<br>categoryBehavior=/Modify/Configuration<br>categoryDeviceGroup=/Assessment Tools<br>catdt=Access and Identity Management<br>categoryOutcome=/Success<br>categoryObject=/Host/Operating System | Регистрация (установка) новой службы в ОС |
| 3847 (0xF07) | Удаление службы | Сведения | Событие: удаление службы<br>Имя службы: | Mon DD hh:mm:ss hostname<br>CEF:0\|GIS\|Blockhost-Net\|3.0<br>\|BH-ServiceControl-3847\|Удаление службы\|Low\|<br>cat=Контроль целостности среды<br>dhost=имя хоста источника события<br>rt=дата возникновения события на клиенте<br>destinationServiceName=содержимое поля ‘Имя службы’<br>externalId=3847<br>categorySignificance=/Informational<br>categoryBehavior=/Modify/Configuration | Разрегистрация (удаление) службы из ОС |

| | | | | | |
|---|---|---|---|---|---|
| | | | | categoryDeviceGroup=/Assessment Tools<br>catdt=Access and Identity Management<br>categoryOutcome=/Success<br>categoryObject=/Host/Operating System | |
| 3848<br>(0xF08) | Изменение параметров службы | Сведения | Событие: изменение параметров службы<br>Имя службы:<br>Старый тип запуска:<br>SERVICE_BOOT_START \|<br>SERVICE_SYSTEM_START \|<br>Автоматически \| Вручную \| Отключено<br>Новый тип запуска: <ключ запуска> \|<br>без изменений<br>Старый путь: <старый путь к службе><br>Новый путь: <новый путь к службе> \|<br>без изменений | Mon DD hh:mm:ss hostname<br>CEF:0\|GIS\|Blockhost-Net\|3.0<br>\|BH-ServiceControl-3848\|Изменение параметров службы\|Low\|<br>cat=Контроль целостности среды<br>dhost=имя хоста источника события<br>rt=дата возникновения события на клиенте<br>cs2=содержимое поля ‘Старый тип Запуска’ cs2Label=Тип запуска службы<br>cs3=содержимое поля ‘Новый тип запуска’ cs3Label=Новый тип запуска службы<br>oldFilePath=содержимое поля ‘Старый путь’<br>filepath=содержимое поля ‘Новый путь’<br>destinationServiceName=содержимое поля ‘Имя службы’<br>externalId=3848<br>categorySignificance=/Informational<br>categoryBehavior=/Modify/Configuration<br>categoryDeviceGroup=/Assessment Tools<br>catdt=Access and Identity Management<br>categoryOutcome=/Success<br>categoryObject=/Host/Operating System | Изменение одного или нескольких параметров одной из служб в ОС |

## Контроль изменения перечня каталогов общего доступа

| Код события | Тип события | Уровень важности | Формат Windows-события | CEF-формат | Условия воспроизведения |
|---|---|---|---|---|---|
| 3846<br>(0xF06) | Установка службы | Сведения | Событие: установка службы<br>Имя службы:<br>Путь к файлу:<br>Тип запуска: SERVICE_BOOT_START \|<br>SERVICE_SYSTEM_START \|<br>Автоматически \| Вручную \| Отключено | Mon DD hh:mm:ss hostname<br>CEF:0\|GIS\|Blockhost-Net\|3.0<br>\|BH-ServiceControl-3846\|Установка службы\|Low\|<br>cat=Контроль целостности среды<br>dhost=имя хоста источника события<br>rt=дата возникновения события на клиенте<br>cs2=содержимое поля ‘Тип запуска’ cs2Label=Тип запуска службы<br>filepath=содержимое поля ‘Путь к файлу’<br>destinationServiceName=содержимое поля ‘Имя службы’<br>externalId=3846<br>categorySignificance=/Informational<br>categoryBehavior=/Modify/Configuration | Регистрация (установка) новой службы в ОС |

| | | | | | |
|---|---|---|---|---|---|
| | | | | categoryDeviceGroup=/Assessment Tools<br>catdt=Access and Identity Management<br>categoryOutcome=/Success<br>categoryObject=/Host/Operating System | |
| 3847<br>(0xF07) | Удаление службы | Сведения | Событие: удаление службы<br>Имя службы: | Mon DD hh:mm:ss hostname<br>CEF:0\|GIS\|Blockhost-Net\|3.0<br>\|BH-ServiceControl-3847\|Удаление службы\|Low\|<br>cat=Контроль целостности среды<br>dhost=имя хоста источника события<br>rt=дата возникновения события на клиенте<br>destinationServiceName=содержимое поля ‘Имя службы’<br>externalId=3847<br>categorySignificance=/Informational<br>categoryBehavior=/Modify/Configuration<br>categoryDeviceGroup=/Assessment Tools<br>catdt=Access and Identity Management<br>categoryOutcome=/Success<br>categoryObject=/Host/Operating System | Разрегистрация (удаление) службы из ОС |
| 3848<br>(0xF08) | Изменение параметров службы | Сведения | Событие: изменение параметров службы<br>Имя службы:<br>Старый тип запуска: SERVICE_BOOT_START \| SERVICE_SYSTEM_START \| Автоматически \| Вручную \| Отключено<br>Новый тип запуска: <ключ запуска> \| без изменений<br>Старый путь: <старый путь к службе><br>Новый путь: <новый путь к службе> \| без изменений | Mon DD hh:mm:ss hostname<br>CEF:0\|GIS\|Blockhost-Net\|3.0<br>\|BH-ServiceControl-3848\|Изменение параметров службы\|Low\|<br>cat=Контроль целостности среды<br>dhost=имя хоста источника события<br>rt=дата возникновения события на клиенте<br>cs2=содержимое поля ‘Старый тип Запуска’ cs2Label=Тип запуска службы<br>cs3=содержимое поля ‘Новый тип запуска’ cs3Label=Новый тип запуска службы<br>oldFilePath=содержимое поля ‘Старый путь’<br>filepath=содержимое поля ‘Новый путь’<br>destinationServiceName=содержимое поля ‘Имя службы’<br>externalId=3848<br>categorySignificance=/Informational<br>categoryBehavior=/Modify/Configuration<br>categoryDeviceGroup=/Assessment Tools<br>catdt=Access and Identity Management<br>categoryOutcome=/Success<br>categoryObject=/Host/Operating System | Изменение одного или нескольких параметров одной из служб в ОС |

## Контроль аппаратной среды

| Код события | Тип события | Уровень важности | Формат Windows-события | CEF-формат | Условия воспроизведения |
|---|---|---|---|---|---|
| 3862 (0xF16) | Замена процессора | Сведения | Событие: замена процессора<br>Старые параметры:<br>Название:<br>ИД в компьютере:<br>Новые параметры:<br>Название:<br>ИД в компьютере: | Mon DD hh:mm:ss hostname CEF:0\|GIS\|Blockhost-Net\|3.0 \|BH-HardwareControl-3862\|Замена процессора\|Low\| cat=Контроль целостности среды dhost=имя хоста источника события rt=дата возникновения события на клиенте cs1=Название:<Название>, ИД в компьютере:<ИД в компьютере> cs1Label=Старые параметры cs2= Название:<Название>, ИД в компьютере:<ИД в компьютере> cs2Label=Новые параметры externalId=3862 categorySignificance=/Informational categoryBehavior=/Modify/Configuration categoryDeviceGroup=/Assessment Tools catdt=Access and Identity Management categoryOutcome=/Success categoryObject=/Host/Operating System | Изменение параметров вычислительного процессора, установленного в компьютере. Например, замена процессора в компьютере. |
| 3863 (0xF17) | Замена материнской платы | Сведения | Событие: замена материнской платы<br>Старые параметры:<br>Модель:<br>Производитель:<br>ИД партии продукта:<br>ИД продукта:<br>Серийный номер:<br>Версия:<br>Новые параметры:<br>Модель:<br>Производитель:<br>ИД партии продукта:<br>ИД продукта:<br>Серийный номер:<br>Версия: | Mon DD hh:mm:ss hostname CEF:0\|GIS\|Blockhost-Net\|3.0 \|BH-HardwareControl-3863\|Замена материнской платы\|Low\| cat=Контроль целостности среды dhost=имя хоста источника события rt=дата возникновения события на клиенте cs1=Модель:<Модель>, Производитель:<Производитель>, ИД партии продукта:<ИД партии продукта>, ИД продукта:<ИД продукта>, Серийный номер:<Серийный номер>, Версия:<Версия> cs1Label=Старые параметры cs2=Модель:<Модель>, Производитель:<Производитель>, ИД партии продукта:<ИД партии продукта>, ИД продукта:<ИД продукта>, Серийный номер:<Серийный номер>, Версия:<Версия> cs2Label=Новые параметры externalId=3863 categorySignificance=/Informational categoryBehavior=/Modify/Configuration | Изменение параметров материнской платы, установленной в компьютере. Например, замена материнской платы в компьютере или перенос жесткого диска с установленным СЗИ на другой компьютер. |

| | | | | | |
|---|---|---|---|---|---|
| | | | | categoryDeviceGroup=/Assessment Tools<br>catdt=Access and Identity Management<br>categoryOutcome=/Success<br>categoryObject=/Host/Operating System | |
| 3864<br>(0xF18) | Добавление жесткого диска | Сведения | Событие: добавление жесткого диска<br>Параметры:<br>Модель:<br>Производитель:<br>Размер:<br>Серийный номер:<br>ИД ресурса:<br>ИД в компьютере:<br>Интерфейс: | Mon DD hh:mm:ss hostname<br>CEF:0\|GIS\|Blockhost-Net\|3.0<br>\|BH-HardwareControl-3864\|Добавление жесткого диска\|Low\|<br>cat=Контроль целостности среды<br>dhost=имя хоста источника события<br>rt=дата возникновения события на клиенте<br>cs3=Модель:<Модель>, Производитель:<Производитель>, Размер:<Размер>, Серийный номер:<Серийный номер>, ИД ресурса:<ИД ресурса>, ИД в компьютере:<ИД в компьютере>, Интерфейс:<Интерфейс><br>cs3Label=Параметры<br>externalId=3864<br>categorySignificance=/Informational<br>categoryBehavior=/Modify/Configuration<br>categoryDeviceGroup=/Assessment Tools<br>catdt=Access and Identity Management<br>categoryOutcome=/Success<br>categoryObject=/Host/Operating System | В компьютере был обнаружен жесткий диск с указанными параметрами. Например, в компьютер был установлен второй жесткий диск. |
| 3865<br>(0xF19) | Не удалось обнаружить жесткий диск | Сведения | Событие: не удалось обнаружить жесткий диск<br>Параметры:<br>Модель:<br>Производитель:<br>Размер:<br>Серийный номер:<br>ИД ресурса:<br>ИД в компьютере:<br>Интерфейс: | Mon DD hh:mm:ss hostname<br>CEF:0\|GIS\|Blockhost-Net\|3.0<br>\|BH-HardwareControl-3865\|Не удалось обнаружить жесткий диск\|Low\|<br>cat=Контроль целостности среды<br>dhost=имя хоста источника события<br>rt=дата возникновения события на клиенте<br>cs3=Модель:<Модель>, Производитель:<Производитель>, Размер:<Размер>, Серийный номер:<Серийный номер>, ИД ресурса:<ИД ресурса>, ИД в компьютере:<ИД в компьютере>, Интерфейс:<Интерфейс><br>cs3Label=Параметры<br>externalId=3865<br>categorySignificance=/Informational<br>categoryBehavior=/Modify/Configuration<br>categoryDeviceGroup=/Assessment Tools<br>catdt=Access and Identity Management<br>categoryOutcome=/Failure<br>categoryObject=/Host/Operating System | Из компьютера был удален жесткий диск с указанными параметрами. В случае наличия в компьютере нескольких жестких дисков, при удалении одного из них будет сформировано данное событие. |

| | | | | | |
|---|---|---|---|---|---|
| 3867 (0xF1B) | Добавление CD-привода | Сведения | Событие: добавление CD-привода<br>Параметры:<br>Производитель:<br>Серийный номер:<br>Тип носителей:<br>ИД в компьютере: | Mon DD hh:mm:ss hostname CEF:0\|GIS\|Blockhost-Net\|3.0 \|BH-HardwareControl-3867\|Добавление CD-привода\|Low\| cat=Контроль целостности среды dhost=имя хоста источника события rt=дата возникновения события на клиенте cs3=Производитель:<Производитель>, Серийный Номер:<Серийный Номер>, Тип носителей:<Тип носителей>, ИД в компьютере:<ИД в компьютере> cs3Label=Параметры externalId=3867 categorySignificance=/Informational categoryBehavior=/Modify/Configuration categoryDeviceGroup=/Assessment Tools catdt=Access and Identity Management categoryOutcome=/Success categoryObject=/Host/Operating System | В компьютере был обнаружен CD-привод с указанными параметрами. Например, в компьютер был установлен новый CD-привод. |
| 3868 (0xF1C) | Не удалось обнаружить CD-привод | Сведения | Событие: не удалось обнаружить CD-привод<br>Параметры:<br>Производитель:<br>Серийный номер:<br>Тип носителей:<br>ИД в компьютере: | Mon DD hh:mm:ss hostname CEF:0\|GIS\|Blockhost-Net\|3.0 \|BH-HardwareControl-3868 \|Не удалось обнаружить CD-привод\|Low\| cat=Контроль целостности среды dhost=имя хоста источника события rt=дата возникновения события на клиенте cs3=Производитель:<Производитель>, Серийный Номер:<Серийный Номер>, Тип носителей:<Тип носителей>, ИД в компьютере:<ИД в компьютере> cs3Label=Параметры externalId=3868 categorySignificance=/Informational categoryBehavior=/Modify/Configuration categoryDeviceGroup=/Assessment Tools catdt=Access and Identity Management categoryOutcome=/Failure categoryObject=/Host/Operating System | Из компьютера был удален CD-привод с указанными параметрами.<br>В случае наличия в компьютере одного или нескольких CD-приводов, при удалении одного из них будет сформировано данное событие. |
| 3870 (0xF1E) | Добавление сетевого адаптера | Сведения | Событие: добавление сетевого адаптера<br>Параметры:<br>Название:<br>Тип адаптера:<br>Производитель:<br>MAC адрес:<br>ИД в компьютере:<br>GUID: | Mon DD hh:mm:ss hostname CEF:0\|GIS\|Blockhost-Net\|3.0 \|BH-HardwareControl-3870\|Добавление сетевого адаптера\|Low\| cat=Контроль целостности среды dhost=имя хоста источника события rt=дата возникновения события на клиенте cs3=Название:<Название>, Тип адаптера:<Тип адаптера>, Производитель:<Производитель>, MAC | В компьютере был обнаружен сетевой адаптер с указанными параметрами. Например, в компьютер был установлен новый сетевой адаптер. |

| | | | | | |
|---|---|---|---|---|---|
| | | | | адрес:<MAC адрес>, ИД в компьютере:<ИД в компьютере>, GUID:<GUID> cs3Label=Параметры externalId=3870 categorySignificance=/Informational categoryBehavior=/Modify/Configuration categoryDeviceGroup=/Assessment Tools catdt=Access and Identity Management categoryOutcome=/Success categoryObject=/Host/Operating System | |
| 3871 (0xF1F) | Не удалось обнаружить сетевой адаптер | Сведения | Событие: не удалось обнаружить сетевой адаптер<br>Параметры:<br>Название:<br>Тип адаптера:<br>Производитель:<br>MAC адрес:<br>ИД в компьютере:<br>GUID: | Mon DD hh:mm:ss hostname CEF:0\|GIS\|Blockhost-Net\|3.0 \|BH-HardwareControl-3871\|Не удалось обнаружить сетевой адаптер\|Low\| cat=Контроль целостности среды dhost=имя хоста источника события rt=дата возникновения события на клиенте cs3= Название:<Название>, Тип адаптера:<Тип адаптера>, Производитель:<Производитель>, MAC адрес:<MAC адрес>, ИД в компьютере:<ИД в компьютере>, GUID:<GUID> externalId=3871 categorySignificance=/Informational categoryBehavior=/Modify/Configuration categoryDeviceGroup=/Assessment Tools catdt=Access and Identity Management categoryOutcome=/Failure categoryObject=/Host/Operating System | Из компьютера был удален сетевой адаптер с указанными параметрами. В случае наличия в компьютере одного или нескольких сетевых адаптеров, при удалении одного из них будет сформировано данное событие. |
| 3872 (0xF20) | Изменение параметров сетевого адаптера | Сведения | Событие: изменение параметров сетевого адаптера<br>Старые параметры:<br>Название:<br>Тип адаптера:<br>Производитель:<br>MAC адрес:<br>ИД в компьютере:<br>GUID:<br>Новые параметры:<br>Название:<br>Тип адаптера:<br>Производитель:<br>MAC адрес:<br>ИД в компьютере:<br>GUID: | Mon DD hh:mm:ss hostname CEF:0\|GIS\|Blockhost-Net\|3.0 \|BH-HardwareControl-3872\|Изменение параметров сетевого адаптера\|Low\| cat=Контроль целостности среды dhost=имя хоста источника события rt=дата возникновения события на клиенте cs1=Название:<Название>, Тип адаптера:<Тип адаптера>, Производитель:<Производитель>, MAC адрес:<MAC адрес>, ИД в компьютере:<ИД в компьютере>, GUID:<GUID> cs1Label=Старые параметры cs2=Название:<Название>, Тип адаптера:<Тип адаптера>, Производитель:<Производитель>, MAC адрес:<MAC адрес>, ИД в компьютере:<ИД в компьютере>, | Изменение параметров сетевого адаптера, установленного в компьютере. Например, замена одного сетевого адаптера на другой. |

| | | | | | |
|---|---|---|---|---|---|
| | | | | GUID:<GUID><br>cs2Label=Новые параметры<br>externalId=3872<br>categorySignificance=/Informational<br>categoryBehavior=/Modify/Configuration<br>categoryDeviceGroup=/Assessment Tools<br>catdt=Access and Identity Management<br>categoryOutcome=/Success | |
| 3873 (0xF21) | Замена видеоконтроллера | Сведения | Событие: замена видеоконтроллера<br>Старые параметры:<br>Название:<br>Объем памяти:<br>Видеопроцессор:<br>ИД в компьютере:<br>Новые параметры:<br>Название:<br>Объем памяти:<br>Видеопроцессор:<br>ИД в компьютере: | Mon DD hh:mm:ss hostname<br>CEF:0\|GIS\|Blockhost-Net\|3.0<br>\|BH-HardwareControl-3873\|Замена видеоконтроллера\|Low\|<br>cat=Контроль целостности среды<br>dhost=имя хоста источника события<br>rt=дата возникновения события на клиенте<br>cs1=Название:<Название>, Объем памяти:<Объем памяти>, Видеопроцессор:<Видеопроцессор>, ИД в компьютере:<ИД в компьютере><br>cs1Label=Старые параметры<br>cs2=Название:<Название>, Объем памяти:<Объем памяти>, Видеопроцессор:<Видеопроцессор>, ИД в компьютере:<ИД в компьютере><br>cs2Label=Новые параметры<br>externalId=3873<br>categorySignificance=/Informational<br>categoryBehavior=/Modify/Configuration<br>categoryDeviceGroup=/Assessment Tools<br>catdt=Access and Identity Management<br>categoryOutcome=/Success | Изменение параметров видеоконтроллера, установленного в компьютере. Например, замена одного контроллера на другой. |
| 3874 (0xF22) | Добавление модуля оперативной памяти | Сведения | Событие: добавление модуля оперативной памяти<br>Параметры:<br>Обозначение модуля:<br>Емкость:<br>Модель:<br>Название:<br>Производитель:<br>Серийный номер: | Mon DD hh:mm:ss hostname<br>CEF:0\|GIS\|Blockhost-Net\|3.0<br>\|BH-HardwareControl-3874\|Добавление модуля оперативной памяти\|Low\|<br>cat=Контроль целостности среды<br>dhost=имя хоста источника события<br>rt=дата возникновения события на клиенте<br>cs3=Обозначение модуля:<Обозначение модуля>, Емкость:<Емкость>, Модель:<Модель>, Название:<Название>, Производитель:<Производитель>, Серийный номер:<Серийный номер><br>cs3Label=Параметры<br>externalId=3874<br>categorySignificance=/Informational<br>categoryBehavior=/Modify/Configuration<br>categoryDeviceGroup=/Assessment Tools | Обнаружение нового модуля оперативной памяти в ОС. Событие может быть сформировано при обнаружении дополнительного модуля памяти (при увеличении объема памяти). Или при замене одного модуля памяти на другой. |

| | | | | | |
|---|---|---|---|---|---|
| | | | | catdt=Access and Identity Management<br>categoryOutcome=/Success | |
| 3875<br>(0xF23) | Не удалось обнаружить модуль оперативной памяти | Сведения | Событие: не удалось обнаружить модуль оперативной памяти<br>Параметры:<br>Обозначение модуля:<br>Емкость:<br>Модель:<br>Название:<br>Производитель:<br>Серийный номер: | Mon DD hh:mm:ss hostname<br>CEF:0\|GIS\|Blockhost-Net\|3.0<br>\|BH-HardwareControl-3875\|Не удалось обнаружить модуль оперативной памяти\|Low\|<br>cat=Контроль целостности среды<br>dhost=имя хоста источника события<br>rt=дата возникновения события на клиенте<br>cs3=Обозначение модуля:<Обозначение модуля>, Емкость:<Емкость>, Модель:<Модель>, Название:<Название>, Производитель:<Производитель>, Серийный номер:<Серийный номер><br>cs3Label=Параметры<br>externalId=3875<br>categorySignificance=/Informational<br>categoryBehavior=/Modify/Configuration<br>categoryDeviceGroup=/Assessment Tools<br>catdt=Access and Identity Management<br>categoryOutcome=/Failure | Из компьютера был удален модуль оперативной памяти. Событие будет сформировано при удалении одного из установленных в компьютере модулей. Либо при замене одного модуля памяти на другой. |

# Система развертывания

| Код события | Тип события | Уровень важности | Формат Windows-события | CEF-формат | Условия воспроизведения |
|---|---|---|---|---|---|
| 3585<br>(0xE01) | Создание задачи на установку агента системы развертывания | Сведения | Событие: создание задачи на установку агента системы развертывания<br>Имя задачи:<br>Имя инстал. пакета:<br>Дистрибутив:<br>Версия дистрибутива:<br>Параметры командной строки: | Конвертация в CEF отсутствует (событие не передается в SIEM-систему) | |
| 3586<br>(0xE02) | Создание задачи на установку произвольной программы | Сведения | Событие: создание задачи на установку произвольной программы<br>Имя задачи:<br>Имя инстал. пакета:<br>Дистрибутив:<br>Версия дистрибутива:<br>Параметры командной строки: | Конвертация в CEF отсутствует (событие не передается в SIEM-систему) | |
| 3587<br>(0xE03) | Создание задачи на удаление Блокхост-Сеть | Сведения | Событие: создание задачи на удаление Блокхост-Сеть Клиент | Конвертация в CEF отсутствует (событие не передается в SIEM- | |

| | | | | | |
|---|---|---|---|---|---|
| | Клиент | | Имя задачи: | систему) | |
| 3588 (0xE04) | Создание задачи на удаление программы, установленной с помощью системы развертывания | Сведения | Событие: создание задачи на удаление программы из списка инст. пакетов<br>Имя задачи:<br>Имя инстал. пакета:<br>Дистрибутив:<br>Версия дистрибутива:<br>Параметры командной строки: | Конвертация в CEF отсутствует (событие не передается в SIEM-систему) | |
| 3589 (0xE05) | Создание задачи на удаление программы командным скриптом | Сведения | Событие: создание задачи на удаление программы командным скриптом<br>Имя задачи:<br>Файл скрипта:<br>Параметры командной строки: | Конвертация в CEF отсутствует (событие не передается в SIEM-систему) | |
| 3590 (0xE06) | Редактирование задачи на установку агента системы развертывания | Сведения | Событие: редактирование задачи на установку агента системы развертывания<br>Имя задачи: | Конвертация в CEF отсутствует (событие не передается в SIEM-систему) | |
| 3591 (0xE07) | Редактирование задачи на установку произвольной программы | Сведения | Событие: редактирование задачи на установку произвольной программы<br>Имя задачи: | Конвертация в CEF отсутствует (событие не передается в SIEM-систему) | |
| 3592 (0xE08) | Редактирование задачи на удаление БлокхостСеть Клиент | Сведения | Событие: редактирование задачи на удаление БлокхостСеть Клиент<br>Имя задачи: | Конвертация в CEF отсутствует (событие не передается в SIEM-систему) | |
| 3593 (0xE09) | Редактирование задачи на удаление программы из списка инст. пакетов | Сведения | Событие: редактирование задачи на удаление программы из списка инст. пакетов<br>Имя задачи: | Конвертация в CEF отсутствует (событие не передается в SIEM-систему) | |
| 3594 (0xE0A) | Редактирование задачи на удаление программы командным скриптом | Сведения | Событие: редактирование задачи на удаление программы командным скриптом<br>Имя задачи: | Конвертация в CEF отсутствует (событие не передается в SIEM-систему) | |
| 3595 (0xE0B) | Удаление задачи на установку агента системы развертывания | Сведения | Событие: удаление задачи на установку агента системы развертывания<br>Имя задачи: | Конвертация в CEF отсутствует (событие не передается в SIEM-систему) | |
| 3596 (0xE0C) | Удаление задачи на установку произвольной программы | Сведения | Событие: удаление задачи на установку произвольной программы<br>Имя задачи: | Конвертация в CEF отсутствует (событие не передается в SIEM-систему) | |
| 3597 (0xE0D) | Удаление задачи на удаление БлокхостСеть | Сведения | Событие: удаление задачи на удаление БлокхостСеть Клиент | Конвертация в CEF отсутствует (событие не передается в SIEM- | |

| | | | | | |
|---|---|---|---|---|---|
| | Клиент | | Имя задачи: | систему) | |
| 3598 (0xE0E) | Удаление задачи на удаление программы из списка инст. пакетов | Сведения | Событие: удаление задачи на удаление программы из списка инст. пакетов<br>Имя задачи: | Конвертация в CEF отсутствует (событие не передается в SIEM-систему) | |
| 3599 (0xE0F) | Удаление задачи на удаление программы командным скриптом | Сведения | Событие: удаление задачи на удаление программы командным скриптом<br>Имя задачи: | Конвертация в CEF отсутствует (событие не передается в SIEM-систему) | |
| 3600 (0xE10) | Запуск задачи на установку агента системы развертывания | Сведения | Событие: запуск задачи на установку агента системы развертывания<br>Имя задачи:<br>Имя инстал. пакета:<br>Дистрибутив:<br>Версия дистрибутива:<br>Параметры командной строки: | Конвертация в CEF отсутствует (событие не передается в SIEM-систему) | |
| 3601 (0xE11) | Запуск задачи на установку произвольной программы | Сведения | Событие: запуск задачи на установку произвольной программы<br>Имя задачи:<br>Имя инстал. пакета:<br>Дистрибутив:<br>Версия дистрибутива:<br>Параметры командной строки: | Конвертация в CEF отсутствует (событие не передается в SIEM-систему) | |
| 3602 (0xE12) | Запуск задачи на удаление БлокхостСеть Клиент | Сведения | Событие: запуск задачи на удаление БлокхостСеть Клиент<br>Имя задачи: | Конвертация в CEF отсутствует (событие не передается в SIEM-систему) | |
| 3603 (0xE13) | Запуск задачи на удаление программы из списка инст. пакетов | Сведения | Событие: запуск задачи на удаление программы из списка инст. пакетов<br>Имя задачи:<br>Имя инстал. пакета:<br>Дистрибутив:<br>Версия дистрибутива:<br>Параметры командной строки: | Конвертация в CEF отсутствует (событие не передается в SIEM-систему) | |
| 3604 (0xE14) | Запуск задачи на удаление программы командным скриптом | Сведения | Событие: запуск задачи на удаление программы командным скриптом<br>Имя задачи:<br>Файл скрипта:<br>Параметры командной строки: | Конвертация в CEF отсутствует (событие не передается в SIEM-систему) | |
| 3605 (0xE15) | Остановка задачи на установку агента системы развертывания | Сведения | Событие: остановка задачи на установку агента системы развертывания<br>Имя задачи: | Конвертация в CEF отсутствует (событие не передается в SIEM-систему) | |
| 3606 | Остановка задачи на | Сведения | Событие: остановка задачи на | Конвертация в CEF отсутствует | |

| | | | | | |
|---|---|---|---|---|---|
| (0xE16) | установку произвольной программы | | установку произвольной программы<br>Имя задачи: | (событие не передается в SIEM-систему) | |
| 3607 (0xE17) | Остановка задачи на удаление БлокхостСеть Клиент | Сведения | Событие: остановка задачи на удаление БлокхостСеть Клиент<br>Имя задачи: | Конвертация в CEF отсутствует (событие не передается в SIEM-систему) | |
| 3608 (0xE18) | Остановка задачи на удаление программы из списка инст. пакетов | Сведения | Событие: остановка задачи на удаление программы из списка инст. пакетов<br>Имя задачи: | Конвертация в CEF отсутствует (событие не передается в SIEM-систему) | |
| 3609 (0xE19) | Остановка задачи на удаление программы командным скриптом | Сведения | Событие: остановка задачи на удаление программы командным скриптом<br>Имя задачи: | Конвертация в CEF отсутствует (событие не передается в SIEM-систему) | |
| 3610 (0xE1A) | Создание инсталляционного пакета | Сведения | Событие: создание инсталляционного пакета<br>Имя пакета:<br>Дистрибутив:<br>Версия дистрибутива:<br>Параметры командной строки: | Конвертация в CEF отсутствует (событие не передается в SIEM-систему) | |
| 3611 (0xE1B) | Редактирование инсталляционного пакета | Сведения | Событие: редактирование инсталляционного пакета<br>Имя пакета:<br>Дистрибутив:<br>Версия дистрибутива:<br>Параметры командной строки: | Конвертация в CEF отсутствует (событие не передается в SIEM-систему) | |
| 3612 (0xE1C) | Удаление инсталляционного пакета | Сведения | Событие: удаление инсталляционного пакета<br>Имя пакета: | Конвертация в CEF отсутствует (событие не передается в SIEM-систему) | |

# Специальные (custom) поля CEF

| Имя поля | Название (лэйбл) поля | Категории использования специального поля | Описание специального поля |
|---|---|---|---|
| Cs1 | cs1Label=Режим работы СЗИ | Временные ограничения Контроль печати Контроль целостности файлов Очистка остаточной информации Контроль портов Дискреционный доступ Контроль процессов Контроль запуска программ Аутентификация | Режим функционирования СЗИ: мягкий или полный функционал. Мягкий режим – особый режим функционирования СЗИ, в котором настройки безопасности отключены и отрабатывают только на уровне аудита их выполнения. Полный функционал - нормальный режим работы СЗИ при котором все настройки безопасности отрабатывают штатно. |
| Cs1 | cs1Label=Тип консоли | События клиента СЗИ | Консоль - источник события. Консоль, с который было произведено изменение настроек или инициировано |

| | | | |
|---|---|---|---|
| | | | появления события аудита |
| Cs1 | cs1Label=Привилегии администратора | Действия администратора | Уровень доступа администратора консоли СЗИ. Есть два уровня доступа в версии Блокхост-сеть 3.0 – аудитор (только чтение) и администратор (полный доступ). |
| Cs1 | cs1Label=Дополнительная информация | Служебные события | Дополнительная информация служебного события. |
| Cs1 | cs1Label=Тип запуска драйвера | Контроль среды | Тип запуска драйвера, поставленного на контроль. |
| Cs1 | cs1Label=Старые параметры | Контроль среды – Контроль аппаратной конфигурации | Старые параметры при изменении конфигурации аппаратных устройств контролируемого компьютера. |
| Cs2 | cs2Label=Тип аутентификации | Аутентификация | Тип аутентификации БХС. Параметр может принимать следующие значения в зависимости от режима входа пользователя: аутентификация по токену, аутентификация по паролю СЗИ, аутентификация windows. |
| Cs2 | cs2Label=Привилегии доступа | Дискреционный доступ | Привилегии доступа пользователя при доступе к файловому ресурсу. |
| Cs2 | cs2Label=Имя порта | Контроль портов | Идентификатор устройства контроля портов. |
| Cs2 | cs2Label=Имя принтера | Контроль печати | Имя принтера, на котором был распечатан документ. |
| Cs2 | cs2Label=Изменения конфигурации | События клиента СЗИ Действия администратора | Перечь изменений конфигурации СЗИ, которые произвел администратор при изменениях настроек. |
| Cs2 | cs2Label=Тип запуска службы | Контроль среды - Контроль установки/удаления служб | Тип запуска контролируемой службы |
| Cs2 | cs2Label=UUID программы | Контроль среды - Контроль установки/удаления программ | UUID установленной программы |
| Cs2 | cs2Label=Имя драйвера | Контроль среды - Контроль установки/удаления драйверов | Имя драйвера в ОС |
| Cs2 | cs2Label=Имя общего ресурса | Контроль среды - Контроль изменения перечня каталогов общего доступа | Имя каталога, к которому обеспечен общий доступ |
| Cs2 | cs2Label=Новые  параметры | Контроль среды – Контроль аппаратной конфигурации | Новые параметры при изменении конфигурации аппаратных устройств контролируемого компьютера |
| Cs3 | cs3Label=Идентификатор токена | Аутентификация События клиента СЗИ | Аппаратный идентификатор токена двухфакторной аутентификации |
| Cs3 | cs3Label=Тип доступа | Дискреционный доступ | Тип доступа пользователя к файловому ресурсу |
| Cs3 | cs3Label=Новый тип запуска службы | Контроль среды - Контроль установки/удаления служб | Обновленный тип запуска контролируемой службы |
| Cs3 | cs3Label=Новая версия программы | Контроль среды - Контроль установки/удаления программ | Новая версия программы после изменения |

| | | | |
|---|---|---|---|
| Cs3 | cs3Label=Новое имя общего ресурса | Контроль среды - Контроль изменения перечня каталогов общего доступа | Имя общего ресурса после изменения |
| Cs3 | cs3Label=Параметры | Контроль среды – Контроль аппаратной конфигурации | Перечень параметров конфигурации аппаратных устройств контролируемого компьютера |
| Cs4 | cs4Label=Мандатная метка | Временные ограничения Контроль печати Дискреционный доступ Аутентификация | Мандатная метка пользователя |
| Cs4 | cs4Label=Имя программы | Контроль среды - Контроль установки/удаления программ | Имя программы, поставленной на контроль |
| Cs4 | cs4Label=Новый путь | Контроль среды - Контроль изменения перечня каталогов общего доступа | Новый путь к общему ресурсу |
| Cs5 | cs5Label=Мандатная метка ресурса | Дискреционный доступ Контроль печати | Мандатная метка ресурса |
| Cs5 | cs5Label=Примечание | Контроль среды - Контроль изменения перечня каталогов общего доступа | Описание ресурса общего доступа |
| Cs6 | cs6Label=Имя токена | Аутентификация События клиента СЗИ | Идентификатор токена двухфакторной аутентификации |