GIS ГАЗИНФОРМ СЕРВИС

Средство защиты информации от несанкционированного доступа «Блокхост-Сеть 4»

Руководство администратора безопасности
Часть 2. Развертывание и аудит
Приложение 1

Санкт-Петербург, 2024

Содержание

Введение

Настоящее приложение предназначено для администраторов средства защиты информации от несанкционированного доступа «Блокхост-Сеть 4» и содержит описание списка фиксируемых событий СЗИ от НСД «Блокхост-Сеть 4» под управлением ОС Windows/Linux и описание списка фиксируемых событий СДЗ «SafeNode System Loader».

1 Список регистрируемых событий СЗИ от НСД «Блокхост-Сеть 4»

1.1 Дискреционный доступ

Код события	Тип события	Уровень важности	ОС	Формат события ОС	CEF-формат	Условие воспроизведения
257 (0x101)	Доступ к файловому объекту	Сведения	Windows	Событие: доступ к файловому объекту Пользователь: домен\логин SID пользователя: Метка пользователя: Имя объекта: Метка объекта: Имя процесса: Тип доступа: Привилегии: [запись]|[чтение]|[исполнение] Режим работы СЗИ: мягкий режим | полный функционал ОС клиента:	Mon DD hh:mm:ss hostname CEF:0|GIS|Blockhost-Net|4.4|BH-DiscretAccess-257|Доступ к файловому объекту|Low| cat=Дискреционное управление доступом dhost=имя хоста источника события rt=дата возникновения события на клиенте cs1=содержимое поля ‘Метка пользователя’ cs1label=Мандатная метка пользователя cs2=содержимое поля ‘Метка объекта’ cs2Label=мандатная метка объекта cs3=содержимое поля ‘Тип доступа’ cs3Label=Тип доступа cs4=содержимое поля ‘Привилегии’ cs4Label=Привилегии cs5=содержимое поля ‘ОС клиента’ cs5Label=ОС клиента filepath=содержимое поля ‘Имя Объекта’ sproc=содержимое поля ‘Имя процесса’ suser=содержимое поля ‘Пользователь’ suid=содержимое поля ‘SID пользователя msg=содержимое поля «Режим работы СЗИ»’ externalId=257 categorySignificance=/Informational	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).

					categoryBehavior=/Access/Start categoryDeviceGroup=/Identity Management catdt=Access and Identity Management categoryOutcome=/Success categoryObject=/Host/Resource/File	
258 (0x102)	Отказ на доступ к файловому объекту	Предупреждение	Windows	Событие: отказ на доступ к файловому объекту Пользователь: SID пользователя: Метка пользователя: Имя объекта: Метка объекта: Имя процесса: ип доступа: Привилегии: [запись]|[чтение]|[исполнение] Режим работы СЗИ: мягкий режим | полный функционал ОС клиента:	Mon DD hh:mm:ss hostname CEF:0|GIS|Blockhost-Net|4.4|BH-DiscretAccess-258|Отказ на доступ к файловому объекту|Medium| cat=Дискреционное управление доступом dhost=имя хоста источника события rt=дата возникновения события на клиенте cs1=содержимое поля ‘Метка пользователя’ cs1label=Мандатная метка пользователя cs2=содержимое поля ‘Метка объекта’ cs2Label=мандатная метка объекта cs3=содержимое поля ‘Тип доступа’ cs3Label=Тип доступа cs4=содержимое поля ‘Привилегии’ cs4Label=Привилегии cs5=содержимое поля ‘ОС клиента’ cs5Label=ОС клиента filepath=содержимое поля ‘Имя Объекта’ sproc=содержимое поля ‘Имя процесса’ suser=содержимое поля ‘Пользователь’ suid=содержимое поля ‘SID пользователя’ msg=содержимое поля «Режим работы СЗИ externalId=258 categorySignificance=/Informational/Warning	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 записи).

					categoryBehavior=/Access categoryDeviceGroup=/Identity Management catdt=Access and Identity Management categoryOutcome=/Failure categoryObject=/Host/Resource/File	

1.2 Запуск приложений

Код события	Тип события	Уровень важности	ОС	Формат события ОС	CEF-формат	Условия воспроизведения
3877 (0xF25)	Запуск процесса	Сведения	Windows	Событие: запуск процесса Процесс: Пользователь: домен\логин SID пользователя: Режим работы СЗИ: мягкий режим | полный функционал ОС клиента:	Mon DD hh:mm:ss hostname CEF:0|GIS|Blockhost-Net|4.4 |BH-AppLaunch-3877|Запуск процесса|Low| cat=Запуск исполняемых файлов dhost=имя хоста источника события rt=дата возникновения события на клиенте cs1=содержимое поля ‘ОС клиента’ cs1Label=ОС клиента suser=содержимое поля ‘Пользователь’ suid=содержимое поля ‘SID пользователя’ sproc=содержимое поля ‘Процесс’ msg=содержимое поля ‘Режим работы СЗИ’ externalId=3877 categorySignificance=/Informational categoryBehavior=/Access/Start categoryDeviceGroup=/Identity Management catdt=Access and Identity Management categoryOutcome=/Success categoryObject=/Host/Resource/File	Выполнение запуска одного из процессов, контролируемого СЗИ.
3878 (0xF26)	Завершение процесса	Сведения	Windows	Событие: завершение процесса Процесс: Пользователь: домен\логин SID пользователя: Режим работы СЗИ: мягкий режим | полный функционал ОС клиента:	Mon DD hh:mm:ss hostname CEF:0|GIS|Blockhost-Net|4.4 |BH-AppLaunch-3878|Завершение процесса|Low| cat=Запуск исполняемых файлов dhost=имя хоста источника события rt=дата возникновения события на клиенте cs1=содержимое поля ‘ОС клиента’ cs1Label=ОС клиента suser=содержимое поля ‘Пользователь’ suid=содержимое поля ‘SID пользователя’ sproc=содержимое поля ‘Процесс’ msg=содержимое поля ‘Режим работы СЗИ’ externalId=3878 categorySignificance=/Informational categoryBehavior=/Access/Stop categoryDeviceGroup=/Identity Management	Завершение работы одного из процессов, контролируемого СЗИ.

					catdt=Access and Identity Management categoryOutcome=/Success categoryObject=/Host/Resource/File	
3876 (0xF24)	Отказ на запуск процесса	Предупреждение	Windows	Событие: отказ за запуск процесса Причина: отказ по политике замкнутой среды Процесс: Пользователь: домен\логин SID пользователя: Режим работы СЗИ: мягкий режим | полный функционал ОС клиента:	Mon DD hh:mm:ss bhhostname CEF:0|GIS|Blockhost-Net|4.4 |BH-AppLaunch-3876|Отказ на запуск процесса|Medium| cat=Запуск исполняемых файлов dhost=имя хоста источника события rt=дата возникновения события на клиенте cs1=содержимое поля 'ОС клиента' cs1Label=ОС клиента reason=содержимое поля 'Причина' suser=содержимое поля 'Пользователь' suid=содержимое поля 'SID пользователя' sproc=содержимое поля 'Процесс' msg=содержимое поля 'Режим работы СЗИ' externalId=3876 categorySignificance=/Informational/Warning categoryBehavior=/Access/Stop categoryDeviceGroup=/Identity Management catdt=Access and Identity Management categoryOutcome=/Failure categoryObject=/Host/Resource/File	Событие аудита формируется, если настройки механизма «Замкнутая программная среда» не предполагают возможности запуска процесса соответствующим пользователем.

1.3 Аудит доступа к медиафайлам

Код события	Тип события	Уровень важности	ОС	Формат события ОС	CEF-формат	Условия воспроизведения
3879 (0xF27)	Доступ к файлу	Сведения	Windows	Событие: доступ к файлу Процесс: Файл: Пользователь: домен\логин SID пользователя: Режим работы СЗИ: мягкий режим | полный функционал ОС клиента:	Mon DD hh:mm:ss hostname CEF:0|GIS|Blockhost-Net|4.4 |BH-MediaAccess-3879|Доступ к файлу|Low| cat=Аудит доступа к медиафайлам dhost=имя хоста источника события rt=дата возникновения события на клиенте cs1=содержимое поля 'ОС клиента' cs1Label=ОС клиента suser=содержимое поля 'Пользователь' suid=содержимое поля 'SID пользователя' sproc=содержимое поля 'Процесс' filename=содержимое поля Файл msg=содержимое поля 'Режим работы СЗИ' externalId=3879 categorySignificance=/Informational categoryBehavior=/Access/Start categoryDeviceGroup=/Identity Management catdt=Access and Identity Management categoryOutcome=/Success categoryObject=/Host/Resource/File	Получение доступа к файлу определенного типа (аудио, видео или изображение). Аудит ведется для всех файлов типа.

1.4 Управление входом в ОС

Код события	Тип события	Уровень важности	ОС	Формат события ОС	CEF-формат	Условия воспроизведения
1029 (0x405)	Выход пользователя из системы	Сведения	Windows	Событие: выход пользователя из системы Пользователь: домен\логин SID пользователя: Метка пользователя: Режим работы СЗИ: мягкий режим | полный функционал ОС клиента:	Mon DD hh:mm:ss hostname CEF:0|GIS|Blockhost-Net|4.4 |BH-Auth- 1029|Выход пользователя из системы|Low| cat=Вход в ОС dhost=имя хоста источника события rt=дата возникновения события на клиенте cs1=содержимое поля ‘Метка пользователя’ cs1Label=Мандатная метка пользователя cs5=содержимое поля ‘ОС клиента’ cs5Label=ОС клиента suser=содержимое поля ‘Пользователь’ suid=содержимое поля ‘SID пользователя’ msg=содержимое поля ‘Режим работы СЗИ’ externalId=1029 categorySignificance=/Informational categoryBehavior=/Access/Stop categoryDeviceGroup=/Identity Management catdt=Access and Identity Management categoryOutcome=/Success categoryObject=/Host/Operating System	Выход пользователя из ОС (завершение сеанса пользователя).
3880 (0xF28)	Локальный вход в систему	Сведения	Windows, Linux	Событие: локальный вход в систему Пользователь: домен\логин SID пользователя: Метка пользователя: Выбранный тип входа: Пароль | Сертификат | БВПП Фактический тип входа: Доверять ОС | По токену | По паролю | Нет данных | Нет прав на вход Серийный номер токена: Режим работы СЗИ: мягкий режим | полный функционал ОС клиента:	Mon DD hh:mm:ss hostname CEF:0|GIS|Blockhost-Net|4.4 |BH-Auth- 3880|Локальный вход в систему|Low| cat=Вход в ОС dhost=имя хоста источника события rt=дата возникновения события на клиенте cs1=содержимое поля ‘Метка пользователя’ cs1Label=Мандатная метка пользователя cs2=содержимое поля ‘Выбранный тип входа’ cs2Label=Тип аутентификации cs3=содержимое поля ‘Серийный номер токена’ cs3Label=Серийный номер токена cs4=содержимое поля ‘Фактический тип входа’ cs4Label=Фактический тип входа cs5=содержимое поля ‘ОС клиента’ cs5Label=ОС клиента suser=содержимое поля ‘Пользователь’ suid=содержимое поля ‘SID пользователя’ msg=содержимое поля ‘Режим работы СЗИ’ externalId=3880	Успешный интерактивный вход пользователя в ОС. Поле ‘Серийный номер токена’ имеет значение только в случае, если вход выполняется по токену.

					categorySignificance=/Informational categoryBehavior=/Access/Start categoryDeviceGroup=/Identity Management catdt=Access and Identity Management categoryOutcome=/Success categoryObject=/Host/Operating System	
3881 (0xF29)	Отказ на локальный вход в систему	Предупреждение	Windows, Linux	Событие: отказ на локальный вход в систему Причина: пароль не соответствует политике аутентификации СЗИ | <другие причины> Пользователь: домен\логин SID пользователя: Метка пользователя: Выбранный тип входа: Пароль | Сертификат | БВПП Фактический тип входа: Доверять ОС | По токену | По паролю | Нет данных | Нет прав на вход Серийный номер токена: Режим работы СЗИ: мягкий режим | полный функционал ОС клиента:	Mon DD hh:mm:ss hostname CEF:0|GIS|Blockhost-Net|4.4 |BH-Auth- 3881|Отказ на локальный вход в систему|Medium| cat=Вход в ОС dhost=имя хоста источника события rt=дата возникновения события на клиенте cs1=содержимое поля ‘Метка пользователя’ cs1Label=Мандатная метка пользователя cs2=содержимое поля ‘Выбранный тип входа’ cs2Label=Тип аутентификации cs3=содержимое поля ‘Серийный номер токена’ cs3Label=Серийный номер токена cs4=содержимое поля ‘Фактический тип входа’ cs4Label=Фактический тип входа cs5=содержимое поля ‘ОС клиента’ cs5Label=ОС клиента reason=содержимое поля ‘Причина’ suser=содержимое поля ‘Пользователь’ suid=содержимое поля ‘SID пользователя’ msg=содержимое поля ‘Режим работы СЗИ’ externalId=3881 categorySignificance=/Informational/Warning categoryBehavior=/Authorization/Verify categoryDeviceGroup=/Identity Management catdt=Access and Identity Management categoryOutcome=/Failure categoryObject=/Host/Operating System	Блокировка интерактивного входа пользователя в ОС по следующим причинам: • неправильный пароль, токен или пинкод; • несоответствие политикам ОС или БХС; • отсутствие пользователя или его группы в консоли БХС; • блокировка пользователя администратором. Поле ‘Серийный номер токена’ имеет значение только в случае, если вход выполняется по токену.
3888 (0xF30)	Вход в систему по RDP	Сведения	Windows	Событие: вход в систему по RDP Пользователь: домен\логин SID пользователя: Метка пользователя: Выбранный тип входа: Пароль | Сертификат | БВПП Фактический тип входа: Доверять ОС | По токену | По паролю | Нет данных | Нет прав на вход Серийный номер токена: Режим работы СЗИ: мягкий режим | полный функционал	Mon DD hh:mm:ss hostname CEF:0|GIS|Blockhost-Net|4.4 |BH-Auth-3888|Вход в систему по RDP|Low| cat=Вход в ОС dhost=имя хоста источника события rt=дата возникновения события на клиенте cs1=содержимое поля ‘Метка пользователя’ cs1Label=Мандатная метка пользователя cs2=содержимое поля ‘Выбранный тип входа’ cs2Label=Тип аутентификации cs3=содержимое поля ‘Серийный номер	Успешный вход пользователя в систему с помощью RDP-сессии. Поле ‘Серийный номер токена’ имеет значение только в случае, если вход выполняется по токену.

				ОС клиента:	токена’ cs3Label=Серийный номер токена cs4=содержимое поля ‘Фактический тип входа’ cs4label=Фактический тип входа cs5=содержимое поля ‘ОС клиента’ cs5Label=ОС клиента suser=содержимое поля ‘Пользователь’ suid=содержимое поля ‘SID пользователя’ msg=содержимое поля ‘Режим работы СЗИ’ externalId=3888 categorySignificance=/Informational categoryBehavior=/Access/Start categoryDeviceGroup=/Identity Management catdt=Access and Identity Management categoryOutcome=/Success categoryObject=/Host/Operating System	
3889 (0xF31)	Отказ на вход в систему по RDP	Предупреждение	Windows	Событие: отказ на вход в систему по RDP Причина: пароль не соответствует политике аутентификации СЗИ | <другие причины> Пользователь: домен\логин SID пользователя: Метка пользователя: Выбранный тип входа: Пароль | Сертификат | БВПП Фактический тип входа: Доверять ОС | По токену | По паролю | Нет данных | Нет прав на вход) Серийный номер токена: Режим работы СЗИ: мягкий режим | полный функционал ОС клиента:	Mon DD hh:mm:ss hostname CEF:0|GIS|Blockhost-Net|4.4 |BH-Auth-3889|Отказ на вход в систему по RDP|Medium| cat=Вход в ОС dhost=имя хоста источника события rt=дата возникновения события на клиенте cs1=содержимое поля ‘Метка пользователя’ cs1Label=Мандатная метка пользователя cs2=содержимое поля ‘Выбранный тип входа’ cs2Label=Тип аутентификации cs3=содержимое поля ‘Серийный номер токена’ cs3Label=Серийный номер токена cs4=содержимое поля ‘Фактический тип входа’ cs4label=Фактический тип входа cs5=содержимое поля ‘ОС клиента’ cs5Label=ОС клиента reason=содержимое поля ‘Причина’ suser=содержимое поля ‘Пользователь’ suid=содержимое поля ‘SID пользователя’ msg=содержимое поля ‘Режим работы СЗИ’ externalId=3889 categorySignificance=/Informational/Warning categoryBehavior=/Authentication/Verify categoryDeviceGroup=/Identity Management catdt=Access and Identity Management categoryOutcome=/Failure categoryObject=/Host/Operating System	Блокировка входа пользователя в ОС по RDP по любой из следующих причин: • неправильный пароль, токен или пинкод; • несоответствие политикам ОС или БХС; • отсутствие пользователя или его группы в консоли БХС; • блокировка пользователя администратором. Поле ‘Серийный номер токена’ имеет значение только в случае, если вход выполняется по токену.
3890 (0xF32)	Доступ к сетевому ресурсу	Сведения	Windows	Событие: доступ к ресурсу с совместным доступом по сети	Mon DD hh:mm:ss hostname CEF:0|GIS|Blockhost-Net|4.4	Доступ к сетевым ресурсам (принтеры, сканеры и т.д.) с других

				Пользователь: домен\логин SID пользователя: Метка пользователя: Режим работы СЗИ: мягкий режим | полный функционал ОС клиента:	|BH-Auth-3890|Доступ к ресурсу с совместным доступом по сети|Low| cat=Вход в ОС dhost=имя хоста источника события rt=дата возникновения события на клиенте cs1=содержимое поля 'Метка пользователя' cs1Label=Мандатная метка пользователя cs5=содержимое поля 'ОС клиента' cs5Label=ОС клиента suser=содержимое поля 'Пользователь' suid=содержимое поля 'SID пользователя' msg=содержимое поля 'Режим работы СЗИ' externalId=3890 categorySignificance=/Informational categoryBehavior=/Access categoryDeviceGroup=/Identity Management catdt=Access and Identity Management categoryOutcome=/Success categoryObject=/Host/Operating System	узлов сети. Событие формируется на узле, на котором находится ресурс общего доступа.
3891 (0xF33)	Отказ на доступ к сетевому ресурсу	Предупреждение	Windows	Событие: отказ на доступ к ресурсу с совместным доступом по сети Причина: пароль не соответствует политике аутентификации СЗИ | <другие причины> Пользователь: домен\логин SID пользователя: Метка пользователя: Режим работы СЗИ: мягкий режим | полный функционал ОС клиента:	Mon DD hh:mm:ss hostname CEF:0|GIS|Blockhost-Net|4.4 |BH-Auth-3891|Отказ на доступ к ресурсу с совместным доступом по сети|Medium| cat=Вход в ОС dhost=имя хоста источника события rt=дата возникновения события на клиенте cs1=содержимое поля 'Метка пользователя' cs1Label=Мандатная метка пользователя cs5=содержимое поля 'ОС клиента' cs5Label=ОС клиента reason=содержимое поля 'Причина' suser=содержимое поля 'Пользователь' suid=содержимое поля 'SID пользователя' msg=содержимое поля 'Режим работы СЗИ' externalId=3891 categorySignificance=/Informational/Warning categoryBehavior=/Authentication/Verify categoryDeviceGroup=/Identity Management catdt=Access and Identity Management categoryOutcome=/Failure categoryObject=/Host/Operating System	Отказ на доступ к сетевым ресурсам (принтеры, сканеры и т.д.) с других узлов сети. Событие формируется на узле, на котором находится ресурс общего доступа.
3892 (0xF34)	Аутентификация через RunAs или открытие сессии	Сведения	Windows	Событие: аутентификация через RunAs Пользователь: домен\логин SID пользователя: Метка пользователя: Режим работы СЗИ: мягкий режим | полный функционал ОС клиента:	Mon DD hh:mm:ss hostname CEF:0|GIS|Blockhost-Net|4.4 |BH-Auth-3892|Аутентификация через RunAs|Low| cat=Вход в ОС dhost=имя хоста источника события rt=дата возникновения события на клиенте cs1=содержимое поля 'Метка пользователя' cs1Label=Мандатная метка пользователя	Успешный запуск приложения от имени другого пользователя («Запуск от имени…»).

					cs5=содержимое поля ‘ОС клиента’ cs5Label=ОС клиента suser=содержимое поля ‘Пользователь’ suid=содержимое поля ‘SID пользователя’ msg=содержимое поля ‘Режим работы СЗИ’ externalId=3892 categorySignificance=/Informational categoryBehavior=/Access/Start categoryDeviceGroup=/Identity Management catdt=Access and Identity Management categoryOutcome=/Success categoryObject=/Host/Operating System	
3893 (0xF35)	Отказ на аутентификацию через RunAs или открытие сессии	Предупреждение	Windows	Событие: отказ на аутентификацию через RunAs Причина: Пользователь: домен\логин SID пользователя: Метка пользователя: Режим работы СЗИ: мягкий режим | полный функционал ОС клиента:	Mon DD hh:mm:ss hostname CEF:0|GIS|Blockhost-Net|4.4 |BH-Auth- 3893|Отказ на аутентификацию через RunAs |Medium| cat=Вход в ОС dhost=имя хоста источника события rt=дата возникновения события на клиенте cs1=содержимое поля ‘Метка пользователя’ cs1Label=Мандатная метка пользователя cs5=содержимое поля ‘ОС клиента’ cs5Label=ОС клиента suser=содержимое поля ‘Пользователь’ suid=содержимое поля SID пользователя msg=содержимое поля ‘Режим работы СЗИ’ externalId=3893 categorySignificance=/Informational/Warning categoryBehavior=/Authentication/Verify categoryDeviceGroup=/Identity Management catdt=Access and Identity Management categoryOutcome=/Failure categoryObject=/Host/Operating System	Отказ на запуск приложения от имени другого пользователя («Запуск от имени…»).
3894 (0xF36)	Пользователь приостановил сеанс работы на компьютере	Сведения	Windows	Событие: пользователь приостановил сеанс работы на компьютере Пользователь: домен\логин SID пользователя: Метка пользователя: Режим работы СЗИ: мягкий режим | полный функционал ОС клиента:	Mon DD hh:mm:ss hostname CEF:0|GIS|Blockhost-Net|4.4 |BH-Auth-3894|Пользователь приостановил сеанс работы на компьютере|Low| cat=Вход в ОС dhost=имя хоста источника события rt=дата возникновения события на клиенте cs1=содержимое поля ‘Метка пользователя’ cs1Label=Мандатная метка пользователя cs5=содержимое поля ‘ОС клиента’ cs5Label=ОС клиента suser=содержимое поля ‘Пользователь’ suid=содержимое поля ‘SID пользователя’ externalId=3894 msg=содержимое поля ‘Режим работы СЗИ’ categorySignificance=/Informational	Блокировка сессии пользователя по требованию пользователя или средствами СЗИ.

					categoryBehavior=/Access/Stop categoryDeviceGroup=/Identity Management catdt=Access and Identity Management categoryOutcome=/Success categoryObject=/Host/Operating System	
3895 (0xF37)	Пользователь возобновил сеанс работы на компьютере	Сведения	Windows	Событие: пользователь возобновил сеанс работы на компьютере Пользователь: домен\логин SID пользователя: Метка пользователя: Выбранный тип входа: Пароль | Сертификат | БВПП Фактический тип входа: Доверять ОС | По токену | По паролю | Нет данных | Нет прав на вход Серийный номер токена: Режим работы СЗИ: мягкий режим | полный функционал ОС клиента:	Mon DD hh:mm:ss hostname CEF:0|GIS|Blockhost-Net|4.4 |BH-Auth-3895|Пользователь возобновил сеанс работы на компьютере|Low| cat=Вход в ОС dhost=имя хоста источника события rt=дата возникновения события на клиенте cs1=содержимое поля ‘Метка пользователя’ cs1Label=Мандатная метка пользователя cs2=содержимое поля ‘Выбранный тип входа’ cs2Label=Тип аутентификации cs3=содержимое поля ‘Серийный номер токена’ cs3Label=Серийный номер токена cs4=содержимое поля ‘Фактический тип входа’ cs4Label=Фактический тип входа cs5=содержимое поля ‘ОС клиента’ cs5Label=ОС клиента suser=содержимое поля ‘Пользователь’ suid=содержимое поля ‘SID пользователя’ externalId=3895 msg=содержимое поля ‘Режим работы СЗИ’ categorySignificance=/Informational/Warning categoryBehavior=/Access/Start categoryDeviceGroup=/Identity Management catdt=Access and Identity Management categoryOutcome=/Success	Возобновление заблокированной сессии пользователя. Поле ‘Серийный номер токена’ имеет значение только в случае, если вход выполняется по токену.
3896 (0xF38)	Отказ в возобновлении сеанса пользователя	Предупреждение	Windows	Событие: отказ в возобновлении сеанса пользователя Причина: пароль не соответствует требованиям безопасности | <другие причины> Пользователь: домен\логин SID пользователя: Метка пользователя: Выбранный тип входа: Пароль | Сертификат | БВПП Фактический тип входа: Доверять ОС | По токену | По паролю | Нет данных | Нет прав на вход Серийный номер токена: Режим работы СЗИ: мягкий	Mon DD hh:mm:ss hostname CEF:0|GIS|Blockhost-Net|4.4 |BH-Auth-3896|Отказ в возобновлении сеанса пользователя|High| cat=Вход в ОС dhost=имя хоста источника события rt=дата возникновения события на клиенте cs1=содержимое поля ‘Метка пользователя’ cs1Label=Мандатная метка пользователя cs2=содержимое поля ‘Выбранный тип входа’ cs2Label=Тип аутентификации cs3=содержимое поля ‘Серийный номер токена’ cs3Label=Серийный номер токена cs4=содержимое поля ‘Фактический тип	Отказ в возобновлении сеанса пользователя. Возможные причины отказа: • пароль/пинкод токена не отвечают требованием политики СЗИ; • пароль/пинкод токена некорректен, пользователь предоставил неверный токен; • пользователь не предоставил токен. Поле ‘Серийный номер токена’ имеет значение только в случае, если вход выполняется по токену.

				режим | полный функционал ОС клиента:	входа' cs4Label=Фактический тип входа cs5=содержимое поля 'ОС клиента' cs5Label=ОС клиента reason=содержимое поля 'Причина' suser=содержимое поля 'Пользователь' suid=содержимое поля 'SID пользователя' msg=содержимое поля 'Режим работы СЗИ' externalId=3896 categorySignificance=/Informational/Error categoryBehavior=/Authorization/Verify categoryDeviceGroup=/Identity Management catdt=Access and Identity Management categoryOutcome=/Failure categoryObject=/Host/Operating System	
3897 (0xF39)	Смена пароля пользователя	Сведения	Windows, Linux	Событие: смена пароля пользователя Пользователь: домен\логин SID пользователя: Выбранный тип входа: Пароль | Сертификат | БВПП Фактический тип входа: Доверять ОС | По токену | По паролю | Нет данных | Нет прав на вход Серийный номер токена: Инициатор смены пароля: пользователь | Блокхост-сеть Режим работы СЗИ: мягкий режим | полный функционал ОС клиента:	Mon DD hh:mm:ss hostname CEF:0|GIS|Blockhost-Net|4.4 |BH-Auth- 3897|Сменапароляпользователя|Low| cat=Вход в ОС dhost=имя хоста источника события rt=дата возникновения события на клиенте cs2=содержимое поля 'Выбранный тип входа' cs2Label=Тип аутентификации cs3=содержимое поля 'Серийный номер токена' cs3Label=Серийный номер токена cs4=содержимое поля 'Фактический тип входа' cs4Label=Фактический тип входа cs5=содержимое поля 'ОС клиента' cs5Label=ОС клиента suser=содержимое поля 'Инициатор' duser=содержимое поля 'Пользователь' suid=содержимое поля 'SID пользователя' msg=содержимое поля 'Режим работы СЗИ' externalId=3897 categorySignificance=/Informational categoryBehavior=/Authentication/Modify categoryDeviceGroup=/Identity Management catdt=Access and Identity Management categoryOutcome=/Success categoryObject=/Host/Operating System	Смена пароля пользователя на клиентском компьютере. Смена пароля может быть выполнена в следующих случаях: • при входе пользователя в ОС; • по требованию пользователя (ctrl+alt+del); • автоматическая смена по требованию политики СЗИ при использовании режима безопасного входа по паролю
3904 (0xF40)	Отказ при смене пароля пользователя	Предупреждение	Windows, Linux	Событие: отказ при смене пароля пользователя Причина: пароль не соответствует политике аутентификации СЗИ | <другие причины>	Mon DD hh:mm:ss hostname CEF:0|GIS|Blockhost-Net|4.4 |BH-Auth-3904|Отказ при смене пароля пользователя|High| cat=Вход в ОС dhost=имя хоста источника события	Отказ на смену пароля пользователя на клиентском компьютере. Смена пароля может быть выполнена в следующих случаях: • при входе пользователя в ОС;

				Пользователь: домен\логин SID пользователя: Выбранный тип входа: Пароль | Сертификат | БВПП Фактический тип входа: Доверять ОС | По токену | По паролю | Нет данных | Нет прав на вход Серийный номер токена: Инициатор смены пароля: пользователь | Блокхост-сеть Режим работы СЗИ: мягкий режим | полный функционал ОС клиента:	rt=дата возникновения события на клиенте cs2=содержимое поля 'Выбранный тип входа' cs2Label=Тип аутентификации cs3=содержимое поля 'Серийный номер токена' cs3Label=Серийный номер токена cs4=содержимое поля 'Фактический тип входа' cs4Label=Фактический тип входа cs5=содержимое поля 'ОС клиента' cs5Label=ОС клиента reason=содержимое поля 'Причина' suser=содержимое поля 'Инициатор' duser=содержимое поля 'Пользователь' suid=содержимое поля 'SID пользователя' msg=содержимое поля 'Режим работы СЗИ' externalId=3904 categorySignificance=/Informational/Error categoryBehavior=/Authentication/Modify categoryDeviceGroup=/Identity Management catdt=Access and Identity Management categoryOutcome=/Failure categoryObject=/Host/Operating System	• по требованию пользователя (ctrl+alt+del) ; • администратором СЗИ через клиентскую или серверную консоль СЗИ • автоматическая смена по требованию политики СЗИ при использовании режима безопасного входа по паролю
3905 (0xF41)	Смена пин-кода токена	Сведения	Windows, Linux	Событие: смена пин-кода токена Пользователь: домен\логин Серийный номер токена: Режим работы СЗИ: мягкий режим | полный функционал ОС клиента:	Mon DD hh:mm:ss hostname CEF:0|GIS|Blockhost-Net|4.4 |BH-Auth-3905|Смена пин-кода токена|Low| cat=Вход в ОС dhost=имя хоста источника события rt=дата возникновения события на клиенте cs3=содержимое поля 'Серийный номер токена' cs3Label=Серийный номер токена cs5=содержимое поля 'ОС клиента' cs5Label=ОС клиента suser=содержимое поля 'Пользователь' msg=содержимое поля 'Режим работы СЗИ' externalId=3905 categorySignificance=/Informational categoryBehavior=/Authentication/Modify categoryDeviceGroup=/Identity Management catdt=Access and Identity Management categoryOutcome=/Success categoryObject=/Host/Resource	Смена пин-кода токена на клиентском компьютере. Смена пароля может быть выполнена в следующих случаях: • при входе пользователя в ОС; • по требованию пользователя (ctrl+alt+del)
3906 (0xF42)	Отказ при смене пин-кода токена	Предупреждение	Windows, Linux	Событие: отказ при смене пин-кода токена Причина: Пользователь: домен\логин Серийный номер токена: Режим работы СЗИ: мягкий	Mon DD hh:mm:ss hostname CEF:0|GIS|Blockhost-Net|4.4 |BH-Auth-3906|Отказ при смене пин-кода токена|High| cat=Вход в ОС dhost=имя хоста источника события	Отказ на смену пин-кода токена на клиентском компьютере. Смена пароля может быть выполнена в следующих случаях: • при входе пользователя в ОС; • по требованию пользователя

				режим | полный функционал ОС клиента:	rt=дата возникновения события на клиенте cs3=содержимое поля ‘Серийный номер токена’ cs3Label=Серийный номер токена cs5=содержимое поля ‘ОС клиента’ cs5Label=ОС клиента reason=содержимое поля ‘Причина’ suser=содержимое поля ‘Пользователь’ msg=содержимое поля ‘Режим работы СЗИ’ externalId=3906 categorySignificance=/Informational/Error categoryBehavior=/Authentication/Modify categoryDeviceGroup=/Identity Management catdt=Access and Identity Management categoryOutcome=/Failure categoryObject=/Host/Resource	(ctrl+alt+del)
3991 (0xF97)	Запись безопасного пароля пользователя на токен	Сведения	Windows, Linux	Событие: запись безопасного пароля пользователя на токен Пользователь: домен\логин SID пользователя: Серийный номер токена: Режим работы СЗИ: мягкий режим | полный функционал ОС клиента:	Mon DD hh:mm:ss hostname CEF:0|GIS|Blockhost-Net|4.4 |BH-Auth-3991|Запись безопасного пароля пользователя на токен|Low| cat=Вход в ОС dhost=имя хоста источника события rt=дата возникновения события на клиенте cs3=содержимое поля ‘Серийный номер токена’ cs3Label=Серийный номер токена cs5=содержимое поля ‘ОС клиента’ cs5Label=ОС клиента suser=содержимое поля ‘Пользователь’ suid=содержимое поля ‘SID пользователя’ msg=содержимое поля ‘Режим работы СЗИ’ externalId=3991 categorySignificance=/Informational categoryBehavior=/Authorization/Modify categoryDeviceGroup=/Identity Management catdt=Access and Identity Management categoryOutcome=/Success categoryObject=/Host/Operating System	Запись безопасного пароля пользователя на токен происходит в следующих случаях: - когда пользователь первый раз использует токен для безопасного входа по паролю - когда необходимо перезаписать безопасный пароль на токене (срок действия пароля истек, пароль был сброшен администратором безопасности, смена пароля пользователем по Ctrl-Alt-Delete)
3992 (0xF98)	Отказ при записи безопасного пароля пользователя на токен	Ошибка	Windows, Linux	Событие: отказ при записи безопасного пароля пользователя на токен Причина: Пользователь: домен\логин SID пользователя: Серийный номер токена: Режим работы СЗИ: мягкий режим | полный функционал ОС клиента:	Mon DD hh:mm:ss hostname CEF:0|GIS|Blockhost-Net|4.4 |BH-Auth-3992|Отказ при записи безопасного пароля пользователя на токен |High| cat=Вход в ОС dhost=имя хоста источника события rt=дата возникновения события на клиенте cs3=содержимое поля ‘Серийный номер токена’ cs3Label=Серийный номер токена cs5=содержимое поля ‘ОС клиента’	Событие формируется в случае, если процесс формирования безопасного пароля или его записи на токен закончился неудачей.

					cs5Label=ОС клиента reason=содержимое поля ‘Причина’ suser=содержимое поля ‘Пользователь’ suid=содержимое поля ‘SID пользователя’ msg=содержимое поля ‘Режим работы СЗИ’ externalId=3992 categorySignificance=Informational/Error categoryBehavior=/Authorization/Modify categoryDeviceGroup=/Identity Management catdt=Access and Identity Management categoryOutcome=/Error categoryObject=/Host/Operating System	
3993 (0xF99)	Переход пользователя на безопасный вход по паролю	Сведения	Windows, Linux	Событие: переход пользователя на безопасный вход по паролю Пользователь: домен\логин SID пользователя: Серийный номер токена: Режим работы СЗИ: мягкий режим | полный функционал ОС клиента:	Mon DD hh:mm:ss hostname CEF:0|GIS|Blockhost-Net|4.4 |BH-Auth-3993|Переход пользователя на безопасный вход по паролю|Low| cat=Вход в ОС dhost=имя хоста источника события rt=дата возникновения события на клиенте cs3=содержимое поля ‘Серийный номер токена’ cs3Label=Серийный номер токена cs5=содержимое поля ‘ОС клиента’ cs5Label=ОС клиента поля ‘Пользователь’ suid=содержимое поля ‘SID пользователя’ msg=содержимое поля ‘Режим работы СЗИ’ externalId=3993 categorySignificance=/Informational categoryBehavior=/Authorization/Modify categoryDeviceGroup=/Identity Management catdt=Access and Identity Management categoryOutcome=/Success categoryObject=/Host/Operating System	Смена пин-кода токена Событие формируется, когда токен с безопасным паролем в первый раз используется пользователем для входа в ОС.
3994 (0xF9A)	Отказ при переходе пользователя на безопасный вход по паролю	Ошибка	Windows, Linux	Событие: отказ при переходе пользователя на безопасный вход по паролю Причина: Пользователь: домен\логин SID пользователя: Серийный номер токена: Режим работы СЗИ: мягкий режим | полный функционал ОС клиента:	Mon DD hh:mm:ss hostname CEF:0|GIS|Blockhost-Net|4.4 |BH-Auth-3994|Отказ при переходе пользователя на безопасный вход по паролю|High| cat=Вход в ОС dhost=имя хоста источника события rt=дата возникновения события на клиенте cs3=содержимое поля ‘Серийный номер токена’ cs3Label=Серийный номер токена cs5=содержимое поля ‘ОС клиента’ cs5Label=ОС клиента reason=содержимое поля ‘Причина’ suser=содержимое поля ‘Пользователь’ suid=содержимое поля ‘SID пользователя’	Событие формируется, если процесс первоначального создания контейнера с безопасным паролем на токене завершился ошибкой.

					msg=содержимое поля ‘Режим работы СЗИ’ externalId=3994 categorySignificance=Informational/Error categoryBehavior=/Authorization/Modify categoryDeviceGroup=/Identity Management catdt=Access and Identity Management categoryOutcome=/Error categoryObject=/Host/Operating System	
4055 (0xFD7)	Завершение сеанса доступа	Сведения	Linux	Событие: завершение сеанса доступа Пользователь: домен\логин SID пользователя: Режим работы СЗИ: мягкий режим | полный функционал ОС клиента: Причина: извлечение токена Серийный номер токена: Идентификатор сеанса:	Mon DD hh:mm:ss hostname CEF:0|GIS|Blockhost-Net|4.4 |BH-Auth-4055|Завершение сеанса доступа|Low| cat=Вход в ОС dhost=имя хоста источника события rt=дата возникновения события на клиенте cs3=содержимое поля ‘Серийный номер токена’ cs3Label=Серийный номер токена cs5=содержимое поля ‘ОС клиента’ cs5Label=ОС клиента reason=содержимое поля ‘Причина’ suser=содержимое поля ‘Пользователь’ suid=содержимое поля ‘SID пользователя’ msg=содержимое поля ‘Режим работы СЗИ’ externalId=4055 categorySignificance=/Informational categoryBehavior=/Access/Stop categoryDeviceGroup=/Identity Management catdt=Access and Identity Management categoryOutcome=/Success categoryObject=/Host/Operating System	Сеанс завершен по причине извлечения токена
4056 (0xFD8)	Блокирование сеанса доступа	Сведения	Linux	Событие: блокирование сеанса доступа Пользователь: домен\логин SID пользователя: Режим работы СЗИ: мягкий режим | полный функционал ОС клиента: Причина: извлечение токена Серийный номер токена: Идентификатор сеанса:	Mon DD hh:mm:ss hostname CEF:0|GIS|Blockhost-Net|4.4 |BH-Auth-4056|Блокирование сеанса доступа |Low| cat=Вход в ОС dhost=имя хоста источника события rt=дата возникновения события на клиенте cs3=содержимое поля ‘Серийный номер токена’ cs3Label=Серийный номер токена cs5=содержимое поля ‘ОС клиента’ cs5Label=ОС клиента reason=содержимое поля ‘Причина’ suser=содержимое поля ‘Пользователь’ suid=содержимое поля ‘SID пользователя’ msg=содержимое поля ‘Режим работы СЗИ’ externalId=4056 categorySignificance=/Informational categoryBehavior=/Access/Stop	Сеанс заблокирован по причине извлечения токена

					categoryDeviceGroup=/Identity Management catdt=Access and Identity Management categoryOutcome=/Success categoryObject=/Host/Operating System	

1.5 Контроль устройств

Код события	Тип события	Уровень важности	ОС	Формат события ОС	CEF-формат	Условия воспроизведения
1028 (0x403)	Включение USB-устройства	Сведения	Windows	Событие: включение USB-устройства Тип устройства: <класс USB-устройства> Идентификатор: VID&PID/Serial Путь устройства: Метка устройства: Режим работы СЗИ: мягкий режим | полный функционал ОС клиента:	Mon DD hh:mm:ss hostname CEF:0|GIS|Blockhost-Net|4.4 |BH-DeviceControl-1028|Включение USB-устройства|Low| cat=Контроль устройств dhost=имя хоста источника события rt=дата возникновения события на клиенте cs1=содержимое поля 'Тип устройства' cs1Label=Тип устройства cs2=содержимое поля 'Идентификатор' cs2Label=Идентификатор устройства cs3=содержимое поля 'Метка устройства' cs3Label=Метка устройства cs5=содержимое поля 'ОС клиента' cs5Label=ОС клиента filepath=содержимое поля 'Путь устройства' msg=содержимое поля 'Режим работы СЗИ' externalId=1028 categorySignificance=/Informational categoryBehavior=/Access/Start categoryDeviceGroup=/Identity Management catdt=Access and Identity Management categoryOutcome=/Success categoryObject=/Host/Resource	USB-устройство идентифицировано ОС
1027 (0x404)	Отключение USB-устройства	Предупреждение	Windows	Событие: отключение USB-устройства Тип устройства: <класс USB-устройства> Идентификатор: VID&PID/Serial Путь устройства: Метка устройства: Режим работы СЗИ: мягкий режим | полный функционал ОС клиента:	Mon DD hh:mm:ss hostname CEF:0|GIS|Blockhost-Net|4.4 |BH-DeviceControl-1027|Отключение USB-устройства|Medium| cat=Контроль устройств dhost=имя хоста источника события rt=дата возникновения события на клиенте cs1=содержимое поля 'Тип устройства' cs1Label=Тип устройства cs2=содержимое поля 'Идентификатор' cs2Label=Идентификатор устройства cs3=содержимое поля 'Метка устройства' cs3Label=Метка устройства cs5=содержимое поля 'ОС клиента' cs5Label=ОС клиента filepath=содержимое поля 'Путь устройства'	USB-устройство отключено

					msg=содержимое поля ‘Режим работы СЗИ’ externalId=1027 categorySignificance=/Informational/Warning categoryBehavior=/Access categoryDeviceGroup=/Identity Management catdt=Access and Identity Management categoryOutcome=/Failure categoryObject=/Host/Resource	
1030 (0x406)	Доступ к USB-устройству разрешен	Сведения	Windows	Событие: доступ к USB-устройству разрешен Тип устройства: <класс USB-устройства> Идентификатор: VID&PID/Serial Путь устройства: Метка устройства: Пользователь: SID пользователя: Метка пользователя: Тип доступа: чтение | запись Файл: Режим работы СЗИ: мягкий режим | полный функционал ОС клиента:	Mon DD hh:mm:ss hostname CEF:0|GIS|Blockhost-Net|4.4 |BH-DeviceControl-1030|Доступ к USB-устройству разрешен|Low| cat=Контроль устройств dhost=имя хоста источника события rt=дата возникновения события на клиенте cs1=содержимое поля ‘Тип устройства’ cs1Label=Тип устройства cs2=содержимое поля ‘Идентификатор’ cs2Label=Идентификатор устройства cs3=содержимое поля ‘Метка устройства’ cs3Label=Метка устройства cs4=содержимое поля ‘Тип доступа’ cs4Label=Тип доступа cs5=содержимое поля ‘ОС клиента’ cs5Label=ОС клиента filepath=содержимое поля ‘Путь устройства’ filename=содержимое поля ‘Файл’ suser=содержимое поля ‘Пользователь’ msg=содержимое поля ‘Режим работы СЗИ’ externalId=1030 categorySignificance=/Informational categoryBehavior=/Access/Start categoryDeviceGroup=/Identity Management catdt=Access and Identity Management categoryOutcome=/Success categoryObject=/Host/Resource	Событие формируется в случае успешного доступа пользователя к устройствам, относящихся к классам «Устройства хранения данных» и «Переносные устройств (WPD)». Поле «Файл» заполняется только для устройств класса «Устройства хранения данных».
1031 (0x407)	Доступ к USB-устройству запрещен	Предупреждение	Windows	Событие: доступ к USB-устройству запрещен Тип устройства: <класс USB-устройства> Идентификатор: VID&PID/Serial Путь устройства: Метка устройства: Пользователь: SID пользователя: Метка пользователя: Тип доступа: чтение | запись Файл: Режим работы СЗИ: мягкий режим | полный функционал	Mon DD hh:mm:ss hostname CEF:0|GIS|Blockhost-Net|4.4 |BH-DeviceControl-1031|Доступ к USB-устройству запрещен|Medium| cat=Контроль устройств dhost=имя хоста источника события rt=дата возникновения события на клиенте cs1=содержимое поля ‘Тип устройства’ cs1Label=Тип устройства cs2=содержимое поля ‘Идентификатор’ cs2Label=Идентификатор устройства cs3=содержимое поля ‘Метка устройства’ cs3Label=Метка устройства cs4=содержимое поля ‘Тип доступа’	Событие формируется в случае отказа на доступ пользователя к устройствам, относящихся к классам «Устройства хранения данных» и «Переносные устройств (WPD)». Поле «Файл» заполняется только для устройств класса «Устройства хранения данных».

				ОС клиента:	cs4Label=Тип доступа cs5=содержимое поля ‘ОС клиента’ cs5Label=ОС клиента filepath=содержимое поля ‘Путь устройства’ filename=содержимое поля ‘Файл’ suser=содержимое поля ‘Пользователь’ msg=содержимое поля ‘Режим работы СЗИ’ externalId=1031 categorySignificance=/Informational/Warning categoryBehavior=/Access categoryDeviceGroup=/Identity Management catdt=Access and Identity Management categoryOutcome=/Failure categoryObject=/Host/Resource	

1.6 Очистка оперативной памяти

Код события	Тип события	Уровень важности	ОС	Формат события ОС	CEF-формат	Условия воспроизведения
1537 (0x601)	Очистка памяти процесса	Сведения	Windows	Событие: очистка памяти процесса Имя процесса: Путь: Режим работы СЗИ: мягкий режим | полный функционал ОС клиента:	Mon DD hh:mm:ss hostname CEF:0|GIS|Blockhost-Net|4.4 |BH-MemoryClean-1537|Очистка памяти процесса|Low| cat=Очистка оперативной памяти dhost=имя хоста источника события rt=дата возникновения события на клиенте cs1=содержимое поля ‘ОС клиента’ cs1Label=ОС клиента sproc=содержимое поля ‘Имя процесса’ msg=содержимое поля ’Режим работы СЗИ’ externalId=1537 categorySignificance=/Informational categoryBehavior=/Delete categoryDeviceGroup=/Data Security catdt=Access and Identity Management categoryOutcome=/Success categoryObject=/Host/Application	Очистка памяти процесса после завершения работы процесса, указанного в перечне обрабатываемых файлов подсистемы очистки остаточной информации.
1539 (0x603)	Не удалось запустить очистку памяти	Ошибка	Linux	Событие: Не удалось запустить очистку памяти Причина: Режим работы СЗИ:	Mon DD hh:mm:ss hostname CEF:0|GIS|Blockhost-Net|4.4 |BH-MemoryClean-1539| Не удалось запустить очистку памяти |High| cat=Очистка оперативной памяти dhost=имя хоста источника события rt=дата возникновения события на клиенте msg=содержимое поля ’Режим работы СЗИ’ externalId=1539 categorySignificance=/Informational/Error categoryBehavior=/Error categoryDeviceGroup=/Data Security	ОП не работает по указанной причине.

					catdt=Access and Identity Management categoryOutcome=/Failure categoryObject=/Host/Application	
1540 (0x604)	Фатальный сбой при загрузке модуля контроля памяти	Ошибка	Linux	Событие: Фатальный сбой при загрузке модуля контроля памяти Действие:	Mon DD hh:mm:ss hostname CEF:0|GIS|Blockhost-Net|4.4 |BH-MemoryClean-1540| Фатальный сбой при загрузке модуля контроля памяти |High| cat=Очистка оперативной памяти dhost=имя хоста источника события rt=дата возникновения события на клиенте externalId=1540 categorySignificance=/Informational/Error categoryBehavior=/Error categoryDeviceGroup=/Data Security catdt=Access and Identity Management categoryOutcome=/Failure categoryObject=/Host/Application	Фатальная ошибка при инициализации ОП во время предыдущего запуска, инициализация не завершена.

1.7 Гарантированное удаление файлов

Код события	Тип события	Уровень важности	ОС	Формат события ОС	CEF-формат	Условия воспроизведения
769 (0x301)	Гарантированное удаление файлового объекта	Сведения	Windows	Событие: гарантированное удаление файлового объекта Пользователь: домен\логин SID пользователя: Имя объекта: Режим работы СЗИ: мягкий режим | полный функционал ОС клиента:	Mon DD hh:mm:ss hostname CEF:0|GIS|Blockhost-Net|4.4 |BH-FileClean-769|Гарантированное удаление файлового объекта|Low| cat=Гарантированное удаление файлов dhost=имя хоста источника события rt=дата возникновения события на клиенте cs1=содержимое поля 'ОС клиента' cs1Label=ОС клиента filepath=содержимое поля 'Имя Объекта' suser=содержимое поля 'Пользователь' suid=содержимое поля 'SID пользователя' msg=содержимое поля 'Режим работы СЗИ' externalId=769 categorySignificance=/Informational categoryBehavior=/Delete categoryDeviceGroup=/Data Security catdt=Access and Identity Management categoryOutcome=/Success categoryObject=/Host/File	Выполнение гарантированного удаления файлового объекта с диска.
771 (0x303)	Невозможно завершить операцию гарантированного удаления	Ошибка	Windows	Событие: невозможно завершить операцию гарантированного удаления Пользователь: домен\логин SID пользователя: Имя объекта:	Mon DD hh:mm:ss hostname CEF:0|GIS|Blockhost-Net|4.4 |BH-FileClean-771|Невозможно завершить операцию гарантированного удаления|High| cat=Гарантированное удаление файлов	Выполнение гарантированного удаления файлового объекта с диска не было выполнено из-за возникшей ошибки.

				Режим работы СЗИ: мягкий режим | полный функционал ОС клиента:	dhost=имя хоста источника события rt=дата возникновения события на клиенте cs1=содержимое поля ‘ОС клиента’ cs1Label=ОС клиента filepath=содержимое поля ‘Имя Объекта’ suser=содержимое поля ‘Пользователь’ suid=содержимое поля ‘SID пользователя’ msg=содержимое поля ’Режим работы СЗИ’ externalId=771 categorySignificance=/Informational/Error categoryBehavior=/Delete categoryDeviceGroup=/Data Security catdt=Access and Identity Management categoryOutcome=/Failure categoryObject=/Host/File	
772 (0x304)	Гарантированное удаление файлового объекта	Сведения	Linux	Событие: гарантированное удаление файлового объекта Пользователь: домен\логин Тип объекта: Имя объекта: Параметры командной строки:	Mon DD hh:mm:ss hostname CEF:0|GIS|Blockhost-Net|4.4 |BH-FileClean-772|Гарантированное удаление файлового объекта|Low| cat=Гарантированное удаление файлов dhost=имя хоста источника события rt=дата возникновения события на клиенте cs1=содержимое поля ‘ОС клиента’ cs1Label=ОС клиента filepath=содержимое поля ‘Имя Объекта’ suser=содержимое поля ‘Пользователь’ externalId=772 categorySignificance=/Informational categoryBehavior=/Delete categoryDeviceGroup=/Data Security catdt=Access and Identity Management categoryOutcome=/Success categoryObject=/Host/File	Выполнение гарантированного удаления файлового объекта с диска.
773 (0x305)	Невозможно завершить операцию гарантированного удаления	Ошибка	Linux	Событие: невозможно завершить операцию гарантированного удаления Пользователь: домен\логин Тип объекта Имя объекта: Описание: Параметры командной строки:	Mon DD hh:mm:ss hostname CEF:0|GIS|Blockhost-Net|4.4 |BH-FileClean-773|Невозможно завершить операцию гарантированного удаления|High| cat=Гарантированное удаление файлов dhost=имя хоста источника события rt=дата возникновения события на клиенте cs1=содержимое поля ‘ОС клиента’ cs1Label=ОС клиента cs2=содержимое поля ‘Описание’ cs2Label=Описание filepath=содержимое поля ‘Имя Объекта’ suser=содержимое поля ‘Пользователь’ externalId=773 categorySignificance=/Informational/Error categoryBehavior=/Delete	Выполнение гарантированного удаления файлового объекта с диска не было выполнено из-за возникшей ошибки.

					categoryDeviceGroup=/Data Security catdt=Access and Identity Management categoryOutcome=/Failure categoryObject=/Host/File	

1.8 Контроль целостности файлов

Код события	Тип события	Уровень важности	ОС	Формат события ОС	CEF-формат	Условия воспроизведения
3968 (0xF80)	Нарушена целостность файла	Предупреждение	Windows	Событие: нарушена целостность файла Имя файла: Путь: Режим работы СЗИ: мягкий режим | полный функционал ОС клиента:	Mon DD hh:mm:ss hostname CEF:0|GIS|Blockhost-Net|4.4 |BH-IntegrityControl-3968|Нарушена целостность файла|Medium| cat=Контроль изменения файлов dhost=имя хоста источника события rt=дата возникновения события на клиенте cs2=содержимое поля 'ОС клиента' cs2Label=ОС клиента filepath=содержимое поля 'Путь' filename=содержимое поля 'Имя файла' msg=содержимое поля 'Режим работы СЗИ' 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.
4046 (0xFCE)	Файл изменен	Предупреждение	Linux	Событие: файл изменен Имя файла: Путь: ОС клиента:	Mon DD hh:mm:ss hostname CEF:0|GIS|Blockhost-Net|4.4 |BH-IntegrityControl-4046|Файл изменен|Medium| cat=Контроль изменения файлов dhost=имя хоста источника события rt=дата возникновения события на клиенте cs2=содержимое поля 'ОС клиента' cs2Label=ОС клиента filepath=содержимое поля 'Путь' filename=содержимое поля 'Имя файла' externalId=4046 categorySignificance=/Informational/Warning categoryBehavior=/Modify categoryDeviceGroup=/Data Security catdt=Access and Identity Management categoryOutcome=/Attempt categoryObject=/Host/File	Изменена контрольная сумма контролируемого файла.
4047 (0xFCF)	Файл удален	Предупреждение	Linux	Событие: файл удален Имя файла: Путь:	Mon DD hh:mm:ss hostname CEF:0|GIS|Blockhost-Net|4.4 |BH-IntegrityControl-4047|Файл	Контролируемый файл не найден в файловой системе клиентского компьютера.

				ОС клиента:	удален|Medium| cat=Контроль изменения файлов dhost=имя хоста источника события rt=дата возникновения события на клиенте cs2=содержимое поля ‘ОС клиента’ cs2Label=ОС клиента filepath=содержимое поля ‘Путь’ filename=содержимое поля ‘Имя файла’ externalId=4047 categorySignificance=/Informational/Warning categoryBehavior=/Modify categoryDeviceGroup=/Data Security catdt=Access and Identity Management categoryOutcome=/Attempt categoryObject=/Host/File	
4048 (0xFD0)	Файл создан	Предупреждение	Linux	Событие: файл создан Имя файла: Путь: ОС клиента:	Mon DD hh:mm:ss hostname CEF:0|GIS|Blockhost-Net|4.4 |BH-IntegrityControl-4048|Файл создан|Medium| cat=Контроль изменения файлов dhost=имя хоста источника события rt=дата возникновения события на клиенте cs2=содержимое поля ‘ОС клиента’ cs2Label=ОС клиента filepath=содержимое поля ‘Путь’ filename=содержимое поля ‘Имя файла’ externalId=4048 categorySignificance=/Informational/Warning categoryBehavior=/Modify categoryDeviceGroup=/Data Security catdt=Access and Identity Management categoryOutcome=/Attempt categoryObject=/Host/File	В контролируемом каталоге обнаружен новый файл.
3969 (0xF81)	Файл восстановлен из резервной копии	Предупреждение	Windows	Событие: файл восстановлен из резервной копии Имя файла: Путь: Режим работы СЗИ: мягкий режим | полный функционал ОС клиента:	Mon DD hh:mm:ss hostname CEF:0|GIS|Blockhost-Net|4.4 |BH-IntegrityControl-3969|Файл восстановлен из резервной копии|Medium| cat=Контроль изменения файлов dhost=имя хоста источника события rt=дата возникновения события на клиенте cs2=содержимое поля ‘ОС клиента’ cs2Label=ОС клиента filepath=содержимое поля ‘Путь’ filename=содержимое поля ‘Имя файла’ msg=содержимое поля 'Режим работы СЗИ’ externalId=3969 categorySignificance=/Informational/Warning categoryBehavior=/Modify categoryDeviceGroup=/Data Security catdt=Access and Identity Management	Выполнено восстановление измененного файла из резервной копии.

					categoryOutcome=/Success categoryObject=/Host/File	
3970 (0xF82)	Не удалось восстановить файл из резервной копии	Ошибка	Windows	Событие: не удалось восстановить файл из резервной копии Причина: нет доступа к файлу Имя файла: Путь: Режим работы СЗИ: мягкий режим | полный функционал ОС клиента:	Mon DD hh:mm:ss hostname CEF:0|GIS|Blockhost-Net|4.4 |BH-IntegrityControl-3970|Не удалось восстановить файл из резервной копии|High| cat=Контроль изменения файлов dhost=имя хоста источника события rt=дата возникновения события на клиенте cs2=содержимое поля ‘ОС клиента’ cs2Label=ОС клиента filepath=содержимое поля ‘Путь’ filename=содержимое поля ‘Имя файла’ msg=содержимое поля 'Режим работы СЗИ’ externalId=3970 categorySignificance=/Informational/Error categoryBehavior=/Modify categoryDeviceGroup=/Data Security catdt=Access and Identity Management categoryOutcome=/Failure categoryObject=/Host/File	В процессе восстановления файла из резервной копии произошла ошибка. Восстановление файла не было выполнено.
3971 (0xF83)	Отказ на вход пользователя из-за нарушения контроля целостности	Предупреждение	Windows	Событие: отказ на вход пользователя из-за нарушения контроля целостности Пользователь: domain\login SID пользователя: Метка пользователя: Режим работы СЗИ: мягкий режим | полный функционал ОС клиента:	Mon DD hh:mm:ss hostname CEF:0|GIS|Blockhost-Net|4.4 |BH-IntegrityControl-3971|Отказ на вход пользователя из-за нарушения контроля целостности|Medium| cat=Контроль изменения файлов dhost=имя хоста источника события rt=дата возникновения события на клиенте cs1=содержимое поля ‘Метка пользователя’ cs1Label=Мандатная метка пользователя cs2=содержимое поля ‘ОС клиента’ cs2Label=ОС клиента suser=содержимое поля ‘Пользователь’ suid=содержимое поля ‘SID пользователя’ msg=содержимое поля 'Режим работы СЗИ’ externalId=3971 categorySignificance=/Informational/Warning categoryBehavior=/Access/Stop categoryDeviceGroup=/Data Security catdt=Access and Identity Management categoryOutcome=/Success 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	Windows	Событие: блокировка сессии пользователя из-за нарушения контроля целостности файлов Пользователь: домен\логин SID пользователя: Метка пользователя:	Mon DD hh:mm:ss hostname CEF:0|GIS|Blockhost-Net|4.4 |BH-IntegrityControl-3907|Блокировка сессии пользователя из-за нарушения контроля целостности файлов |Medium|	Блокировка сессии пользователя из-за нарушения целостности одного из контролируемых файлов. Происходит в случае, если в параметрах работы СЗИ задана соответствующая настройка.

				Режим работы СЗИ: мягкий режим | полный функционал ОС клиента:	cat=Контроль изменения файлов dhost=имя хоста источника события rt=дата возникновения события на клиенте cs1=содержимое поля ‘Метка пользователя’ cs1Label=Мандатная метка пользователя cs2=содержимое поля ‘ОС клиента’ cs2Label=ОС клиента suser=содержимое поля ‘Пользователь’ suid=содержимое поля ‘SID пользователя’ msg=содержимое поля 'режим работы СЗИ’ externalId=3907 categorySignificance=/Informational/Warning categoryBehavior=/Access/Stop categoryDeviceGroup=/Data Security catdt=Access and Identity Management categoryOutcome=/Success categoryObject=/Actor/User	

1.9 Контроль печати

Код события	Тип события	Уровень важности	ОС	Формат события ОС	CEF-формат	Условия воспроизведения
1334 (0x536)	Печать документа	Сведения	Windows	Событие: печать документа Пользователь: домен\логин SID пользователя: Метка пользователя: Имя процесса: Имя принтера: Имя документа: Метка документа: Размер документа: Количество страниц для печати: Режим работы СЗИ: мягкий режим | полный функционал ОС клиента:	Mon DD hh:mm:ss hostname CEF:0|GIS|Blockhost-Net|4.4 |BH-PrintControl-1334|Печать документа|Low| cat=Контроль печати dhost=имя хоста источника события rt=дата возникновения события на клиенте cs1=содержимое поля ‘Метка пользователя’ cs1Label=Мандатная метка пользователя cs2=содержимое поля ‘Имя принтера‘ cs2Label=Имя принтера cs3=содержимое поля ‘Метка документа’ cs3Label=Метка документа cs4=содержимое поля ‘ОС клиента’ cs4Label=ОС клиента cn1=содержимое поля ‘Количество страниц для печати’ cn1Label=Количество страниц fname=содержимое поля ‘Имя документа’ fsize=содержимое поля ‘Размер документа’ sproc=содержимое поля ‘Имя процесса’ suser=содержимое поля ‘Пользователь’ suid=содержимое поля ‘SID пользователя’ msg=содержимое поля ‘Режим работы СЗИ’ externalId=1334 categorySignificance=/Informational categoryBehavior=/Print	Успешная печать документа. Событие формируется в случае, если на клиенте СЗИ включен контроль печати.

					categoryDeviceGroup=/Application catdt=Access and Identity Management categoryOutcome=/Success categoryObject=/Host/Application	
1333 (0x535)	Отказ в печати документа	Предупреждение	Windows	Событие: отказ в печати документа Пользователь: домен\логин SID пользователя: Метка пользователя: Имя процесса: Имя принтера: Имя документа: Метка документа: Размер документа: Количество страниц для печати: Режим работы СЗИ: мягкий режим | полный функционал ОС клиента:	Mon DD hh:mm:ss hostname CEF:0|GIS|Blockhost-Net|4.4 |BH-PrintControl-1333|Отказ в печати документа|Medium| cat=Контроль печати dhost=имя хоста источника события rt=дата возникновения события на клиенте cs1=содержимое поля ‘Метка пользователя’ cs1Label=Мандатная метка пользователя cs2=содержимое поля ‘Имя принтера‘ cs2Label=Имя принтера cs3=содержимое поля ‘Метка документа’ cs3Label=Метка документа cs4=содержимое поля ‘ОС клиента’ cs4Label=ОС клиента cs5=содержимое поля ‘Количество страниц для печати’ cs5Label=Количество страниц fname=содержимое поля ‘Имя документа’ fsize=содержимое поля ‘Размер документа’ sproc=содержимое поля ‘Имя процесса’ suser=содержимое поля ‘Пользователь’ suid=содержимое поля ‘SID пользователя’ msg=содержимое поля ‘Режим работы СЗИ’ externalId=1333 categorySignificance=/Informational/Warning categoryBehavior=/Print categoryDeviceGroup=/Application catdt=Access and Identity Management categoryOutcome=/Failure categoryObject=/Host/Application	Событие формируется в случае, если попытка печати документа выполняется из процесса, у которого нет разрешения на печать.

1.10 Контроль целостности среды

1.10.1 Контроль установки/удаления драйверов

Код события	Тип события	Уровень важности	ОС	Формат события ОС	CEF-формат	Условия воспроизведения
3841 (0xF01)	Установка драйвера	Сведения	Windows	Событие: установка драйвера Имя драйвера: Путь к файлу: Тип запуска: SERVICE_BOOT_START | SERVICE_SYSTEM_START | SERVICE_AUTO_START |	Mon DD hh:mm:ss hostname CEF:0|GIS|Blockhost-Net|4.3 |BH-DriversControl-3841|Установка драйвера|Low| cat=Контроль целостности среды dhost=имя хоста источника события rt=дата возникновения события на	Регистрация (установка) нового драйвера в ОС

				SERVICE_DEMAND_START | SERVICE_DISABLED ОС клиента:	клиенте cs1=содержимое поля ‘Тип запуска’ cs1Label=Тип запуска драйвера cs2=содержимое поля ‘Имя драйвера’ cs2Label=Имя драйвера cs5=содержимое поля ‘ОС клиента’ cs5Label=ОС клиента filepath=содержимое поля ‘Имя Объекта’ externalId=3841 categorySignificance=/Informational categoryBehavior=/Modify/Configuration categoryDeviceGroup=/Assessment Tools catdt=Access and Identity Management categoryOutcome=/Success categoryObject=/Host/Operating System	
3842 (0xF02)	Удаление драйвера	Сведения	Windows	Событие: удаление драйвера Имя драйвера: ОС клиента:	Mon DD hh:mm:ss hostname CEF:0|GIS|Blockhost-Net|4.3 |BH-DriversControl-3842|Удаление драйвера|Low| cat=Контроль целостности среды dhost=имя хоста источника события rt=дата возникновения события на клиенте cs2=содержимое поля ‘Имя драйвера’ cs2Label=Имя драйвера cs5=содержимое поля ‘ОС клиента’ cs5Label=ОС клиента externalId=3842 categorySignificance=/Informational categoryBehavior=/Modify/Configuration categoryDeviceGroup=/Assessment Tools catdt=Access and Identity Management categoryOutcome=/Success categoryObject=/Host/Operating System	Разрегистрация (удаление) драйвера из ОС
3843 (0xF03)	Изменение параметров драйвера	Сведения	Windows	Событие: изменение параметров драйвера Имя драйвера: Старый тип запуска: SERVICE_BOOT_START | SERVICE_SYSTEM_START | SERVICE_AUTO_START | SERVICE_DEMAND_START | SERVICE_DISABLED Новый тип запуска: <ключ запуска> | без изменений Старый путь: <старый путь к драйверу> Новый путь: <новый путь к драйверу> | без изменений ОС клиента:	Mon DD hh:mm:ss hostname CEF:0|GIS|Blockhost-Net|4.3 |BH-DriversControl-3843| Изменение параметров драйвера|Low| cat=Контроль целостности среды dhost=имя хоста источника события rt=дата возникновения события на клиенте cs2=содержимое поля ‘Имя драйвера’ cs2Label=Имя драйвера cs4=содержимое поля ‘Старый тип запуска’ cs4Label=Старый тип запуска драйвера cs3=содержимое поля ‘Новый тип запуска’ cs3Label=Новый тип запуска драйвера cs5=содержимое поля ‘ОС клиента’	Изменение одного или нескольких параметров одного из драйверов в ОС

					cs5Label=ОС клиента oldFilePath=содержимое поля ‘Старый путь’ filepath=содержимое поля ‘Новый путь’ externalId=3843 categorySignificance=/Informational categoryBehavior=/Modify/Configuration categoryDeviceGroup=/Assessment Tools catdt=Access and Identity Management categoryOutcome=/Success categoryObject=/Host/Operating System	

1.10.2 Контроль установки/удаления служб

Код события	Тип события	Уровень важности	ОС	Формат события ОС	CEF-формат	Условия воспроизведения
3846 (0xF06)	Установка службы	Сведения	Windows	Событие: установка службы Имя службы: Путь к файлу: Тип запуска: SERVICE_BOOT_START | SERVICE_SYSTEM_START | Автоматически | Вручную | Отключено ОС клиента:	Mon DD hh:mm:ss hostname CEF:0|GIS|Blockhost-Net|4.4|BH-ServiceControl-3846|Установка службы|Low| cat=Контроль целостности среды dhost=имя хоста источника события rt=дата возникновения события на клиенте cs1=содержимое поля ‘Тип запуска’ cs1Label=Тип запуска службы cs4=содержимое поля ‘ОС клиента’ cs4Label=ОС клиента 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	Windows	Событие: удаление службы Имя службы: ОС клиента:	Mon DD hh:mm:ss hostname CEF:0|GIS|Blockhost-Net|4.4|BH-ServiceControl-3847|Удаление службы|Low| cat=Контроль целостности среды dhost=имя хоста источника события rt=дата возникновения события на клиенте cs4=содержимое поля ‘ОС клиента’ cs4Label=ОС клиента destinationServiceName=содержимое поля	Разрегистрация (удаление) службы из ОС

					‘Имя службы’ externalId=3847 categorySignificance=/Informational categoryBehavior=/Modify/Configuration categoryDeviceGroup=/Assessment Tools catdt=Access and Identity Management categoryOutcome=/Success categoryObject=/Host/Operating System	
3848 (0xF08)	Изменение параметров службы	Сведения	Windows	Событие: изменение параметров службы Имя службы: Старый тип запуска: SERVICE_BOOT_START | SERVICE_SYSTEM_START | Автоматически | Вручную | Отключено Новый тип запуска: <ключ запуска> | без изменений Старый путь: <старый путь к службе> Новый путь: <новый путь к службе> | без изменений ОС клиента:	Mon DD hh:mm:ss hostname CEF:0|GIS|Blockhost-Net|4.4 |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=Старый тип запуска службы cs3=содержимое поля ‘Новый тип запуска’ cs3Label=Новый тип запуска службы cs4=содержимое поля ‘ОС клиента’ cs4Label=ОС клиента oldFilePath=содержимое поля ‘Старый путь’ filepath=содержимое поля ‘Новый путь’ destinationServiceName=содержимое поля ‘Имя службы’ externalId=3848 categorySignificance=/Informational categoryBehavior=/Modify/Configuration categoryDeviceGroup=/Assessment Tools catdt=Access and Identity Management categoryOutcome=/Success categoryObject=/Host/Operating System	Изменение одного или нескольких параметров одной из служб в ОС

1.10.3 Контроль установки/удаления приложений

Код события	Тип события	Уровень важности	ОС	Формат события ОС	CEF-формат	Условия воспроизведения
3851 (0xF0B)	Установка приложения	Сведения	Windows	Событие: установка приложения Название: UUID: Версия: ОС клиента:	Mon DD hh:mm:ss hostname CEF:0|GIS|Blockhost-Net|4.4 |BH-ServiceControl-3851|Установка приложения|Low| cat=Контроль целостности среды dhost=имя хоста источника события rt=дата возникновения события на клиенте cs1=содержимое поля ‘UUID’ cs1Label=UUID приложения	Регистрация нового приложения в ОС

					cs2=содержимое поля ‘Название’ cs2Label=Имя приложения cs3=содержимое поля ‘Версия’ cs3Lable=Версия приложения cs6=содержимое поля ‘ОС клиента’ cs6Label=ОС клиента externalId=3851 categorySignificance=/Informational categoryBehavior=/Modify/Configuration categoryDeviceGroup=/Assessment Tools catdt=Access and Identity Management categoryOutcome=/Success categoryObject=/Host/Operating System	
3852 (0xF0C)	Удаление приложения	Сведения	Windows	Событие: удаление приложения Название: UUID: Версия: ОС клиента:	Mon DD hh:mm:ss hostname CEF:0|GIS|Blockhost-Net|4.4 |BH-ServiceControl- 3852|Удалениеприложения|Low| cat=Контроль целостности среды dhost=имя хоста источника события rt=дата возникновения события на клиенте cs1=содержимое поля ‘UUID’ cs1Label=UUID приложения cs2=содержимое поля ‘Название’ cs2Label=Имя приложения cs3=содержимое поля ‘Версия’ cs3Lable=Версия приложения cs6=содержимое поля ‘ОС клиента’ cs6Label=ОС клиента externalId=3852 categorySignificance=/Informational categoryBehavior=/Modify/Configuration categoryDeviceGroup=/Assessment Tools catdt=Access and Identity Management categoryOutcome=/Success categoryObject=/Host/Operating System	Регистрация отсутствия приложения в ОС
3853 (0xF0D)	Изменение версии приложения	Сведения	Windows	Событие: изменение версии приложения Название: UUID: Старая версия: Новая версия: ОС клиента:	Mon DD hh:mm:ss hostname CEF:0|GIS|Blockhost-Net|4.4 |BH-ServiceControl-3853|Изменение версии приложения|Low| cat=Контроль целостности среды dhost=имя хоста источника события rt=дата возникновения события на клиенте cs1=содержимое поля ‘UUID’ cs1Label=UUID приложения cs2=содержимое поля ‘Название’ cs2Label=Имя приложения cs4=содержимое поля ‘Новая версия’ cs4Label=Новая версия приложения	Изменение версии установленного приложения

					cs5=содержимое поля ‘Старая версия’ cs5Lable=Старая версия приложения cs6=содержимое поля ‘ОС клиента’ cs6Label=ОС клиента externalId=3853 categorySignificance=/Informational categoryBehavior=/Modify/Configuration categoryDeviceGroup=/Assessment Tools catdt=Access and Identity Management ategoryOutcome=/Success categoryObject=/Host/Operating System	

1.10.4 Контроль изменения перечня каталогов общего доступа

Код события	Тип события	Уровень важности	ОС	Формат события ОС	CEF-формат	Условия воспроизведения
3856 (0xF10)	Предоставление общего доступа к каталогу	Сведения	Windows	Событие: предоставление общего доступа к каталогу Имя: Путь: Примечание: ОС клиента:	Mon DD hh:mm:ss hostname CEF:0|GIS|Blockhost-Net|4.4 |BH-ShareControl-3856|Предоставление общего доступа к каталогу|Low| cat=Контроль целостности среды dhost=имя хоста источника события rt=дата возникновения события на клиенте filepath=содержимое поля ‘Путь’ cs1=содержимое поля ‘Имя’ cs1Label=Имя общего ресурса cs4=содержимое поля ‘ОС клиента’ cs4Label=ОС клиента externalId=3856 categorySignificance=/Informational categoryBehavior=/Modify/Configuration categoryDeviceGroup=/Assessment Tools catdt=Access and Identity Management categoryOutcome=/Success categoryObject=/Host/Operating System	Событие формируется в случае, если была выполнена настройка общего доступа к каталогу.
3857 (0xF11)	Прекращение общего доступа к каталогу	Сведения	Windows	Событие: прекращение общего доступа к каталогу Имя: Путь: ОС клиента:	Mon DD hh:mm:ss hostname CEF:0|GIS|Blockhost-Net|4.4 |BH-ShareControl-3857|Прекращение общего доступа к каталогу |Low| cat=Контроль целостности среды dhost=имя хоста источника события rt=дата возникновения события на клиенте filepath=содержимое поля ‘Путь’ cs1=содержимое поля ‘Имя’ cs1Label=Имя общего ресурса cs4=содержимое поля ‘ОС клиента’ cs4Label=ОС клиента externalId=3857	Событие формируется в случае, если общий доступ к каталогу был закрыт.

					categorySignificance=/Informational categoryBehavior=/Modify/Configuration categoryDeviceGroup=/Assessment Tools catdt=Access and Identity Management categoryOutcome=/Success categoryObject=/Host/Operating System	
3858 (0xF12)	Изменение параметров каталога с общим доступом	Сведения	Windows	Событие: изменение параметров каталога с общим доступом Старое имя: Новое имя: Старый путь: Новый путь: ОС клиента:	Mon DD hh:mm:ss hostname CEF:0|GIS|Blockhost-Net|4.4 |BH-ShareControl-3858|Изменение параметров каталога с общим доступом |Low| cat=Контроль целостности среды dhost=имя хоста источника события rt=дата возникновения события на клиенте filepath=содержимое поля ‘Новый Путь’ oldFilePath=содержимое поля ‘Старый путь’ cs2=содержимое поля ‘Старое имя’ cs2Label=Старое имя общего ресурса cs3=содержимое поля ‘Новое имя’ cs3Label=Новое имя общего ресурса cs4=содержимое поля ‘ОС клиента’ cs4Label=ОС клиента externalId=3858 categorySignificance=/Informational categoryBehavior=/Modify/Configuration categoryDeviceGroup=/Assessment Tools catdt=Access and Identity Management categoryOutcome=/Success categoryObject=/Host/Operating System	Событие формируется в случае, если параметры (имя или путь) каталога, к которому предоставляется общий доступ, были изменены.

1.10.5 Контроль аппаратной среды

Код события	Тип события	Уровень важности	ОС	Формат события ОС	CEF-формат	Условия воспроизведения
3862 (0xF16)	Замена процессора	Сведения	Windows	Событие: замена процессора Старые параметры: Название: ИД в компьютере: Новые параметры: Название: ИД в компьютере: ОС клиента:	Mon DD hh:mm:ss hostname CEF:0|GIS|Blockhost-Net|4.4 |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> cs1Label=Старые параметры cs2=Название:<название>, ИД в компьютере:<ИД> cs2Label=Новые параметры cs4=содержимое поля ‘ОС клиента’ cs4Label=ОС клиента	Изменение параметров вычислительного процессора, установленного в компьютере. Например, замена процессора в компьютере.

					externalId=3862 categorySignificance=/Informational categoryBehavior=/Modify/Configuration categoryDeviceGroup=/Assessment Tools catdt=Access and Identity Management categoryOutcome=/Success categoryObject=/Host/Operating System	
3863 (0xF17)	Замена материнской платы	Сведения	Windows	Событие: замена материнской платы Старые параметры: Модель: Производитель: ИД партии продукта: ИД продукта: Серийный номер устройства: Версия: Новые параметры: Модель: Производитель: ИД партии продукта: ИД продукта: Серийный номер устройства: Версия: ОС клиента:	Mon DD hh:mm:ss hostname CEF:0|GIS|Blockhost-Net|4.4 |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>, ИД продукта:<ИД>, Серийный номер устройства:<номер>, Версия:<версия> cs1Label=Старые параметры cs2=Модель:<модель>, Производитель:<производитель>, ИД партии продукта:<ИД>, ИД продукта:<ИД>, Серийный номер устройства:<номер>, Версия:<версия> cs2Label=Новые параметры cs4=содержимое поля ‘ОС клиента’ cs4Label=ОС клиента externalId=3863 categorySignificance=/Informational categoryBehavior=/Modify/Configuration categoryDeviceGroup=/Assessment Tools catdt=Access and Identity Management categoryOutcome=/Success categoryObject=/Host/Operating System	Изменение параметров материнской платы, установленной в компьютере. Например, замена материнской платы в компьютере или перенос жесткого диска с установленным СЗИ на другой компьютер.
3864 (0xF18)	Добавление жесткого диска	Сведения	Windows	Событие: добавление жесткого диска Параметры: Модель: Производитель: Размер: Серийный номер устройства: ИД ресурса: ИД в компьютере: Интерфейс: ОС клиента:	Mon DD hh:mm:ss hostname CEF:0|GIS|Blockhost-Net|4.4 |BH-HardwareControl-3864|Добавление жесткого диска|Low| cat=Контроль целостности среды dhost=имя хоста источника события rt=дата возникновения события на клиенте cs3=Модель:<модель>, Производитель:<производитель>, Размер:<размер>, Серийный номер устройства: <номер>, ИД ресурса:<ИД>, ИД в компьютере:<ИД>, Интерфейс:<интерфейс> cs3Label=Параметры cs4=содержимое поля ‘ОС клиента’ cs4Label=ОС клиента	В компьютере был обнаружен жесткий диск с указанными параметрами. Например, в компьютер был установлен второй жесткий диск.

					externalId=3864 categorySignificance=/Informational categoryBehavior=/Modify/Configuration categoryDeviceGroup=/Assessment Tools catdt=Access and Identity Management categoryOutcome=/Success categoryObject=/Host/Operating System	
3865 (0xF19)	Не удалось обнаружить жесткий диск	Сведения	Windows	Событие: не удалось обнаружить жесткий диск Параметры: Модель: Производитель: Размер: Серийный номер устройства: ИД ресурса: ИД в компьютере: Интерфейс: ОС клиента:	Mon DD hh:mm:ss hostname CEF:0|GIS|Blockhost-Net|4.4 |BH-HardwareControl-3865|Не удалось обнаружить жесткий диск|Low| cat=Контроль целостности среды dhost=имя хоста источника события rt=дата возникновения события на клиенте cs3=Модель:<модель>, Производитель:<производитель>, Размер:<размер>, Серийный номер устройства:<номер>, ИД ресурса:<ИД>, ИД в компьютере:<ИД>, Интерфейс:<интерфейс> cs3Label=Параметры cs4=содержимое поля ‘ОС клиента’ cs4Label=ОС клиента externalId=3865 categorySignificance=/Informational categoryBehavior=/Modify/Configuration categoryDeviceGroup=/Assessment Tools catdt=Access and Identity Management categoryOutcome=/Failure 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	Windows	Событие: добавление CD-привода Параметры: Производитель: Серийный номер устройства: Тип носителей: ИД в компьютере: ОС клиента:	Mon DD hh:mm:ss hostname CEF:0|GIS|Blockhost-Net|4.4 |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 устройства:<номер>, Тип носителей:<тип>, ИД в компьютере:<ИД> cs3Label=Параметры cs4=содержимое поля ‘ОС клиента’ cs4Label=ОС клиента 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	Не удалось	Сведения	Windows	Событие: не удалось обнаружить	Mon DD hh:mm:ss hostname	Из компьютера был удален CD-

(0xF1C)	обнаружить CD-привод			CD-привод Параметры: Производитель: Серийный номер устройства: Тип носителей: ИД в компьютере: ОС клиента:	CEF:0|GIS|Blockhost-Net|4.4 |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 устройства:<номер>, Тип носителей:<тип>, ИД в компьютере:<ИД> cs3Label=Параметры cs4=содержимое поля 'ОС клиента' cs4Label=ОС клиента externalId=3868 categorySignificance=/Informational categoryBehavior=/Modify/Configuration categoryDeviceGroup=/Assessment Tools catdt=Access and Identity Management categoryOutcome=/Failure categoryObject=/Host/Operating System	привод с указанными параметрами. 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	Windows	Событие: добавление сетевого адаптера Параметры: Название: Тип адаптера: Производитель: MAC адрес: ИД в компьютере: GUID: ОС клиента:	Mon DD hh:mm:ss hostname CEF:0|GIS|Blockhost-Net|4.4 |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>, Производитель:<производитель>, MAC адрес:<адрес>, ИД в компьютере:<ИД>, GUID:<GUID> cs3Label=Параметры cs4=содержимое поля 'ОС клиента' cs4Label=ОС клиента externalId=3870 categorySignificance=/Informational categoryBehavior=/Modify/Configuration categoryDeviceGroup=/Assessment Tools catdt=Access and Identity Management categoryOutcome=/Success categoryObject=/Host/Operating System	В компьютере был обнаружен сетевой адаптер с указанными параметрами. Например, в компьютер был установлен новый сетевой адаптер.
3871 (0xF1F)	Не удалось обнаружить сетевой адаптер	Сведения	Windows	Событие: не удалось обнаружить сетевой адаптер Параметры: Название: Тип адаптера: Производитель: MAC адрес: ИД в компьютере: GUID:	Mon DD hh:mm:ss hostname CEF:0|GIS|Blockhost-Net|4.4 |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>,	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.

				ОС клиента:	Производитель:<производитель>, MAC адрес:<адрес>, ИД в компьютере:<ИД>, GUID:<GUID> cs3Label=Параметры cs4=содержимое поля ‘ОС клиента’ cs4Label=ОС клиента externalId=3871 categorySignificance=/Informational categoryBehavior=/Modify/Configuration categoryDeviceGroup=/Assessment Tools catdt=Access and Identity Management categoryOutcome=/Failure categoryObject=/Host/Operating System	
3872 (0xF20)	Изменение параметров сетевого адаптера	Сведения	Windows	Событие: изменение параметров сетевого адаптера Старые параметры: Название: Тип адаптера: Производитель: MAC адрес: ИД в компьютере: GUID: Новые параметры: Название: Тип адаптера: Производитель: MAC адрес: ИД в компьютере: GUID: ОС клиента:	Mon DD hh:mm:ss hostname CEF:0|GIS|Blockhost-Net|4.4 |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>, Производитель:<производитель>, MAC адрес:<адрес>, ИД в компьютере:<ИД>, GUID:<GUID> cs1Label=Старые параметры cs2=Название:<название>, Тип адаптера:<тип>, Производитель:<производитель>, MAC адрес:<адрес>, ИД в компьютере:<ИД>, GUID:<GUID> cs2Label=Новые параметры cs4=содержимое поля ‘ОС клиента’ cs4Label=ОС клиента externalId=3872 categorySignificance=/Informational categoryBehavior=/Modify/Configuration categoryDeviceGroup=/Assessment Tools catdt=Access and Identity Management categoryOutcome=/Success	Изменение параметров сетевого адаптера, установленного в компьютере. Например, замена одного сетевого адаптера на другой.
3873 (0xF21)	Замена видеоконтроллера	Сведения	Windows	Событие: замена видеоконтроллера Старые параметры: Название: Объем памяти: Видеопроцессор: ИД в компьютере: Новые параметры: Название: Объем памяти:	Mon DD hh:mm:ss hostname CEF:0|GIS|Blockhost-Net|4.4 |BH-HardwareControl-3873|Замена видеоконтроллера|Low| cat=Контроль целостности среды dhost=имя хоста источника события rt=дата возникновения события на клиенте cs1=Название:<название>, Объем памяти:<объем>, Видеопроцессор:<видеопроцессор>, ИД в	Изменение параметров видеоконтроллера, установленного в компьютере. Например, замена одного контроллера на другой.

				Видеопроцессор: ИД в компьютере: ОС клиента:	компьютере:<ИД> cs1Label=Старые параметры cs2=Название:<название>, Объем памяти:<объем>, Видеопроцессор:<видеопроцессор>, ИД в компьютере:<ИД> cs2Label=Новые параметры cs4=содержимое поля 'ОС клиента' cs4Label=ОС клиента externalId=3873 categorySignificance=/Informational categoryBehavior=/Modify/Configuration categoryDeviceGroup=/Assessment Tools catdt=Access and Identity Management categoryOutcome=/Success	
3874 (0xF22)	Добавление модуля оперативной памяти	Сведения	Windows	Событие: добавление модуля оперативной памяти Параметры: Обозначение модуля: Емкость: Модель: Название: Производитель: Серийный номер устройства: ОС клиента:	Mon DD hh:mm:ss hostname CEF:0|GIS|Blockhost-Net|4.4 |BH-HardwareControl-3874|Добавление модуля оперативной памяти|Low| cat=Контроль целостности среды dhost=имя хоста источника события rt=дата возникновения события на клиенте cs3=Обозначение модуля:<обозначение>, Емкость:<емкость>, Модель:<модель>, Название:<название>, Производитель:<производитель>, Серийный номер устройства:<номер> cs3Label=Параметры cs4=содержимое поля 'ОС клиента' cs4Label=ОС клиента externalId=3874 categorySignificance=/Informational categoryBehavior=/Modify/Configuration categoryDeviceGroup=/Assessment Tools catdt=Access and Identity Management categoryOutcome=/Success	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.
3875 (0xF23)	Не удалось обнаружить модуль оперативной памяти	Сведения	Windows	Событие: не удалось обнаружить модуль оперативной памяти Параметры: Обозначение модуля: Емкость: Модель: Название: Производитель: Серийный номер устройства: ОС клиента:	Mon DD hh:mm:ss hostname CEF:0|GIS|Blockhost-Net|4.4 |BH-HardwareControl-3875|Не удалось обнаружить модуль оперативной памяти|Low| cat=Контроль целостности среды dhost=имя хоста источника события rt=дата возникновения события на клиенте cs3=Обозначение модуля:<обозначение>, Емкость:<емкость>, Модель:<модель>, Название:<название>, Производитель:<производитель>, Серийный номер устройства:<номер> cs3Label=Параметры	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.

					cs4=содержимое поля ‘ОС клиента’ cs4Label=ОС клиента externalId=3875 categorySignificance=/Informational categoryBehavior=/Modify/Configuration categoryDeviceGroup=/Assessment Tools catdt=Access and Identity Management categoryOutcome=/Failure	

1.11 События сервера СЗИ

Код события	Тип события	Уровень важности	ОС	Формат события ОС	CEF-формат	Условия воспроизведения
3961 (0xF79)	Подключение клиента к серверу	Сведения	Windows	Событие: подключение клиента к серверу Имя клиента: домен\хост IP клиента:	Mon DD hh:mm:ss hostname CEF:0|GIS|Blockhost-Net|4.4 |BH-ServerSZI-3961|Подключение клиента к серверу|Low| cat=События сервера СЗИ dhost=имя хоста источника события rt=дата возникновения события на клиенте sourceAddress=содержимое поля ‘IP клиента’ sourceHostName=содержимое поля ‘Имя клиента’ externalId=3961 categorySignificance=/Informational categoryBehavior=/Communicate categoryDeviceGroup=/Application catdt=Access and Identity Management categoryOutcome=/Success categoryObject=/Host/Application	Подключение клиента к серверу СЗИ.
3960 (0xF78)	Отключение клиента от сервера	Сведения	Windows	Событие: отключение клиента от сервера Имя клиента: домен\хост IP клиента:	Mon DD hh:mm:ss hostname CEF:0|GIS|Blockhost-Net|4.4 |BH-ServerSZI-3960|Отключение клиента от сервера|Low| cat=События сервера СЗИ dhost=имя хоста источника события rt=дата возникновения события на клиенте sourceAddress=содержимое поля ‘IP клиента’ sourceHostName=содержимое поля ‘Имя клиента’ externalId=3960 categorySignificance=/Informational categoryBehavior=/Communicate categoryDeviceGroup=/Application catdt=Access and Identity Management categoryOutcome=/Success categoryObject=/Host/Application	Отключение клиента от сервера СЗИ.

3908 (0xF44)	Отказ в подключении клиента к серверу	Ошибка	Windows	Событие: отказ в подключении клиента к серверу Причина: Имя клиента: домен\хост IP клиента:	Mon DD hh:mm:ss hostname CEF:0|GIS|Blockhost-Net|4.4 |BH-ServerSZI-3908|Отказ в подключении клиента к серверу|High| cat=События сервера СЗИ dhost=имя хоста источника события rt=дата возникновения события на клиенте sourceAddress=содержимое поля ‘IP клиента’ sourceHostName=содержимое поля ‘Имя клиента’ reason=содержимое поля ‘Причина’ externalId=3908 categorySignificance=/Informational/Error categoryBehavior=/Communicate categoryDeviceGroup=/Application catdt=Access and Identity Management categoryOutcome=/Failure categoryObject=/Host/Application	Отказ в подключении клиента к серверу СЗИ. Возможные причины отказа - клиент с таким именем уже есть на сервере.
3909 (0xF45)	Подключение к родительскому серверу	Сведения	Windows	Событие: подключение к родительскому серверу Имя сервера: домен\хост IP сервера:	Mon DD hh:mm:ss hostname CEF:0|GIS|Blockhost-Net|4.4 |BH-ServerSZI-3909|Подключение к родительскому серверу|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=3909 categorySignificance=/Informational categoryBehavior=/Communicate categoryDeviceGroup=/Application catdt=Access and Identity Management categoryOutcome=/Success categoryObject=/Host/Application	Восстановление связи с родительским сервером СЗИ. Событие формируется на подчиненном сервере.
3910 (0xF46)	Отключение от родительского сервера	Сведения	Windows	Событие: отключение от родительского сервера Имя сервера: домен\хост IP сервера:	Mon DD hh:mm:ss hostname CEF:0|GIS|Blockhost-Net|4.4 |BH-ServerSZI-3910|Отключение от родительского 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=3910 categorySignificance=/Informational	Потеря связи с родительским сервером СЗИ. Событие формируется на подчиненном сервере.

					categoryBehavior=/Communicate categoryDeviceGroup=/Application catdt=Access and Identity Management categoryOutcome=/Success categoryObject=/Host/Application	
3911 (0xF47)	Отказ в подключении к родительскому серверу	Ошибка	Windows	Событие: отказ в подключении к родительскому серверу Причина: Имя сервера: домен\хост IP сервера:	Mon DD hh:mm:ss hostname CEF:0|GIS|Blockhost-Net|4.4 |BH-ServerSZI-3911|Отказ в подключении к родительскому серверу|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’ reason=содержимое поля ‘Причина’ externalId=3911 categorySignificance=/Informational/Error categoryBehavior=/Communicate categoryDeviceGroup=/Application catdt=Access and Identity Management categoryOutcome=/Failure categoryObject=/Host/Application	Нижележащему (подчиненному) серверу отказано в подключении к головному (родительскому) серверу СЗИ. Событие формируется на подчиненном сервере.
3912 (0xF48)	Подключение к дочернему серверу	Сведения	Windows	Событие: подключение к дочернему серверу Имя сервера: домен\хост IP сервера:	Mon DD hh:mm:ss hostname CEF:0|GIS|Blockhost-Net|4.4 |BH-ServerSZI-3912|Подключение к дочернему серверу|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. Событие формируется на родительском сервере.
3913 (0xF49)	Отключение от дочернего сервера	Сведения	Windows	Событие: отключение от дочернего сервера Имя сервера: домен\хост IP сервера:	Mon DD hh:mm:ss hostname CEF:0|GIS|Blockhost-Net|4.4 |BH-ServerSZI-3913|Отключение от дочернего сервера|Low| cat=События сервера СЗИ dhost=имя хоста источника события rt=дата возникновения события на клиенте sourceAddress=содержимое поля ‘IP	Потеря связи с нижележащим (подчиненным) сервером СЗИ. Событие формируется на родительском сервере.

					сервера’ sourceHostName=содержимое поля ‘Имя сервера’ externalId=3913 categorySignificance=/Informational categoryBehavior=/Communicate categoryDeviceGroup=/Application catdt=Access and Identity Management categoryOutcome=/Success categoryObject=/Host/Application	
3920 (0xF50)	Отказ в подключении к дочернему серверу	Ошибка	Windows	Событие: отказ в подключении к дочернему серверу Причина: Имя сервера: домен\хост IP сервера:	Mon DD hh:mm:ss hostname CEF:0|GIS|Blockhost-Net|4.4 |BH-ServerSZI-3920|Отказ в подключении к дочернему серверу|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’ reason=содержимое поля ‘Причина’ externalId=3920 categorySignificance=/Informational/Error categoryBehavior=/Communicate categoryDeviceGroup=/Application catdt=Access and Identity Management categoryOutcome=/Failure categoryObject=/Host/Application	Головному (родительскому) серверу отказано в подключении к нижележащему (подчиненному) серверу СЗИ. Событие формируется на родительском сервере.
3922 (0xF52)	Сервер администрирования запущен	Сведения	Windows, Linux	Событие: сервер администрирования запущен	Mon DD hh:mm:ss hostname CEF:0|GIS|Blockhost-Net|4.4 |BH-ServerSZI-3922|Сервер администрирования запущен|Low| cat=События сервера СЗИ dhost=имя хоста источника события rt=дата возникновения события на клиенте externalId=3922 categorySignificance=/Informational categoryBehavior=Execute/Start categoryDeviceGroup=/Application catdt=Access and Identity Management categoryOutcome=/Success	Запуск и инициализация служб сервера СЗИ.
3923 (0xF53)	Сервер администрирования остановлен	Сведения	Windows, Linux	События: сервер администрирования остановлен	Mon DD hh:mm:ss hostname CEF:0|GIS|Blockhost-Net|4.4 |BH-ServerSZI-3923|Сервер администрирования остановлен|Medium| cat=События сервера СЗИ dhost=имя хоста источника события rt=дата возникновения события на клиенте externalId=3923	Остановка служб сервера СЗИ.

					categorySignificance=/Informational/Warning categoryBehavior=Execute/Stop categoryDeviceGroup=/Application catdt=Access and Identity Management categoryOutcome=/Success	
3924 (0xF54)	Ошибка при запуске сервера администрирования	Ошибка	Windows, Linux	Событие: ошибка при запуске сервера администрирования Причина: не удалось запустить службы <список служб> | <другие причины>	Mon DD hh:mm:ss hostname CEF:0|GIS|Blockhost-Net|4.4 |BH-ServerSZI-3924|Ошибка при запуске сервера администрирования|High| cat=События сервера СЗИ dhost=имя хоста источника события rt=дата возникновения события на клиенте reason=содержимое поля 'Причина' externalId=3924 categorySignificance=/Informational/Error categoryBehavior=Execute categoryDeviceGroup=/Application catdt=Access and Identity Management categoryOutcome=/Failure	В процессе запуска и инициализации служб сервера СЗИ произошла ошибка.
3972 (0xF84)	Запуск сбора аудита с подчиненных серверов	Сведения	Windows	Событие: запуск сбора аудита с подчиненных серверов Тип запуска: по расписанию | по требованию	Конвертация в CEF отсутствует (событие не передается в SIEM-систему)	Запущен процесс сбора событий аудита с подчиненных серверов по одной из следующих причин: - в соответствие с расписанием, определенным администратором - по требованию администратора
3973 (0xF85)	Завершение сбора аудита с подчиненных серверов	Сведения	Windows	Событие: завершение сбора аудита с подчиненных серверов Тип запуска: по расписанию | по требованию	Конвертация в CEF отсутствует (событие не передается в SIEM-систему)	Завершен процесс сбора событий аудита с подчиненных серверов по одной из следующих причин: - в соответствие с расписанием, определенным администратором - по требованию администратора
3974 (0xF86)	Запуск сбора аудита с клиентских компьютеров	Сведения	Windows	Событие: запуск сбора аудита с клиентских компьютеров Тип запуска: по расписанию | по требованию	Конвертация в CEF отсутствует (событие не передается в SIEM-систему)	Запущен процесс сбора событий аудита с клиентских компьютеров по одной из следующих причин: - в соответствие с расписанием, определенным администратором - по требованию администратора
3975 (0xF87)	Завершение сбора аудита с клиентских компьютеров	Сведения	Windows	Событие: завершение сбора аудита с клиентских компьютеров Тип запуска: по расписанию | по требованию	Конвертация в CEF отсутствует (событие не передается в SIEM-систему)	Завершен процесс сбора событий аудита с клиентских компьютеров по одной из следующих причин: - в соответствие с расписанием, определенным администратором - по требованию администратора
3989 (0xF95)	Прерывание сбора аудита с клиентских компьютеров из-за исключающего интервала	Сведения	Windows	Событие: прерывание сбора аудита с клиентских компьютеров из-за 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 сбора аудита с подсерверов из-за исключающего интервала	Сведения	Windows	Событие: прерывание сбора аудита с подсерверов из-за 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	Windows	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	Windows	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 (0xF8F)	Недостаточно места на сервере для сохранения событий аудита	Ошибка	Windows	Событие: недостаточно места на сервере для сохранения событий аудита Рекомендация: произведите очистку хранилища событий методом автоархивации	Конвертация в CEF отсутствует (событие не передается в SIEM-систему)	На компьютере с сервером СЗИ недостаточно дискового пространства для сохранения событий аудита в хранилище для долгосрочного хранения событий.
3984 (0xF90)	Ошибка при записи событий аудита в	Ошибка	Windows	Событие: ошибка при записи событий аудита в кэш событий	Конвертация в CEF отсутствует (событие не передается в SIEM-систему)	Размер временного хранилища событий аудита на сервере СЗИ

	кэш событий			Причина: превышен максимальный размер кэша событий		превысил допустимый размер. Максимальный допустимый размер хранилища определяется администратором в настройках сервера СЗИ.
3985 (0xF91)	Запуск создания архива событий аудита по расписанию	Сведения	Windows	Событие: запуск создания архива событий аудита по расписанию Тип архивации: перемещение событий в файл архива | удаление событий Имя файла: <имя файла> Начиная с: 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	Windows	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	Windows	Событие: ошибка при создании архива событий аудита 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	Windows	Событие: ошибка при попытке экспорта событий аудита в SIEM-систему 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.

1.12 События клиента СЗИ

Код события	Тип события	Уровень важности	ОС	Формат события ОС	CEF-формат	Условия воспроизведения
3089 (0xC11)	Подключение клиента к серверу	Сведения	Windows, Linux	Событие: подключение клиента к серверу IP сервера: ОС клиента:	Mon DD hh:mm:ss hostname CEF:0|GIS|Blockhost-Net|4.4 |BH-ClientSZI-3089|Подключение клиента к серверу|Low| cat=События клиента СЗИ dhost=имя хоста источника события rt=дата возникновения события на клиенте cs3=содержимое поля 'ОС клиента' cs3Label=ОС клиента sourceAddress=содержимое поля 'IP сервера' externalId=3089 categorySignificance=/Informational categoryBehavior=/Communicate categoryDeviceGroup=/Application catdt=Access and Identity Management categoryOutcome=/Success categoryObject=/Host/Application	Подключение клиента к серверу СЗИ.

3925 (0xF55)	Отключение клиента от сервера	Сведения	Windows, Linux	Событие: отключение клиента от сервера IP сервера: ОС клиента:	Mon DD hh:mm:ss hostname CEF:0|GIS|Blockhost-Net|4.4 |BH-ClientSZI-3925|Отключение клиента от сервера|Low| cat=События клиента СЗИ dhost=имя хоста источника события rt=дата возникновения события на клиенте cs3=содержимое поля 'ОС клиента' cs3Label=ОС клиента sourceAddress=содержимое поля 'IP сервера' externalId=3925 categorySignificance=/Informational categoryBehavior=/Communicate categoryDeviceGroup=/Application catdt=Access and Identity Management categoryOutcome=/Success categoryObject=/Host/Application	Отключение клиента от сервера СЗИ.
3090 (0xC12)	Отказ в подключении клиента к серверу	Ошибка	Windows, Linux	Событие: отказ в подключении клиента к серверу Причина: IP сервера: ОС клиента:	Mon DD hh:mm:ss hostname CEF:0|GIS|Blockhost-Net|4.4 |BH-ClientSZI-3090|Отказ от подключения клиента к серверу|High| cat=События клиента СЗИ dhost=имя хоста источника события rt=дата возникновения события на клиенте cs3=содержимое поля 'ОС клиента' cs3Label=ОС клиента reason=содержимое поля 'Причина' sourceAddress=содержимое поля 'IP сервера' externalId=3090 categorySignificance=/Informational/Error categoryBehavior=/Communicate categoryDeviceGroup=/Application catdt=Access and Identity Management categoryOutcome=/Failure 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	Windows, Linux	Событие: сервер не найден IP сервера: ОС клиента:	Mon DD hh:mm:ss hostname CEF:0|GIS|Blockhost-Net|4.4 |BH-ClientSZI-3091|Сервер не найден|High| cat=События клиента СЗИ dhost=имя хоста источника события rt=дата возникновения события на клиенте cs3=содержимое поля 'ОС клиента' cs3Label=ОС клиента sourceAddress=содержимое поля 'IP сервера' externalId=3091 categorySignificance=/Informational/Error categoryBehavior=/Communicate	Клиенту не удалось установить соединение с сервером СЗИ по имеющемуся адресу.

					categoryDeviceGroup=/Application catdt=Access and Identity Management categoryOutcome=/Failure categoryObject=/Host/Application	
3926 (0xF56)	Клиент запущен	Информация	Windows, Linux	Событие: клиент запущен ОС клиента:	Mon DD hh:mm:ss hostname CEF:0|GIS|Blockhost-Net|4.4 |BH-ClientSZI-3926|Клиент запущен|Low| cat=События клиента СЗИ dhost=имя хоста источника события rt=дата возникновения события на клиенте cs3=содержимое поля 'ОС клиента' cs3Label=ОС клиента externalId=3926 categorySignificance=/Informational categoryBehavior=/Access/Start categoryDeviceGroup=/Application catdt=Access and Identity Management categoryOutcome=/Success categoryObject=/Host/Application	Завершение запуска и инициализации всех служб клиента СЗИ.
3927 (0xF57)	Клиент остановлен	Информация	Windows, Linux	Событие: клиент остановлен ОС клиента:	Mon DD hh:mm:ss hostname CEF:0|GIS|Blockhost-Net|4.4 |BH-ClientSZI-3927|Клиент остановлен|Low| cat=События клиента СЗИ dhost=имя хоста источника события rt=дата возникновения события на клиенте cs3=содержимое поля 'ОС клиента' cs3Label=ОС клиента externalId=3927 categorySignificance=/Informational categoryBehavior=/Access/Stop categoryDeviceGroup=/Application catdt=Access and Identity Management categoryOutcome=/Success categoryObject=/Host/Application	Остановка всех служб клиента СЗИ.
3928 (0xF58)	Ошибка при запуске клиента	Ошибка	Windows, Linux	Событие: ошибка при запуске клиента Причина: не удалось запустить службы <список служб> ОС клиента:	Mon DD hh:mm:ss hostname CEF:0|GIS|Blockhost-Net|4.4 |BH-ClientSZI-3928|Ошибка при запуске клиента|High| cat=События клиента СЗИ dhost=имя хоста источника события rt=дата возникновения события на клиенте cs3=содержимое поля 'ОС клиента' cs3Label=ОС клиента reason=содержимое поля 'Причина' externalId=3928 categorySignificance=/Informational/Error categoryBehavior=/Access categoryDeviceGroup=/Application catdt=Access and Identity Management	В процессе запуска и инициализации служб клиента СЗИ произошла ошибка.

					categoryOutcome=/Failure categoryObject=/Host/Application	
4029 (0xFBD)	Изменение параметров работы клиента СЗИ	Сведения	Windows, Linux	Событие: изменение параметров работы клиента СЗИ Инициатор: Изменения в политике: нет изменений | <изменение политики> ОС клиента: Изменения настроек клиента: нет изменений | <изменение настроек клиента> ОС клиента:	Mon DD hh:mm:ss hostname CEF:0|GIS|Blockhost-Net|4.4 |BH-ClientSZI-4029|Изменение параметров работы клиента СЗИ|Low| cat=События клиента СЗИ dhost=имя хоста источника события rt=дата возникновения события на клиенте suser=содержимое поля 'Инициатор' cs1=содержимое поля 'Изменение настроек клиента' cs1Label=Изменения конфигурации cs2=содержимое поля 'Изменение в политике' cs2Label=Изменения в политике externalId=4029 cs3=содержимое поля 'ОС клиента' cs3Label=ОС клиента categorySignificance=/Informational categoryBehavior=/Modify/Configuration categoryDeviceGroup=/Application catdt=Access and Identity Management categoryOutcome=/Success categoryObject=/Host/Application	Изменение работы клиента СЗИ выполняется администратором информационной безопасности одним из следующих способов: - модификация действующей клиентской политики СЗИ в группе, в которую включен клиент СЗИ - модификация настроек механизмов безопасности клиента СЗИ, задаваемых индивидуально для каждого клиента СЗИ
4030 (0xFBE)	Прекращение действия лицензии	Предупреждение	Windows, Linux	Событие: прекращение действия лицензии Причина: истечение срока действия лицензии ОС клиента:	Mon DD hh:mm:ss hostname CEF:0|GIS|Blockhost-Net|4.4 |BH-ClientSZI-4030|Прекращение действия лицензии|Medium| cat=События клиента СЗИ dhost=имя хоста источника события rt=дата возникновения события на клиенте cs3=содержимое поля 'ОС клиента' cs3Label=ОС клиента reason=истечение срока действия лицензии externalId=4030 categorySignificance=/Warning categoryBehavior=/Modify categoryDeviceGroup=/Application catdt=Access and Identity Management categoryOutcome=/Failure categoryObject=/Host/Application	Событие создается клиентом СЗИ, если при валидации лицензии обнаруживается, что срок действия лицензии истек.
4045 (0xFCD)	Ошибка инициализации пакета аутентификации	Ошибка	Windows	Событие: ошибка инициализации пакета аутентификации Название пакета: kerberos | ntlm | <другой пакет> Код ошибки:	Mon DD hh:mm:ss hostname CEF:0|GIS|Blockhost-Net|4.4 |BH-ClientSZI-4045|Ошибка инициализации пакета аутентификации |High| cat=События клиента СЗИ dhost=имя хоста источника события rt=дата возникновения события на клиенте cs4=содержимое поля 'Название пакета'	Событие создается клиентом СЗИ в случае возникновения ошибки в процессе загрузки пакета аутентификации, чаще всего Kerberos или NTLM.

					cs4Label=Имя пакета cs5=содержимое поля ‘Код ошибки’ cs5Label=Код ошибки externalId=4045 categorySignificance=/Error categoryBehavior=/Access categoryDeviceGroup=/Application catdt=Access and Identity Management categoryOutcome=/Failure categoryObject=/Host/Application	

1.13 Действия администратора СЗИ

1.13.1 Администрирование

Код	Событие	Уровень	ОС	Шаблон	CEF-формат	Пояснение
3943 (0xF67)	Подключение консоли к серверу	Сведения	Windows	Событие: подключение консоли к серверу Инициатор: домен\логин Тип инициатора: Active Directory | локальный пользователь | собственный пользователь Блокхост-Сеть Полномочия: чтение, запись | чтение	Mon DD hh:mm:ss hostname CEF:0|GIS|Blockhost-Net|4.4 |BH-Admin-3943|Подключение консоли к серверу|Low| cat=Администрирование dhost=имя хоста источника события rt=дата возникновения события на клиенте cs1=содержимое поля ‘Тип инициатора’ cs1Label=Тип инициатора cs2=содержимое поля ‘Полномочия’ cs2Label=Полномочия администратора suser=содержимое поля ‘Инициатор’ externalId=3943 categorySignificance=/Informational categoryBehavior=/Access categoryDeviceGroup=/Application catdt=Access and Identity Management categoryOutcome=/success categoryObject=/Host/Application	Подключение консоли управления к серверу СЗИ выполнено из-под пользователя, которому была предоставлена возможность работать с сервером с соответствующим уровнем полномочий.
3944 (0xF68)	Отказ на подключение консоли к серверу	Ошибка	Windows	Событие: отказ на подключение консоли к серверу Причина: недостаточно прав Инициатор: домен\логин Тип инициатора: Active Directory | локальный пользователь | собственный пользователь Блокхост-Сеть	Mon DD hh:mm:ss hostname CEF:0|GIS|Blockhost-Net|4.4 |BH-Admin-3944|Отказ на подключение консоли к серверу|High| cat=Администрирование dhost=имя хоста источника события rt=дата возникновения события на клиенте cs1=содержимое поля ‘Тип инициатора’ cs1Label=Тип инициатора suser=содержимое поля ‘Инициатор’ reason=содержимое поля ‘Причина’ externalId=3944 categorySignificance=/Informational/Error	Выполнена попытка подключения консоли управления к серверу СЗИ из-под пользователя, которому не были предоставлены какие-либо полномочия для работы с сервером.

					categoryBehavior=/Access categoryDeviceGroup=/Application catdt=Access and Identity Management categoryOutcome=/Failure categoryObject=/Host/Application	
4024 (0xFB8)	Перемещение клиента в дереве иерархии	Сведения	Windows	Событие: перемещение клиента в дереве иерархии Инициатор: домен\логин Имя клиента: IP клиента: Из группы: В группу:	Mon DD hh:mm:ss hostname CEF:0|GIS|Blockhost-Net|4.4 |BH-Admin-4024|Перемещение клиента в дереве иерархии|Low| cat=Администрирование dhost=имя хоста источника события rt=дата возникновения события на клиенте cs3=содержимое поля ‘Из группы’ cs3Label=Старая группа клиента cs4=содержимое поля ‘В группу’ cs4Label=Новая группа клиента dvc=содержимое поля ‘IP клиента’ dvchost=содержимое поля ‘Имя клиента’ suser=содержимое поля ‘Инициатор’ externalId=4024 categorySignificance=/Informational categoryBehavior=/Modify/configuration categoryDeviceGroup=/Database catdt=Access and Identity Management categoryOutcome=/success categoryObject=/Host/Application	
4025 (0xFB9)	Перемещение группы в дереве иерархии	Сведения	Windows	Событие: перемещение группы в дереве иерархии Инициатор: домен\логин Имя группы: Из группы: В группу:	Mon DD hh:mm:ss hostname CEF:0|GIS|Blockhost-Net|4.4 |BH-Admin-4025|Перемещение группы в дереве иерархии|Low| cat=Администрирование dhost=имя хоста источника события rt=дата возникновения события на клиенте cs5=содержимое поля ‘Имя группы’ cs5Label=Группа клиента cs3=содержимое поля ‘Из группы’ cs3Label=Старая группа клиента cs4=содержимое поля ‘В группу’ cs4Label=Новая группа клиента suser=содержимое поля ‘Инициатор’ externalId=4025 categorySignificance=/Informational categoryBehavior=/Modify/configuration categoryDeviceGroup=/Database catdt=Access and Identity Management categoryOutcome=/success categoryObject=/Host/Application	
4026 (0xFBA)	Удаление клиента из дерева иерархии	Сведения	Windows	Событие: удаление клиента из дерева иерархии	Mon DD hh:mm:ss hostname CEF:0|GIS|Blockhost-Net|4.4	

				Инициатор: домен\логин Имя клиента: IP клиента: Из группы:	|BH-Admin-4026|Удаление клиента из дерева иерархии|Low| cat=Администрирование dhost=имя хоста источника события rt=дата возникновения события на клиенте cs5=содержимое поля 'Из группы' cs5Label=Группа клиента dvc=содержимое поля 'IP клиента' dvchost=содержимое поля 'Имя клиента' suser=содержимое поля 'Инициатор' externalId=4026 categorySignificance=/Informational categoryBehavior=/Modify/configuration categoryDeviceGroup=/Database catdt=Access and Identity Management categoryOutcome=/success categoryObject=/Host/Application	
4027 (0xFBB)	Изменение имени группы	Сведения	Windows	Событие: изменение имени группы Инициатор: домен\логин Старое имя: Новое имя:	Mon DD hh:mm:ss hostname CEF:0|GIS|Blockhost-Net|4.4 |BH-Admin-4027|Изменение имени группы|Low| cat=Администрирование dhost=имя хоста источника события rt=дата возникновения события на клиенте cs3=содержимое поля 'Старое имя' cs3Label=Старая группа клиента cs4=содержимое поля 'Новое имя' cs4Label=Новая группа клиента suser=содержимое поля 'Инициатор' externalId=4027 categorySignificance=/Informational categoryBehavior=/Modify/configuration categoryDeviceGroup=/Database catdt=Access and Identity Management categoryOutcome=/success categoryObject=/Host/Application	
4028 (0xFBC)	Создание группы в дереве иерархии	Сведения	Windows	Событие: Создание группы в дереве иерархии Инициатор: домен\логин Имя группы: Родительская группа:	Mon DD hh:mm:ss hostname CEF:0|GIS|Blockhost-Net|4.4 |BH-Admin-4028|Создание группы в дереве иерархии|Low| cat=Администрирование dhost=имя хоста источника события rt=дата возникновения события на клиенте cs5=содержимое поля 'Имя группы' cs5Label=Группа клиента cs4=содержимое поля 'Родительская группа' cs4Label=Новая группа клиента	

					suser=содержимое поля ‘Инициатор’ externalId=4028 categorySignificance=/Informational categoryBehavior=/Modify/configuration categoryDeviceGroup=/Database catdt=Access and Identity Management categoryOutcome=/success categoryObject=/Host/Application	
4031 (0xFBF)	Удаление группы из дерева иерархии	Сведения	Windows	Событие: удаление группы из дерева иерархии Инициатор: домен\логин Имя группы:	Mon DD hh:mm:ss hostname CEF:0|GIS|Blockhost-Net|4.4 |BH-ServiceControl-4031|Удаление группы из дерева иерархии|Low| cat=Администрирование dhost=имя хоста источника события rt=дата возникновения события на клиенте cs5=содержимое поля ‘Имя группы’ cs5Label=Группа клиента suser=содержимое поля ‘Инициатор’ externalId=4031 categorySignificance=/Informational categoryBehavior=/Modify/configuration categoryDeviceGroup=/Database catdt=Access and Identity Management categoryOutcome=/Success categoryObject=/Host/Application	
4032 (0xFC0)	Создание политики	Сведения	Windows	Событие: подключение консоли к серверу Инициатор: домен\логин Тип инициатора: Active Directory | локальный пользователь | собственный пользователь Блокхост-Сеть Полномочия: чтение, запись | чтение	Mon DD hh:mm:ss hostname CEF:0|GIS|Blockhost-Net|4.4 |BH-Admin-3943|Подключение консоли к серверу|Low| cat=Администрирование dhost=имя хоста источника события rt=дата возникновения события на клиенте cs1=содержимое поля ‘Тип инициатора’ cs1Label=Тип инициатора cs2=содержимое поля ‘Полномочия’ cs2Label=Полномочия администратора suser=содержимое поля ‘Инициатор’ externalId=3943 categorySignificance=/Informational categoryBehavior=/Access categoryDeviceGroup=/Application catdt=Access and Identity Management categoryOutcome=/success categoryObject=/Host/Application	Данное событие записывается в журнал сервера СЗИ при создании политики любого типа. Все политики создаются с настройками по умолчанию, которые соответствуют настройкам политик в группе «Все машины» сразу после установки сервера СЗИ.
4033 (0xFC1)	Изменение политики	Сведения	Windows	Событие: отказ на подключение консоли к серверу Причина: недостаточно прав Инициатор: домен\логин Тип инициатора: Active Directory | локальный пользователь |	Mon DD hh:mm:ss hostname CEF:0|GIS|Blockhost-Net|4.4 |BH-Admin-3944|Отказ на подключение консоли к серверу|High| cat=Администрирование	Событие создается при редактировании политики администратором.

				собственный пользователь Блокхост-Сеть	dhost=имя хоста источника события rt=дата возникновения события на клиенте cs1=содержимое поля ‘Тип инициатора’ cs1Label=Тип инициатора suser=содержимое поля ‘Инициатор’ reason=содержимое поля ‘Причина’ externalId=3944 categorySignificance=/Informational/Error categoryBehavior=/Access categoryDeviceGroup=/Application catdt=Access and Identity Management categoryOutcome=/Failure categoryObject=/Host/Application	
4034 (0xFC2)	Привязка политики к группе	Сведения	Windows	Событие: перемещение клиента в дереве иерархии Инициатор: домен\логин Имя клиента: IP клиента: Из группы: В группу:	Mon DD hh:mm:ss hostname CEF:0|GIS|Blockhost-Net|4.4 |BH-Admin-4024|Перемещение клиента в дереве иерархии|Low| cat=Администрирование dhost=имя хоста источника события rt=дата возникновения события на клиенте cs3=содержимое поля ‘Из группы’ cs3Label=Старая группа клиента cs4=содержимое поля ‘В группу’ cs4Label=Новая группа клиента dvc=содержимое поля ‘IP клиента’ dvchost=содержимое поля ‘Имя клиента’ suser=содержимое поля ‘Инициатор’ externalId=4024 categorySignificance=/Informational categoryBehavior=/Modify/configuration categoryDeviceGroup=/Database catdt=Access and Identity Management categoryOutcome=/success categoryObject=/Host/Application	Событие создается при привязке (линковке) политики к группе компьютеров.
4035 (0xFC3)	Отвязка политики от группы	Сведения	Windows	Событие: перемещение группы в дереве иерархии Инициатор: домен\логин Имя группы: Из группы: В группу:	Mon DD hh:mm:ss hostname CEF:0|GIS|Blockhost-Net|4.4 |BH-Admin-4025|Перемещение группы в дереве иерархии|Low| cat=Администрирование dhost=имя хоста источника события rt=дата возникновения события на клиенте cs5=содержимое поля ‘Имя группы’ cs5Label=Группа клиента cs3=содержимое поля ‘Из группы’ cs3Label=Старая группа клиента cs4=содержимое поля ‘В группу’ cs4Label=Новая группа клиента suser=содержимое поля ‘Инициатор’	Событие создается при отвязке политики от группы компьютеров.

					externalId=4025 categorySignificance=/Informational categoryBehavior=/Modify/configuration categoryDeviceGroup=/Database catdt=Access and Identity Management categoryOutcome=/success categoryObject=/Host/Application	
4036 (0xFC4)	Удаление политики	Сведения	Windows	Событие: удаление клиента из дерева иерархии Инициатор: домен\логин Имя клиента: IP клиента: Из группы:	Mon DD hh:mm:ss hostname CEF:0|GIS|Blockhost-Net|4.4 |BH-Admin-4026|Удаление клиента из дерева иерархии|Low| cat=Администрирование dhost=имя хоста источника события rt=дата возникновения события на клиенте cs5=содержимое поля 'Из группы' cs5Label=Группа клиента dvc=содержимое поля 'IP клиента' dvchost=содержимое поля 'Имя клиента' suser=содержимое поля 'Инициатор' externalId=4026 categorySignificance=/Informational categoryBehavior=/Modify/configuration categoryDeviceGroup=/Database catdt=Access and Identity Management categoryOutcome=/success categoryObject=/Host/Application	Событие создается при удалении политики из базы данных сервера
4037 (0xFC5)	Изменение настроек клиента	Сведения	Windows	Событие: изменение имени группы Инициатор: домен\логин Старое имя: Новое имя:	Mon DD hh:mm:ss hostname CEF:0|GIS|Blockhost-Net|4.4 |BH-Admin-4027|Изменение имени группы|Low| cat=Администрирование dhost=имя хоста источника события rt=дата возникновения события на клиенте cs3=содержимое поля 'Старое имя' cs3Label=Старая группа клиента cs4=содержимое поля 'Новое имя' cs4Label=Новая группа клиента suser=содержимое поля 'Инициатор' externalId=4027 categorySignificance=/Informational categoryBehavior=/Modify/configuration categoryDeviceGroup=/Database catdt=Access and Identity Management categoryOutcome=/success categoryObject=/Host/Application	Данное событие записывается в журнал сервера СЗИ при изменении настроек любого механизма безопасности вне политик.

1.13.2 Лицензирование

Код	Событие	Уровень	ОС	Шаблон	CEF-формат	Пояснение
4038 (0xFC6)	Добавление лицензии	Сведения	Windows	Событие: добавление лицензии Инициатор: домен\логин Ключ лицензии: Email администратора: Тип лицензии: Количество подключений: Действует с: Действует до:	Конвертация в CEF отсутствует (событие не передается в SIEM-систему)	Событие создается в результате успешной активации лицении.
4039 (0xFC7)	Удаление лицензии	Сведения	Windows	Событие: удаление лицензии Инициатор: домен\логин Ключ лицензии: Email администратора: Тип лицензии: Количество подключений: Действует с: Действует до:	Конвертация в CEF отсутствует (событие не передается в SIEM-систему)	Событие создается в результате удаления лицензии из Блокхост-Сеть.4
4040 (0xFC8)	Изменение лицензии	Предупреждение	Windows	Событие: изменение лицензии Ключ лицензии: Email: Инициатор: Сервер лицензирования Изменения в лицензии: <изменение параметров лицензии>[1]	Конвертация в CEF отсутствует (событие не передается в SIEM-систему)	Событие создается в момент проверки лицензии на валидность сервером БХ-Сеть, если параметры лицензии были изменены организацией, выдавшей эту лицензию. Инициатор всегда сервер лицензирования т.к. пока что не поддерживается функционал перевыпуска лицензии
4041 (0xFC9)	Истечение срока действия лицензии	Предупреждение	Windows	Событие: истечение срока действия лицензии Ключ лицензии: Email администратора: Тип лицензии: Количество подключений: Действует с: Действует до:	Конвертация в CEF отсутствует (событие не передается в SIEM-систему)	Событие создается, если срок действия лицензии истек. Проверка срока действия лицензии осуществляется сервером СЗИ в момент валидации лицензии.
4042 (0xFCA)	Ошибка при валидации лицензии	Ошибка	Windows	Событие: ошибка при валидации лицензии Причина: Ключ лицензии: Email администратора: Тип лицензии: Количество подключений: Действует с: Действует до:	Конвертация в CEF отсутствует (событие не передается в SIEM-систему)	Событие создается, если серверу СЗИ не удалось выполнить валидацию лицензии.

[1] См. приложение А

1.14 Управление жизненным циклом токенов

Код	Событие	Уровень	ОС	Шаблон	CEF-формат	Пояснение
4000 (0xFA0)	Регистрация токена	Сведения	Windows	Событие: регистрация токена Инициатор: домен\логин Событие: регистрация токена Инициатор: домен\логин Токен: тип токена, серийный номер, инвентарный номер Комментарий:	Mon DD hh:mm:ss hostname CEF:0|GIS|Blockhost-Net|4.4 |BH-TokenSystem- 4000|Регистрация токена|Low| cat=Управление жизненным циклом токенов dhost=имя хоста источника события rt=дата возникновения события на клиенте cs1=содержимое поля 'Токен' cs1Label=Токен cs2=содержимое поля 'Комментарий' cs2Label=Комментарий suser=содержимое поля 'Инициатор' externalId=4000 categorySignificance=/Informational categoryBehavior=/Modify/Configuration categoryDeviceGroup=/Database catdt=Access and Identity Management categoryOutcome=/Success categoryObject=/Host/Application	Данное событие записывается в журнал сервера СЗИ при регистрации токена в базе данных системы управления жизненным циклом токена
4001 (0xFA1)	Ошибка при регистрации токена	Ошибка	Windows	Событие: ошибка при регистрации токена Причина: Инициатор: домен\логин Токен: тип токена, серийный номер, инвентарный номер	Mon DD hh:mm:ss hostname CEF:0|GIS|Blockhost-Net|4.4 |BH-TokenSystem- 4001|Ошибка при регистрации токена|High| cat=Управление жизненным циклом токенов dhost=имя хоста источника события rt=дата возникновения события на клиенте cs1=содержимое поля 'Токен' cs1Label=Токен externalId=4001 reason=содержимое поля 'Причина' suser=содержимое поля 'Инициатор' categorySignificance=/Informational/Error categoryBehavior=/Modify/Configuration categoryDeviceGroup=/Database catdt=Access and Identity Management categoryOutcome=/Failure categoryObject=/Host/Application	Данное событие записывается в журнал сервера СЗИ при ошибке регистрации токена в базе данных системы управления жизненным циклом токена
4002 (0xFA2)	Удаление токена	Сведения	Windows	Событие: удаление токена Инициатор: домен\логин Токен: тип токена, серийный номер, инвентарный номер	Mon DD hh:mm:ss hostname CEF:0|GIS|Blockhost-Net|4.4 |BH-TokenSystem- 4002|Удаление токена|Low| cat=Управление жизненным циклом токенов dhost=имя хоста источника события	Данное событие записывается в журнал сервера СЗИ при удалении токена из базы данных системы управления жизненным циклом токена

					rt=дата возникновения события на клиенте cs1=содержимое поля ‘Токен’ cs1Label=Токен suser=содержимое поля ‘Инициатор’ externalId=4002 categorySignificance=/Informational categoryBehavior=/Modify/Configuration categoryDeviceGroup=/Database catdt=Access and Identity Management categoryOutcome=/Success categoryObject=/Host/Application	
4003 (0xFA3)	Ошибка при удалении токена	Ошибка	Windows	Событие: ошибка при удалении токена Причина: Инициатор: домен\логин Токен: тип токена, серийный номер, инвентарный номер	Mon DD hh:mm:ss hostname CEF:0|GIS|Blockhost-Net|4.4 |BH-TokenSystem- 4003|Ошибка при удалении токена|High| cat=Управление жизненным циклом токенов dhost=имя хоста источника события rt=дата возникновения события на клиенте cs1=содержимое поля ‘Токен’ cs1Label=Токен suser=содержимое поля ‘Инициатор’ reason=содержимое поля ‘Причина’ externalId=4003 categorySignificance=/Informational/Error categoryBehavior=/Modify/Configuration categoryDeviceGroup=/Database catdt=Access and Identity Management categoryOutcome=/Failure categoryObject=/Host/Application	Данное событие записывается в журнал сервера СЗИ при ошибке удаления токена из базы данных системы управления жизненным циклом токена
4006 (0xFA6)	Назначение токена пользователю для входа по управляемому сертификату PKI	Сведения	Windows	Событие: назначение токена пользователю для входа по управляемому сертификату PKI Инициатор: домен\логин Пользователь: домен\логин SID пользователя: ФИО пользователя: Токен: тип токена, серийный номер, инвентарный номер Комментарий: Выпущенный сертификат для входа: УЦ, S/N, CN Взятые под наблюдение сертификаты: перечень сертификатов Удаленные с токена сертификаты: перечень сертификатов	Mon DD hh:mm:ss hostname CEF:0|GIS|Blockhost-Net|4.4 |BH-TokenSystem- 4006|Назначение токена пользователю для входа по управляемому сертификату PKI |Low| cat=Управление жизненным циклом токенов dhost=имя хоста источника события rt=дата возникновения события на клиенте cs1=содержимое поля ‘Токен’ cs1Label=Токен cs2=содержимое поля ‘Комментарий’ cs2Label=Комментарий cs3=содержимое поля ‘ФИО пользователя’ cs3Label=ФИО пользователя cs4=содержимое поля ‘Выпущенный сертификат для входа’ cs4Label=Выпущенный сертификат для входа	Данное событие записывается в журнал сервера СЗИ при назначении пользователю токена для входа с использованием управляемого сертификата PKI

					cs5=содержимое поля ‘Взятые под наблюдение сертификаты’ cs5Label=Взятые под наблюдение сертификаты cs6=содержимое поля ‘Удаленные с токена сертификаты’ cs6Label=Удаленные с токена сертификаты suser=содержимое поля ‘Инициатор’ duser=содержимое поля ‘Пользователь’ suid=содержимое поля ‘SID пользователя’ externalId=4006 ccategorySignificance=/Informational categoryBehavior=/Modify/Configuration categoryDeviceGroup=/Database catdt=Access and Identity Management categoryOutcome=/Success categoryObject=/Host/Application	
4007 (0xFA7)	Ошибка при назначении токена пользователю для входа по управляемому сертификату PKI	Ошибка	Windows	Событие: ошибка при назначении токена пользователю для входа по управляемому сертификату PKI Причина: Инициатор: домен\логин Пользователь: домен\логин ФИО пользователя: Токен: тип токена, серийный номер, инвентарный номер	Mon DD hh:mm:ss hostname CEF:0|GIS|Blockhost-Net|4.4 |BH-TokenSystem- 4007|Ошибка при назначении токена пользователю для входа по управляемому сертификату PKI|High| cat=Управление жизненным циклом токенов dhost=имя хоста источника события rt=дата возникновения события на клиенте cs1=содержимое поля ‘Токен’ cs1Label=Токен cs3=содержимое поля ‘ФИО пользователя’ cs3Label=ФИО пользователя suser=содержимое поля ‘Инициатор’ duser=содержимое поля ‘Пользователь’ reason=содержимое поля ‘Причина’ externalId=4007 categorySignificance=/Informational/Error categoryBehavior=/Modify/Configuration categoryDeviceGroup=/Database catdt=Access and Identity Management categoryOutcome=/Failure categoryObject=/Host/Application	Данное событие записывается в журнал сервера СЗИ при ошибке назначении пользователю токена для входа с использованием управляемого сертификата PKI
4043 (0xFCB)	Назначение токена пользователю для входа по стороннему сертификату PKI	Сведения	Windows	Событие: назначение токена пользователю для входа по стороннему сертификату PKI Инициатор: домен\логин Пользователь: домен\логин SID пользователя: ФИО пользователя: Токен: тип токена, серийный номер, инвентарный номер	Mon DD hh:mm:ss hostname CEF:0|GIS|Blockhost-Net|4.4 |BH-TokenSystem- 4043|Назначение токена пользователю для входа по стороннему сертификату PKI |Low| cat=Управление жизненным циклом токенов dhost=имя хоста источника события rt=дата возникновения события на клиенте	Данное событие записывается в журнал сервера СЗИ при назначении пользователю токена для входа с использованием стороннего сертификата PKI

				Комментарий: Взятые под наблюдение сертификаты: перечень сертификатов	cs1=содержимое поля ‘Токен’ cs1Label=Токен cs2=содержимое поля ‘Комментарий’ cs2Label=Комментарий cs3=содержимое поля ‘ФИО пользователя’ cs3Label=ФИО пользователя cs5=содержимое поля ‘Взятые под наблюдение сертификаты’ cs5Label=Взятые под наблюдение сертификаты suser=содержимое поля ‘Инициатор’ duser=содержимое поля ‘Пользователь’ suid=содержимое поля ‘SID пользователя’ externalId=4043 ccategorySignificance=/Informational categoryBehavior=/Modify/Configuration categoryDeviceGroup=/Database catdt=Access and Identity Management categoryOutcome=/Success categoryObject=/Host/Application	
4044 (0xFCC)	Ошибка при назначении токена пользователю для входа по стороннему сертификату PKI	Ошибка	Windows	Событие: ошибка при назначении токена пользователю для входа по стороннему сертификату PKI Причина: Инициатор: домен\логин Пользователь: домен\логин ФИО пользователя: Токен: тип токена, серийный номер, инвентарный номер	Mon DD hh:mm:ss hostname CEF:0|GIS|Blockhost-Net|4.4 |BH-TokenSystem-4044|Ошибка при назначении токена пользователю для входа по стороннему сертификату PKI|High| cat=Управление жизненным циклом токенов dhost=имя хоста источника события rt=дата возникновения события на клиенте cs1=содержимое поля ‘Токен’ cs1Label=Токен cs3=содержимое поля ‘ФИО пользователя’ cs3Label=ФИО пользователя suser=содержимое поля ‘Инициатор’ duser=содержимое поля ‘Пользователь’ reason=содержимое поля ‘Причина’ externalId=4044 categorySignificance=/Informational/Error categoryBehavior=/Modify/Configuration categoryDeviceGroup=/Database catdt=Access and Identity Management categoryOutcome=/Failure categoryObject=/Host/Application	Данное событие записывается в журнал сервера СЗИ при ошибке назначении пользователю токена для входа с использованием управляемого сертификата PKI
4008 (0xFA8)	Назначение токена пользователю для безопасного входа по паролю	Сведения	Windows	Событие: назначение токена пользователю для безопасного входа по паролю Инициатор: домен\логин Пользователь: домен\логин ФИО пользователя:	Mon DD hh:mm:ss hostname CEF:0|GIS|Blockhost-Net|4.4 |BH-TokenSystem-4008|Назначение токена пользователю для безопасного входа по паролю|Low| cat=Управление жизненным циклом	Данное событие записывается в журнал при назначении токена пользователю для безопасного входа по паролю

				SID пользователя: Токен: тип токена, серийный номер, инвентарный номер Комментарий: Взятые под наблюдения сертификаты: перечень сертификатов	токенов dhost=имя хоста источника события rt=дата возникновения события на клиенте cs1=содержимое поля ‘Токен’ cs1Label=Токен cs3=содержимое поля ‘ФИО пользователя’ cs3Label=ФИО пользователя cs5=содержимое поля ‘Взятые под наблюдения сертификаты’ cs5Label=Взятые под наблюдения сертификаты suser=содержимое поля ‘Инициатор’ duser=содержимое поля ‘Пользователь’ suid=содержимое поля ‘SID пользователя’ externalId=4008 categorySignificance=/Informational categoryBehavior=/Modify/Configuration categoryDeviceGroup=/Database catdt=Access and Identity Management categoryOutcome=/Success categoryObject=/Host/Application	
4009 (0xFA9)	Ошибка при назначении токена пользователю для безопасного входа по паролю	Ошибка	Windows	Событие: ошибка при назначении токена пользователю для безопасного входа по паролю Причина: Инициатор: домен\логин Пользователь: домен\логин Токен: тип токена, серийный номер, инвентарный номер	Mon DD hh:mm:ss hostname CEF:0|GIS|Blockhost-Net|4.4 |BH-TokenSystem-4009|Ошибка при назначении токена пользователю для безопасного входа по паролю|High| cat=Управление жизненным циклом токенов dhost=имя хоста источника события rt=дата возникновения события на клиенте cs1=содержимое поля ‘Токен’ cs1Label=Токен reason=содержимое поля ‘Причина’ suser=содержимое поля ‘Инициатор’ duser=содержимое поля ‘Пользователь’ externalId=4009 categorySignificance=/Informational/Error categoryBehavior=/Modify/Configuration categoryDeviceGroup=/Database catdt=Access and Identity Management categoryOutcome=/Failure categoryObject=/Host/Application	Данное событие записывается в журнал при ошибке назначении токена пользователю для безопасного входа по паролю
4010 (0xFAA)	Назначение токена пользователю для учета	Сведения	Windows	Событие: назначение токена пользователю для учета Инициатор: домен\логин Пользователь: домен\логин ФИО пользователя: SID пользователя: Токен: тип токена, серийный номер, инвентарный номер	Mon DD hh:mm:ss hostname CEF:0|GIS|Blockhost-Net|4.4 |BH-TokenSystem-4010|Назначение токена пользователю для учета|Low| cat=Управление жизненным циклом токенов dhost=имя хоста источника события rt=дата возникновения события на клиенте	Данное событие записывается в журнал при назначении пользователю токена для учета

				Взятые под наблюдение сертификаты: перечень сертификатов	cs1=содержимое поля ‘Токен’ cs1Label=Токен cs3=содержимое поля ‘ФИО пользователя’ cs3Label=ФИО пользователя cs5=содержимое поля ‘Взятые под наблюдения сертификаты’ cs5Label=Взятые под наблюдения сертификаты suser=содержимое поля ‘Инициатор’ duser=содержимое поля ‘Пользователь’ suid=содержимое поля ‘SID пользователя’ externalId=4010 categorySignificance=/Informational categoryBehavior=/Modify/Configuration categoryDeviceGroup=/Database catdt=Access and Identity Management categoryOutcome=/Success categoryObject=/Host/Application	
4011 (0xFAB)	Ошибка при назначении токена пользователю для учета	Ошибка	Windows	Событие: ошибка при назначении токена пользователю для учета Причина: Инициатор: домен\логин Пользователь: домен\логин Токен: тип токена, серийный номер, инвентарный номер	Mon DD hh:mm:ss hostname CEF:0|GIS|Blockhost-Net|4.4 |BH-TokenSystem- 4011|Ошибка при назначении токена пользователю для учета|High| cat=Управление жизненным циклом токенов dhost=имя хоста источника события rt=дата возникновения события на клиенте cs1=содержимое поля ‘Токен’ cs1Label=Токен suser=содержимое поля ‘Инициатор’ duser=содержимое поля ‘Пользователь’ reason=содержимое поля ‘Причина’ externalId=4011 categorySignificance=/Informational/Error categoryBehavior=/Modify/Configuration categoryDeviceGroup=/Database catdt=Access and Identity Management categoryOutcome=/Failure categoryObject=/Host/Application	Данное событие записывается в журнал при ошибке назначении токена пользователю для учета
4004 (0xFA4)	Изъятие токена у пользователя	Сведения	Windows	Событие: изъятие токена у пользователя Инициатор: домен\логин Пользователь: домен\логин Токен: тип токена, серийный номер, инвентарный номер	Mon DD hh:mm:ss hostname CEF:0|GIS|Blockhost-Net|4.4 |BH-TokenSystem- 4004|Изъятие токена у пользователя|Low| cat=Управление жизненным циклом токенов dhost=имя хоста источника события rt=дата возникновения события на клиенте cs1=содержимое поля ‘Токен’ cs1Label=Токен suser=содержимое поля ‘Инициатор’	Данное событие записывается в журнал при изъятии токена у пользоателя.

					duser=содержимое поля ‘Пользователь’ externalId=4004 categorySignificance=/Informational categoryBehavior=/Modify/Configuration categoryDeviceGroup=/Database catdt=Access and Identity Management categoryOutcome=/Success categoryObject=/Host/Application	
4005 (0xFA5)	Ошибка при изъятии токена у пользователя	Ошибка	Windows	Событие: ошибка при изъятии токена у пользователя Причина: Инициатор: домен\логин Пользователь: домен\логин ФИО пользователя: Токен: тип токена, серийный номер, инвентарный номер	Mon DD hh:mm:ss hostname CEF:0|GIS|Blockhost-Net|4.4 |BH-TokenSystem- 4005|Ошибка при изъятии токена у пользов ателя|High| cat=Управление жизненным циклом токенов dhost=имя хоста источника события rt=дата возникновения события на клиенте cs1=содержимое поля ‘Токен’ cs1Label=Токен cs3=содержимое поля ‘ФИО пользователя’ cs3Label=ФИО пользователя suser=содержимое поля ‘Инициатор’ duser=содержимое поля ‘Пользователь’ reason=содержимое поля ‘Причина’ externalId=4005 categorySignificance=/Informational/Error categoryBehavior=/Modify/Configuration categoryDeviceGroup=/Database catdt=Access and Identity Management categoryOutcome=/Failure categoryObject=/Host/Application	Данное событие записывается в журнал сервера СЗИ при ошибке изъятия токена у пользователя
4012 (0xFAC)	Включение токена	Сведения	Windows	Событие: включение токена Инициатор: домен\логин Пользователь: Токен: тип токена, серийный номер, инвентарный номер Возобновляемый сертификат: УЦ, S/N, CN	Mon DD hh:mm:ss hostname CEF:0|GIS|Blockhost-Net|4.4 |BH-TokenSystem-4012|Включение токена |Low| cat=Управление жизненным циклом токенов dhost=имя хоста источника события rt=дата возникновения события на клиенте cs1=содержимое поля ‘Токен’ cs1Label=Токен cs4=содержимое поля ‘Возобновляемый сертификат’ cs4Label=Выпущенный сертификат для входа suser=содержимое поля ‘Инициатор’ duser=содержимое поля ‘Пользователь’ externalId=4012 categorySignificance=/Informational categoryBehavior=/Modify/Configuration	Данное событие записывается в журнал при включении токена?

					categoryDeviceGroup=/Database catdt=Access and Identity Management categoryOutcome=/Success categoryObject=/Host/Application	
4013 (0xFAD)	Ошибка при включении токена	Ошибка	Windows	Событие: ошибка при выключении токена Причина: Инициатор: домен\логин Пользователь: домен\логин Токен: тип токена, серийный номер, инвентарный номер Возобновляемый сертификат: УЦ, S/N, CN	Mon DD hh:mm:ss hostname CEF:0|GIS|Blockhost-Net|4.4 |BH-TokenSystem- 4013|Ошибка при включении токена|High| cat=Управление жизненным циклом токенов dhost=имя хоста источника события rt=дата возникновения события на клиенте cs1=содержимое поля ‘Токен’ cs1Label=Токен cs4=содержимое поля ‘Возобновляемый сертификат’ cs4Label=Выпущенный сертификат для входа suser=содержимое поля ‘Инициатор’ duser=содержимое поля ‘Пользователь’ reason=содержимое поля ‘Причина’ externalId=4013 categorySignificance=/Informational/Error categoryBehavior=/Modify/Configuration categoryDeviceGroup=/Database catdt=Access and Identity Management categoryOutcome=/Failure categoryObject=/Host/Application	Данное событие записывается в журнал при возникновении ошибки включения токена
4014 (0xFAE)	Выключение токена	Сведения	Windows	Событие: выключение токена Инициатор: домен\логин Пользователь: домен\логин Токен: тип токена, серийный номер, инвентарный номер Временно отзываемый сертификат: УЦ, S/N, CN	Mon DD hh:mm:ss hostname CEF:0|GIS|Blockhost-Net|4.4 |BH-TokenSystem- 4014|Выключение токена|Low| cat=Управление жизненным циклом токенов dhost=имя хоста источника события rt=дата возникновения события на клиенте cs1=содержимое поля ‘Токен’ cs1Label=Токен cs4=содержимое поля ‘Временно отзываемый сертификат’ cs4Label=Выпущенный сертификат для входа suser=содержимое поля ‘Инициатор’ duser=содержимое поля ‘Пользователь’ externalId=4014 categorySignificance=/Informational categoryBehavior=/Modify/Configuration categoryDeviceGroup=/Database catdt=Access and Identity Management categoryOutcome=/Success	Данное событие записывается в журнал при выключении токена

					categoryObject=/Host/Application	
4015 (0xFAF)	Ошибка при выключении токена	Ошибка	Windows	Событие: ошибка при выключении токена Причина: Инициатор: домен\логин Пользователь: домен\логин Токен: тип токена, серийный номер, инвентарный номер Временно отзываемый сертификат: УЦ, S/N, CN	Mon DD hh:mm:ss hostname CEF:0|GIS|Blockhost-Net|4.4 |BH-TokenSystem-4015|Ошибка при выключении токена|High | cat=Управление жизненным циклом токенов dhost=имя хоста источника события rt=дата возникновения события на клиенте cs1=содержимое поля 'Токен' cs1Label=Токен cs4=содержимое поля 'Временно отзываемый сертификат' cs4Label=Выпущенный сертификат для входа reason=содержимое поля 'Причина' suser=содержимое поля 'Инициатор' duser=содержимое поля 'Пользователь' externalId=4015 categorySignificance=/Informational/Error categoryBehavior=/Modify/Configuration categoryDeviceGroup=/Database catdt=Access and Identity Management categoryOutcome=/Failure categoryObject=/Host/Application	Данное событие записывается в журнал в случае возникновения ошибки при выключении токена
4016 (0xFB0)	Отзыв токена	Сведения	Windows	Событие: отзыв токена Инициатор: домен\логин Пользователь: домен\логин Токен: тип токена, серийный номер, инвентарный номер Отзываемый сертификат: УЦ, S/N, CN	Mon DD hh:mm:ss hostname CEF:0|GIS|Blockhost-Net|4.4 |BH-TokenSystem-4016|Отзыв токена|Low| cat=Управление жизненным циклом токенов dhost=имя хоста источника события rt=дата возникновения события на клиенте cs1=содержимое поля 'Токен' cs1Label=Токен cs4=содержимое поля 'Отзываемый сертификат' cs4Label=Выпущенный сертификат для входа suser=содержимое поля 'Инициатор' duser=содержимое поля 'Пользователь' externalId=4016 categorySignificance=/Informational categoryBehavior=/Modify/Configuration categoryDeviceGroup=/Database catdt=Access and Identity Management categoryOutcome=/Success categoryObject=/Host/Application	Данное событие записывается в журнал при успешном отзыве токена
4017 (0xFB1)	Ошибка при отзыве	Ошибка	Windows	Событие: ошибка при отзыве токена Причина:	CEF:0|GIS|Blockhost-Net|4.4 |BH-TokenSystem-4017|Ошибка при отзыве	Данное событие записывается в журнал в случае возникновения

	токена			Инициатор: домен\логин Пользователь: домен\логин Токен: тип токена, серийный номер, инвентарный номер Отзываемый сертификат: УЦ, S/N, CN	токена|High| cat=Управление жизненным циклом токенов dhost=имя хоста источника события rt=дата возникновения события на клиенте cs1=содержимое поля 'Токен' cs1Label=Токен cs4=содержимое поля 'Отзываемый сертификат' cs4Label=Выпущенный сертификат для входа reason=содержимое поля 'Причина' suser=содержимое поля 'Инициатор' duser=содержимое поля 'Пользователь' externalId=4017 categorySignificance=/Informationa/Error categoryBehavior=/Modify/Configuration categoryDeviceGroup=/Database catdt=Access and Identity Management categoryOutcome=/Failure categoryObject=/Host/Application	ошибки при отзыве токена
4018 (0xFB2)	Синхронизация токена	Сведения	Windows	Событие: синхронизация токена Инициатор: домен\логин Пользователь: домен\логин Токен: тип токена, серийный номер, инвентарный номер Изменения: <изменения на токене>[2]	Mon DD hh:mm:ss hostname CEF:0|GIS|Blockhost-Net|4.4|BH-TokenSystem-4018|Синхронизация токена|Low| cat=Управление жизненным циклом токенов dhost=имя хоста источника события rt=дата возникновения события на клиенте cs1=содержимое поля 'Токен' cs1Label=Токен cs5=содержимое поля 'Изменения' cs5Label=Взятые под наблюдения сертификаты suser=содержимое поля 'Инициатор' duser=содержимое поля 'Пользователь' externalId=4018 categorySignificance=/Informational categoryBehavior=/Modify/Configuration categoryDeviceGroup=/Identity Management catdt=Access and Identity Management categoryOutcome=/Success categoryObject=/Host/Application	Данное событие записывается в журнал аудита при синхронизации токена на клиенте или сервере Блокхост-сеть
4019 (0xFB3)	Ошибка при синхронизации токена	Ошибка	Windows	Событие: ошибка при синхронизации токена Причина: Инициатор: домен\логин	Mon DD hh:mm:ss hostname CEF:0|GIS|Blockhost-Net|4.4|BH-TokenSystem-4019|Ошибка при синхронизации токена|Hi	Данное событие записывается в журнал аудита при ошибке синхронизации токена

[2] См. приложение В

				Пользователь: домен\логин Токен: тип токена, серийный номер, инвентарный номер	gh| cat=Управление жизненным циклом токенов dhost=имя хоста источника события rt=дата возникновения события на клиенте cs1=содержимое поля ‘Токен’ cs1Label=Токен reason=содержимое поля ‘Причина’ suser=содержимое поля ‘Инициатор’ duser=содержимое поля ‘Пользователь’ externalId=4019 reason=содержимое поля ‘Причина’ categorySignificance=/Informational/Error categoryBehavior=/Modify/Configuration categoryDeviceGroup=/Identity Management catdt=Access and Identity Management categoryOutcome=/Failure categoryObject=/Host/Application	
4020 (0xFB4)	Изменение параметров токена	Сведения	Windows	Событие: изменение параметров токена Инициатор: домен\логин Токен: тип токена, серийный номер, инвентарный номер Комментарий:	Mon DD hh:mm:ss hostname CEF:0|GIS|Blockhost-Net|4.4 |BH-TokenSystem- 4020|Измененииепараметровтокена|Low| cat=Управление жизненным циклом токенов dhost=имя хоста источника события rt=дата возникновения события на клиенте cs1=содержимое поля ‘Токен’ cs1Label=Токен cs2=содержимое поля ‘Комментарий’ cs2Label=Комментарий suser=содержимое поля ‘Инициатор’ externalId=4020 categorySignificance=/Informational categoryBehavior=/Modify/Configuration categoryDeviceGroup=/Identity Management catdt=Access and Identity Management categoryOutcome=/Success categoryObject=/Host/Application	Данное событие записывается в журнал аудита при успешном изменении параметра токена
4021 (0xFB5)	Ошибка при изменении параметров токена	Ошибка	Windows	Событие: ошибка при изменении параметров токена Причина: Инициатор: домен\логин Токен: тип токена, серийный номер, инвентарный номер	Mon DD hh:mm:ss hostname CEF:0|GIS|Blockhost-Net|4.4 |BH-TokenSystem- 4021|Ошибка при изменении параметров токена|High| cat=Управление жизненным циклом токенов dhost=имя хоста источника события rt=дата возникновения события на клиенте cs1=содержимое поля ‘Токен’ cs1Label=Токен reason=содержимое поля ‘Причина’	Данное событие записывается в журнал аудита при ошибке изменении параметров токена

					suser=содержимое поля ‘Инициатор’ externalId=4021 categorySignificance=/Informational/Error categoryBehavior=/Modify/Configuration categoryDeviceGroup=/Identity Management catdt=Access and Identity Management categoryOutcome=/Failure categoryObject=/Host/Application	
4022 (0xFB6)	Ошибка при отправке уведомления пользователю	Ошибка	Windows	Событие: ошибка при отправке уведомления пользователю Причина:	Mon DD hh:mm:ss hostname CEF:0|GIS|Blockhost-Net|4.4 |BH-TokenSystem-4022|Ошибка при отправке уведомления пользователю|High| cat=Управление жизненным циклом токенов dhost=имя хоста источника события rt=дата возникновения события на клиенте reason=содержимое поля ‘Причина’ externalId=4022 categorySignificance=/Informational/Error categoryBehavior=/Communicate categoryDeviceGroup=/Identity Management catdt=Access and Identity Management categoryOutcome=/Failure categoryObject=/Host/Application	Данное событие записывается в журнал аудита при ошибке отправки уведомления пользователю
4023 (0xFB7)	Ошибка при отправке уведомления администратору	Ошибка	Windows	Событие: ошибка при отправке уведомления администратору Причина:	Mon DD hh:mm:ss hostname CEF:0|GIS|Blockhost-Net|4.4 |BH-TokenSystem-4023|Ошибка при отправке уведомления администратору|High| cat=Управление жизненным циклом токенов dhost=имя хоста источника события rt=дата возникновения события на клиенте reason=содержимое поля ‘Причина’ externalId=4023 categorySignificance=/Informational/Error categoryBehavior=/Communicate categoryDeviceGroup=/Identity Management catdt=Access and Identity Management categoryOutcome=/Failure categoryObject=/Host/Application	Данное событие записывается в журнал аудита при ошибке отправки уведомления администратору
4049 (0xFD1)	Замена токена мастер-сервером	Сведения	Windows	Событие: замена токена мастер-сервером Мастер-сервер: имя сервера Старый токен: тип токена, серийный номер, инвентарный номер Новый токен: тип токена, серийный номер, инвентарный номер	Mon DD hh:mm:ss hostname CEF:0|GIS|Blockhost-Net|4.4 |BH-TokenSystem-4049|Замена токена мастер-сервером|Low| cat=Управление жизненным циклом токенов dhost=имя хоста источника события rt=дата возникновения события на клиенте sourceHostName= содержимое поля	Данное событие записывается в журнал сервера СЗИ при замене токена мастер-сервером в базе данных системы управления жизненным циклом токена

					‘Мастер-сервер’ cs1=содержимое поля ‘Старый токен’ cs1Label=Старый токен externalId=4049 categorySignificance=/Informational categoryBehavior=/Modify/Configuration categoryDeviceGroup=/Database catdt=Access and Identity Management categoryOutcome=/Success categoryObject=/Host/Application	
4057 (0xFD9)	Привязка токена пользователю SafeNode	Сведения	Windows	Событие: привязка токена пользователю SafeNode Инициатор: домен\логин Пользователь: логин Токен: тип токена, серийный номер, инвентарный номер	Mon DD hh:mm:ss hostname CEF:0|GIS|Blockhost-Net|4.4 |BH-TokenSystem-4057 | Привязка токена пользователю SafeNode |Low| cat=Управление жизненным циклом токенов dhost=имя хоста источника события rt=дата возникновения события на клиенте cs1=содержимое поля ‘Токен’ cs1Label=Токен suser=содержимое поля ‘Инициатор’ duser=содержимое поля ‘Пользователь’ externalId= 4057 ccategorySignificance=/Informational categoryBehavior=/Modify/Configuration categoryDeviceGroup=/Database catdt=Access and Identity Management categoryOutcome=/Success categoryObject=/Host/Application	Данное событие записывается в журнал сервера СЗИ при привязке пользователя SafeNode.
4058 (0xFDA)	Отвязка токена от пользователя SafeNode	Сведения	Windows	Событие: Отвязка токена от пользователя SafeNode Инициатор: домен\логин Пользователь: логин Токен: тип токена, серийный номер, инвентарный номер	Mon DD hh:mm:ss hostname CEF:0|GIS|Blockhost-Net|4.4 |BH-TokenSystem-4058| Отвязка токена от пользователя SafeNode |Low| cat=Управление жизненным циклом токенов dhost=имя хоста источника события rt=дата возникновения события на клиенте cs1=содержимое поля ‘Токен’ cs1Label=Токен suser=содержимое поля ‘Инициатор’ duser=содержимое поля ‘Пользователь’ externalId=4058 categorySignificance=/Informational categoryBehavior=/Modify/Configuration categoryDeviceGroup=/Database catdt=Access and Identity Management categoryOutcome=/Success categoryObject=/Host/Application	Данное событие записывается в журнал при отвязке токена от пользователя SafeNode.

1.15 Установка/удаление программ

Код события	Тип события	Уровень важности	ОС	Формат события ОС	CEF-формат	Условия воспроизведения
3585 (0xE01)	Создание задачи на установку агента системы развертывания	Сведения	Windows	Событие: создание задачи на установку агента системы развертывания Инициатор: домен\логин Имя задачи: Имя инстал. пакета: Дистрибутив: Версия дистрибутива: Параметры командной строки:	Конвертация в CEF отсутствует (событие не передается в SIEM-систему)	
3586 (0xE02)	Создание задачи на установку произвольной программы	Сведения	Windows	Событие: создание задачи на установку произвольной программы Инициатор: домен\логин Имя задачи: Имя инстал. пакета: Дистрибутив: Версия дистрибутива: Параметры командной строки:	Конвертация в CEF отсутствует (событие не передается в SIEM-систему)	
3587 (0xE03)	Создание задачи на удаление Блокхост-Сеть Клиент	Сведения	Windows	Событие: создание задачи на удаление Блокхост-Сеть Клиент Инициатор: домен\логин Имя задачи:	Конвертация в CEF отсутствует (событие не передается в SIEM-систему)	
3588 (0xE04)	Создание задачи на удаление программы, установленной с помощью системы развертывания	Сведения	Windows	Событие: создание задачи на удаление программы из списка инст. пакетов Инициатор: домен\логин Имя задачи: Имя инстал. пакета: Дистрибутив: Версия дистрибутива: Параметры командной строки:	Конвертация в CEF отсутствует (событие не передается в SIEM-систему)	
3589 (0xE05)	Создание задачи на удаление программы командным скриптом	Сведения	Windows	Событие: создание задачи на удаление программы командным скриптом Инициатор: домен\логин Имя задачи: Файл скрипта: Параметры командной строки:	Конвертация в CEF отсутствует (событие не передается в SIEM-систему)	
3590 (0xE06)	Редактирование задачи на установку агента системы развертывания	Сведения	Windows	Событие: редактирование задачи на установку агента системы развертывания Инициатор: домен\логин Имя задачи:	Конвертация в CEF отсутствует (событие не передается в SIEM-систему)	
3591 (0xE07)	Редактирование задачи на установку	Сведения	Windows	Событие: редактирование задачи на установку произвольной	Конвертация в CEF отсутствует (событие не передается в SIEM-систему)	

	произвольной программы			программы Инициатор: домен\логин Имя задачи:		
3592 (0xE08)	Редактирование задачи на удаление БлокхостСеть Клиент	Сведения	Windows	Событие: редактирование задачи на удаление БлокхостСеть Клиент Инициатор: домен\логин Имя задачи:	Конвертация в CEF отсутствует (событие не передается в SIEM-систему)	
3593 (0xE09)	Редактирование задачи на удаление программы из списка инст. пакетов	Сведения	Windows	Событие: редактирование задачи на удаление программы из списка инст. пакетов Инициатор: домен\логин Имя задачи:	Конвертация в CEF отсутствует (событие не передается в SIEM-систему)	
3594 (0xE0A)	Редактирование задачи на удаление программы командным скриптом	Сведения	Windows	Событие: редактирование задачи на удаление программы командным скриптом Инициатор: домен\логин Имя задачи:	Конвертация в CEF отсутствует (событие не передается в SIEM-систему)	
3595 (0xE0B)	Удаление задачи на установку агента системы развертывания	Сведения	Windows	Событие: удаление задачи на установку агента системы развертывания Инициатор: домен\логин Имя задачи:	Конвертация в CEF отсутствует (событие не передается в SIEM-систему)	
3596 (0xE0C)	Удаление задачи на установку произвольной программы	Сведения	Windows	Событие: удаление задачи на установку произвольной программы Инициатор: домен\логин Имя задачи:	Конвертация в CEF отсутствует (событие не передается в SIEM-систему)	
3597 (0xE0D)	Удаление задачи на удаление БлокхостСеть Клиент	Сведения	Windows	Событие: удаление задачи на удаление БлокхостСеть Клиент Инициатор: домен\логин Имя задачи:	Конвертация в CEF отсутствует (событие не передается в SIEM-систему)	
3598 (0xE0E)	Удаление задачи на удаление программы из списка инст. пакетов	Сведения	Windows	Событие: удаление задачи на удаление программы из списка инст. пакетов Инициатор: домен\логин Имя задачи:	Конвертация в CEF отсутствует (событие не передается в SIEM-систему)	
3599 (0xE0F)	Удаление задачи на удаление программы командным скриптом	Сведения	Windows	Событие: удаление задачи на удаление программы командным скриптом Инициатор: домен\логин Имя задачи:	Конвертация в CEF отсутствует (событие не передается в SIEM-систему)	
3600 (0xE10)	Запуск задачи на установку агента системы развертывания	Сведения	Windows	Событие: запуск задачи на установку агента системы развертывания Тип запуска: автоматически | вручную Инициатор: домен\логин Имя задачи: Имя инстал. пакета:	Конвертация в CEF отсутствует (событие не передается в SIEM-систему)	

				Дистрибутив: Версия дистрибутива: Параметры командной строки:		
3601 (0xE11)	Запуск задачи на установку произвольной программы	Сведения	Windows	Событие: запуск задачи на установку произвольной программы Тип запуска: автоматически |вручную Инициатор: домен\логин Имя задачи: Имя инстал. пакета: Дистрибутив: Версия дистрибутива: Параметры командной строки:	Конвертация в CEF отсутствует (событие не передается в SIEM-систему)	
3602 (0xE12)	Запуск задачи на удаление БлокхостСеть Клиент	Сведения	Windows	Событие: запуск задачи на удаление Блокхост-Сеть Клиент Тип запуска: автоматически |вручную Инициатор: домен\логин Имя задачи:	Конвертация в CEF отсутствует (событие не передается в SIEM-систему)	
3603 (0xE13)	Запуск задачи на удаление программы из списка инст. пакетов	Сведения	Windows	Событие: запуск задачи на удаление программы из списка инст. Пакетов Тип запуска: автоматически |вручную Инициатор: домен\логин Имя задачи: Имя инстал. пакета: Дистрибутив: Версия дистрибутива: Параметры командной строки:	Конвертация в CEF отсутствует (событие не передается в SIEM-систему)	
3604 (0xE14)	Запуск задачи на удаление программы командным скриптом	Сведения	Windows	Событие: запуск задачи на удаление программы командным скриптом Тип запуска: автоматически |вручную Инициатор: домен\логин Имя задачи: Файл скрипта: Параметры командной строки:	Конвертация в CEF отсутствует (событие не передается в SIEM-систему)	
3605 (0xE15)	Остановка задачи на установку агента системы развертывания	Сведения	Windows	Событие: остановка задачи на установку агента системы развертывания Инициатор: домен\логин Имя задачи:	Конвертация в CEF отсутствует (событие не передается в SIEM-систему)	
3606 (0xE16)	Остановка задачи на установку произвольной программы	Сведения	Windows	Событие: остановка задачи на установку произвольной программы Инициатор: домен\логин	Конвертация в CEF отсутствует (событие не передается в SIEM-систему)	

				Имя задачи:		
3607 (0xE17)	Остановка задачи на удаление БлокхостСеть Клиент	Сведения	Windows	Событие: остановка задачи на удаление БлокхостСеть Клиент Инициатор: домен\логин Имя задачи:	Конвертация в CEF отсутствует (событие не передается в SIEM-систему)	
3608 (0xE18)	Остановка задачи на удаление программы из списка инст. пакетов	Сведения	Windows	Событие: остановка задачи на удаление программы из списка инст. пакетов Инициатор: домен\логин Имя задачи:	Конвертация в CEF отсутствует (событие не передается в SIEM-систему)	
3609 (0xE19)	Остановка задачи на удаление программы командным скриптом	Сведения	Windows	Событие: остановка задачи на удаление программы командным скриптом Инициатор: домен\логин Имя задачи:	Конвертация в CEF отсутствует (событие не передается в SIEM-систему)	
3610 (0xE1A)	Создание инсталляционного пакета	Сведения	Windows	Событие: создание инсталляционного пакета Инициатор: домен\логин Имя пакета: Дистрибутив: Версия дистрибутива: Параметры командной строки:	Конвертация в CEF отсутствует (событие не передается в SIEM-систему)	
3611 (0xE1B)	Редактирование инсталляционного пакета	Сведения	Windows	Событие: редактирование инсталляционного пакета Инициатор: домен\логин Имя пакета: Дистрибутив: Версия дистрибутива: Параметры командной строки:	Конвертация в CEF отсутствует (событие не передается в SIEM-систему)	
3612 (0xE1C)	Удаление инсталляционного пакета	Сведения	Windows	Событие: удаление инсталляционного пакета Инициатор: домен\логин Имя пакета:	Конвертация в CEF отсутствует (событие не передается в SIEM-систему)	
4050 (0xFD2)	Создание задачи на удаление модуля аутентификации	Сведения	Linux	Событие: создание задачи на удаление модуля аутентификации Инициатор: домен\логин Имя задачи:	Конвертация в CEF отсутствует (событие не передается в SIEM-систему)	
4051 (0xFD3)	Редактирование задачи на удаление модуля аутентификации	Сведения	Linux	Событие: редактирование задачи на удаление модуля аутентификации Инициатор: домен\логин Имя задачи:	Конвертация в CEF отсутствует (событие не передается в SIEM-систему)	
4052 (0xFD4)	Удаление задачи на удаление модуля аутентификации	Сведения	Linux	Событие: удаление задачи на удаление модуля аутентификации Инициатор: домен\логин Имя задачи:	Конвертация в CEF отсутствует (событие не передается в SIEM-систему)	
4053 (0xFD5)	Запуск задачи на удаление модуля аутентификации	Сведения	Linux	Событие: запуск задачи на удаление модуля аутентификации Тип запуска: автоматически	Конвертация в CEF отсутствует (событие не передается в SIEM-систему)	

				|вручную Инициатор: домен\логин Имя задачи:		
4054 (0xFD6)	Остановка задачи на удаление модуля аутентификации	Сведения	Linux	Событие: остановка задачи на удаление модуля аутентификации Инициатор: домен\логин Имя задачи:	Конвертация в CEF отсутствует (событие не передается в SIEM-систему)	

1.16 Служебные события

Код события	Тип события	Уровень важности	ОС	Формат события ОС	CEF-формат	Условия воспроизведения
3958 (0xF76)	Ошибка выполнения операции	Ошибка	Windows	Событие: ошибка выполнения операции Действие: Причина: Дополнительные данные:	Конвертация в CEF отсутствует (событие не передается в SIEM-систему)	

2 События аудита СДЗ «SafeNode System Loader»

2.1 События клиента СДЗ

Код события	Тип события	Уровень важности	Формат Windows-события	CEF-формат	Условие воспроизведения
5000 (0x1388)	Загрузка ОС	Сведения	Событие: загрузка ОС Пользователь:	Mon DD hh:mm:ss hostname CEF:0|GIS|Blockhost-Net|4.4 |SafeNode-SystemLoader-5000|Загрузка ОС|Low| cat=События клиента СДЗ dhost=имя хоста источника события rt=дата возникновения события на клиенте suser=содержимое поля 'Пользователь' externalId=5000 categorySignificance=/Informational categoryBehavior=/Access/Start categoryDeviceGroup=/Application catdt=Access and Identity Management categoryOutcome=/Success categoryObject=/Host/Application	
5001 (0x1389)	Не удалось загрузить ОС	Ошибка	Событие: не удалось загрузить ОС Причина: отсутствуют доступные для загрузки ОС Пользователь:	Mon DD hh:mm:ss hostname CEF:0|GIS|Blockhost-Net|4.4 |SafeNode-SystemLoader-5001|Не удалось загрузить ОС|High| cat=События клиента СДЗ dhost=имя хоста источника события rt=дата возникновения события на клиенте suser=содержимое поля 'Пользователь' externalId=5001 categorySignificance=/Informational categoryBehavior=/Access/Start categoryDeviceGroup=/Application catdt=Access and Identity Management categoryOutcome=/Failure categoryObject=/Host/Application	
5005 (0x138D)	Взятие под управление БлокхостСеть	Сведения	Событие: взятие под управление БлокхостСеть	Mon DD hh:mm:ss hostname CEF:0|GIS|Blockhost-Net|4.4 |SafeNode-SystemLoader-5005|Взятие под управление БлокхостСеть |Low| cat=События клиента СДЗ dhost=имя хоста источника события rt=дата возникновения события на клиенте externalId=5005 categorySignificance=/Informational categoryBehavior= /Modify/Configuration categoryDeviceGroup=/Application catdt=Access and Identity Management	

				categoryOutcome=/Success categoryObject=/Host/Application	
5006 (0x138E)	Выход из-под управления БлокхостСеть	Сведения	Событие: выход из-под управления БлокхостСеть	Mon DD hh:mm:ss hostname CEF:0|GIS|Blockhost-Net|4.4 |SafeNode-SystemLoader-5006|Выход из-под управления БлокхостСеть|Low| cat=События клиента СДЗ dhost=имя хоста источника события rt=дата возникновения события на клиенте externalId=5006 categorySignificance=/Informational categoryBehavior= /Modify/Configuration categoryDeviceGroup=/Application catdt=Access and Identity Management categoryOutcome=/Success categoryObject=/Host/Application	
5007 (0x138F)	Ошибка взятия под управление БлокхостСеть	Ошибка	Событие: ошибка взятия под управление БлокхостСеть Причина: неверный пароль администратора СДЗ | несовместимые версии БХ-Сеть и СДЗ	Mon DD hh:mm:ss hostname CEF:0|GIS|Blockhost-Net|4.4 |SafeNode-SystemLoader-5007|Ошибка взятия под управление БлокхостСеть|High| cat=События клиента СДЗ dhost=имя хоста источника события reason=содержимое поля ‘Причина’ rt=дата возникновения события на клиенте externalId=5007 categorySignificance=/Informational categoryBehavior= /Modify/Configuration categoryDeviceGroup=/Application catdt=Access and Identity Management categoryOutcome=/Failure categoryObject=/Host/Application	

2.2 Управление входом в СДЗ

Код события	Тип события	Уровень важности	Формат Windows-события	CEF-формат	Условия воспроизведения
5050 (0x13BA)	Аутентификация пользователя	Сведения	Событие: аутентификация пользователя Пользователь:	Mon DD hh:mm:ss hostname CEF:0|GIS|Blockhost-Net|4.4 |SafeNode-SystemLoader-5050 |Аутентификация пользователя|Low| cat=Управление входом в СДЗ dhost=имя хоста источника события rt=дата возникновения события на клиенте suser=содержимое поля ’Пользователь’ externalId=5050 categorySignificance=/Informational categoryBehavior=/Access/Start categoryDeviceGroup=/Application catdt=Access and Identity Management	

				categoryOutcome=/Success categoryObject=/Host/Application	
5051 (0x13BB)	Смена пин-кода токена	Сведения	Событие: смена пин-кода токена Пользователь:	Mon DD hh:mm:ss hostname CEF:0|GIS|Blockhost-Net|4.4 |SafeNode-SystemLoader-5051|Смена пин-кода токена|Low| cat=Управление входом в СДЗ dhost=имя хоста источника события rt=дата возникновения события на клиенте suser=содержимое поля 'Пользователь' externalId=5051 categorySignificance=/Informational categoryBehavior=/Modify/Configuration categoryDeviceGroup=/Application catdt=Access and Identity Management categoryOutcome=/Success categoryObject=/Host/Application	
5052 (0x13BC)	Смена пароля пользователя	Сведения	Событие: смена пароля пользователя Пользователь:	Mon DD hh:mm:ss hostname CEF:0|GIS|Blockhost-Net|4.4 |SafeNode-SystemLoader-5052|Смена пароля пользователя|Low| cat=Управление входом в СДЗ dhost=имя хоста источника события rt=дата возникновения события на клиенте suser=содержимое поля 'Пользователь' externalId=5052 categorySignificance=/Informational categoryBehavior=/Modify/Configuration categoryDeviceGroup=/Application catdt=Access and Identity Management categoryOutcome=/Success categoryObject=/Host/Application	
5053 (0x13BD)	Отказ на аутентификацию пользователя	Предупреждение	Событие: отказ на аутентификацию пользователя Причина: Пользователь: Возможные значения поля «Причина»: • неверный пароль • неверный PIN-код • персональный идентификатор не подключен к ЭВМ • неверный персональный идентификатор • попытка аутентификации заблокированного пользователя	Mon DD hh:mm:ss hostname CEF:0|GIS|Blockhost-Net|4.4 |SafeNode-SystemLoader-5053|Отказ на аутентификацию пользователя|Medium| cat=Управление входом в СДЗ dhost=имя хоста источника события rt=дата возникновения события на клиенте suser=содержимое поля 'Пользователь' reason=содержимое поля 'Причина' externalId=5053 categorySignificance=/Informational categoryBehavior=/Access/Start categoryDeviceGroup=/Application catdt=Access and Identity Management categoryOutcome=/Failure categoryObject=/Host/Application	

			• попытка аутентификации незарегистрированного пользователя • неверная хэш-сумма на персональном идентификаторе • сертификат на персональном идентификаторе некорректен, не найден или просрочен		

2.3 Контроль целостности

2.3.1 Контроль целостности файлов

Код события	Тип события	Уровень важности	Формат Windows-события	CEF-формат	Условия воспроизведения
5100 (0x13EC)	Нарушена целостность файлового объекта	Предупреждение	Событие: нарушена целостность файлового объекта Имя объекта: Пользователь:	Mon DD hh:mm:ss hostname CEF:0|GIS|Blockhost-Net|4.4 |SafeNode-SystemLoader-5100|Нарушена целостность файлового объекта|Medium| cat=Контроль целостности dhost=имя хоста источника события rt=дата возникновения события на клиенте suser=содержимое поля 'Пользователь' filepath=содержимое поля 'Имя объекта' externalId=5100 categorySignificance=/Informational/Warning categoryBehavior=/Modify categoryDeviceGroup=/Data Security catdt=Access and Identity Management categoryOutcome=/Attempt categoryObject=/Host/File	
Ght5101 (0x13ED)	Файловый объект не найден	Предупреждение	Событие: файловый объект не найден Имя объекта: Пользователь:	Mon DD hh:mm:ss hostname CEF:0|GIS|Blockhost-Net|4.4 |SafeNode-SystemLoader-5101|Файловый объект не найден|Medium| cat=Контроль целостности dhost=имя хоста источника события rt=дата возникновения события на клиенте suser=содержимое поля 'Пользователь' filepath=содержимое поля 'Имя объекта' externalId=5101 categorySignificance=/Informational/Warning categoryBehavior=/Access categoryDeviceGroup=/Data Security catdt=Access and Identity Management categoryOutcome=/Failure	

				categoryObject=/Host/File	

2.3.2 Контроль целостности реестра

Код события	Тип события	Уровень важности	Формат Windows-события	CEF-формат	Условия воспроизведения
5120 (0x1400)	Нарушена целостность объекта реестра	Предупреждение	Событие: нарушена целостность объекта реестра Имя объекта: Пользователь:	Mon DD hh:mm:ss hostname CEF:0|GIS|Blockhost-Net|4.4 |SafeNode-SystemLoader-5120|Нарушена целостность объекта реестра|Medium| cat=Контроль целостности dhost=имя хоста источника события rt=дата возникновения события на клиенте suser=содержимое поля 'Пользователь' cs1=содержимое поля 'Имя объекта' cs1Label= Имена объектов реестра externalId=5120 categorySignificance=/Informational/Warning categoryBehavior=/Modify categoryDeviceGroup=/Data Security catdt=Access and Identity Management categoryOutcome=/Attempt categoryObject=/Host/Operating system	
5121 (0x1401)	Объект реестра не найден	Предупреждение	Событие: объект реестра не найден Имя объекта: Пользователь:	Mon DD hh:mm:ss hostname CEF:0|GIS|Blockhost-Net|4.4 |SafeNode-SystemLoader-5121|Объект реестра не найден|Medium| cat=Контроль целостности dhost=имя хоста источника события rt=дата возникновения события на клиенте suser=содержимое поля 'Пользователь' cs1=содержимое поля 'Имя объекта' cs1Label= Имена объектов реестра externalId=5121 categorySignificance=/Informational/Warning categoryBehavior=/Access categoryDeviceGroup=/Data Security catdt=Access and Identity Management categoryOutcome=/Failure categoryObject=/Host/Operating system	

2.3.3 Контроль целостности аппаратной среды

Код события	Тип события	Уровень важности	Формат Windows-события	CEF-формат	Условия воспроизведения
5140 (0x1414)	Устройство изменено	Предупреждение	Событие: устройство изменено Имя устройства: Пользователь:	Mon DD hh:mm:ss hostname CEF:0|GIS|Blockhost-Net|4.4 |SafeNode-SystemLoader-5140|Устройство изменено|Medium|	

				cat=Контроль целостности dhost=имя хоста источника события rt=дата возникновения события на клиенте suser=содержимое поля 'Пользователь' cs2=содержимое поля 'Имя устройства' cs2Label= Имена устройств externalId=5140 categorySignificance=/Informational/Warning categoryBehavior=/Modify categoryDeviceGroup=/Data Security catdt=Access and Identity Management categoryOutcome=/Attempt categoryObject=/Host/Operating system	
5141 (0x1415)	Устройство не найдено	Предупреждение	Событие: устройство не найдено Имя устройства: Пользователь:	Mon DD hh:mm:ss hostname CEF:0|GIS|Blockhost-Net|4.4 |SafeNode-SystemLoader-5141|Устройство не найдено|Medium| cat=Контроль целостности dhost=имя хоста источника события rt=дата возникновения события на клиенте suser=содержимое поля 'Пользователь' cs2=содержимое поля 'Имя устройства' cs2Label= Имена устройств externalId=5141 categorySignificance=/Informational/Warning categoryBehavior=/Access categoryDeviceGroup=/Data Security catdt=Access and Identity Management categoryOutcome=/Failure categoryObject=/Host/Operating system	

2.3.4 Контроль целостности загрузочных секторов

Код события	Тип события	Уровень важности	Формат Windows-события	CEF-формат	Условия воспроизведения
5160 (0x1428)	Загрузочный сектор изменен	Предупреждение	Событие: загрузочный сектор изменен Имя сектора: Пользователь:	Mon DD hh:mm:ss hostname CEF:0|GIS|Blockhost-Net|4.4 |SafeNode-SystemLoader-5160|Загрузочный сектор изменен|Medium| cat=Контроль целостности dhost=имя хоста источника события rt=дата возникновения события на клиенте suser=содержимое поля 'Пользователь' cs3=содержимое поля 'Имя сектора' cs3Label= Имя сектора externalId=5160 categorySignificance=/Informational/Warning categoryBehavior=/Modify categoryDeviceGroup=/Data Security	

				catdt=Access and Identity Management categoryOutcome=/Attempt categoryObject=/Host/Operating system	
5161 (0x1429)	Загрузочный сектор не найден	Предупреждение	Событие: загрузочный сектор не найден Имя сектора: Пользователь:	Mon DD hh:mm:ss hostname CEF:0|GIS|Blockhost-Net|4.4 |SafeNode-SystemLoader-5161|Загрузочный сектор не найден|Medium| cat=Контроль целостности dhost=имя хоста источника события rt=дата возникновения события на клиенте suser=содержимое поля 'Пользователь' cs3=содержимое поля 'Имя сектора' cs3Label= Имя сектора externalId=5161 categorySignificance=/Informational/Warning categoryBehavior=/Access categoryDeviceGroup=/Data Security catdt=Access and Identity Management categoryOutcome=/Failure categoryObject=/Host/Operating system	

2.3.5 Контроль целостности среды UEFI

Код события	Тип события	Уровень важности	Формат Windows-события	CEF-формат	Условия воспроизведения
5180 (0x143C)	Параметр UEFI изменен	Предупреждение	Событие: параметр UEFI изменен Имя параметра: Пользователь:	Mon DD hh:mm:ss hostname CEF:0|GIS|Blockhost-Net|4.4 |SafeNode-SystemLoader-5180|Параметр UEFI изменен|Medium| cat=Контроль целостности dhost=имя хоста источника события rt=дата возникновения события на клиенте suser=содержимое поля 'Пользователь' cs4=содержимое поля 'Имя параметра' cs4Label= Параметры UEFI externalId=5180 categorySignificance=/Informational/Warning categoryBehavior=/Modify categoryDeviceGroup=/Data Security catdt=Access and Identity Management categoryOutcome=/Attempt categoryObject=/Host/Operating system	
5181 (0x143D)	Параметр UEFI не найден	Предупреждение	Событие: параметр UEFI не найден Имя параметра: Пользователь:	Mon DD hh:mm:ss hostname CEF:0|GIS|Blockhost-Net|4.4 |SafeNode-SystemLoader-5181|Параметр UEFI не найден|Medium| cat=Контроль целостности dhost=имя хоста источника события rt=дата возникновения события на клиенте	

				suser=содержимое поля ’Пользователь’ cs4=содержимое поля ‘Имя параметра’ cs4Label= Параметры UEFI externalId=5181 categorySignificance=/Informational/Warning categoryBehavior=/Access categoryDeviceGroup=/Data Security catdt=Access and Identity Management categoryOutcome=/Failure categoryObject=/Host/Operating system	

2.3.6 Другие события

Код события	Тип события	Уровень важности	Формат Windows-события	CEF-формат	Условия воспроизведения
5200 (0x1450)	Пересчет контрольных сумм объектов	Сведения	Событие: Пересчет контрольных сумм объектов Контроль целостности файловой системы: <список объектов> Контроль целостности реестра: <список объектов> Контроль целостности загрузочных секторов: <список объектов> Контроль целостности среды UEFI: <список объектов> Удаление из списка контролируемых объектов: <список объектов> Контроль изменения аппаратной среды: <список объектов>[3]	Mon DD hh:mm:ss hostname CEF:0|GIS|Blockhost-Net|4.4 |SafeNode-SystemLoader-5200|Пересчет контрольных сумм объектов|Medium| cat=Контроль целостности dhost=имя хоста источника события rt=дата возникновения события на клиенте cs1=содержимое поля ‘Контроль целостности реестра’ cs1Label= Имена объектов реестра cs2=содержимое поля ‘Контроль изменения аппаратной среды’ cs2Label= Имена устройств cs3=содержимое поля ‘Контроль целостности загрузочных секторов cs3Label= Имя сектора cs4=содержимое поля ‘Контроль целостности среды UEFI’ cs4Label= Параметры UEFI cs5=содержимое поля ‘Контроль целостности файловой системы’ cs5Label= Контроль целостности файловой системы cs6=содержимое поля ‘Удаление из списка контролируемых объектов’ cs6Label= Удаление из списка объектов externalId=5200 categorySignificance=/Informational categoryBehavior=/Access categoryDeviceGroup=/Data Security catdt=Access and Identity Management categoryOutcome=/Success categoryObject=/Host/Operating system	

[3] См. приложение Е

3 Приложения к разделу «События аудита Блокхост-Сеть»

Приложение А. Изменение параметров лицензии

Содержание лицензии
Тип лицензии: автономная | серверная
Статус лицензии: действующая | действие приостановлено
Действует с: <dd.mm.yyyy>
Действует до: <dd.mm.yyyy> | неограниченно
Количество подключений: N

Изменение лицензии
Тип лицензии: old_value -> new_value
Статус лицензии: old_value -> new_value
Действует с: old_value -> new_value
Действует до: old_value -> new_value |
Количество подключений: old_value -> new_value

Приложение В. Изменения на токене

Удалены с токена:
    УЦ, серийный номер, CN
    УЦ, серийный номер, CN
    ...
Перевыпущены:
    УЦ, серийный номер, CN
    УЦ, серийный номер, CN
    ...
Отозваны:
    УЦ, серийный номер, CN
    УЦ, серийный номер, CN
    ...
Временно отозваны:
    УЦ, серийный номер, CN
    УЦ, серийный номер, CN
    ...
Возобновлены в действии:
    УЦ, серийный номер, CN
    УЦ, серийный номер, CN

...
Перемещены в наблюдаемые:
УЦ, серийный номер, CN
УЦ, серийный номер, CN
...
Удалены из наблюдаемых:
УЦ, серийный номер, CN
УЦ, серийный номер, CN
...
Добавлены в наблюдаемые:
УЦ, серийный номер, CN
УЦ, серийный номер, CN
...

Приложение С. Формат события со сводной информацией о состоянии сервера/иерархии серверов (вкладка «Статистика»)

Mon DD hh:mm:ss hostname
CEF:0|GIS|Blockhost-Net|4.1|BH-Dashboard -3959|Статус иерархии серверов|Low|
cat=служебные события
dhost=имя хоста источника события
rt=дата возникновения события на клиенте
cs5=<сведения о состоянии иерархии серверов>
cs5label=Сведения о состоянии иерархии серверов
externalId=3959
categorySignificance=/Informational
categoryBehavior=/Communicate
categoryDeviceGroup=/Identity Management
catdt=Access and Identity Management
categoryOutcome=/Success
categoryObject=/Host/Application

Сведения о состоянии иерархии серверов

Total clients: <общее количество клиентов в иерархии>
Auth token: <аутентификация по токену>
Auth login and password: <аутентификация по логину и паролю>
Auth Blockhost-Net: <аутентификация через Блокхост-Сеть>
Online: <клиенты онлайн>
Offline: <клиентаофлайн>

Protected mode: <защищены>
Soft mode: <мягкий режим>

Приложение D. Перечень таблиц custom-полей CEF для разделов аудита

Дискреционный доступ

№	Имя поля	Название (лэйбл) поля	Описание специального поля
1	cs1	cs1Label=Мандатная метка пользователя	Мандатная метка пользователя, выполнившего вход в систему
2	cs2	cs2Label=Мандатная метка объекта	Мандатная метка ресурса, ему выданная администратором безопасности
3	cs3	cs3Label=Тип доступа	Тип доступа пользователя к ресурсу
4	cs4	cs4Label=Привилегии	Привилегии пользователя
5	cs5	cs5Label=ОС клиента	Операционная система клиента, на которой произошло событие

Запуск приложений

№	Имя поля	Название (лэйбл) поля	Описание специального поля
1	cs1	cs1Label= ОС клиента	Операционная система клиента, на которой произошло событие

Аудит доступа к медиафайлам

№	Имя поля	Название (лэйбл) поля	Описание специального поля
1	cs1	cs1Label= ОС клиента	Операционная система клиента, на которой произошло событие

Управление входом в ОС

№	Имя поля	Название (лэйбл) поля	Описание специального поля
1	cs1	cs1Label=Мандатная мета пользователя	Мандатная метка пользователя, выполнившего вход в систему
2	cs2	cs2Label=Тип аутентификации	Режим аутентификации, запрошенный пользователем
3	cs3	cs3Label= cs3Label=Серийный номер токена	Серийный номер токена
4	cs4	cs4Label=Фактический тип входа	Тип входа в ОС, которым пользователь вошел
5	cs5	cs5Label=ОС клиента	Операционная система клиента, на которой произошло событие

Контроль устройств

№	Имя поля	Название (лэйбл) поля	Описание специального поля
1	cs1	cs1Label= Тип устройства’	Тип устройств в контроле устройств
2	cs2	cs2Label= Идентификатор устройства	Аппаратный идентификатор устройства
3	cs3	cs3Label= Метка устройства	Мандатная метка устройства
4	cs4	cs4Label=Тип доступа	Тип доступа, предоставленный к устройству
5	cs5	cs5Label=ОС клиента	Операционная система клиента, на которой произошло событие

Очистка оперативной памяти

номер	Имя поля	Название (лэйбл) поля	Описание специального поля
1	cs1	cs1Label=ОС клиента	Операционная система клиента, на которой произошло событие

Гарантированное удаление файлов

№	Имя поля	Название (лэйбл) поля	Описание специального поля
1	cs1	cs1Label=ОС клиента	Операционная система клиента, на которой произошло событие
2	cs2	cs2Label=Описание	Описание причины отказа операции ГУ

Контроль целостности файлов

№	Имя поля	Название (лэйбл) поля	Описание специального поля
1	cs1	cs1Label=Мандатная мета пользователя	Мандатная метка пользователя, выполнившего вход в систему
2	cs2	cs2Label=ОС клиента	Операционная система клиента, на которой произошло событие

Контроль печати

№	Имя поля	Название (лэйбл) поля	Описание специального поля
1	cs1	cs1Label=Мандатная метка пользователя	Мандатная метка пользователя, выполнившего вход в систему
2	cs2	cs2Label=Имя принтера	Имя принтера, на котором произошла печать документа
3	cs3	cs3Label=Метка документа	Мандатная метка напечатанного документа
4	cs4	cs4Label=ОС клиента	Операционная система клиента, на которой произошло событие
5	cs5	cs5Label=Количество страниц для печати	Количество страниц для печати

Контроль установки/удаления драйверов

№	Имя поля	Название (лэйбл) поля	Описание специального поля
1	cs1	cs1Label=Тип запуска драйвера	Тип запуска драйвера
2	cs2	cs2Label=Имя драйвера	Имя драйвера
3	cs3	cs3Label=Новый тип запуска драйвера	Новый тип запуска драйвера
4	cs4	cs4Label=’Старый тип запуска драйвера’	Старый тип запуска драйвера
5	cs5	cs5Label=ОС клиента	Операционная система клиента, на которой произошло событие

Контроль установки удаления служб

№	Имя поля	Название (лэйбл) поля	Описание специального поля
1	cs1	cs1Label=Тип запуска службы	Описание типа запуска службы
2	cs2	cs2Label=Старый тип запуска службы	Описание старого типа запуска службы
3	cs3	cs3Label=Новый тип запуска службы	Описание нового типа запуска службы
4	cs4	cs4Label=ОС клиента	Операционная система клиента, на которой произошло событие

Контроль установки/удаления приложений

№	Имя поля	Название (лэйбл) поля	Описание специального поля
1	cs1	cs1Label=UUID приложения	UUID приложения
2	cs2	cs2Label=Имя приложения	Имя приложения
3	cs3	cs3Lable=Версия приложения	Версия приложения
4	cs4	cs4Label=Новая версия приложения	Новая версия приложения
5	cs5	cs5Lable=Старая версия приложения	Старая версия приложения
6	cs6	cs6Label=ОС клиента	Операционная система клиента, на которой произошло событие

Контроль изменения перечня каталогов общего доступа

№	Имя поля	Название (лэйбл) поля	Описание специального поля
1	cs1	cs1Label=Имя общего ресурса	Имя общего ресурса
2	cs2	cs2Label=Старое имя общего ресурса	Старое имя общего ресурса
3	cs3	cs3Label=Новое имя общего ресурса	Новое имя общего ресурса
4	cs4	cs4Label=ОС клиента	Операционная система клиента, на которой произошло событие

Контроль аппаратной среды

№	Имя поля	Название (лэйбл) поля	Описание специального поля
1	cs1	cs1Label=Старые параметры	Старые параметры аппаратной конфигурации
2	cs2	cs2Label=Новые параметры	Новые параметры аппаратной конфигурации
3	cs3	cs3Label=Параметры	Параметры аппаратной конфигурации
4	cs4	cs4Label=ОС клиента	Операционная система клиента, на которой произошло событие

События сервера СЗИ

№	Имя поля	Название (лэйбл) поля	Описание специального поля
1	cs1	cs1Label=Тип операционной системы клиента	Тип операционной системы клиента

События клиента СЗИ

№	Имя поля	Название (лэйбл) поля	Описание специального поля
1	cs1	cs1Label=Изменения конфигурации	Изменения настроек в конфигурации клиента
2	cs2	cs2Label=Изменения в политике	Изменение в политике настроек клиента
3	cs3	cs3Label=ОС клиента	Операционная система клиента, на которой произошло событие
4	cs4	cs4Label=Название пакета	Название пакета аутентификации
5	cs5	cs5Label=Код ошибки	Код ошибки при инициализации пакета

Действия администратора СЗИ

№	Имя поля	Название (лэйбл) поля	Описание специального поля

1	cs1	cs1Label=Тип инициатора	Тип учетной записи инициатора подключения
2	cs2	cs2Label=Полномочия администратора	Уровень полномочий администратора, который подключается к консоли
3	cs3	cs3Label=Старая группа клиента	Старая группа клиента
4	cs4	cs4Label=Новая группа клиента	Новая группа клиента
5	cs5	cs5Label=Группа клиента	Имя группы клиента

Управление жизненным циклом токенов

№	Имя поля	Название (лэйбл) поля	Описание специального поля
1	cs1	cs1Label=Токен	Полное описание токена (тип, серийный номер, инвентарный номер), обрабатываемого системой, полное описание старого токена (для события 4049)
2	cs2	cs2Label=Комментарий	Комментарий администратора безопасности
3	cs3	cs3Label=ФИО пользователя	Фамилия, Имя и Отчество пользователя
4	cs4	cs4Label=Выпущенный сертификат для входа	Выпущенный для входа сертификат
5	cs5	cs5Label=Взятые под наблюдение сертификаты	Перечень взятых под наблюдение сертификатов пользователя
6	cs6	cs6Label=Удаленные с токена сертификаты	Перечень удаленных с токена сертификатов пользователя

4 Приложения к разделу «События аудита СДЗ «SafeNode System Loader»»

Приложение Е. Событие «Пересчет контрольных сумм объектов»

Общая структура сообщения о пересчете контрольных сумм

Событие: Пересчет контрольных сумм объектов
Контроль целостности файловой системы:
Пересчет контрольных сумм:
<объект ФС 1>
…
<объект ФС N>
Удаление из списка контролируемых объектов:
<объект ФС 1>
…
<объект ФС N>
Контроль целостности реестра:
Пересчет контрольных сумм:
<объект реестра 1>
…
<объект реестра N>
Удаление из списка контролируемых объектов:
<объект реестра 1>
…
<объект реестра N>
Контроль целостности загрузочных секторов:
Пересчет контрольных сумм:
<загрузочный сектор 1>
…
<загрузочный сектор N>
Удаление из списка контролируемых объектов:
<загрузочный сектор 1>

…
<загрузочный сектор N>
Контроль целостности среды UEFI:
Пересчет контрольных сумм:
<объект UEFI 1>
…
<объект UEFI N>
Удаление из списка контролируемых объектов:
<объект UEFI 1>
…
<объект UEFI N>
Контроль изменения аппаратной среды:
Пересчет контрольных сумм:
<устройство 1>
…
<устройство N>
Удаление из списка контролируемых объектов:
<устройство 1>
…
<устройство N>

Пример

В результате синхронизации политики БХ-Сеть было выполнено

- пересчет контрольных сумм файлов «C:\file1.txt» и «C:\file2.txt»
- пересчет контрольной суммы ветки реестра «HKEY_LOCAL_MACHINE\SYSTEM\GIS1»
- снятие с контроля файлов «C:\file3.txt» и «C:\file4.txt»
- снятие с контроля ветки реестра «HKEY_LOCAL_MACHINE\SYSTEM\GIS2»

Событие: Пересчет контрольных сумм объектов

Контроль целостности файловой системы:

Пересчет контрольных сумм:

C:\file1.txt

C:\file2.txt

Удаление из списка контролируемых объектов:

C:\file3.txt

C:\file4.txt

Контроль целостности реестра:

Пересчет контрольных сумм:

HKEY_LOCAL_MACHINE\SYSTEM\GIS1

Удаление из списка контролируемых объектов:

HKEY_LOCAL_MACHINE\SYSTEM\GIS2

Приложение F. Перечень таблиц custom-полей CEF для разделов аудита

Контроль целостности

№	Имя поля	Название (лэйбл) поля	Описание специального поля
1	cs1	cs1Label=Имена объектов реестра	Имена объектов реестра, взятых на контроль целостности
2	cs2	cs2Label= Имена устройств	Имена устройств, взятых на контроль целостности
3	cs3	cs3Label= Имя сектора	Имена загрузочных секторов, взятых на контроль целостности
4	cs4	cs4Label= Параметры UEFI	Параметры UEFI, взятые на контроль целостности
5	cs5	cs5Label= Контроль целостности файловой системы	Элементы файловой системы, для которых выполняется пересчет контрольных сумм
6	cs6	cs6Label= Удаление из списка объектов	Список элементов, удаленных из списка объектов