Мониторинг ключей реестра Windows

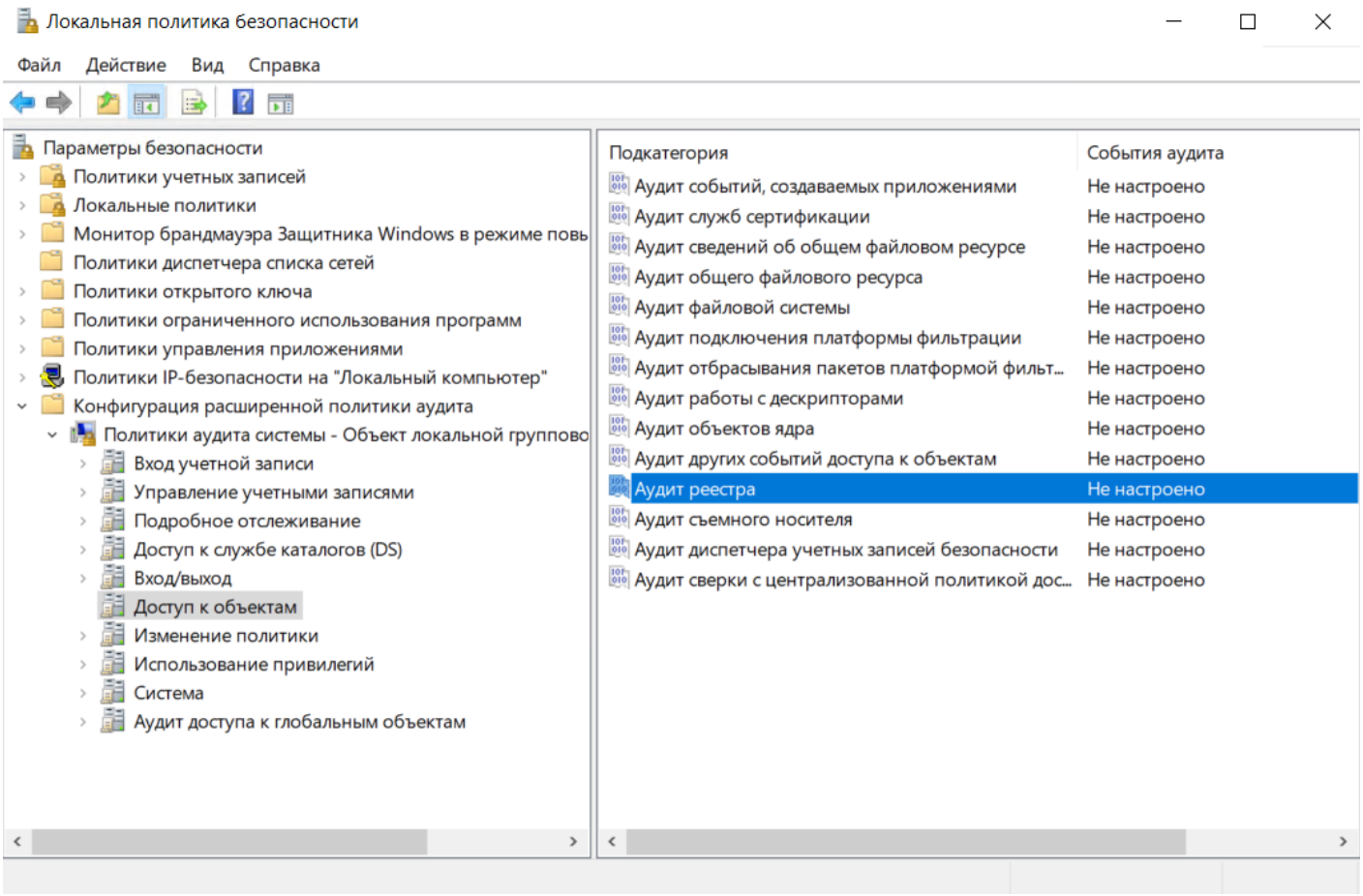
??? ??????????? ?????? ??????? ? KUMA ????? ???????????? ??????????? ????????? ?????? Windows. ??? ????? ?????????? ????????? ??????????? ????? ?? ?????? ? ??????? ? ?????????? ???????, ???????? ? ??????? ??????? ?????????? ??????????. ?????? ????????? ????? ???? ????????? ???????? ?? ???????, ? ????? ?????? ? ??????? ????????? ????????. ? ?????? ???? ????? ?????????? ? ????????? ??????????.

Настройка политики аудита

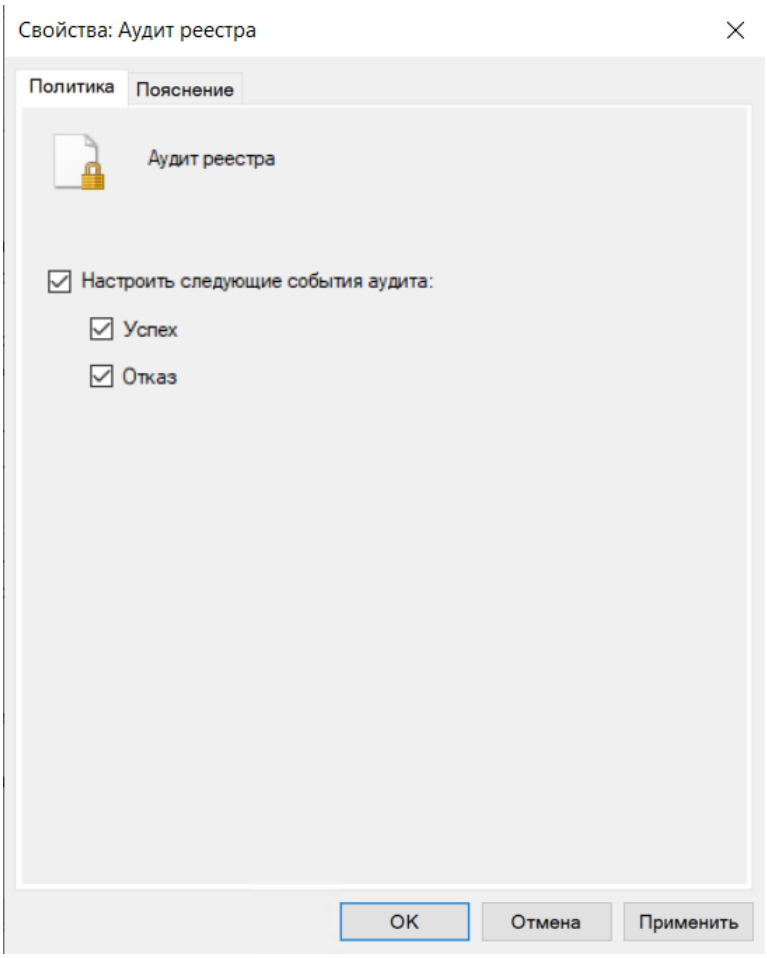
????????? cmd.exe ??-??? ??????? ?????? ????????????? ? ????????? ????????? ???????:

```
auditpol /set /subcategory:"??????" /success:enable /failure:enable
```

?????? ????????? ???????? ???????? ????????? ? ????????? ???????? ???????????. ????? ????????? ???, ???????? ???????? ????????? ???????? ???????????? ? ????????? ? "????????? ????????????" - "???????????? ??????????? ???????? ??????" - "???????? ?????? ???????" - "?????? ????????? ????????? ????????" - "?????? ? ????????".

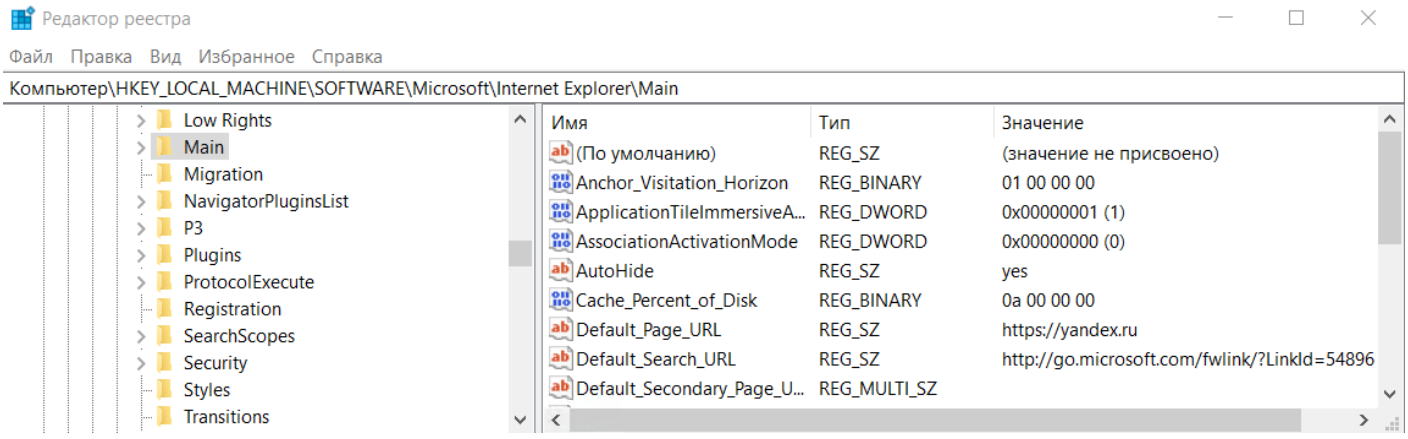


???????? ???????????? "????? ???????" ? ????????? ??????????? ????????

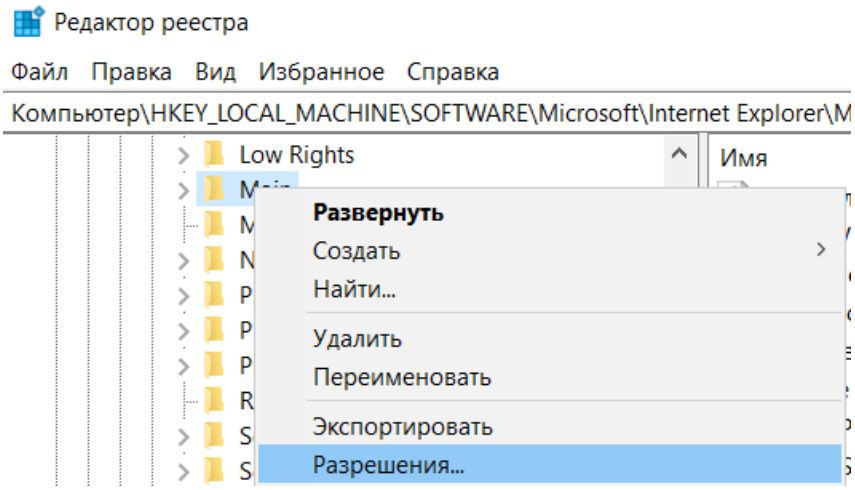


Настройка аудита раздела реестра

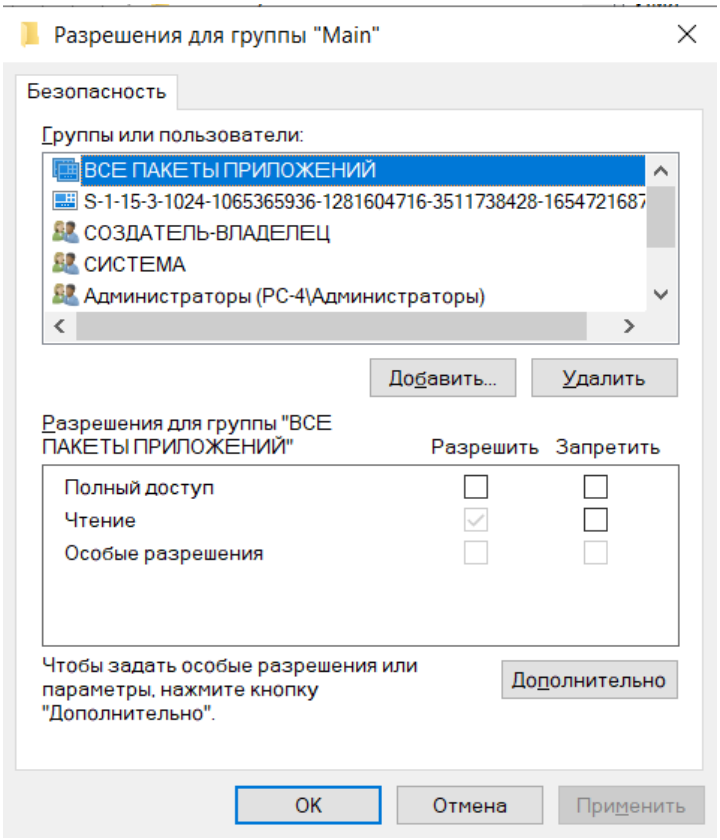
???????? ???????? "???????? ???????" ? ????????? ? ???????, ????? ???????? ?????????? ?????????



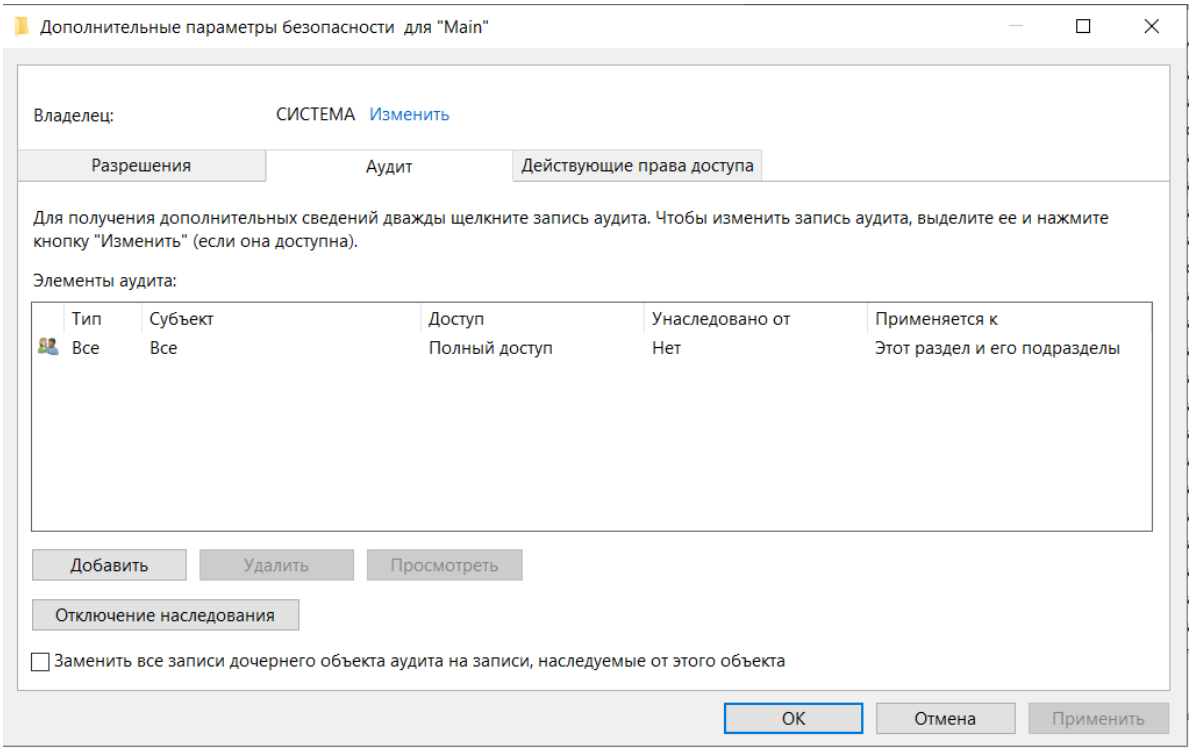
??????? ??? ?? ?????? ??????? ? ???????? ????? ??????????


Редактор реестра
Файл Правка Вид Избранное Справка
Компьютер\HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Internet Explorer\M
Low Rights
Имя
Развернуть
Создать
Найти...
Удалить
Переименовать
Экспортировать
Разрешения...

? ??????????? ???? ??????? ?? ?????? "?????????????"


Разрешения для группы "Main"
Безопасность
Группы или пользователи:
ВСЕ ПАКЕТЫ ПРИЛОЖЕНИЙ
S-1-15-3-1024-1065365936-1281604716-3511738428-1654721687
СОЗДАТЕЛЬ-ВЛАДЕЛЕЦ
СИСТЕМА
Администраторы (PC-4\Администраторы)
Добавить...
Удалить
Разрешения для группы "ВСЕ ПАКЕТЫ ПРИЛОЖЕНИЙ"
Разрешить
Запретить
Полный доступ
Чтение
Особые разрешения
Чтобы задать особые разрешения или параметры, нажмите кнопку "Дополнительно".
Дополнительно
OK
Отмена
Применить

? ????? ???? ????????? ?? ??????? "?????" ? ???????? ??????????? ??????? ?????? ???????. ? ?????? ??????? ???????? ????? ??????? ??????? ???? ????????? ? ???????? ??????? ? ???? ??? ???????????.



????????? ??????????? ?????????.

Результат

? ?????????? ??????????? ???????? ? ??????? ???????????? (security) Windows ????? ?????????? ??????? ? ??????????? ?? ???????????? ??????.

???????, ??????? ????? ??????????:

- 4663(S): An attempt was made to access an object.
- 4656(S, F): A handle to an object was requested.
- 4658(S): The handle to an object was closed.
- 4660(S): An object was deleted.
- 4657(S): A registry value was modified.
- 5039(-): A registry key was virtualized.
- 4670(S): Permissions on an object were changed.

??? ??? ???????? ? KUMA (?? ??????? ??????? 4657):



TenantName	Main
Timestamp	08.11.2023 11:37:09:133
Name	A registry value was modified.
EndTime	08.11.2023 11:37:09:133
DeviceAction	Existing Registry Value modified
DeviceAssetID	PC-4
DeviceEventCategory	Microsoft-Windows-Security-Auditing
DeviceEventClassID	4657
DeviceHostName	pc-4.demo.lab
DeviceNtDomain	DEMO.LAB
DeviceProduct	Windows
DeviceReceiptTime	08.11.2023 11:43:26:756
DeviceTimeZone	+03:00
DeviceVendor	Microsoft
SourceAccountID	bob dylan
SourceAssetID	XDR-KSC
SourceHostName	xdr-ksc.demo.lab
SourceNtDomain	DEMO.LAB
SourceProcessName	Advapi
SourceUserID	S-1-5-21-2175569601-655194666-3432137315-1105
SourceUserName	bob
DestinationHostName	localhost.demo.lab
DestinationNtDomain	DEMO.LAB
DestinationProcessName	C:\Windows\regedit.exe
DestinationUserID	0x493e0ca
DestinationUserName	s-1-5-21-2175569601-655194666-3432137315-1114
DestinationUserPrivileges	SeSecurityPrivilege SeTakeOwnershipPrivilege SeLoadDriverPrivilege SeBackupPrivilege SeRestorePrivilege SeDebugPrivilege SeSystemEnvironmentPrivilege SeImpersonatePrivilege SeDelegateSessionUserImpersonatePrivilege
DeviceCustomIPv6Address2Label	Source IPv6 Address
DeviceCustomNumber1	3
DeviceCustomNumber1Label	LogonType
DeviceCustomString3	0x5300
DeviceCustomString3Label	Process ID
DeviceCustomString4	https://yandex.ru
DeviceCustomString4Label	New Value
DeviceCustomString5	https://google.com
DeviceCustomString5Label	OldValue
DeviceCustomString6	Default_Page_URL
DeviceCustomString6Label	Object Value Name
Service	WMI-Collector (TCP/5550)
ExternalID	1469905
FileID	0x358
FileName	\REGISTRY\MACHINE\SOFTWARE\Microsoft\Internet Explorer\Main
FlexString1	0x493e0ca
FlexString1Label	Destination Logon ID
Type	Base

Revision #1
Created 2023-11-09 09:57:46 UTC by Koala
Updated 2024-12-18 10:16:19 UTC by Koala