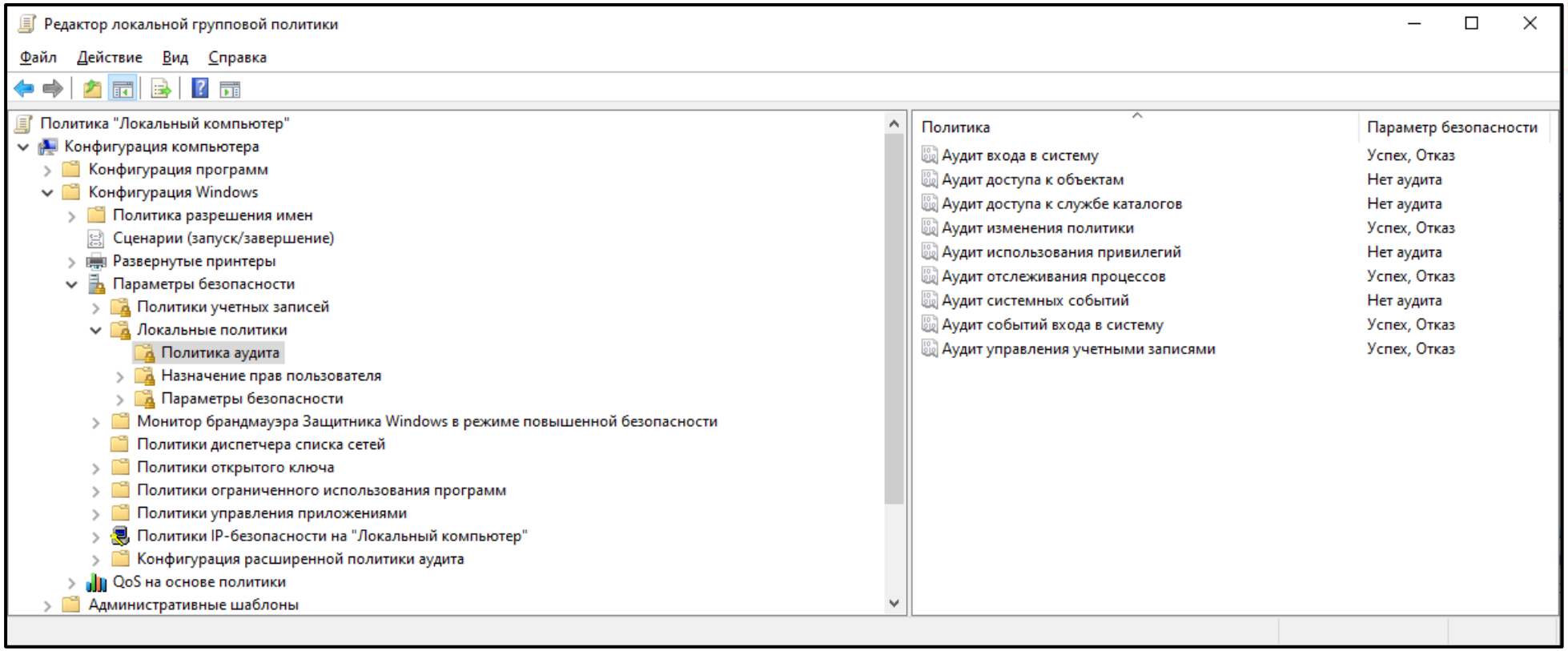
Эшелон
учебный центр

Мониторинг событий ИБ в среде Windows: события, фильтры и директивы корреляции для выявления инцидентов

Каменский Станислав, Специалист группы внедрения СЗИ

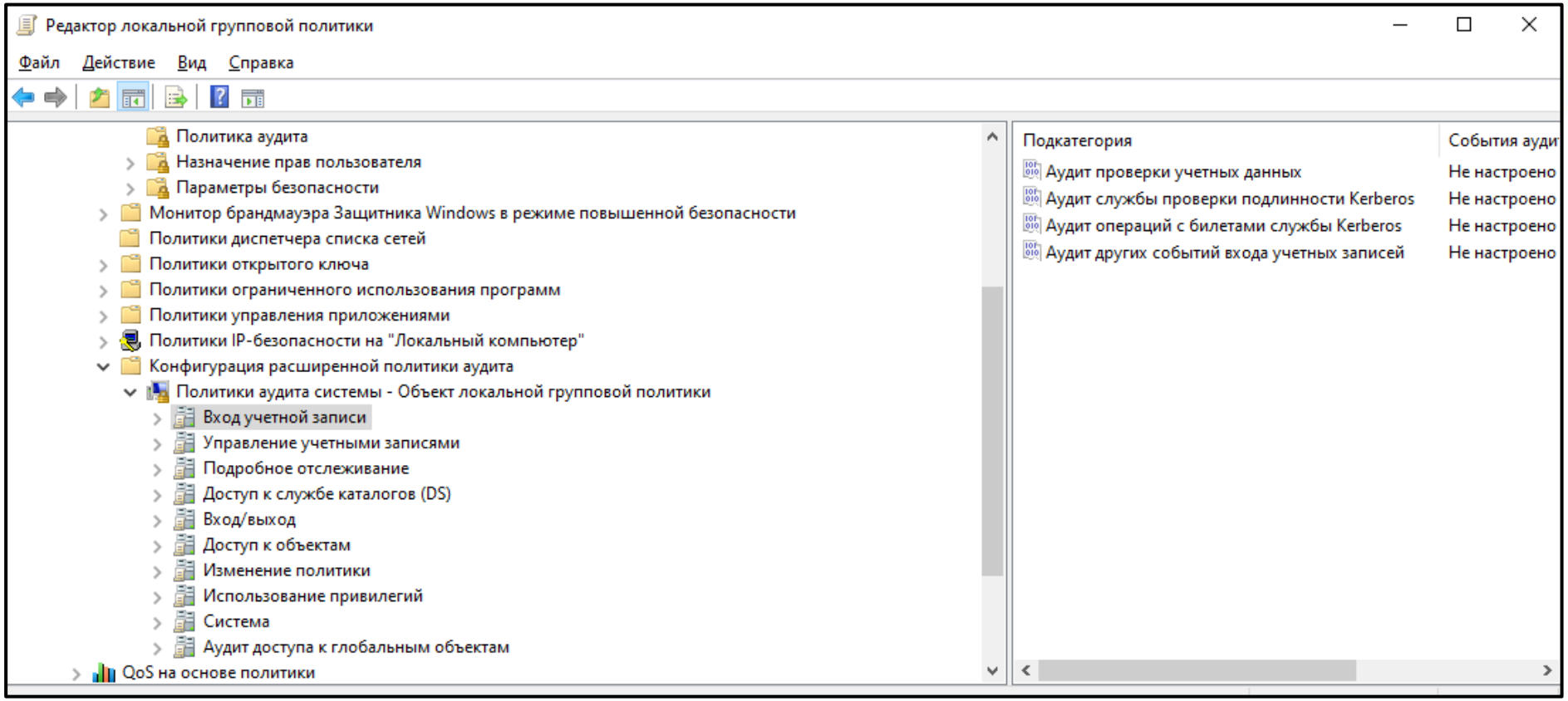
Legacy-настройки журналирования Windows

gpedit.msc



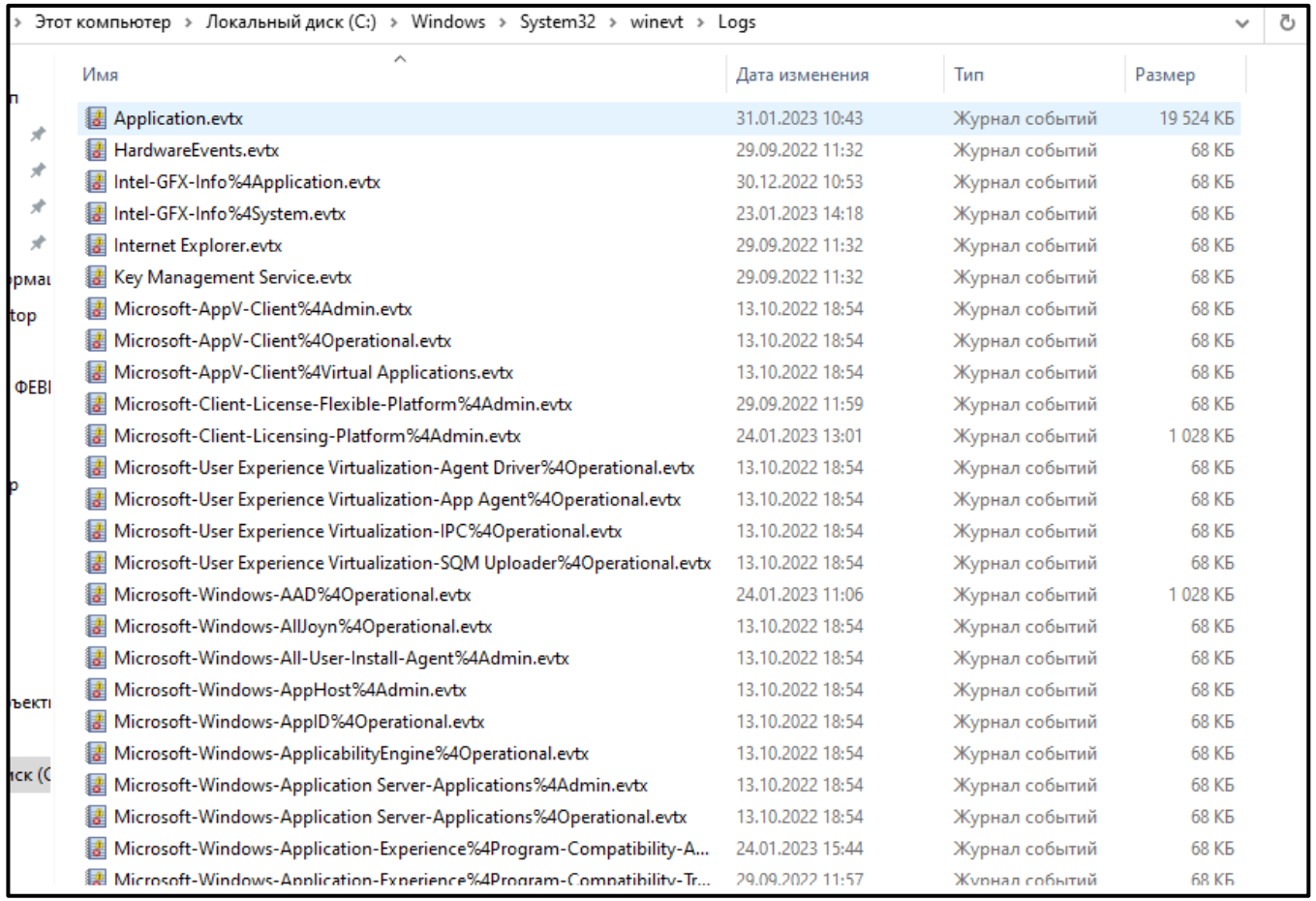
Расширенные настройки журналирования

gpedit.msc



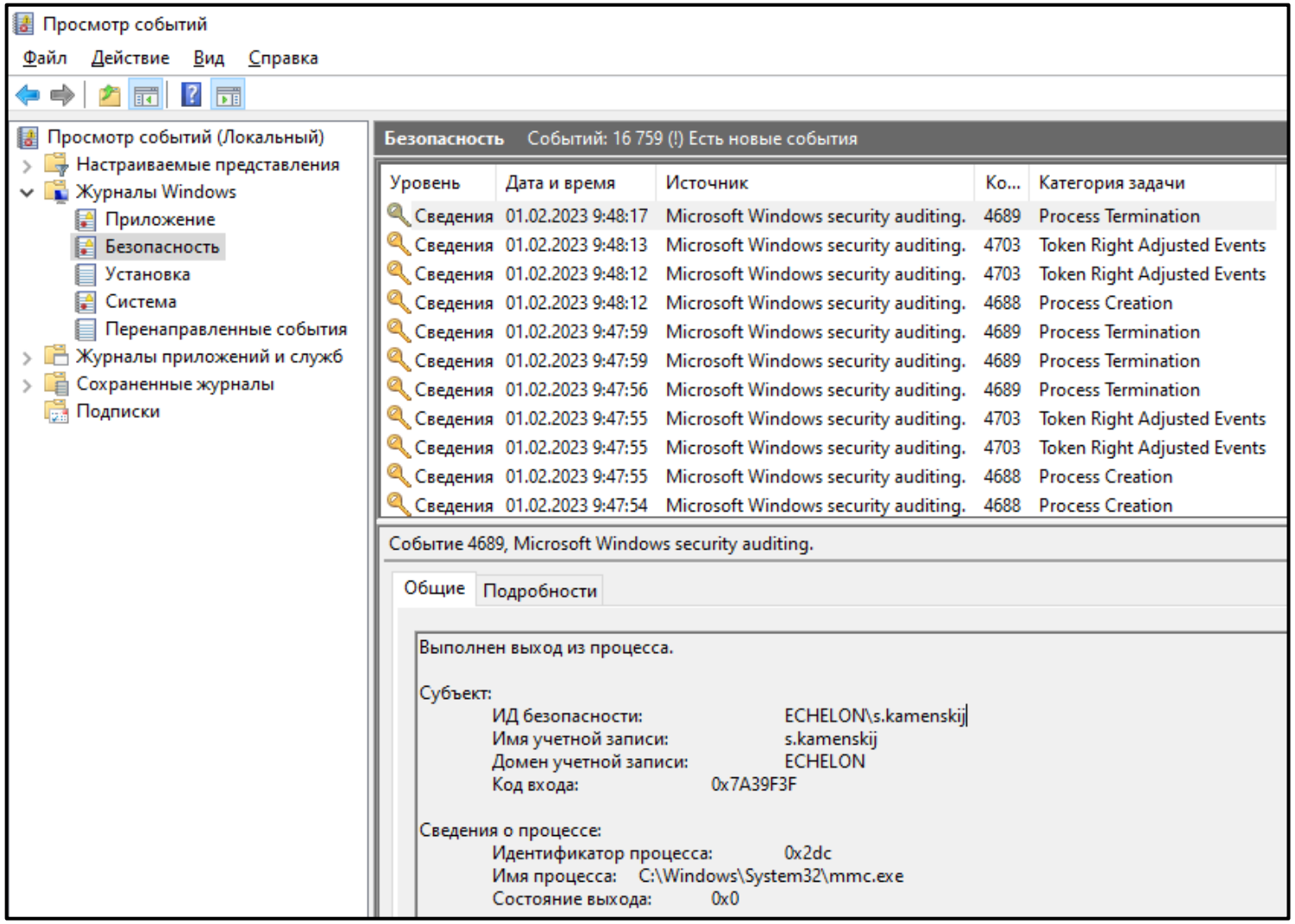
Где находится журнал событий Windows

%SystemRoot%/System32/Winevt/Logs



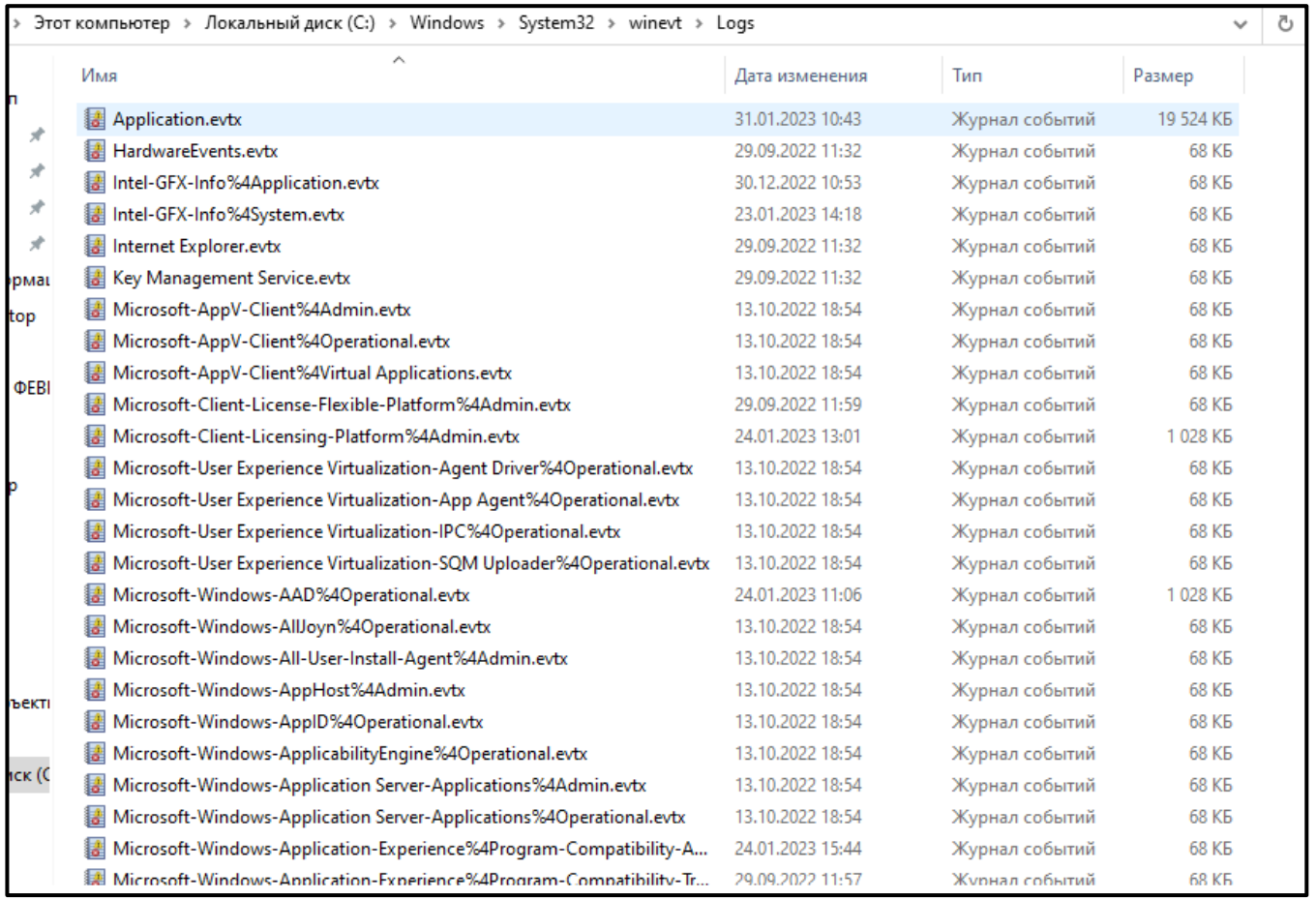
Просмотр журнала

eventvwr.msc



Где находится журнал событий Windows

- Журнал событий представляет собой набор файлов в формате EVTX, хранящихся в системной папке %SystemRoot%/System32/Winevt/Logs



Как полностью выключить журналирование событий в Windows 10?

Теоретически следующая команда должна это делать:

auditpol /set /category:* /success:disable /failure:disable

но практически полностью отключить журналирование невозможно.

https://community.spiceworks.com/topic/2179006-how-to-permanently-disable-auditing-in-windows-10

Категории регистрации событий

- Account Logon
- Account Management
- Detailed Tracking
- DS Access
- Logon/Logoff
- Object Access
- Policy Change
- Privilege Use
- System
- Global Object Access Auditing

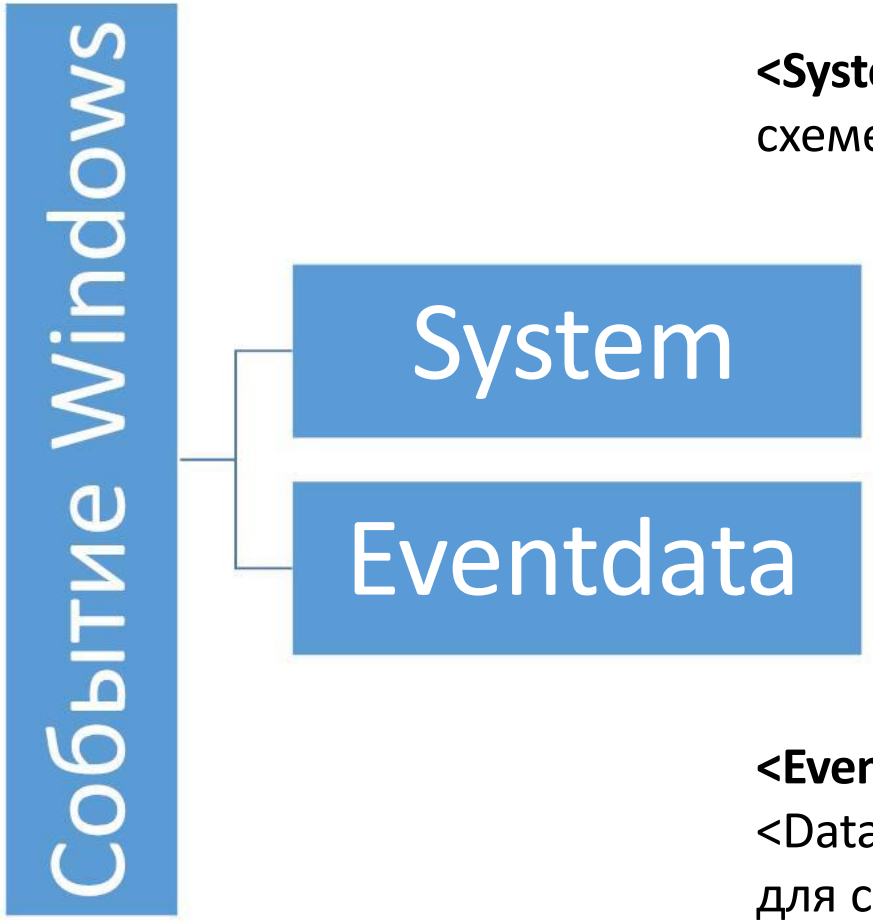
Структура события (1)


```
<Event
xmlns="http://schemas.microsoft.com/win/2004/08/events/event">
        <System>
                <Provider Name=" " Guid="" />
                <EventID></EventID>
                <Version></Version>
                <Level></Level>
                <Task></Task>
                <Opcode></Opcode>
                <Keywords></Keywords>
                <TimeCreated SystemTime="" />
```

Структура события (2)


```
            <EventRecordID></EventRecordID>
            <Correlation />
            <Execution ProcessID="" ThreadID="" />
            <Channel> </Channel>
            <Computer> </Computer>
            <Security />
        </System>
        <EventData>
            <Data Name=""> </Data>
        </EventData>
</Event>
```

Структура события (3)

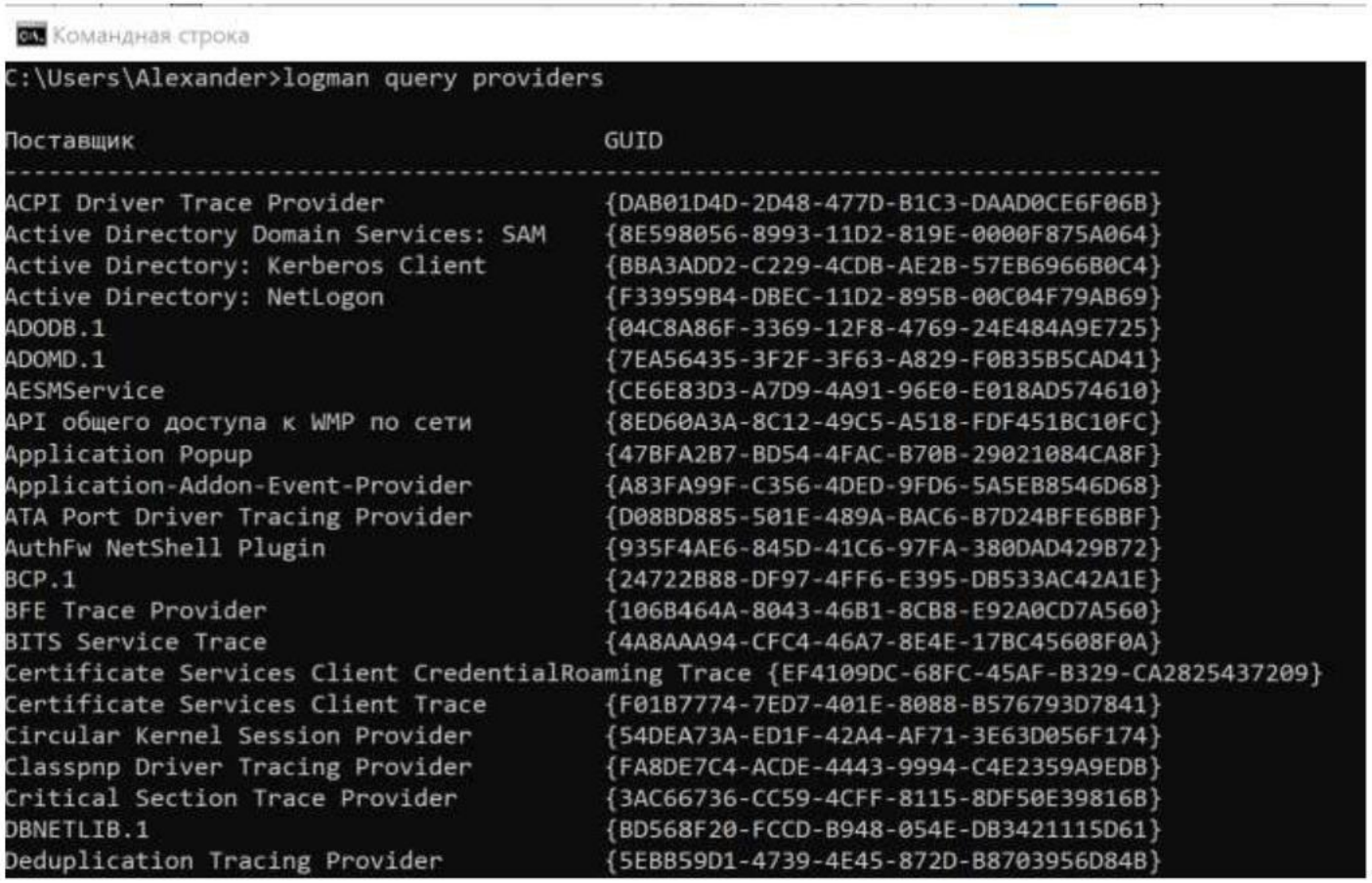


<System>: Содержит список элементов, заданных в схеме.

<EventData>: Содержит различные элементы <Data></Data>, которые определяют специфические для события поля.

Provider

- <Provider /> содержит информацию об источнике, который сообщил о событии безопасности. Секция содержит два параметра Name и GUID.
- Список провайдеров можно получить с помощью команды logman query providers



EventID и Version

- <EventID></EventID> содержит идентификатор события.
- <Version></Version> содержит номер версии события. Если схема события изменяется, то повышается версия события.

Level

- <Level></Level> секция содержит код приоритета события

Название	Код	Описание
Verbose	5	Детальная информация о событии для трассировки.
Informational	0 или 4	Информационное сообщение, например, загрузка DLL
Warning	3	Предупреждение
Error	2	Ошибка
Critical	1	Критическая ошибка, ведущая к останову системы

Task

- <Task></Task> содержит десятичный код категории события (auditing subcategory).

CATEGORY	SUBCATEGORY	DECIMAL	HEX
System	Security State Change	12288	0x3000
	Security System Extension	12289	0x3001
	System Integrity	12290	0x3002
	IPsec Driver	12291	0x3003
	Other System Events	12292	0x3004
Logon/Logoff	Logon	12544	0x3100
	Logoff	12545	0x3101
	Account Lockout	12546	0x3102
	IPsec Main Mode	12547	0x3103
	Special Logon	12548	0x3104
	IPsec Extended Mode	12549	0x3105
	IPsec Quick Mode	12550	0x3106
	Other Logon/Logoff Events	12551	0x3107
	Network Policy Server	12552	0x3108
	User/Device Claims	12553	0x3109
	Group Membership	12554	0x310A
Object Access	File System	12800	0x3200
	Registry	12801	0x3201
	Kernel Object	12802	0x3202
	SAM	12803	0x3203
	Other Object Access Events	12804	0x3204
	Certification Services	12805	0x3205
	Application Generated	12806	0x3206
	Handle Manipulation	12807	0x3207
	File Share	12808	0x3208
	Filtering Platform Packet Drop	12809	0x3209
	Filtering Platform Connection	12810	0x320A
	Detailed File Share	12811	0x320B
	Removable Storage	12812	0x320C
	Central Policy Staging	12813	0x320D
Privilege Use	Sensitive Privilege Use	13056	0x3300
	Non Sensitive Privilege Use	13057	0x3301
	Other Privilege Use Events	13058	0x3302
Detailed Tracking	Process Creation	13312	0x3400
	Process Termination	13313	0x3401
	DPAPI Activity	13314	0x3402
	RPC Events	13315	0x3403
	Plug and Play Events	13316	0x3404
	Token Right Adjusted Events	13317	0x3405
Policy Change	Audit Policy Change	13568	0x3500
	Authentication Policy Change	13569	0x3501
	Authorization Policy Change	13570	0x3502
	MPSSVC Rule-Level Policy Change	13571	0x3503
	Filtering Platform Policy Change	13572	0x3504
	Other Policy Change Events	13573	0x3505
Account Management	User Account Management	13824	0x3600
	Computer Account Management	13825	0x3601
	Security Group Management	13826	0x3602
	Distribution Group Management	13827	0x3603
	Application Group Management	13828	0x3604
	Other Account Management Events	13829	0x3605
DS Access	Directory Service Access	14080	0x3700
	Directory Service Changes	14081	0x3701
	Directory Service Replication	14082	0x3702
	Detailed Directory Service Replication	14083	0x3703
Account Logon	Credential Validation	14336	0x3800
	Kerberos Service Ticket Operations	14337	0x3801
	Other Account Logon Events	14338	0x3802
	Kerberos Authentication Service	14339	0x3803

Windows Security Monitoring: Scenarios and Patterns Andrei Miroshnikov

Opcode и Keywords

- <Opcode></Opcode> содержит десятичный код, который идентифицирует операцию в рамках задачи или содержит определенный глобальный код. Задачи расширенной регистрации событий не содержат кода.
- <Keywords></Keywords> элемент содержит дополнительные ключевые слова для событий. События безопасности содержат следующие значения:
  - 0x8010000000000000: Audit Failure
  - 0x8020000000000000: Audit Success

EventRecordID, Correlation, Execution

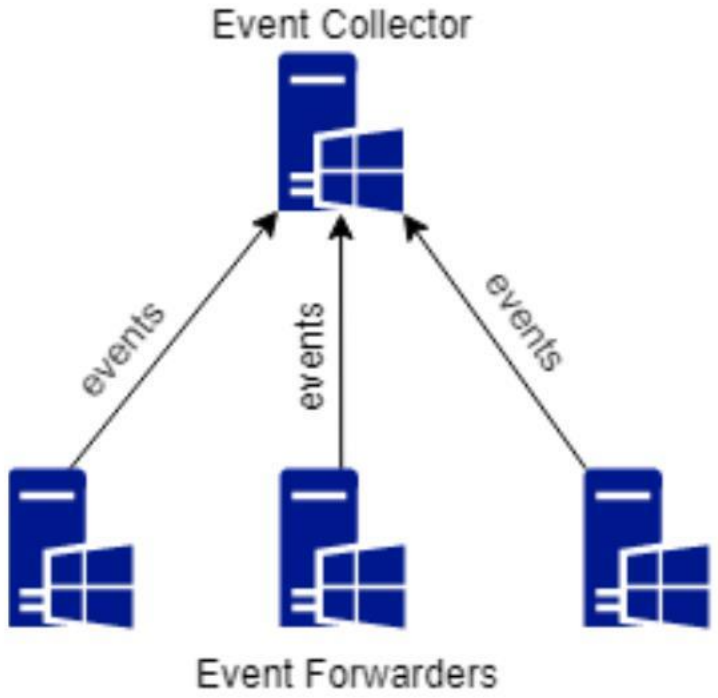
- <EventRecordID></EventRecordID> содержит уникальный идентификатор внутри журнала. Нумерация начинается с 1 после установки системы и увеличивается на 1 для каждого нового события. Очистка журнала не обнуляет счетчик.
- <Correlation /> предоставляет информацию, если есть связанные события.
- <Execution /> содержит следующие два параметра: ProcessID: идентификатор процесса, сообщившего о событии. События безопасности регистрируются процессами lsass.exe или ntoskrnl.exe (идентификатор процесса будет равным 4), ThreadID: идентификатор потока.

Channel, Computer и Security

- <Channel></Channel> содержит имя журнала. Основные журналы: System, Application, Setup, and Security. Все события безопасности должны отправляться в журнал Security.
- <Computer></Computer> содержит имя компьютера (FQDN или NetBIOS имя).
- <Security /> обычно не используется в события безопасности, но может использоваться в прочих событиях для предоставления дополнительной информации, связанной с безопасностью (например, идентификатор пользователя).

WEF & WEC

WEF – встроенный механизм отправки сообщений журналов Windows на выделенный сервер Windows Event Collector (WEC).



WMI-агент KOMRAD Enterprise SIEM (1)

- WMI агент - приложение Microsoft Windows, позволяет собирать данные из:
  - журналов Windows
  - локальных файлов EVTX/Sysmon
  - удалённого Windows Event Collector

- устанавливается с правами администратора как служба Windows с правами системного пользователя;
- подключается к узлу управления агентами SIEM КОМРАД;
- отправляет свой статус в SIEM, получает обновления конфигурации из SIEM;
- позволяет выбрать для сбора событий журналы Windows, настроить фильтры по Коду события Windows, провайдеру журнала;
- сохраняет отметки о позиции сбора с каждого журнала в локальном бинарном файле хранилища состояния агента;

WMI-агент KOMRAD Enterprise SIEM (2)

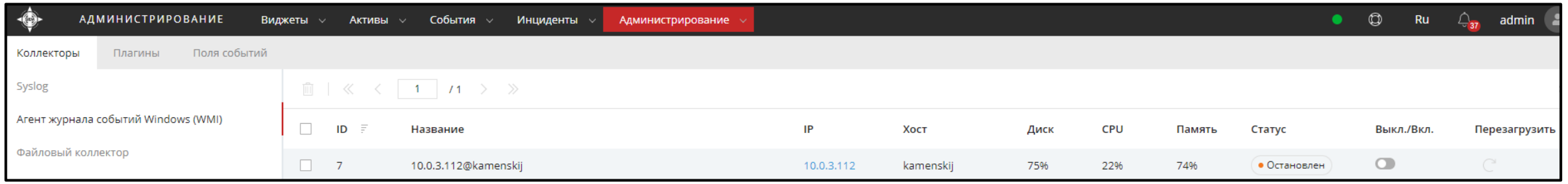
- применяет серию автоматических правил нормализации события Windows, приводит извлечённые события к схеме нормализации Elastic Common Schema либо к пользовательской схеме полей заказчика;
- позволяет применять дополнительные нормализации к полям - извлечение значений с помощью регулярных выражений, ключей и массивов из JSON структур, структуры из текста с помощью Glob паттернов, переименование полей и перекодирование (маппинг) значений полей;
- отправляет нормализованные события сжатыми пакетами через интеграционную шину КОМРАД в центральный модуль обработки SIEM;
- в случае разрыва сетевого соединения накапливает собранные и нормализованные события в локальном файле, после восстановления соединения досылает пакеты;
- осуществляет базовый мониторинг узла - процент доступной памяти, диска, процессора;
- файлы конфигурации и хранилище состояний помещает в отдельную папку, доступную только пользователям с правами администратора;
- (опционально) шифрует конфигурацию и внутреннее состояние с помощью Windows Data Protection API;

Простая установка WMI-агента KOMRAD

1. Загрузить на машину архив с WMI-агентом и распаковать его.
2. Внести в конфигурационный wmi-agent.yaml файл IP-адрес узла, на котором развернута интеграционная шина КОМРАД:

   bus: servers: - nats://10.0.3.124:3490
3. Установить WMI-агент: wmi-agent.exe --service install -c wmi-agent.yaml

4. В интерфейсе KOMRAD **перезагрузить** появившийся агент и увидеть статус «В работе»
5. Выбрать интересующие журналы.



Сбор событий о неуспешном входе в систему

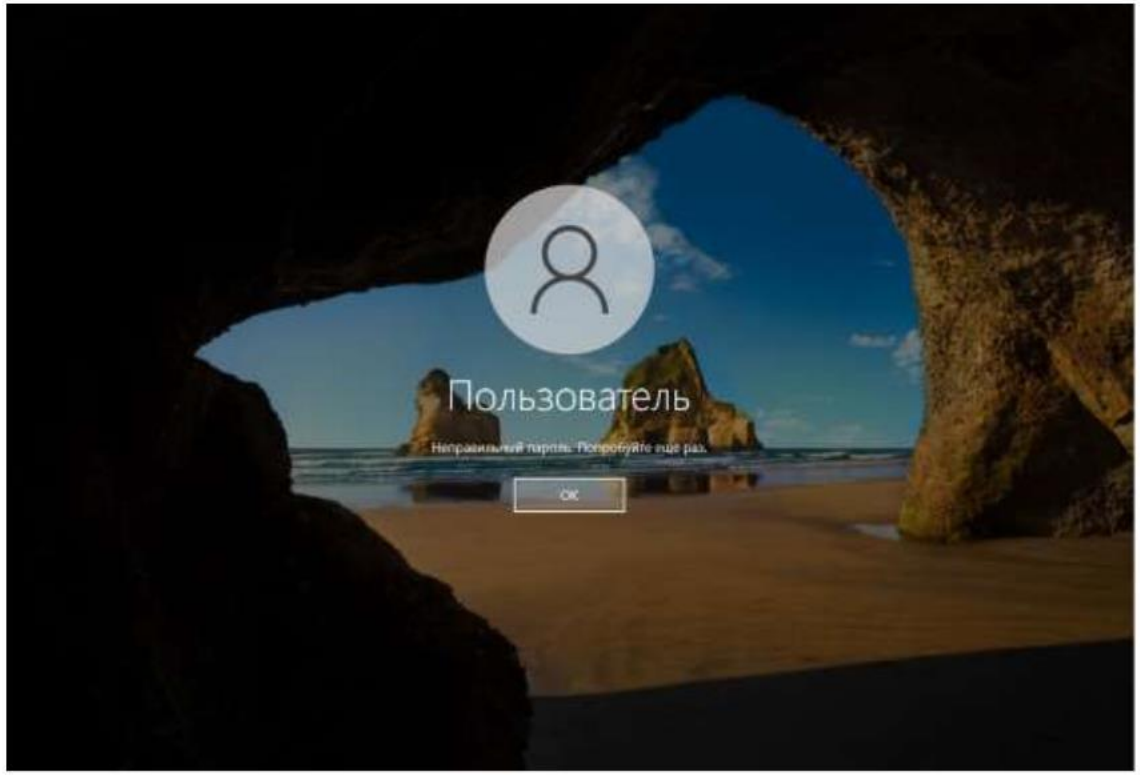
1. Можем для чистоты эксперимента выключить регистрацию событий
auditpol /set /category:* /success:disable /failure:disable

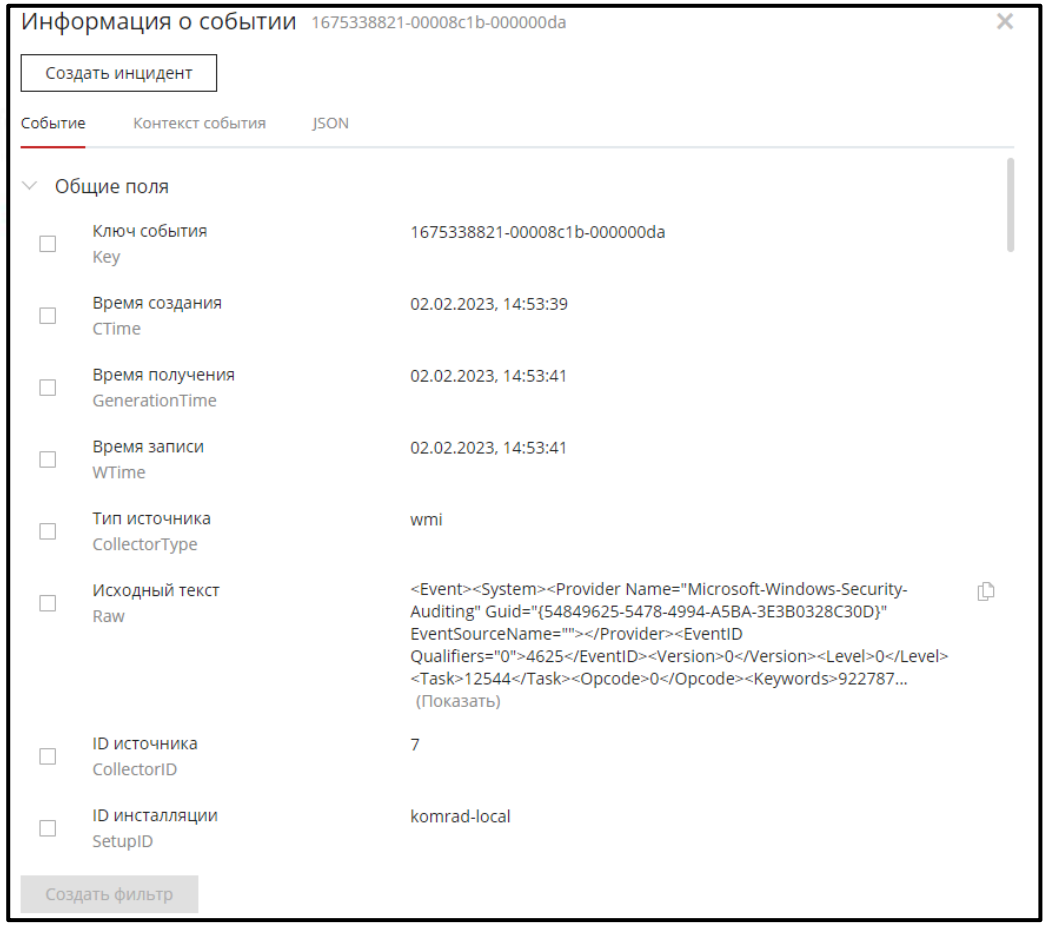
2. Включаем регистрацию событий, связанных со входом в систему:
auditpol /set /subcategory:"Вход в систему" /success:enable /failure:enable

Вывести список категорий и подкатегорий событий можно с помощью следующей команды:
auditpol /list /subcategory:*
Настройки текущей политики можно посмотреть с помощью следующей команды:
auditpol /get /category:*

https://docs.microsoft.com/ru-ru/windows-server/administration/windows-commands/auditpol-set

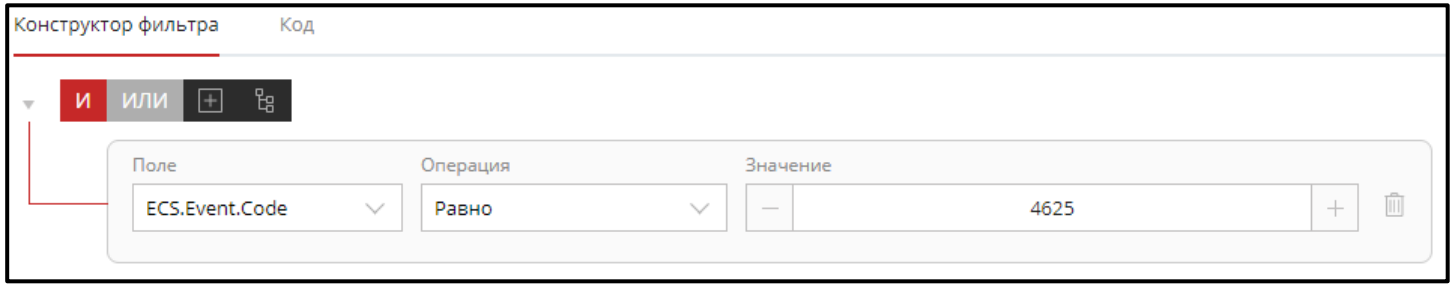
Неуспешная попытка входа в систему

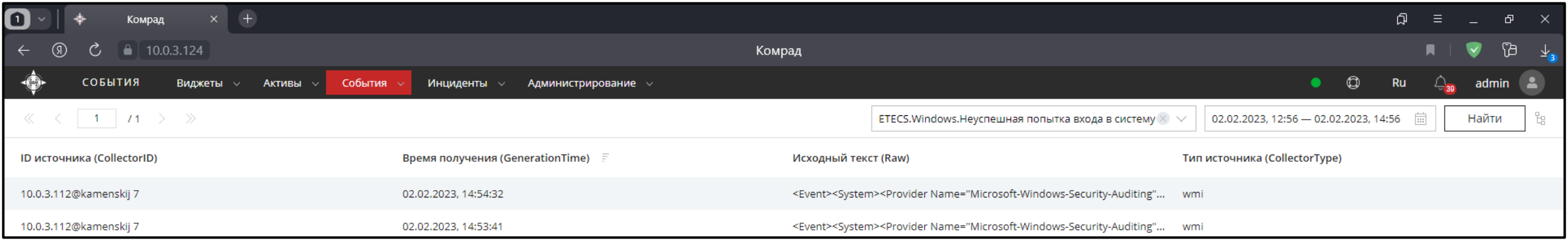




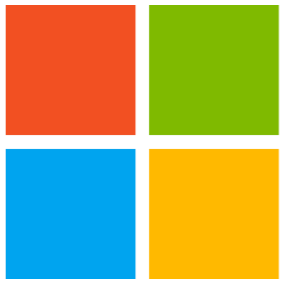
https://docs.microsoft.com/ru-ru/windows/security/threat-protection/auditing/event-4625

События о неуспешной попытке входа





Руководство по настройке журналирования Windows



Microsoft

https://docs.microsoft.com/en-us/windows-server/identity/ad-ds/plan/security-best-practices/audit-policy-recommendations

Минимум для мониторинга Windows

- События, связанные с работой приложений (Application)
- События, связанные с работой Windows (System)
- Управление учетными записями и авторизация (Security)
- Ошибки, связанные с ЭЦП драйверов
- Ошибки, связанные с групповыми политиками
- События защитника Windows (Microsoft-Windows-Windows Defender/Operational)
- Подключение к беспроводным сетям (Microsoft-Windows-NetworkProfile/Operational)
- Манипуляции с отчуждаемыми носителями информации (Microsoft-Windows-DriverFrameworks-UserMode/Operational)
- Печать документа (Microsoft-Windows-PrintService/Operational)

События, связанные с работой приложений

Блокировка по белому списку:

	ID	Level	Event Log	Event Source
AppLocker Block	8003 8004	Error Warning	Microsoft-Windows-AppLocker/EXE and DLL	Microsoft-Windows-AppLocker
AppLocker Warning	8006 8007	Error Warning	Microsoft-Windows-AppLocker/MSI and Script	Microsoft-Windows-AppLocker
SRP Block	865, 866, 867, 868, 882	Warning	Application	Microsoft-Windows-SoftwareRestrictionPolices

Сбои приложений:

	ID	Level	Event Log	Event Source
App Error	1000	Error	Application	Application Error
App Hang	1002	Error	Application	Application Hang
BSOD	1001	Error	System	Microsoft-Windows-WER-SystemErrorReporting
WER	1001	Informational	Application	Windows Error Reporting
EMET	1 2	Warning Error	Application Application	EMET

Системные сбои:

	ID	Level	Event Log	Event Source
Windows Service Fails or Crashes	7022, 7023, 7024, 7026, 7031, 7032, 7034	Error	System	Service Control Manager

События, связанные с работой Windows (1)

Сбои, связанные с обновлением:

	ID	Level	Event Log	Event Source
Windows Update Failed	20, 24, 25, 31, 34, 35	Error	Microsoft-Windows-WindowsUpdateClient/Operational	Microsoft-Windows-WindowsUpdateClient
Hotpatching Failed	1009	Informational	Setup	Microsoft-Windows-Servicing

Изменение конфигурации межсетевого экрана:

	ID	Level	Event Log	Event Source
Firewall Rule Add	2004	Informational	Microsoft-Windows-Windows Firewall With Advanced Security/Firewall	Microsoft-Windows-Windows Firewall With Advanced Security
Firewall Rule Change	2005	Informational	Microsoft-Windows-Windows Firewall With Advanced Security/Firewall	Microsoft-Windows-Windows Firewall With Advanced Security
Firewall Rules Deleted	2006, 2033	Informational	Microsoft-Windows-Windows Firewall With Advanced Security/Firewall	Microsoft-Windows-Windows Firewall With Advanced Security
Firewall Failed to load Group Policy	2009	Error	Microsoft-Windows-Windows Firewall With Advanced Security/Firewall	Microsoft-Windows-Windows Firewall With Advanced Security

События, связанные с работой Windows (2)

Очистка журналов:

	ID	Level	Event Log	Event Source
Event Log was Cleared	104	Informational	System	Microsoft-Windows-Eventlog
Audit Log was Cleared	1102	Informational	Security	Microsoft-Windows-Eventlog

Манипуляции с приложениями:

	ID	Level	Event Log	Event Source
New Kernel Filter Driver	6	Informational	System	Microsoft-Windows-FilterManager
New Windows Service	7045	Informational	System	Service Control Manager
New MSI File Installed	1022, 1033	Informational	Application	MsiInstaller
New Application Installation	903, 904[46]	Informational	Microsoft-Windows-Application-Experience/Program-Inventory[47]	Microsoft-Windows-Application-Experience
Updated Application	905, 906[46]	Informational	Microsoft-Windows-Application-Experience/Program-Inventory	Microsoft-Windows-Application-Experience
Removed Application	907, 908[46]	Informational	Microsoft-Windows-Application-Experience/Program-Inventory	Microsoft-Windows-Application-Experience
Summary of Software Activities	800	Informational	Microsoft-Windows-Application-Experience/Program-Inventory	Microsoft-Windows-Application-Experience
Update Packages Installed	2	Informational	Setup	Microsoft-Windows-Servicing
Windows Update Installed	19	Informational	System	Microsoft-Windows-WindowsUpdateClient

Управление учетными записями и авторизация

	ID	Level	Event Log	Event Source
Account Lockouts	4740	Informational	Security	Microsoft-Windows-Security-Auditing
User Added to Privileged Group	4728, 4732, 4756	Informational	Security	Microsoft-Windows-Security-Auditing
Security-Enabled group Modification	4735	Informational	Security	Microsoft-Windows-Security-Auditing
Successful User Account Login	4624	Informational	Security	Microsoft-Windows-Security-Auditing
Failed User Account Login	4625	Informational	Security	Microsoft-Windows-Security-Auditing
Account Login with Explicit Credentials	4648	Informational	Security	Microsoft-Windows-Security-Auditing

Ошибки, связанные с ЭЦП драйверов

	ID	Level	Event Log	Event Source
Detected an invalid image hash of a file	5038	Informational	Security	Microsoft-Windows-Security-Auditing
Detected an invalid page hash of an image file	6281	Informational	Security	Microsoft-Windows-Security-Auditing
Code Integrity Check	3001, 3002, 3003, 3004, 3010, 3023	Warning, Error	Microsoft-Windows-CodeIntegrity/Operational	Microsoft-Windows-CodeIntegrity
Failed Kernel Driver Loading	219	Warning	System	Microsoft-Windows-Kernel-PnP

Ошибки, связанные с групповыми политиками

	ID	Level	Event Log	Event Source
Internal Error	1125	Error	System	Microsoft-Windows-GroupPolicy
Generic Internal Error	1127	Error	System	Microsoft-Windows-GroupPolicy
Group Policy Application Failed due to Connectivity	1129	Error	System	Microsoft-Windows-GroupPolicy

События защитника Windows

Scan Failed	1005	Error	Microsoft-Windows-Windows Defender/Operational	Microsoft-Windows-Windows Defender
Detected Malware	1006	Warning	Microsoft-Windows-Windows Defender/Operational	Microsoft-Windows-Windows Defender
Action on Malware Failed	1008	Error	Microsoft-Windows-Windows Defender/Operational	Microsoft-Windows-Windows Defender
Failed to remove item from quarantine	1010	Error	Microsoft-Windows-Windows Defender/Operational	Microsoft-Windows-Windows Defender
Failed to update signatures	2001	Error	Microsoft-Windows-Windows Defender/Operational	Microsoft-Windows-Windows Defender
Failed to update engine	2003	Error	Microsoft-Windows-Windows Defender/Operational	Microsoft-Windows-Windows Defender
Reverting to last known good set of signatures	2004	Warning	Microsoft-Windows-Windows Defender/Operational	Microsoft-Windows-Windows Defender
Real-Time Protection failed	3002	Error	Microsoft-Windows-Windows Defender/Operational	Microsoft-Windows-Windows Defender
Unexpected Error	5008	Error	Microsoft-Windows-Windows Defender/Operational	Microsoft-Windows-Windows Defender

Подключение к беспроводным сетям

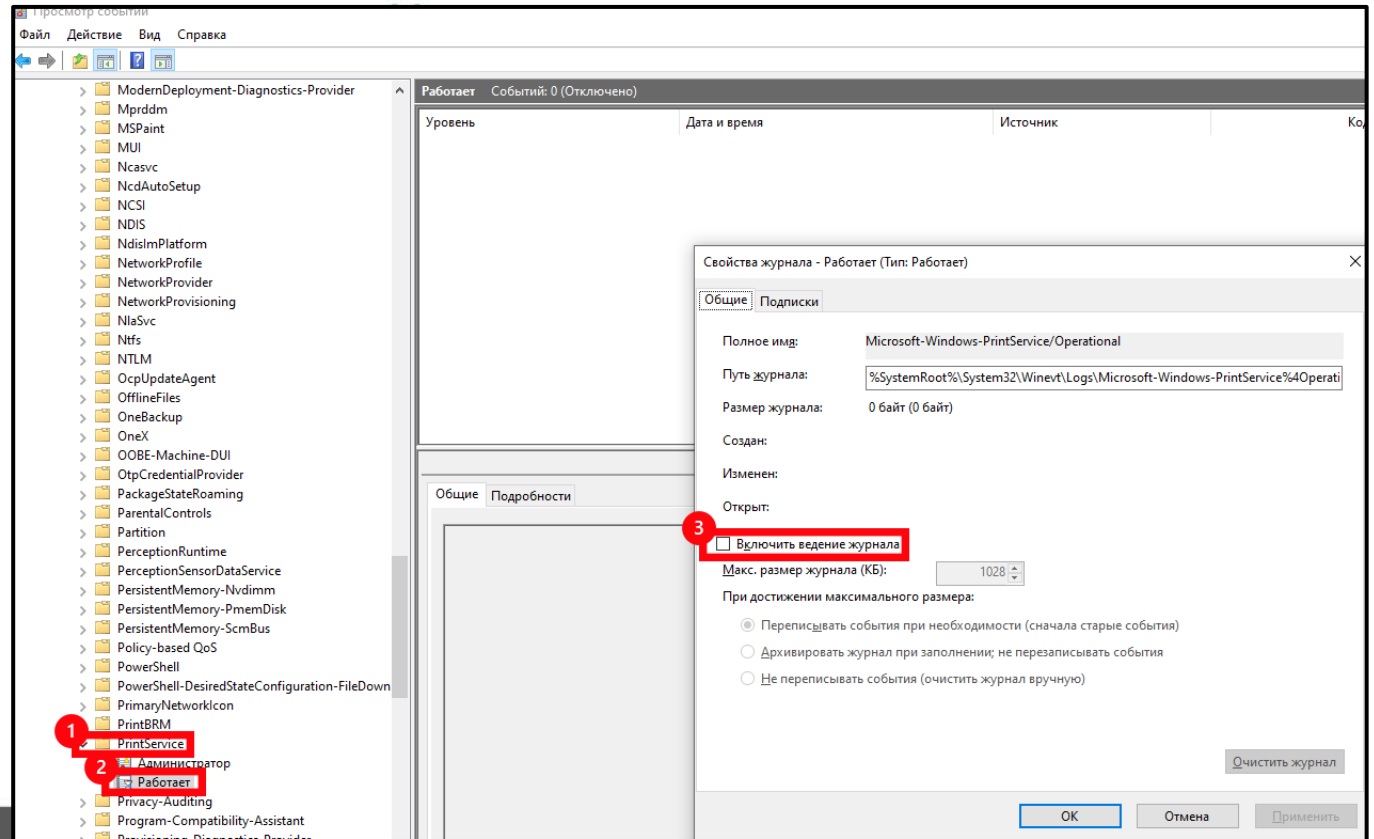
	ID	Level	Event Log	Event Source
Network Connection and Disconnection Status (Wired and Wireless)	10000,10001	Informational	Microsoft-Windows-NetworkProfile/Operational	Microsoft-Windows-NetworkProfile
Starting a Wireless connection	8000, 8011	Informational	Microsoft-Windows-WLAN-AutoConfig/Operational	Microsoft-Windows-WLAN-AutoConfig
Successfully connected to Wireless connection	8001	Informational	Microsoft-Windows-WLAN-AutoConfig/Operational	Microsoft-Windows-WLAN-AutoConfig
Disconnect from Wireless connection	8003	Informational	Microsoft-Windows-WLAN-AutoConfig/Operational	Microsoft-Windows-WLAN-AutoConfig
Wireless Association Status	11000, 11001, 11002	Informational Error	Microsoft-Windows-WLAN-AutoConfig/Operational	Microsoft-Windows-WLAN-AutoConfig
Wireless Security Started, Stopped, Successful, or Failed	11004, 11005, 11010, 11006	Informational Error	Microsoft-Windows-WLAN-AutoConfig/Operational	Microsoft-Windows-WLAN-AutoConfig
Wireless Connection Failed	8002	Error	Microsoft-Windows-WLAN-AutoConfig/Operational	Microsoft-Windows-WLAN-AutoConfig
Wireless Authentication Started and Failed	12011, 12012 12013	Informational Error	Microsoft-Windows-WLAN-AutoConfig/Operational	Microsoft-Windows-WLAN-AutoConfig

Манипуляции с отчуждаемыми носителями информации

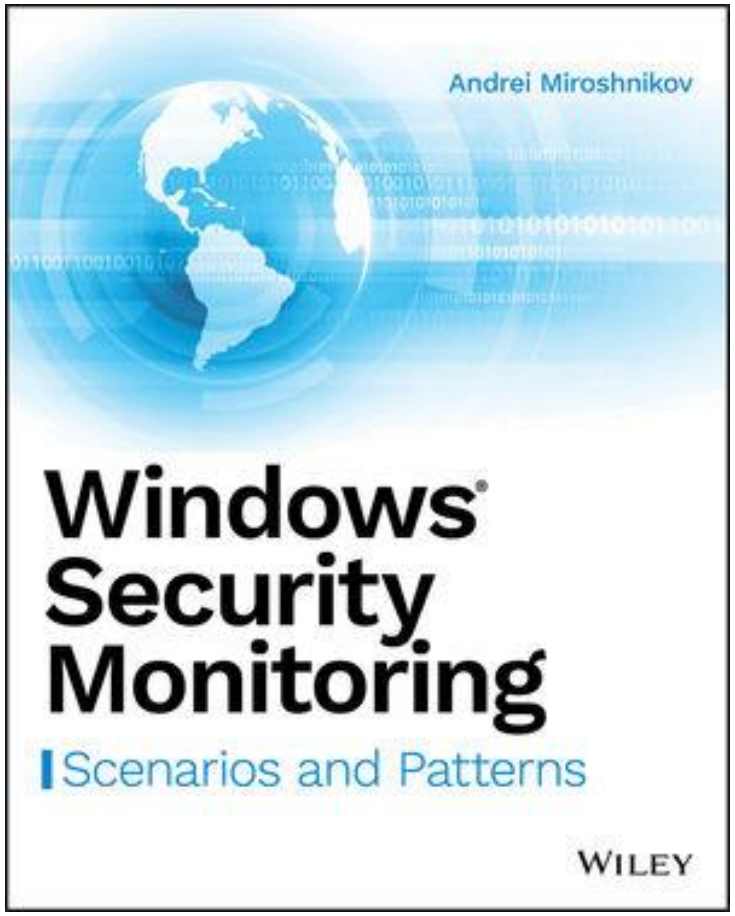
	ID	Level	Event Log	Event Source
New Device Information	43[54]	Informational	Microsoft-Windows-USB-USBHUB3-Analytic[55][56]	Microsoft-Windows-USB-USBHUB3
New Mass Storage Installation	400[57]	Informational	Microsoft-Windows-Kernel-PnP/Device Configuration	Microsoft-Windows-Kernel-PnP
New Mass Storage Installation	410[57]	Informational	Microsoft-Windows-Kernel-PnP/Device Configuration	Microsoft-Windows-Kernel-PnP

Печать документа

	ID	Level	Event Log	Event Source
Printing Document	307	Informational	Microsoft-Windows-PrintService/Operational	Microsoft-Windows-PrintService



Литература



https://www.ultimatewindowssecurity.com/securitylog/encyclopedia

СПАСИБО ЗА ВНИМАНИЕ!

Каменский Станислав
s.kamenskij@npo-echelon.ru


Эшелон
учебный центр