

# Журналирование в Windows

Дисциплина: Администрирование сетевых подсистем

Ибрахим Мохсейн Алькамаль

Российский университет дружбы народов (РУДН)

2025-12-05

# Содержание I

# 1 Введение

## 1.0.1 Значение журналирования

- Контроль и прозрачность работы ОС

## 1.0.2 Цель презентации

# 1 Введение

## 1.0.1 Значение журналирования

- Контроль и прозрачность работы ОС
- Диагностика ошибок и сбоев

## 1.0.2 Цель презентации

# 1 Введение

## 1.0.1 Значение журналирования

- Контроль и прозрачность работы ОС
- Диагностика ошибок и сбоев
- Анализ инцидентов безопасности

## 1.0.2 Цель презентации

## 1.0.1 Значение журналирования

- Контроль и прозрачность работы ОС
- Диагностика ошибок и сбоев
- Анализ инцидентов безопасности
- Мониторинг активности пользователей и служб

## 1.0.2 Цель презентации

## 1.0.1 Значение журналирования

- Контроль и прозрачность работы ОС
- Диагностика ошибок и сбоев
- Анализ инцидентов безопасности
- Мониторинг активности пользователей и служб

## 1.0.2 Цель презентации

- Рассмотреть механизм журналирования

## 1.0.1 Значение журналирования

- Контроль и прозрачность работы ОС
- Диагностика ошибок и сбоев
- Анализ инцидентов безопасности
- Мониторинг активности пользователей и служб

## 1.0.2 Цель презентации

- Рассмотреть механизм журналирования
- Изучить архитектуру Event Log

# 1 Введение

## 1.0.1 Значение журналирования

- Контроль и прозрачность работы ОС
- Диагностика ошибок и сбоев
- Анализ инцидентов безопасности
- Мониторинг активности пользователей и служб

## 1.0.2 Цель презентации

- Рассмотреть механизм журналирования
- Изучить архитектуру Event Log
- Показать инструменты анализа событий

### 2.0.1 Категории событий Windows

- Information

### 2.0.1 Категории событий Windows

- Information
- Warning

### 2.0.1 Категории событий Windows

- Information
- Warning
- Error

### 2.0.1 Категории событий Windows

- Information
- Warning
- Error
- Critical

### 2.0.1 Категории событий Windows

- Information
- Warning
- Error
- Critical
- Audit Success

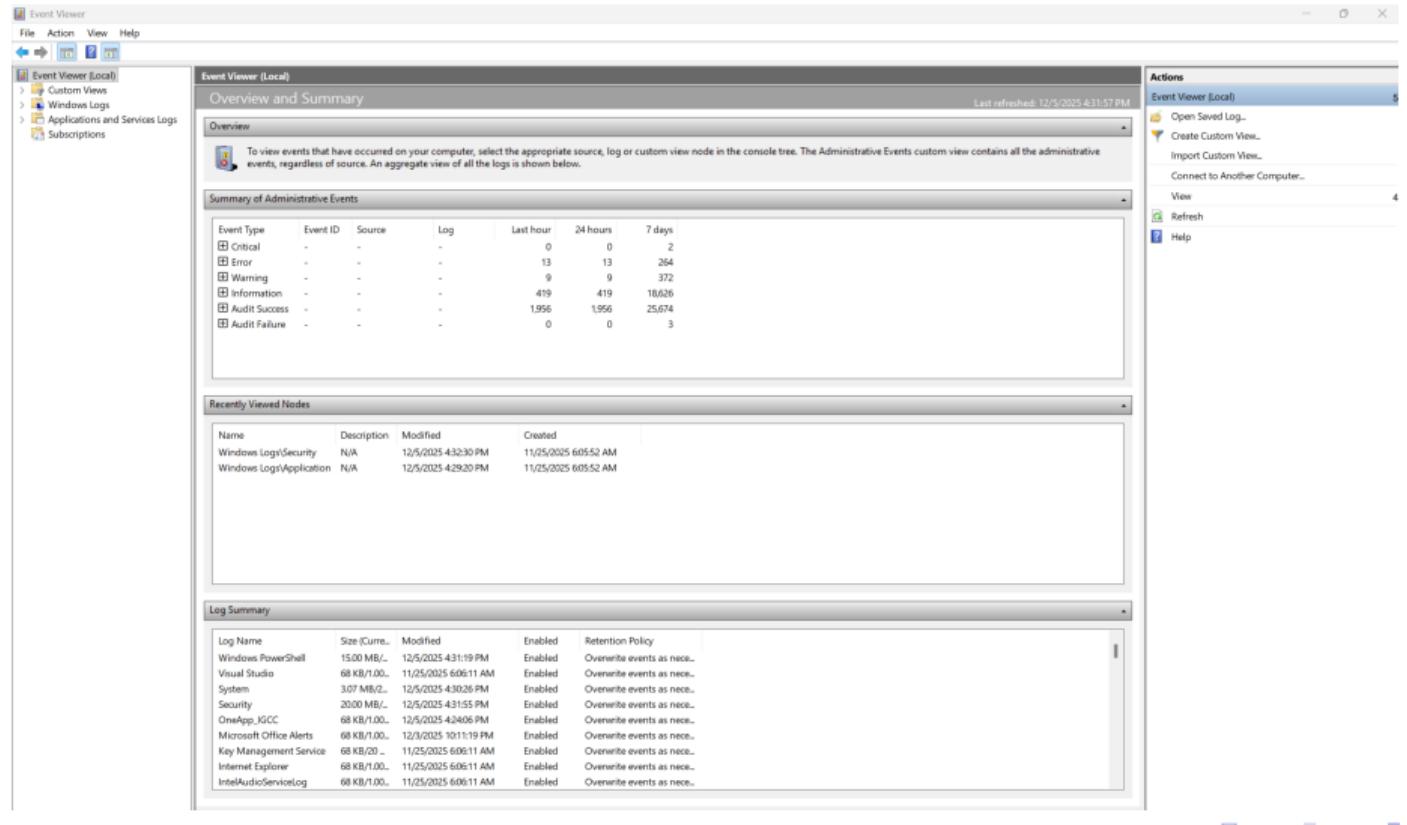
### 2.0.1 Категории событий Windows

- Information
- Warning
- Error
- Critical
- Audit Success
- Audit Failure

## 3 Основные журналы Windows

Журнал	Назначение
Application	События приложений
System	Ошибки драйверов и служб
Security	Аудит входов и изменений
Setup	Установка и конфигурация
Forwarded Events	События с других машин

# 4 Интерфейс Event Viewer



# 5 Архитектура журналирования Windows

## 5.0.1 Основные компоненты

- Event Providers

## 5.0.2 Типы каналов

# 5 Архитектура журналирования Windows

## 5.0.1 Основные компоненты

- Event Providers
- Event Log Service

## 5.0.2 Типы каналов

# 5 Архитектура журналирования Windows

## 5.0.1 Основные компоненты

- Event Providers
- Event Log Service
- Event Channels

## 5.0.2 Типы каналов

# 5 Архитектура журналирования Windows

## 5.0.1 Основные компоненты

- Event Providers
- Event Log Service
- Event Channels
- Event IDs

## 5.0.2 Типы каналов

# 5 Архитектура журналирования Windows

## 5.0.1 Основные компоненты

- Event Providers
- Event Log Service
- Event Channels
- Event IDs

## 5.0.2 Типы каналов

- Administrative

# 5 Архитектура журналирования Windows

## 5.0.1 Основные компоненты

- Event Providers
- Event Log Service
- Event Channels
- Event IDs

## 5.0.2 Типы каналов

- Administrative
- Operational

# 5 Архитектура журналирования Windows

## 5.0.1 Основные компоненты

- Event Providers
- Event Log Service
- Event Channels
- Event IDs

## 5.0.2 Типы каналов

- Administrative
- Operational
- Analytical

# 5 Архитектура журналирования Windows

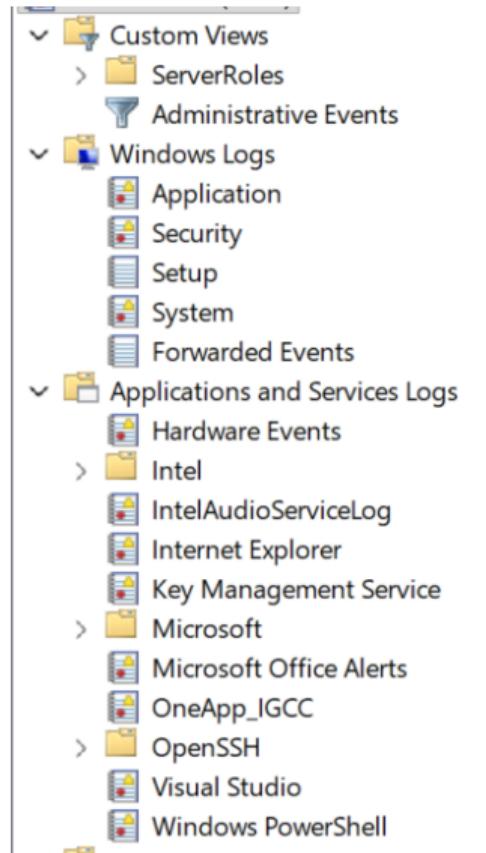
## 5.0.1 Основные компоненты

- Event Providers
- Event Log Service
- Event Channels
- Event IDs

## 5.0.2 Типы каналов

- Administrative
- Operational
- Analytical
- Debug

## 6 Структура каналов журналов



# 7 Инструменты журналирования

## 7.0.1 Event Viewer

- Просмотр событий

## 7.0.1 Event Viewer

- Просмотр событий
- Фильтрация

# 7 Инструменты журналирования

## 7.0.1 Event Viewer

- Просмотр событий
- Фильтрация
- Экспорт журналов

## 7.0.1 Event Viewer

- Просмотр событий
- Фильтрация
- Экспорт журналов
- Создание Custom View

# 8 Фильтрация событий

The screenshot shows the Windows Event Viewer interface. On the left, a list of events from the Application log is displayed, with event 16384 selected. A red box highlights the 'Filter Current Log' dialog box, which is open over the list. The dialog contains various filtering options like Logged, Event level, and Task category. On the right, a context menu is open for event 16384, also with a red box highlighting the 'Filter Current Log...' option under the 'Actions' section.

**Event 16384, Security-SPP**

Log Name:	Application	Source:	Security-SPP
Event ID:	16384	Logged:	12/5/2025 4:48:56 PM
Level:	Information	Task Category:	None
User:	N/A	Keywords:	Classic
OpCode:	Info	Computer:	DESKTOP-0FC1KSQ

**Actions**

- Application
- Open Saved Log...
- Create Custom View...
- Import Custom View...
- Clear Log...
- Filter Current Log...**
- Properties
- Find...
- Save All Events As...
- Attach a Task To this Log...
- View
- Refresh
- Help

**Event 16384, Security-SPP**

- Event Properties
- Attach Task To This Event...
- Copy
- Save Selected Events...
- Refresh
- Help

# 9 PowerShell для журналирования

Основные команды:

```
Get-EventLog -LogName Security -Newest 20
```

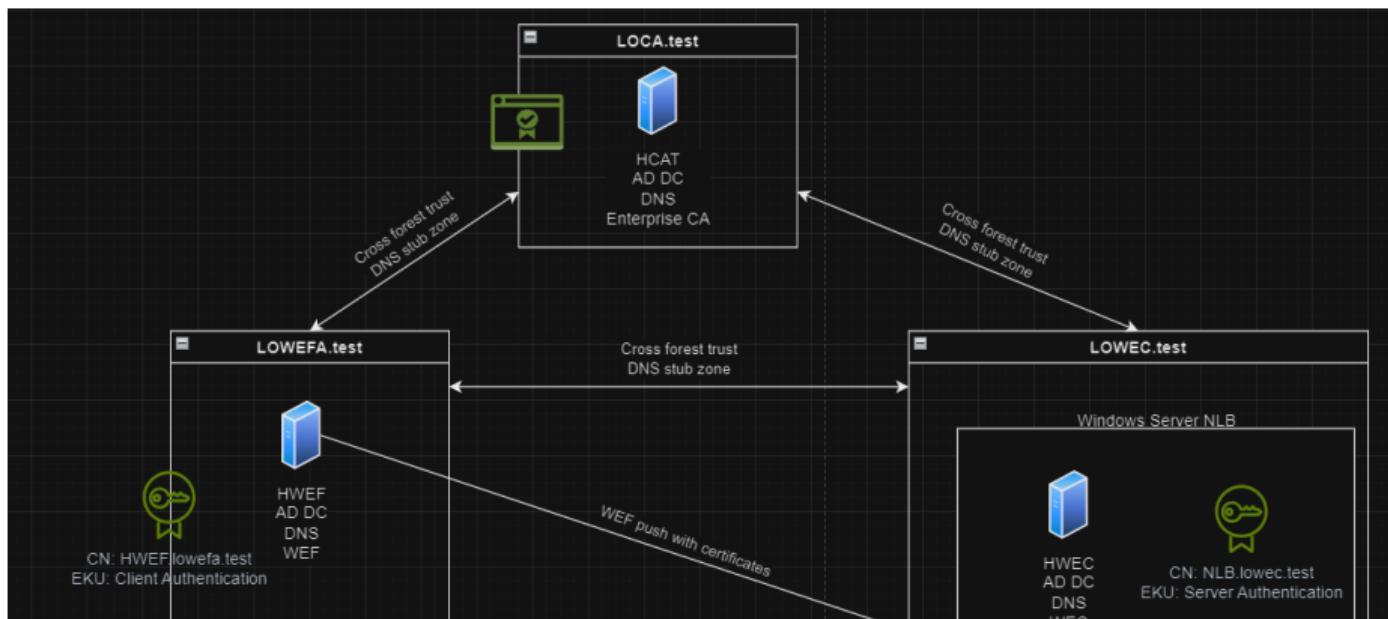
```
Get-WinEvent -LogName Application
```

```
Get-WinEvent -FilterHashtable @{LogName="Security"; ID=4625}
```

# 10 Windows Event Forwarding (WEF)

Используется для:

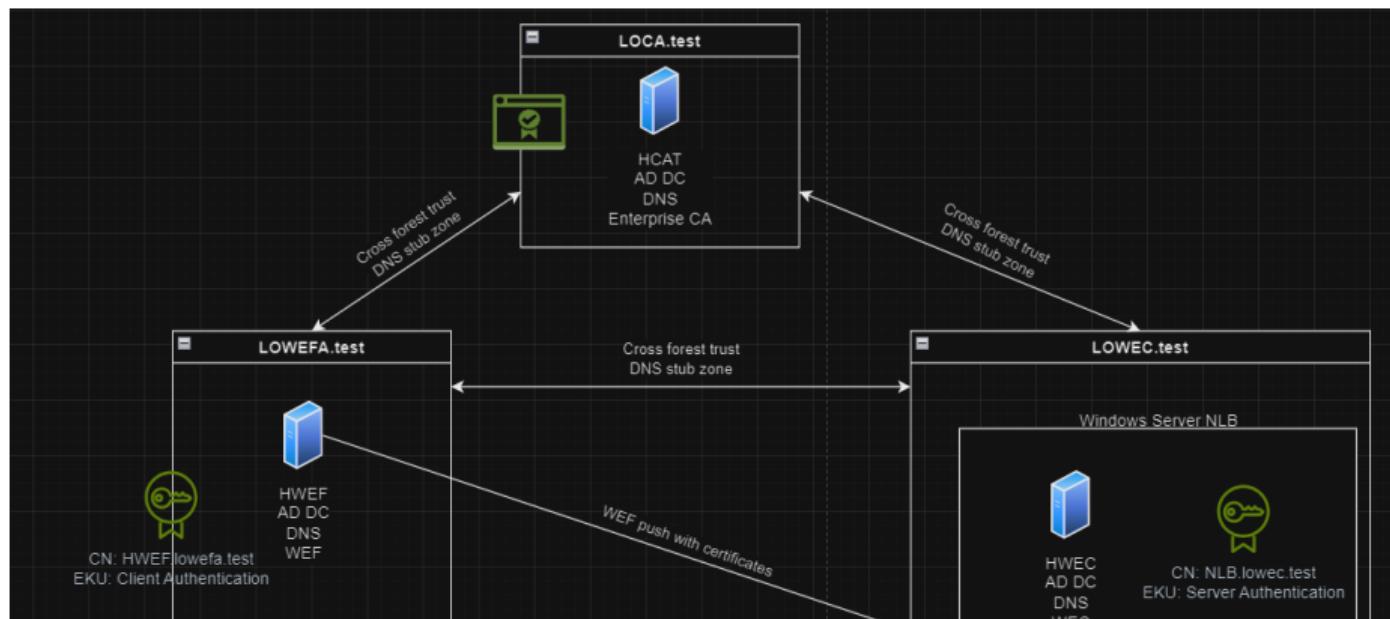
- Централизованного сбора событий



# 10 Windows Event Forwarding (WEF)

Используется для:

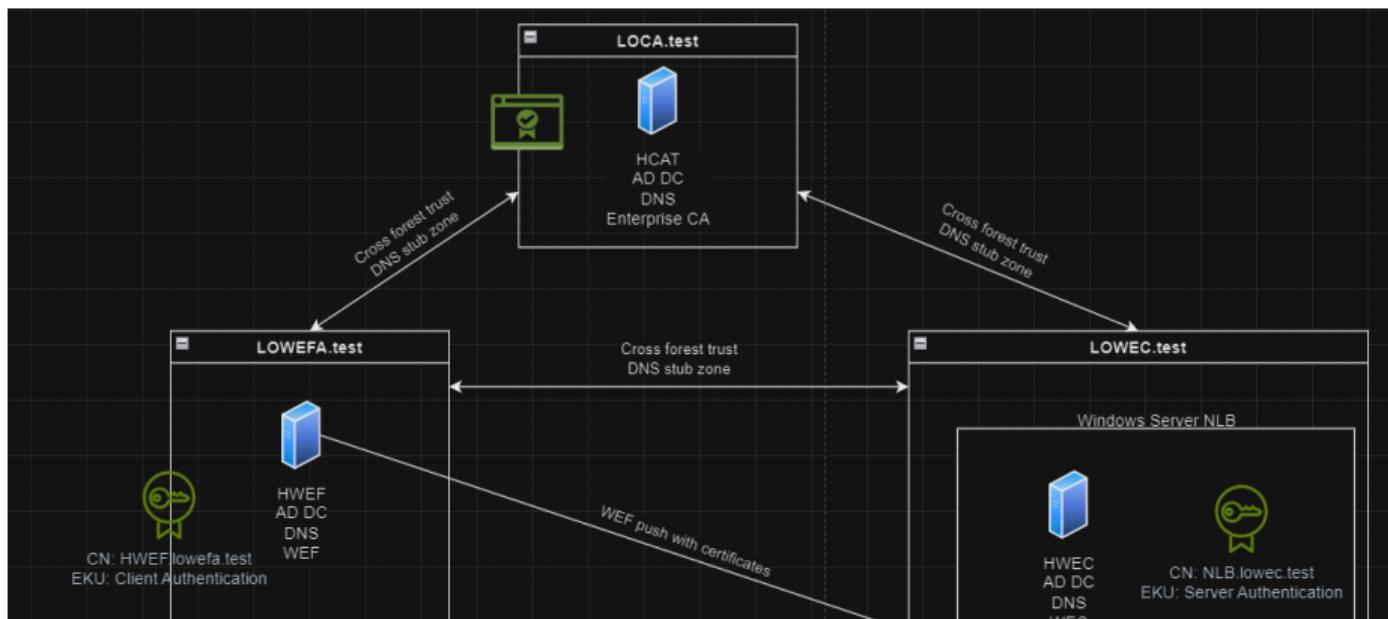
- Централизованного сбора событий
- Интеграции с SIEM



# 10 Windows Event Forwarding (WEF)

Используется для:

- Централизованного сбора событий
- Интеграции с SIEM
- Управления аудитом в корпоративных сетях

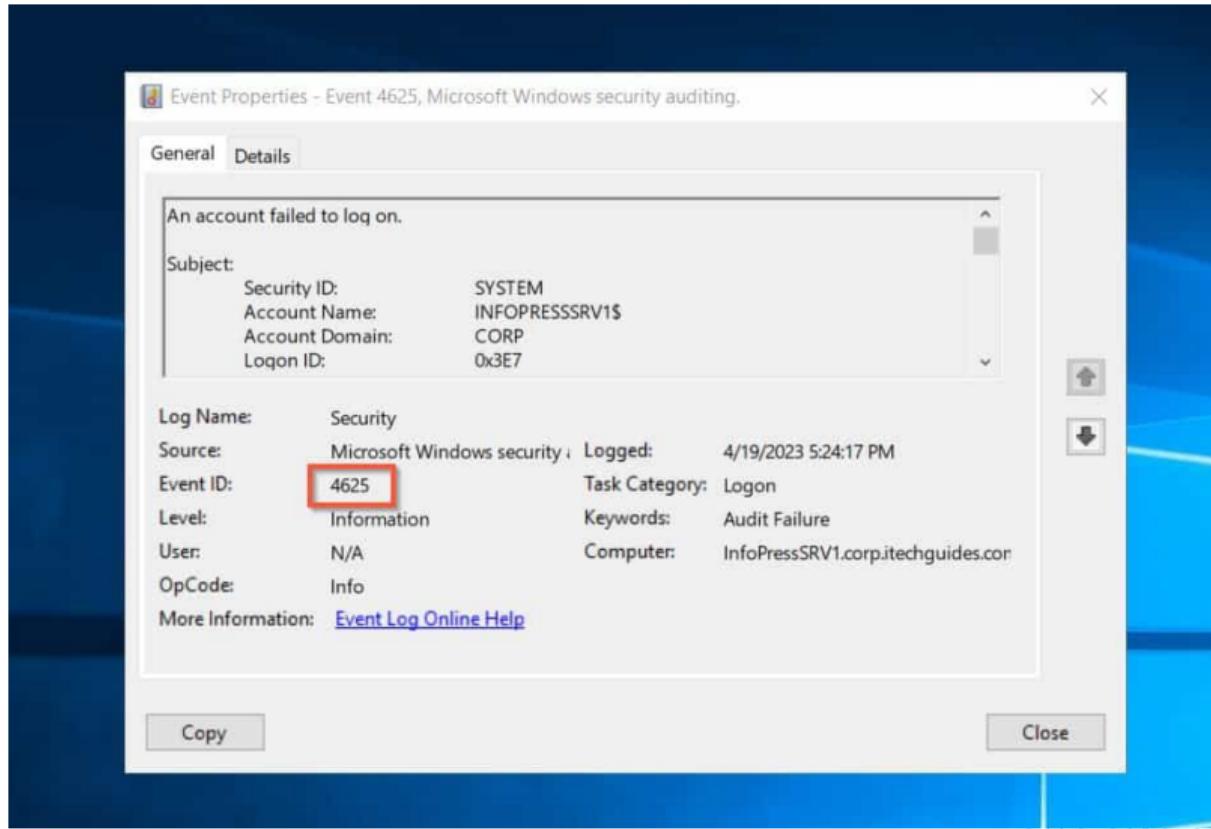


# 11 Журналирование безопасности

## 11.0.1 Основные события Security Log

ID	Описание
4624	Успешный вход
4625	Ошибка входа
4634	Выход
4720	Создание учётной записи
4726	Удаление учётной записи
1102	Очистка журнала

## 12 Пример события 4625



# 13 Расширенный аудит

Набор механизмов включает:

- Local Security Policy

# 13 Расширенный аудит

Набор механизмов включает:

- Local Security Policy
- Advanced Audit Policy Configuration

# 13 Расширенный аудит

Набор механизмов включает:

- Local Security Policy
- Advanced Audit Policy Configuration
- Sysmon

# 13 Расширенный аудит

Набор механизмов включает:

- Local Security Policy
- Advanced Audit Policy Configuration
- Sysmon
- Group Policy Objects

# 14 Настройка Audit Policies

The screenshot shows the Windows Local Security Policy snap-in window. The left pane displays a tree view of security settings, including Account Policies, Local Policies, Windows Defender Firewall with Advanced Security, Network List Manager Policies, Public Key Policies, Software Restriction Policies, Application Control Policies, IP Security Policies on Local Computer, and Advanced Audit Policy Configuration. Under Advanced Audit Policy Configuration, the 'System Audit Policies - Local Group Policy Object' node is expanded, showing sub-categories like Account Logon, Account Management (which is selected), Detailed Tracking, DS Access, Logon/Logoff, Object Access, Policy Change, Privilege Use, System, and Global Object Access Auditing. The right pane lists audit events categorized by subcategory, all of which are currently set to 'Not Configured':

Subcategory	Audit Events
Audit Application Group Management	Not Configured
Audit Computer Account Management	Not Configured
Audit Distribution Group Management	Not Configured
Audit Other Account Management Events	Not Configured
Audit Security Group Management	Not Configured
Audit User Account Management	Not Configured

Преимущества:

- Логирование сетевых подключений

Преимущества:

- Логирование сетевых подключений
- Отслеживание процессов

## Преимущества:

- Логирование сетевых подключений
- Отслеживание процессов
- Поддержка цепочек событий

## Преимущества:

- Логирование сетевых подключений
- Отслеживание процессов
- Поддержка цепочек событий
- Контроль изменений файлов

# 16 Экспорт журнала событий

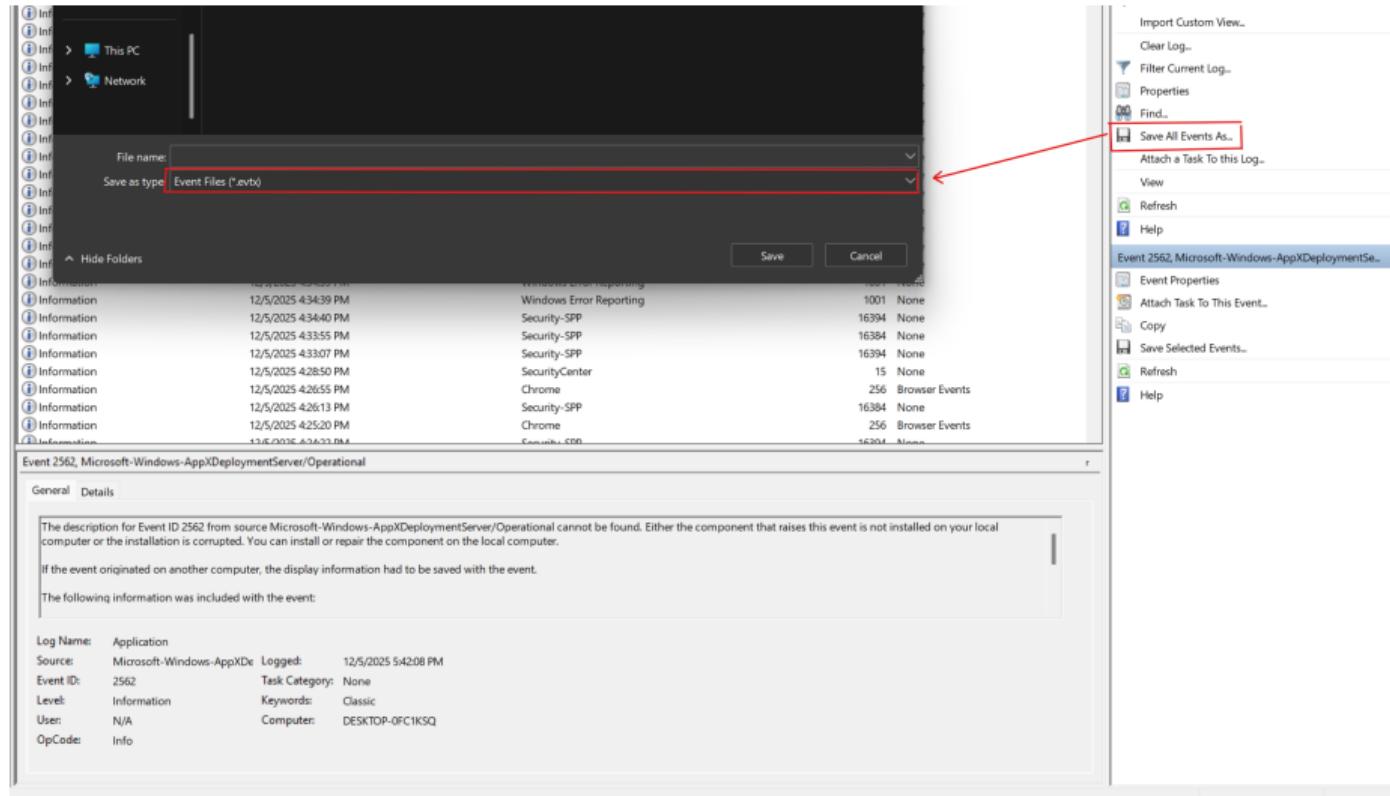


Рисунок 7. Экспорт журнала

# 17 Создание Custom View

The screenshot shows the Windows Event Viewer interface. On the left, a list of events from the Application log is displayed. A red box highlights the 'Create Custom View...' option in the context menu, which is open over the first event in the list. The context menu also includes options like 'Import Custom View...', 'Clear Log...', 'Filter Current Log...', 'Properties', 'Find...', 'Save All Events As...', 'Attach a Task To this Log...', 'View', 'Refresh', and 'Help'. The main window shows the details of Event ID 2562, which is described as a Microsoft Windows AppXDeploymentServer/Operat... error. The event details include the source (Microsoft-Windows-AppXDeploymentServer/Operat...), level (Information), and timestamp (12/5/2025 5:42:08 PM). The event properties table at the bottom lists Log Name: Application, Source: Microsoft-Windows-AppXDeploymentServer/Operat..., Logged: 12/5/2025 5:42:08 PM, Event ID: 2562, Task Category: None, Level: Information, Keywords: Classic, User: N/A, Computer: DESKTOP-0FC1KSQ.

- Журналирование — ключевой инструмент администратора

## 18 Заключение

- Журналирование — ключевой инструмент администратора
- Позволяет обнаруживать атаки

# 18 Заключение

- Журналирование — ключевой инструмент администратора
- Позволяет обнаруживать атаки
- Обеспечивает диагностику и анализ

# 18 Заключение

- Журналирование — ключевой инструмент администратора
- Позволяет обнаруживать атаки
- Обеспечивает диагностику и анализ
- Укрепляет защиту инфраструктуры

- Журналирование — ключевой инструмент администратора
- Позволяет обнаруживать атаки
- Обеспечивает диагностику и анализ
- Укрепляет защиту инфраструктуры
- Интегрируется с SIEM, PowerShell и Sysmon

# 19 Спасибо за внимание!