



## **МИНОБРНАУКИ РОССИИ**

Федеральное государственное бюджетное образовательное учреждение  
высшего образования

**«МИРЭА – Российский технологический университет»**

**РТУ МИРЭА**

---

**Институт кибербезопасности и цифровых технологий (ИКБ)**

**КБ-2 «Информационно-аналитические системы кибербезопасности»**

---

### **ОТЧЕТ О ВЫПОЛНЕНИИ ИНДИВИДУАЛЬНОГО ЗАДАНИЯ №13**

**В РАМКАХ ДИСЦИПЛИНЫ «ПРИНЦИПЫ ПОСТРОЕНИЯ,  
ПРОЕКТИРОВАНИЯ И ЭКСПЛУАТАЦИИ  
ИНФОРМАЦИОННО-АНАЛИТИЧЕСКИХ СИСТЕМ»**

Выполнил:

Студент 4-ого курса

Учебной группы БИСО-02-22

Зубарев В.С.

Москва 2025

The screenshot shows the MaxPatrol 10 interface with the following details:

- Top Bar:** pt MaxPatrol 10, Events for November 22, 2022-24, All assets.
- Left Sidebar:** Groups (All events, Unlinked, All assets), Filters (\* All events, System filters, BAD-based analytics, BAD dashboards, Highest risk sc..., Count of proce..., Processes with..., Process chains...).
- Center Panel:** Filter bar: subject.account.name = "d\_jensen" and\_ \* > ||| time, event\_src.host, text > ↓ time (newest on top) > Execute. A dropdown menu is open over the filter bar with the query: subject.account.name = "d\_jensen" and object = "file" and action = "open".
- Table View:** Shows a list of events with columns: time, event\_src.host, text. The events listed are:
  - 11/23/22, 11:11:32 comp-2159.hv-logistics.stf The user d\_jensen started the Microsoft Office process winword.exe and opened the document with a m...
  - 11/23/22, 11:05:01 comp-2159.hv-logistics.stf The user d\_jensen started the Microsoft Office process excel.exe and opened the document with a macr...
  - 11/22/22, 20:30:09 comp-2159.hv-logistics.stf The user d\_jensen started the Microsoft Office process excel.exe and opened the document with a macr...
  - 11/22/22, 12:34:07 comp-2159.hv-logistics.stf The user d\_jensen started the Microsoft Office process winword.exe and opened the document with a m...
  - 11/22/22, 11:56:02 comp-2159.hv-logistics.stf The user d\_jensen started the Microsoft Office process winword.exe and opened the document with a m...
- Bottom:** Total 9 events, 1 selected.

Рисунок 1 – фильтр

The screenshot shows the MaxPatrol 10 interface with the following details:

- Top Bar:** pt MaxPatrol 10, Events for November 22, 2022-24, All assets.
- Left Sidebar:** Groups (All events, Unlinked, All assets), Filters (\* All events, System filters, BAD-based analytics, BAD dashboards, Highest risk sc..., Count of proce..., Processes with..., Process chains...).
- Center Panel:** Filter bar: subject.account.name = "d\_jensen" and\_ \* > ||| time, event\_src.host, text > ↓ time (newest on top) > Execute. A dropdown menu is open over the filter bar with the query: subject.account.name = "d\_jensen" and object = "file" and action = "open".
- Table View:** Shows a list of events with columns: time, event\_src.host, text. The events listed are:
  - 11/23/22, 20:34:39 comp-2159.hv-logistics.stf The user d\_jensen started the Microsoft Office process winword.exe and opened the document with a m...
  - 11/23/22, 18:16:10 comp-2159.hv-logistics.stf The user d\_jensen started the Microsoft Office process excel.exe and opened the document with a macr...
  - 11/23/22, 11:11:51 comp-2159.hv-logistics.stf The user d\_jensen started the Microsoft Office process excel.exe and opened the document with a macr...
  - 11/23/22, 11:11:45 comp-2159.hv-logistics.stf The user d\_jensen started the Microsoft Office process excel.exe and opened the document with a macr...
  - 11/23/22, 11:11:32 comp-2159.hv-logistics.stf The user d\_jensen started the Microsoft Office process excel.exe and opened the document with a macr...
  - 11/23/22, 11:05:01 comp-2159.hv-logistics.stf The user d\_jensen started the Microsoft Office process winword.exe and opened the document with a m...
  - 11/22/22, 20:30:09 comp-2159.hv-logistics.stf The user d\_jensen started the Microsoft Office process excel.exe and opened the document with a macr...
  - 11/22/22, 12:34:07 comp-2159.hv-logistics.stf The user d\_jensen started the Microsoft Office process winword.exe and opened the document with a m...
  - 11/22/22, 11:56:02 comp-2159.hv-logistics.stf The user d\_jensen started the Microsoft Office process winword.exe and opened the document with a m...
- Bottom:** Total 9 events, 1 selected.

Рисунок 2 - результат вывода

The screenshot shows the MaxPatrol 10 interface. In the center, a detailed view of an event is displayed. The event occurred on 11/23/22 at 11:05:01. The subject account name is "d\_jensen". The event source host is "comp-2159.hv-logistics.stf". The event type is "Microsoft Office process". The text field contains the message: "The user d\_jensen started the Microsoft Office process". To the right of the event details, there is an "Additional information" section with various data fields like status, datafield1, datafield3, etc. Below the event details, there is a "Service data" section. On the left side of the screen, there is a sidebar with filters and a main panel showing a list of events. The list shows several entries for the same Microsoft Word process starting.

Рисунок 3- открытие документа

This screenshot shows the MaxPatrol 10 interface with a new filter applied. A modal dialog box is open in the center, titled "Filter". Inside the dialog, a query is being constructed: "event\_src.host = 'comp-2159.hv-logistics.stf' and msgid in [4103,4104,4688] and subject.account.name = 'd\_jensen'". Below the dialog, the main event list shows nine events. The first event is highlighted. The event details show it occurred on 11/23/22 at 11:11:32, was started by "d\_jensen" on "comp-2159.hv-logistics.stf", and was a Microsoft Office process. The text field indicates the user started the Microsoft Office process. The right side of the screen displays the "Additional information" and "Service data" sections, which are identical to the previous screenshot. The left sidebar shows the same filters and asset groups.

Рисунок 4 - новый фильтр, на основе полученных данных

The screenshot shows the MaxPatrol 10 interface with the following details:

- Header:** MaxPatrol 10, Events, System.
- Left Sidebar:** Groups, All events, Unlinked, All assets (selected), Unmanaged hosts, Filters (All events selected).
- Top Bar:** Copy, Export, Show on topology, and a search bar.
- Event Filter:** Filter: All events \*  
event\_src.host = "comp-2159.hv-logist... > time, event\_src.host, text >  
time (newest on top) > Execute
- Event List:** A table showing 767 events. The columns are time, event\_src.host, and text. The text column contains descriptions like "A PowerShell pipeline is executed on host comp-2195" and "account start process success on host comp-2159".
- Right Panel:** A message box stating "Could not retrieve a list of events: the browser time is different from the server time. Try increasing the time interval for displaying events." Below it is a "Technical details" section and a "Request additional data" button.
- Bottom:** A summary table with columns Subject, Action, Object, Status, and Source, showing details for the selected event.

Рисунок 5 - команда, скачивающая powershell скрипт

The screenshot shows the MaxPatrol 10 interface. The top navigation bar includes 'Events' (selected), 'System', and a date filter for November 23, 2022. The left sidebar has sections for 'Groups', 'All events', 'Unlinked', 'All assets' (selected), and 'Unmanaged hosts'. Under 'Filters', there's a search bar and a list of system filters like 'All events', 'BAD-based analytics', and 'BAD dashboards'. The main area displays an event timeline with a selected entry for November 23, 2022, at 10:56:33 from host 'comp-2159.hv-logistics.stf'. The event details show a PowerShell command execution. A modal window is open, showing the raw log entry: 'event\_src.host = "comp-2159.hv-logistics.stf" and object.name contains ".ps1" and subject.account.name = "d\_jensen"'. Below the timeline, it says 'Total 767 events, 1 selected'. To the right, a message box states 'Could not retrieve a list of events: the browser time is different from the server time. Try increasing the time interval for displaying events.' and a 'Technical details' section with event logs.

## Рисунок 6 - новый фильтр

The screenshot shows the MaxPatrol 10 interface. The left sidebar has sections for Groups (All events, Unlinked, All assets - expanded, Unmanaged hosts), Filters (\* All events selected, System filters, BAD-based analytics, BAD dashboards, Highest risk sc..., Count of proce..., Processes with..., Process chains...), and Events (for November 23, 2022-24). The main area displays a table of events with columns: time, event\_src.host, and text. The table shows 34 events, with the last two rows highlighted in blue. The right side shows detailed event properties for the last event: Subject (d\_jensen hv-logistics\_), Action (execute), Object (powershell.exe, object file\_object, fullname c:\windows\syswow64\qwe.ps1, object file\_object, type script, fullname c:\windows\tasks\qwe.ps1), Status (success), and Source (1792c8d6-2380-0001-0...).

time	event_src.host	text
11/23/22, 11:57:32	comp-2159.hv-logistics.stf	User d_jensen from host created the potentially ma
11/23/22, 11:57:16	comp-2159.hv-logistics.stf	User d_jensen from host created the potentially ma
11/23/22, 11:41:42	comp-2159.hv-logistics.stf	User d_jensen from host created the potentially ma
11/23/22, 11:32:21	comp-2159.hv-logistics.stf	User d_jensen from host created the potentially ma
11/23/22, 11:10:09	comp-2159.hv-logistics.stf	User d_jensen from host created the potentially ma
11/23/22, 10:57:21	comp-2159.hv-logistics.stf	User d_jensen from host created the potentially ma
11/23/22, 10:57:21	comp-2159.hv-logistics.stf	User d_jensen from host created the potentially ma
11/23/22, 10:57:20	comp-2159.hv-logistics.stf	The user d_jensen attempted to run the script "qwe.
11/23/22, 10:57:20	comp-2159.hv-logistics.stf	The user d_jensen attempted to run the script "qwe.
11/23/22, 10:56:18	comp-2159.hv-logistics.stf	User d_jensen from host created the potentially ma

Рисунок 7 - alert.key