



## 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 №2**

**В РАМКАХ ДИСЦИПЛИНЫ «Принципы построения,  
проектирования и эксплуатации информационно-  
аналитических систем»**

Выполнил:

Студент 3-ого курса

Учебной группы БИСО-02-22

Зубарев В.С.

Москва 2025

## Filter

```
object.name contains '.mp4' or object.name contains '.avi' or object.name
contains '.mkv' or object.name contains '.wmv'
```

▶ Execute Ctrl+Enter



Change

Cancel

Рисунок 1 - фильтр поиска видеозаписей

The screenshot shows the MaxPatrol 10 interface. On the left, there's a sidebar with 'Groups' and 'Filters'. Under 'Filters', 'All events' is selected. In the main pane, a search bar at the top has the query: `object.name contains '.mp4' or object.name contains '.avi' or object.name contains '.mkv' or object.name contains '.wmv'`. Below the search bar, a table lists several log entries. One entry from 11/22/22, 11:50:04 shows the file object `/var/www/html/wordpress/wp-content/themes/Landscape-757.mp4`. To the right of the table, a detailed view of the event is shown under 'Interaction roles' and 'Object' sections.

Рисунок 2 – компьютер загружающий видео трафик

The screenshot shows the NAD (Network Analysis Dashboard) interface. At the top, it displays a timeline from 21 ноября 2022 to 23 ноября 2022, 00:00. A search bar indicates `dst.ip = 10.126.11.174`. Below the timeline, it says '96 381 сессия · 58 узлов · 5 503 атаки · 28 944 индикатора компрометации'. The main area is divided into several sections: 'Клиенты по странам' (Clients by countries), 'Серверы по странам' (Servers by countries), 'Прикладные протоколы' (Application protocols), 'Транспортные протоколы' (Transport protocols), and two tables for 'Клиенты по сессиям и трафику' (Clients by sessions and traffic) and 'Серверы по сессиям и трафику' (Servers by sessions and traffic).

Рисунок 3 - справка по целевому устройству

## Клиенты по сессиям и трафику

IP-адрес	Доменное имя	Кол...	Получено
10.156.11.61	proxy-af1.standoff365.com	37 583	4,09 ГБ
10.126.25...	—	22 399	152,73 Мб
172.31.9.1...	—	22 020	15,56 Мб
10.126.25...	—	4828	6,66 Мб

Рисунок 4 - выявление моста загрузки

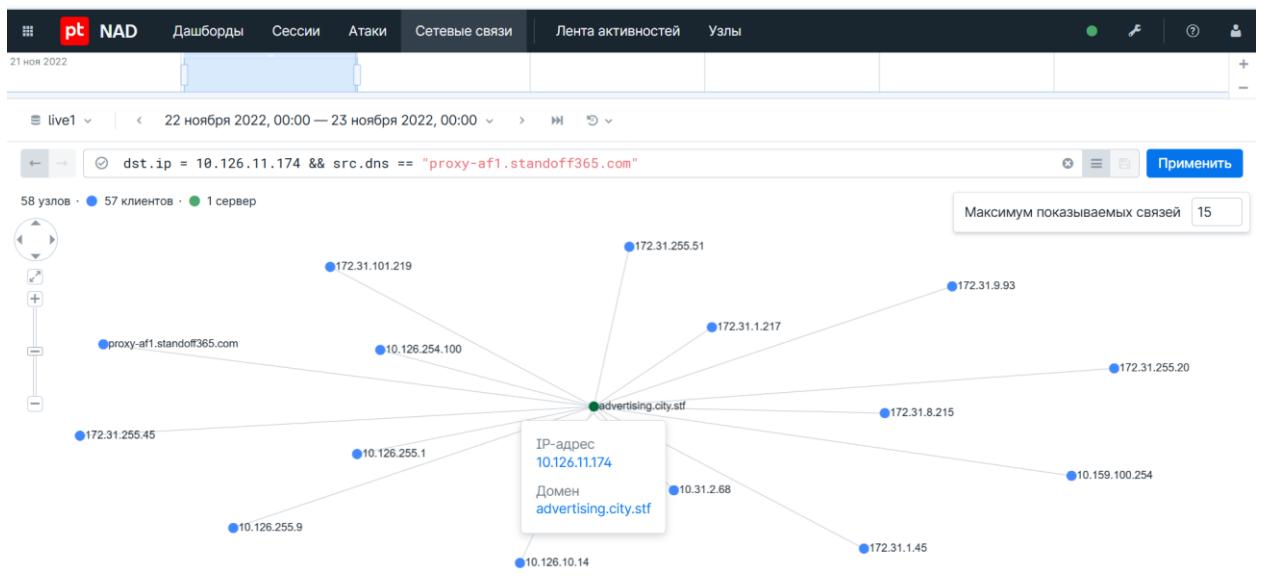


Рисунок 5 - график связей для целевого устройства