



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. The top bar includes the 'pt' logo, 'MaxPatrol 10', and tabs for 'Events' and 'System'. The main area displays a filter: 'Filter: All events *' with the criteria 'object.name contains '.mp4' or object.name contains '.avi' or object.name contains '.mkv' or object.name contains '.wmv'. Below the filter is a table of events with columns 'time', 'event_src.host', and 'text'. The table shows multiple entries for '10.126.11.174' at various times, all with the text 'The file object "/var/www/html/wordpress...'. On the right, the 'Interaction roles' section shows details for a selected event, including 'subject.type: web daemon', 'subject.name: Landscape-757.mp4', and 'object.type: executable_file'.

Рисунок 2 – компьютер загружающий видео трафик

The screenshot shows the NAD interface. The top bar includes the 'pt' logo, 'NAD', and tabs for 'Дашборды', 'Сессии', 'Атаки', 'Сетевые связи', 'Лента активностей', and 'Узлы'. The main area displays a traffic analysis for the IP address '10.126.11.174'. The interface shows a timeline of traffic from 22 ноября 2022, 00:00 to 23 ноября 2022, 00:00. Below the timeline, there are several charts and tables. The 'Прикладные протоколы' chart shows a pie chart with 'http' (6,74 ГБ), 'tftp' (1,08 КБ), 'icmp' (1,98 КБ), and 'Неизвестные' (523,63 МБ). The 'Транспортные протоколы' chart shows a pie chart with 'icmp' (1,98 КБ) and 'udp' (24,97 КБ). The 'Клиенты по странам' and 'Серверы по странам' sections show 'Данные отсутствуют'. The 'Клиенты по сессиям и трафику' table shows data for two IP addresses: '10.156.11.61' and '10.126.25...'. The 'Серверы по сессиям и трафику' table shows data for '10.126.11...'.

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

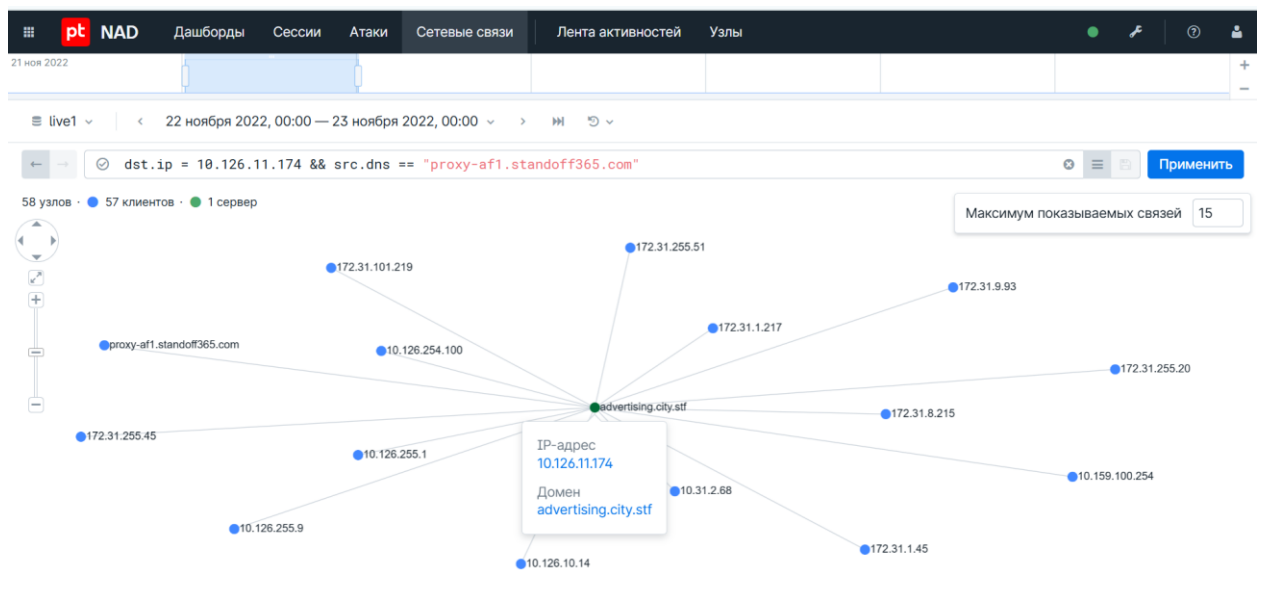


Рисунок 5 - граф связей для целевого устройства