



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 №11

**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

The screenshot shows the PT NAD web interface. At the top, there is a navigation bar with tabs: Дашборды, Сессии, Атаки, Сетевые связи, Лента активностей, and Узлы. The 'Атаки' tab is selected. Below the navigation bar, there is a date range selector from 21 ноября 2022 to 23 ноября 2022, 00:00. A search bar contains the query: dst.ip = 10.126.11.174 & alert.msg == "ATTACK [PTsecurity] log4j RCE aka Log4Shell TCP attempt (CVE-2021-44228)". A button labeled 'Применить' (Apply) is next to it. Below the search bar, there is a summary: 5 403 атаки - 4 292 высокой опасности - 3 средней опасности - 1108 низкой опасности - 0 других событий - 0 срабатываний отмечены как ложные. There is also a link 'Показать временную шкалу' (Show timeline) and a link 'Выпустить отчет' (Release report). The main area displays a table titled 'Показаны 5 000 атак из 5 403. Выбрана 1'. The table has columns: Название, Класс, Обнаружена, IOC, IP-адрес ата..., Страна атаку..., IP-адрес ата..., and Страна атаку...'. The table lists several entries related to the Log4Shell attack.

Рисунок 1 - фильтр PT NAD

The screenshot shows the PT NAD web interface. The navigation bar and date range selector are identical to the first screenshot. The search bar contains the same query: dst.ip = 10.126.11.174 & alert.msg == "ATTACK [PTsecurity] log4j RCE aka Log4Shell TCP attempt (CVE-2021-44228)". A button labeled 'Применить' is present. Below the search bar, there is a summary: 4 720 атак - 3 778 высокой опасности - 0 средней опасности - 942 низкой опасности - 0 других событий - 0 срабатываний отмечены как ложные. There is also a link 'Скрыть временную шкалу' (Hide timeline) and a link 'Выпустить отчет' (Release report). The main area features a timeline chart showing activity spikes around 16:00 and 18:00 on November 22, 2022. Below the chart, a section titled 'ET EXPLOIT Apache log4j RCE Attempt - lower/upper TCP Bypass M2 (CVE-2021-44228)' provides detailed information about the attack. It includes tabs for 'Общие сведения', 'Описание и рекомендации', and 'Сработавшее правило' (which is currently selected). The right side of the panel shows the raw request headers and a sidebar with options: 'Отметить как ложное сраб...', 'Перейти к правилу', and 'Скопировать ссылку'.

Рисунок 2 - Private AT