**А.А. Громов (СПбГУТ)**

Обнаружение компьютерных атак при помощи ELK-SIEM

Работа посвящена изучению способов обнаружения компьютерных атак. Актуальность работы обоснована ростом количества атак на сетевую/серверную инфраструктуру. Столь бурный рост связан с упрощением эксплуатации уязвимостей. В рамках данной работы будет рассмотрено решение от компании Elastic. Главный фактор, по которому было выбрано данное решение - бесплатность. В рамках данной работы был разработан docker-compose файл, который позволяет быстро разворачивать рабочую инфраструктуру, а также были созданы собственные правила корреляции для обнаружения атак.