**KOMRAD Enterprise SIEM 4.5 · Источники** НОУ ДПО «УЦБИ "МАСКОМ"»

# Источники и проверочная база

Материалы подготовлены для занятий в НОУ ДПО «УЦБИ "МАСКОМ"», г. Москва, по темам:

- «Обзор системы управления событиями информационной безопасности KOMRAD Enterprise SIEM»
- «Практическое применение KOMRAD Enterprise SIEM»

Дата занятия по расписанию: 14.05, 09:30-18:20.

## Локальные материалы

- `DEMO_KOMRAD Enterprise SIEM 4.5/komrad_v4.5.22-demo_astra_1.8_amd64.run` - локальный установщик демо-версии KOMRAD 4.5.22 для Astra Linux 1.8.
- `DEMO_KOMRAD Enterprise SIEM 4.5/komrad_v4.5.22-demo_windows_amd64_wmi-installer.exe` - локальный установщик Windows WMI-агента.
- `DEMO_KOMRAD Enterprise SIEM 4.5/license_komrad-v4.5_ВУЗы.lic` - локальный файл лицензии для учебного стенда.
- `DEMO_KOMRAD Enterprise SIEM 4.5/KOMRAD Enterprise SIEM. Quickstart Guide.pdf` - локальное краткое руководство.
- `Задание на ПЗ.docx` - исходная заготовка практического задания.
- `Администрирование KOMRAD (YouTube)/*.txt` - транскрипции/конспекты вебинаров вендора по SOC-процессам, подключению коллекторов, Windows/Linux-источникам, нормализации и фильтрации.
- `ГОСТы про инциденты/*.pdf` - локальная нормативная папка: ГОСТ Р 59547-2021, ГОСТ Р 59548-2022, ГОСТ Р 59709-2022, ГОСТ Р 59710-2022, ГОСТ Р 59711-2022, ГОСТ Р 59712-2022.

## Официальные страницы, проверенные 13.05.2026

- https://npo-echelon.ru/komrad-siem/ - страница продукта и форма получения демоверсии.
- https://docs.etecs.ru/komrad/docs/intro/ - документация KOMRAD 4.5.X: назначение, функциональность, технические характеристики, сертификат ФСТЭК.
- https://docs.etecs.ru/komrad/docs/install/prerequisites/ - требования к системе.
- https://docs.etecs.ru/komrad/docs/install/auto_install/ - автоматическая установка KOMRAD 4.5.X.
- https://docs.etecs.ru/komrad/docs/install/install_astra/ - установка на Astra Linux Special Edition.
- https://docs.etecs.ru/komrad/docs/manage/collectors/wmi_agent/ - Windows WMI-агент.
- https://docs.etecs.ru/komrad/docs/components/tcp-ports/ - перечень TCP-портов.
- https://docs.etecs.ru/komrad/blog/Релиз%204.5/ - описание релиза 4.5.
- https://www.virtualbox.org/manual/topics/installation.html - установка VirtualBox и Extension Pack.

## Что важно не перепутать на занятии

- В официальной документации открыта ветка 4.5.X; часть страниц рядом с ней уже имеет ветку 4.6.X, поэтому для занятия по 4.5 нужно явно выбирать 4.5.X.
- Локальный учебный комплект содержит демо 4.5.22 для Astra Linux 1.8 и Windows WMI-агент; если слушатели скачивают свежую демо-версию у вендора, они должны использовать фактические имена файлов из полученного архива.
- Официальные требования 4.5.X указывают Astra Linux 1.7 с обновлениями и Astra Linux 1.8 как поддерживаемые ОС, а VirtualBox - как поддерживаемую среду виртуализации.
- В практических заданиях ниже команды и IP-адреса приведены как шаблон: преподаватель должен заменить `KOMRAD_IP`, `WIN_IP`, `LINUX_IP` на адреса реального стенда.