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

# Раздаточный конспект: мониторинг ИБ и KOMRAD Enterprise SIEM 4.5

Материалы для слушателей профессиональной переподготовки по информационной безопасности. НОУ ДПО «УЦБИ "МАСКОМ"», г. Москва.

## 1. Что такое мониторинг ИБ

Мониторинг информационной безопасности - это организованный процесс наблюдения за событиями в информационной системе, чтобы своевременно обнаруживать признаки нарушений, расследовать их и реагировать.

Простая логика процесса:

`источник -> событие -> сбор -> нормализация -> хранение -> анализ -> инцидент -> реагирование -> отчет`.

## 2. Что такое SIEM

SIEM - система централизованного управления событиями информационной безопасности. Она собирает события из разных источников, приводит их к единому виду, хранит, позволяет искать и фильтровать события, строить корреляции и управлять инцидентами.

Важно: SIEM не заменяет администратора или аналитика. Она помогает увидеть картину, сократить ручную работу и дать доказательную базу для расследования.

## 3. Нормативные документы занятия

- ГОСТ Р 59547-2021 - мониторинг информационной безопасности, общие положения.
- ГОСТ Р 59548-2022 - регистрация событий безопасности.
- ГОСТ Р 59709-2022 - термины и определения по управлению компьютерными инцидентами.
- ГОСТ Р 59710-2022 - общие положения управления компьютерными инцидентами.
- ГОСТ Р 59711-2022 - организация деятельности по управлению компьютерными инцидентами.
- ГОСТ Р 59712-2022 - руководство по реагированию на компьютерные инциденты.

На занятии эти документы нужны не для заучивания номеров, а для понимания: почему события нужно регистрировать, хранить, анализировать и связывать с реагированием.

## 4. KOMRAD Enterprise SIEM 4.5

KOMRAD Enterprise SIEM - отечественная SIEM-система. По документации версии 4.5.X она поддерживает сбор событий, нормализацию, индексацию, фильтрацию, корреляцию, управление инцидентами, визуализацию и отчеты.

Возможности, которые мы смотрим на занятии:

- сбор событий Windows и Linux;
- нормализация событий;
- события в реальном времени;
- фильтры и поиск;
- дашборды;
- инциденты;
- практическая связь события и реагирования.

## 5. Мини-словарь

| Термин | Простое объяснение |
|---|---|
| Источник событий | Узел или система, где возникает событие: ОС, СЗИ, сетевое устройство, приложение |
| Событие | Запись о факте: вход, ошибка, изменение учетной записи, очистка журнала |
| Нормализация | Приведение разных форматов событий к единой структуре |
| Фильтр | Правило отбора событий по условиям |
| Корреляция | Поиск связи между несколькими событиями |
| Инцидент | Событие или цепочка событий, требующая реакции ИБ |
| Реагирование | Действия по анализу, локализации, устранению и фиксации результата |

## 6. Что нужно запомнить

1. Лог не равен инциденту. Лог - исходный факт, инцидент - результат анализа.
2. Без нормализации трудно сравнивать события разных систем.
3. Очистка журналов, массовые ошибки входа, добавление в администраторы и изменение критичных конфигураций - типовые события, на которые стоит обращать внимание.
4. Отчет по ПЗ должен фиксировать не только "что нажал", но и "что увидел в SIEM" и "какой вывод сделал".