{KOMRAD}
Enterprise SIEM

Эшелон
комплексная безопасность

# KOMRAD Enterprise SIEM

## Соответствие требованиям ФСТЭК России

# Соответствие требованиям ФСТЭК России

| Обозначение и номер меры | Меры обеспечения безопасности значимого объекта | Соответствия | Модель применения | Соответствие документации (где можно найти в нашей документации) |
|---|---|---|---|---|
| ФСТЭК России № 17, 21 | | | | |
| РСБ.3 | Сбор, запись и хранение информации о событиях безопасности | + | Возможность сбора, записи информации о событиях безопасности | Онлайн документация |
| РСБ.4 | Реагирование на сбои при регистрации событий безопасности и программные ошибки, сбои в механизмах сбора информации | + | Осуществляется реагирование на сбои при регистрации событий безопасности. Реагирование предусматривает предупреждение (индикацию) о сбоях через сигнализатор, цвета которого говорят об определённом состоянии. | Онлайн документация |
| РСБ.5 | Мониторинг результатов регистрации событий безопасности и реагирование на них | + | Возможность осуществлять мониторинг (просмотр, анализ) результатов регистрации событий безопасности и реагирование на них | Онлайн документация |

| | | | | |
|---|---|---|---|---|
| РСБ.7 | Защита информации о событиях безопасности | + | Обеспечивается защита информации о событиях безопасности с применением мер защиты от неправомерного доступа, уничтожения или модифицирования | Онлайн документация |
| РСБ.8 | Возможности просмотра информации о действиях отдельных пользователей в информационной системе | + | Возможность просмотра и выгрузки отчётов по действиям отдельных пользователей для последующего анализа | Онлайн документация |
| ЗСВ.3 | Регистрация событий безопасности в виртуальной инфраструктуре | + | Возможность сбора событий с гипервизоров | Онлайн документация |

# Соответствие требованиям ФСТЭК России

| Обозначение и номер меры | Меры обеспечения безопасности значимого объекта | Соответствия | Модель применения | Соответствие документации (где можно найти в нашей документации) |
|---|---|---|---|---|
| ФСТЭК России № 239 | | | | |
| АУД.1 | Инвентаризация информационных ресурсов | + | Функционал KOMRAD Enterprise SIEM<br>Раздел «Активы»<br>При приходе события информационной безопасности информация об активе заносится в БД. Имеется возможность создания задачи на сканирование информационных ресурсов в инфраструктуре | Онлайн документация |

| | | | | |
|---|---|---|---|---|
| АУД.4 | Регистрация событий безопасности | + | Функционал KOMRAD Enterprise SIEM<br>Разделы: «Администрирование-Настройка коллекторов» «Поиск по событиям»<br>Возможность сбора событий информационной безопасности.<br>Возможность просмотра определенных событий среди всех событий, собранных в системе. | Онлайн документация |
| АУД.6 | Защита информации о событиях безопасности | + | Обеспечивается защита информации о событиях безопасности с применением мер защиты от неправомерного доступа, уничтожения или модифицирования | Онлайн документация |
| АУД.7 | Мониторинг безопасности | + | KOMRAD SIEM формирует актуальную сводную информацию о событиях, инцидентах, уязвимостях активов. Также в продукте реализован мониторинг состояния источников событий ИБ | Онлайн документация |

| | | | | |
|---|---|---|---|---|
| АУД.8 | Реагирование на сбои при регистрации событий безопасности | + | Реализованы методом вывода ошибок о сборе событий, уведомлениями о заканчивающемся месте на диске или недоступности компонента | Онлайн документация |
| АУД.9 | Анализ действий отдельных пользователей | + | Возможность просмотра и выгрузки отчётов по действиям отдельных пользователей для последующего анализа | Онлайн документация |
| ИНЦ.1 | Выявление компьютерных инцидентов | + | Функционал KOMRAD Enterprise SIEM<br>Раздел «Инциденты»<br>При приходе события информационной безопасности, подходящего под директиву корреляции создается инцидент информационной безопасности | Онлайн документация |
| ИНЦ.2 | Информирование о компьютерных инцидентах | + | Функционал KOMRAD Enterprise SIEM<br>Разделы: «Администрирование-Уведомления»<br>«Инциденты-Директивы корреляции» | Онлайн документация |

| | | | | |
|---|---|---|---|---|
| | | | «Администрирование-ГосСОПКА» При выявлении инцидента информационной безопасности может быть сформировано почтовое уведомление, сообщение в формате CEF. Также может быть отправлено уведомление в ГосСОПКА | |
| ИНЦ.3 | Анализ компьютерных инцидентов | + | Функционал KOMRAD Enterprise SIEM При выявлении инцидента информационной безопасности создается карточка инцидента, в которую помещены все события в рамках данного инцидента | Онлайн документация |
| ИНЦ.6 | Хранение и защита информации о компьютерных инцидентах | + | Функционал KOMRAD Enterprise SIEM хранит в базе данных PostgreSQL, защитные механизмы реализуются настройками PostgreSQL | Онлайн документация |