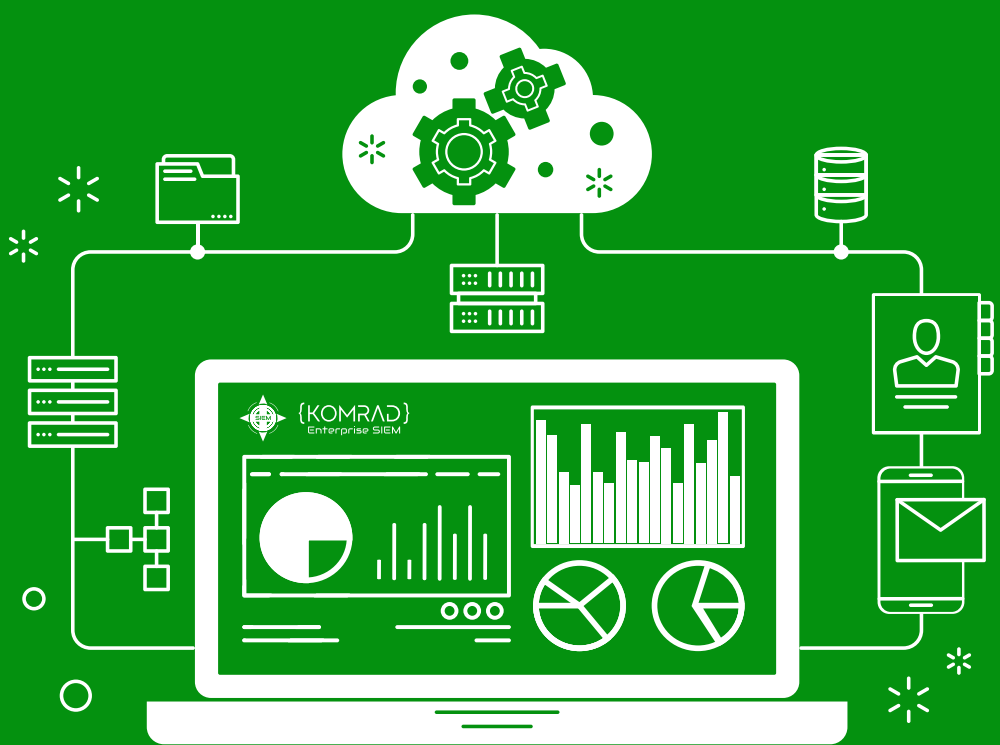
Эшелон
комплексная безопасность



{KOMRAD}
Enterprise SIEM

Система управления событиями ИБ

{KOMRAD}
Enterprise SIEM

Выполнение требований

KOMRAD Enterprise SIEM реализует следующие меры ИБ:

Приказы ФСТЭК России
№ 17
№ 21
№ 31
№ 235
№ 239

- сбор, запись и хранение информации о событиях безопасности;
- обнаружение, идентификация и регистрация инцидентов;
- информирование об инцидентах и реагирование;
- хранение событий в течение необходимого срока;
- управление активами;
- просмотр и анализ информации о действиях пользователей;
- передача инцидентов в ГосСОПКА.

Лицензиаты ФСТЭК России применяют KOMRAD Enterprise SIEM для оказания услуг по мониторингу ИБ в качестве:

- средства управления событиями безопасности информации;
- средства управления инцидентами ИБ.

Сертификаты

Сертификат **ФСТЭК России №3498**, подтверждающий выполнение требований:

- руководящего документа «Требования по безопасности информации, устанавливающие уровни доверия к средствам технической защиты информации и средствам обеспечения безопасности информационных технологий (ФСТЭК России 2020) – по 4 уровню доверия и технических условиях НПЕШ.60010-04ТУ при выполнении указаний по эксплуатации приведенных в формуляре НПЕШ.60010-04 30.

Сертификат **Минобороны России** №6498, подтверждающий выполнение требований:

- руководящего документа «Защита от несанкционированного доступа к информации. Часть 1. Программное обеспечение средств защиты информации. Классификация по уровню контроля отсутствия недекларированных возможностей» (Гостехкомиссия России, 1999) – **по 2 уровню** контроля;
- по соответствию реальных и декларируемых в документации функциональных возможностей.

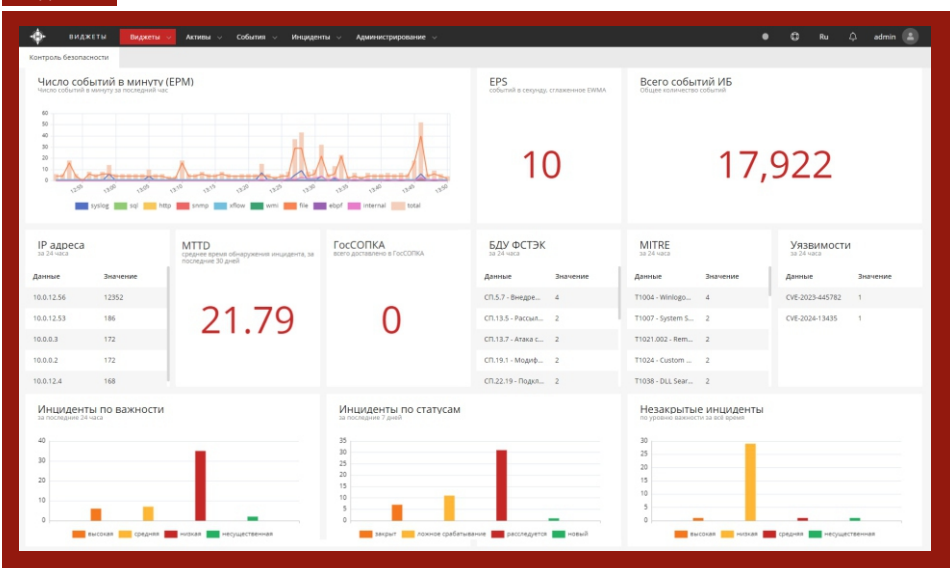
Реестр российского ПО

KOMRAD Enterprise SIEM включен в **единый реестр российских программ** для электронных вычислительных машин и баз данных. Приказ Минкомсвязи России от 18.03.2016 г. №112.

KOMRAD Enterprise SIEM – гибкая и масштабируемая система централизованного управления событиями информационной безопасности, поддерживающая широкий спектр источников событий.

KOMRAD Enterprise SIEM позволяет осуществлять централизованный сбор событий информационной безопасности, выявлять инциденты и оперативно на них реагировать. Применение комплекса позволяет эффективно выполнять требования, предъявляемые регуляторами к защите персональных данных, к обеспечению безопасности государственных информационных систем и контролю критической информационной инфраструктуры предприятия. KOMRAD Enterprise SIEM позволяет отправлять данные о событиях и инцидентах во внешние системы (например, ГосСОПКА).

Виджеты



Ключевые технические характеристики:

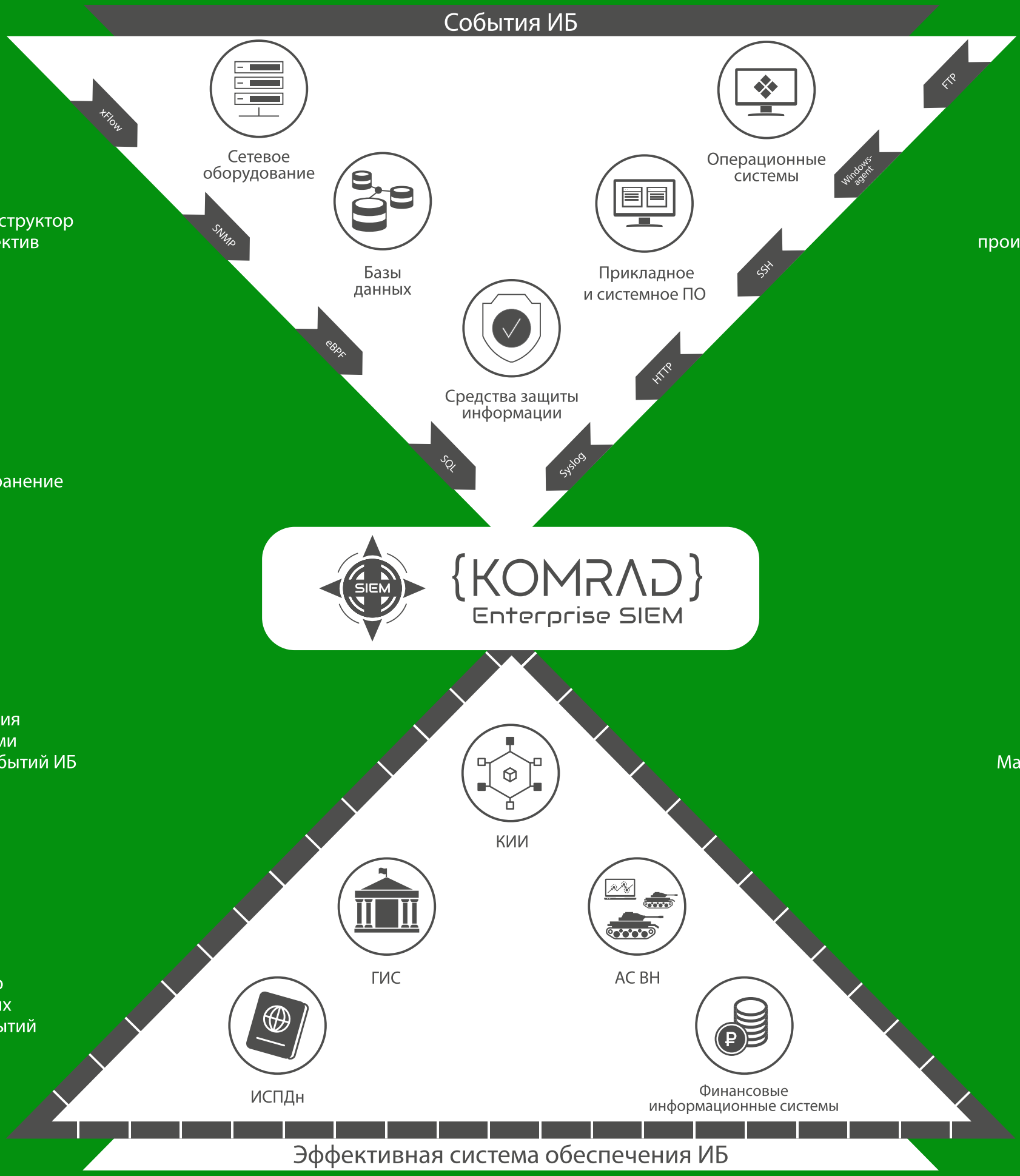
- сбор событий с помощью Syslog, SNMP, SQL, FTP, SSH, xFlow, HTTP, eBPF;
- автоматическая нормализация событий в форматах CEF, RFC 5424 (Syslog Protocol), RFC 3164 (BSD Syslog Protocol), EVTX, XML, JSON;
- возможность разбора событий в произвольном формате с помощью регулярных выражений для подключения нестандартных источников событий информационной безопасности;
- возможность использования готовых паттернов Grok для нормализации событий информационной безопасности с помощью Regex;
- поддержка Elastic Common Schema и схемы событий ArcSight;
- возможность создавать собственные поля событий;
- широкий спектр поддерживаемых отечественных СЗИ;
- встроенные виджеты с возможностью редактирования, а также модуль Grafana для визуализации данных;
- горячее и холодное хранение событий на основе ClickHouse;
- визуальный конструктор правил фильтрации и корреляции событий;
- возможность создания сложных правил фильтрации событий на языке Lua;
- возможность установки коллекторов на удалённые хосты через веб-интерфейс; базовый пакет правил корреляции под Windows и Linux (auditd);
- регистрация инцидентов информационной безопасности;
- возможность интеграции со внешними системами: поддержка API, gRPC, HTTP, ГосСОПКА, передачи карточки инцидента в формате CEF, возможность составления иерархии;
- расширенный пакет правил корреляции (более 700 правил);
- поддержка следующих сертифицированных сред функционирования: ОС Astra Linux Special Edition 1.7, 1.8, РЕД ОС 8, Альт Рабочая станция 10, ОСОН «ОСнова», версия 2;
- различные возможности отправки уведомлений (Telegram, E-mail, Kafka, Webhook;
- автоматическая установка на один узел;
- интеграция с LDAP-сервером.

Визуальный конструктор запросов и директив корреляции

Экономичное хранение

Гибкая интеграция с нестандартными источниками событий ИБ

Широкий спектр поддерживаемых источников событий



Высокая производительность

Визуальный анализ данных

Масштабирование

Оперативное оповещение об инциденте

Функциональные возможности

Лог-менеджмент:

- высокопроизводительный сбор событий информационной безопасности в инфраструктуре масштаба предприятия;
- нормализация – приведение событий к единому формату;
- визуальный конструктор правил фильтрации событий;
- возможность разработки кастомизированных правил фильтрации на языке Lua;
- защита информации от потери;
- возможность использования репутационных списков;
- предустановленные плагины: Suricata, Nginx, Auditd, DNS, eBPF, Sigma, Zeek JSON и др.

Менеджмент инцидентов:

- визуальный конструктор директив корреляции;
- агрегация инцидентов;
- уведомление о факте регистрации инцидента в интерфейсе пользователя, по электронной почте, в Telegram, в вышестоящую систему;
- выполнение пользовательских сценариев реагирования на инциденты (Python, Bash, Lua, Perl);
- история генерации инцидента показывает всю последовательность действий коррелятора при определении инцидента;
  назначение ответственного;
- возможность использования матриц атак: (БДУ ФСТЭК, MITRE ATT&CK).

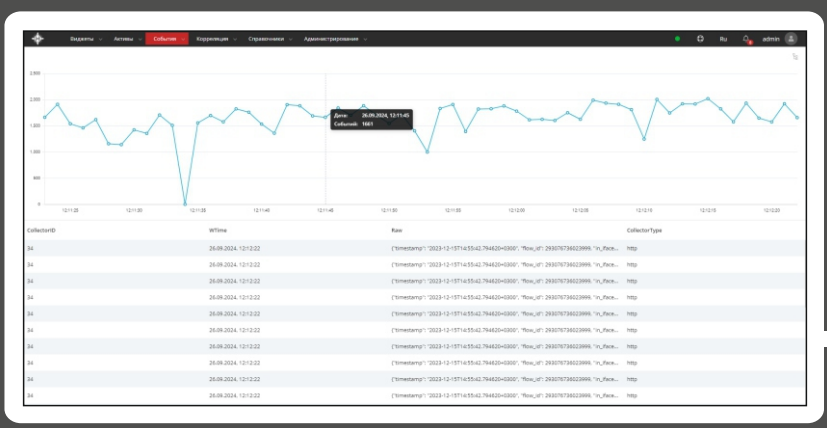
Масштабирование:

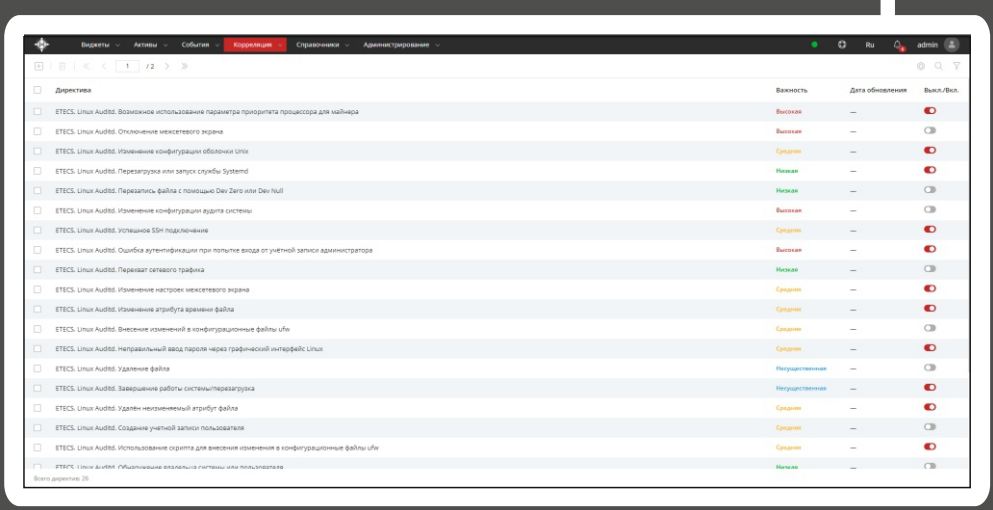
- горизонтальное: установка на отдельные узлы в сети следующих компонентов системы:
  - коллектор (сбор, фильтрация и нормализация событий);
  - процессор (обработка и регистрация событий);
  - хранилище (хранение событий);
  - коррелятор (корреляция событий);
  - сервер (управления системой).
- вертикальное: возможность передачи инцидентов из KOMRAD Enterprise SIEM нижнего уровня в KOMRAD Enterprise SIEM верхнего уровня с синхронизацией статусов инцидентов;
- возможность максимального сжатия событий с помощью СУБД ClickHouse.

Средства аналитики и визуализации, отчеты:

- отображение данных событий в виде графиков и диаграмм:
  линейные, столбчатые, круговые, радиальные и др.;
- формирование отчетов;
- модуль Grafana;
- возможность передачи всей аналитической информации в модуль Grafana.

Мониторинг событий ИБ





{KOMRAD}
Enterprise SIEM

Эшелон
комплексная безопасность

Сканер-ВС
анализ защищенности

РУБИКОН
межсетевой экран и система обнаружения вторжений

{KOMRAD}
Enterprise SIEM

ГЕНЕРАТОР
генерация и управление паролями

ПИК Эшелон
контроль целостности

ПУЛЬСАР
генератор шума

AKVS

О компании

НПО «Эшелон» специализируется на разработке сертифицированных средств защиты информации и ведет свою деятельность на основании более 50 лицензий и аттестатов аккредитации ФСТЭК России, ФСБ России и Минобороны России. Компания регулярно занимает ведущие позиции в рейтингах CNews и «Эксперт РА».

Головной офис в Москве

107023, г. Москва, ул. Электрозаводская, д. 24
+7 (495) 223-23-92 (многоканальный)
npo-echelon.ru
sales@npo-echelon.ru
vk.com/npo_echelon