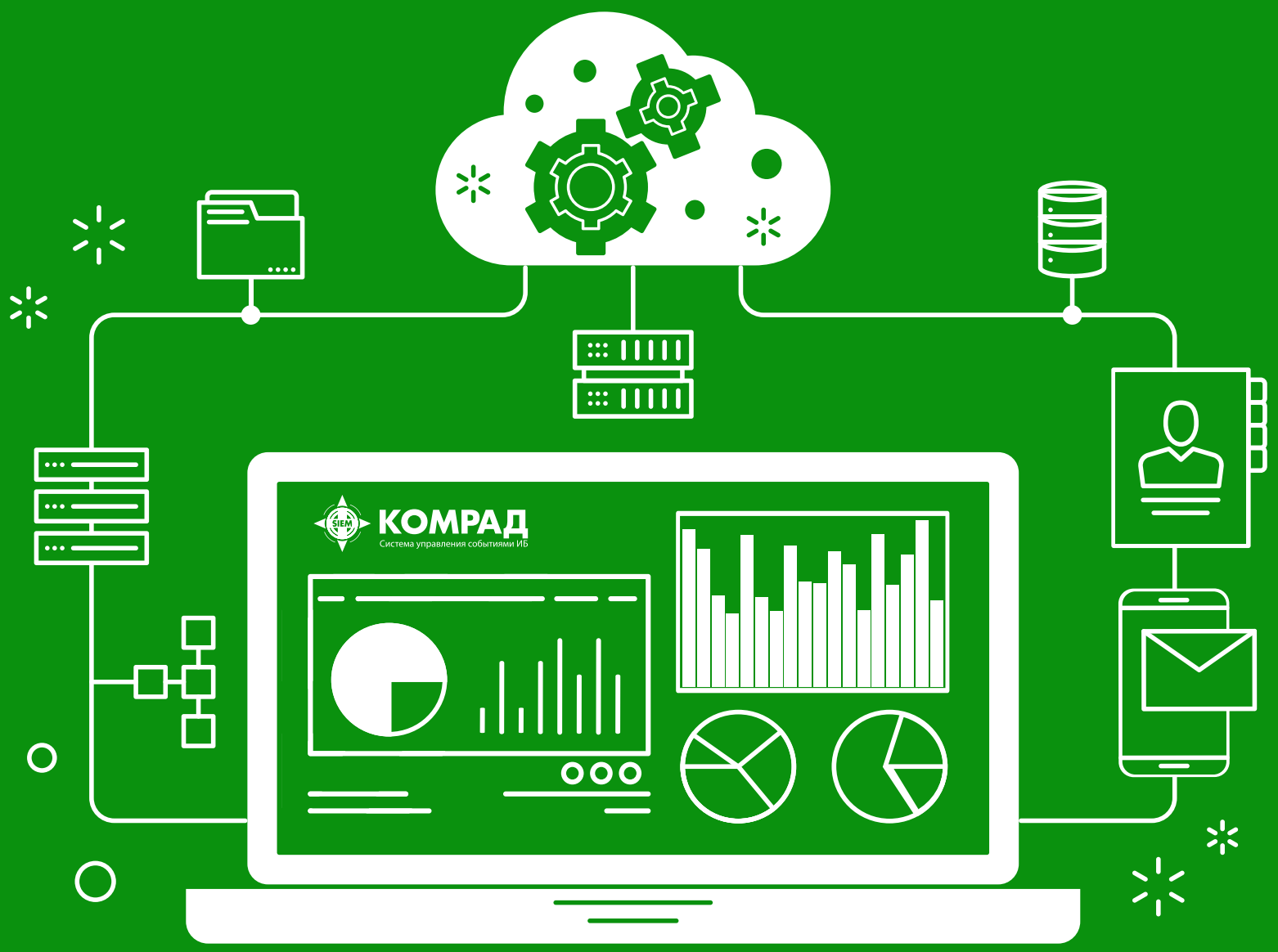
Эшелон
комплексная безопасность



КОМРАД

система управления событиями ИБ

КОМРАД
Система управления событиями ИБ

Выполнение требований

Приказ ФСТЭК России № 17			Приказ ФСТЭК России № 21			Приказ ФСТЭК России № 31		
Условное обозначение и номер меры								
РСБ.1	РСБ.5	РСБ.5 У.1	РСБ.1	РСБ.5	РСБ.5 У.1	РСБ.1	РСБ.5	РСБ.5 У.1
УПД.2			УПД.2			УПД.2		

Сертификаты

Сертификат **Минобороны России №2315**, подтверждающий выполнение требований Приказа МО РФ, в том числе:

- 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 (НДВ-2);
- по соответствию реальных и декларируемых в документации функциональных возможностей.

Сертификат **ФСТЭК России №3498**, 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 4 уровню** контроля и технических условий при выполнении указаний по эксплуатации, приведенных в формуляре НПЕШ.60010-03 30.

Реестр российского ПО

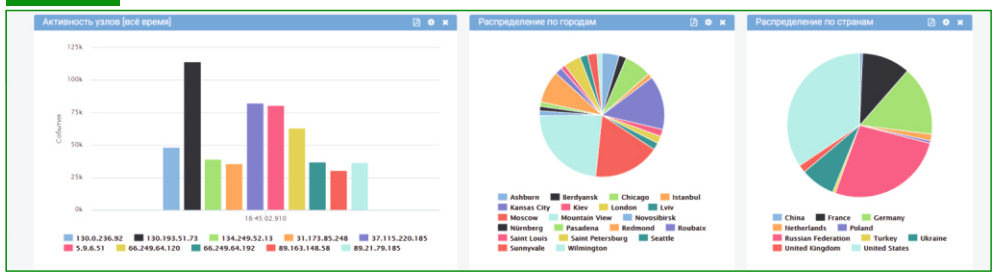
«КОМРАД» включен в **единый реестр российских программ** для электронных вычислительных машин и баз данных. Приказ Минкомсвязи России от 18.03.2016 г. №112.

КОМРАД
Система управления событиями ИБ

«КОМРАД» — гибкая и производительная система централизованного управления событиями информационной безопасности, совместимая с отечественными средствами защиты информации.

Применение «КОМРАД» позволяет осуществлять централизованный мониторинг событий ИБ, выявлять инциденты ИБ, оперативно реагировать на возникающие угрозы, выполнить требования, предъявляемые регуляторами к защите персональных данных, а также к обеспечению безопасности государственных информационных систем.

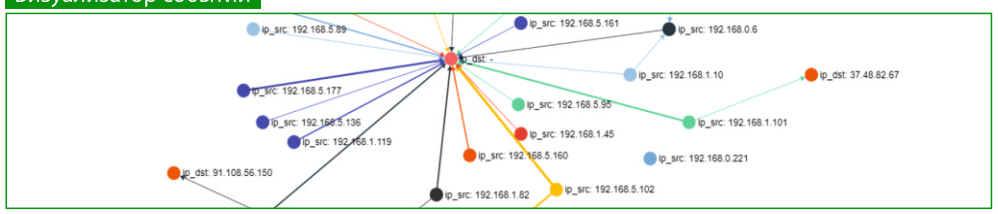
Виджеты



Ключевые особенности:

- высокая производительность;
- визуальный интерфейс для создания правил корреляции событий;
- возможность гибкой настройки и подключения нестандартных источников событий информационной безопасности;
- предустановленные виджеты;
- возможность масштабирования решения и создания системы мониторинга информационной безопасности любого масштаба;
- широкий спектр поддерживаемых отечественных СЗИ;
- оперативное оповещение и реагирование на внутренние и внешние угрозы безопасности автоматизированной системы;
- контроль выполнения заданных требований по безопасности информации, сбор статистики и построение отчетов по защищенности;
- предустановленные правила корреляции;
- настраиваемые визуальные показатели состояния информационной системы для любого уровня сотрудников организации;
- интуитивно понятный интерфейс пользователя.

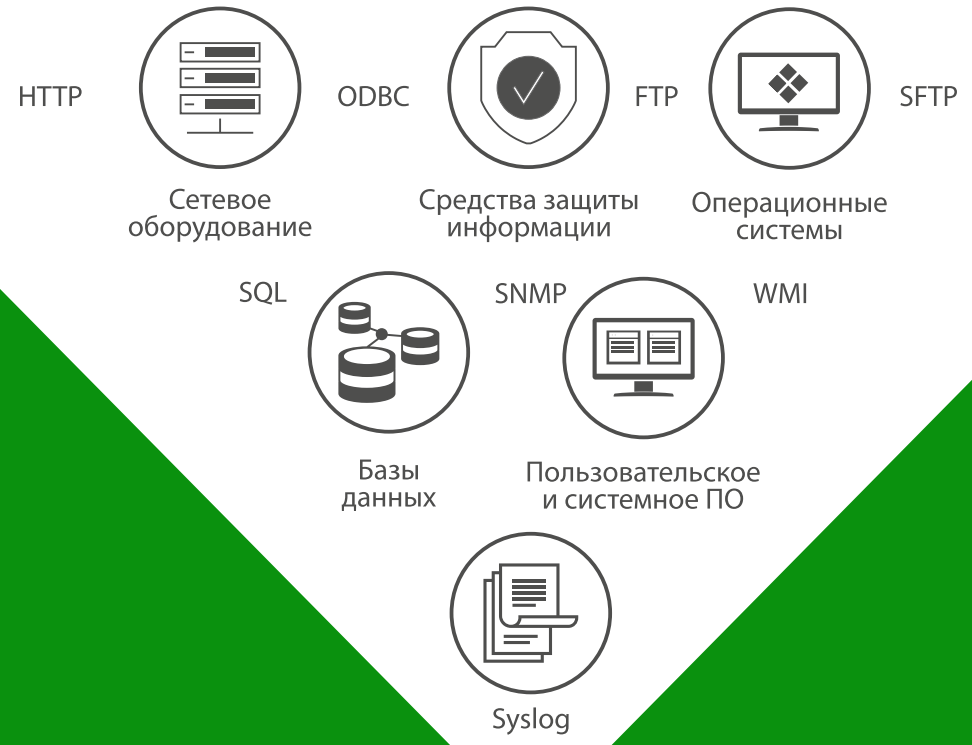
Визуализатор событий



Технические характеристики:

- сбор событий по протоколам Syslog (в том числе в формате CEF), Syslog-ng, SNMPv2, SNMPv3, HTTP, SQL, ODBC, WMI, FTP, SFTP, SSH;
- производительность: 10 000 EPS на серверной платформе со следующими характеристиками: 2 CPU Intel Xeon E5 2640v4, ОЗУ: 64 Гбайт, HDD: 2 Тбайт.

События ИБ



визуальный конструктор запросов и директив корреляции

высокая производительность

гибкая интеграция с нестандартными источниками событий ИБ

широкий спектр поддерживаемых источников событий

ролевая модель управления доступом

визуальный анализ данных

удобный пользовательский интерфейс

оперативное оповещение об инциденте

КОМРАД

SIEM

Система управления событиями ИБ

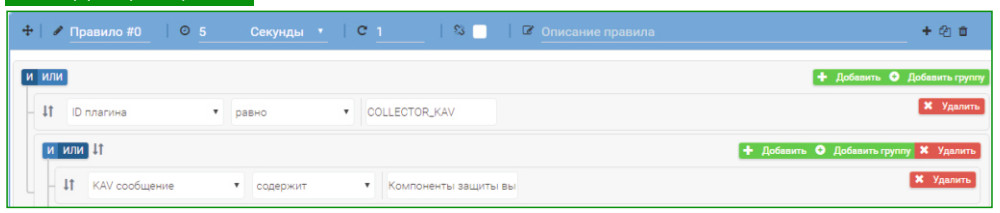
Эффективная система обеспечения ИБ

Функциональные возможности

Лог-менеджмент:

- **высокопроизводительный сбор событий** позволяет осуществлять централизованный сбор событий в инфраструктуре масштаба предприятия;
- **нормализация** — приведение журналов всех источников к единому формату для упрощения их анализа;
- **хранение событий** в исходном («сыром») и нормализованном виде; возможно использование исходных событий при проведении расследований инцидентов ИБ;
- **мониторинг событий в реальном времени** позволяет анализировать события, как только они поступили в систему;
- **быстрый полнотекстовый поиск** позволяет найти нужное событие среди миллионов похожих практически мгновенно;
- **фильтрация событий** осуществляется при помощи удобного конструктора запросов к базе событий;
- **визуализация событий** — представление анализируемых данных в виде графиков и диаграмм (линейные, столбчатые, круговые, радиальные и др.);
- **визуальное задание границ отображения данных** — диаграмма событий позволяет задать точный временной интервал для отображения событий;
- **сохранение запросов** — любой запрос к базе событий можно сохранить в системе для быстрого обращения к нему в повседневной работе;
- **экспорт** — любую выборку событий можно сохранить в форматах PDF и CSV.

Конструктор запросов



Корреляция событий:

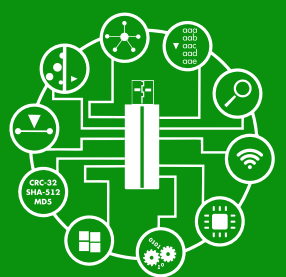
- **формирование инцидентов** — при обнаружении цепочек критичных событий безопасности формируется инцидент ИБ;
- **наглядные директивы корреляции** — интуитивно понятный графический конструктор директив делает процесс создания директивы легким и доступным;
- **многоуровневая корреляция** — возможность задания неограниченного количества уровней и правил в конструкторе директив;
- **поддержка методики шаблонов поведения** — пакеты директив корреляции отражают возможную цепь событий (аномалий), которая соответствует модели реальной атаки;
- **настраиваемая система оповещений** — возможность оповещения об инцидентах различными способами (всплывающие уведомления, электронная почта, выполнение пользовательских сценариев и др.);
- **управление инцидентами** — автоматическое назначение группы ответственных за инцидент лиц, система статусов и меток, настройка видимости инцидентов.

SIEM

КОМРАД

Система управления событиями ИБ

Эшелон
комплексная безопасность



Сканер-ВС
анализ защищенности

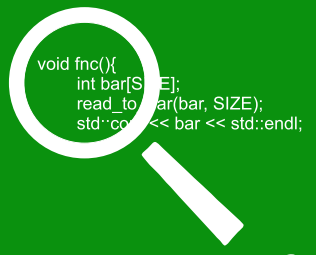
РУБИКОН
межсетевой экран и система обнаружения вторжений

КОМРАД
Система управления событиями ИБ

МДЗ-Эшелон
модуль доверенной загрузки

ГЕНЕРАТОР
генерация и управление паролями

ПИК Эшелон
контроль целостности



АК-ВС²
анализ безопасности кода

AppChecker
анализ безопасности приложений

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».

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