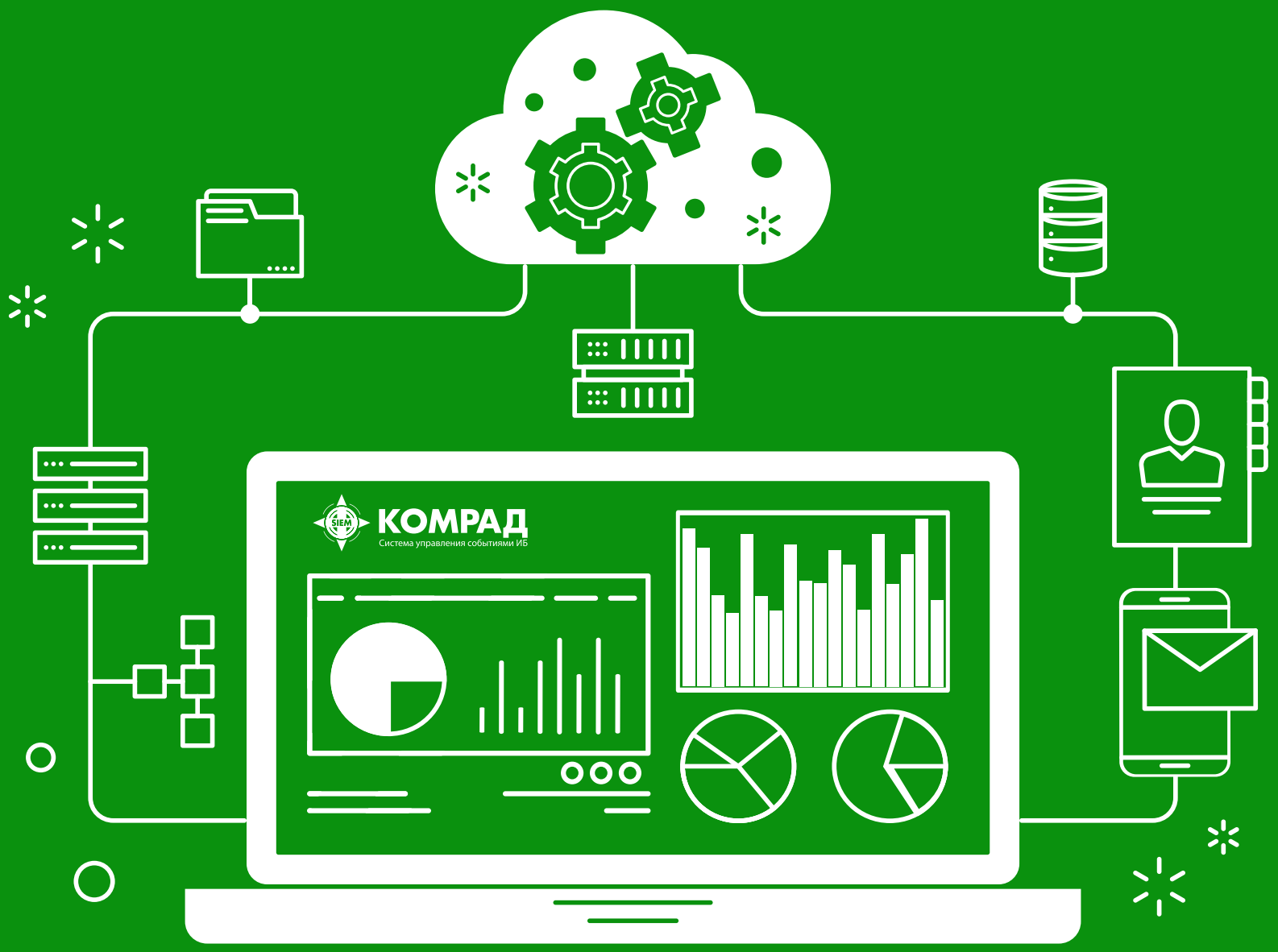
Эшелон
комплексная безопасность



КОМРАД

система управления событиями ИБ

КОМРАД

Система управления событиями ИБ

Выполнение требований

Приказы ФСТЭК России
№ 17
№ 21
№ 31

КОМРАД реализует следующие меры ИБ:

- сбор, запись и хранение информации о событиях безопасности;
- мониторинг и реагирование на события;
- обнаружение, идентификация и регистрация инцидентов;
- информирование об инцидентах;
- хранение событий в течении необходимого срока;
- просмотр и анализ информации о действиях пользователей.

Лицензиаты ФСТЭК России применяют КОМРАД 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 «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 на изделие.

Сертификат **Минобороны России №3899**, 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.

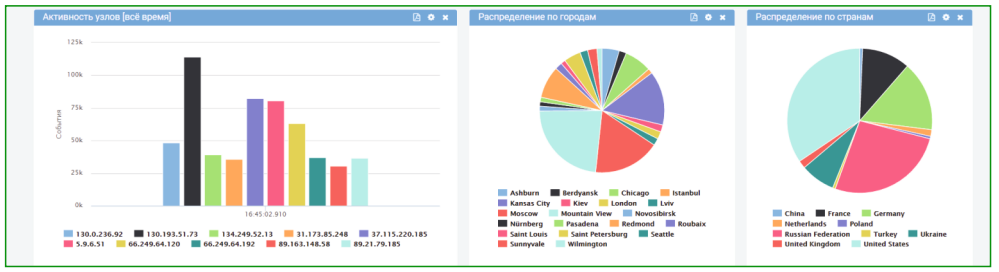
Реестр российского ПО

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

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

Применение КОМРАДа позволяет осуществлять централизованный мониторинг событий ИБ, выявлять и оперативно реагировать на инциденты ИБ, выполнять требования, предъявляемые регуляторами к защите персональных данных, а также к обеспечению безопасности государственных информационных систем и контролю критической информационной инфраструктуры предприятия. «КОМРАД» позволяет отправлять данные о событиях и инцидентах ИБ во внешние системы (например, ГосСОПКА).

Виджеты



Ключевые особенности:

- 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.

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, Netflow v5, v7;
- производительность: 10 000 EPS на серверной платформе со следующими характеристиками: 2 CPU Intel Xeon E5 2640v4, ОЗУ: 64 Гбайт, HDD: 2 Тбайт.

визуальный конструктор запросов и директив корреляции

высокая производительность

гибкая интеграция с нестандартными источниками событий ИБ

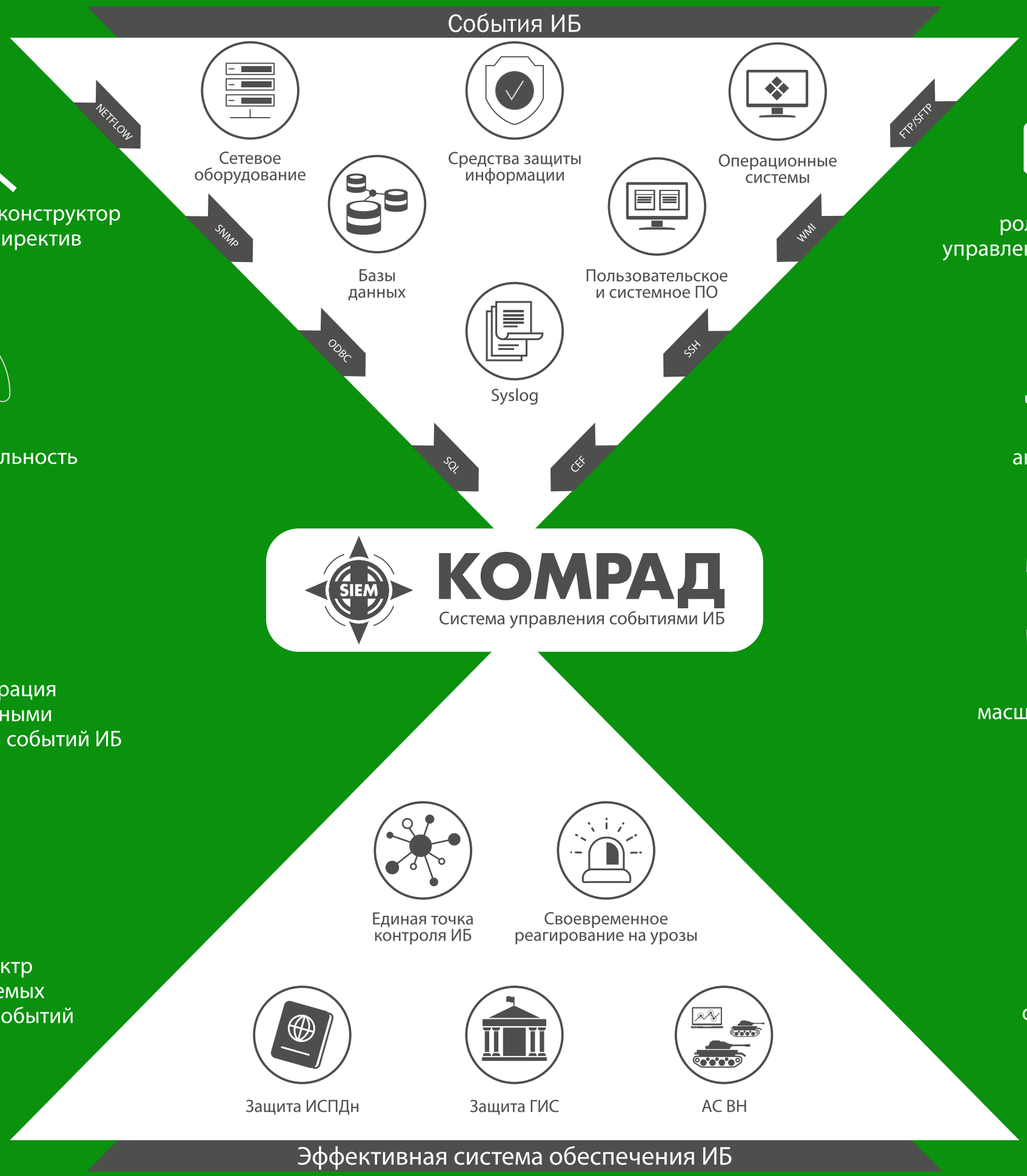
широкий спектр поддерживаемых источников событий

ролевая модель управления доступом

визуальный анализ данных

масштабирование

оперативное оповещение об инциденте

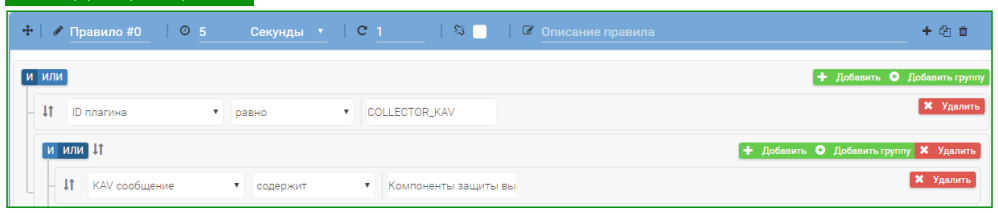


Функциональные возможности

Лог-менеджмент:

- **высокопроизводительный сбор событий** в инфраструктуре масштаба предприятия;
- **нормализация** — приведение журналов всех источников к единому формату для упрощения 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 сразу при поступлении 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



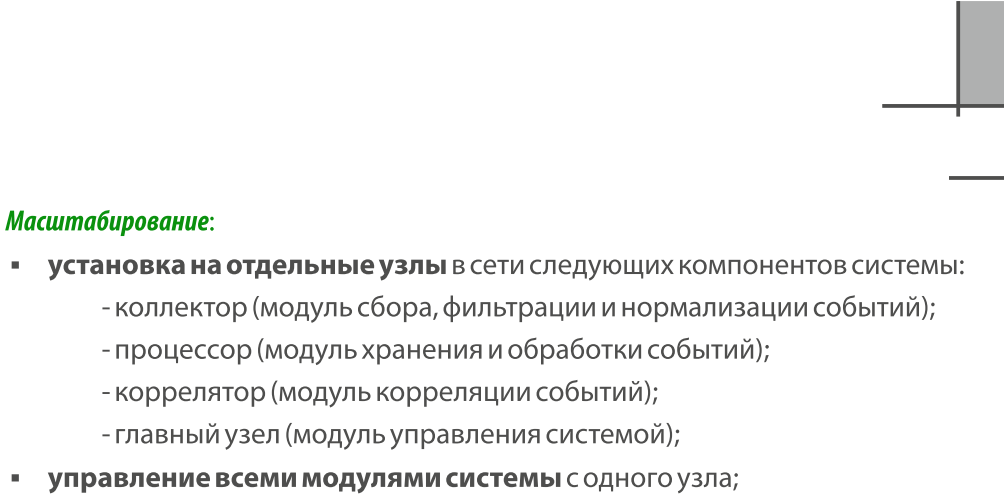
Корреляция событий:

- **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.

Масштабирование:

- **установка на отдельные узлы** в сети следующих компонентов системы:
  - коллектор (модуль сбора, фильтрации и нормализации событий);
  - процессор (модуль хранения и обработки событий);
  - коррелятор (модуль корреляции событий);
  - главный узел (модуль управления системой);
- **управление всеми модулями системы** с одного узла;
- **обеспечение буферизации событий** информационной безопасности при отправке из модуля сбора в модуль хранения и обработки событий;
- **подключение нескольких модулей корреляции** к одному хранилищу событий;
- **подключение нескольких модулей хранения** и обработки событий к одному модулю корреляции;
- **подключение к модулю управления нескольких модулей** хранения и обработки событий;
- **сквозной поиск событий** в нескольких модулях хранения и обработки событий;
- **подключение нескольких модулей сбора, фильтрации и нормализации** сообщений к одному модулю хранения и обработки событий.

Масштабирование компонентов



Средства аналитики и визуализации, отчеты:

- **отображение событий в виде графиков и диаграмм**: линейные, столбчатые, круговые, радиальные и др.;
- **отображение данных по инцидентам** в графическом формате;
- **конфигурирование и редактирование** диаграмм;
- **создание и редактирование отдельных панелей** с диаграммами;
- **создание и редактирование шаблонов** диаграмм;
- **переход к выборке хранимых событий** нажатием на диаграмму;
- **формирование отчётов по фильтрам** (системным и пользовательским);
- **формирование отчётов из состава имеющихся шаблонов** в системе: по событиям и инцидентам;
- **наличие оперативных графиков** (дашбордов) по событиям и инцидентам;
- **экспорт данных** и создание отчетов в формате PDF, CSV, HTML.

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».

Головной офис в Москве

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

Офис в Санкт-Петербурге

199178, г. Санкт-Петербург, наб. реки Смоленки, д. 14
+7 (812) 635-89-04
www.npo-echelon.ru/spb/
mail@nwechelon.ru