

УНИКАЛЬНАЯ ТЕХНОЛОГИЯ СБОРА СОБЫТИЙ

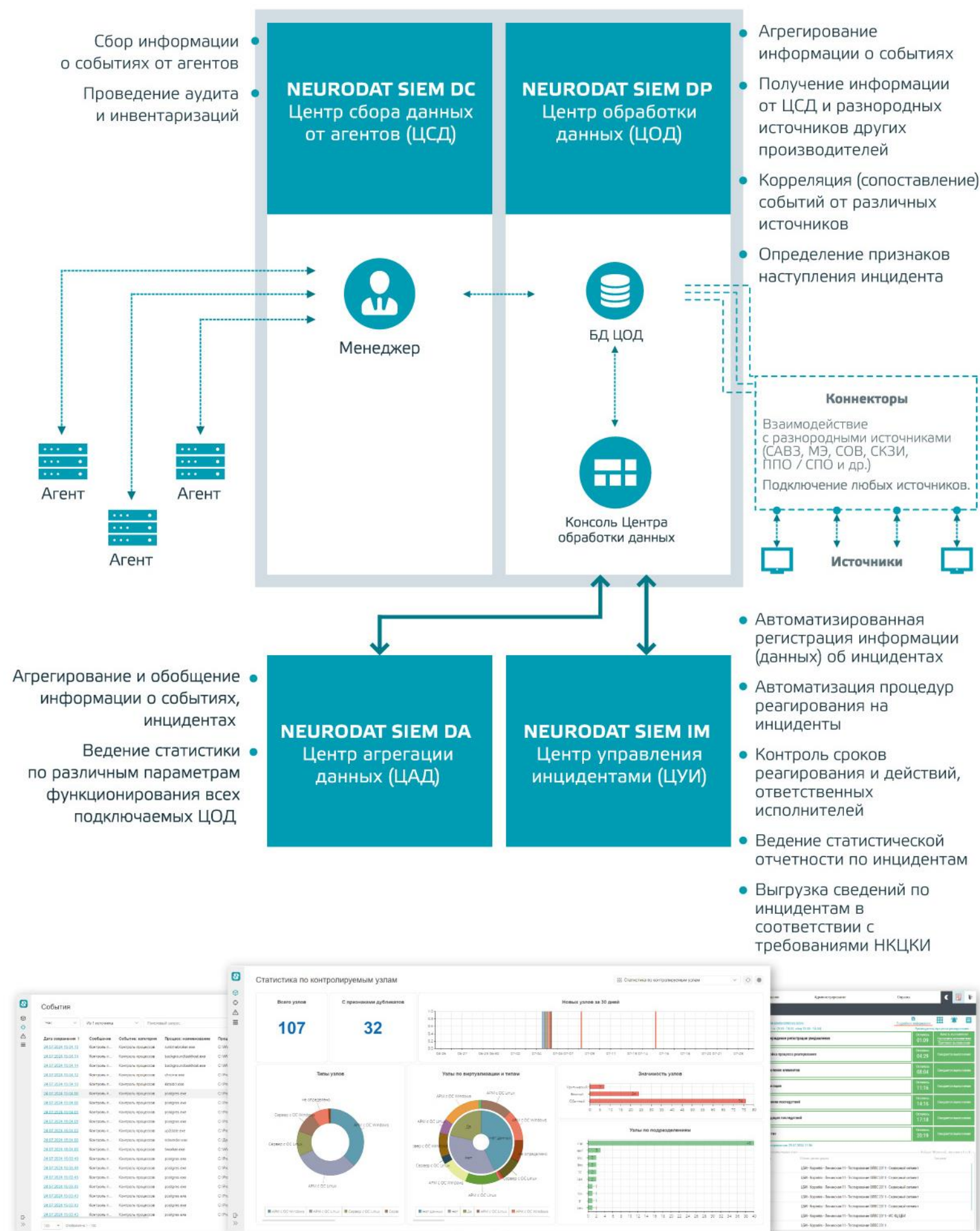
NEURODAT SIEM осуществляет сбор событий с компьютеров и серверов вычислительной сети на основе использования агентской технологии, реализующей следующие функции:

- сбор информации о составе и выполненных настройках (инвентаризации с возможностью формирования соответствующих формуляров)
- мониторинг действий пользователей в режиме времени, близком к реальному
- контроль соответствия заданным конфигурациям безопасности
- контроль установленных обновлений ПО

СНИЖЕНИЕ ОПЕРАЦИОННЫХ ЗАТРАТ ЗА СЧЕТ АВТОМАТИЗАЦИИ

- выполнения регламентов реагирования на инциденты
- выдачи рекомендаций по реагированию на инцидент на основе действий, ранее выполненных при реагировании на аналогичные инциденты
- группировки одинаковых инцидентов для реагирования в рамках одного процесса
- назначения ответственных исполнителей по реагированию на инцидент

КОМПОНЕНТЫ NEURODAT SIEM



ОСНОВНЫЕ ПРЕИМУЩЕСТВА

- ИМПОРТОЗАМЕЩЕНИЕ** - независимость от импортных технологий. Продукт внесен в Реестр отечественного ПО и имеет сертификат ФСТЭК России
- РАСШИРЕННАЯ ПОДДЕРЖКА** - возможность доработки в соответствии с потребностями заказчика
- ВСТРОЕННАЯ ЭКСПЕРТИЗА** - значительное количество предустановленных правил регистрации инцидентов и помощь заказчикам при разработке собственных правил
- НЕСТАНДАРТНЫЕ ИСТОЧНИКИ** - подключение нестандартных источников событий через разработку специализированных коннекторов
- АГЕНТЫ МОНИТОРИНГА** - расширенный сбор информации с АРМ и серверов в режиме реального времени. Централизованное управление агентами из единого интерфейса
- УПРАВЛЕНИЕ ИНЦИДЕНТАМИ** - встроенный модуль управления инцидентами для построения процесса реагирования любой сложности
- КОНТРОЛЬ ИНФРАСТРУКТУРЫ** - подробная инвентаризация узлов сети, контроль изменений, сводные отчеты по программно-аппаратному обеспечению
- ЭКОНОМИЯ РЕСУРСОВ** - невысокие аппаратные требования при внедрении системы, простота обслуживания

ФУНКЦИОНАЛЬНЫЕ ВОЗМОЖНОСТИ

- автоматизированный сбор, анализ и обработка событий безопасности (журналы СЗИ, баз данных, ОС, информация о процессах, подключаемых устройствах, установке ПО, службах и т.п.)
- централизованное долговременное хранение информации о событиях безопасности
- контроль работоспособности систем – поставщиков информации для NEURODAT SIEM
- инвентаризация узлов сети как с использованием агентов, так и безагентным способом

- автоматическое выявление инцидентов ИБ на основе анализа и корреляции событий, поступающих от различных источников
- автоматизация процесса реагирования на различные типы инцидентов
- предоставление рекомендаций по реагированию на инциденты
- передача информации об инцидентах в специализированное средство обмена данными с НКЦКИ
- визуализация статистики по событиям безопасности, узлам сети, зарегистрированным инцидентам

СЕРТИФИКАЦИЯ ФСТЭК РОССИИ ПО ТРЕБОВАНИЯМ БЕЗОПАСНОСТИ ИНФОРМАЦИИ
 Сертификат соответствия № 4375 требованиям по 4 уровню доверия и Задания по безопасности

NEURODAT – ЗАРЕГИСТРИРОВАННАЯ ТОРГОВАЯ МАРКА ООО «ЦБИ»
 № 4283 от 29.03.2018 в Едином реестре российских программ для ЭВМ и БД

NEURODAT SIEM может использоваться в составе:

- значимых объектов КИИ 1 категории
- ГИС 1 класса защищенности
- АСУ производственными и технологическими процессами 1 класса защищенности
- ИСПДн при необходимости обеспечения 1 уровня защищенности персональных данных
- ИС общего пользования II класса

ООО «ЦБИ» — одна из ведущих компаний России, специализирующихся в области безопасности информационных технологий. Компания ООО «ЦБИ» существует с 1995 года.

Благодаря высокому профессионализму своих специалистов, комплексному подходу к решаемым задачам и разумной ценовой политике компания занимает прочные позиции на рынке.

Уже более 28 лет ООО «ЦБИ» успешно оказывает услуги по обеспечению информационной безопасности. За это время нашими клиентами стали тысячи организаций.

Помимо высокого качества предоставляемых услуг, наших клиентов привлекают уникальные разработки ООО «ЦБИ» в области методического и инструментального обеспечения, такого как современная система мониторинга информационной безопасности NEURODAT SIEM.

НАДЕЕМСЯ, ВЫ ЗАХОТИТЕ УБЕДИТЬСЯ В ЭТОМ ЛИЧНО, ПРИГЛАШАЕМ ЖЕЛАЮЩИХ К ПАРТНЕРСТВУ.

Адрес: 141090 Московская область, г. Королев, мкр. Юбилейный, ул. Ленинская, д 11
 Телефон: +7 (495) 580-52-18

www.cbi-info.ru neurodat@cbi-info.ru

СИСТЕМА МОНИТОРИНГА ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ NEURODAT SIEM — БОЛЬШЕ, ЧЕМ ПРОСТО SIEM

NEURODAT



СИСТЕМА МОНИТОРИНГА ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ NEURODAT SIEM ЯВЛЯЕТСЯ

- средством (системой) управления событиями безопасности информации
- средством (системой) управления инцидентами информационной безопасности
- средством контроля подключения устройств

NEURODAT SIEM

наблюдает за процессами на всех компьютерах сети и ее границе

контролирует изменения конфигурации сети

анализирует события других систем безопасности

консолидирует всю полученную информацию для обнаружения инцидентов