РАЗРАБОТЧИК

ОБЩЕСТВО С ОГРАНИЧЕННОЙ ОТВЕТСТВЕННОСТЬЮ

«М-ТЕ»

ОПИСАНИЕ

«SIEM САПР»

Листов 11

Санкт-Петербург

2018

1. СОДЕРЖАНИЕ

2. Наименование

Полное наименование: **SIEM Система Анализа и Принятия Решений**.

Краткое наименование: **SIEM САПР**.

SIEM (Security information and event management) — объединение двух терминов, обозначающих область применения ПО: SIM (Security information management) — управление информационной безопасностью и SEM (Security event management) — управление событиями безопасности. Технология SIEM (см. Рисунок 1) предназначена для анализа информации, поступающей от различных систем, таких как DLP, IDS, антивирусов, различного оборудования (ЗЭС, Cisco, FortiGate, маршрутизаторы и т.д.) и дальнейшего выявления отклонения от норм по каким-либо критериям. Как только выявлено отклонение — генерируется инцидент.

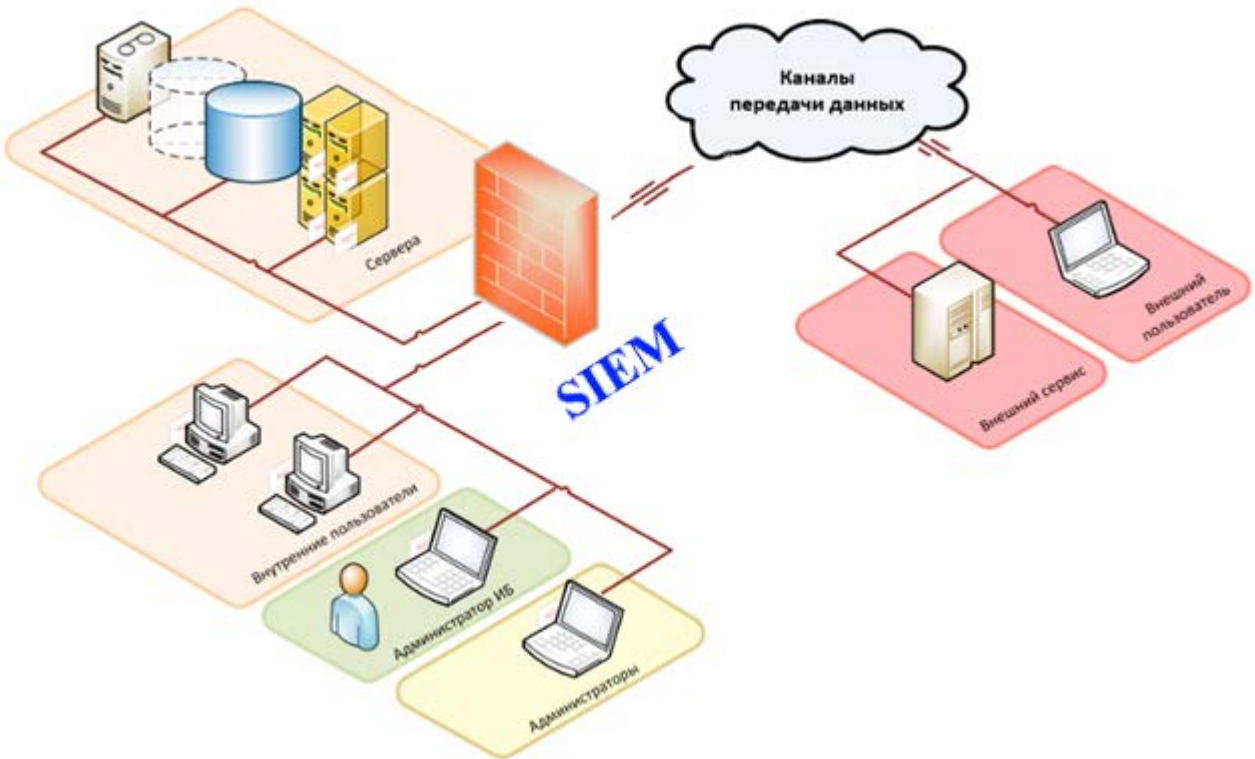

Рисунок 1

3. Описание SIEM САПР

Структуру **SIEM САПР** можно представить в виде пирамиды из 3-х уровней (см. Рисунок 1).

Рисунок 2

SIEM САПР аналитическая платформа, собирающая информацию со 2-го уровня (см. Рисунок 2).

SIEM САПР консолидирует и анализирует события информационной безопасности (далее по тексту ИБ) на основе искусственных нейронных сетей от **телекоммуникационного оборудования, сетевых устройств, программ по ИБ (такие как DLP системы, ССИ, АСУД РПДн, Антивирусы и т.д) и системного журнала Windows**.

SIEM САПР осуществляет ретроспективный анализ и обеспечивает расследование инцидентов информационной безопасности, анализируя активность в сети, а также предупреждает о возможных событиях ИБ.

SIEM САПР находится в постоянном обучении своей искусственной нейронной сети, для адаптации к изменениям в инфраструктуре или в производственных процессах (см. Рисунок 3).

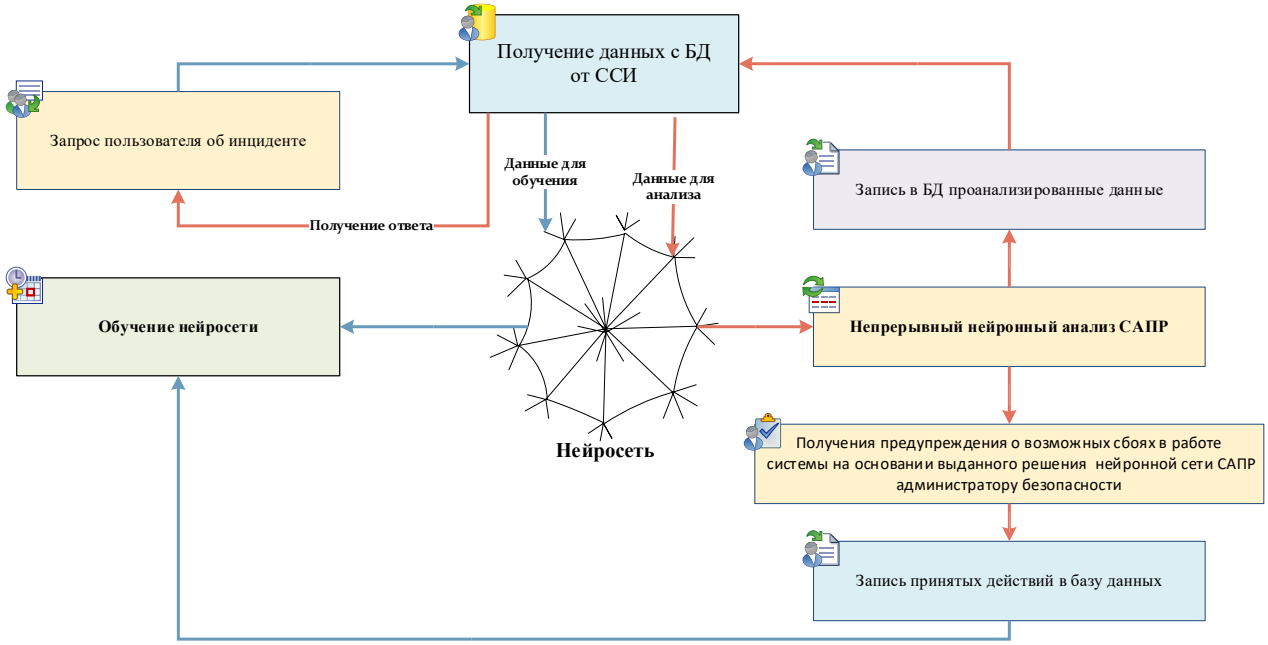

Рисунок 3

Функциональные возможности САПР:

- оперативно обнаруживает атаки и нарушения ИБ (см. Рисунок 4);

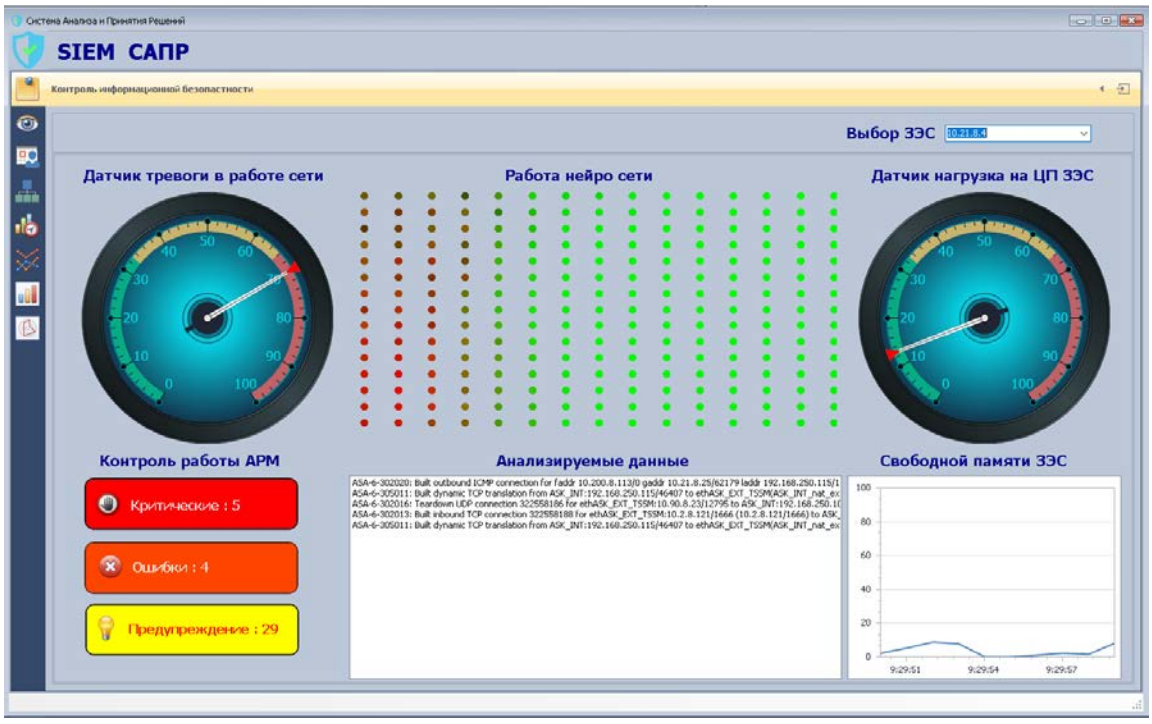

Рисунок 4

- соотносит в режиме реального времени события от разных устройств, программного обеспечения и выявляет инциденты ИБ, а также сбои в работе оборудования и ПО;
- автоматически реагирует на инциденты;
- производит нормализацию, агрегацию, фильтрацию, категоризацию, приоритезацию событий ИБ, с помощью искусственной нейронной сети;
- формирует базу знаний по инцидентам (см. Рисунок 5);

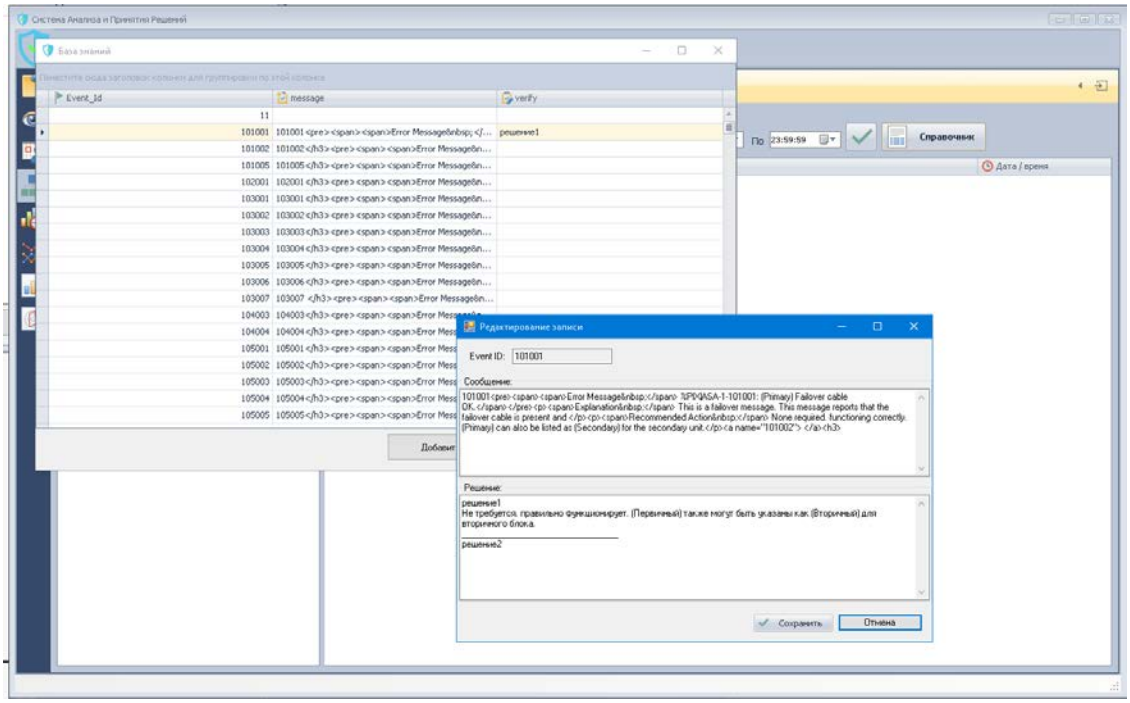

Рисунок 5

- помогает проводить обследование и расследование инцидентов;
- оценивает и предупреждает о возможных событиях ИБ по настроенным алгоритмам алертов в искусственной нейросети;
- обеспечивает централизованный просмотр событий и инцидентов ИБ путем интеграции существующего в организации ПО, телекоммуникационного оборудования, сетевых устройств и других источников в единую систему анализа данных;
- увеличивает скорость выявления, расследования и реагирования на инциденты ИБ (см. Рисунок 6, 7);

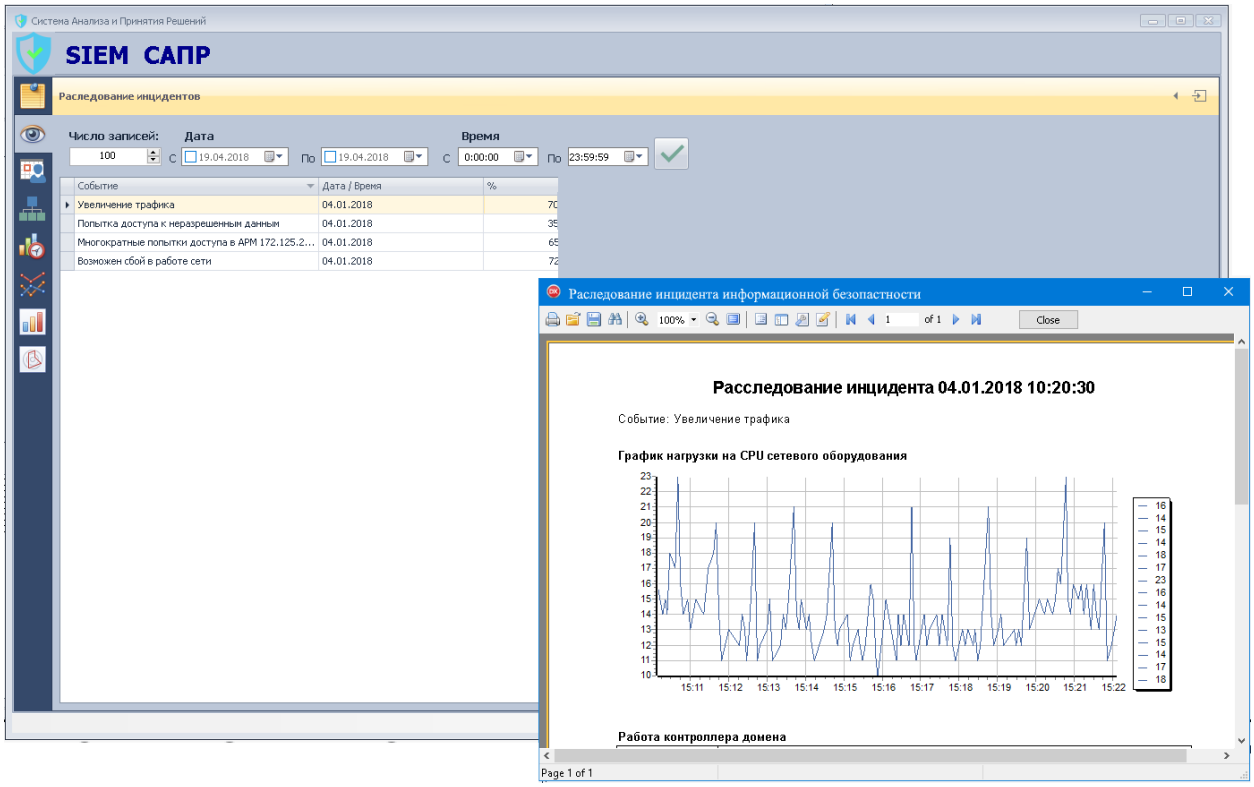

Рисунок 6

- имеет возможности фильтрации данных (см. Рисунок 7);

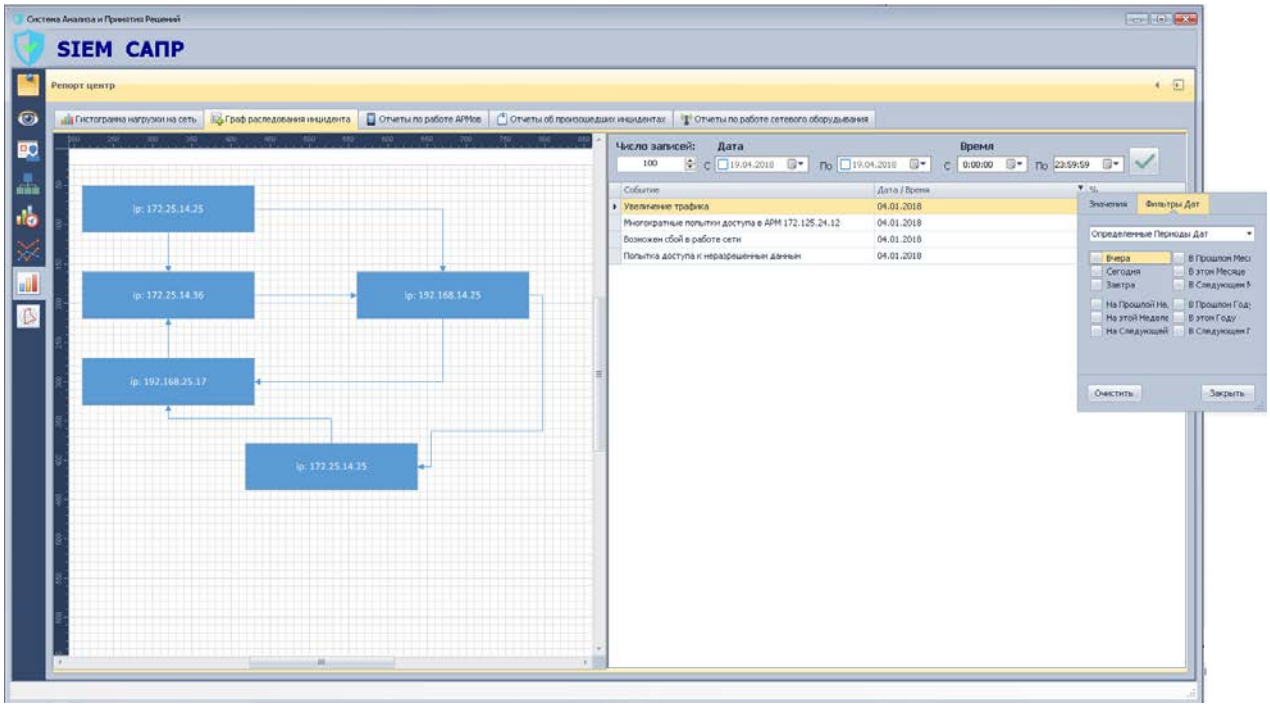

Рисунок 7

- осуществляет сбор протоколов работы контроллеров домена и АРМ(ов), а также построение графиков нагрузки (см. Рисунок 8):
  - нагрузки на центральный процессор:

- общая нагрузка на ЦП;
- нагрузка по каждому ядру в отдельности;
- отображение пяти процессов которые потребляют наибольше количество ресурсов ЦП.

– использования оперативной памяти:

- объем свободной памяти;
- объем занятой оперативной памяти;
- отображение пяти процессов которые потребляют наибольшее количество ресурсов оперативной памяти.

– нагрузки на сетевой интерфейс;

– статуса сетевого адаптера;

– нагрузки на логические диски;

– свободном месте на логических дисках;

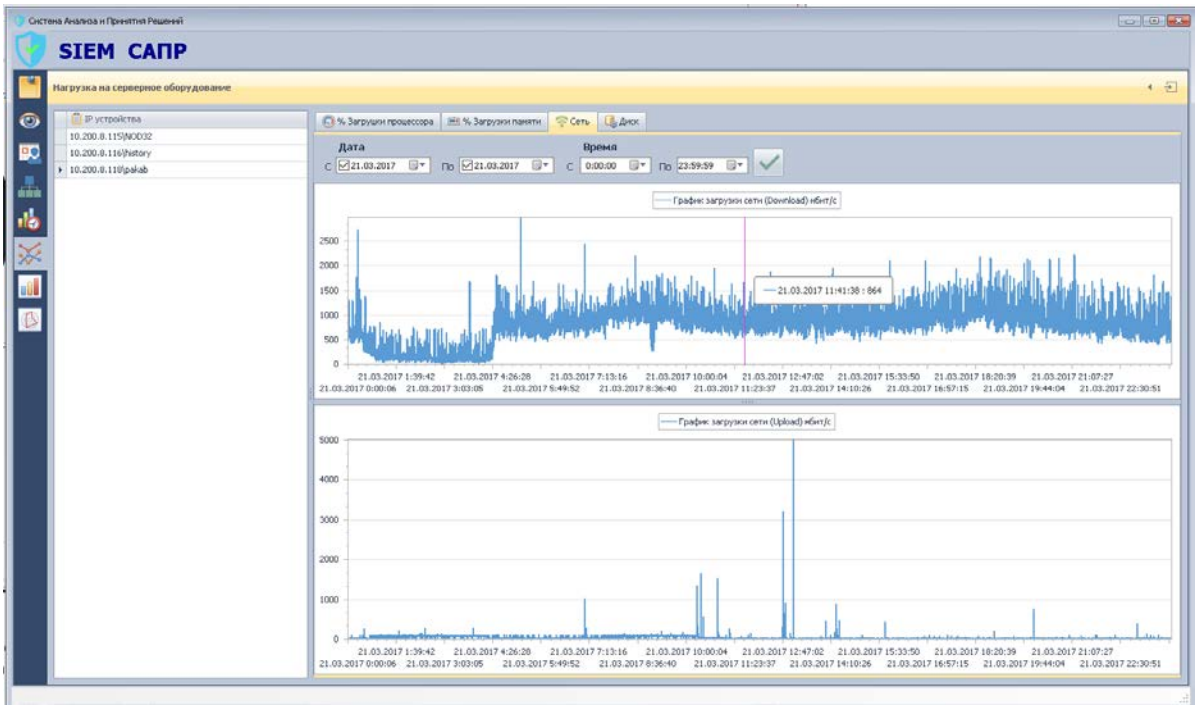

Рисунок 8

- осуществляет сбор протоколов работы с сетевых устройств с возможностью просмотра нагрузки на центральный процессор и память устройства;

- производит контроль беспроводного доступа пользователей к объектам доступа информационной системы до начала информационного взаимодействия с информационной системой;
- обеспечивает мониторинг точек беспроводного подключения устройств к информационной системе на предмет выявления несанкционированного беспроводного подключения устройств.
- отслеживает изменения в установленном/используемом программном обеспечении;
- обнаруживает ПО, запрещенное регламентом и сообщает об этом администратору безопасности;
- при запуске ПО, запрещенного регламентом, делает снимок экрана и сохранять его на сервере для дальнейшего анализа администратором безопасности;
- строит гистограмму нагрузки на сеть за весь период по дням с возможностью выбора интервалов времени, для планирования работ в определенное время (см. Рисунок 9);

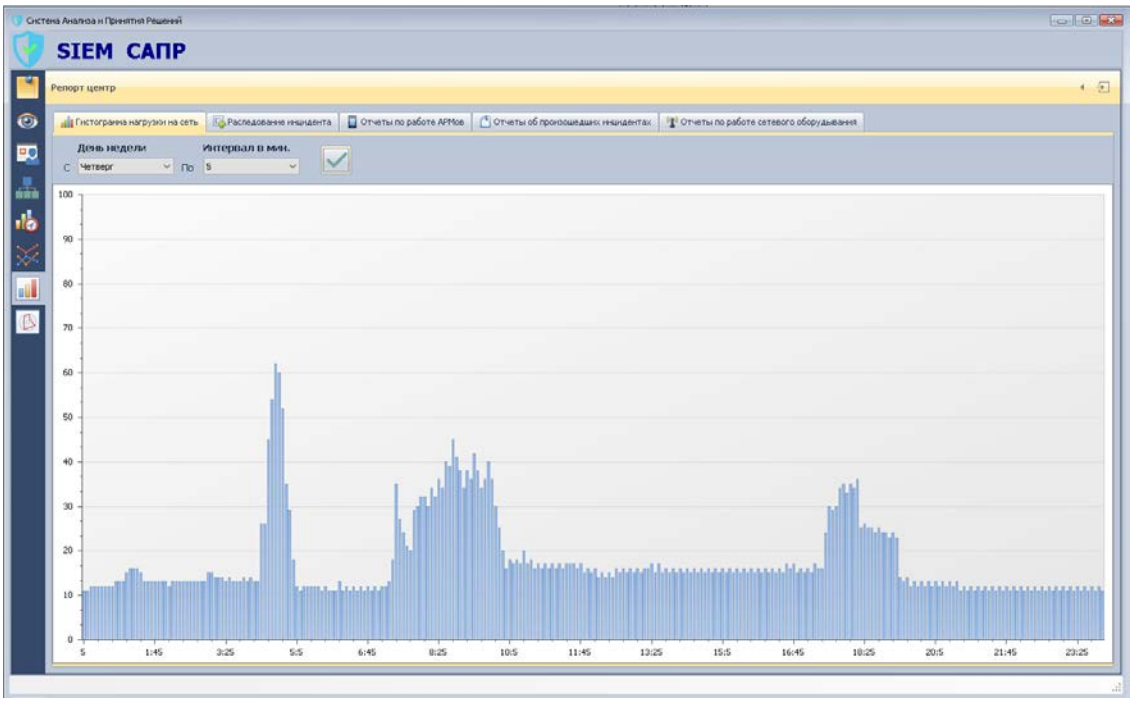

Рисунок 9

- предоставляет возможность увидеть работу нейронной сети в реальном времени и в обученном состоянии (см. Рисунок 4, 10);

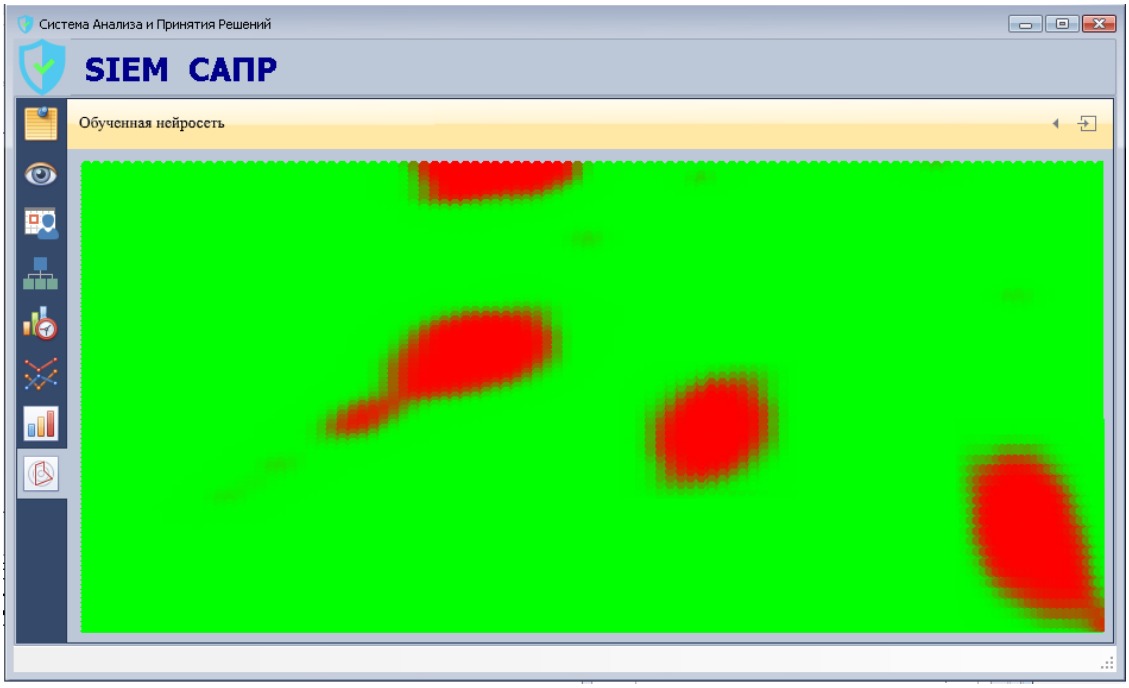

Рисунок 10

- осуществляет корреляцию и обработку событий ИБ по правилам обученной искусственной нейронной сети;
- предоставляет возможность построения всевозможных отчетов в репорт центре таких как:
  - нагрузки на центральный процессор, память, дисковое пространство АРМ(ов);
  - отчеты об произошедших инцидентах:
    - нарушение в работе сети;
    - нарушение безопасности;
    - несанкционированном доступе;
    - о неоднократных попытках доступа к АРМ(ам);
    - сбоях в работе серверов;
    - сбоях в работе программного обеспечения;
    - и т.д.
  - нагрузке в работе сетевого оборудования;
  - расследование инцидентов.

4. Результаты внедрения SIEM САПР

- внедрение единого стандарта на сбор, хранение и обработку событий ИБ в обслуживаемой корпоративной сети Заказчика;
- контроль параметров конфигурации и работы объектов ИТ - инфраструктуры в масштабе времени, близком к реальному;
- оперативное оповещение администратора безопасности и обеспечение возможности реагирования на внутренние и внешние угрозы безопасности;
- повышение эффективности управления событиями ИБ в ИТ - инфраструктуре за счёт автоматизации и упрощения процедур администрирования и периодического контроля журналов событий;
- ретроспективный анализ ситуации в инфраструктуре в режиме реального времени;
- автоматизация процессов обнаружения угроз и аномалий;
- автоматизация процессов регистрации и контроля инцидентов;
- аудит политик и стандартов соответствия, контроль и отчетность по событиям безопасности;
- задокументированное корректное реагирование на возникающие угрозы ИБ и ИТ в режиме реального времени;
- возможность расследования инцидентов и аномалий, в том числе произошедших давно.