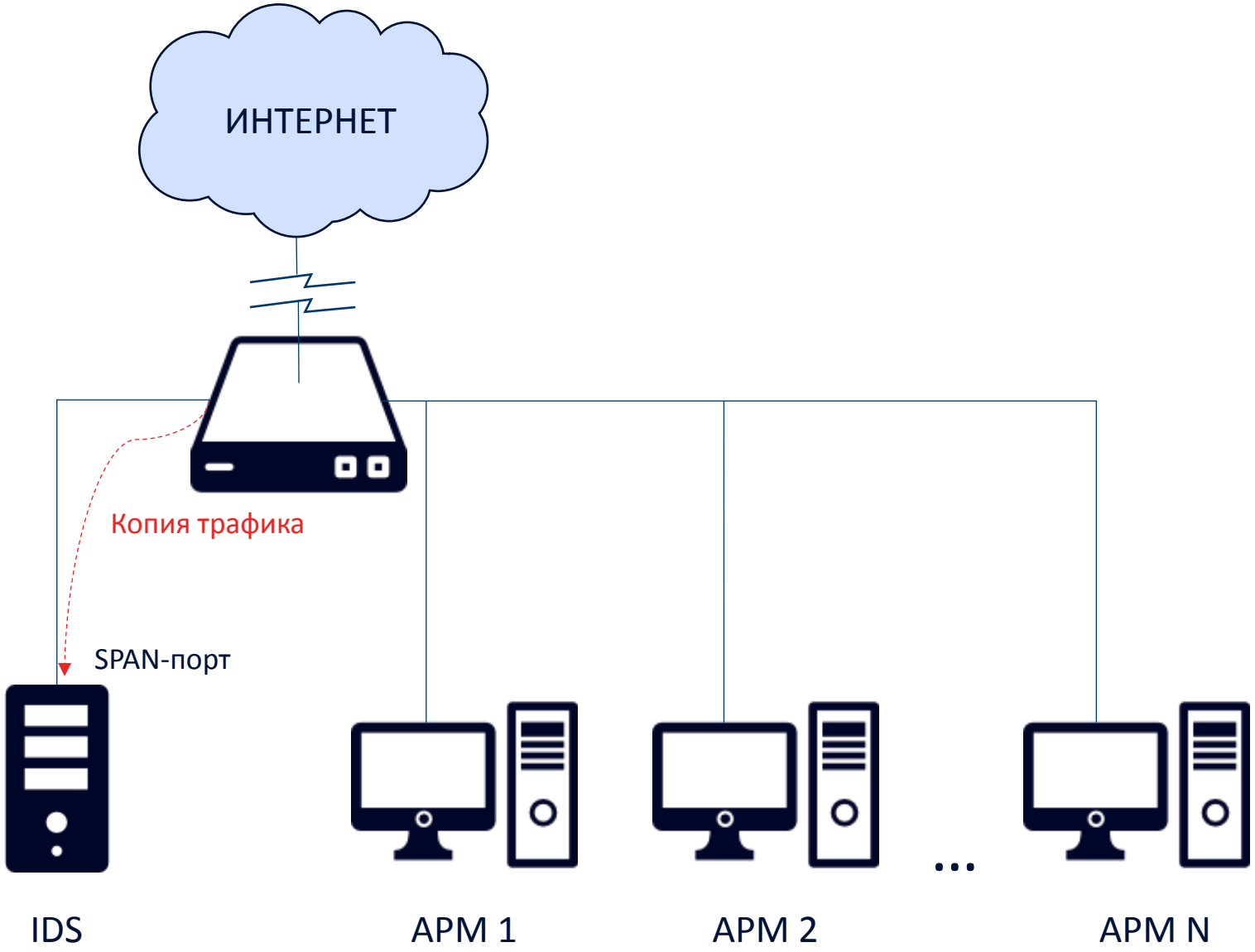
Сравнение технических решений реализации систем обнаружения вторжений

Веселкин Егор
Системный аналитик
Центра разработки технологий компании «РНТ»

Что такое система обнаружения вторжений?



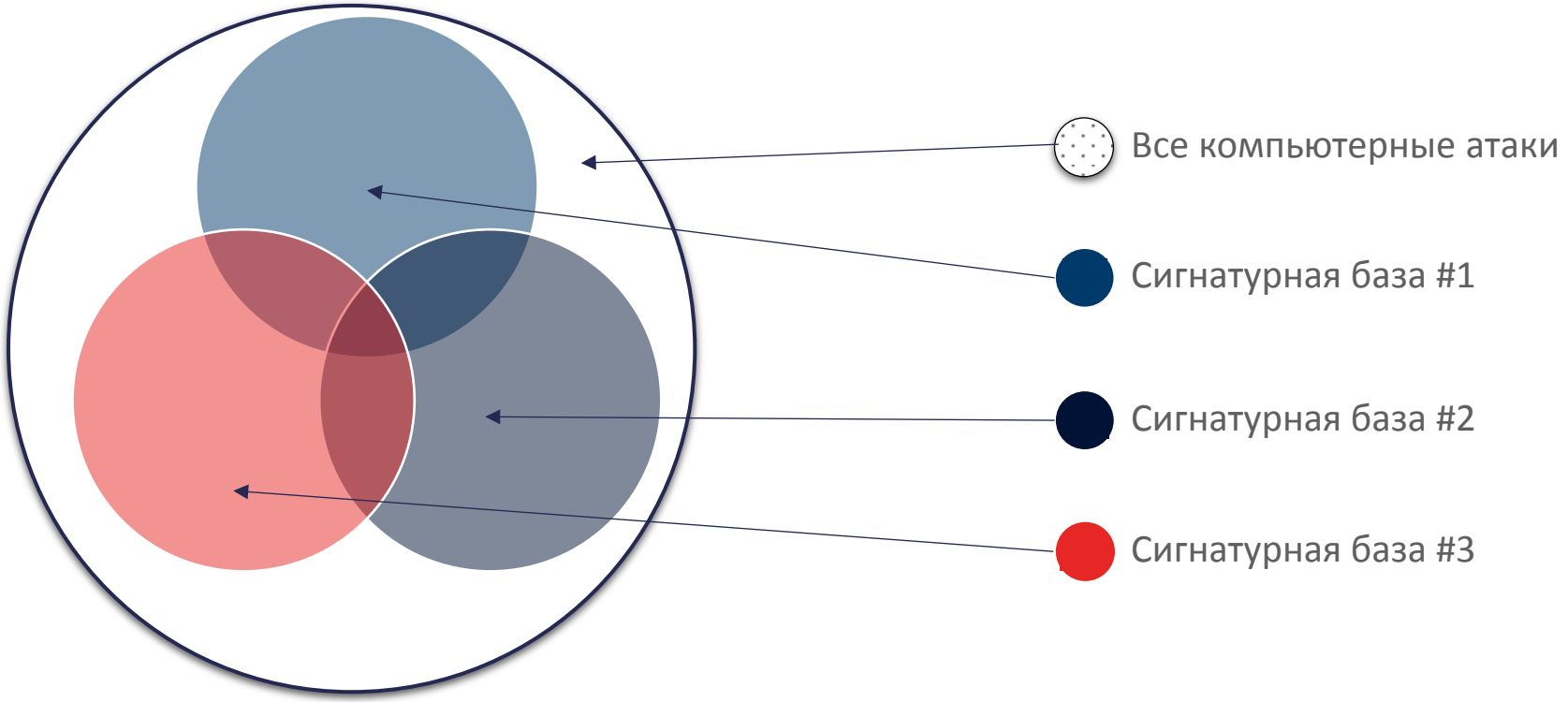
СИСТЕМА ОБНАРУЖЕНИЯ КОМПЬЮТЕРНЫХ АТАК

(IDS - Intrusion Detection System):

это программное или программно-аппаратное средство, предназначенное для автоматического выявления компьютерных атак, направленных на нарушение свойств безопасности информации защищаемых ресурсов организации.

Snort и Suricata

	SNORT	SURICATA
СОЗДАТЕЛЬ	Cisco (Sourcefire VRT)	Open Information Security Foundation
СИГНАТУРЫ	Cisco's TRAC and SecApps (Sourcefire VRT)	Emerging Threats
КОЛИЧЕСТВО	≈ 47 000	≈ 26 000



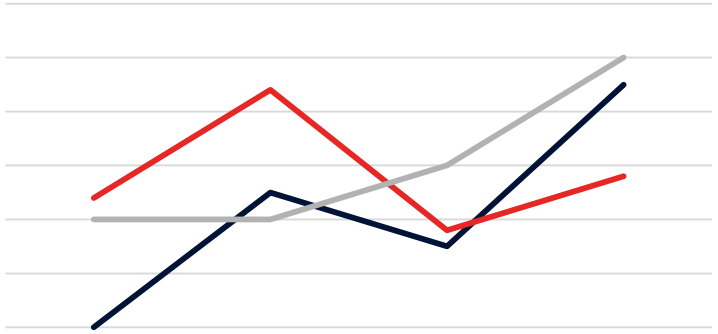
Сравнение IDS

Качественные характеристики:

- → Простота использования
- → Интерфейс
- → Удобство внедрения
- → Наличие необходимой сопроводительной документации

Количественные характеристики:

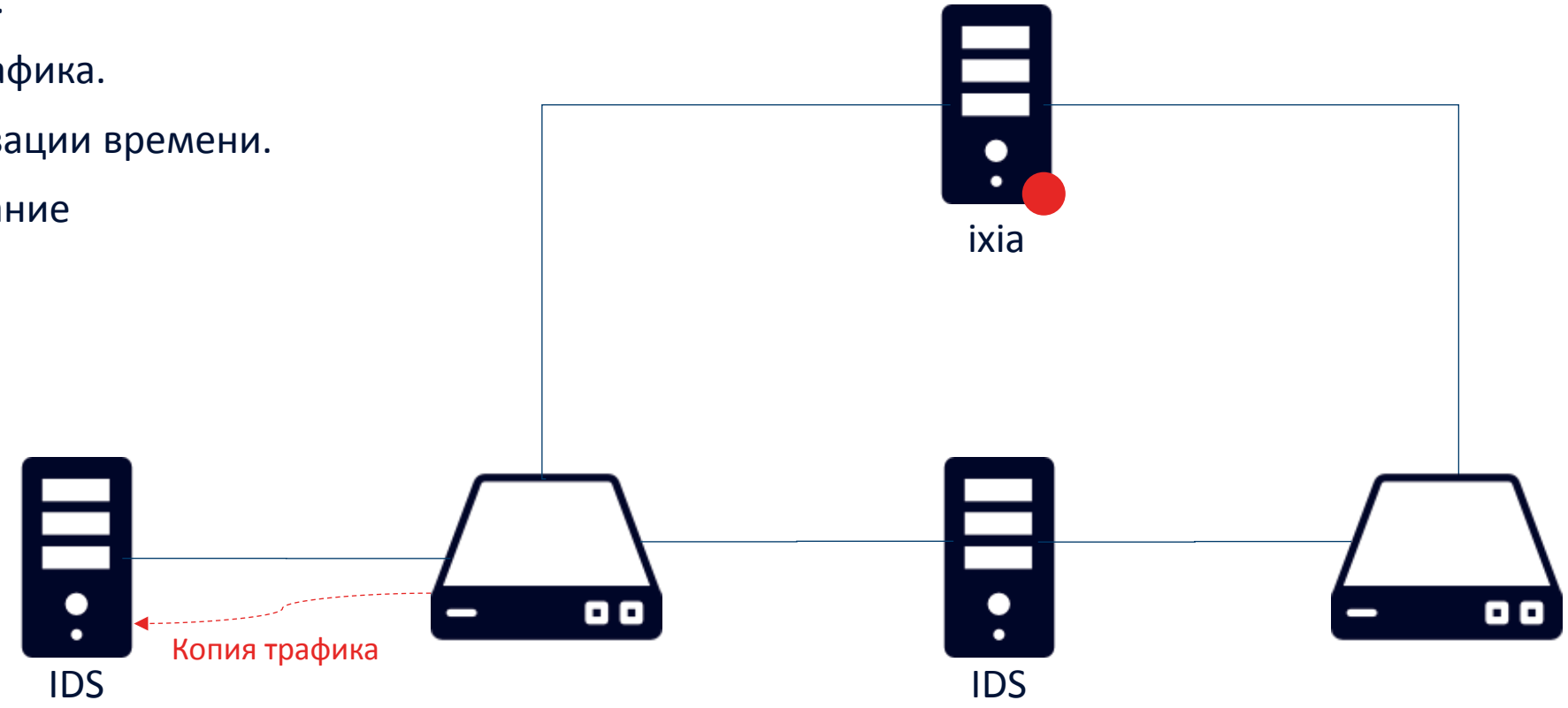
- → Объем базы сигнатур
- → Максимальная скорость обработки трафика
- → Загрузка CPU
- → Загрузка оперативной памяти



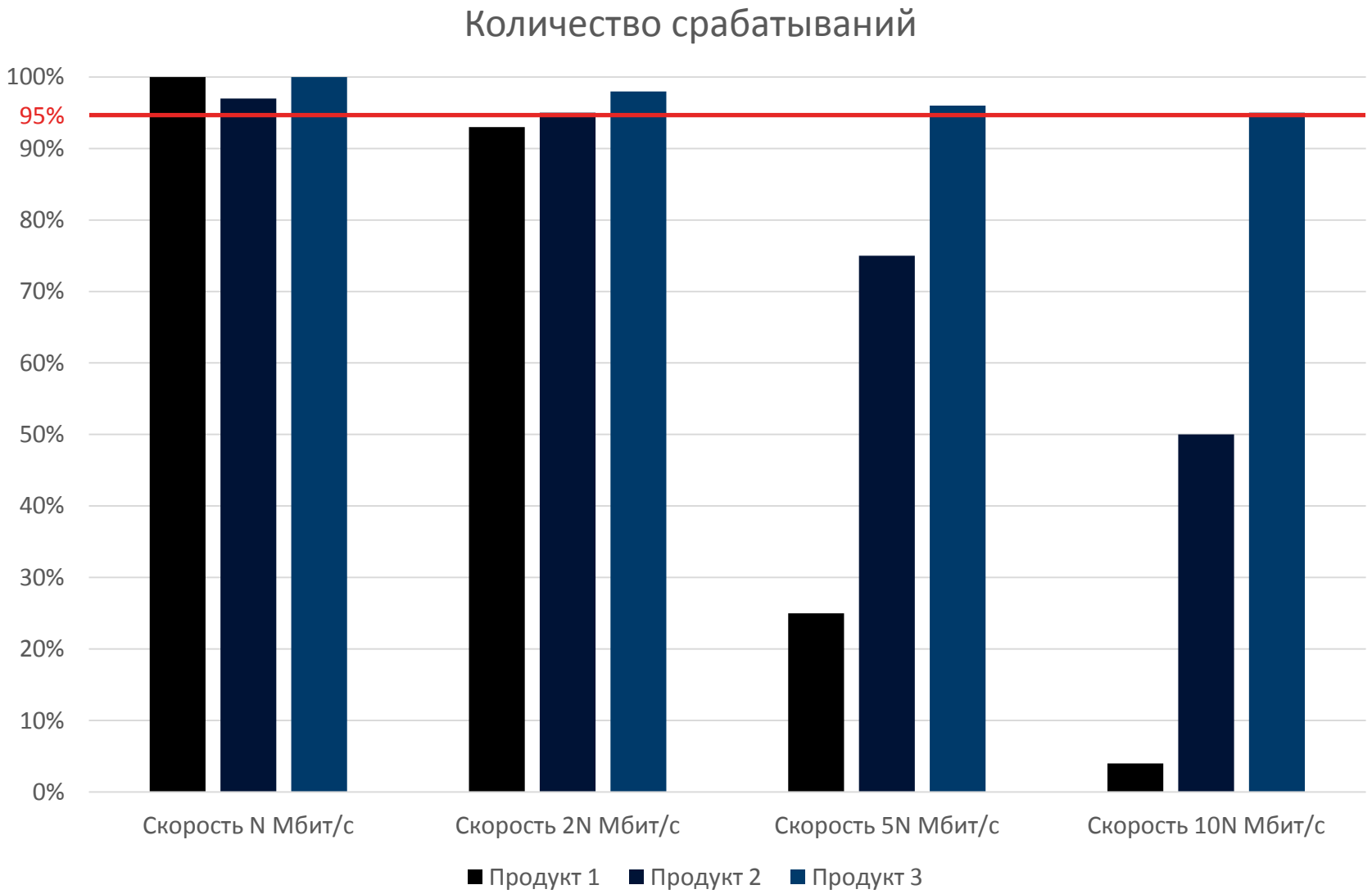
Организация Стенда

Состав стенда:

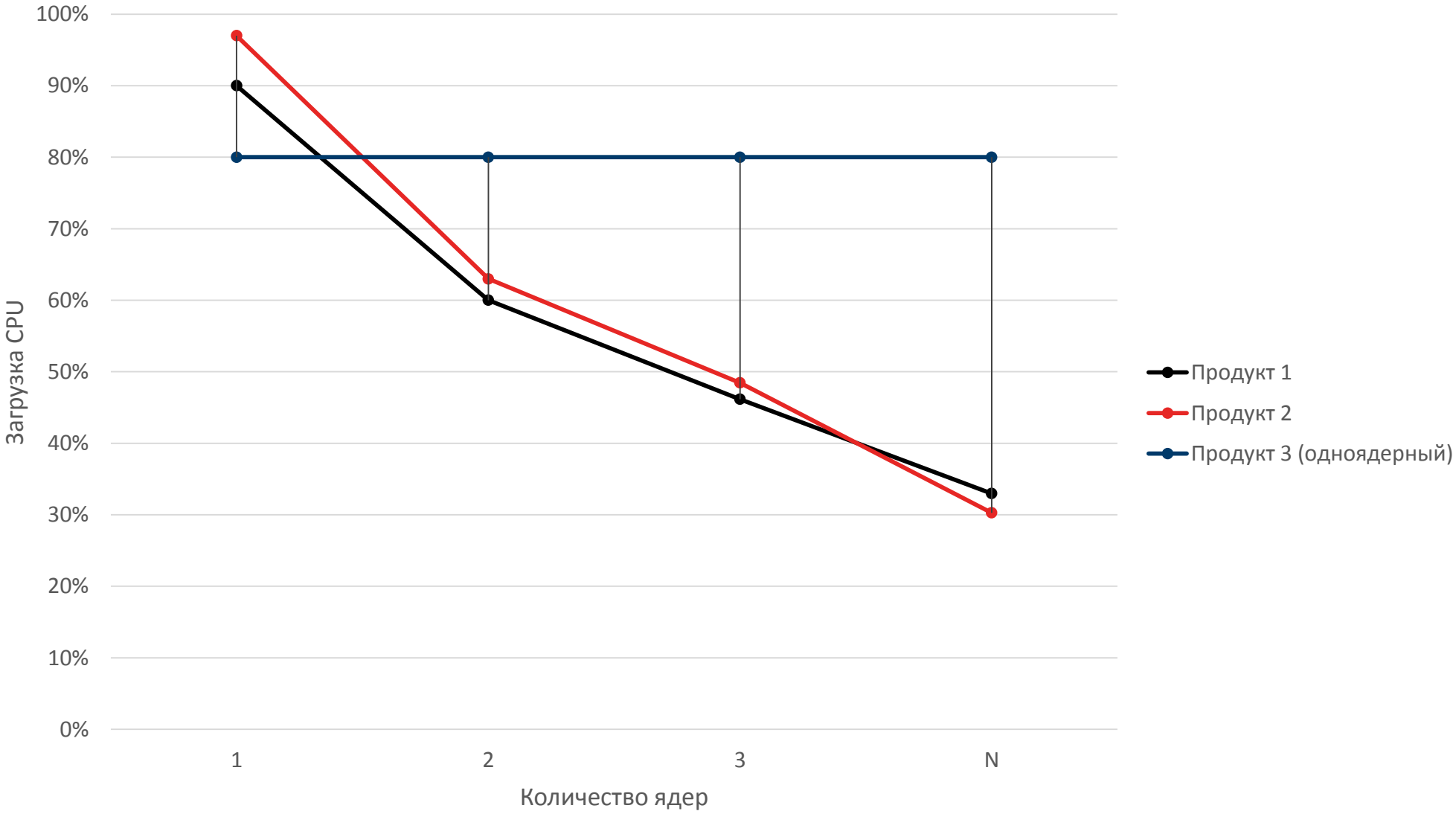
- Средства генерации компьютерных атак.
- Средства генерации нормального трафика (нагрузки).
- Уязвимые ресурсы.
- Систему записи трафика.
- Систему синхронизации времени.
- Сетевое оборудование



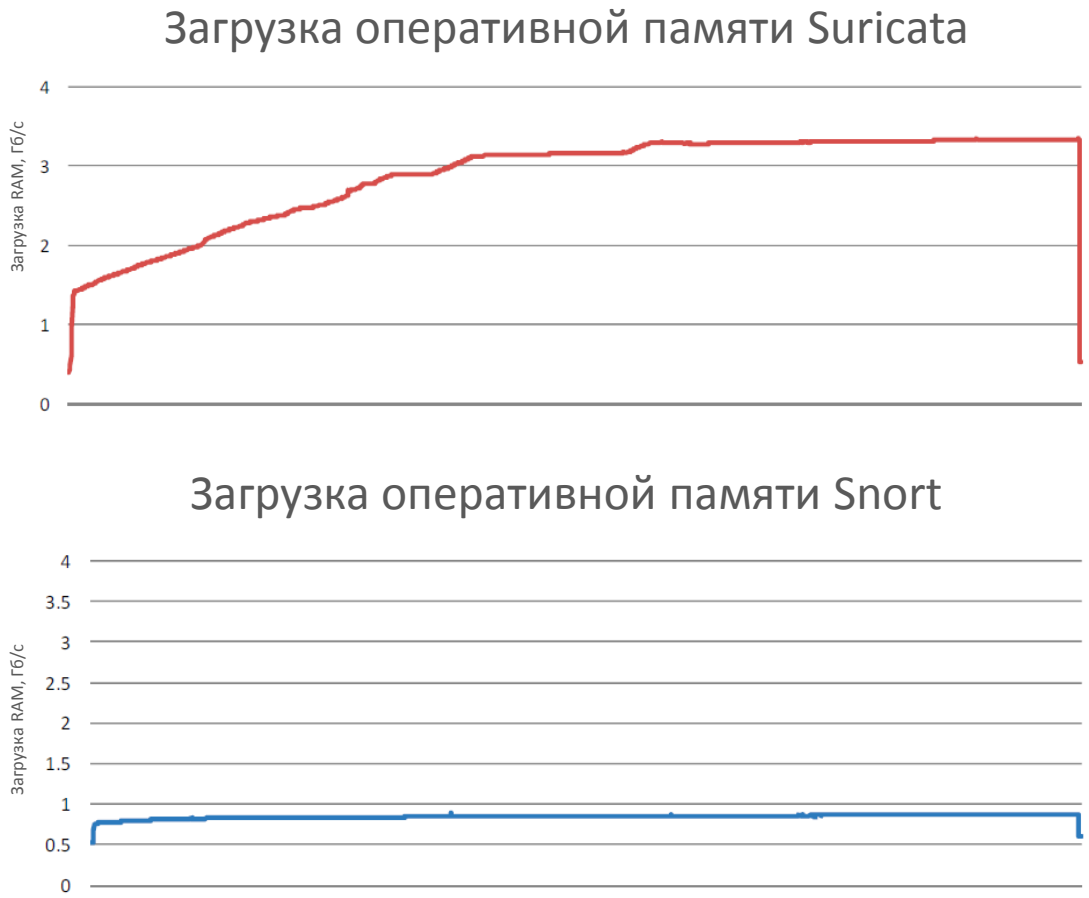
Сравнение IDS : скорость обработки трафика

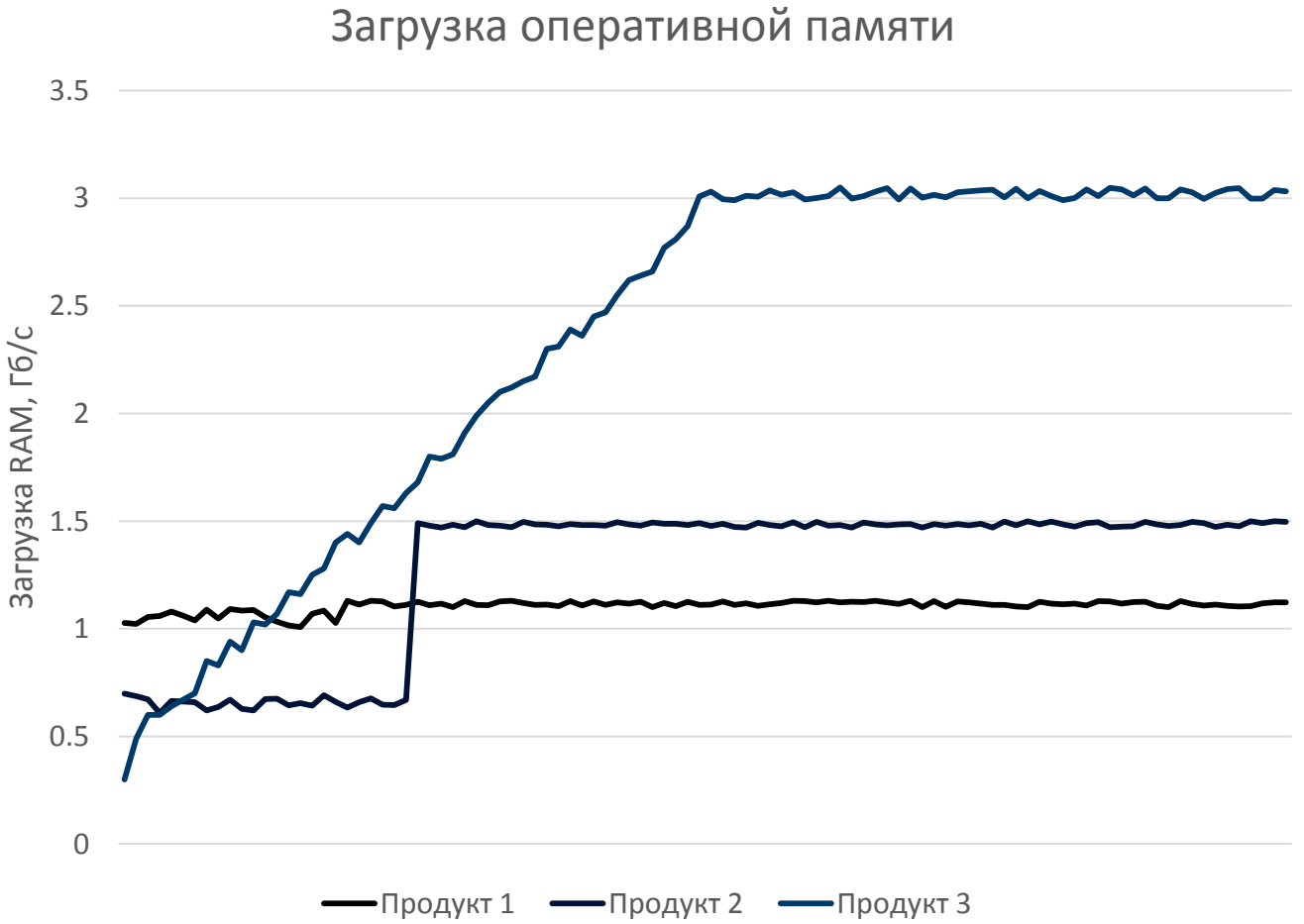


Сравнение IDS : загрузка CPU



Сравнение IDS : загрузка RAM





Сравнение IDS: Прочие отличия

- Блокирование источника компьютерной атаки и способ блокирования
- Запись системой сетевого трафика, содержащего компьютерную атаку, для его дальнейшего разбора
- Дополнительные возможности оповещения администратора/оператора о зафиксированных событиях. (SMS, e-mail, мессенджеры)
- Криптографическая защита канала управления
- Наличие сертификатов соответствия

ТЕРРИТОРИЯ БЕЗОПАСНОСТИ

Стенд B55

129515, Москва,
2-я Останкинская улица, д.6
+7 (495) 777 75 77
rnt@rnt.ru
www.rnt.ru

РОССИЙСКИЕ НАУКОЁМКИЕ ТЕХНОЛОГИИ