

The background is a solid blue color. In the top-left corner, there is a faint, semi-transparent image of a globe showing the Americas. Overlaid on the blue background are several white, semi-transparent geometric shapes: a large circle, a smaller circle, and a complex polygonal shape that resembles a stylized gear or a network node. The text is centered in the upper half of the image.

Обнаружение атак. Система RealSecure

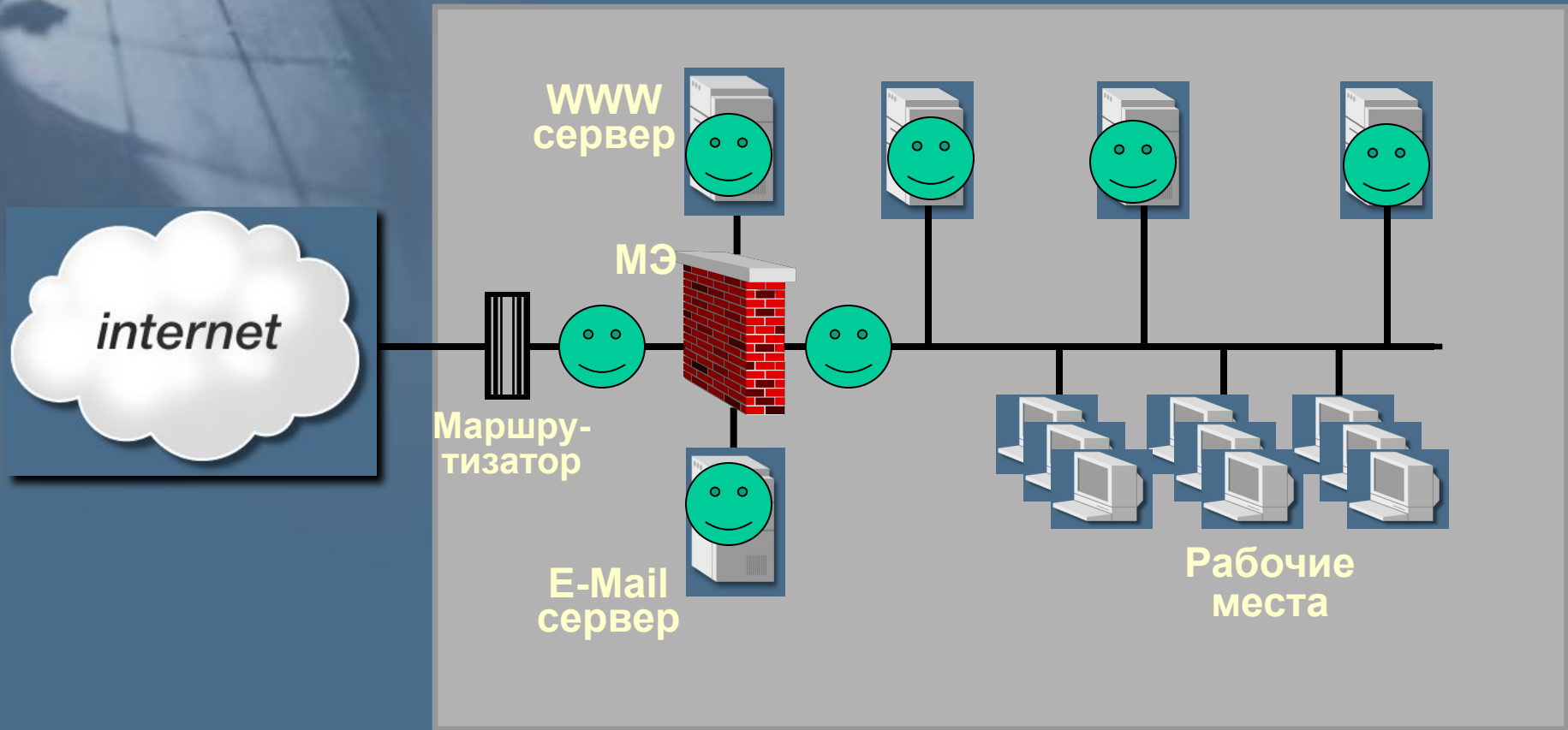
Средства защиты сетей

- МЭ
- Средства анализа защищённости
- Средства обнаружения атак

Архитектура систем обнаружения атак

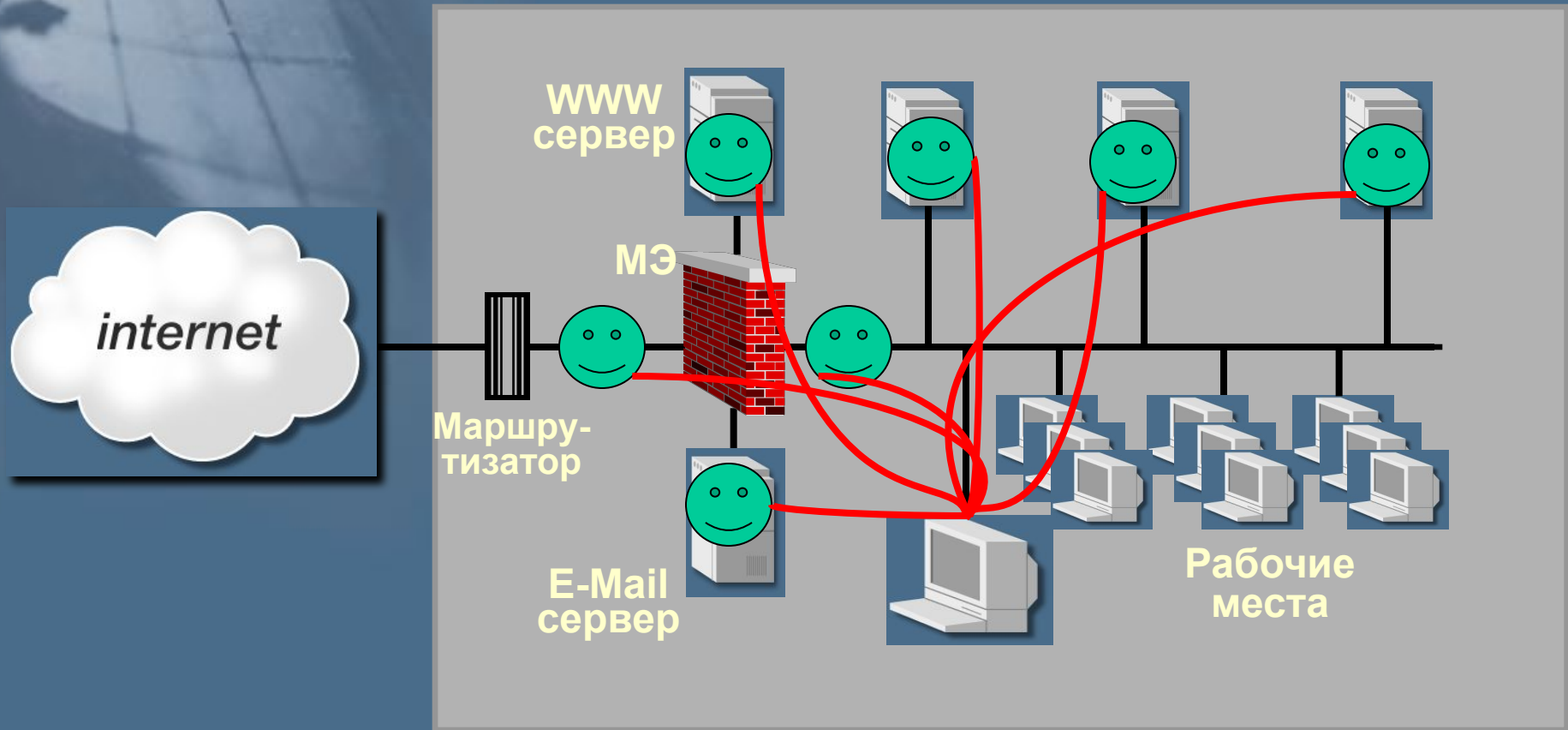
- Модуль слежения
- Модуль управления

Архитектура систем обнаружения атак



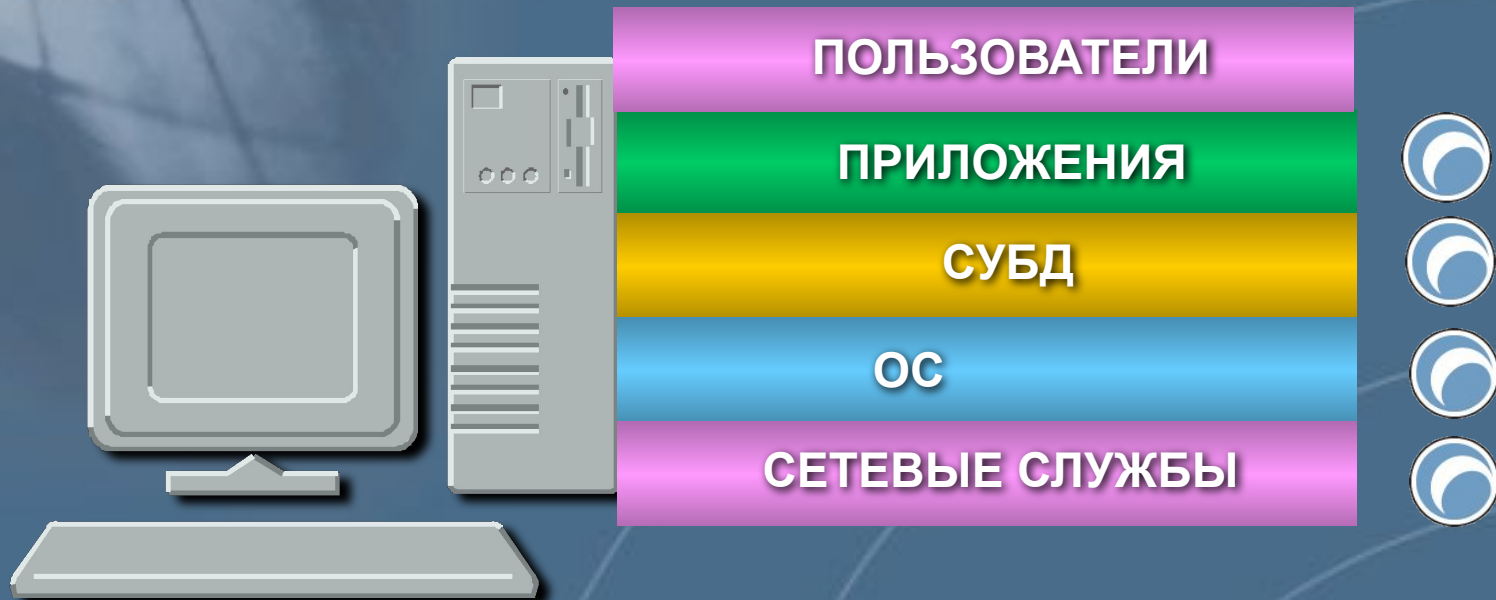
Сенсоры

Архитектура систем обнаружения атак



Управляющие компоненты

Классификация систем обнаружения атак



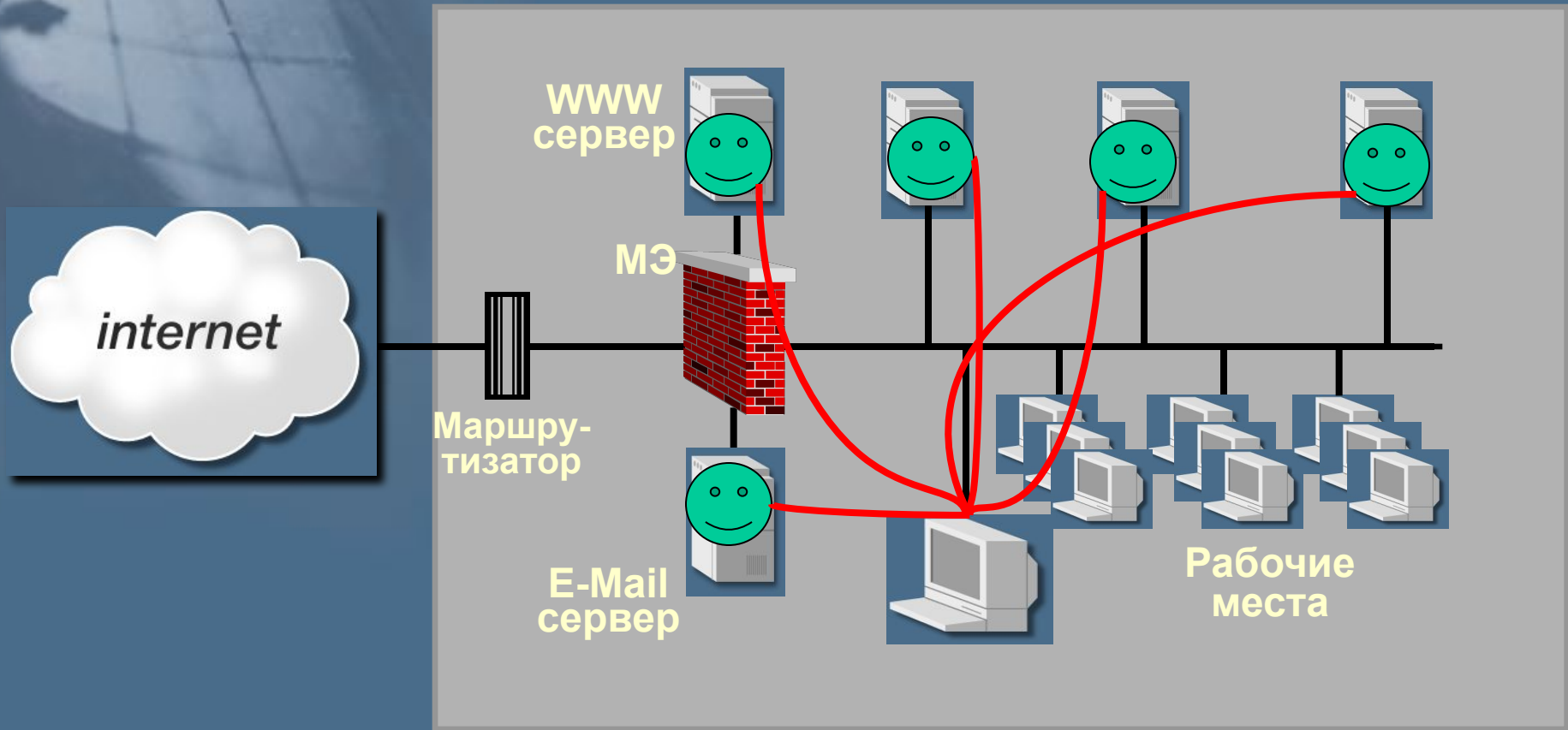
По уровням информационной инфраструктуры

Классификация систем обнаружения атак

- Системы на базе узла
- Системы на базе сегмента

По принципу реализации

Системы обнаружения атак на базе узла



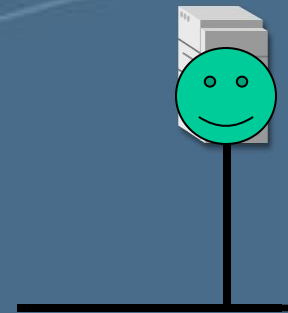
Системы обнаружения атак на базе узла

Источники данных:

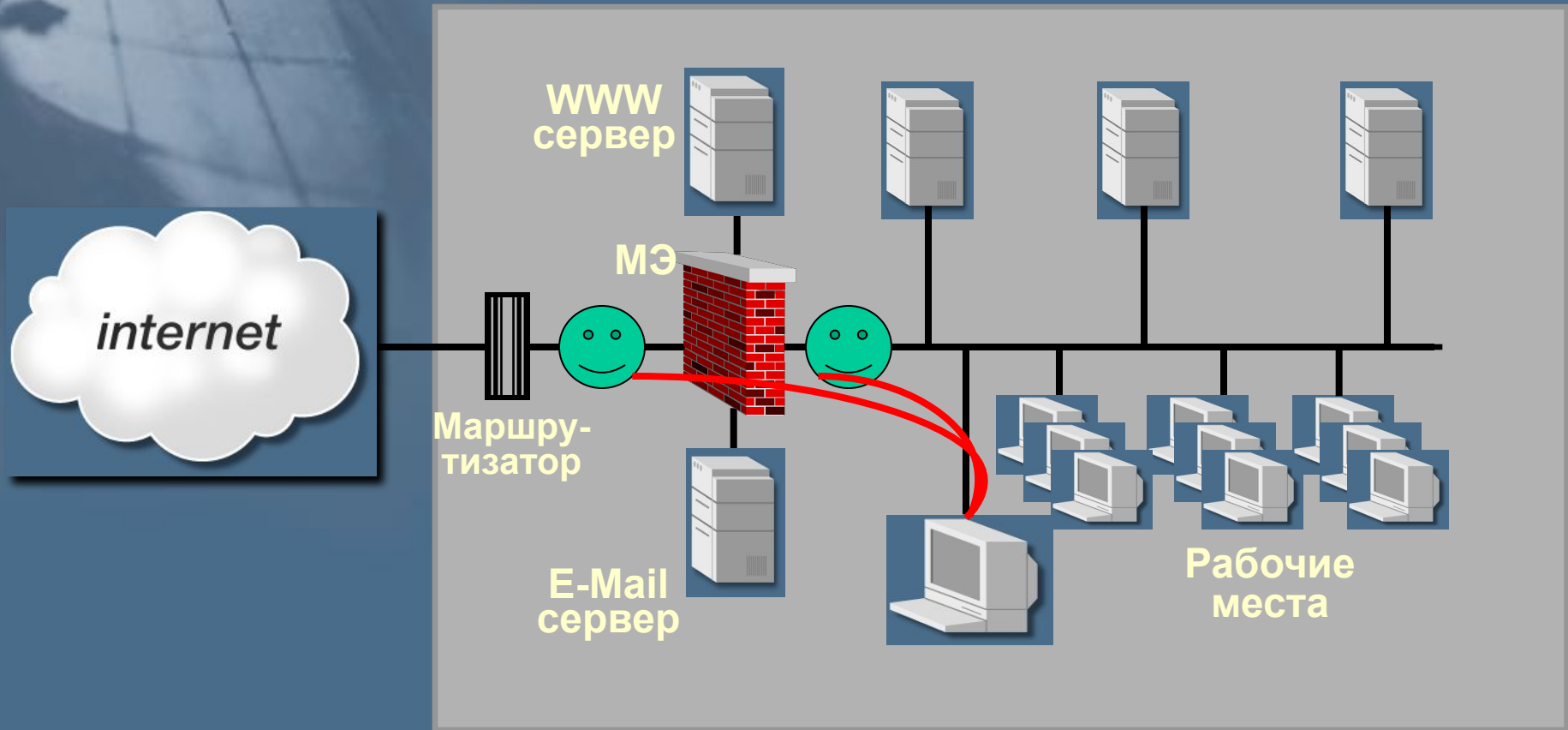
- Журналы аудита
- Действия пользователей

Необязательно:

Сетевые пакеты (фреймы), направленные к узлу и от узла



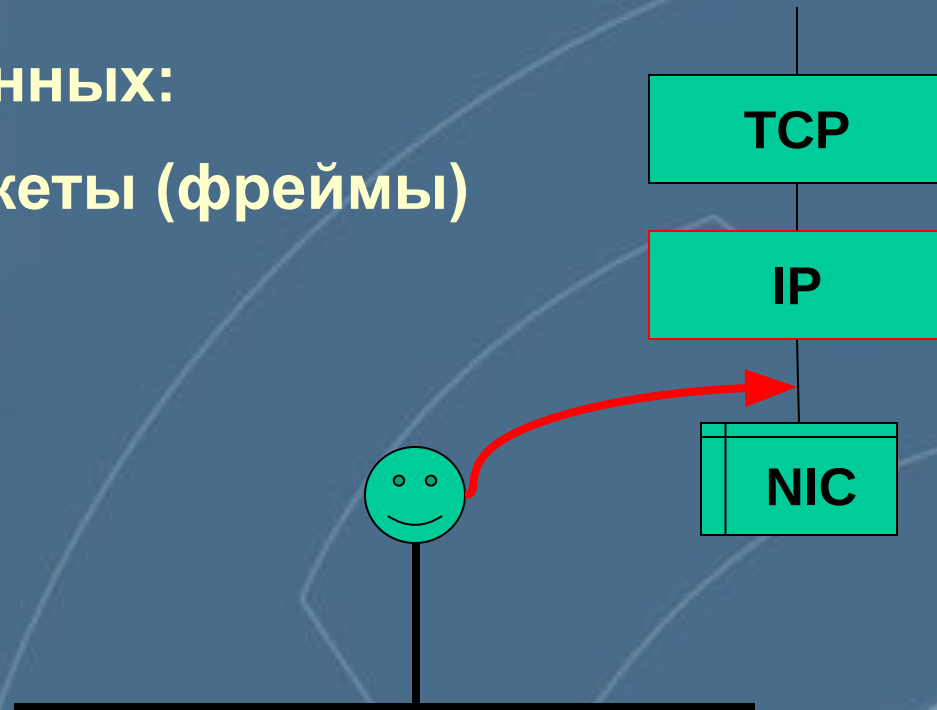
Системы обнаружения атак на базе сети



Системы обнаружения атак на базе сети

Источник данных:

- Сетевые пакеты (фреймы)



Классификация систем обнаружения атак



Обнаружение аномалий



Анализ сигнатур

По технологии обнаружения

Системы обнаружения атак

	Net Prowler	Secure IDS	eTrust Intrusion Detection	RealSecure	Snort
Производитель	Axent Technologies	Cisco Systems	Computer Associates	Internet Security Systems	Net
Платформа	Windows NT	Защищенная версия Solaris	Windows NT	Windows NT (2000)	Unix
Технология обнаружения	Сигнатуры атак	Сигнатуры атак	Сигнатуры атак	Сигнатуры атак	Сигнатуры атак
Принцип реализации	На базе сети	На базе сети	На базе сети + ВОЗМОЖНОСТИ МЭ	На базе сети и на базе узла	На базе сети

RealSecure - система обнаружения атак в реальном времени

- ✓ *Устанавливается в сетевом сегменте или на отдельном узле*
- ✓ *Просматривает весь трафик сегмента или действия пользователя конкретного узла*
- ✓ *Анализирует трафик с целью обнаружения атак и других событий, связанных с безопасностью*
- ✓ *В случае обнаружения предпринимает ответные действия*



Компоненты RealSecure

Модули слежения

Модули управления

**Сетевой модуль
(Network Sensor)**



**Системный агент
(OS Sensor)**



Server Sensor



Компоненты RealSecure

Модули слежения

Модули управления



*Workgroup
Manager*

Server Manager

*Командная
строка*

Компоненты RealSecure

Модули управления



Workgroup Manager

- *Event Collector*
- *Enterprise Database*
- *Asset Database*
- *Console*

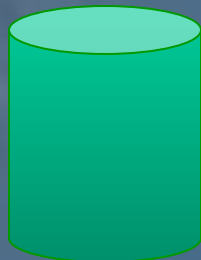
Server Manager

Командная строка

Компоненты RealSecure версии 6.0



Консоли



Event Collector
(сбор событий с сенсоров)

Сетевой модуль
(*Network Sensor*)



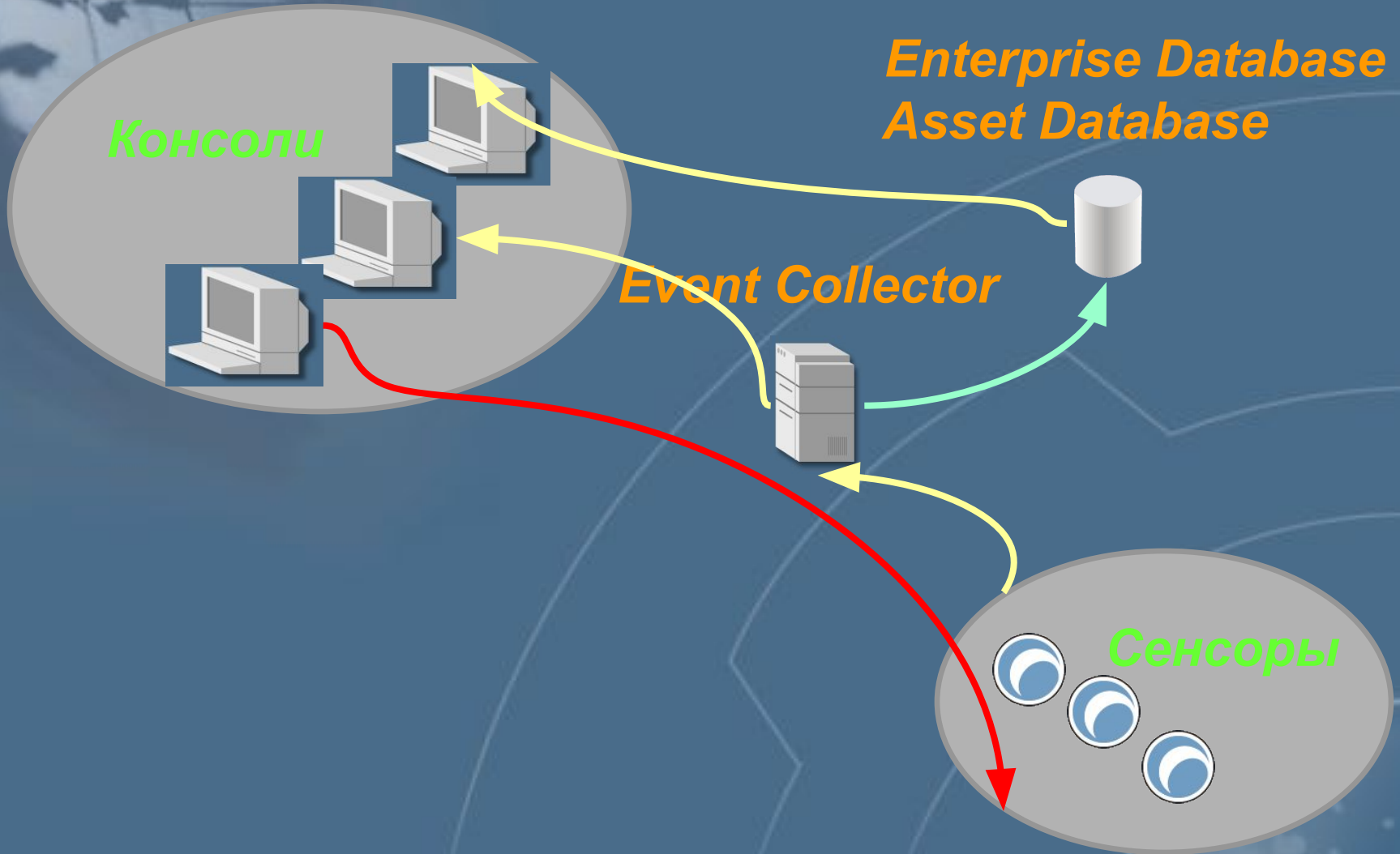
Системный агент
(*OS Sensor*)



Server Sensor

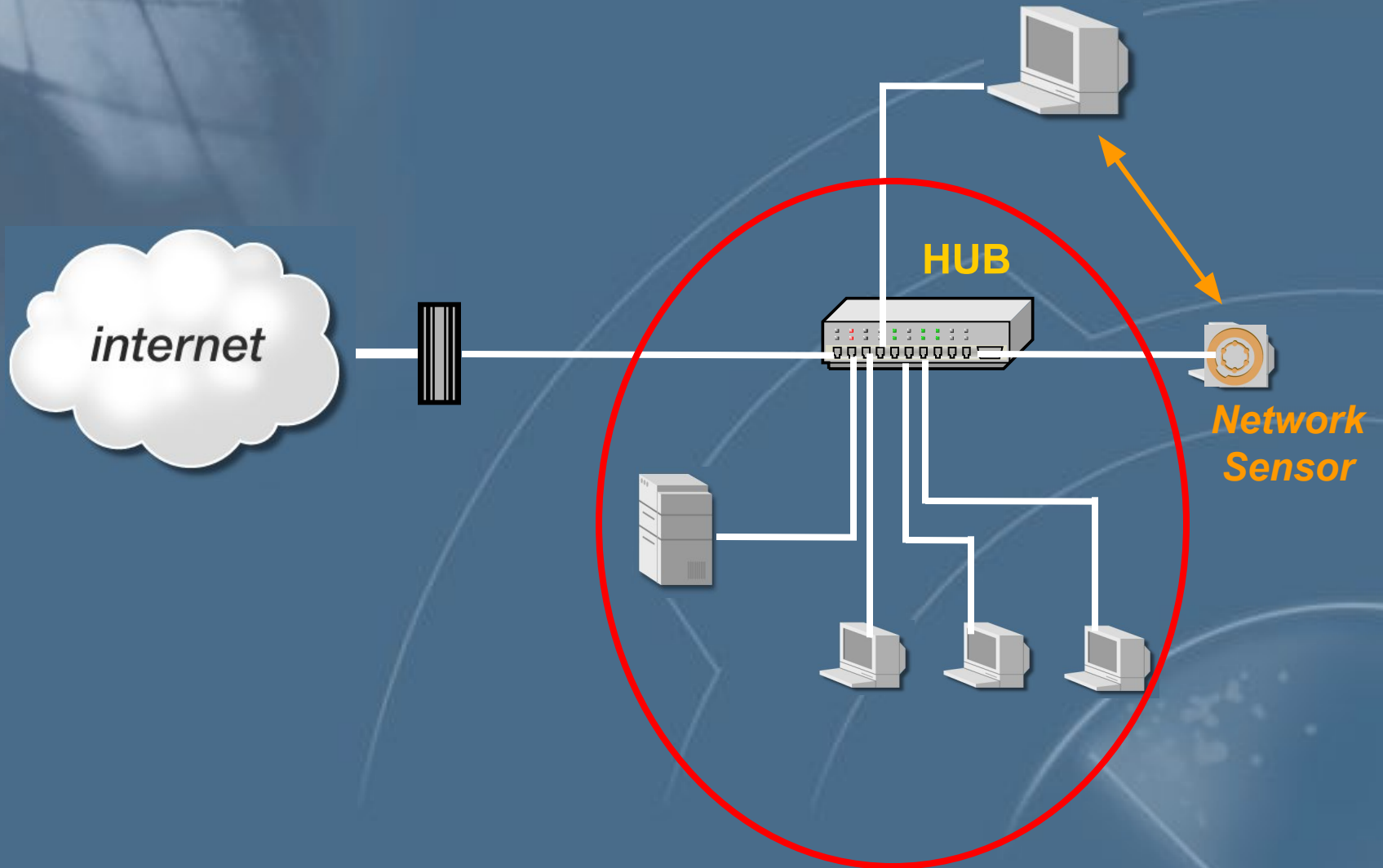


Архитектура

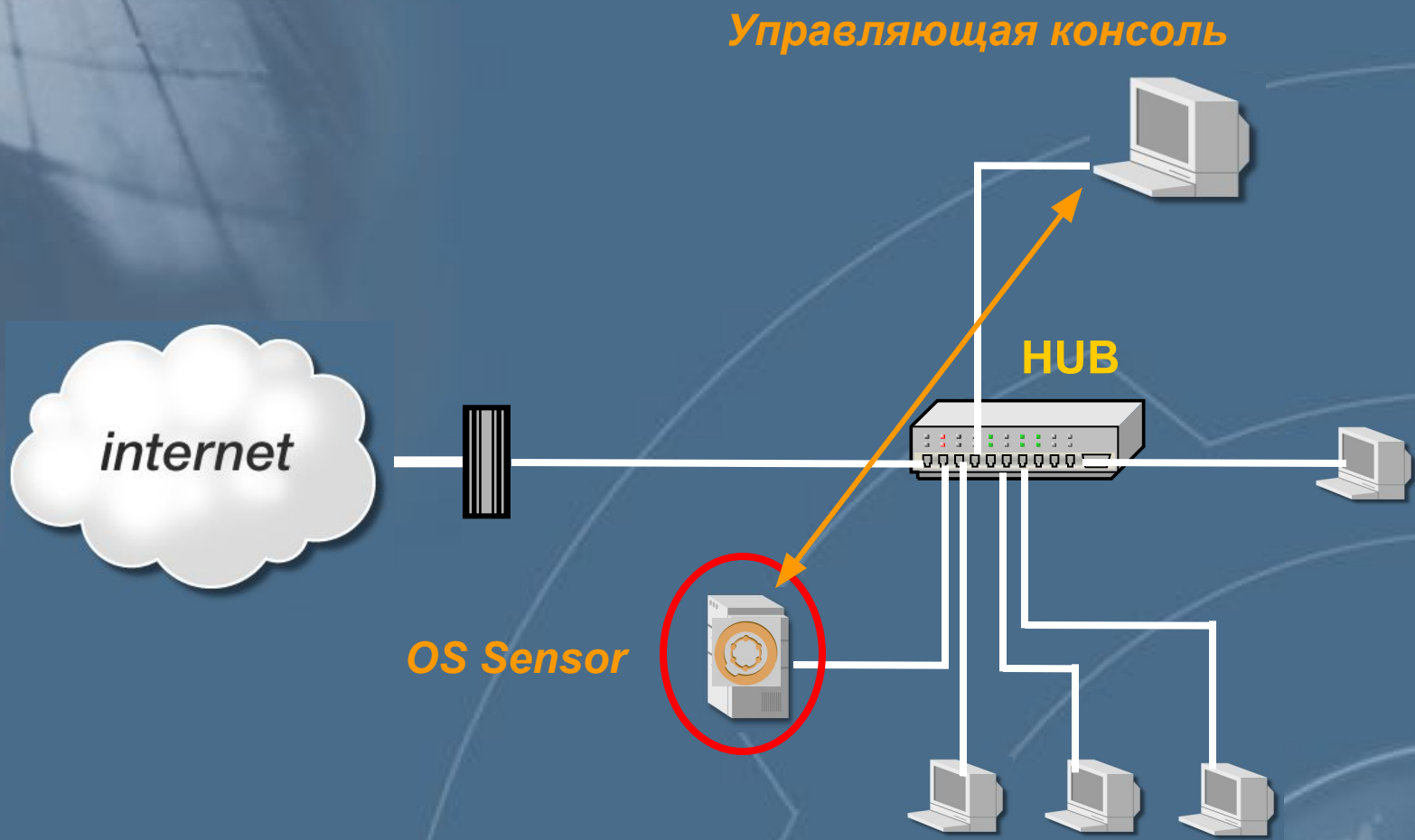


Расположение сетевого модуля

Управляющая консоль

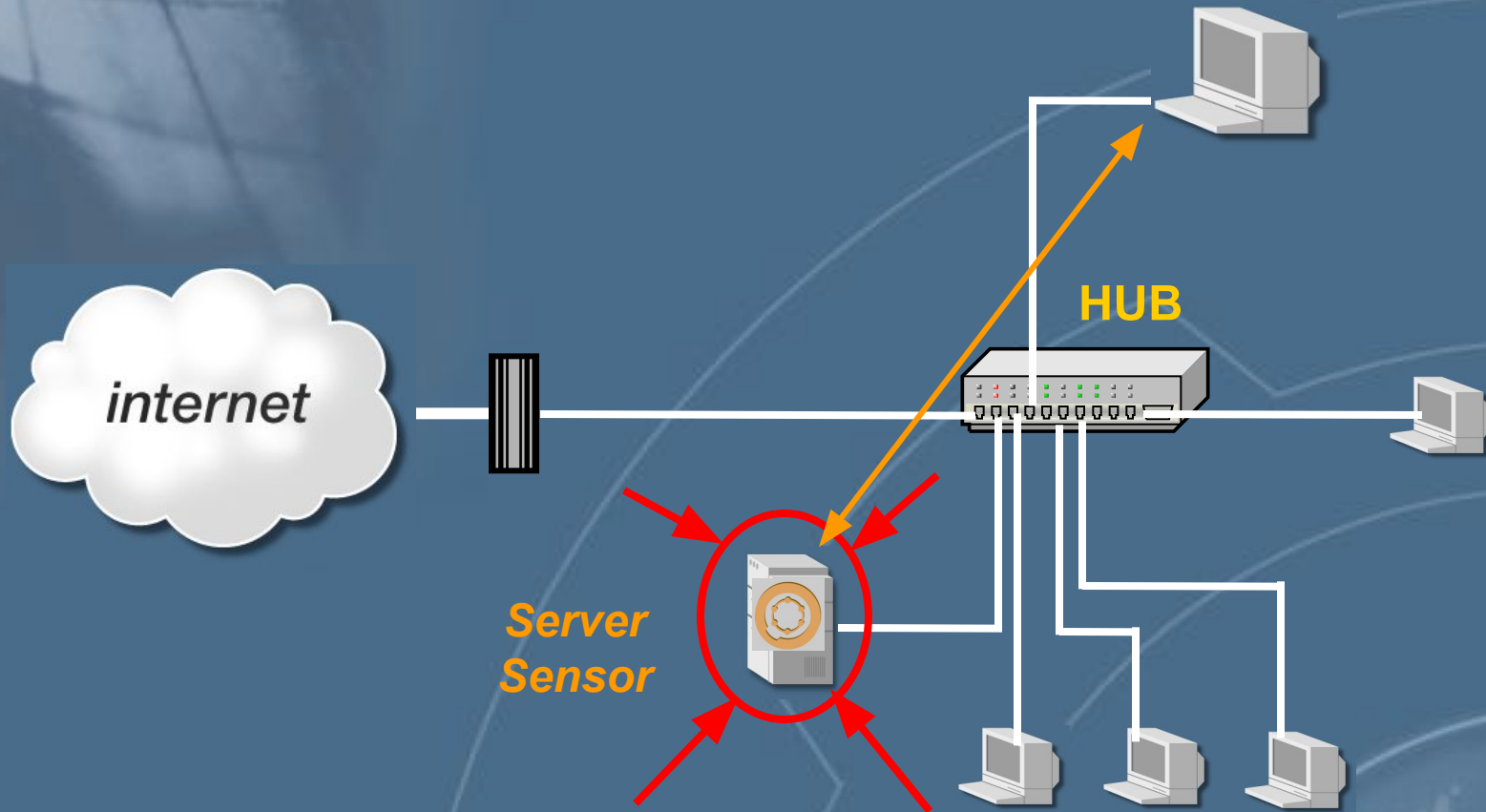


Расположение системного агента

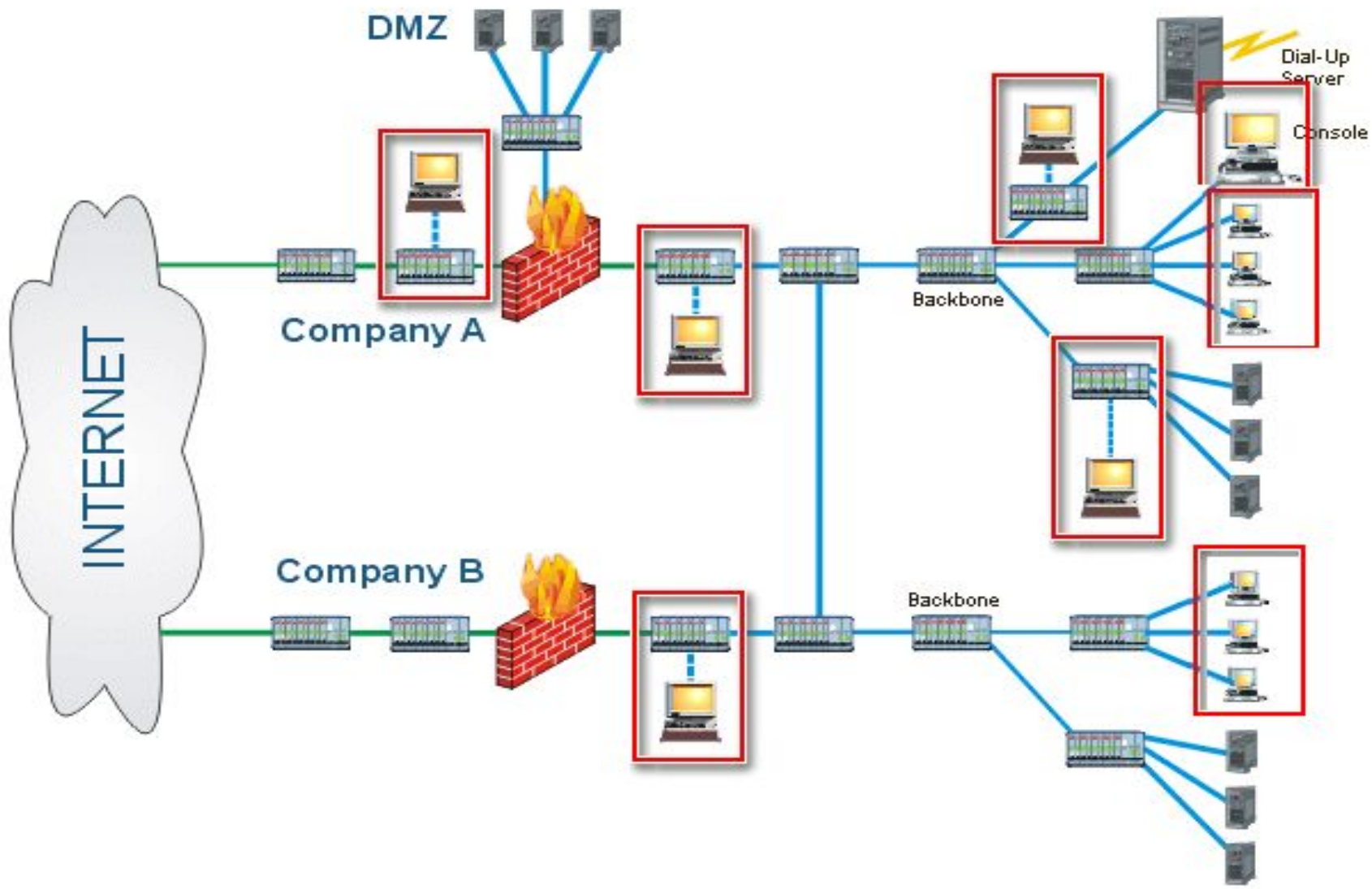


Расположение Server Sensor

Управляющая консоль



Примеры размещения RealSecure



Категории контролируемых событий

- *Атаки*
 - *Уровня сети (Сканирование портов, SYN Flood, Ping of Death)*
 - *Уровня СУБД (MS SQL Server)*
 - *Уровня приложений (Атаки на MS IIS, MS Exchange)*
- *Установленные соединения*
 - *TELNET, FTP, SMTP*
- *Пользовательские события*
 - *HTTP – запросы, содержимое почтовых сообщений*

Механизмы реагирования RealSecure

Разрыв соединения

Реконфигурация межсетевого экрана

Выполнение программы, определённой пользователем

Отправка сообщения

На консоль

По протоколу SNMP

По E-mail

Регистрация события в БД

Расширенная регистрация с возможностью последующего воспроизведения

Network Sensor

Особенности:

- обнаружение в реальном режиме времени
- независимость от операционной системы
- обнаружение атак до достижения ею цели
- невозможность обнаружения (Stealth-режим)

RealSecure и межсетевые экраны

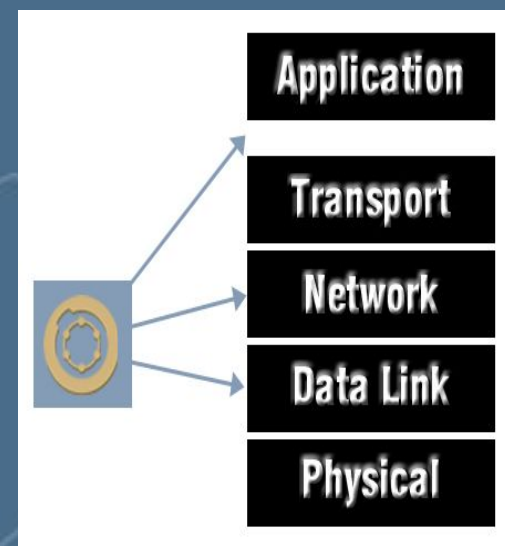
- Модемы
- Атаки через «туннели»
- Атаки со стороны авторизованных пользователей
- Атаки на межсетевые экраны

Server Sensor

Обнаружение атак на всех уровнях на конкретный узел сети

Особенности:

- *производительность*
- *обнаружение всех атак*
- *работа в коммутируемых сетях*
- *работают в сетях с шифрованием*



Функции персонального межсетевого экрана

ИНФОРМЗАЩИТА

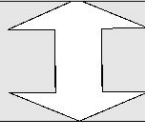
НАУЧНО-ИНЖЕНЕРНОЕ ПРЕДПРИЯТИЕ

Server Sensor

3. High Module

User-level Application

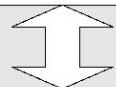
Protocol Sensor High Level Tap



UDP/TCP/ICMP

IP and IPSEC

Protocol Sensor Low Level Tap

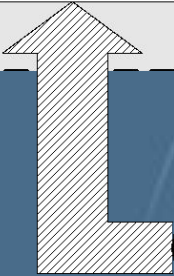


NIC

2. Стек TCPIP

1. Low Module

Kernel



Inbound/Outbound Traffic for Host

Что делает управляющая консоль?



Предоставляет интерфейс для конфигурирования модулей слежения



На консоль поступают сообщения от модулей слежения и данные, записанные модулями слежения

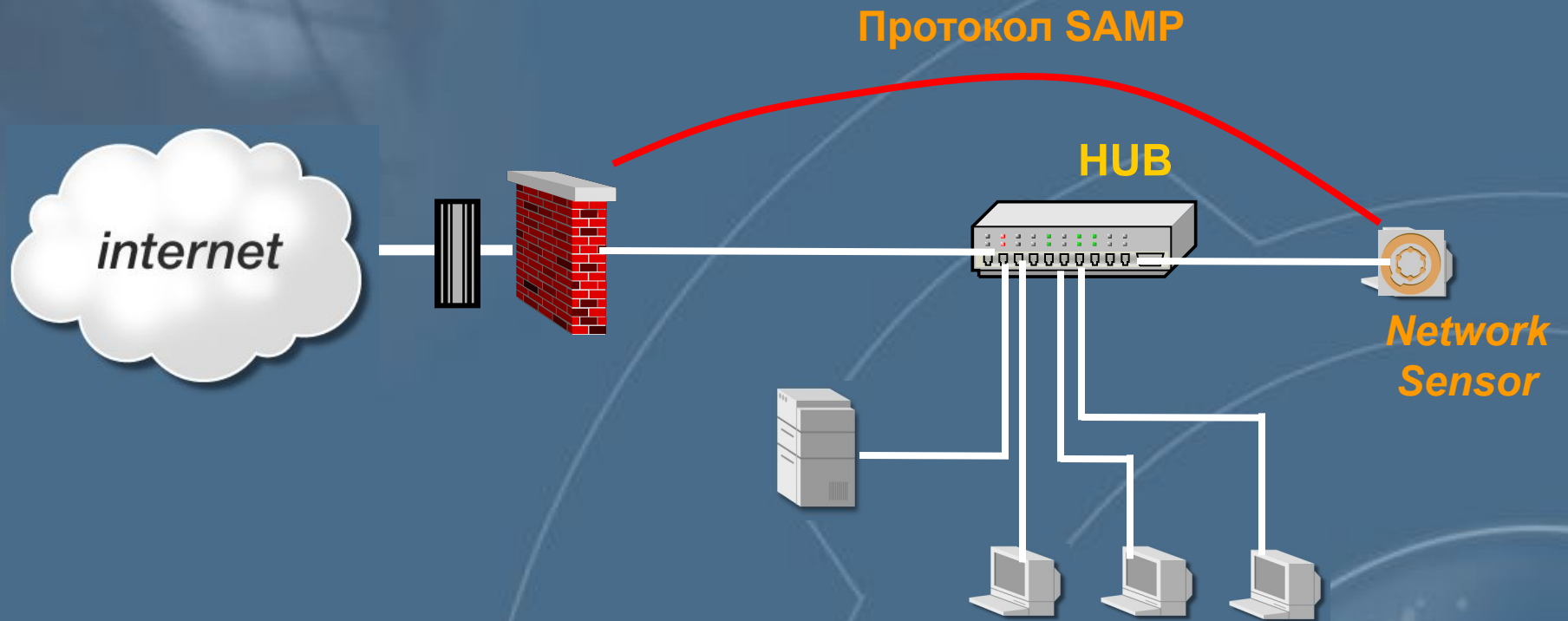


Позволяет формировать отчёты на основе собранных данных

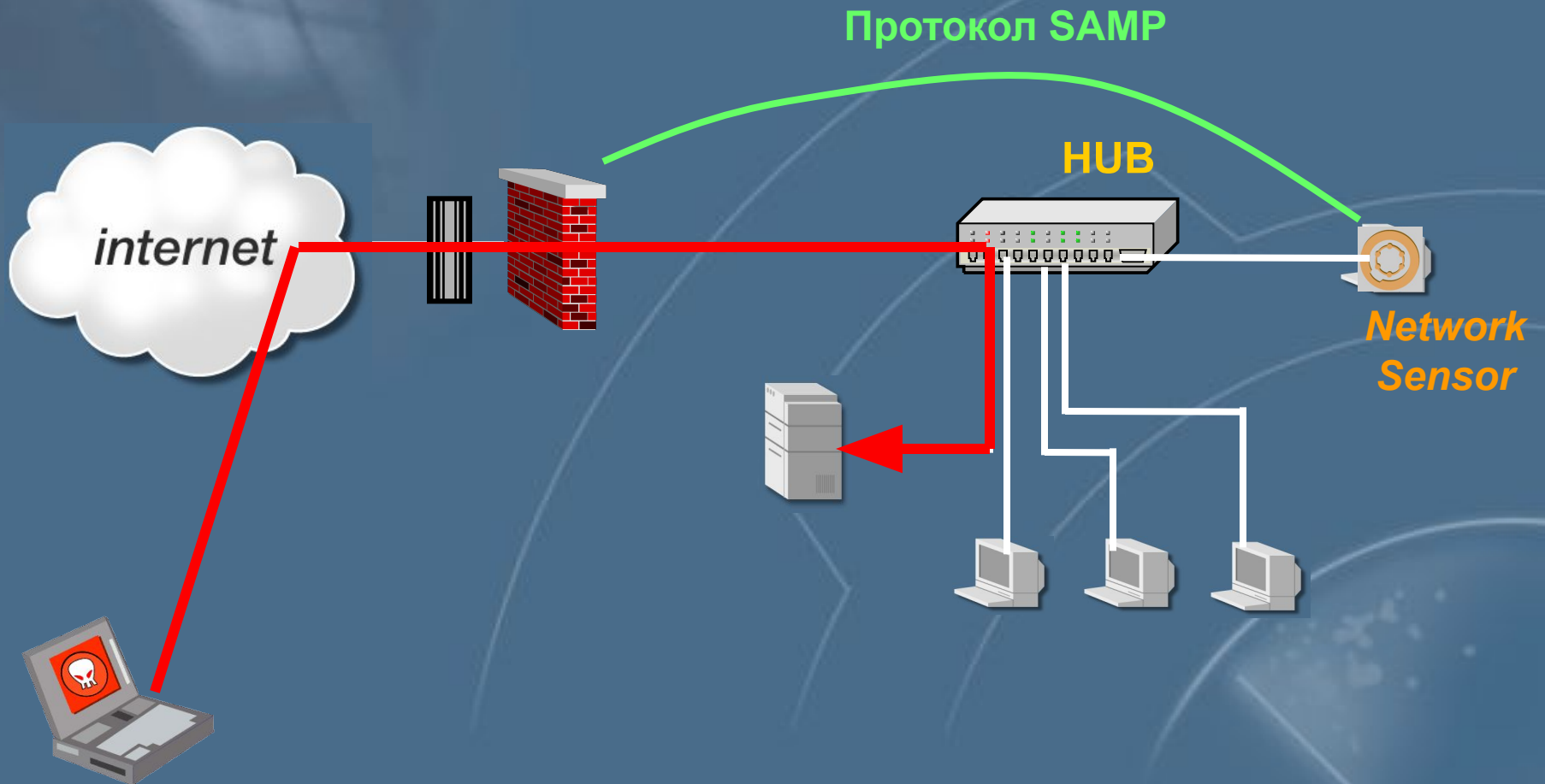
Концепция OPSec

- Использование OPSec SDK, предоставляющих необходимые API
- Применение открытых протоколов
 - CVP(Content Vectoring Protocol)
 - UFP (URL Filter Protocol)
 - SAMP (Suspicious Activity Monitoring Protocol)
 - LEA (Log Export API)
 - OMI (Object Management Interface)
- Использование языка INSPECT

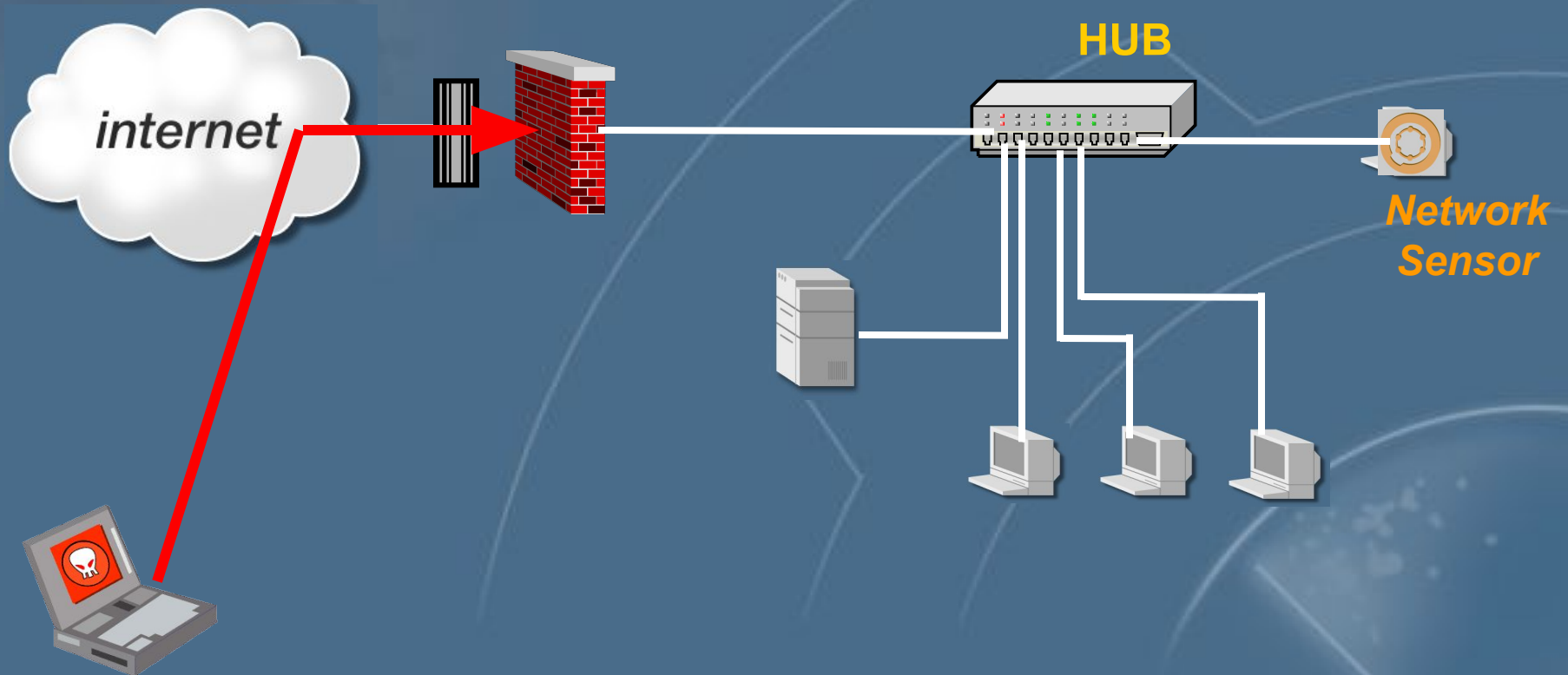
Реконфигурация МЭ



Реконфигурация МЭ



Реконфигурация МЭ



The background is a solid blue color. In the top-left corner, there is a faint, semi-transparent image of a globe showing the continents. Overlaid on the globe and extending across the background are several thin, white, curved lines that resemble network connections or data paths. The text is centered in the upper half of the image.

Система обнаружения атак Snort

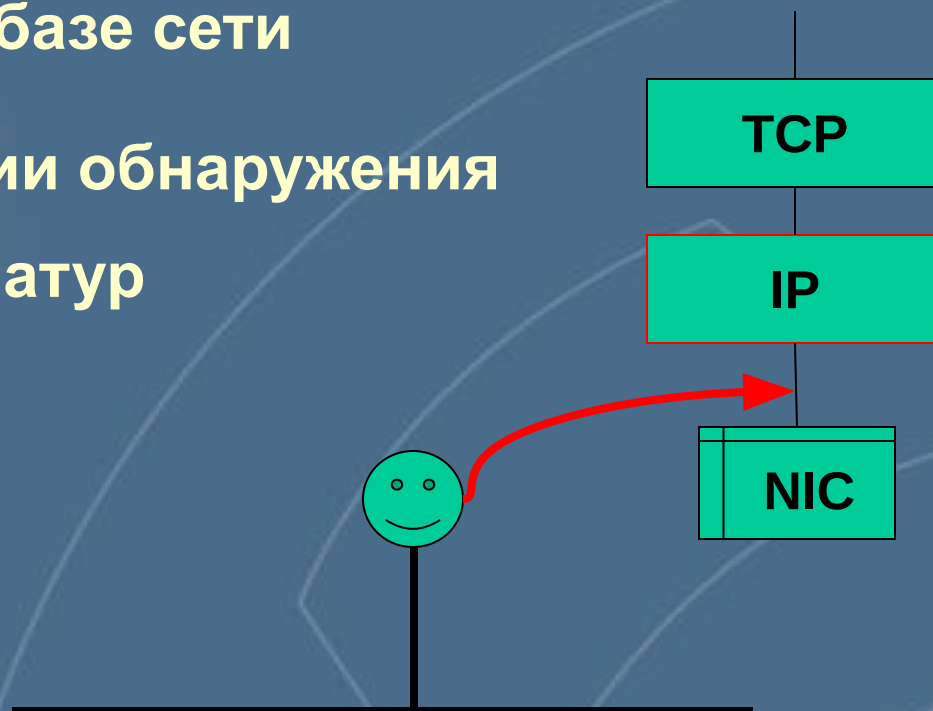
Архитектура

По принципу реализации

- Система на базе сети

По технологии обнаружения

- Анализ сигнатур



Режимы работы

- **Sniffer Mode**
- **Packet Logger**
- **Intrusion Detection System**

Sniffer Mode

Вывод на экран содержимого пакетов

`./snort -v`

IP	TCP UDP ICMP
----	--------------------

`./snort -vd`

IP	TCP UDP ICMP	Данные
----	--------------------	--------

`./snort -vde`

Ethernet	IP	TCP UDP ICMP	Данные
----------	----	--------------------	--------

Packet Logger

Запись содержимого пакетов в файл

```
./snort -vde -l  
./log
```

подкаталог **log** в текущем каталоге

Intrusion Detection System

Обнаружение событий

```
./snort -vde -l ./log -c  
snort.conf
```

**Правила срабатывания
(контролируемые события)**