

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. In the bottom-right corner, there are several concentric, semi-transparent white lines that resemble radar waves or a signal scan, emanating from a point. The text is centered in the upper half of the image.

Средства обнаружения атак

Архитектура систем обнаружения атак

- Модуль слежения
- Модуль управления

- Системы на базе узла
- Системы на базе сегмента

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

Модуль слежения

Управляющая консоль



*Сетевой модуль
(Network Sensor)*



*Системный агент
(OS Sensor)*



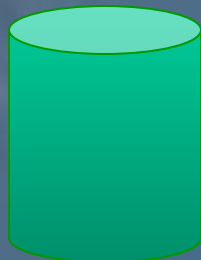
Server Sensor



Компоненты RealSecure версии 6.0



Консоли



Event Collector
(сбор событий с сенсоров)

Сетевой модуль
(*Network Sensor*)



Системный агент
(*OS Sensor*)

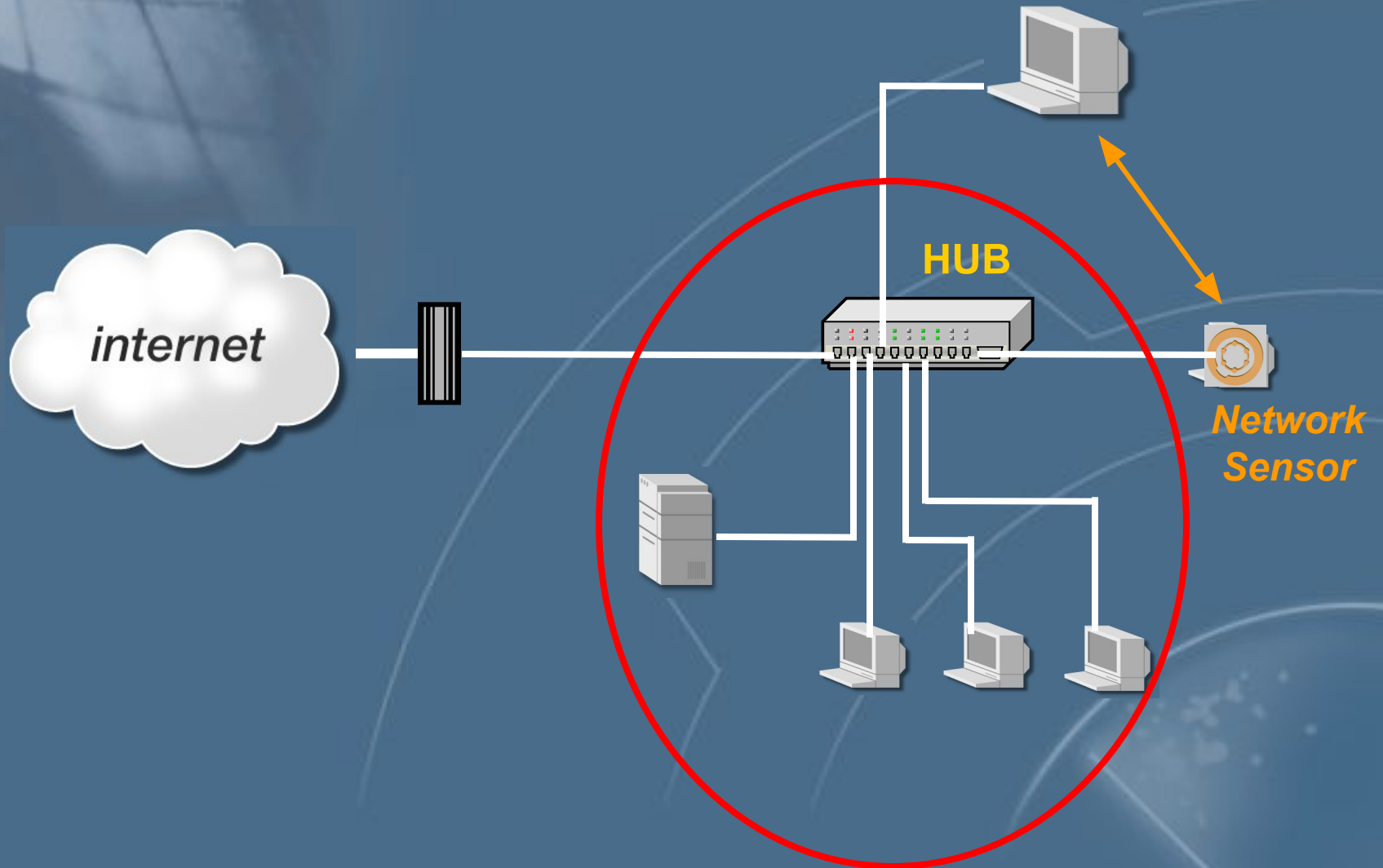


Server Sensor

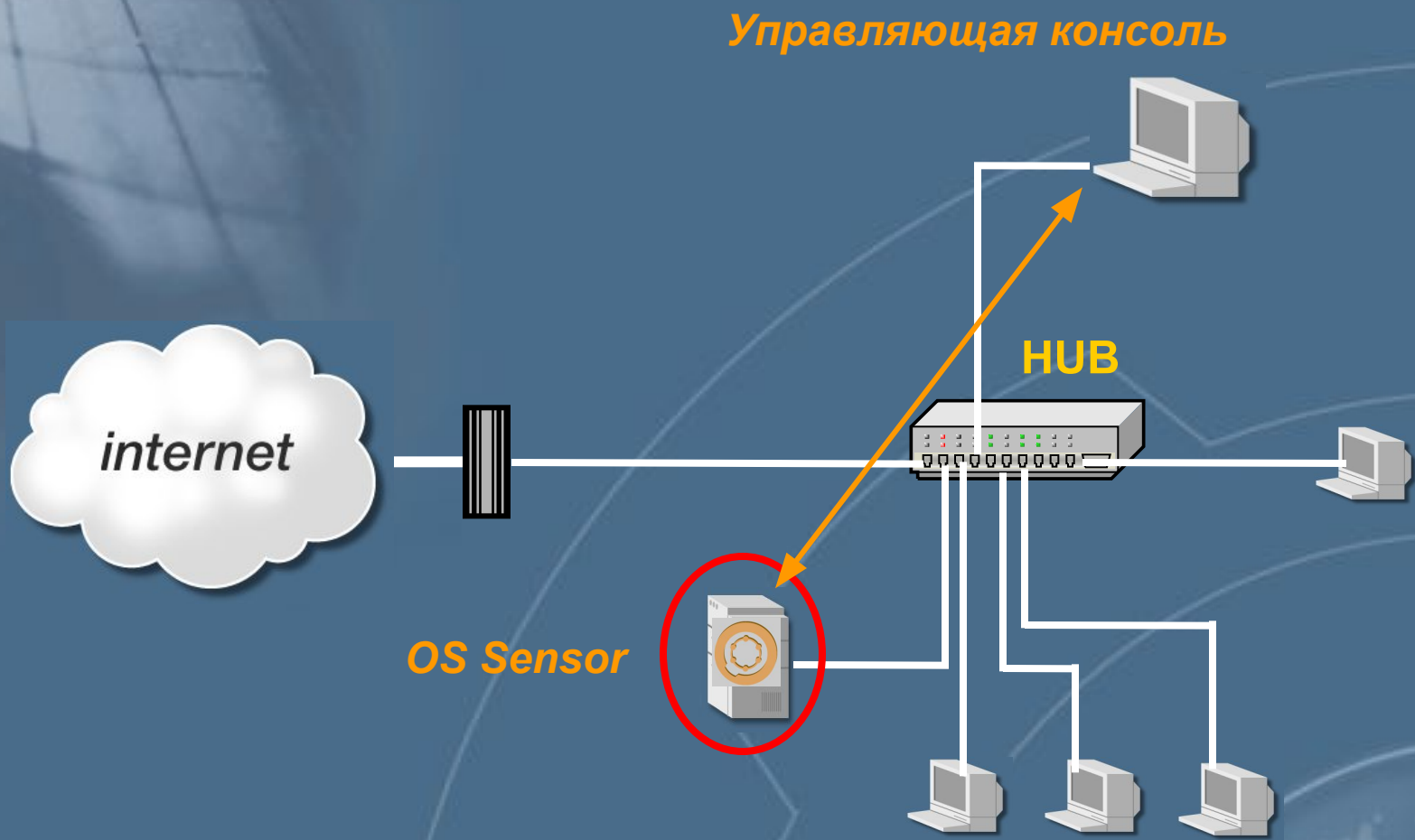


Расположение сетевого модуля

Управляющая консоль

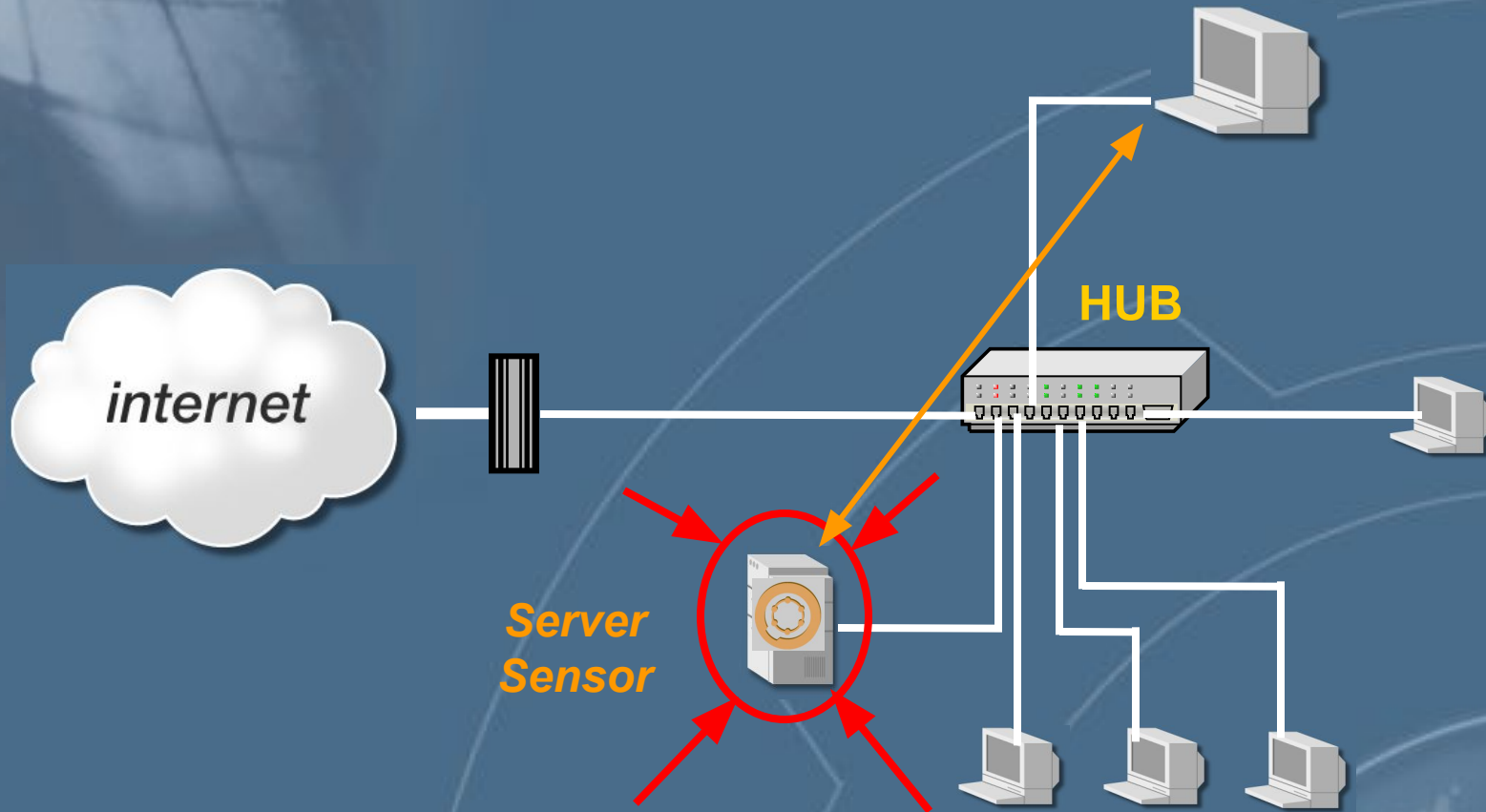


Расположение системного агента

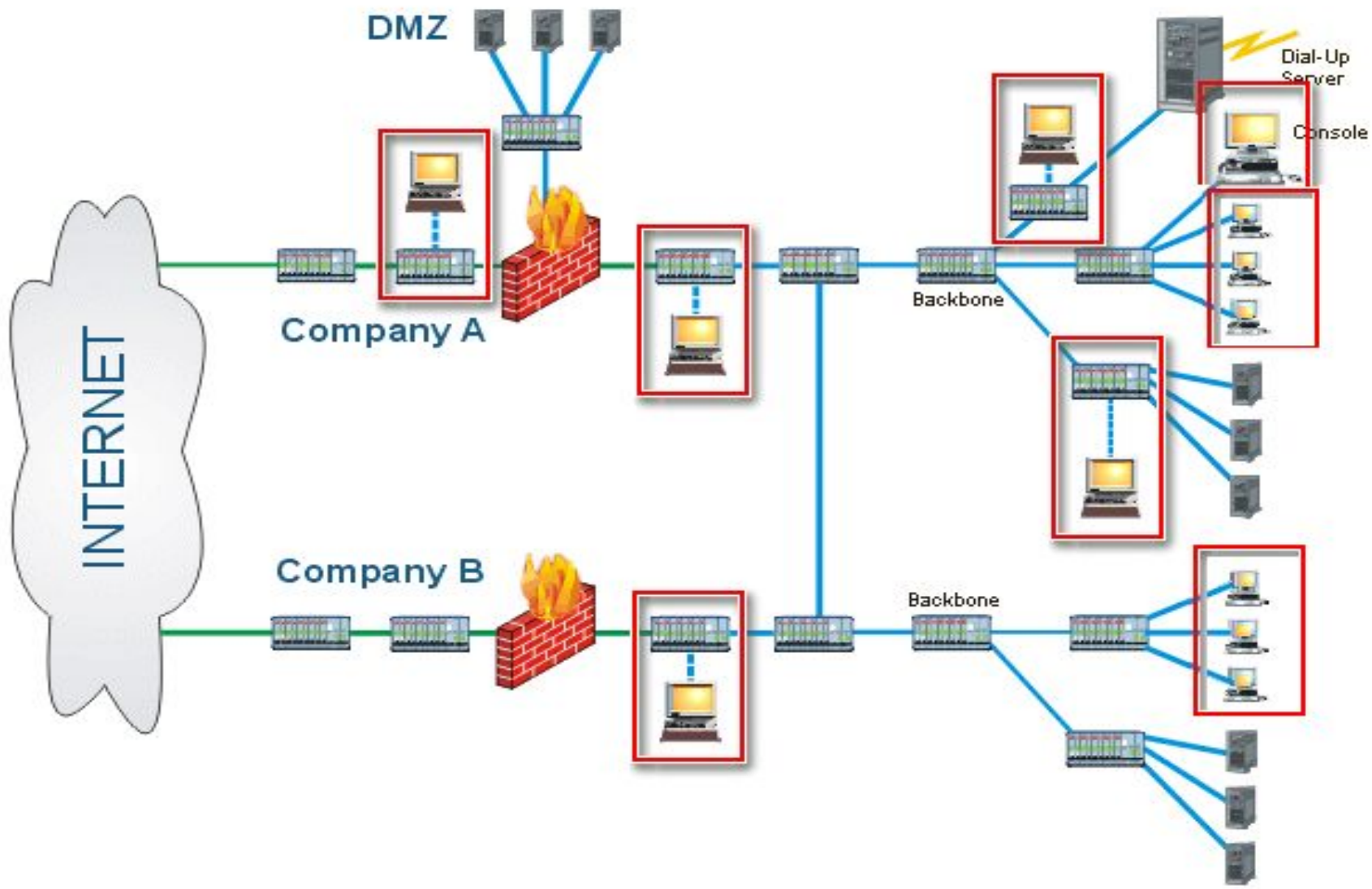


Расположение Server Sensor

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

Поддержка Ethernet, Fast Ethernet, Token Ring и FDDI

Поддержка протоколов SMB/NetBIOS и стека протоколов TCP/IP (IP, TCP, UDP, ICMP и других на их основе)

Функционирование под управлением Windows NT и Solaris

ИНФОРМЗАЩИТА

НАУЧНО-ИНЖЕНЕРНОЕ ПРЕДПРИЯТИЕ

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

Производительность

- Чем больше ОЗУ, тем эффективнее работает сетевой модуль слежения
- Чем больше в компьютере процессоров, тем эффективнее происходит анализ трафика
- В высокозагруженных сетях требуется использовать высокопроизводительные компьютеры
- Желательно запускать на выделенном компьютере

OS Sensor

Чтение записей журнала регистрации

- сравнение записей с политикой аудита
- реагирование в случае нарушений

Пользователь может:

- задавать варианты реагирования на события
- определять новые события
- контролировать неиспользуемые порты

Системный агент

Системный агент под управлением Windows NT

- Windows NT Security Log
- Windows NT Event Log
- Windows NT Application Log
- Unix Syslog
- Cisco Syslog

*Системный агент под управлением Unix
(Solaris, HP UX, AIX)*

- *локальный Syslog*
- *удаленный Syslog*
- *Cisco Syslog*
- *BSM log*

OS Sensor

Особенности:

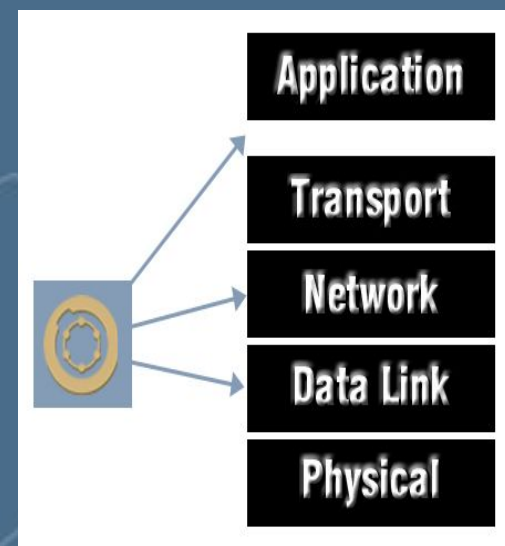
- *контроль конкретного компьютера*
- *обнаружение атак уровня ОС*
- *работают в коммутируемых сетях*
- *последующий анализ данных*

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

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

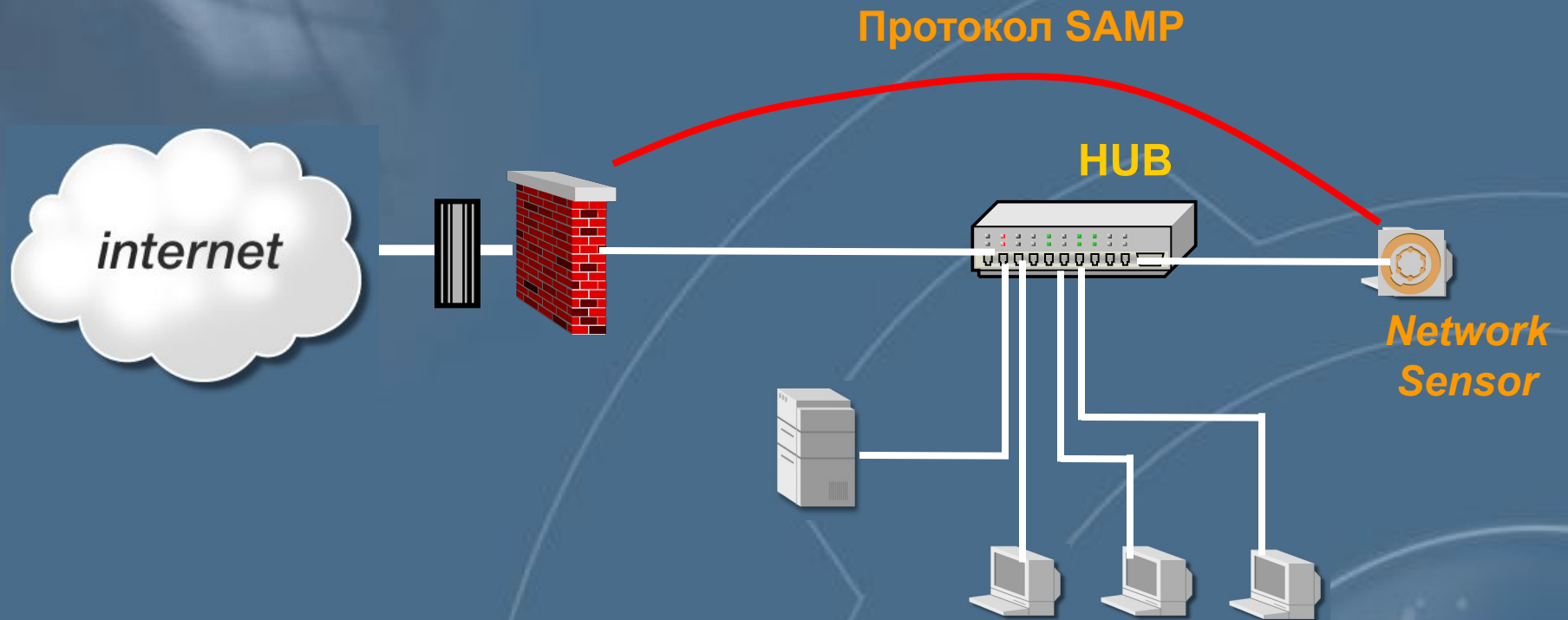
RealSecure Manager

- Management Console
 - Windows NT
- RealSecure Manager for HP OpenView v1.3
 - Windows NT
 - Solaris SPARC
- RealSecure Manager for Tivoli v1.3
 - Windows NT
 - Solaris SPARC
- RealSecure Management SDK v1.1

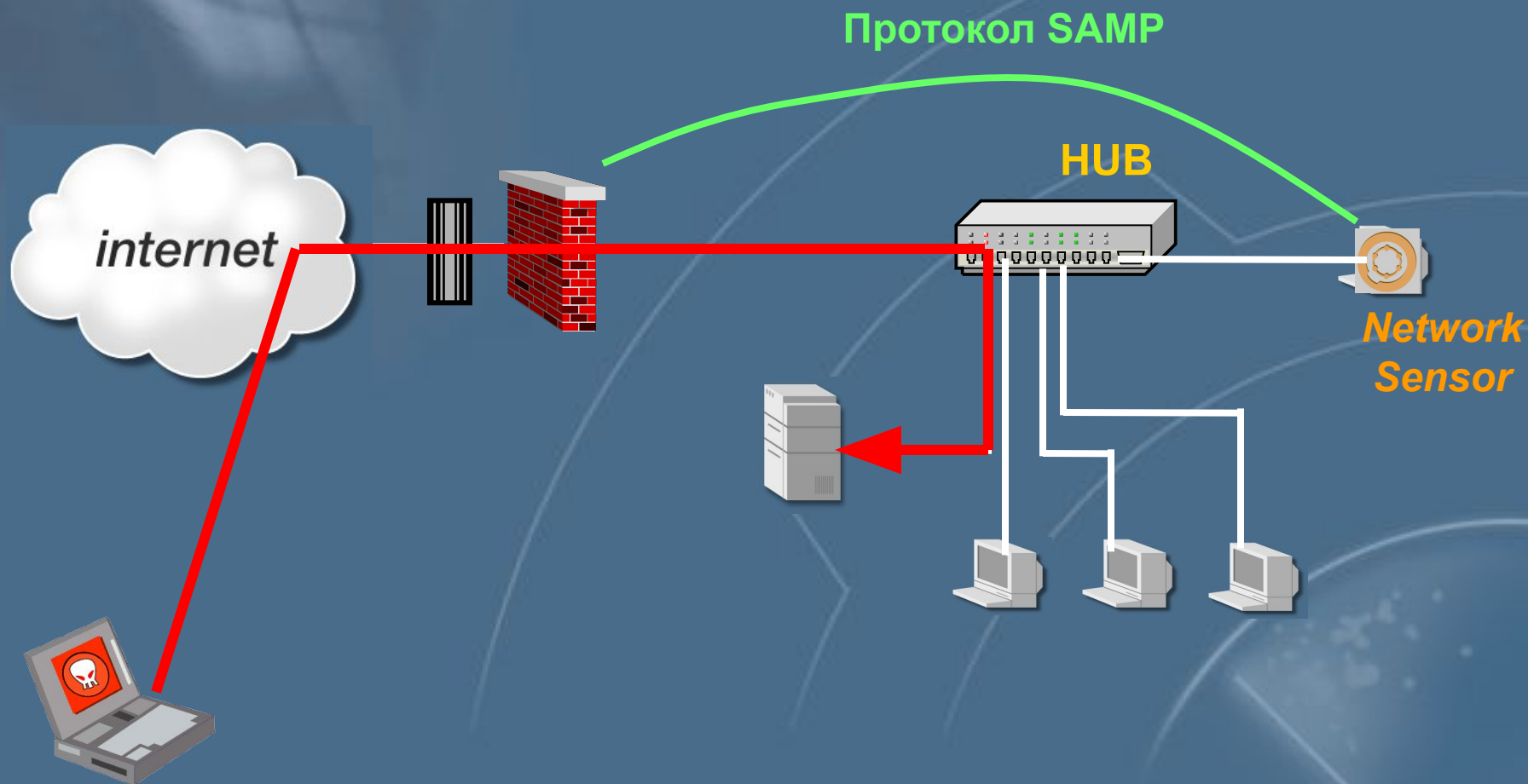
Концепция OPSec

- 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

