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 slide are several thin, white, curved lines that represent a network or data flow. The main title is centered in the upper half of the slide.

# Обнаружение сетевых атак

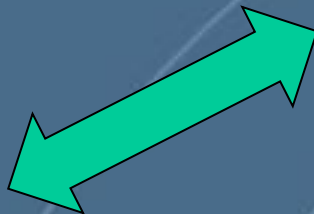
Раздел 2 – Тема 14

# Средства защиты сетей

- МЭ
- Средства анализа защищённости
- Средства обнаружения атак

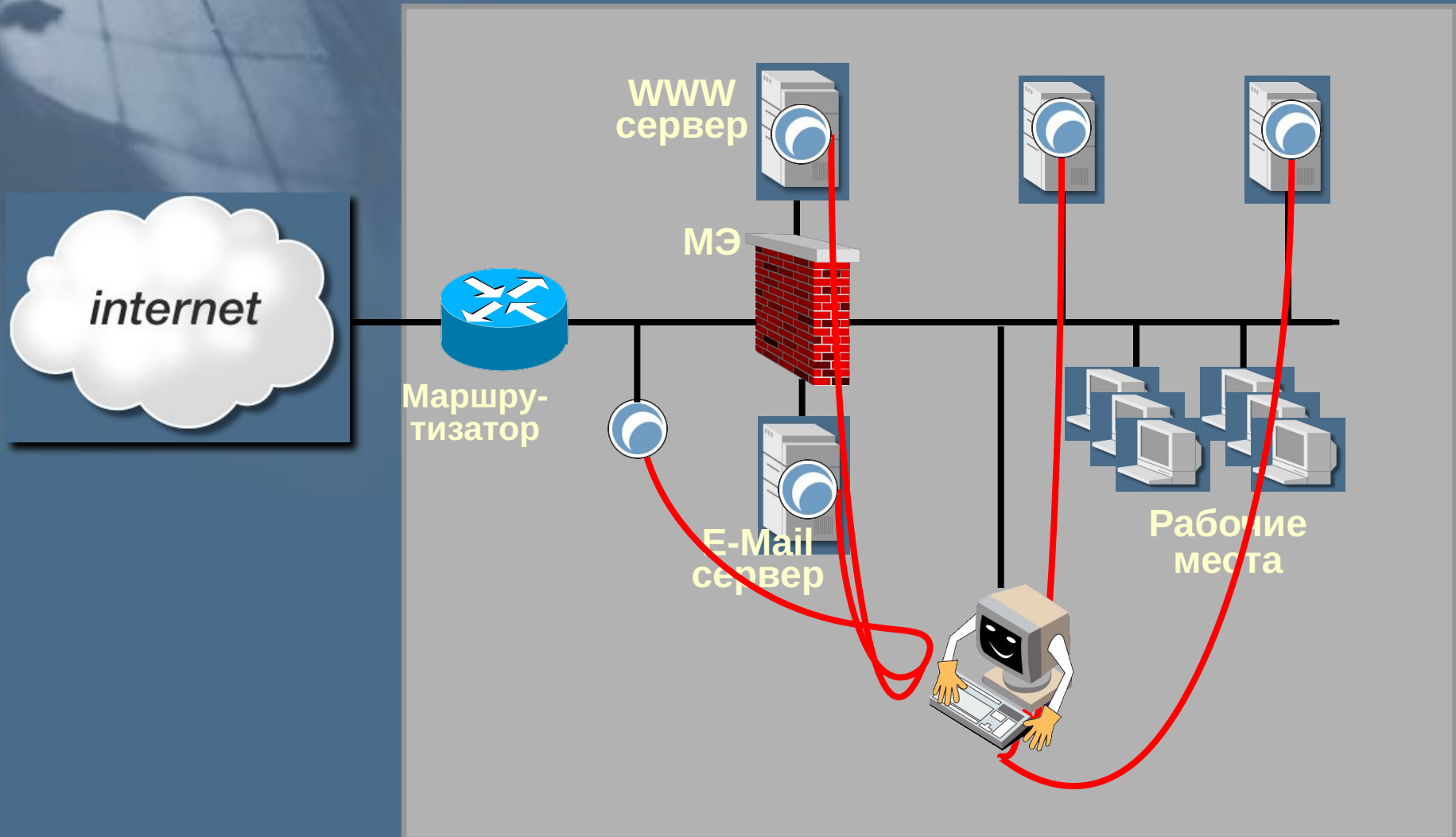
# Архитектура систем обнаружения атак

Модуль  
управления



Модуль  
слежения

# Архитектура систем обнаружения атак

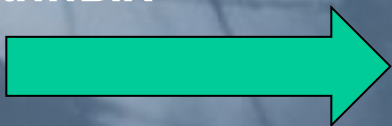


# Архитектура модуля слежения



# Классификация систем обнаружения атак

Источники  
данных



- Системы на базе узла
- Системы на базе сегмента

Уровень приложений

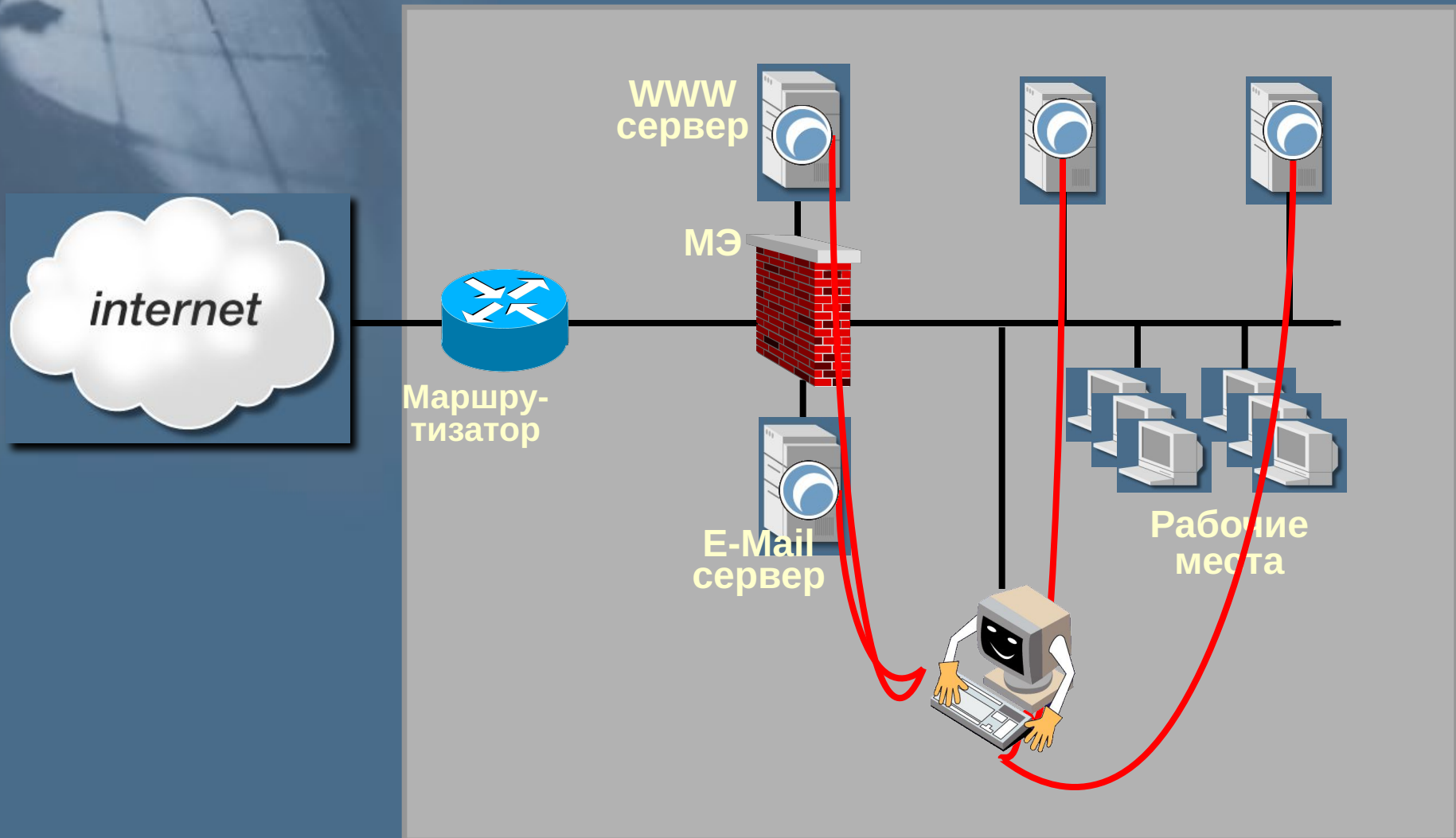
Уровень СУБД

Уровень ОС

Уровень сети

По источнику данных (принципу реализации)

# Системы обнаружения атак на базе узла



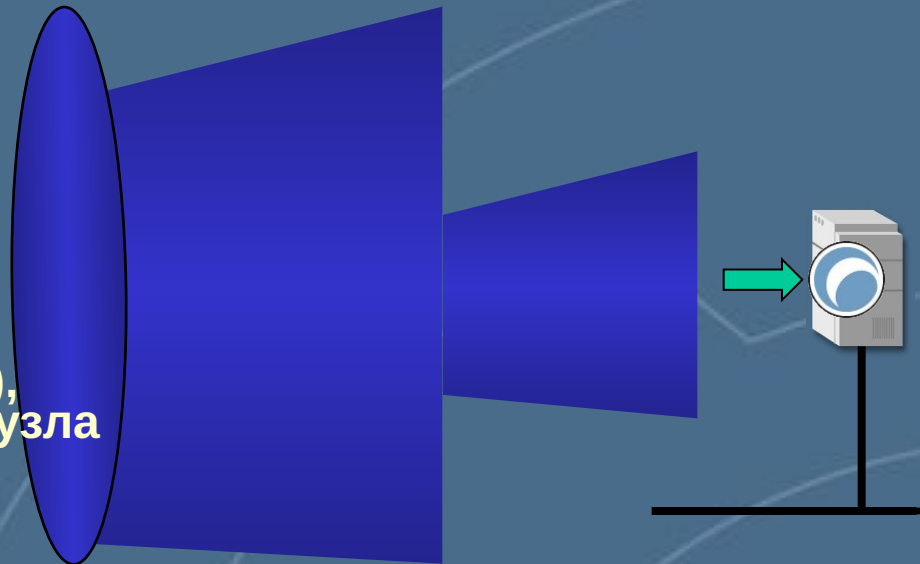
# Системы обнаружения атак на базе узла

Источники данных:

- Журналы аудита
- Действия пользователей

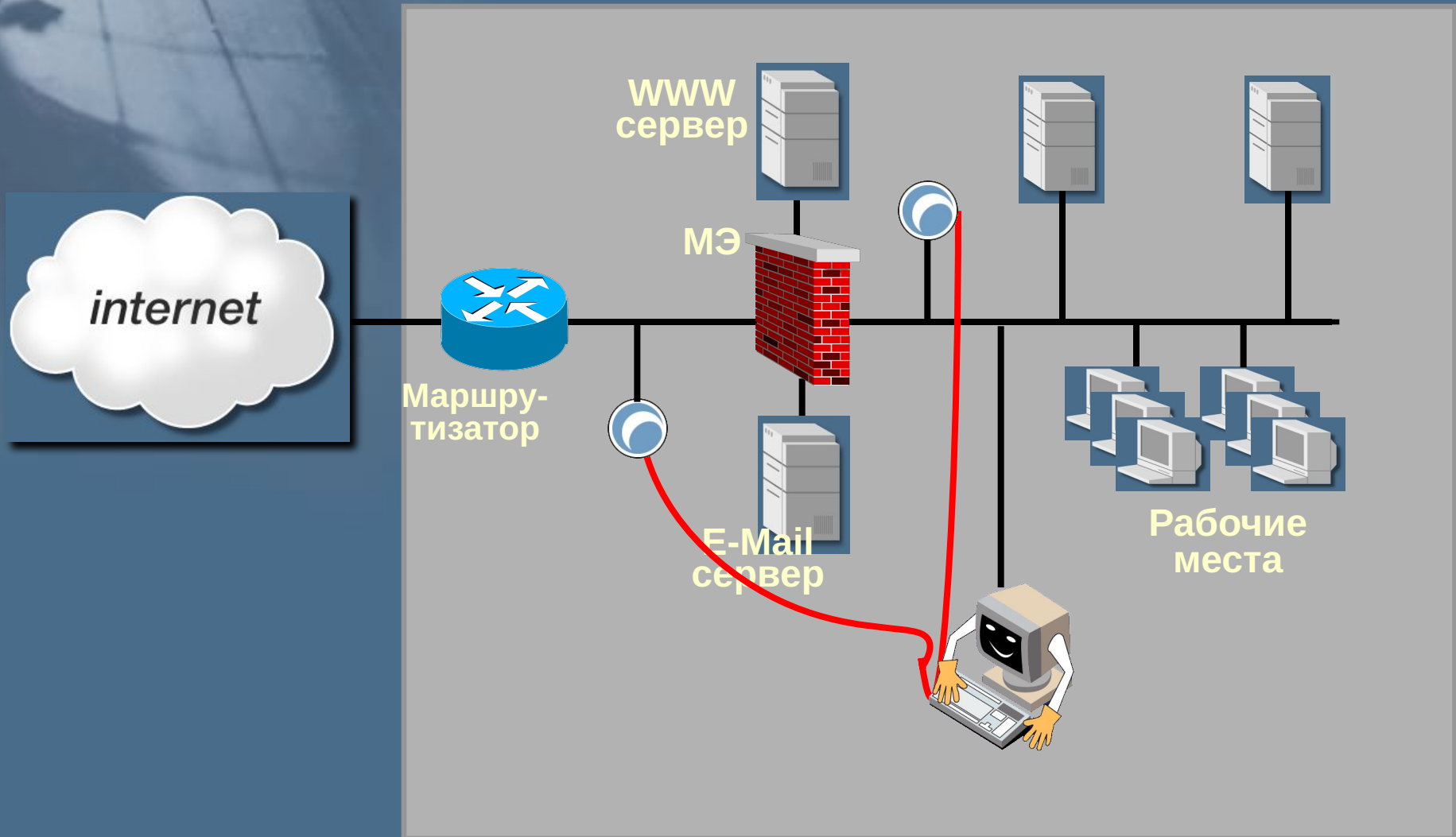
**Необязательно:**

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





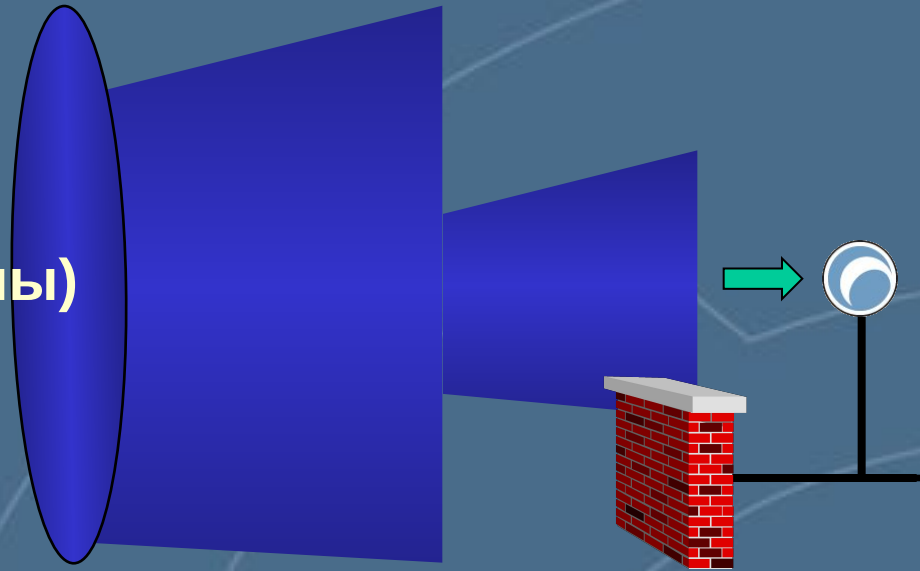
# Системы обнаружения атак на базе сети



# Системы обнаружения атак на базе сети

Источник данных:

- Сетевые пакеты (фреймы)



# Классификация систем обнаружения атак

Алгоритм (технология)  
обнаружения

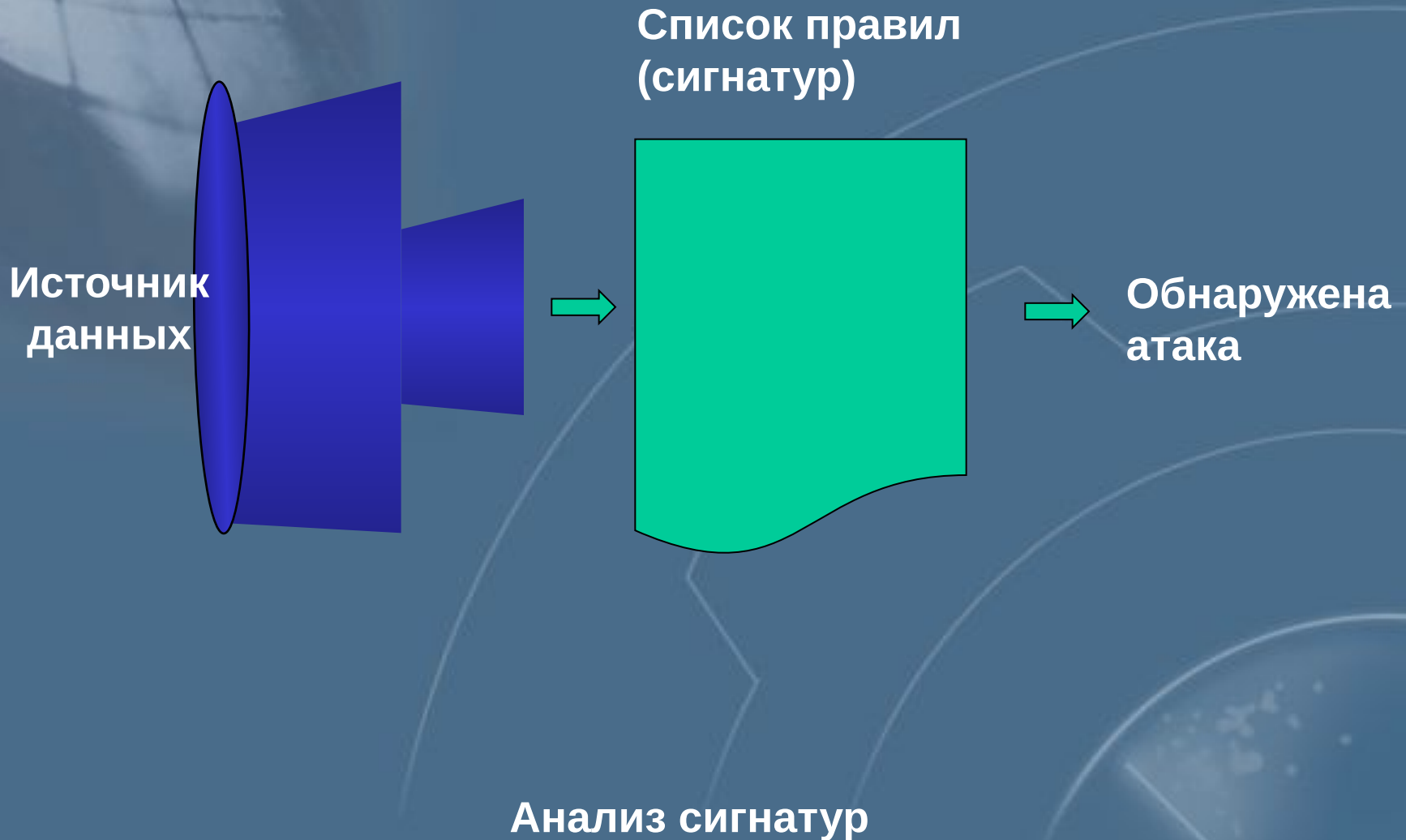


Обнаружение аномалий

Обнаружение злоупотреблений

По технологии обнаружения

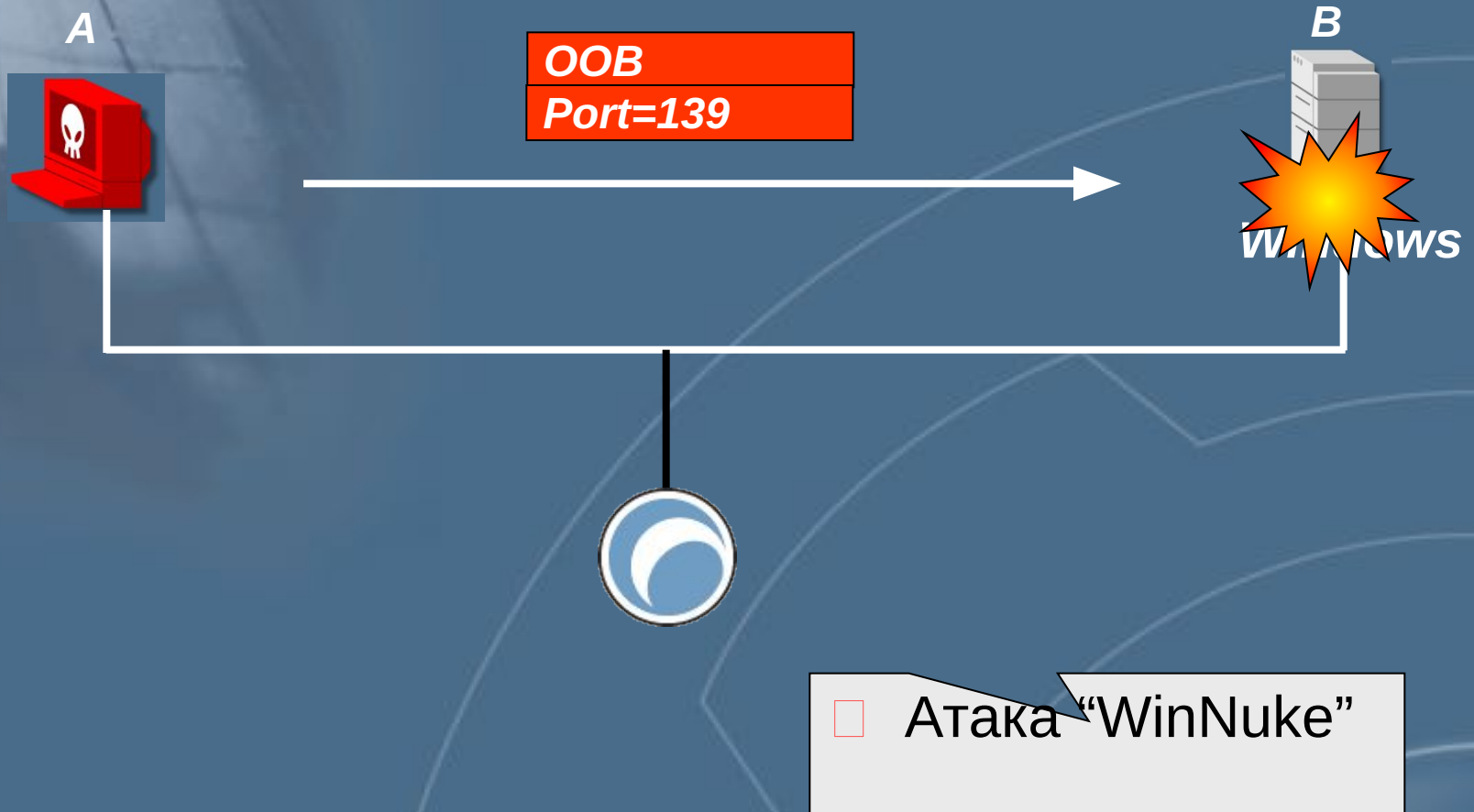
# Обнаружение злоупотреблений



# Сигнатуры для сетевых IDS

- Синтаксический разбор отдельных пакетов (Packet grepping signature)
- Анализ протоколов (protocol analysis signature)
- Анализ протоколов с учётом состояния (stateful protocol analysis signature)

# Анализ сигнатур



Синтаксический разбор отдельных пакетов

# Анализ сигнатур

X



```
telnet ftp-server 21
220 edu-main2k Microsoft FTP Service (Version 5.0).
USER ftp
331 Anonymous access allowed, send identity (e-mail name) as password.
PASS www@
230 Anonymous user logged in.
SITE EXEC
.....
```

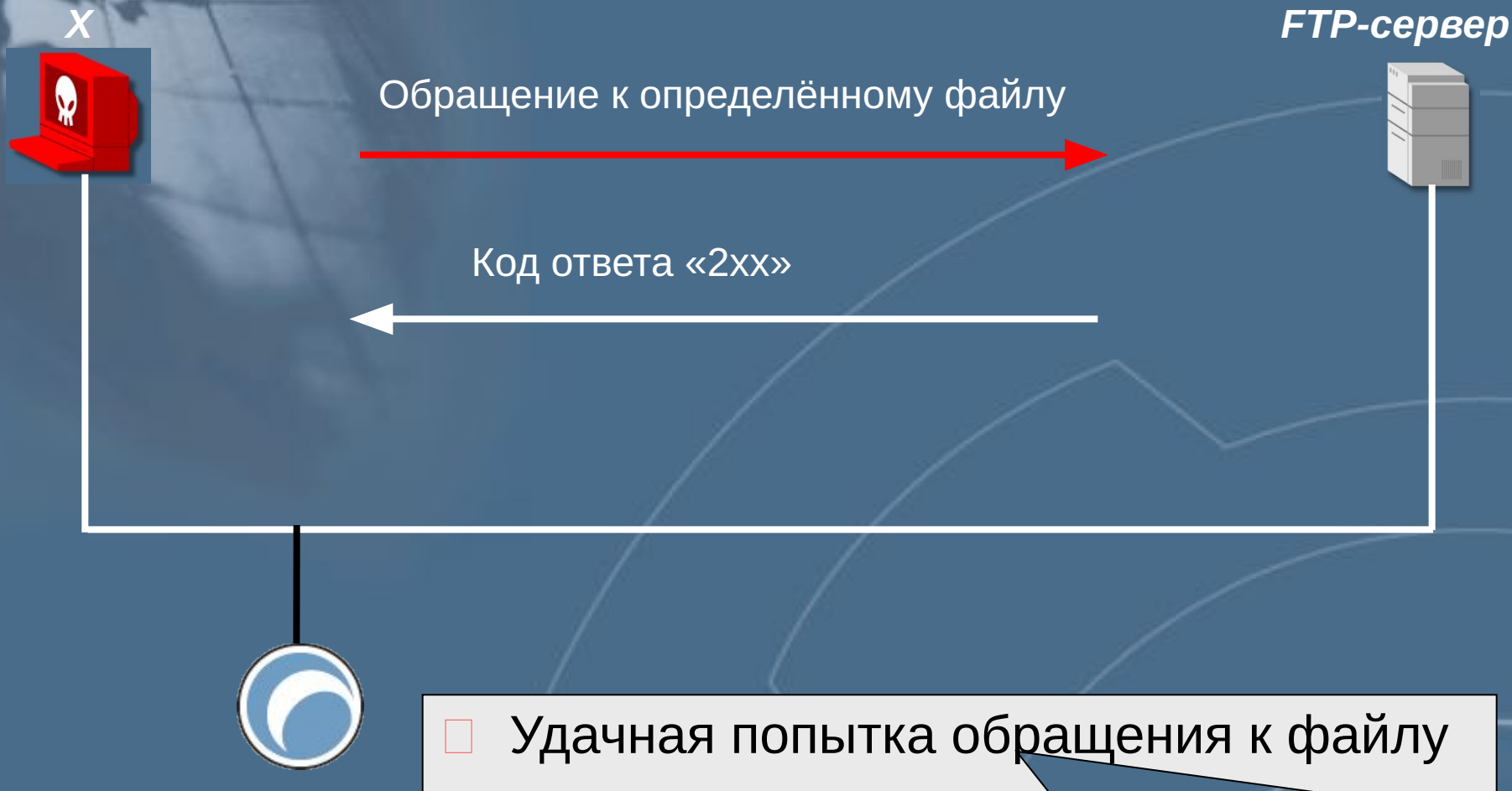
FTP-сервер



Атака "FTP\_SITE\_EXEC"

Анализ протоколов

# Анализ сигнатур



Анализ протоколов с учётом состояния  
(сопоставление запросов и ответов)



# Анализ сигнатур



SYN	Узел А
SYN	Узел А
SYN	Узел А
SYN	Узел А
SYN	Узел А



Атака "SynFlood"

Анализ протоколов с учётом состояния  
(отслеживание количества запросов в единицу времени)

# Системы обнаружения атак

	Sourcefire IMS	Secure IDS	eTrust Intrusion Detection	RealSecur e	Snort
Производитель	Sourcefire	Cisco Systems	Computer Associates	Internet Security Systems	Net
Платформа	Unix	Защищенна я версия Solaris	Windows NT	Windows NT (2000)	Unix
Технология обнаружения	Сигна туры атак	Сигна туры атак	Сигна туры атак	Сигна туры атак	Сигна туры атак
Принцип реализации	На базе сети	На базе сети	На базе сети + ВОЗМОЖН ОСТИ МЭ	На базе сети и на базе узла	На базе сети

# Система обнаружения атак Snort



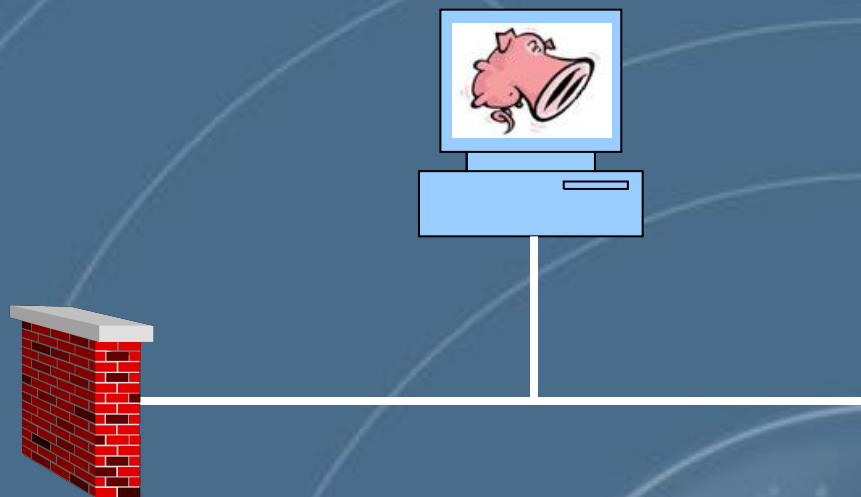
# Архитектура

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)**

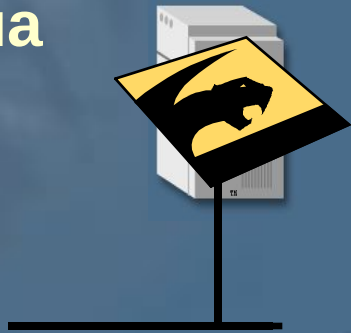


# Практическая работа 16

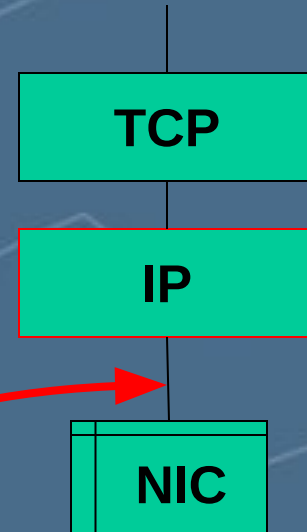
Работа с программой Snort

# Система обнаружения атак RealSecure

На базе узла



На базе сети



# Компоненты RealSecure



*Модули слежения*

*Модули управления*

*Сетевой модуль  
(Network Sensor)*

*Серверный модуль  
(Server Sensor)*

# Компоненты RealSecure



*Модули слежения*

*Модули управления*

*Workgroup  
Manager*

*Sensor  
Manager*

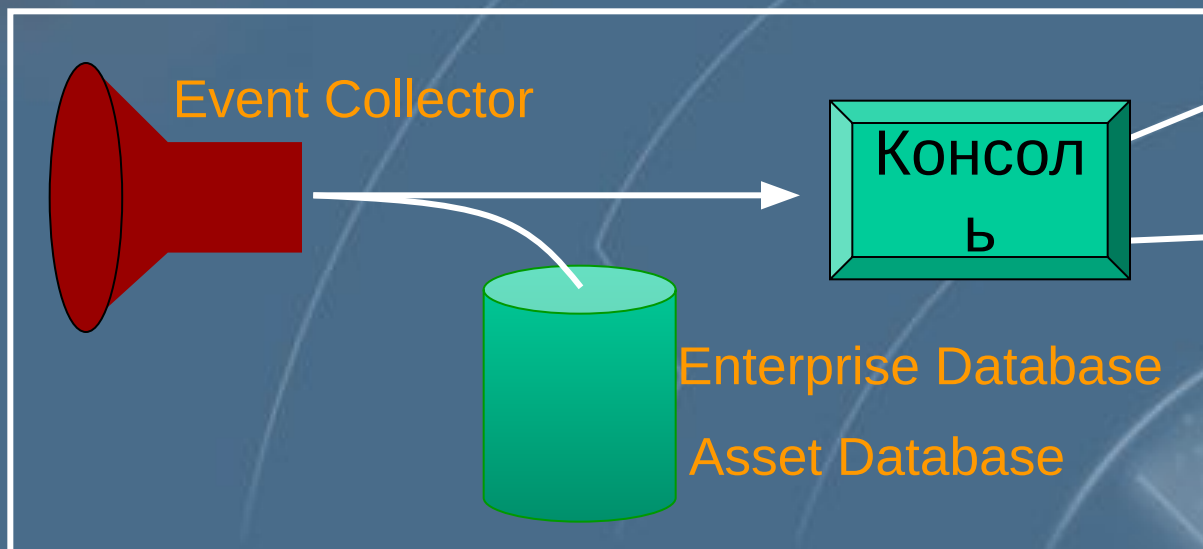
*Командная  
строка*

*Site Protector*

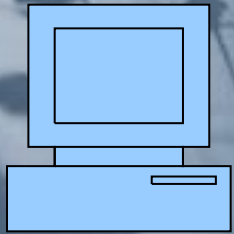
# Компоненты RealSecure

## Workgroup Manager

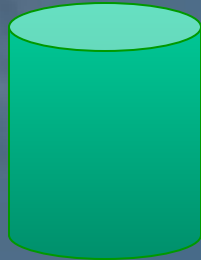
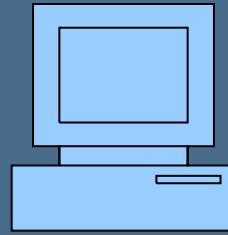
- *Event Collector*
- *Enterprise Database*
- *Asset Database*
- *Console*



# Трёхуровневая архитектура



*Консоли*

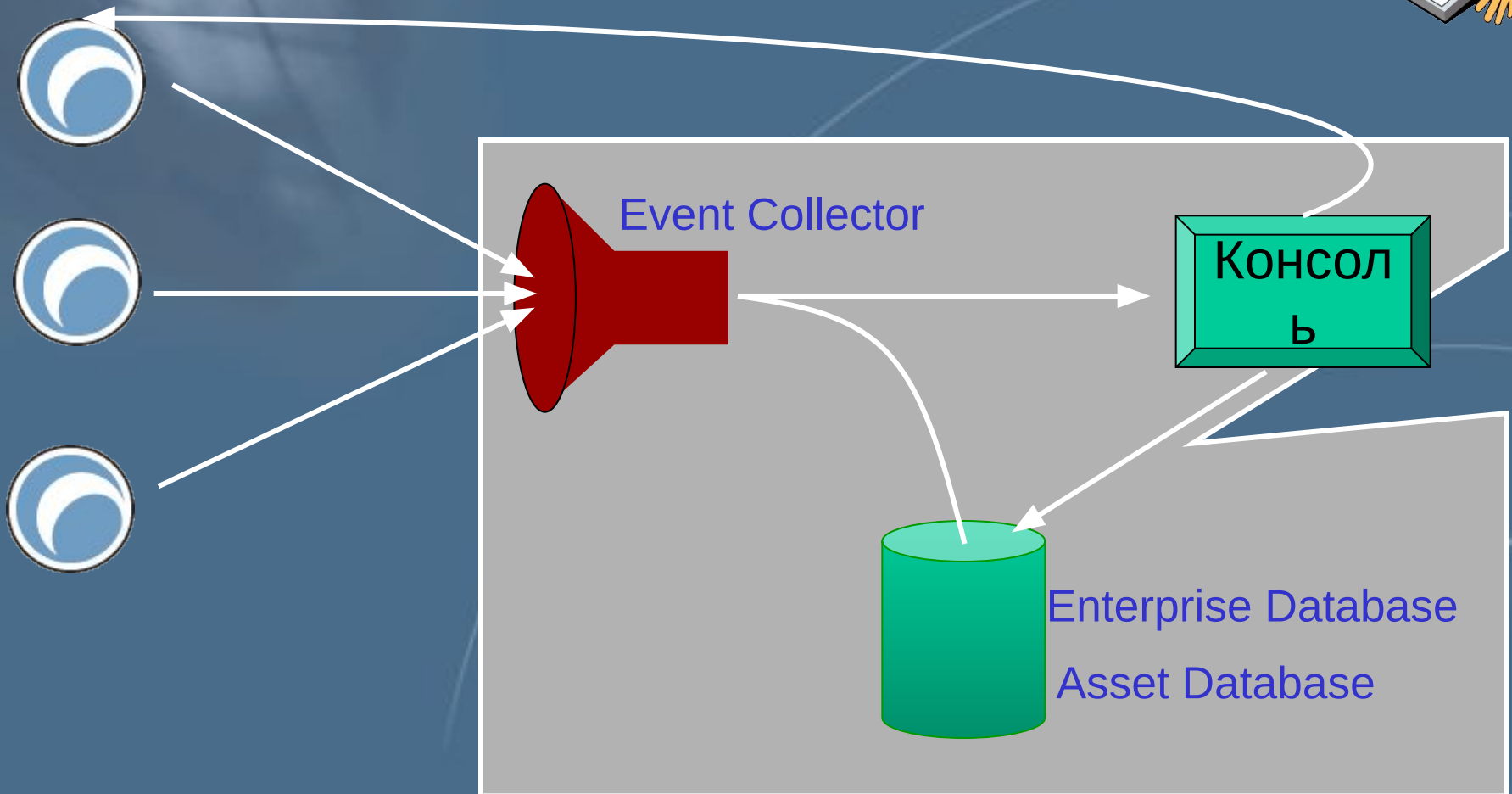


*Компонент, отвечающий за сбор событий с сенсоров*

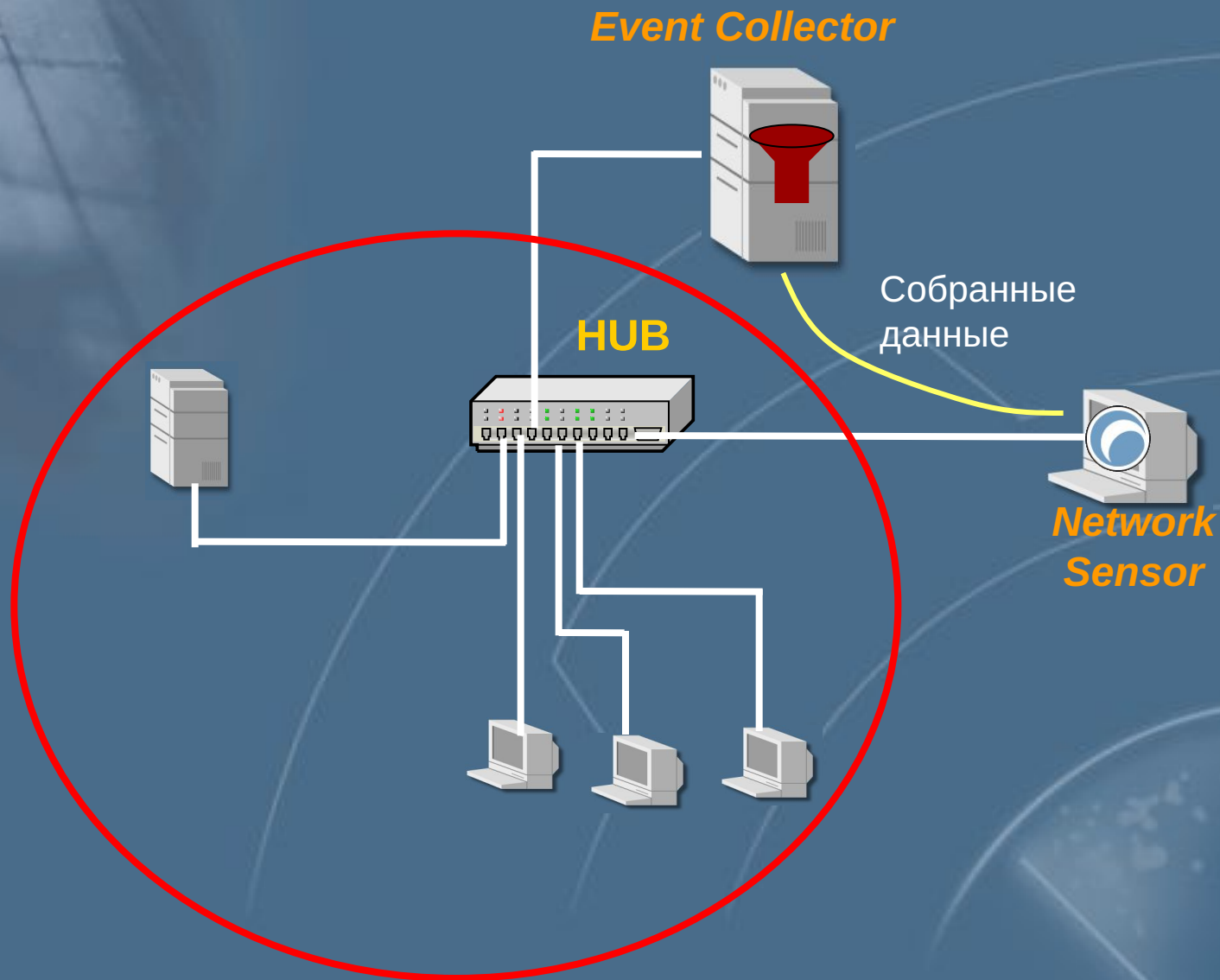


*Модули слежения*

# Взаимодействие компонентов RealSecure



# Расположение сетевого модуля слежения





# Механизмы реагирования RealSecure

*Разрыв соединения*

*Реконфигурация межсетевого экрана*

*Выполнение программы, определённой пользователем*

*Отправка сообщения*

*На консоль*

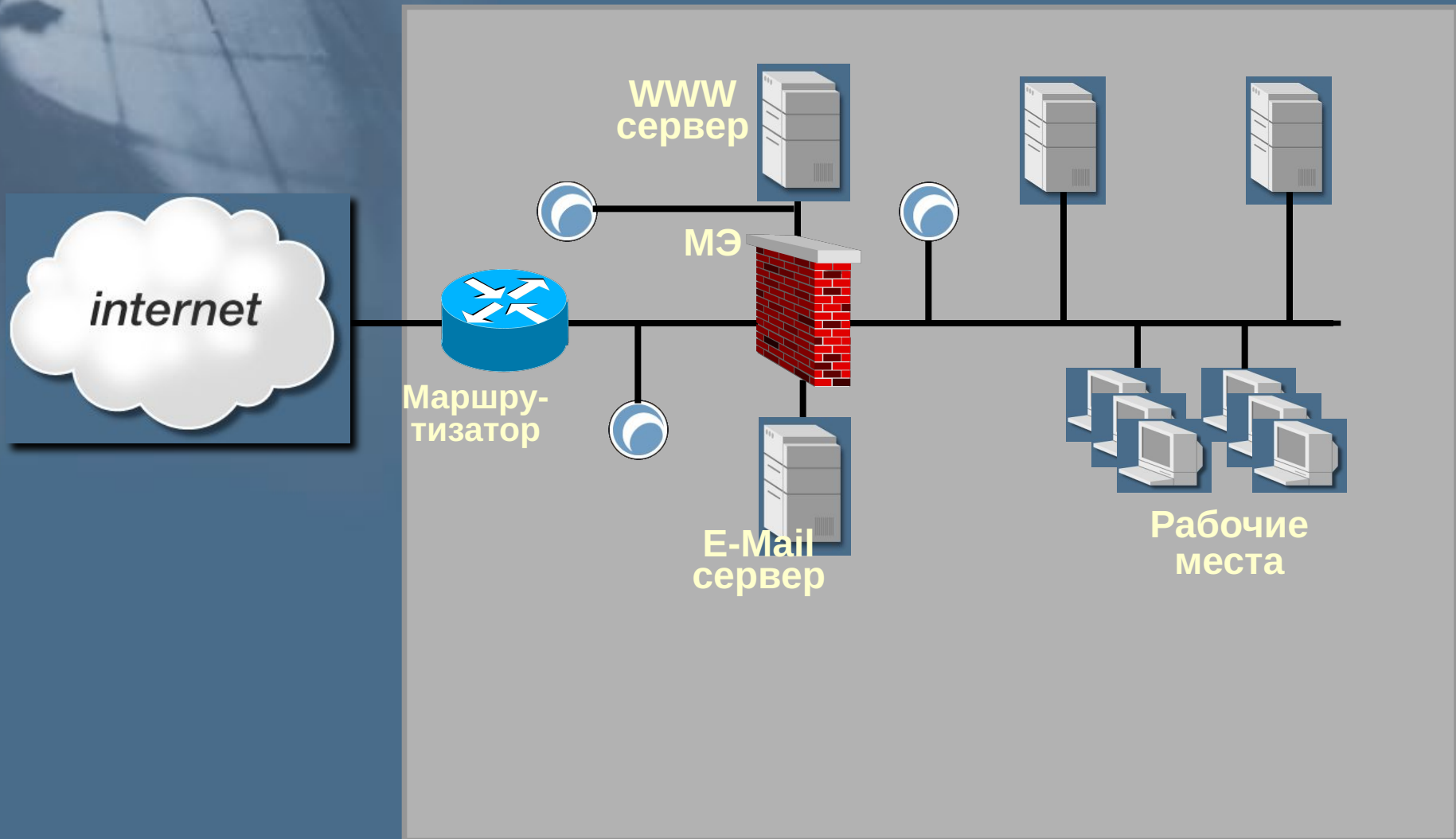
*По протоколу SNMP*

*По E-mail*

*Регистрация события в БД*

*Расширенная регистрация с возможностью последующего воспроизведения сессии прикладного уровня*

# Размещение модулей слежения



# Практическая работа 16

Работа с программой RealSecure

# Обнаружение атак и МЭ

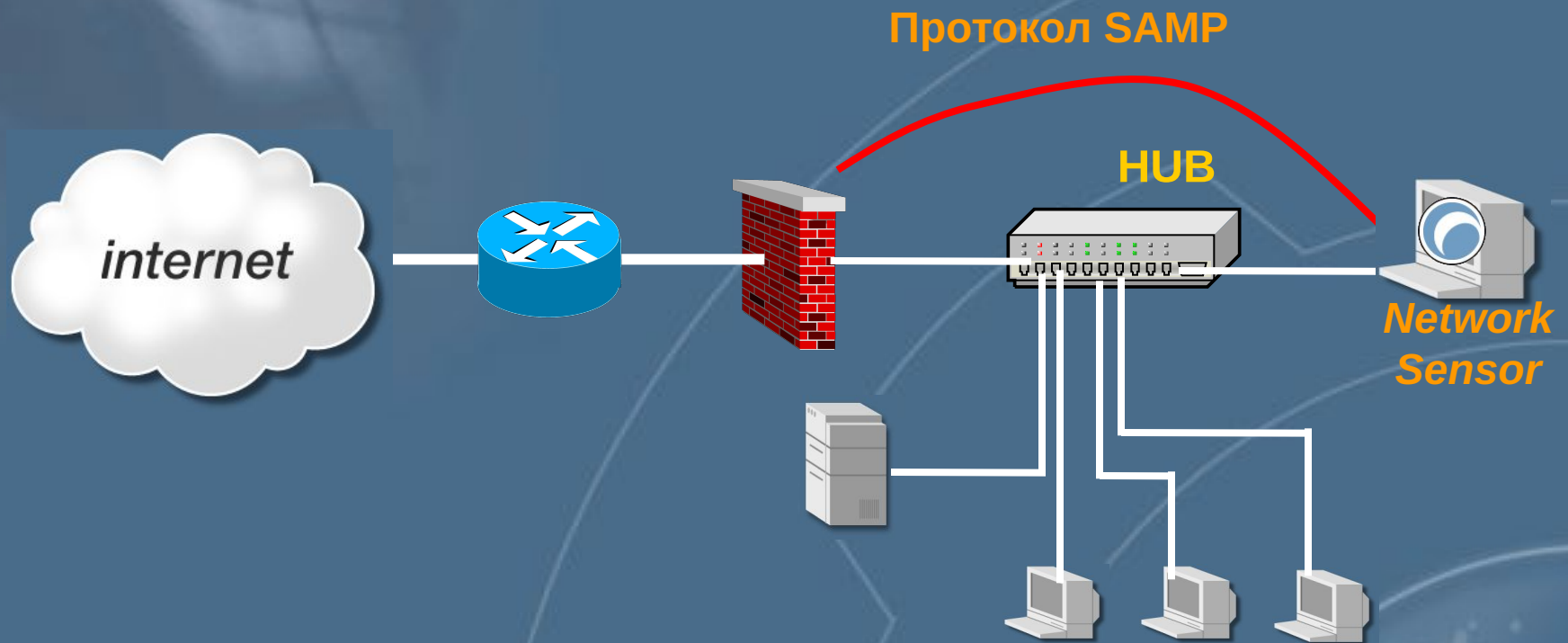


Концепция OPSec

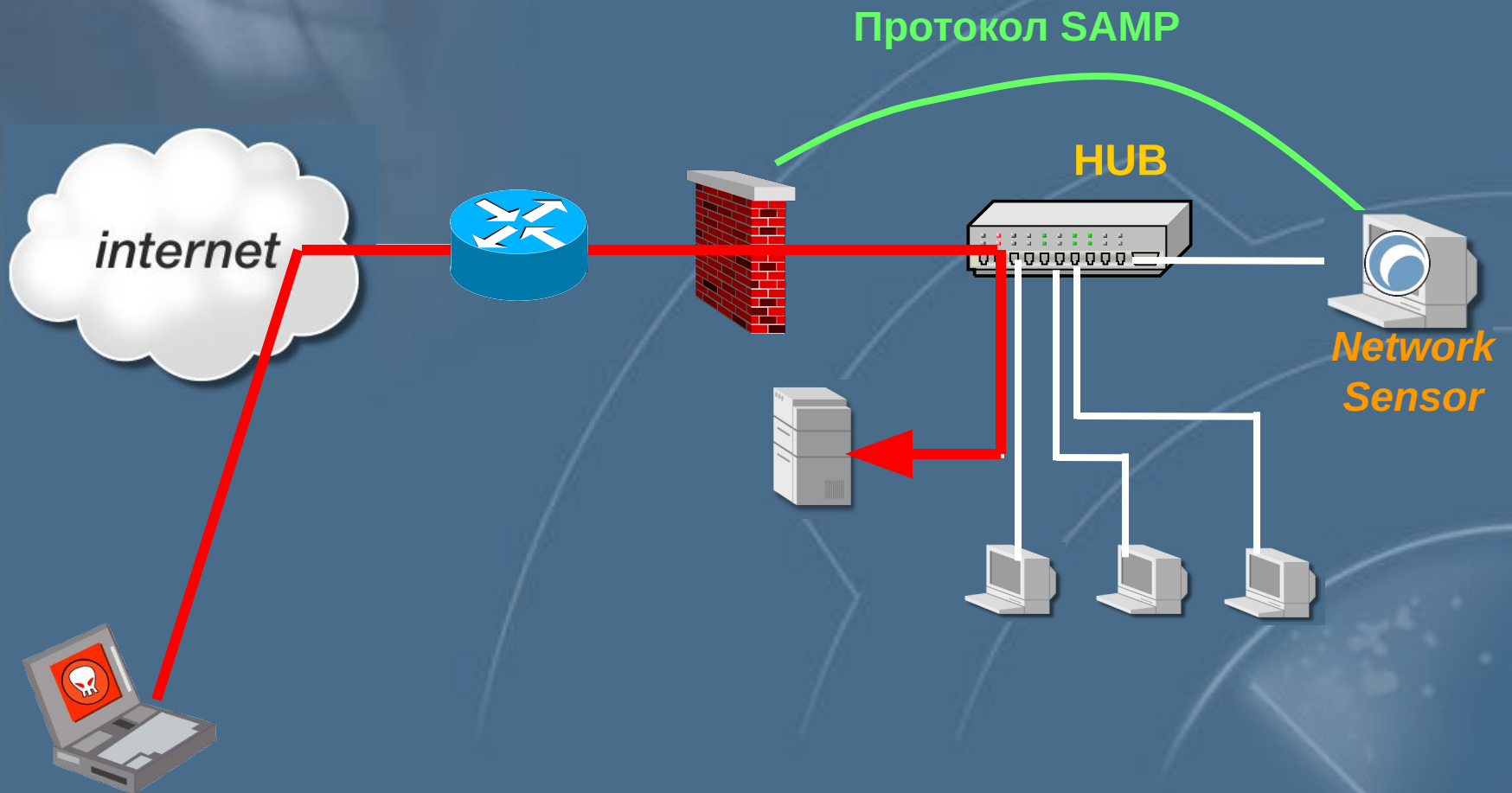
# Концепция OPSec

- OPSec SDK (набор необходимых API)
- Открытые протоколы
  - CVP(Content Vectoring Protocol)
  - UFP (URL Filter Protocol)
  - **SAMP (Suspicious Activity Monitoring Protocol)**
- Язык INSPECT

# Реконфигурация МЭ



# Реконфигурация МЭ



# Реконфигурация МЭ

