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 blue background are several thin, white, curved lines that form abstract geometric shapes, possibly representing orbits or data paths.

Средства анализа защищённости

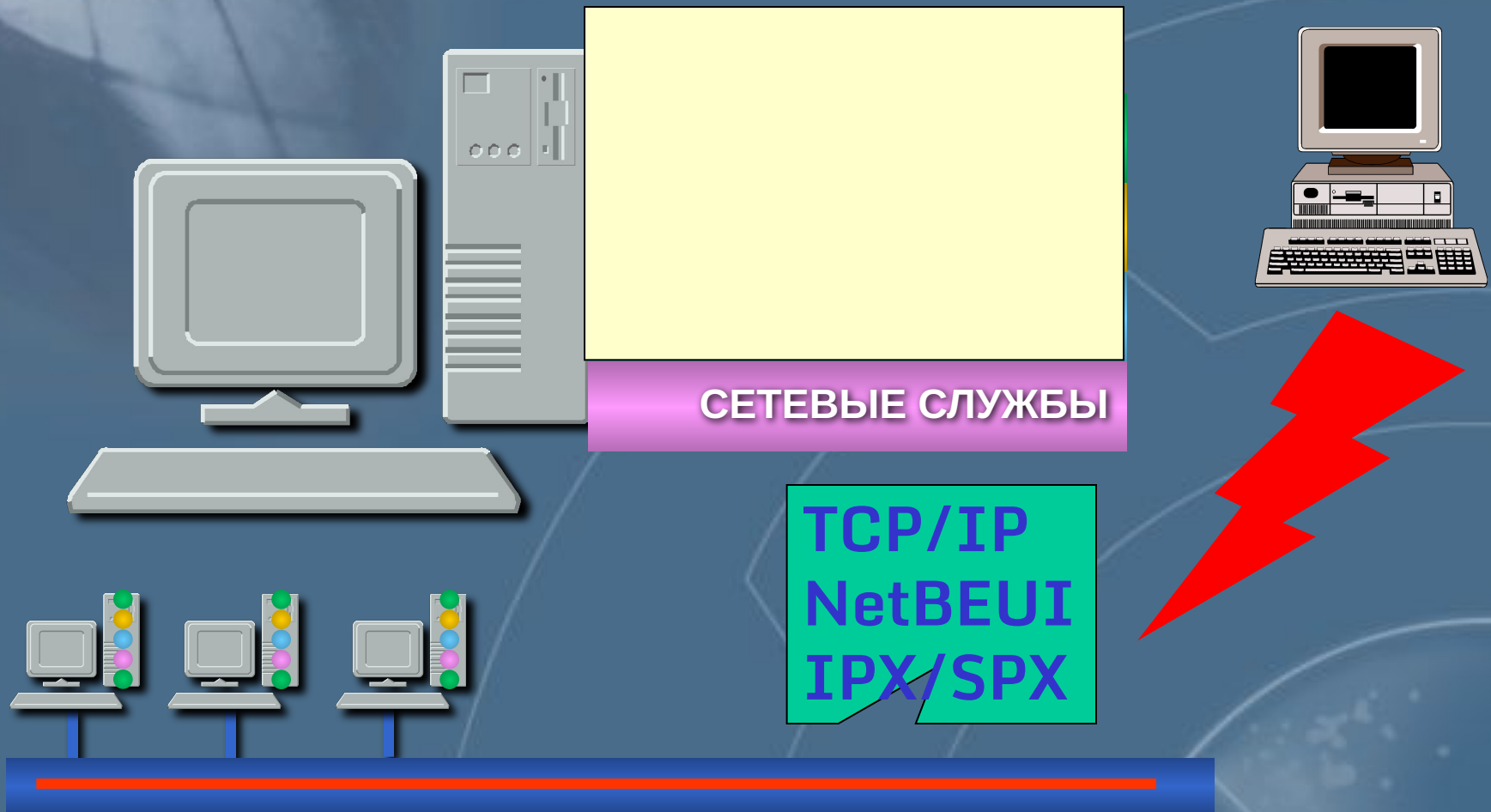
Раздел 2 – Тема 12

Средства защиты сетей

- МЭ
- Средства анализа защищённости
- Средства обнаружения атак

Одна из составляющих комплекса средств сетевой безопасности

Анализ защищенности на уровне сети



Средства анализа защищённости

| | | | | | | | | |
|--|---------------------------|---------------------|------------------------------|----------------------------------|--------------------------------|---------------------------|-------------|----------------------------|
| | Net Recon | HackerShield | Retina | Internet Scanner | Nessus Security Scanner | CyberCop Scanner | SARA | SAINT |
| Производитель | Axent Technologies | BindView | eEye Digital Security | Internet Security Systems | | Network Associates | | WW Digital Security |
| Платформа | Windows NT | Windows NT | Windows NT | Windows NT Workstation | Unix | Windows NT | Unix | Unix |
| Возможность обновления | + | + | + | + | + | + | - | - |
| Возможность создания собственных проверок | - | - | - | - | + | + | + | + |

Средства анализа защищённости

| | Net Recon | HackerShield | Retina | Internet Scanner | Nessus Security Scanner | CyberCop Scanner | SARA | SAINT |
|---------------------------------------|-----------|--------------|--------|------------------|-------------------------|------------------|------|-------|
| Работа из командной строки | - | - | - | + | + | + | + | + |
| Поддержка CVE | - | + | - | + | + | - | + | + |
| Автоматическое устранение уязвимостей | - | + | + | - | - | + | - | - |
| Открытость кода | - | - | - | - | + | - | + | + |
| Коммерческий или бесплатный | + | + | + | + | - | + | - | - |
| Интерфейс (по пятибалльной шкале) | 4,5 | 4 | 4 | 4,5 | 3 | 4,5 | 2 | 2 |
| Отчеты (по пятибалльной шкале) | 3,5 | 2 | 2 | 3,5 | 3,5 | 3 | 2 | 2 |

Этапы анализа защищенности на уровне сети

Сбор информации о сети

Категорирование сетевых устройств

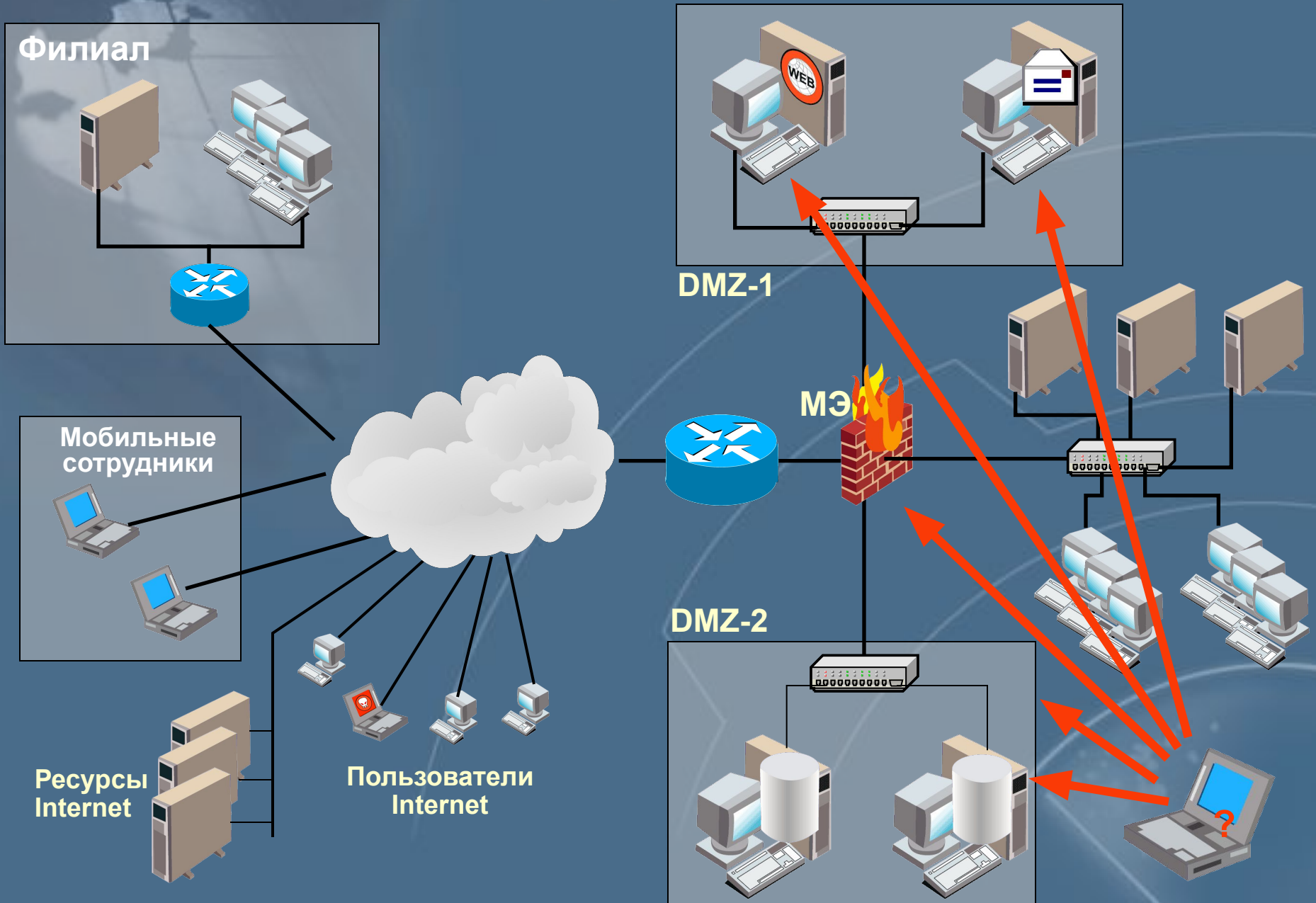
Выбор объектов сканирования и вариантов
размещения сканера (сканеров)

Выбор (разработка) политик сканирования

Составление расписания сканирования

Сканирование и анализ результатов

Сбор информации о сети



Категорирование сетевых устройств

Пример

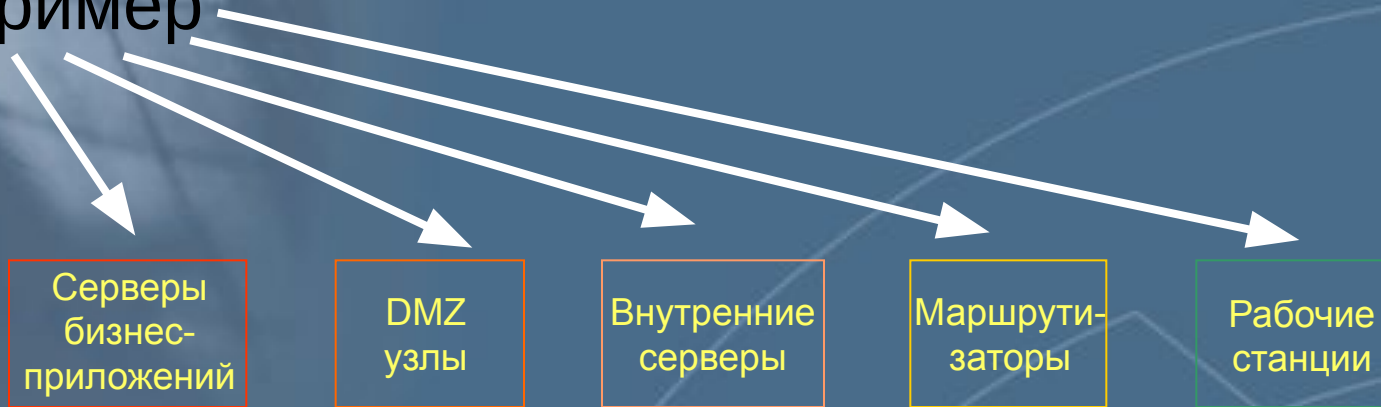
Серверы
бизнес-
приложений

DMZ
узлы

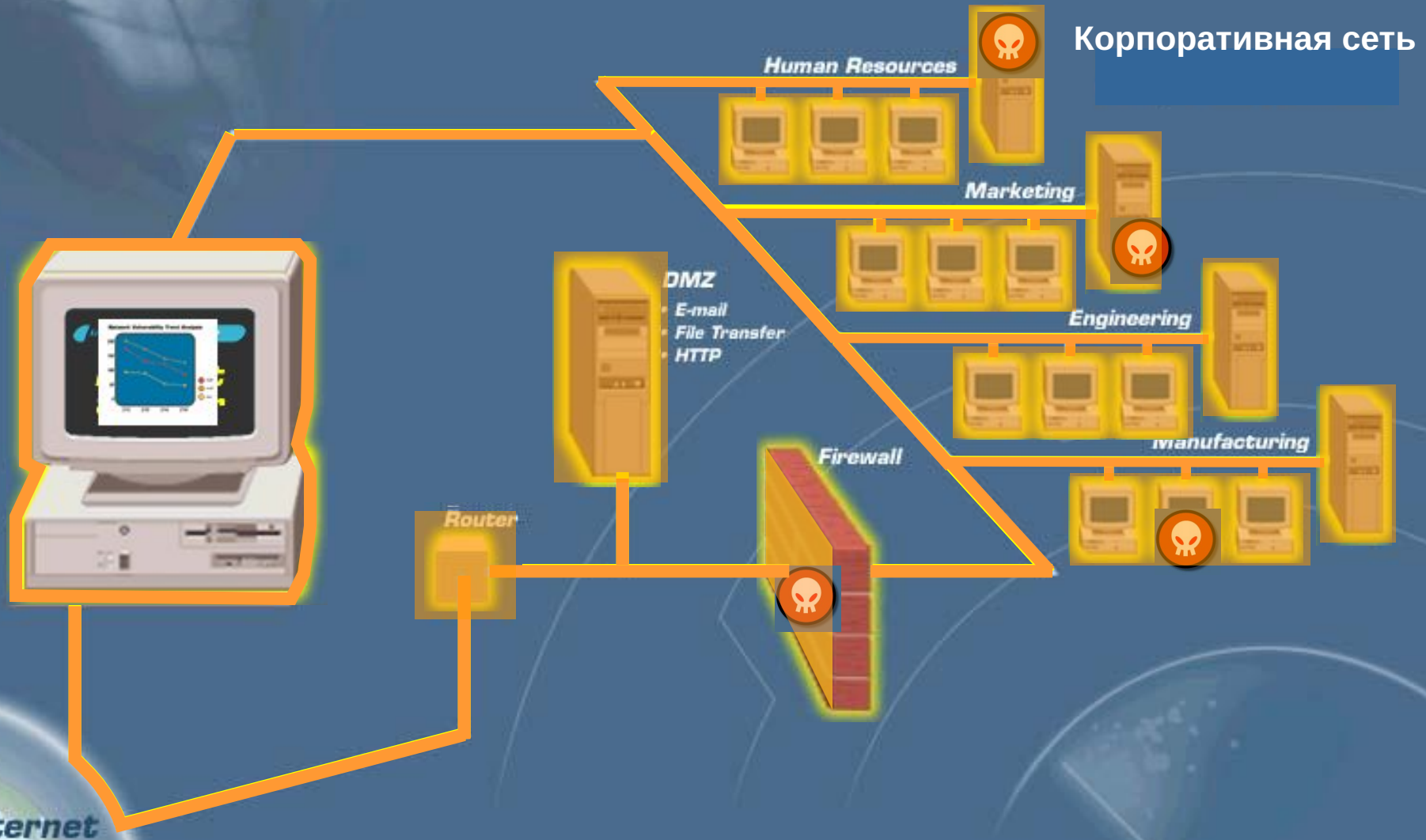
Внутренние
серверы

Маршрути-
заторы

Рабочие
станции



Выбор объектов сканирования и вариантов расположения средств анализа защищённости



Выбор политик сканирования

Политика для рабочих станций

Серверы
бизнес-
приложений

DMZ
узлы

Внутренние
серверы

Маршрути-
заторы

Рабочие
станции

Политика для критичных узлов
(максимальная защита)

Составление расписания сканирования

Сканировать в 18-00 раз в день

Серверы
бизнес-
приложений

DMZ
узлы

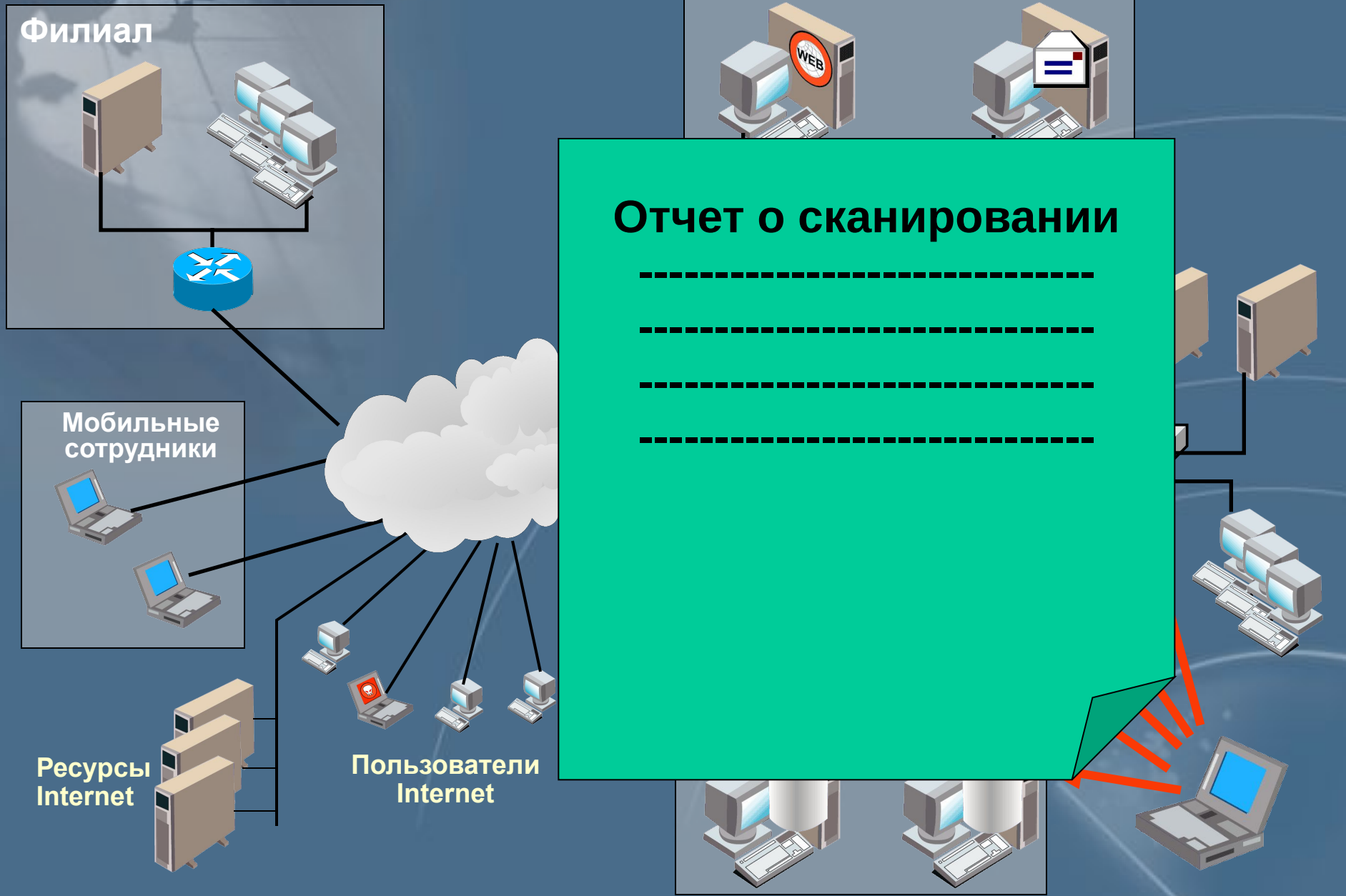
Внутренние
серверы

Маршрути-
заторы

Рабочие
станции

Сканировать в 7-00 раз в неделю

Сканирование и анализ результатов



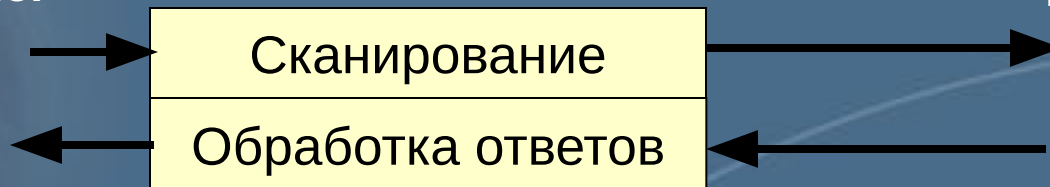
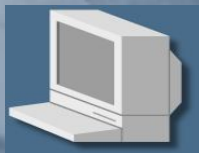
The background is a solid blue color. In the top-left corner, there is a faint, semi-transparent image of a globe showing the continents. Overlaid on the blue background are several thin, white, curved lines that suggest a network or data flow. The main text is centered in the upper half of the image.

Internet Scanner

(пример сканера сетевого уровня)

Схема работы системы Internet Scanner

Internet Scanner



Сканируемый узел



- Модуль сканирования
- Интерфейс пользователя
- Модуль генерации отчётов
- База данных проверок

Характеристики Internet Scanner

Свыше 1000 проверок

Гибкая настройка

Параллельное сканирование до 128 узлов сети

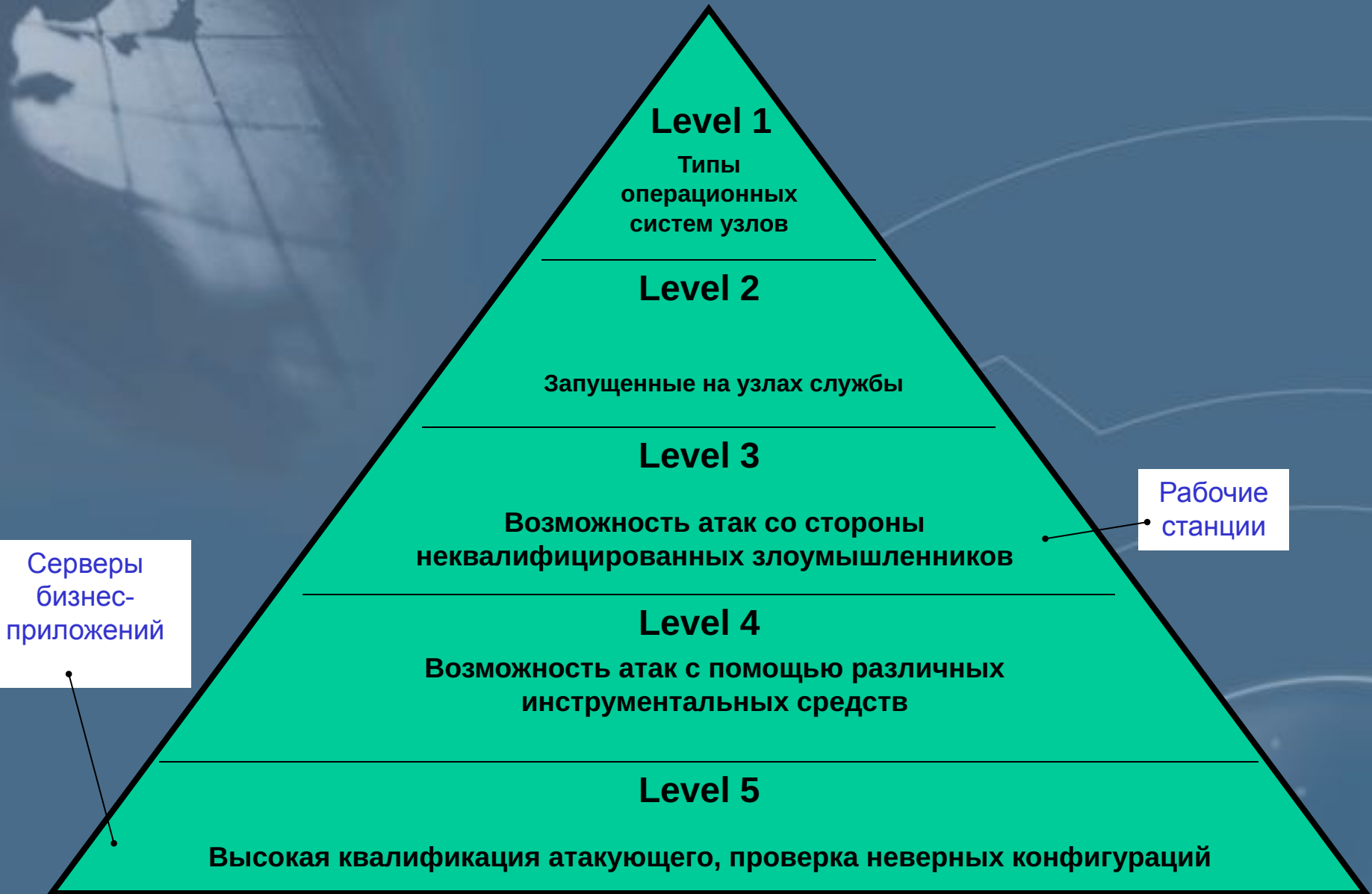
Запуск по расписанию

Работа из командной строки

Различные уровни детализации отчетов

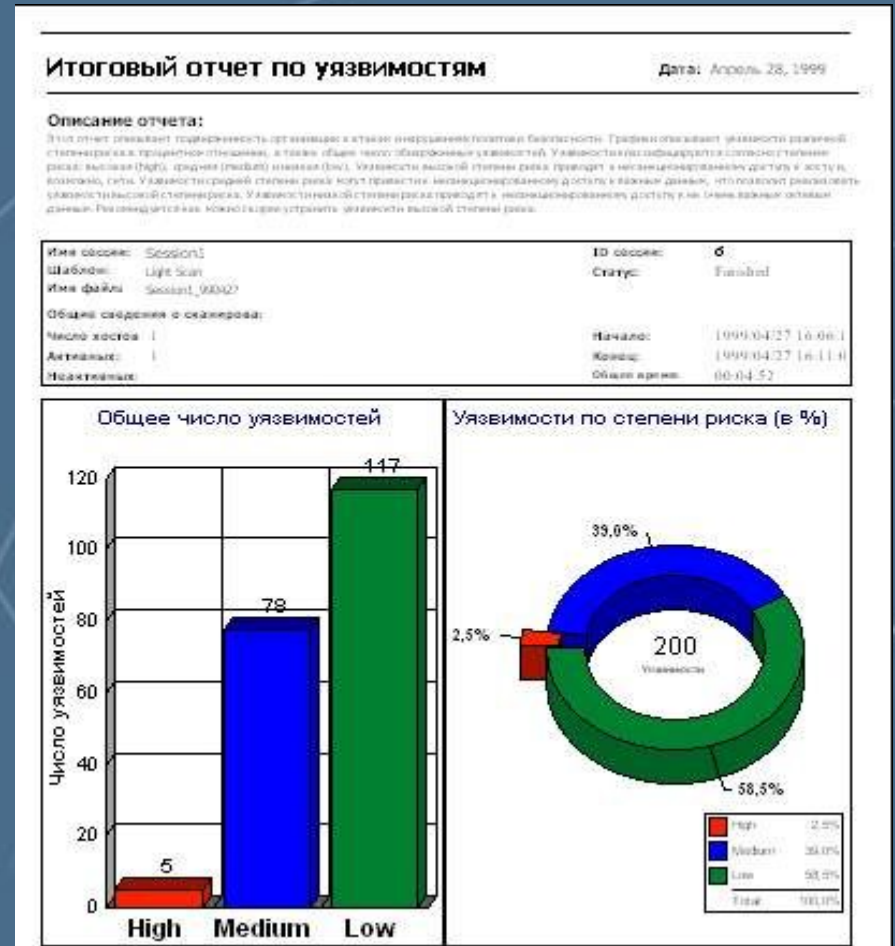
Создание собственных проверок

Уровни сканирования



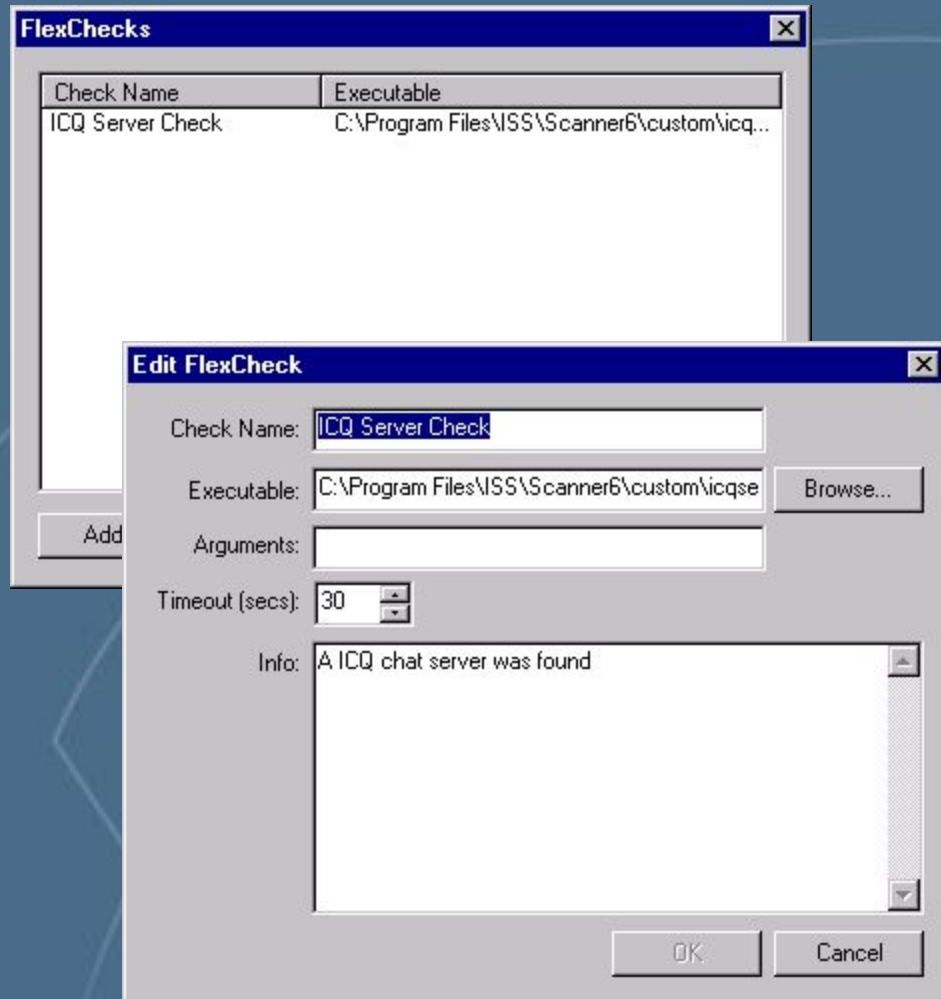
Категории отчетов

- Для руководства компании
- Для руководителей отделов
- Для технических специалистов



Добавление своих проверок

- Любой язык высокого уровня (C, Pascal, Perl и т.д.)



Недостатки Internet Scanner

Сбои при определении служб UDP

Повышенные требования к полосе пропускания сети

Отсутствие централизованного управления



Способы сканирования

Main window



Iss_WinNT.exe.lnk

Console Mode

```
ISS Internet Scanner
Key Name: C:\Program Files\ISS\Scanner6\scan.key
Policy Name: L2 Classification
Scanning 1 Host(s)...
Scanning Host: 200.0.0.125
-
```

Command line



_default.pif

Практическая работа 13

Знакомство с программой Internet Scanner

- Установка программы
- Установка ключа
- Первый запуск программы