Средства анализа защищённости

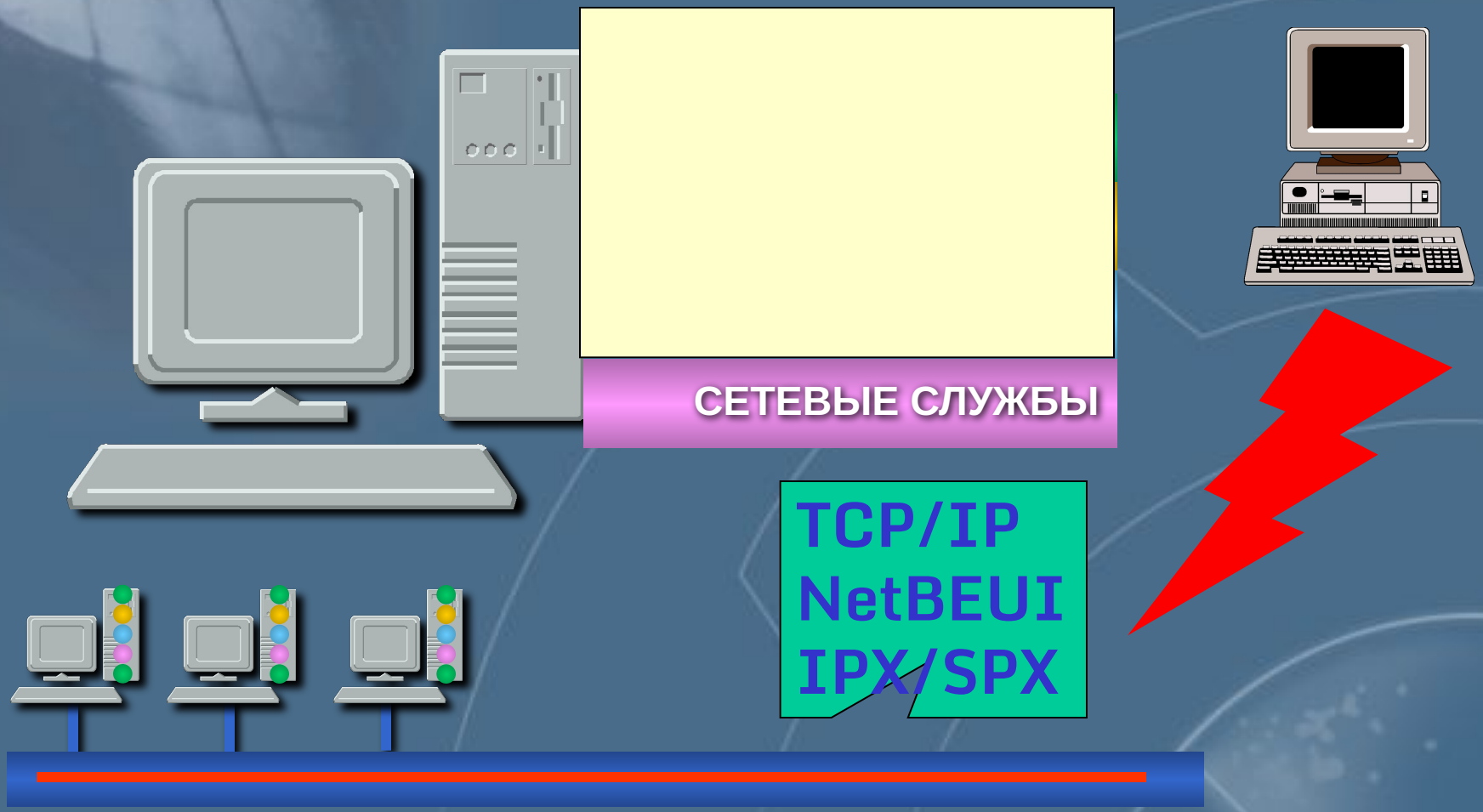
Раздел 2 – Тема 12

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 Associations		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 команд-ной 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 пяти-балльной 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

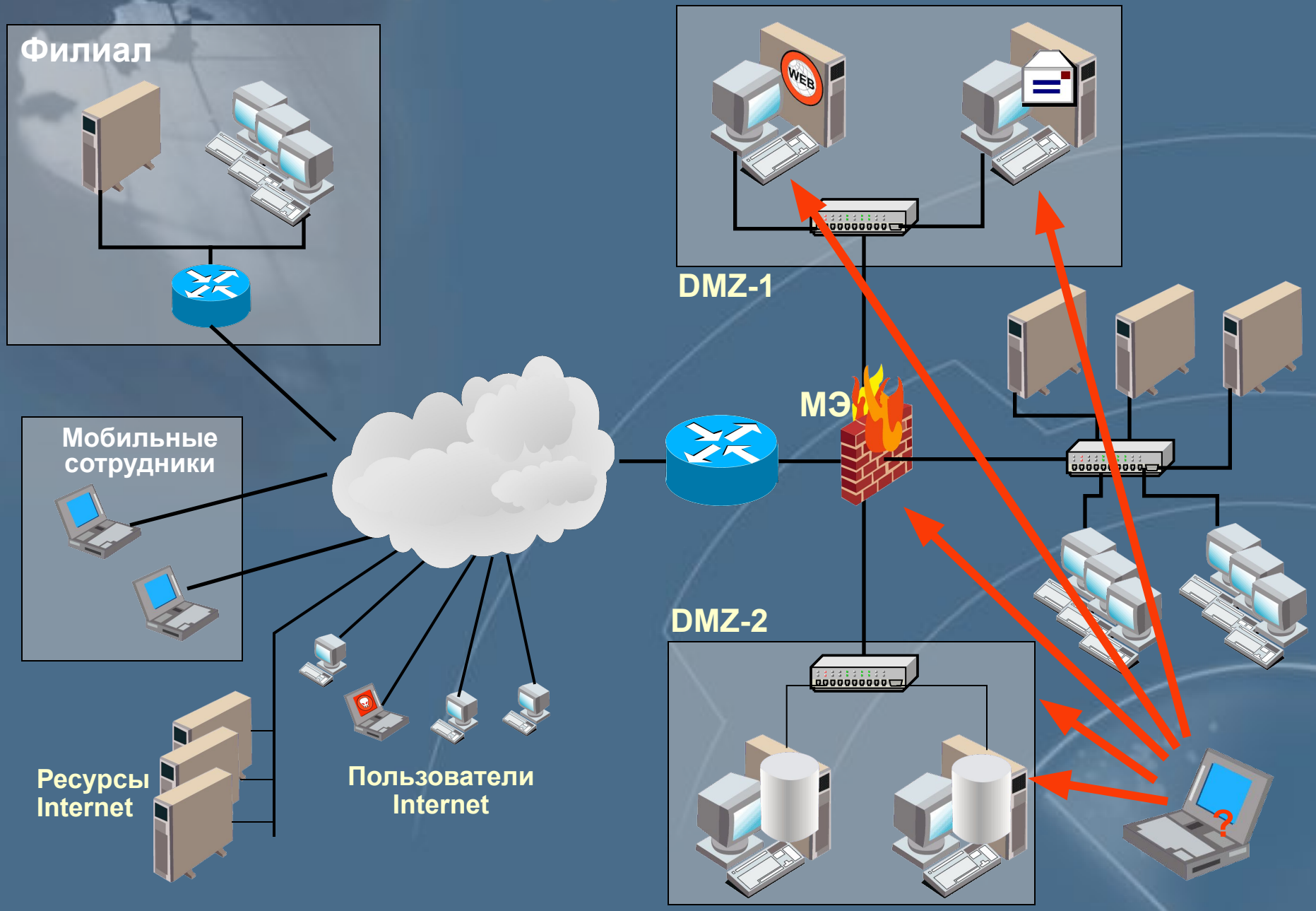
Выбор объектов сканирования и вариантов размещения сканера (сканеров)

Выбор (разработка) политик сканирования

Составление расписания сканирования

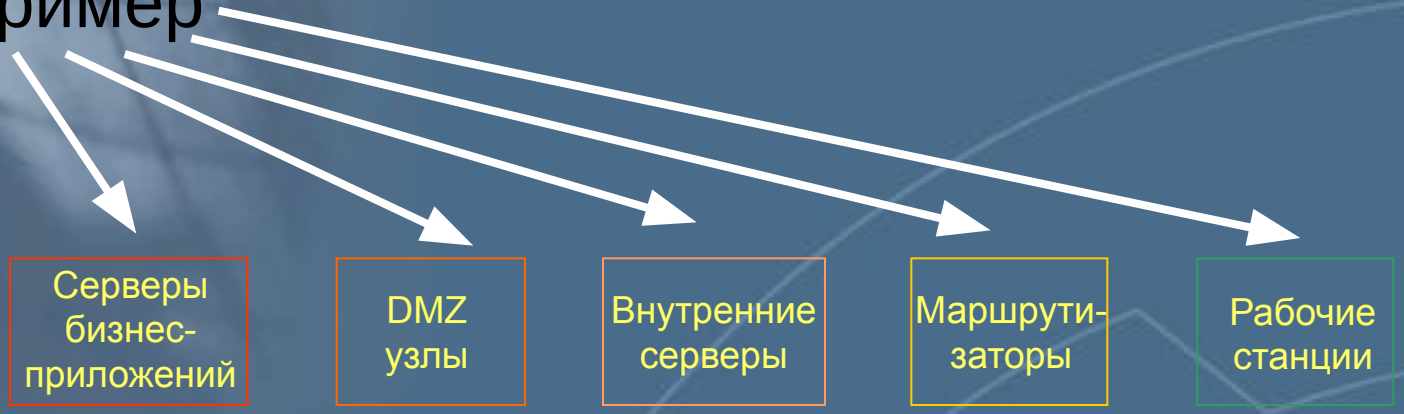
Сканирование и анализ результатов

Сбор информации о сети

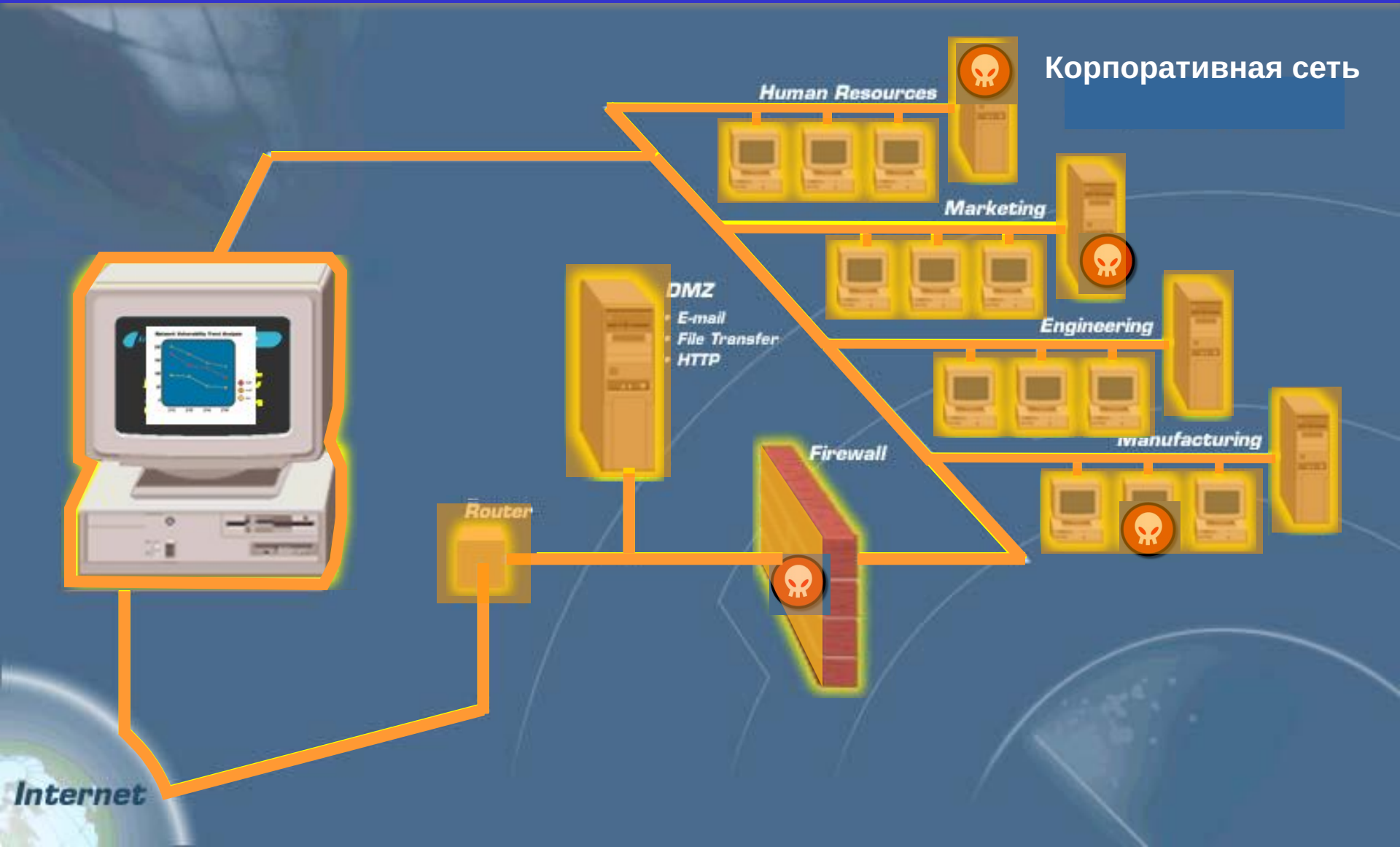


Категорирование сетевых устройств

Пример

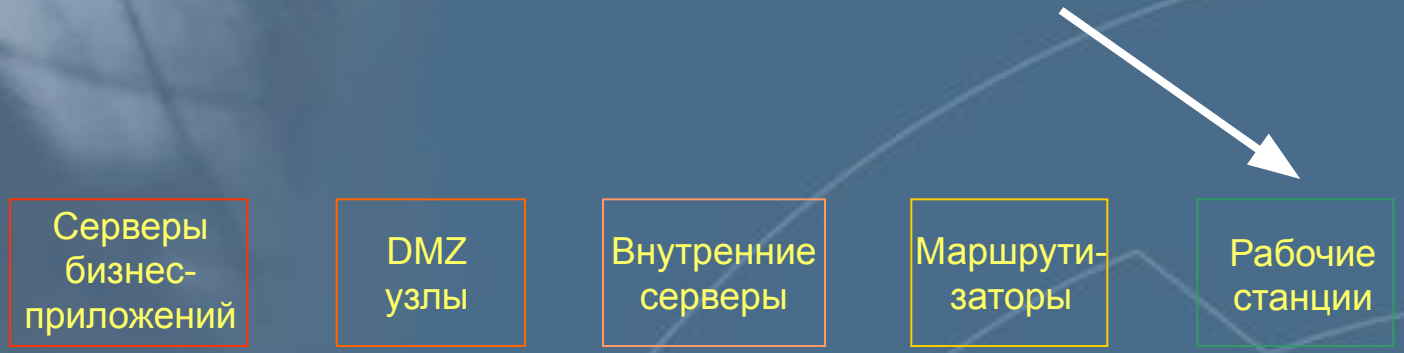


Выбор объектов сканирования и вариантов расположения средств анализа защищённости



Выбор политик сканирования

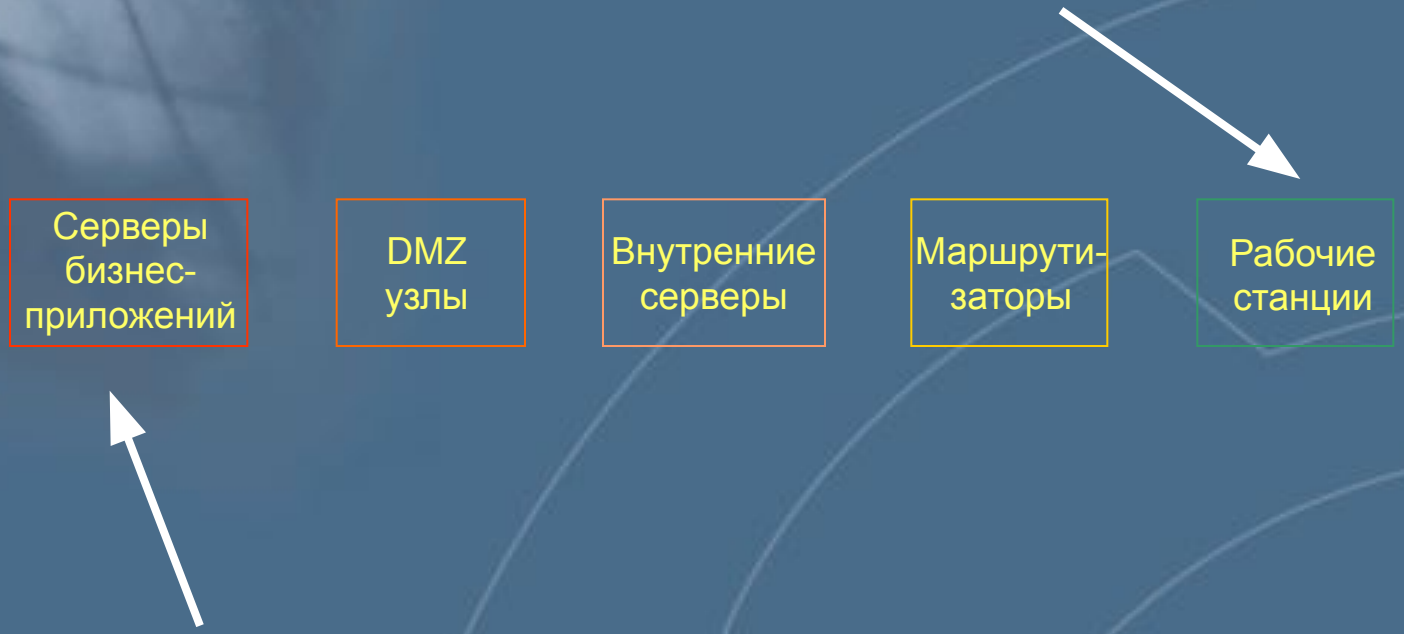
Политика для рабочих станций



Политика для критичных узлов (максимальная защита)

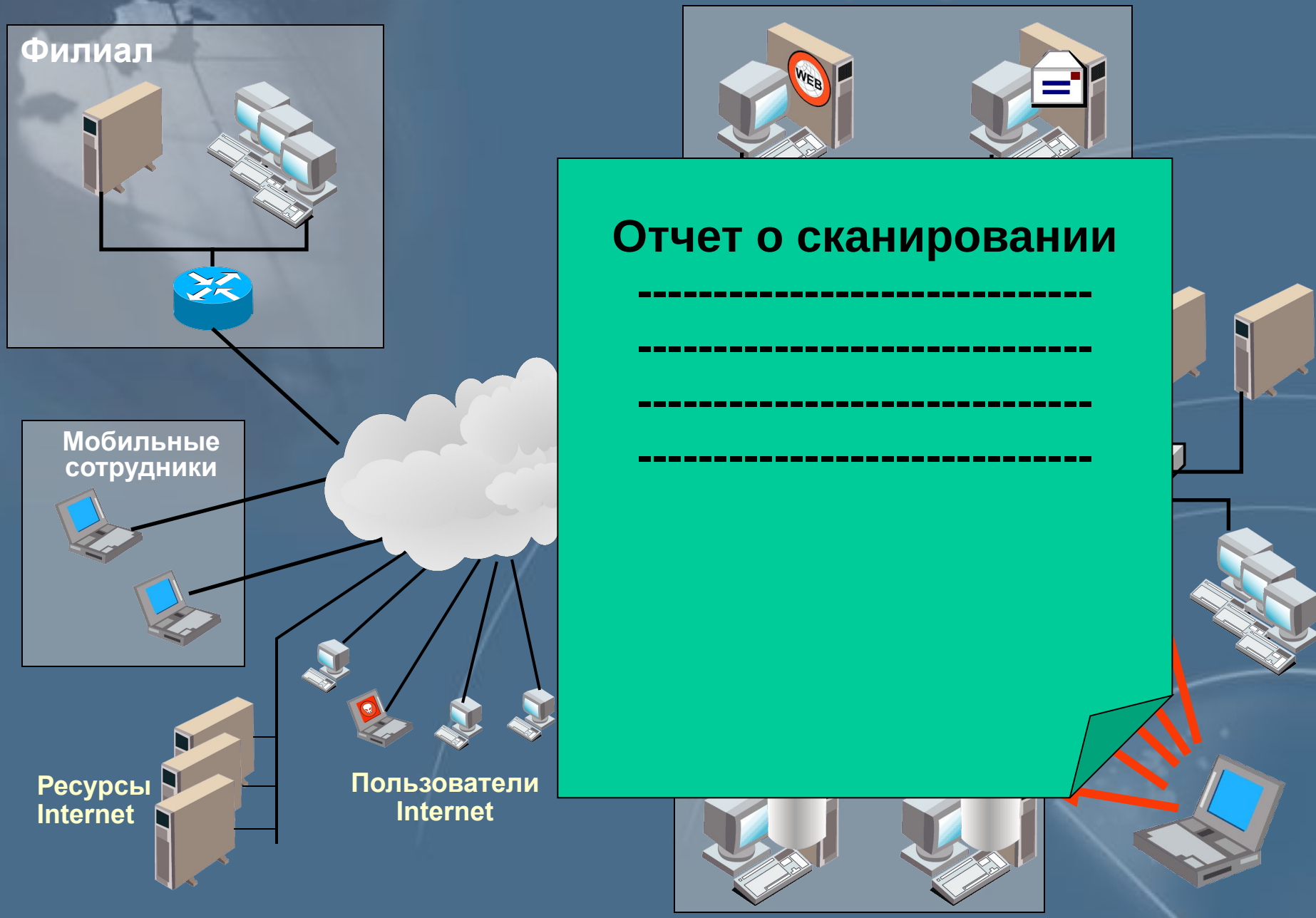
Составление расписания сканирования

Сканировать в 18-00 раз в день



Сканировать в 7-00 раз в неделю

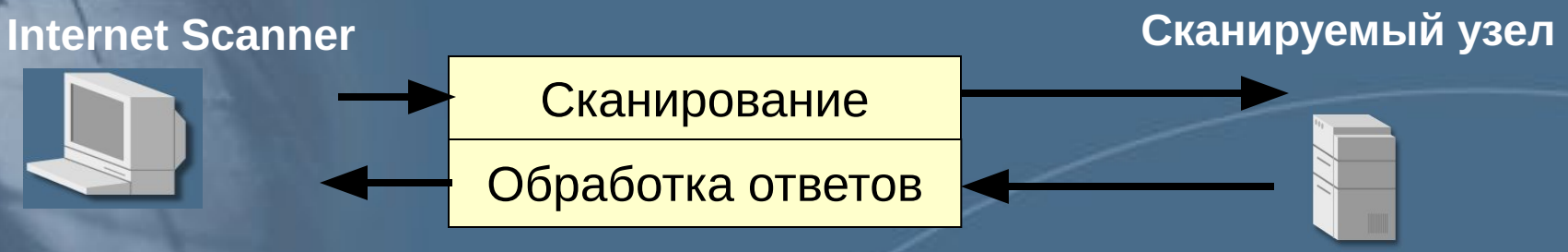
Сканирование и анализ результатов



Internet Scanner

(пример сканера сетевого уровня)

Схема работы системы Internet Scanner



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

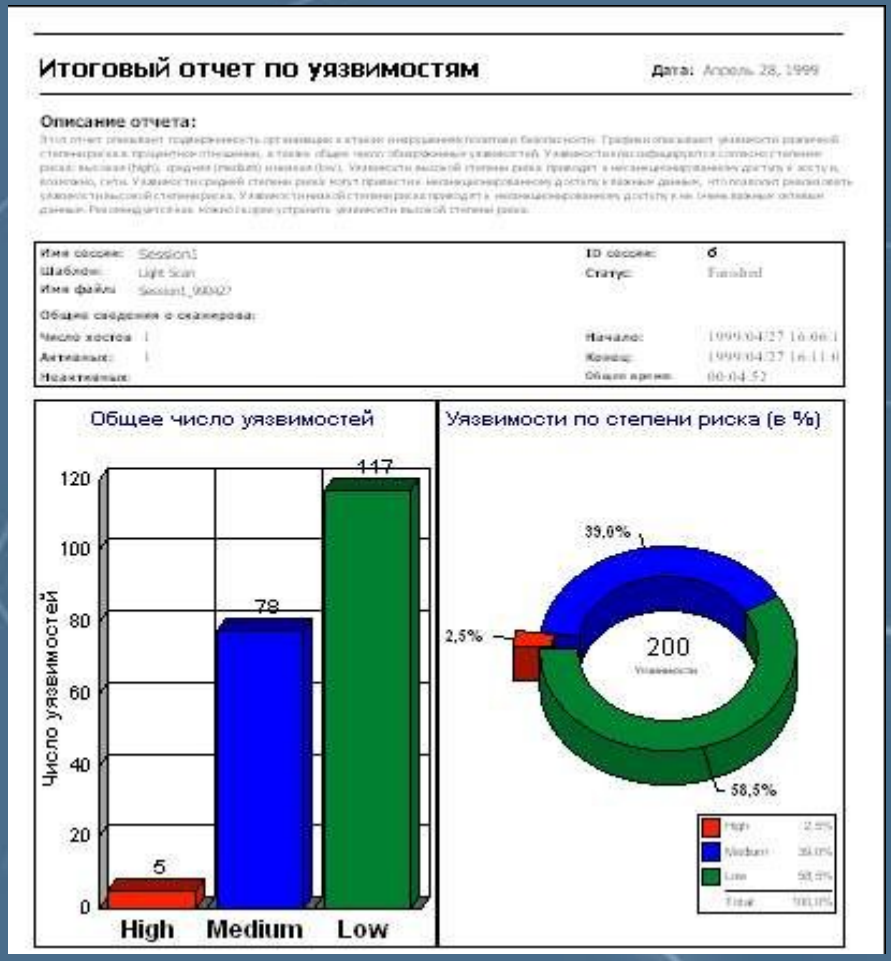
Характеристики Internet Scanner

- 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

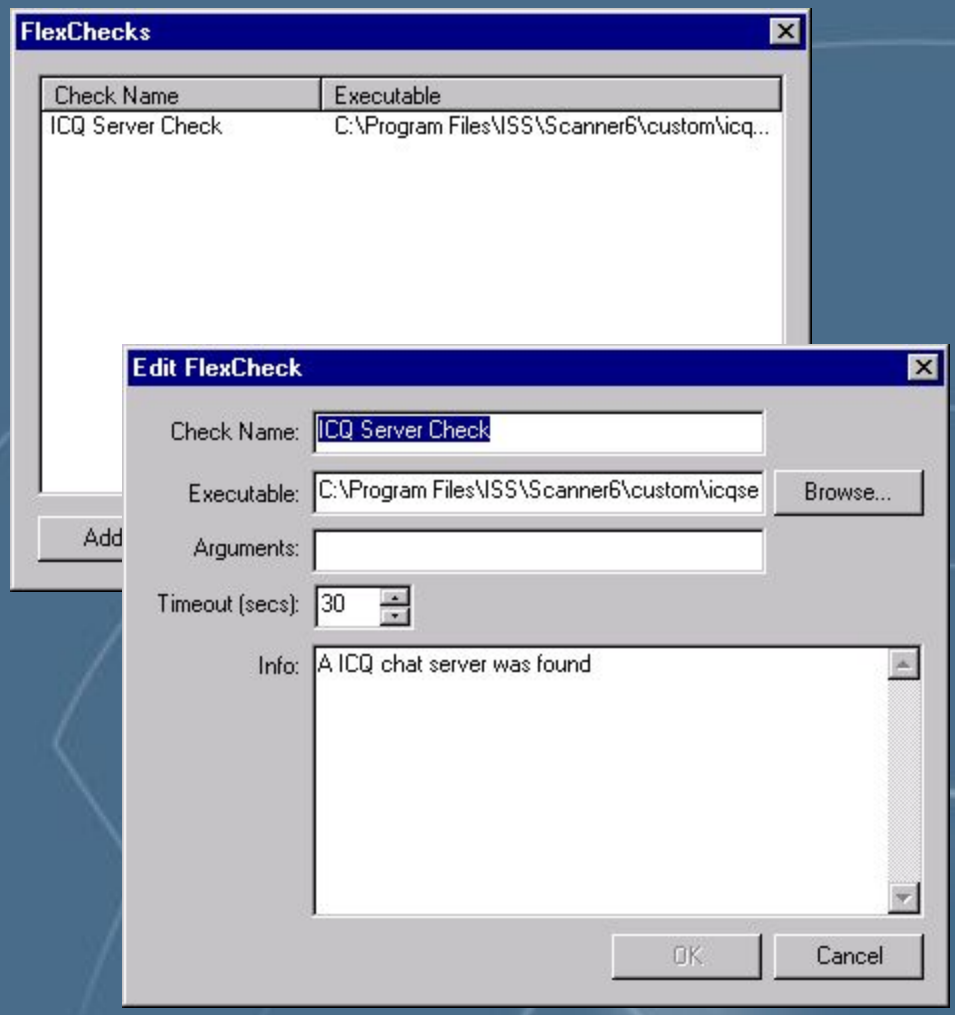
Категории отчетов

- 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

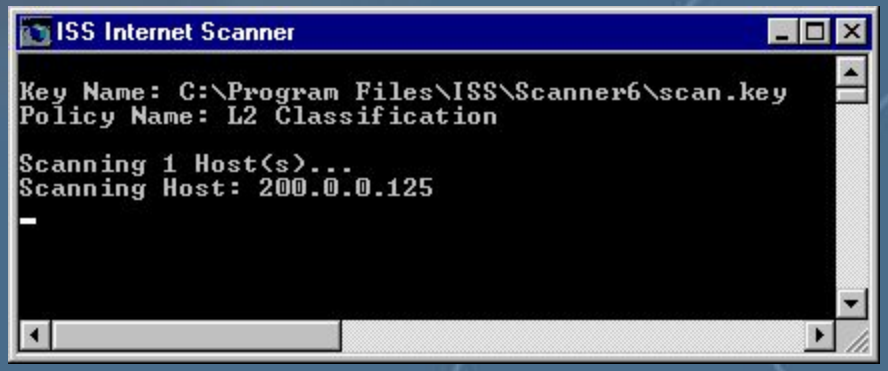
Отсутствие централизованного управления

Способы сканирования

Main window

Iss_WinNT.exe.lnk

Console Mode



Command line

_default.pif

Практическая работа 13

Знакомство с программой Internet Scanner

- Установка программы
- Установка ключа
- Первый запуск программы