

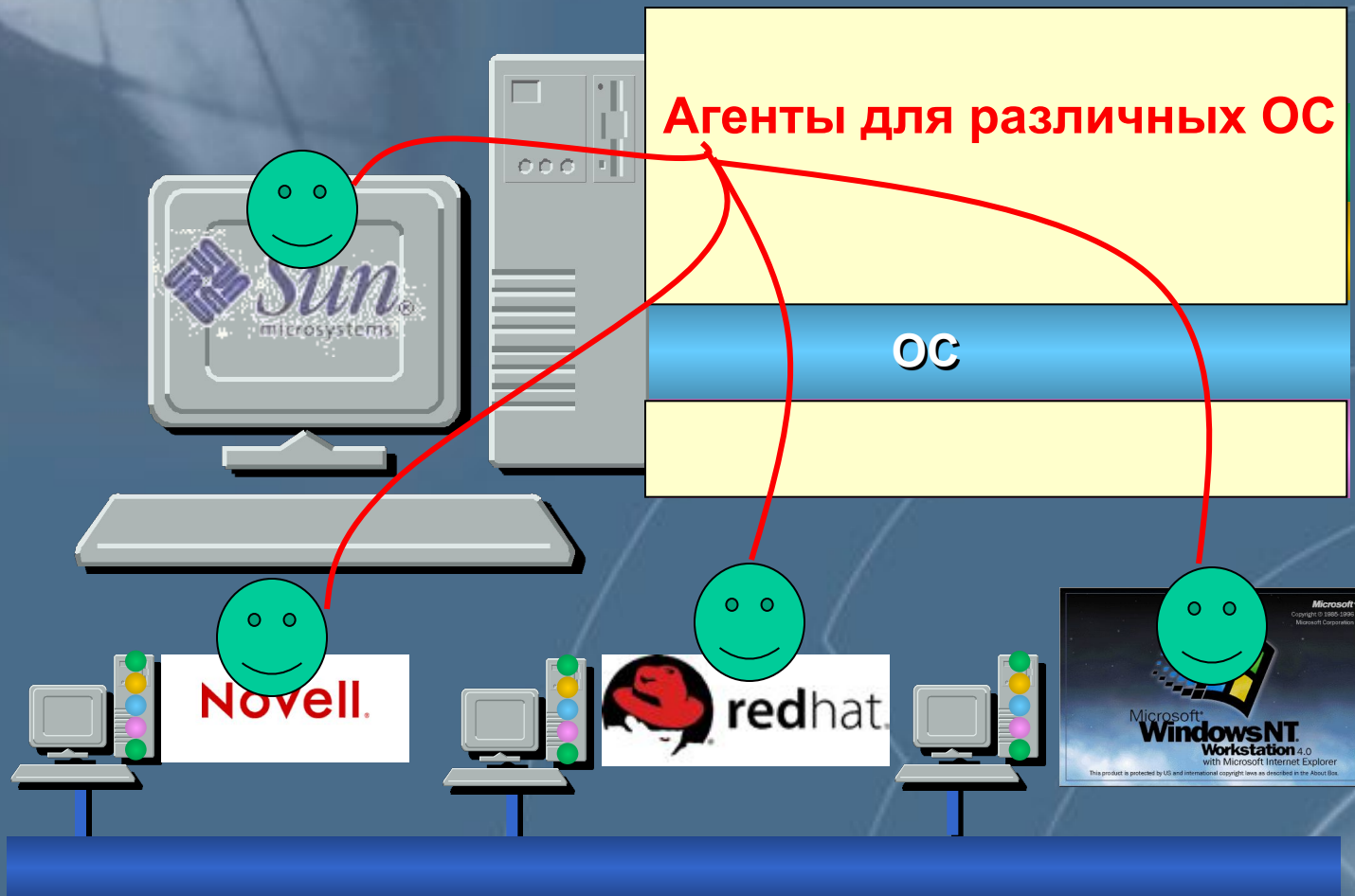
The background is a solid blue color. In the top-left corner, there is a faint, semi-transparent image of a globe showing the continents. On the right side, there are several concentric, semi-transparent white lines forming a circular pattern, resembling a radar or scanning effect. The text 'System Scanner' is centered in the middle of the page.

# System Scanner

**ИНФОРМЗАЩИТА**

НАУЧНО-ИНЖЕНЕРНОЕ ПРЕДПРИЯТИЕ

# Анализ защищенности на уровне операционной системы



# Анализ защищенности на уровне операционной системы

Моделирование действий внутренних хакеров

Прямой доступ к операционной системе

Обнаружение нарушений политики безопасности

Анализ всех настроек операционной системы

Обнаружение «следов» хакеров

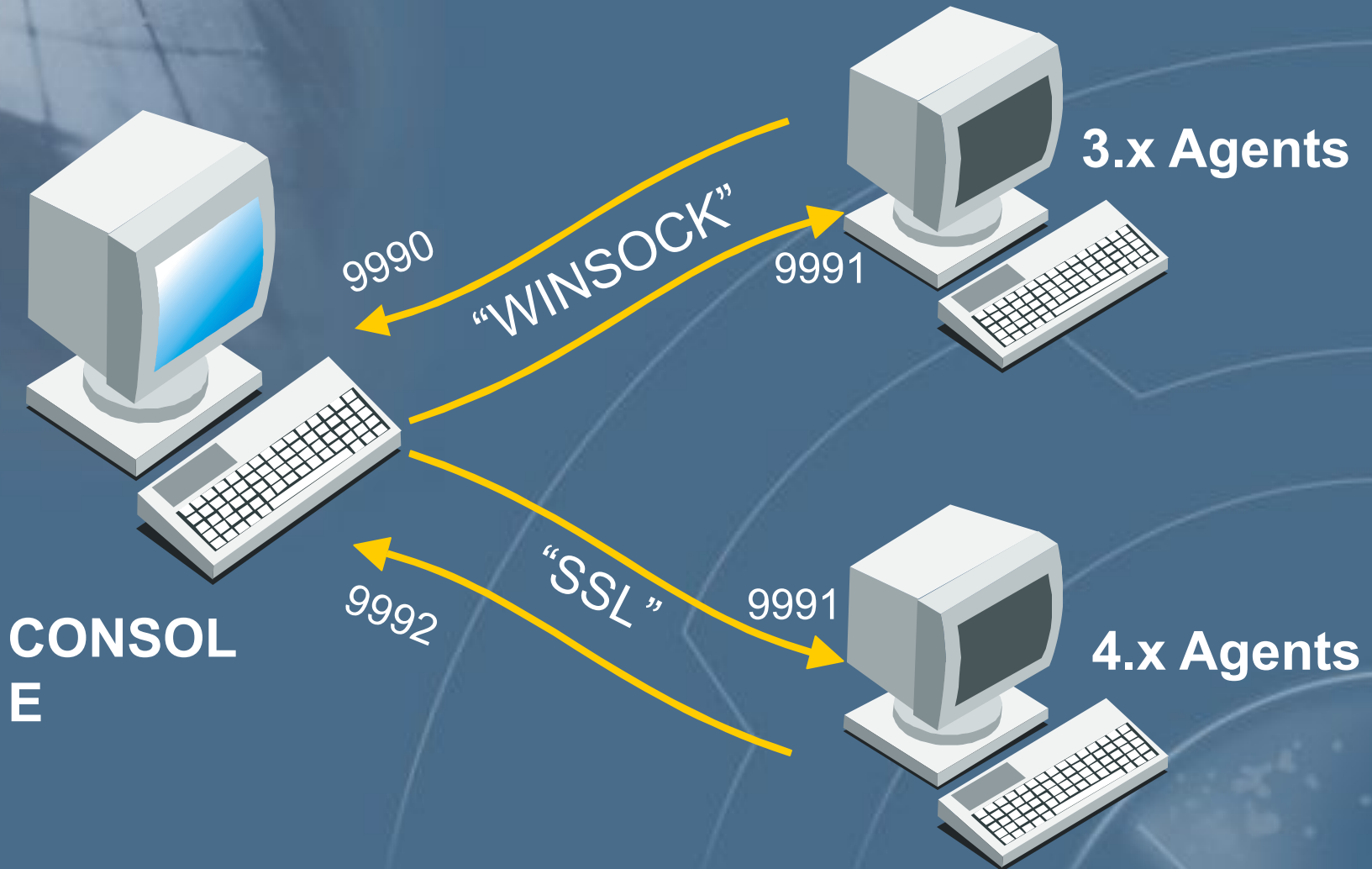
Взгляд на безопасность компьютера «изнутри»

# Система System Scanner

Анализ защищенности рабочих станций и серверов под управлением ОС Windows NT, Windows 2000, UNIX (Solaris, SunOS, HP UX, AIX, Linux, IRIX и т.д.)

- *System Scanner Manager*
- *System Scanner Agent*

# Связь между консолью и агентами



# Возможности System Scanner

- Более 550 проверок для Windows и более 425 проверок для Unix
- Централизованное управление
- Создание своих проверок
- Задание степени глубины сканирования
- Обновление компонентов
- Контроль целостности файлов и реестра
- Запуск проверок по расписанию
- Чтение и анализ логов Windows NT и Unix

# Поддерживаемые ОС

## System Scanner 4.0 Console

Windows NT SP4, SP5

## System Scanner Agents

## Version 4.0

Windows NT (Intel) NT 4.0 SP4, SP5

SUN Solaris 2 2.6, 2.7

Windows 2000 Release 1

## System Scanner 3 Agent

## 3.x Agents

Digital UNIX (Tru64 UNIX) V3.2C, V4.0D

HPUX 9.05 9.x, 10.10, 10.20

IBM AIX 3 3.2.5, 4.1, 4.2

NCR (SVR4 on Intel) SVR 4.0

Sequent PTX/4 2.x, 4.0, 4.2, 4.2X (Large files)

Windows NT (Intel) 3.51

SCO Openserver 5.0

SCO Unixware 2.0, 2.1

SIEMENS SINIX 5.43

SIEMENS (PYRAMID) DC/OSx

Sun Solaris 1 1.x

Sun Solaris 2 2.51, 2.6

ICL DRS/NX 6 (or /NX 7) NX 6, NX7, 7M+

**ИНФОРМЗАЩИТА**

НАУЧНО-ИНЖЕНЕРНОЕ ПРЕДПРИЯТИЕ

# Поддерживаемые ОС

## System Scanner Agents

## Version 4.0

SUN Solaris 2	2.6
HP/UX	11.0
IBM AIX	4.3
Linux	Red Hat Version 6.1
Compaq Tru64 Unix (Digital UNIX)	4.0.D, 5.0
SCO UnixWare on Intel	7.0
SCO OpenServer	5.x
Sequent Ptx/4	4.2x, inc (large files)
Siemens SINIX	5.44
SUN Solaris 8	8 (Q4 '2000)



# Категории проверок

- **Контроль целостности файлов**
  - MD5, размер, наследование, привилегии
- **Системная конфигурация**
  - Trusts, crontabs, daemons
- **Компрометация системы**
  - Неизвестные файлы, режим promiscuous
- **Учетные записи**
  - Root equivalent, dormant
- **Проверка паролей**
  - Словарь, перебор и перестановка, отсутствие
- **Права доступа и наследование файлов**
  - SUID/SGID, r-w-x, owner, group

# Варианты реагирования

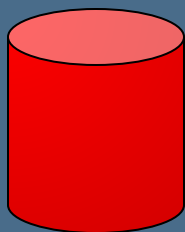
Печать отчетов

*Crystal reports, HTML, Text*



Уведомление на консоль

*SNMP Alerts, Email,  
Другие программы*



*Сохранение в ODBC-базе данных  
данные могут быть экспортированы*

**ИНФОРМЗАЩИТА**

НАУЧНО-ИНЖЕНЕРНОЕ ПРЕДПРИЯТИЕ

# Схема лицензирования

Evaluation key – ключ для оценки продукта  
(срок действия - 15 дней)

Engagement key – временный ключ  
(срок действия – 30 дней)

Permanent key – постоянный ключ  
(срок действия - не лимитирован)

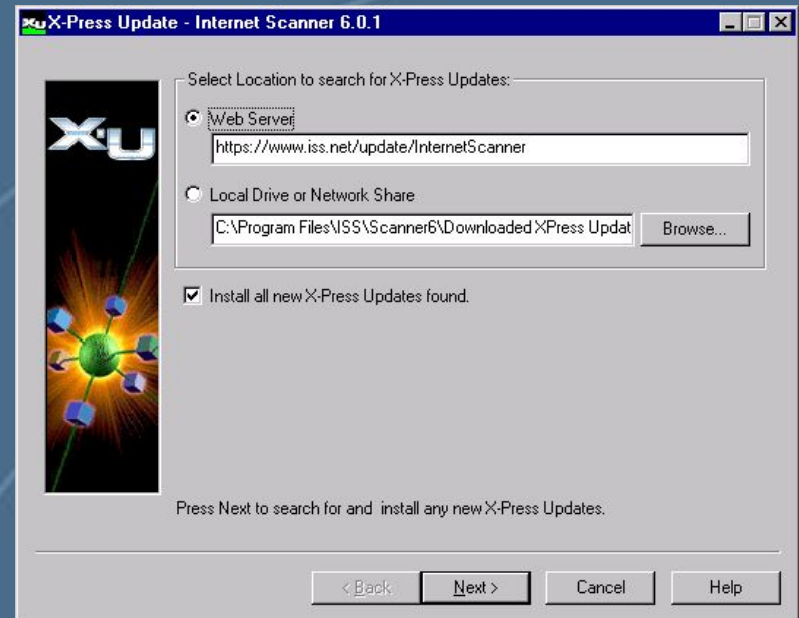
# Механизмы обновления

- Основная версия – раз в год  
Пример: System Scanner 3.2 → 4.0
- Дополнительные версии – раз в квартал  
Пример: System Scanner 4.0 → 4.1
- Обновления XPress Update – по мере появления новых уязвимостей  
Пример: XPU 4, XPU 5
- Пользовательские проверки FlexCheck

# Обновление компонентов

## Обновление:

- сигнатур атак
- отчетов
- шаблонов (Policy)
- файлов подсказки
- дополнительных утилит
- интерфейса
- и т.д.

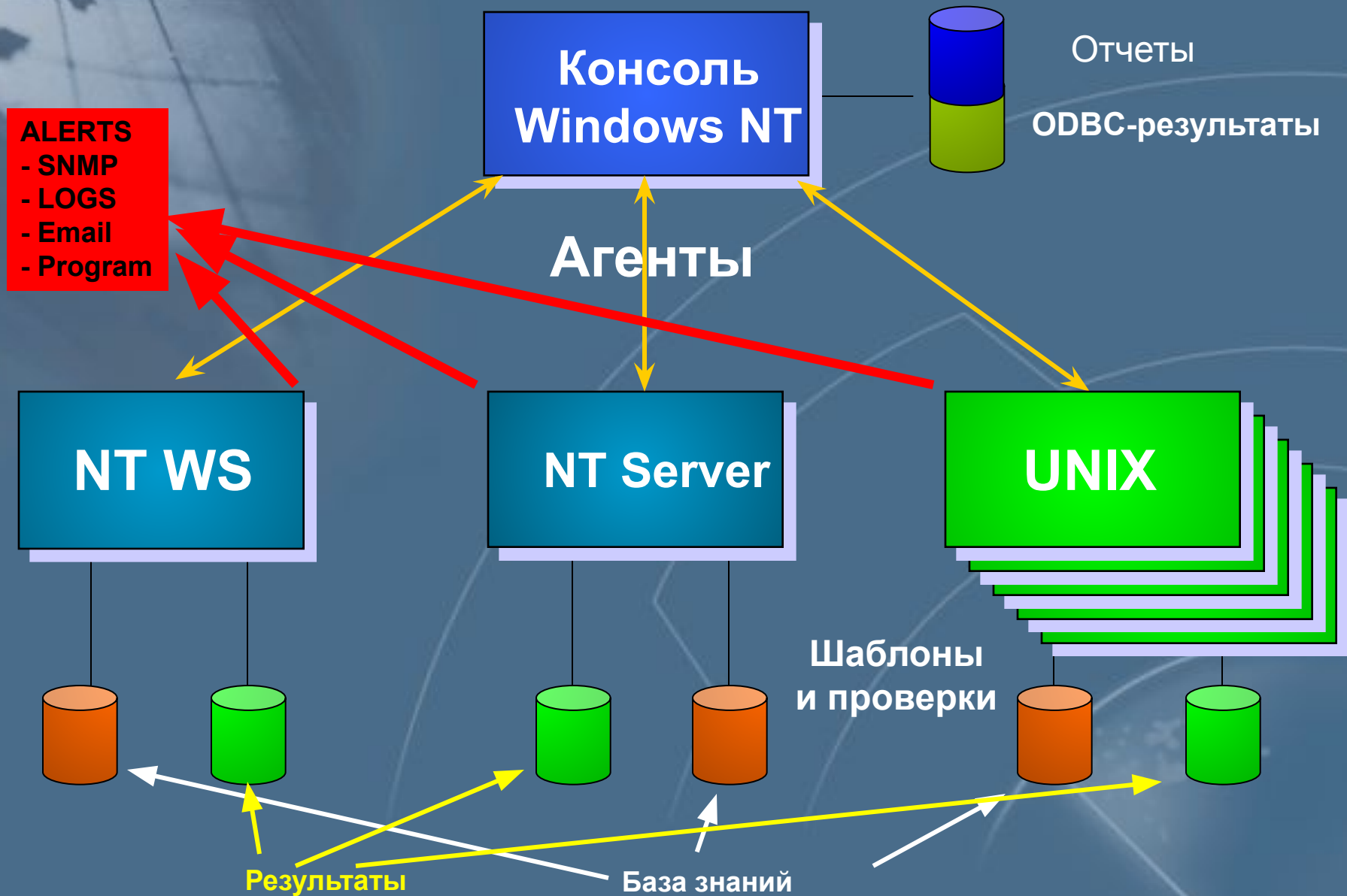


Локально (с диска) и удаленно (через Internet)

**ИНФОРМЗАЩИТА**

НАУЧНО-ИНЖЕНЕРНОЕ ПРЕДПРИЯТИЕ

# Архитектура System Scanner



# Архитектура System Scanner v4.2

