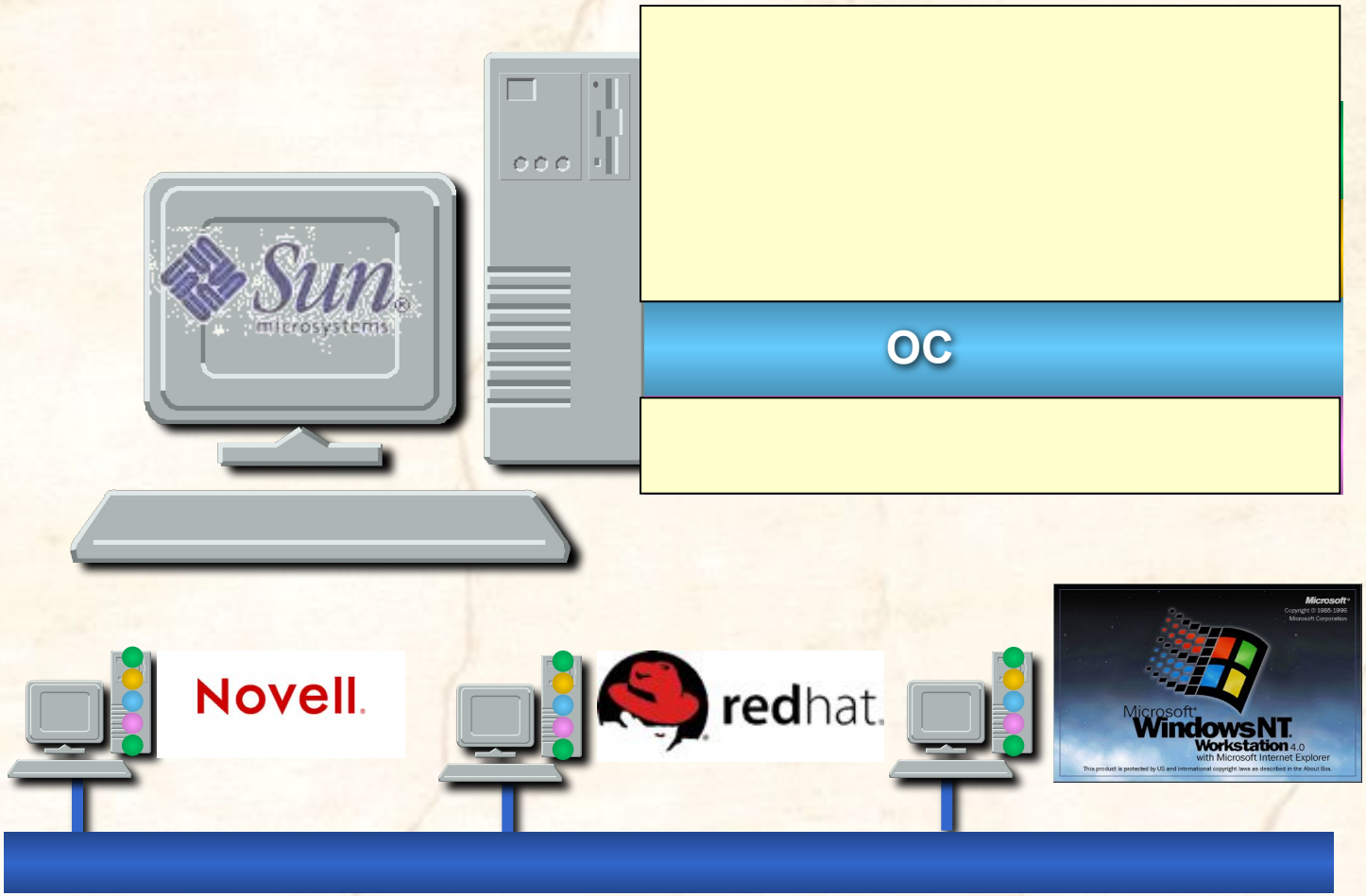
Безопасность Windows NT Server 4.0

Корпоративная сеть

Уровни информационной инфраструктуры



Корпоративная сеть

Windows NT

- **Клиентские рабочие станции**

Корпоративная сеть

Windows NT

- Клиентские рабочие станции
- Серверы бизнес приложений
- Серверы БД
- Серверы файлов и печати

Корпоративная сеть

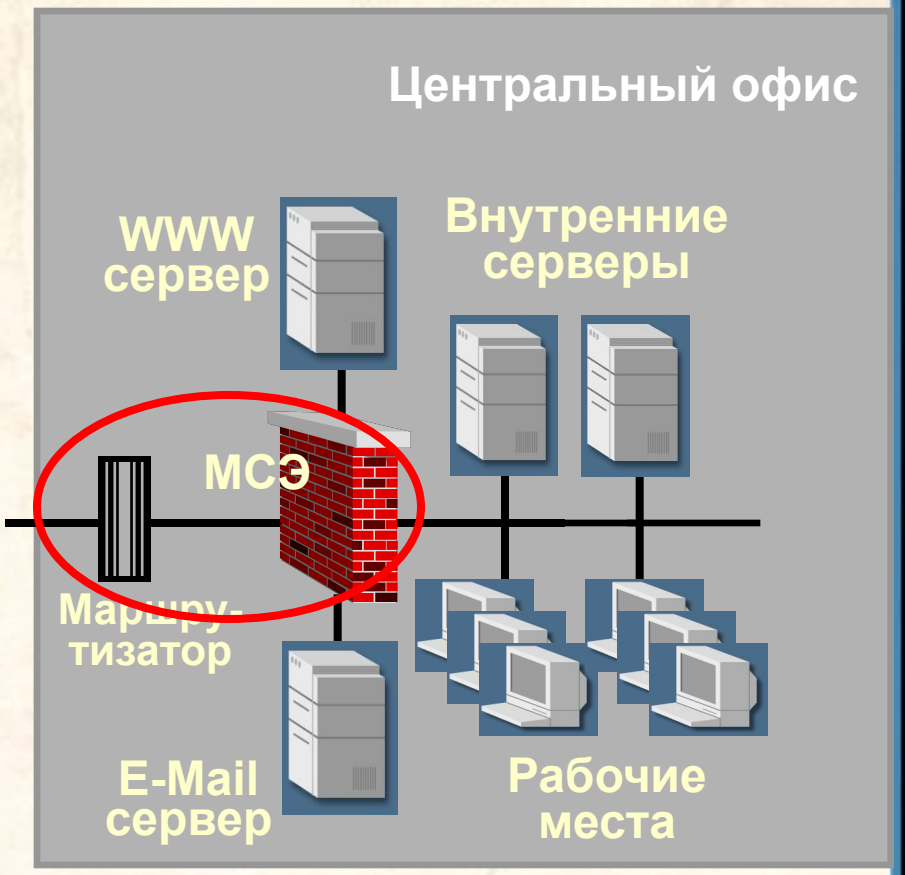
Windows NT

- Клиентские рабочие станции
- Серверы бизнес приложений
- Серверы БД
- Серверы файлов и печати
- Серверы DMZ

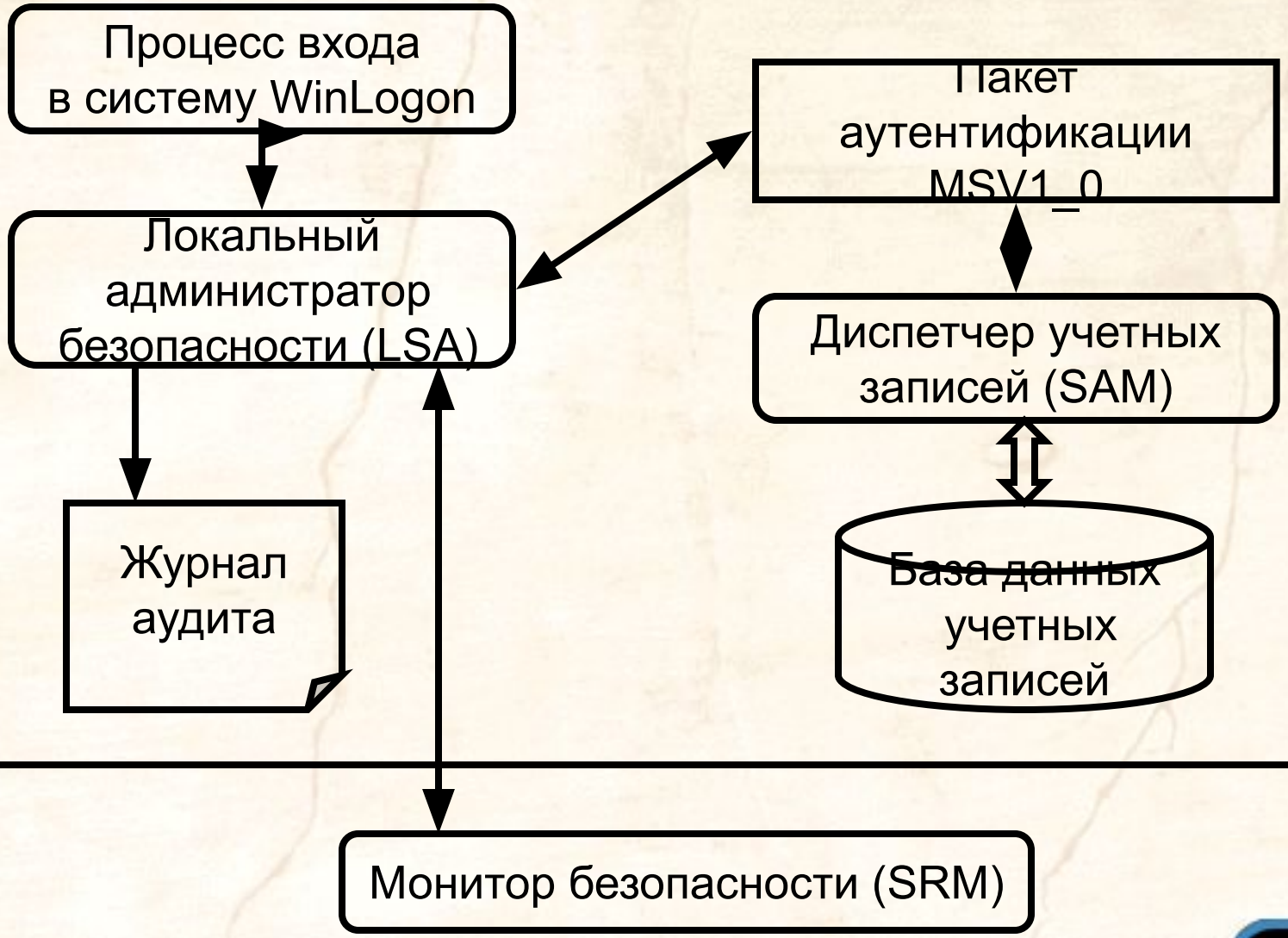
Корпоративная сеть

Windows NT

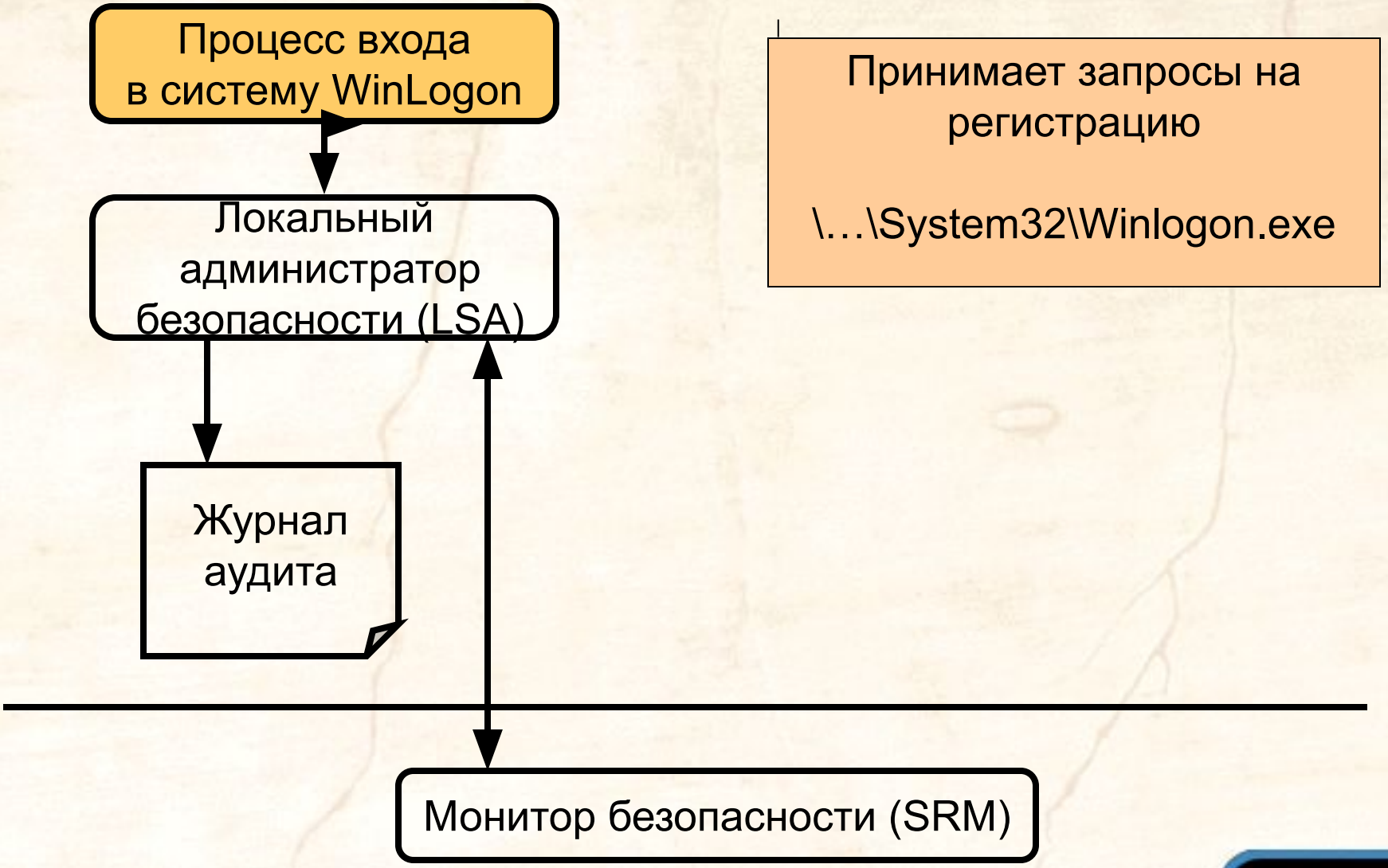
- Клиентские рабочие станции
- Серверы бизнес приложений
- Серверы БД
- Серверы файлов и печати
- Серверы DMZ
- Маршрутизаторы, МЭ



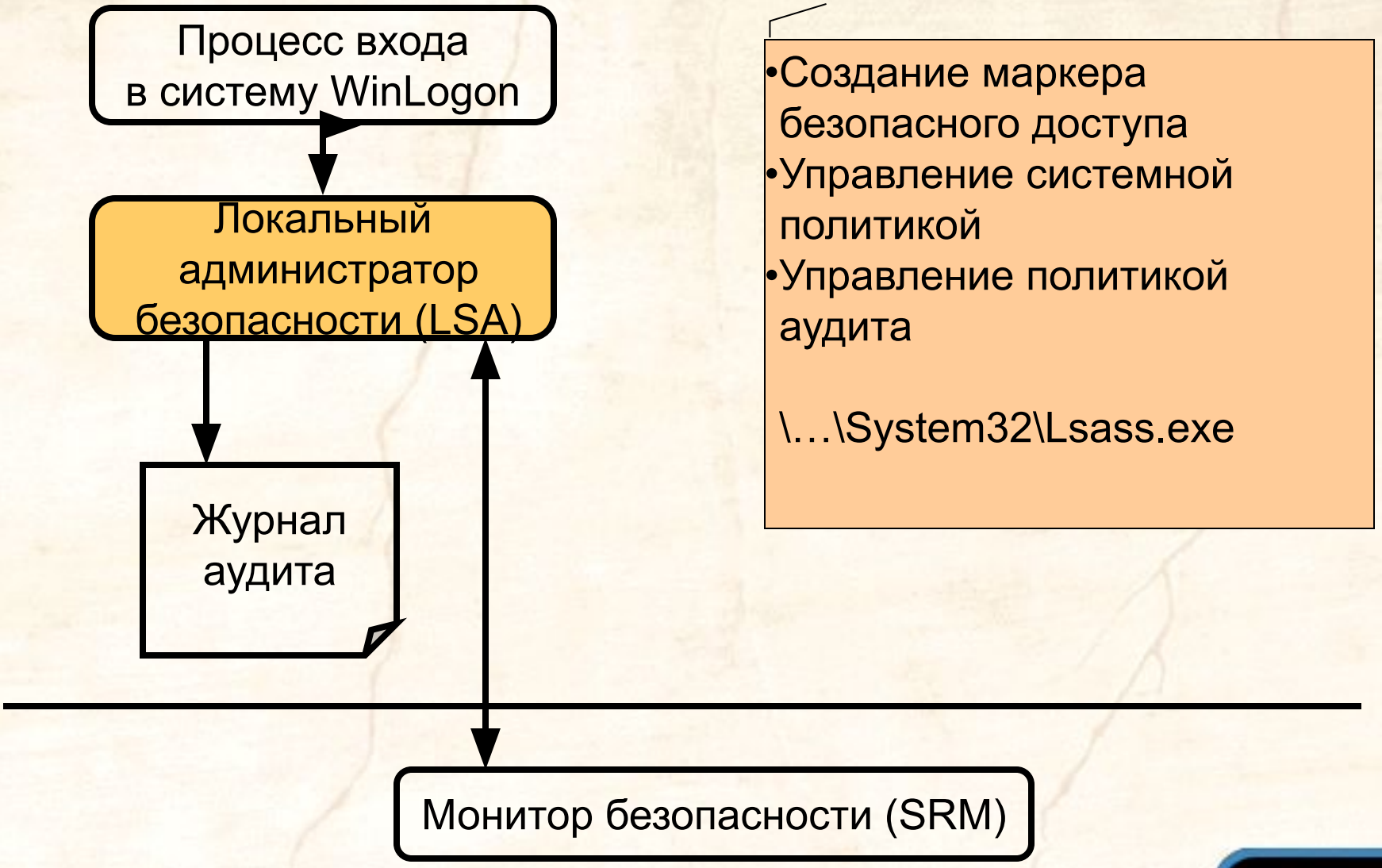
Система безопасности



Система безопасности



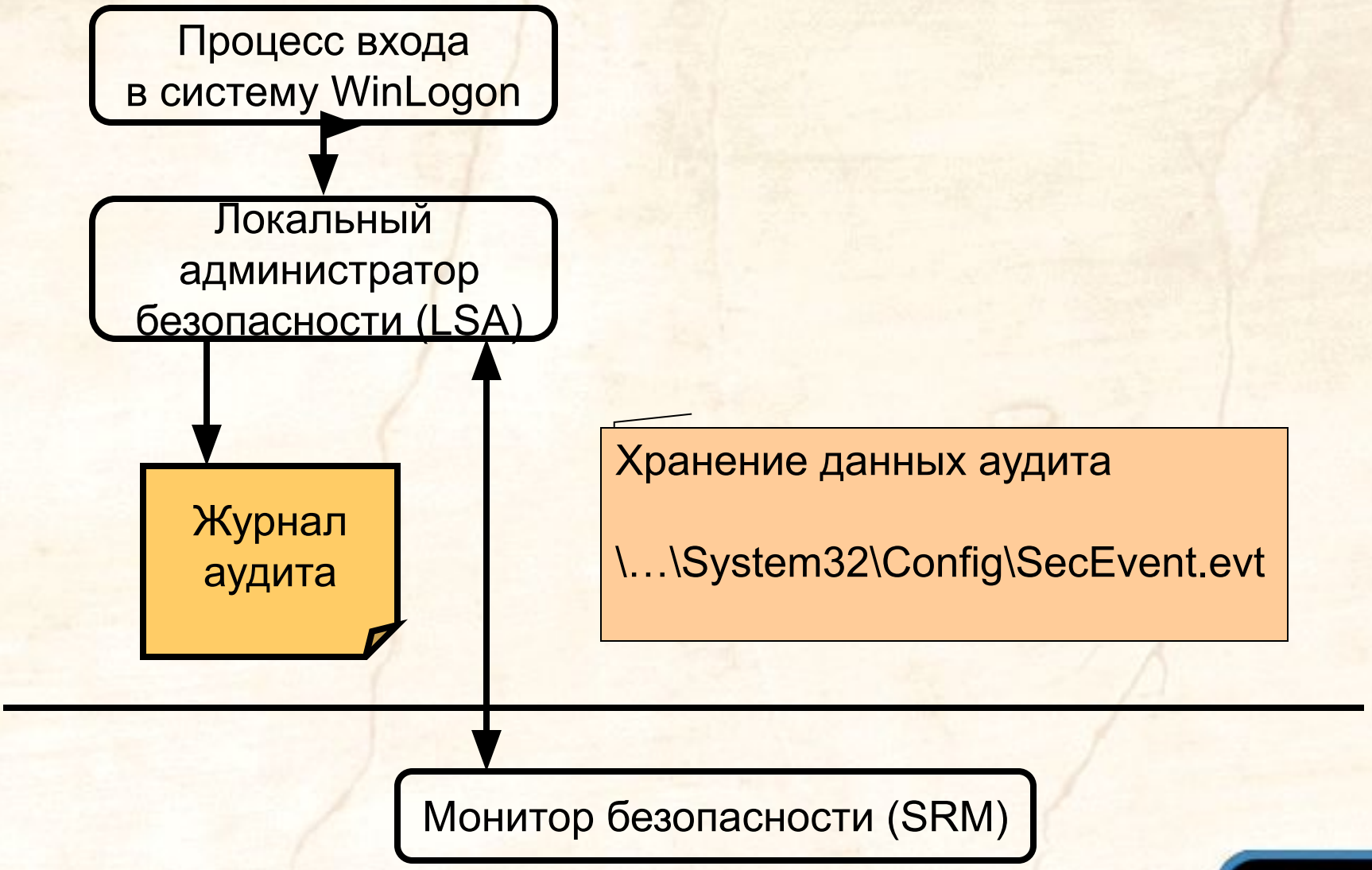
Система безопасности



- Создание маркера безопасного доступа
- Управление системной политикой
- Управление политикой аудита

\…\System32\Lsass.exe

Система безопасности



Система безопасности

Проверка имени и пароля

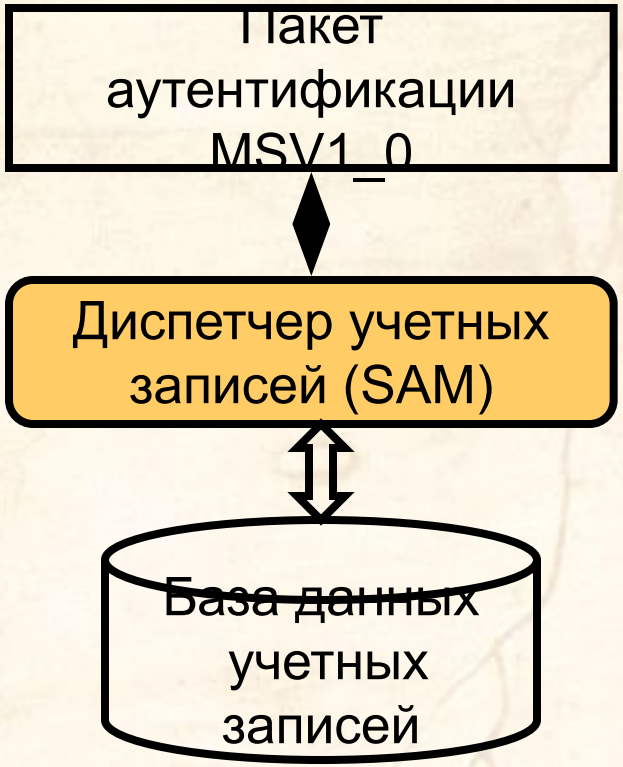
\…\System32\Msv1_0.dll

Монитор безопасности (SRM)

Система безопасности

Поддержка базы данных пользовательских бюджетов

\…\System32\Samsrv.dll

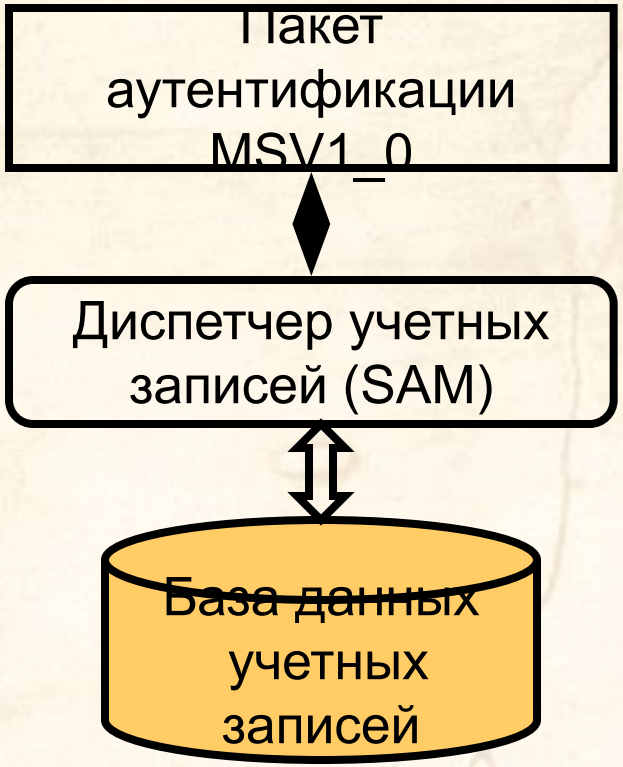


Монитор безопасности (SRM)

Система безопасности

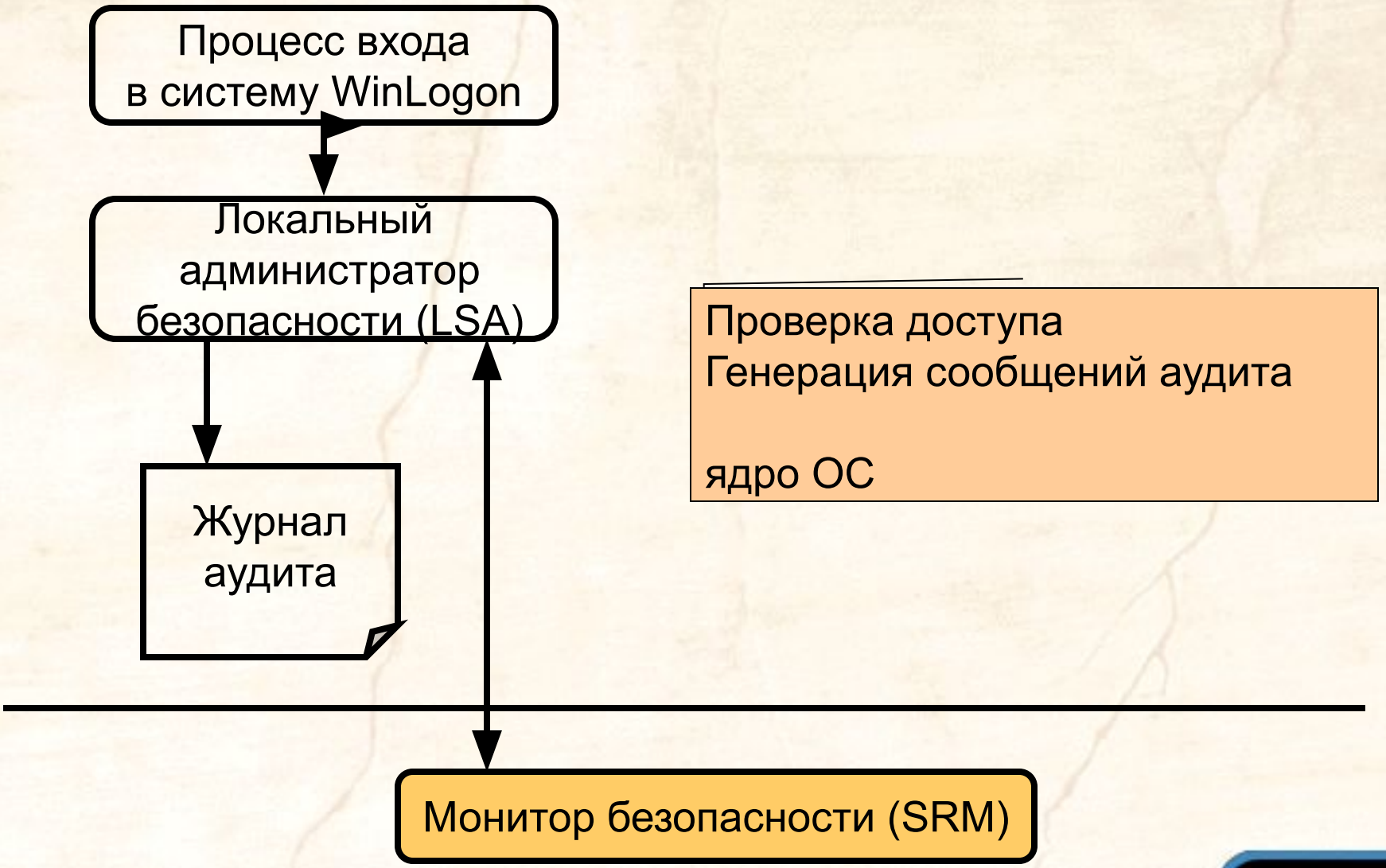
Хранение информации о бюджетах пользователей, групп, компьютеров

Хранится в нескольких местах
- \…\System32\config\sam
- \…\repair\sam._
- ERD



Монитор безопасности (SRM)

Система безопасности



Бюджеты

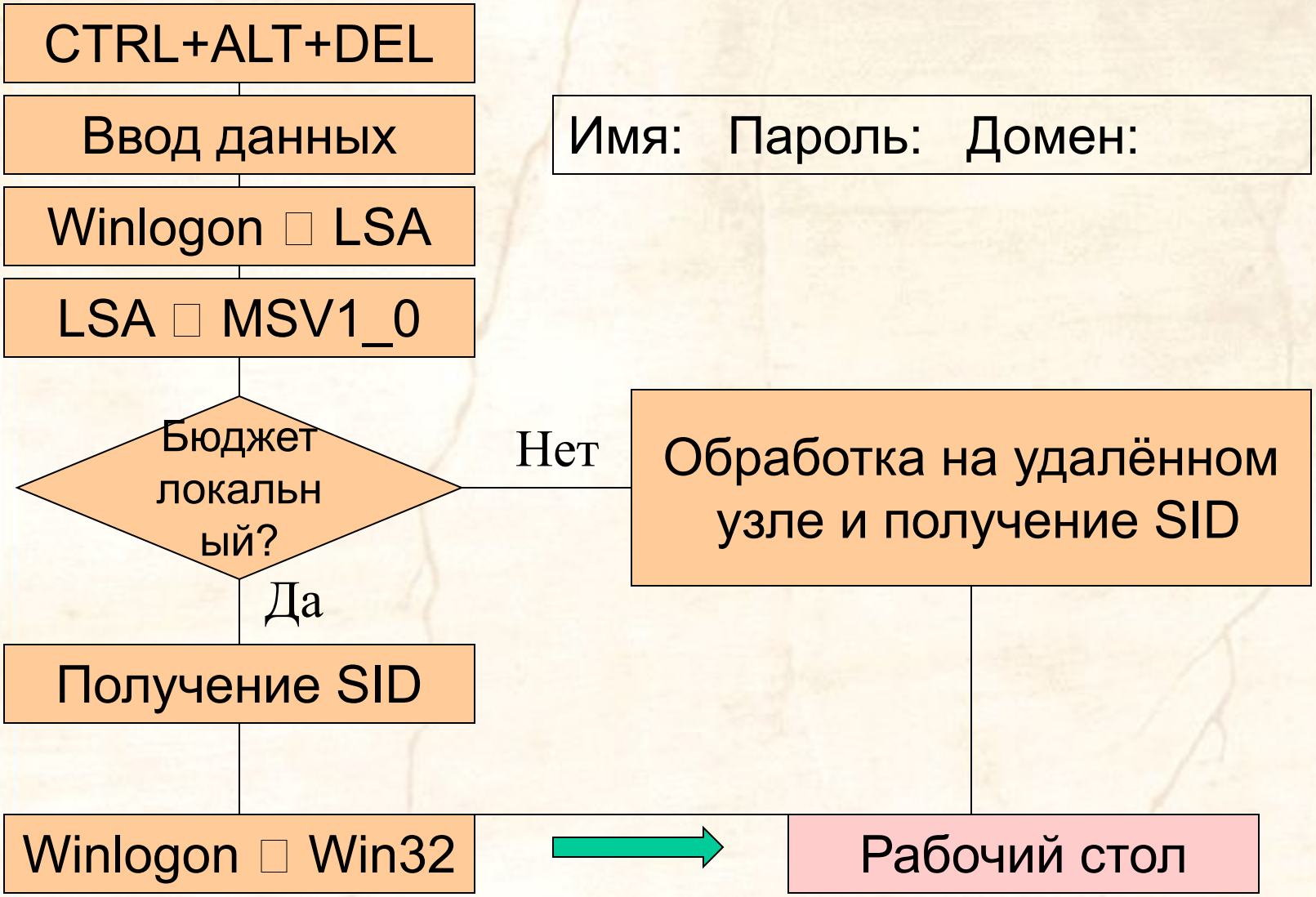
SID (Security ID)

Пользователь

Группа

Компьютер

Процесс регистрации



База данных SAM

- База данных SAM хранит два криптографических хэша для каждого пароля:
  - **LAN Manager Password**. Используется для совместимости со старыми версиями ОС Microsoft и не может быть больше 14 символов.
  - **Windows NT Password**. Базируется на Unicode и ограничен 128 символами.

База данных SAM

LAN Manager Password.

user: user1
password: qwerty

1. QWERTY
2. QWERTY00000000
3. QWERTY0 0000000
4. 
5. no ce + no ce = хэш (16 байт)

База данных SAM

Windows NT Password.

user: user1
password: qwerty

1. Конвертирование в UNICODE
2. Шифрование по MD4

Сетевая аутентификация

Способы аутентификации (начиная с SP 4)

- LAN Manager
- NTLM
- NTLMv2

Сетевая аутентификация

Hive: HKEY_LOCAL_MACHINE

Key: System\CurrentControlSet\Control\Lsa

Name: LMCompatibilityLevel

Type: REG_DWORD

Value: 0 - 5

Настройка системы безопасности

Системная политика

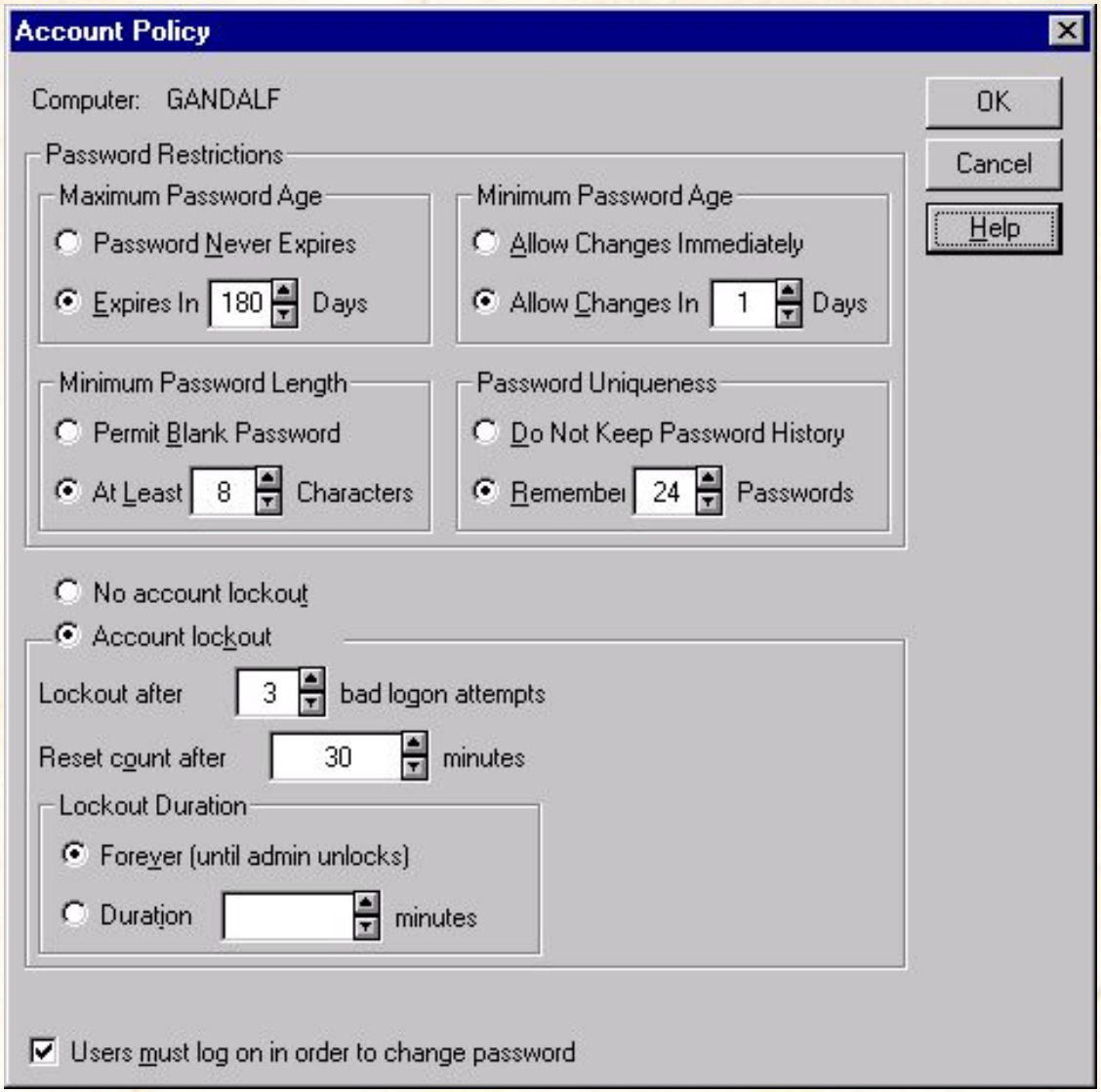
Настройка прав пользователей

Исправление ошибок ОС

Настройка доступа к объектам

Установка ключей реестра

Системная политика



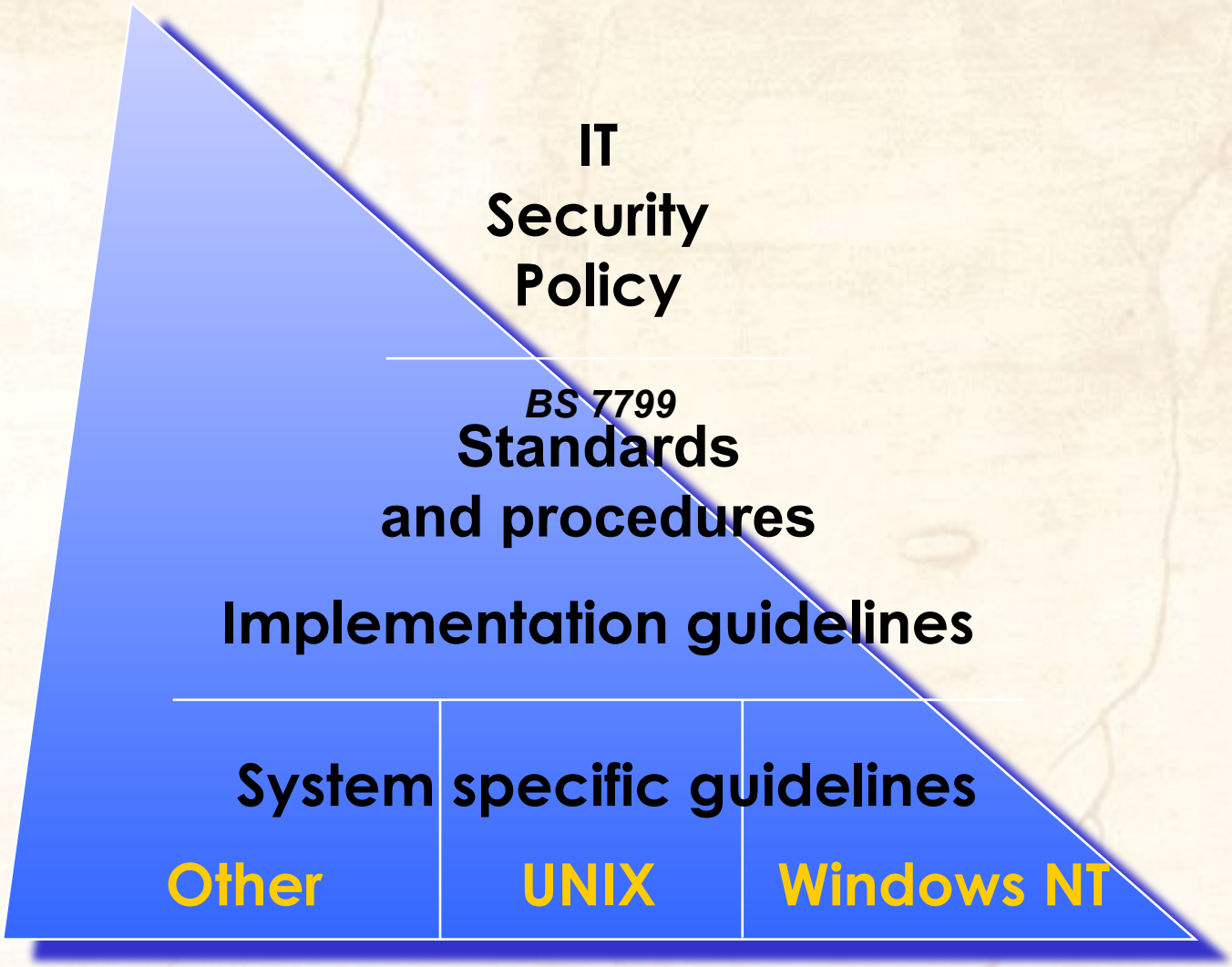
Права пользователей

Файлы и папки

Ключи реестра

Службы

Процесс настройки



‘http://www.c-cure.org/’ and
‘http://www2.dti.gov.uk/cii/security.html’

Утилиты для настройки

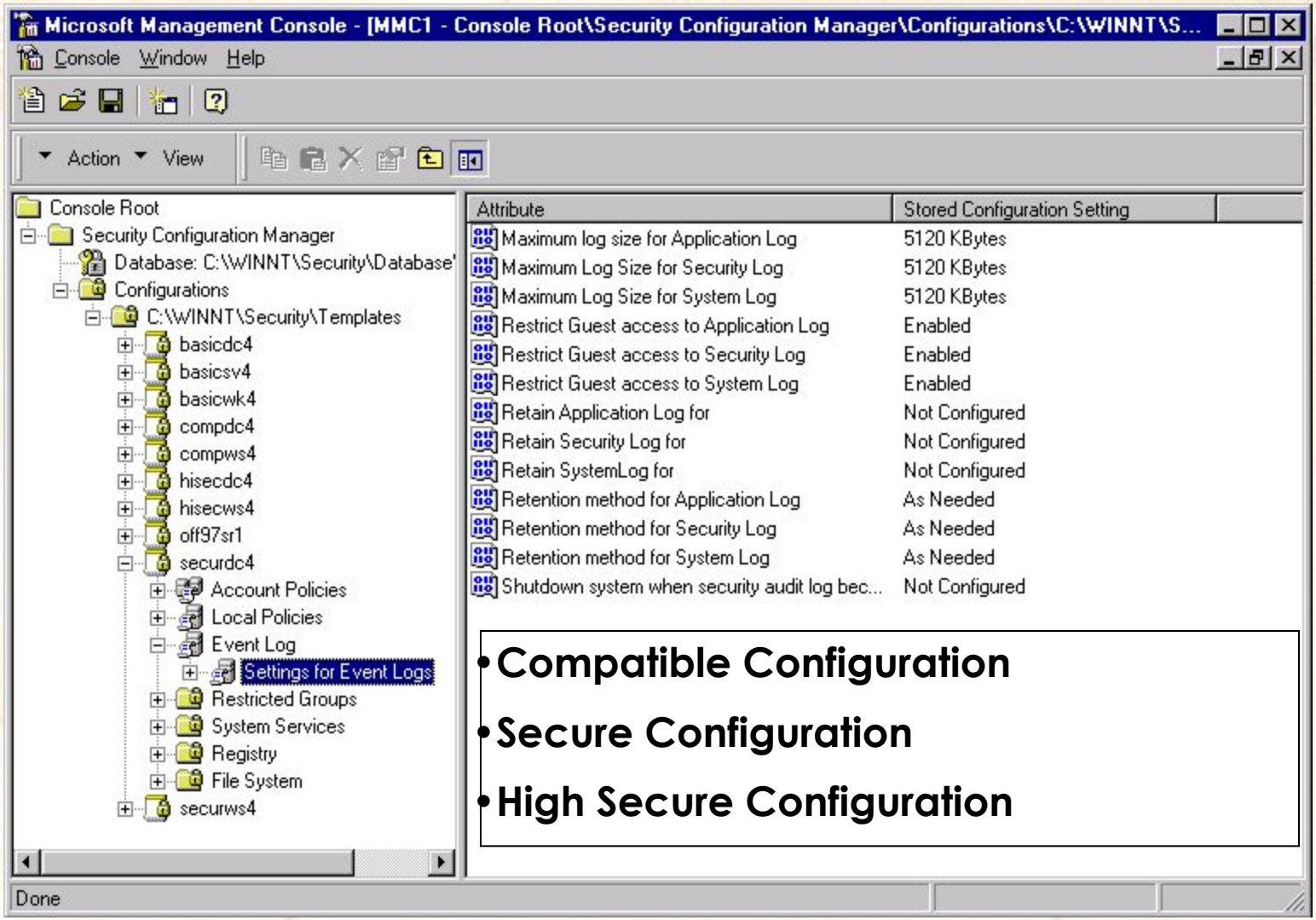
C2 Config - Windows NT Resource Kit

Security Configuration Manager (SCM)

Руководства по настройке

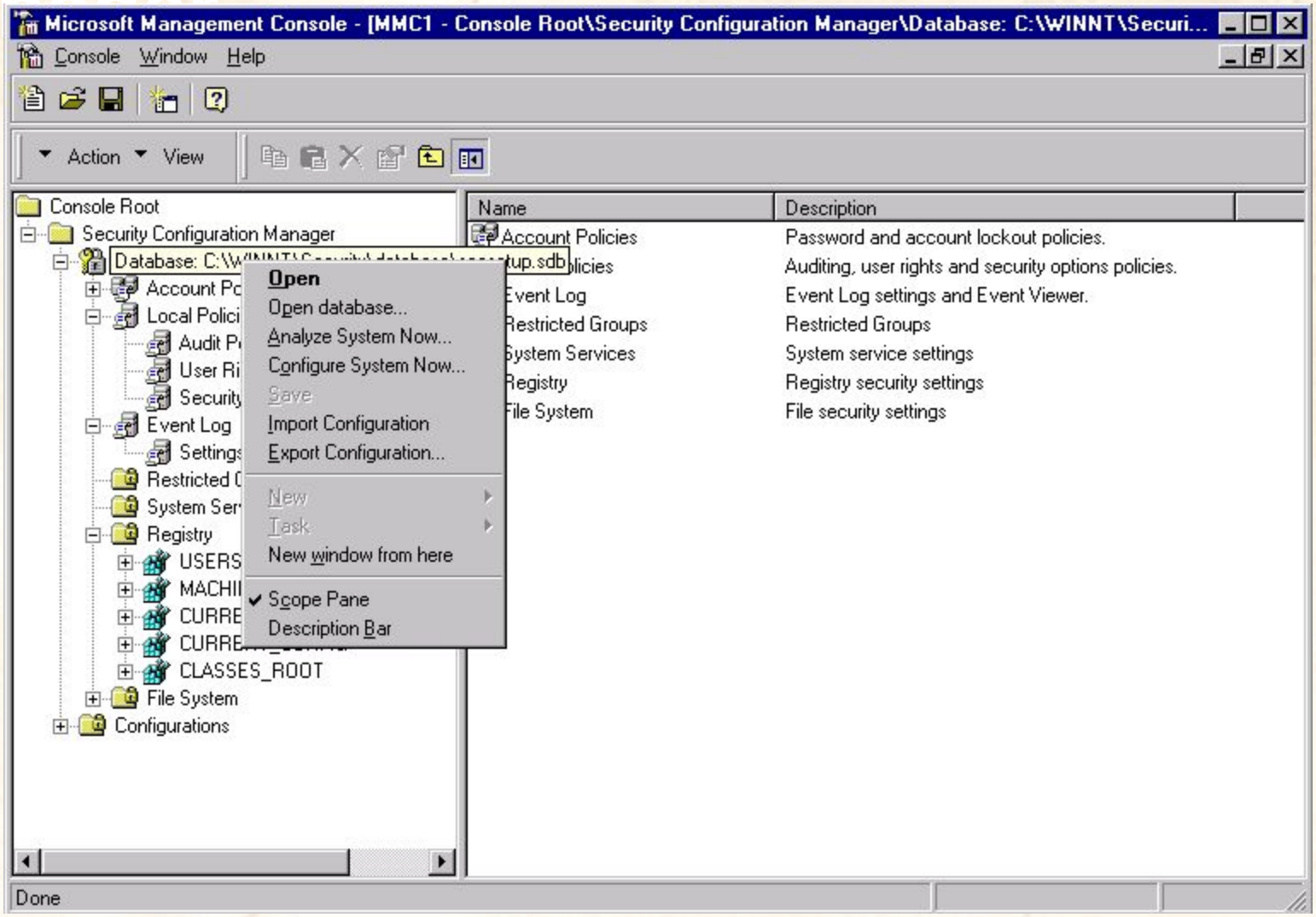
- NSA Guide
- Windows NT Security Guidelines

Security Configuration



- Compatible Configuration
- Secure Configuration
- High Secure Configuration

Security Configuration



Security Configuration