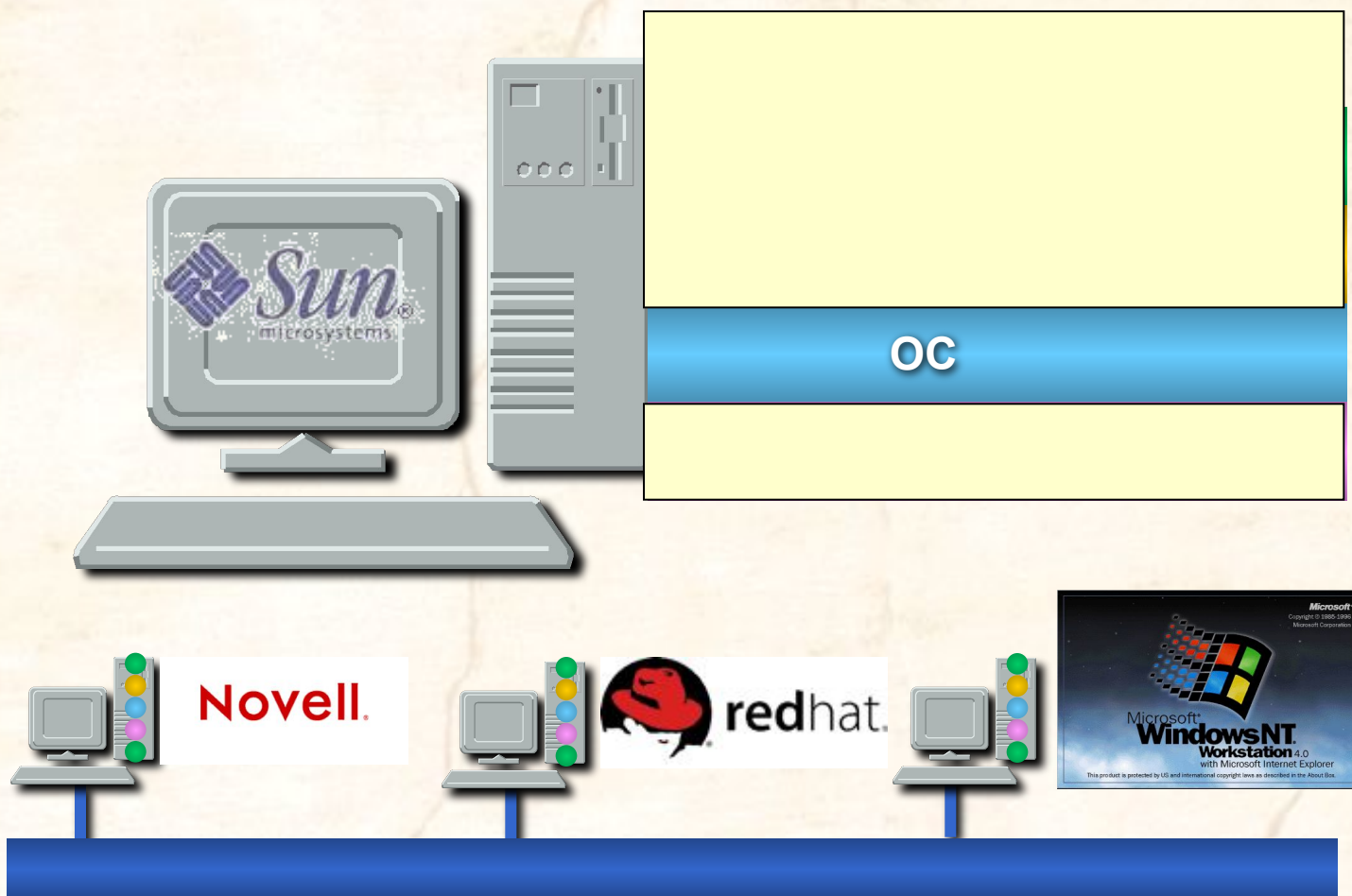


Безопасность Windows NT Server 4.0



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

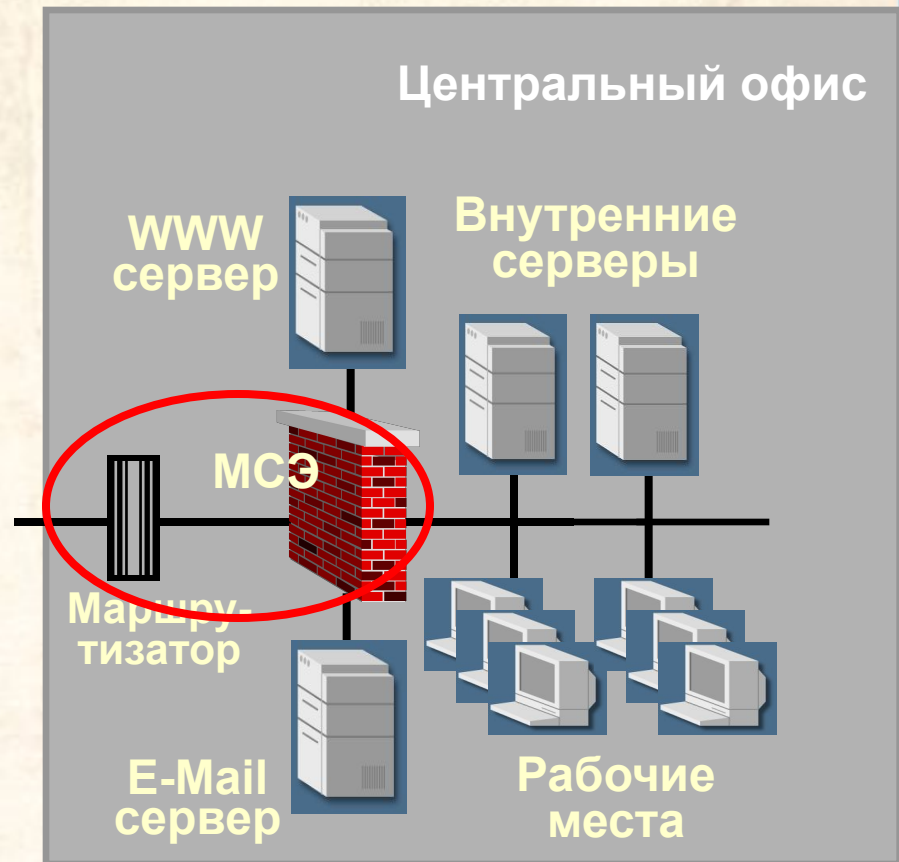
- Клиентские рабочие станции
- Серверы бизнес приложений
- Серверы БД
- Серверы файлов и печати
- **Серверы DMZ**



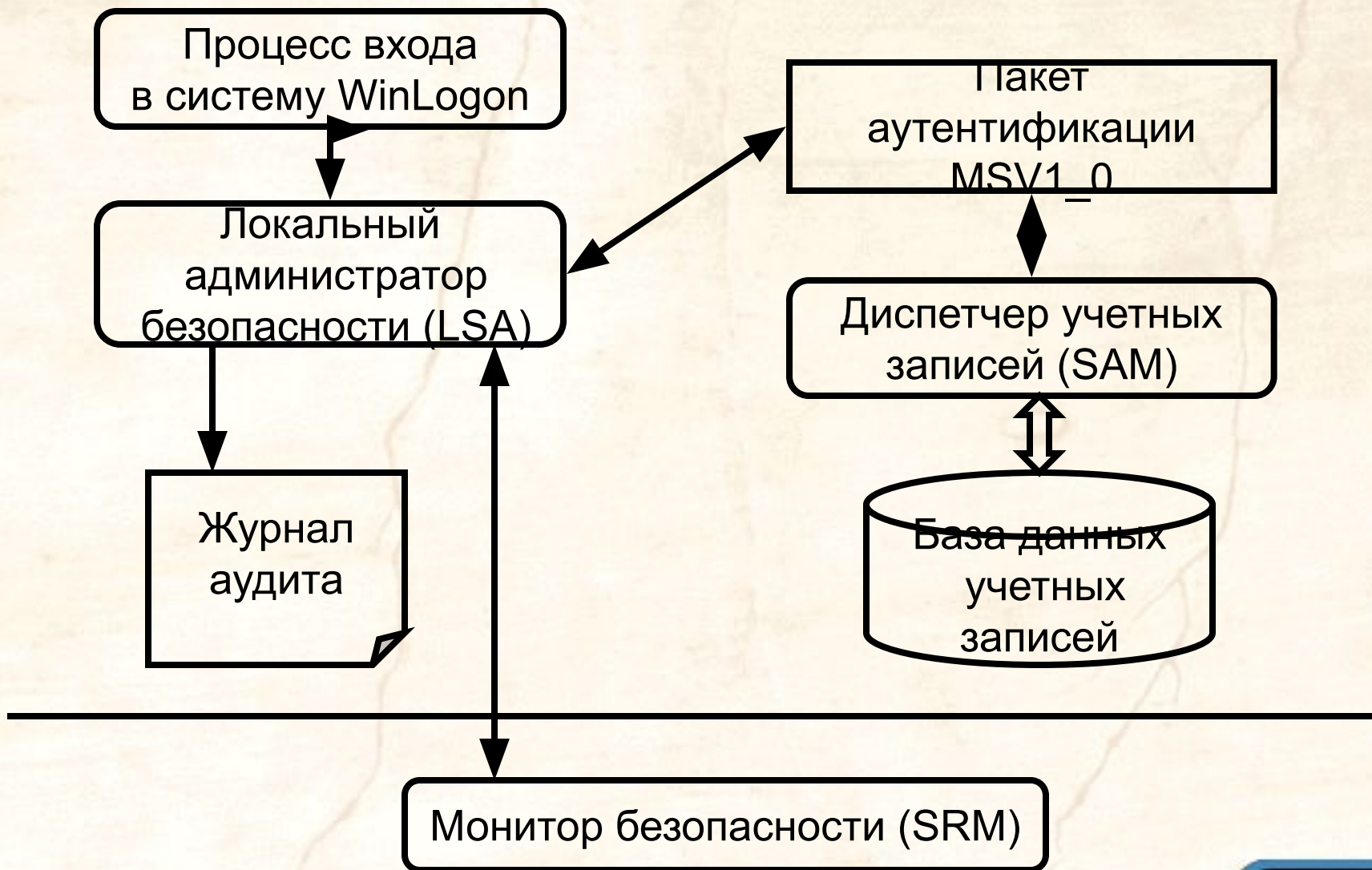
Корпоративная сеть

Windows NT

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



Система безопасности



Система безопасности

Процесс входа
в систему WinLogon

Локальный
администратор
безопасности (LSA)

Журнал
аудита

Монитор безопасности (SRM)

Принимает запросы на
регистрацию

\\...\System32\Winlogon.exe

Система безопасности

Процесс входа
в систему WinLogon

Локальный
администратор
безопасности (LSA)

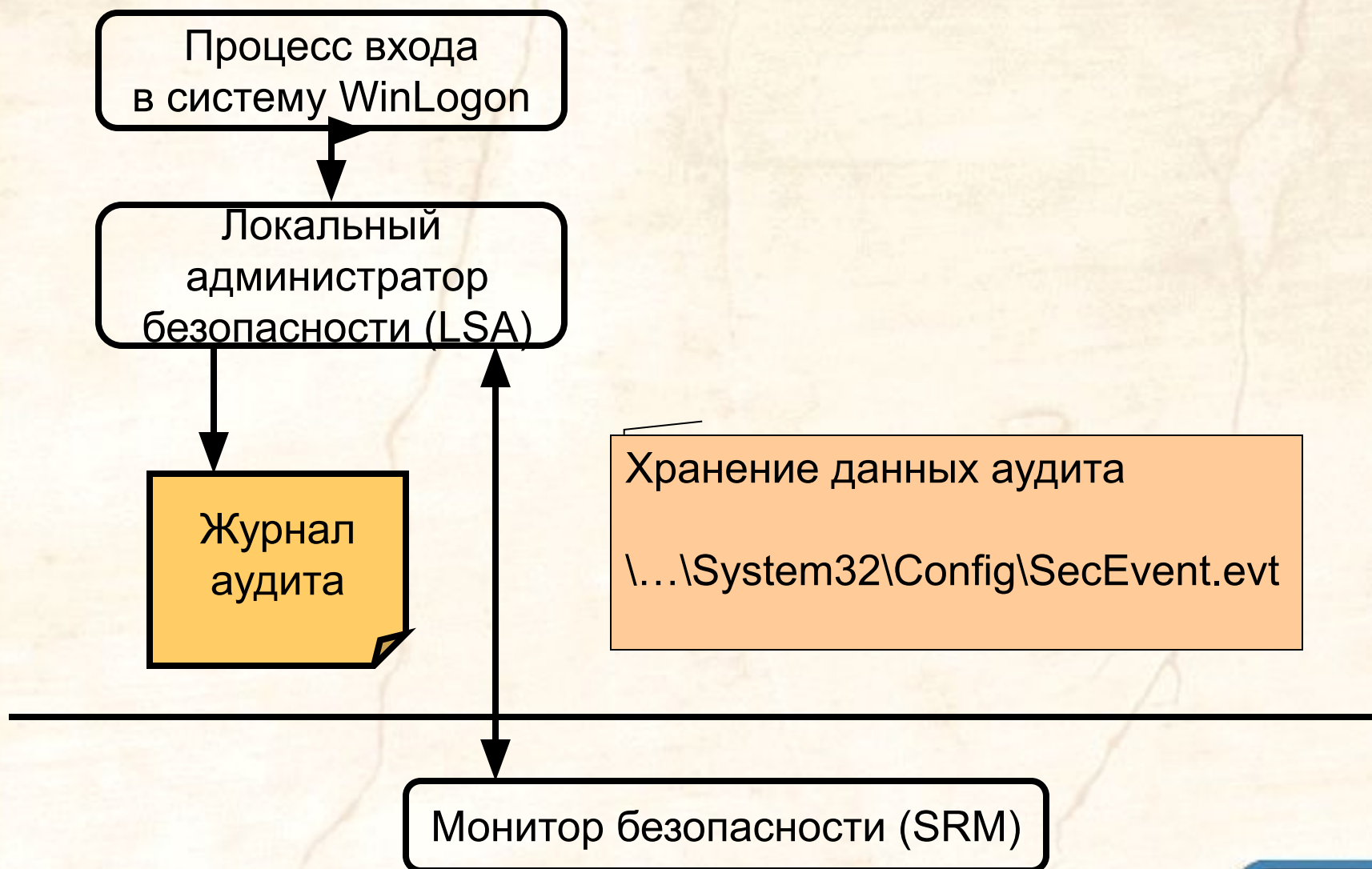
Журнал
аудита

Монитор безопасности (SRM)

- 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

Пакет
аутентификации
MSV1_0

Диспетчер учетных
записей (SAM)

База данных
учетных
записей

Монитор безопасности (SRM)

Система безопасности

Поддержка базы данных
пользовательских бюджетов

\\...\System32\Samsrv.dll

Пакет
аутентификации
MSV1_0

Диспетчер учетных
записей (SAM)

База данных
учетных
записей

Монитор безопасности (SRM)

Система безопасности

Хранение информации о бюджетах пользователей, групп, компьютеров

Хранится в нескольких местах

- \...\System32\config\sam
- \...\repair\sam._
- ERD

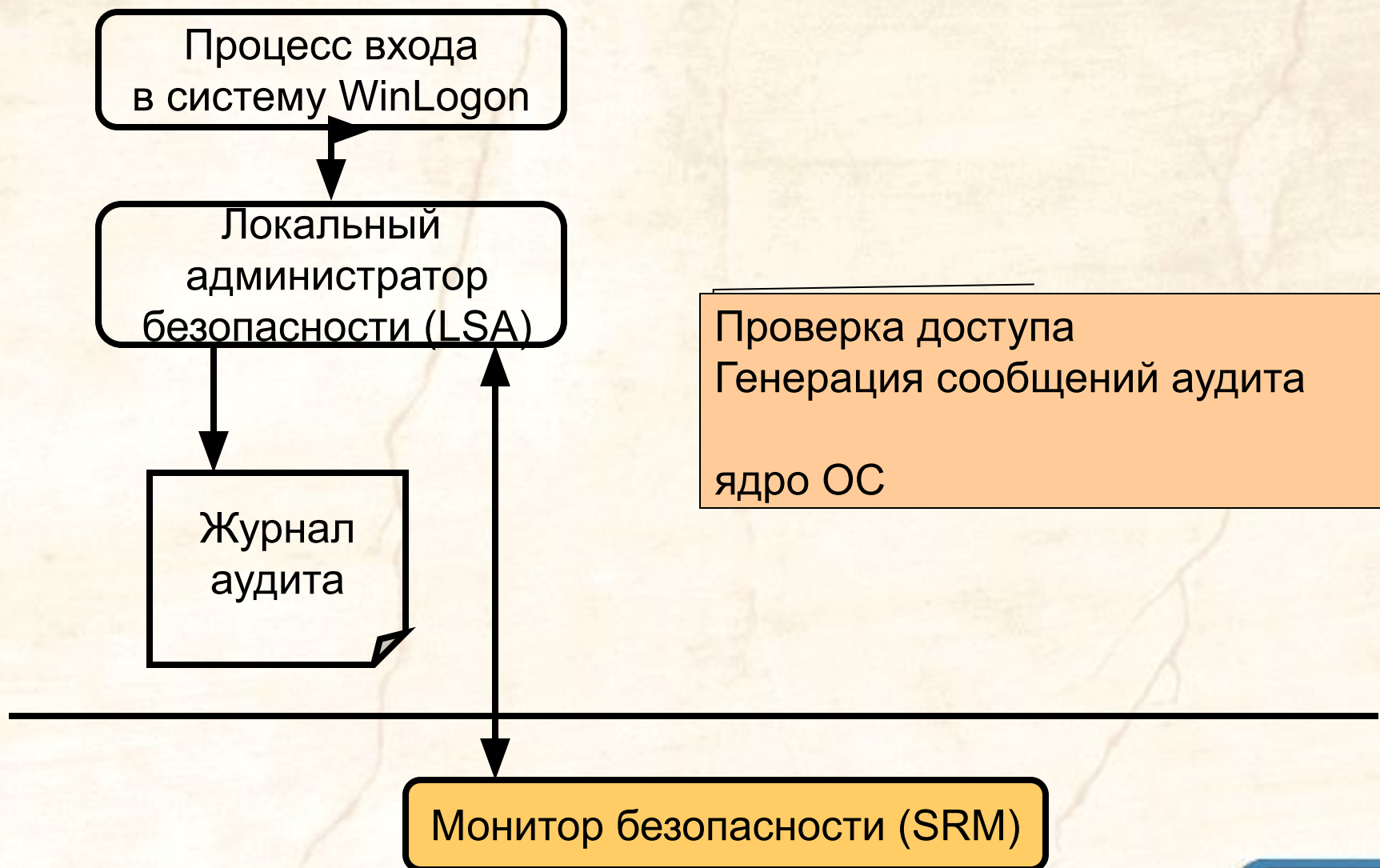
Пакет аутентификации MSV1_0

Диспетчер учетных записей (SAM)

База данных учетных записей

Монитор безопасности (SRM)

Система безопасности



Бюджеты

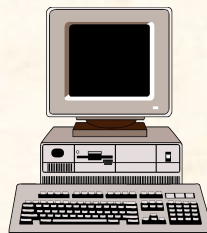
SID (Security ID)



Пользователь



Группа



Компьютер

Процесс регистрации

CTRL+ALT+DEL

Ввод данных

Winlogon □ LSA

LSA □ MSV1_0

Бюджет
локаль
ный?

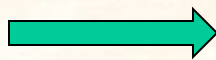
Нет

Обработка на удалённом
узле и получение SID

Да

Получение SID

Winlogon □ Win32



Рабочий стол

Имя: Пароль: Домен:

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 00000000

4.



5.

no



+

no



= 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

Account Policy ✕

Computer: GANDALF

OK
Cancel
Help

Password Restrictions

Maximum Password Age

Password Never Expires

Expires In Days

Minimum Password Age

Allow Changes Immediately

Allow Changes In Days

Minimum Password Length

Permit Blank Password

At Least Characters

Password Uniqueness

Do Not Keep Password History

Remember Passwords

No account lockout

Account lockout

Lockout after bad logon attempts

Reset count after minutes

Lockout Duration

Forever (until admin unlocks)

Duration minutes

Users must log on in order to change password

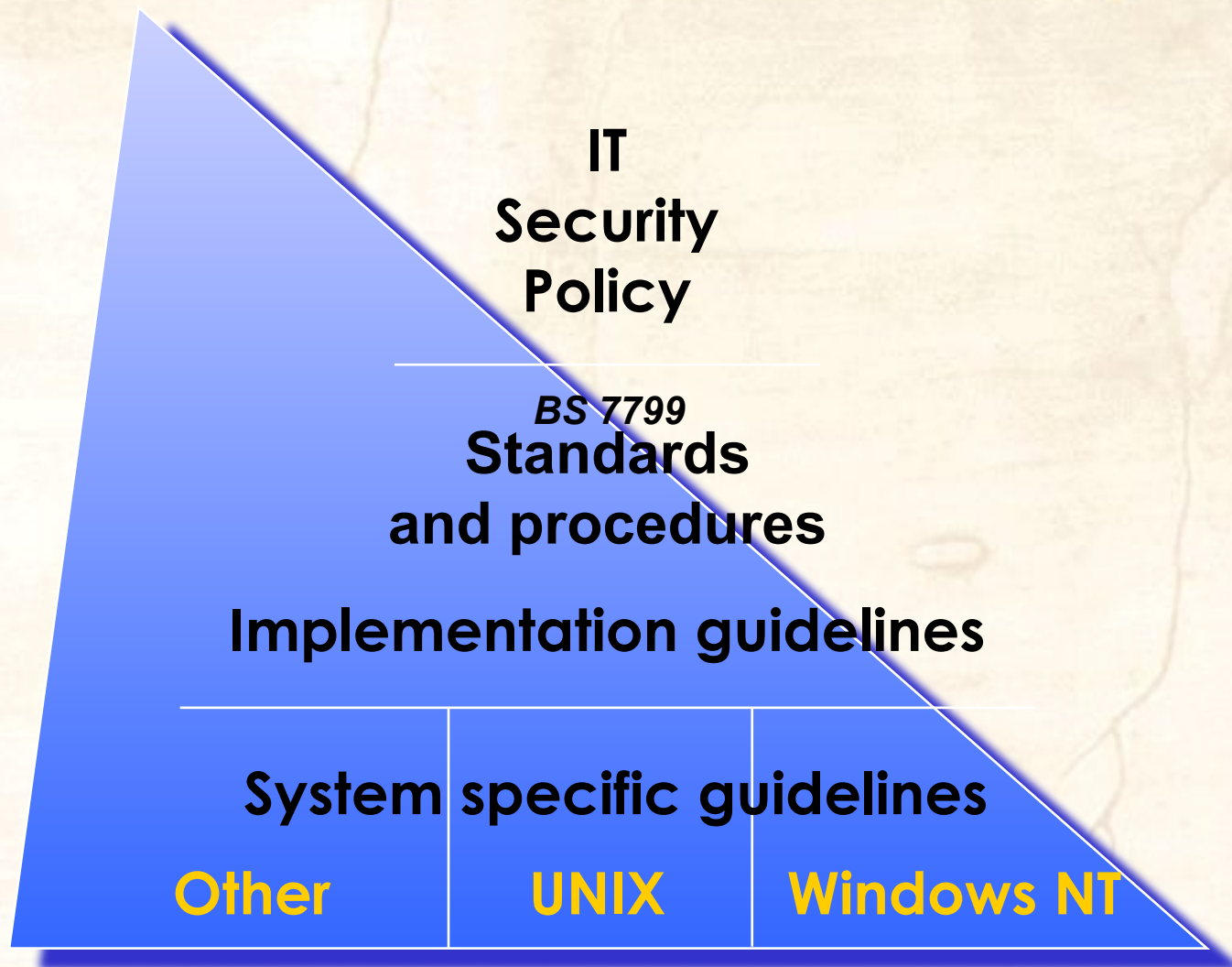
Права пользователей

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

Ma

The screenshot displays the Microsoft Management Console (MMC) interface for Security Configuration Manager. The left pane shows a tree view of the console root, with 'Settings for Event Logs' selected under the 'Event Log' folder. The right pane shows a list of configuration settings for event logs, including log sizes, retention methods, and access restrictions.

Attribute	Stored Configuration Setting
Maximum log size for Application Log	5120 KBytes
Maximum Log Size for Security Log	5120 KBytes
Maximum Log Size for System Log	5120 KBytes
Restrict Guest access to Application Log	Enabled
Restrict Guest access to Security Log	Enabled
Restrict Guest access to System Log	Enabled
Retain Application Log for	Not Configured
Retain Security Log for	Not Configured
Retain SystemLog for	Not Configured
Retention method for Application Log	As Needed
Retention method for Security Log	As Needed
Retention method for System Log	As Needed
Shutdown system when security audit log bec...	Not Configured

- **Compatible Configuration**
- **Secure Configuration**
- **High Secure Configuration**

Security Configuration

Master

The screenshot displays the Microsoft Management Console (MMC) interface for the Security Configuration Manager. The console tree on the left shows the hierarchy: Console Root > Security Configuration Manager > Database: C:\WINNT\Security\... > Local Policies > Security. A context menu is open over the Security folder, listing options such as Open, Save, Import Configuration, and Export Configuration. The main pane on the right shows a table of configurations.

Name	Description
Account Policies	Password and account lockout policies.
Event Log	Event Log settings and Event Viewer.
Restricted Groups	Restricted Groups
System Services	System service settings
Registry	Registry security settings
File System	File security settings

Security Configuration

Manager

Microsoft Management Console - [MMC1 - Console Root\Security Configuration Manager\Database: C:\WINNT\Security...]

Console Window Help

Action View

Console Root

- Security Configuration Manager
 - Database: C:\WINNT\Security\database\
 - Account Policies
 - Local Policies
 - Audit Policy**
 - User Rights Assignment
 - Security Options
 - Event Log
 - Settings for Event Logs
 - Restricted Groups
 - System Services
 - Registry
 - USERS
 - MACHINE
 - CURRENT_USER
 - CURRENT_CONFIG
 - CLASSES_ROOT
 - File System
 - Configurations

Attribute	Stored Configuration ...	Analyzed System Set...
Audit Account Management	Success,Failure	Failure
Audit Logon Events	Failure	Failure
Audit Object Access	No Auditing	Failure
Audit Policy Change	Success,Failure	Failure
Audit Privilege Use	Failure	Failure
Audit Process Tracking	No Auditing	No Auditing
Audit System Events	Success,Failure	Failure

Done