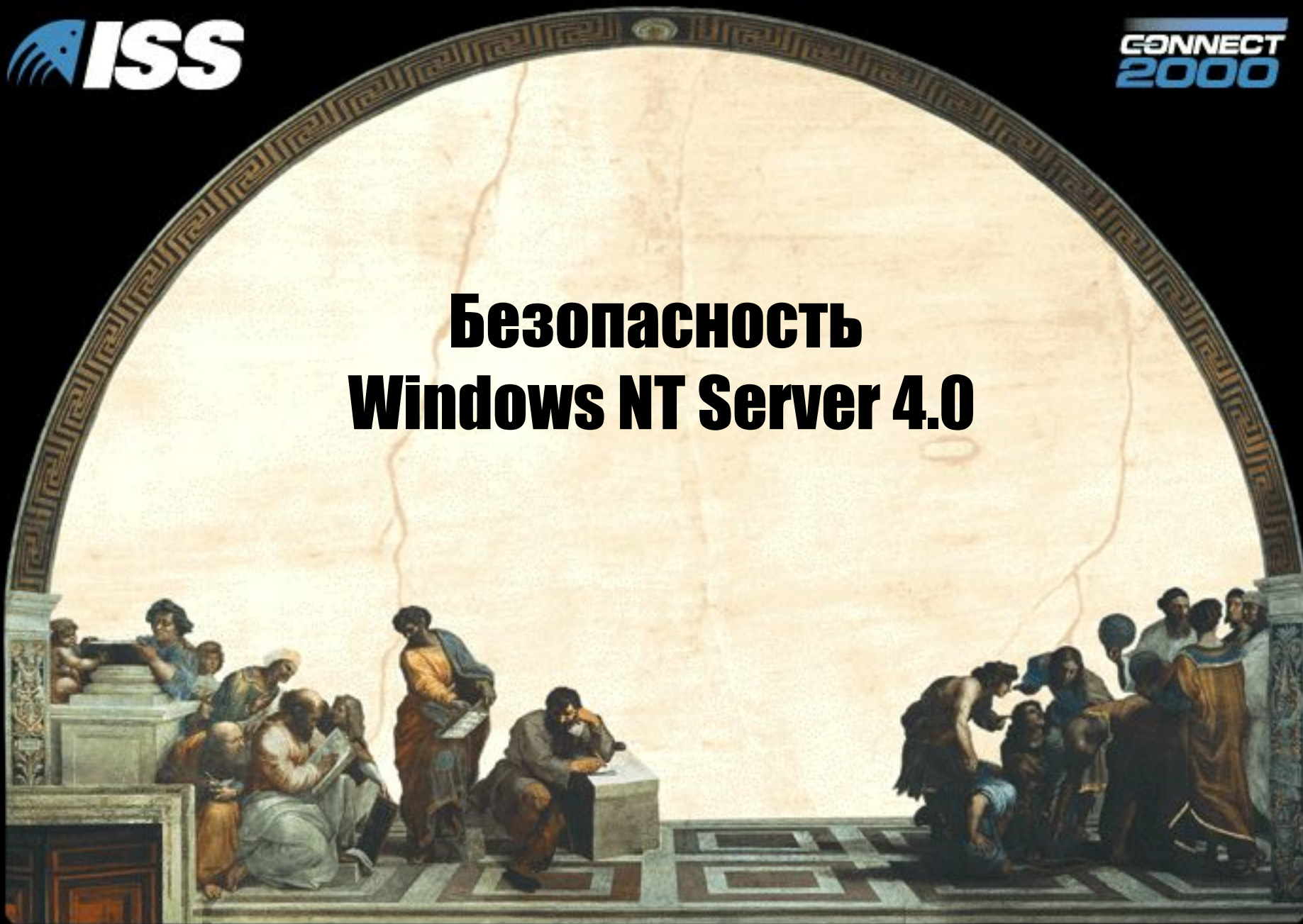
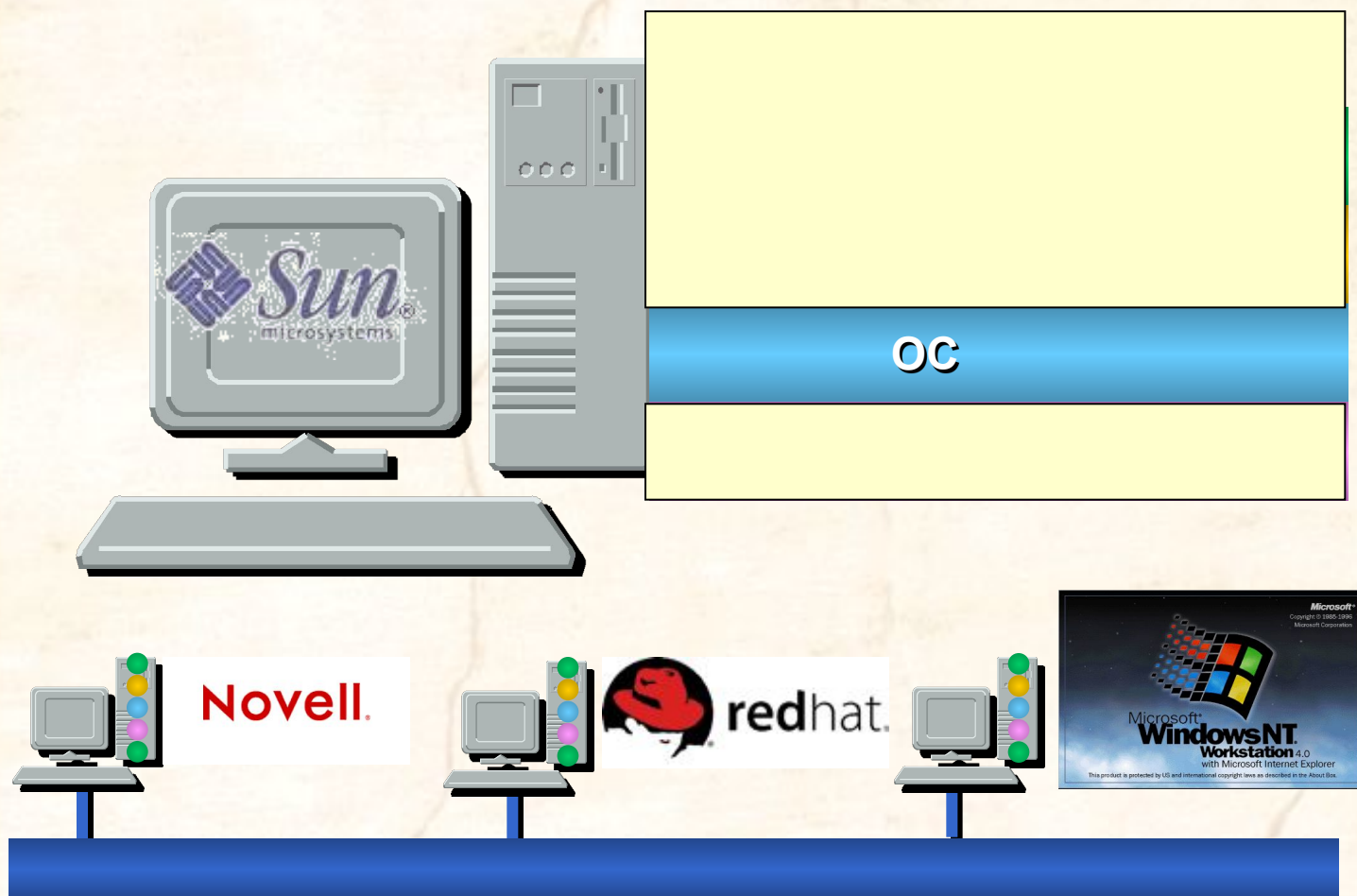


Безопасность Windows NT Server 4.0



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**



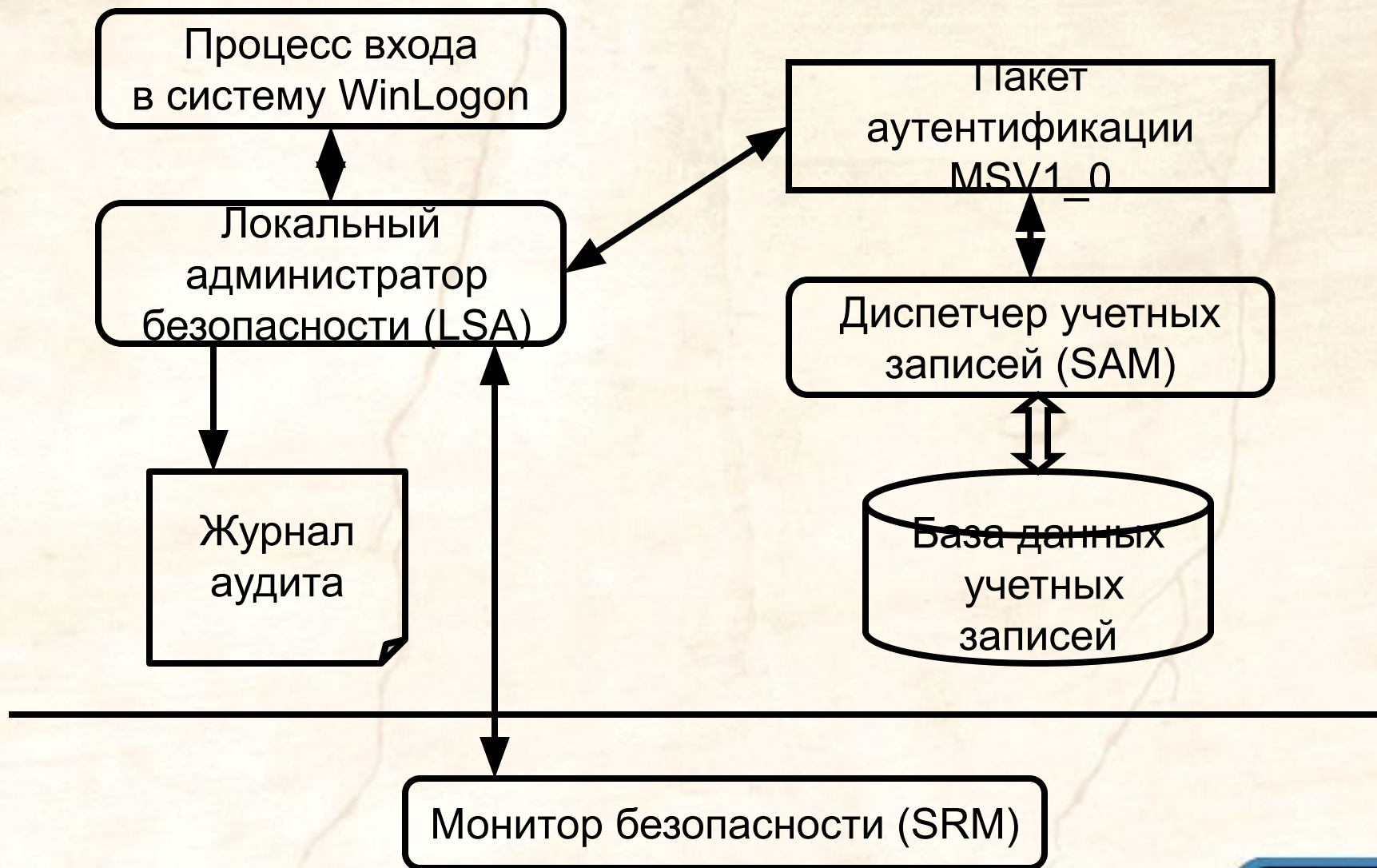
Корпоративная сеть

Windows NT

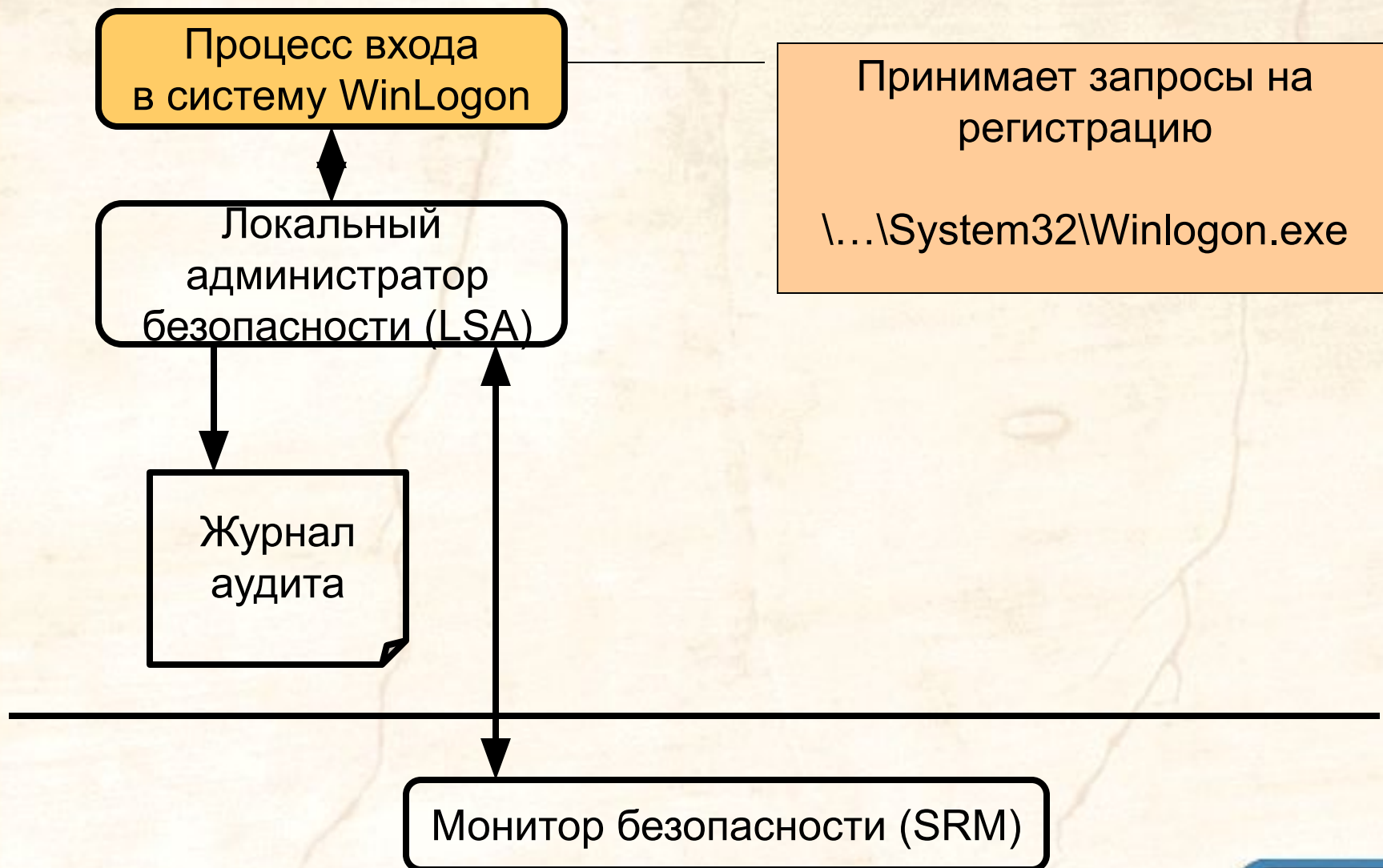
- Клиентские рабочие станции
- Серверы бизнес приложений
- Серверы БД
- Серверы файлов и печати
- Серверы DMZ
- Маршрутизаторы, МЭ



Система безопасности



Система безопасности



Система безопасности

Процесс входа
в систему WinLogon

Локальный
администратор
безопасности (LSA)

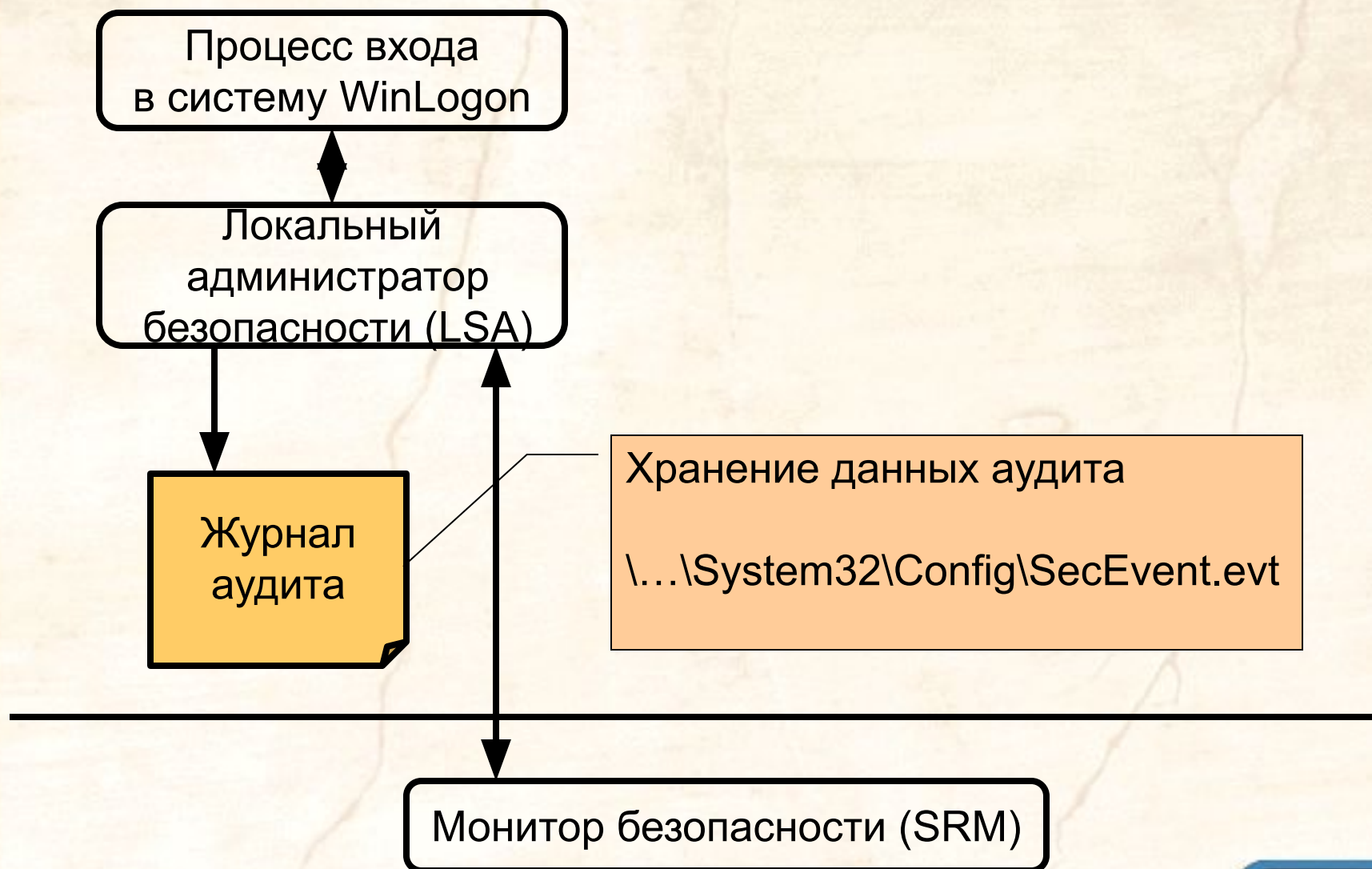
Журнал
аудита

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

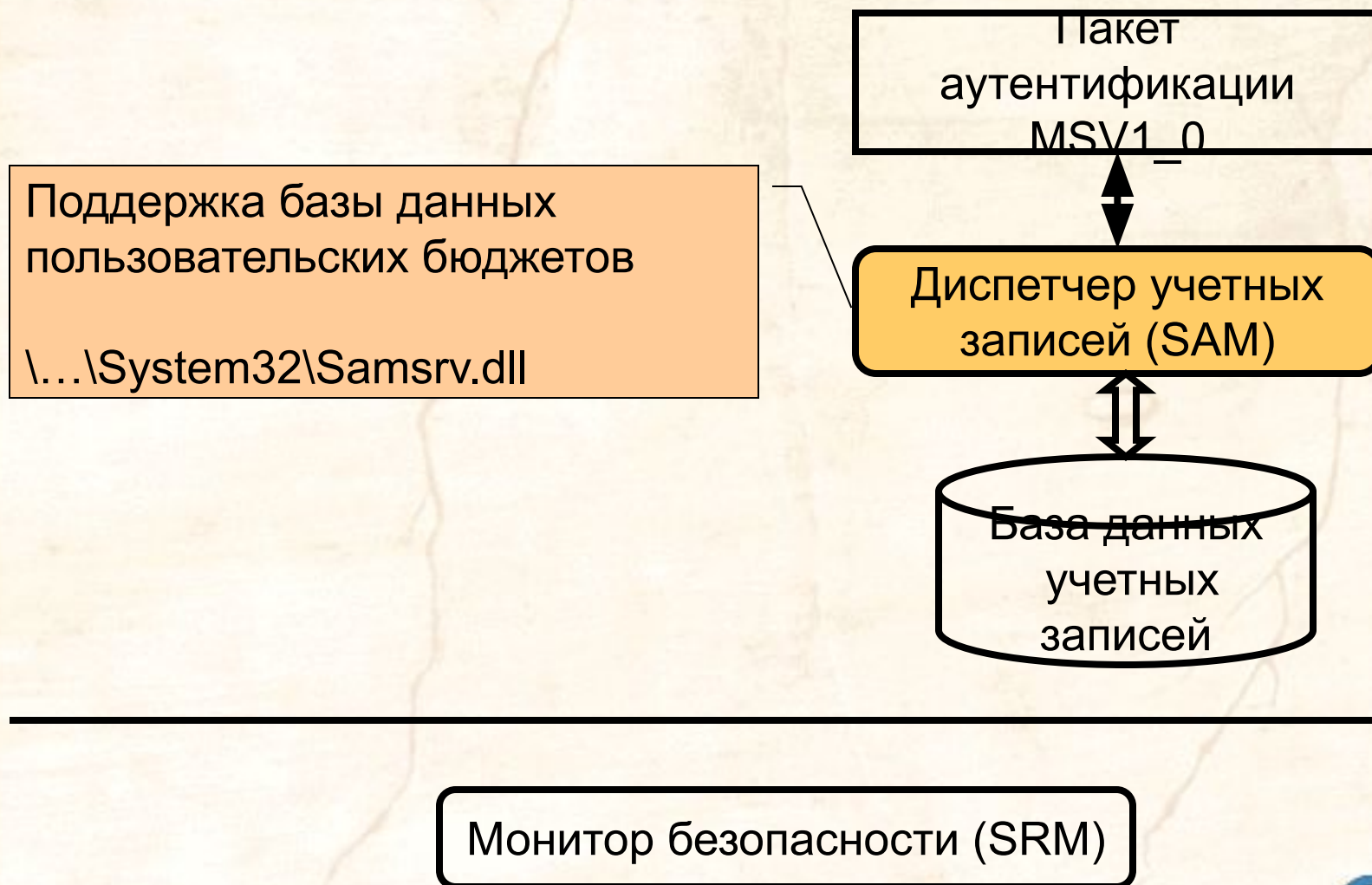
Пакет
аутентификации
MSV1_0

Диспетчер учетных
записей (SAM)

База данных
учетных
записей

Монитор безопасности (SRM)

Система безопасности

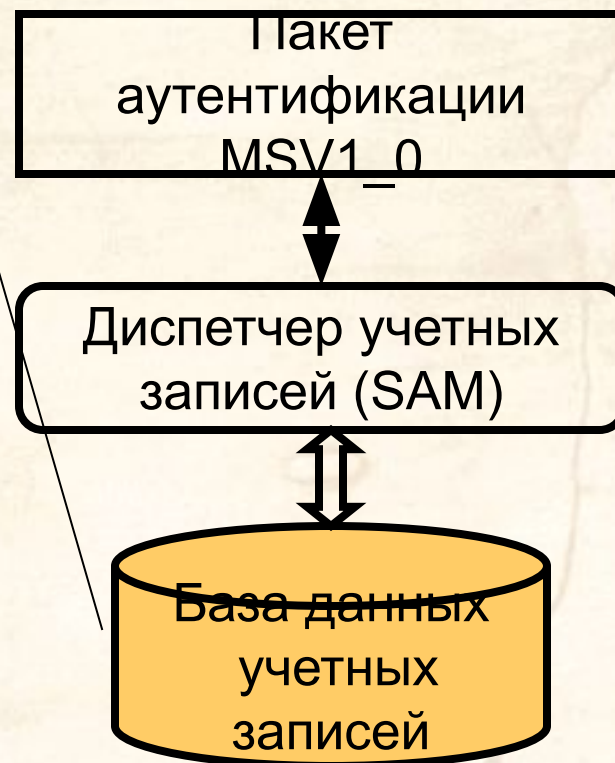


Система безопасности

Хранение информации о бюджетах пользователей, групп, компьютеров

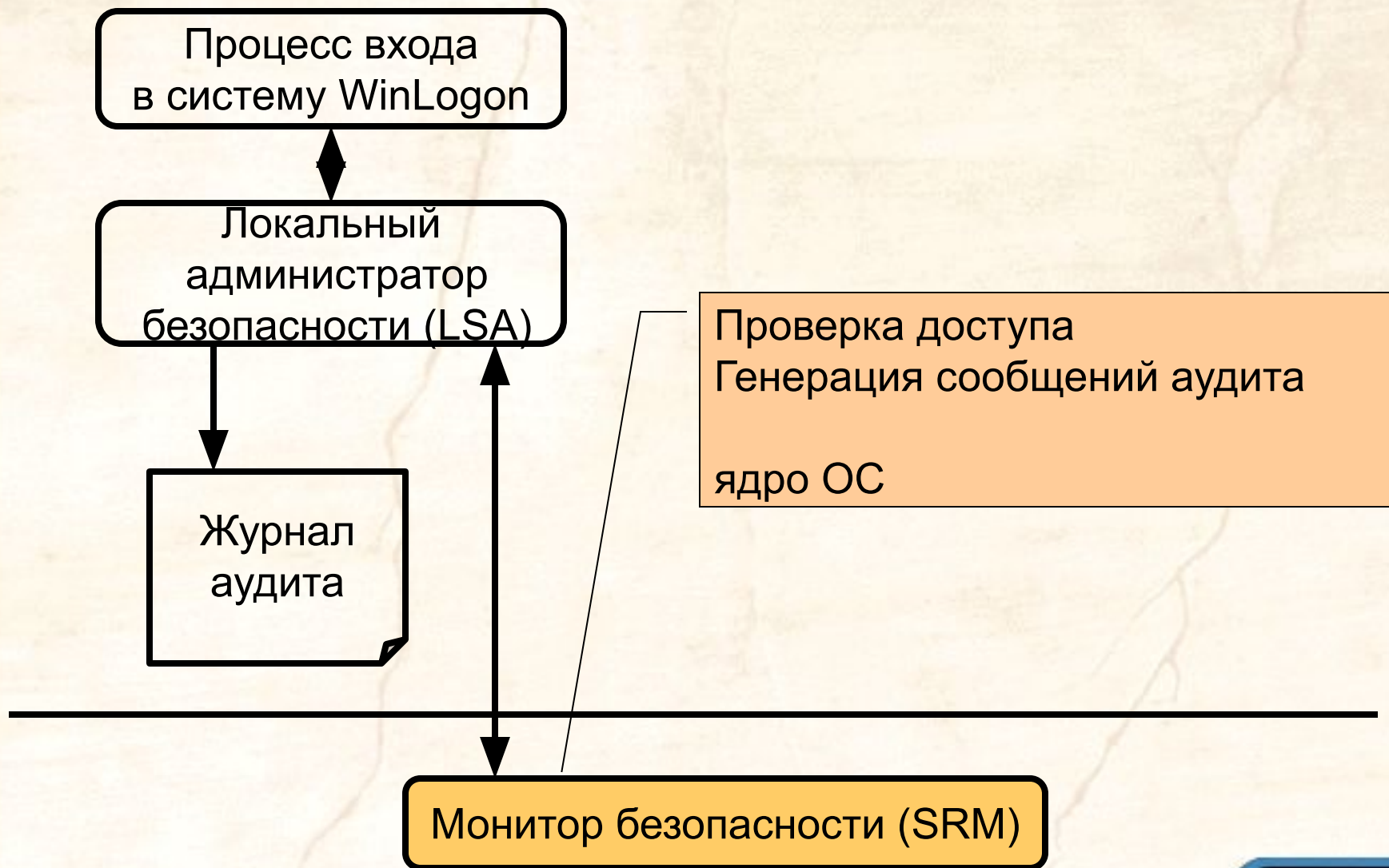
Хранится в нескольких местах

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

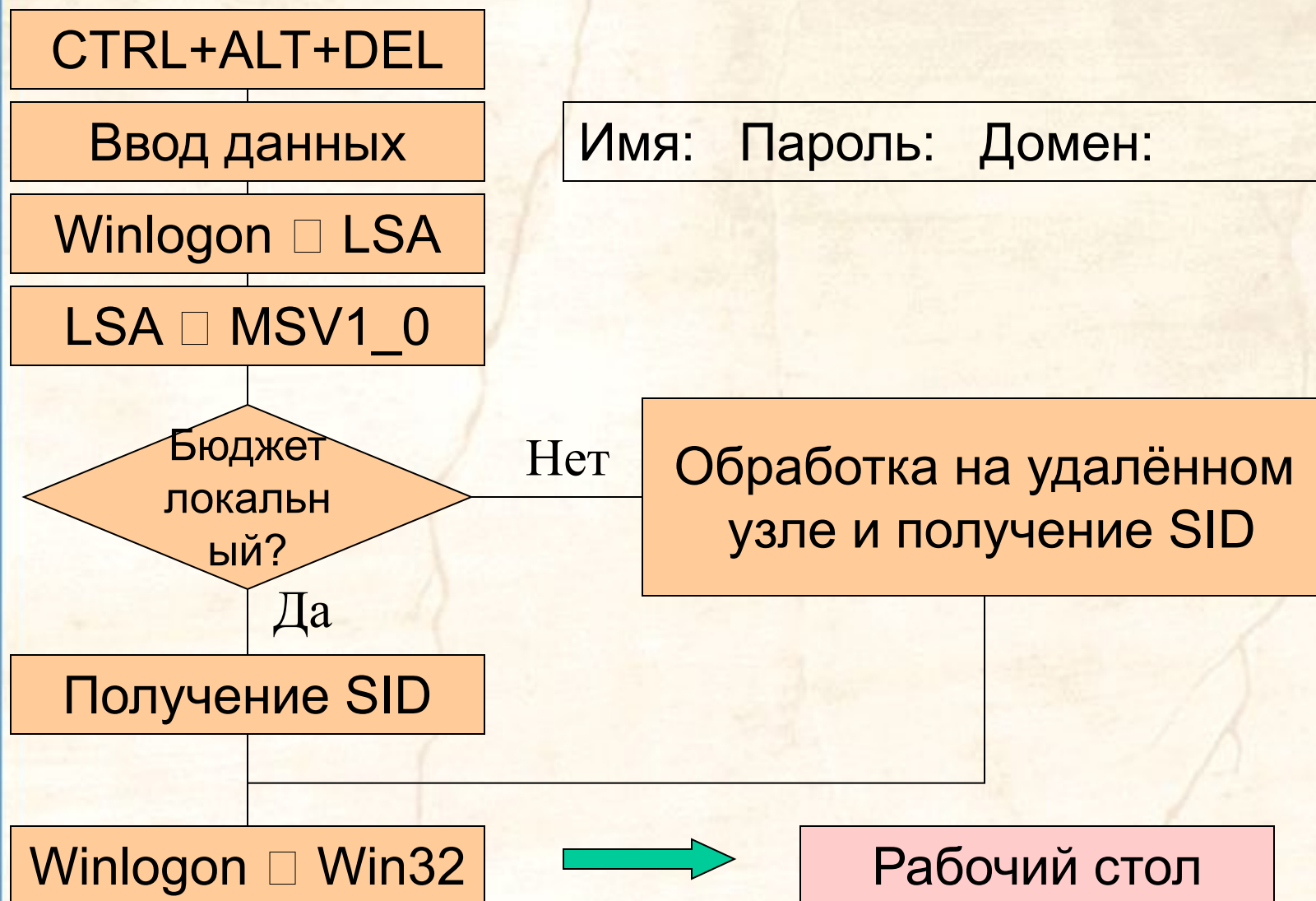


Монитор безопасности (SRM)

Система безопасности

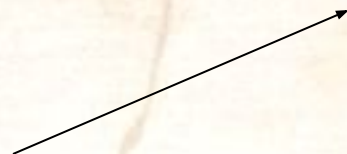


Процесс регистрации



Бюджеты

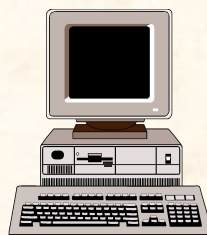
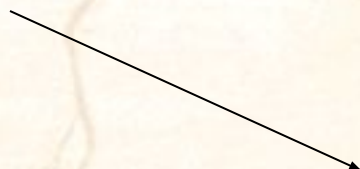
SID (Security ID)



Пользователь



Группа



Компьютер

Бюджеты

SID (Security ID)

S-R-I-S...

S-1-5-21-917267712-1342860078-1792151419-500

RID

подзначение (subauthority value(s))

Значение идентификатора полномочий
(identifier-authority value)

Уровень контроля (revision level)

Обозначение SID

Маркер безопасного доступа

Пользователь
Master (SID)

Группы

Users (SID)

Interactive (SID)

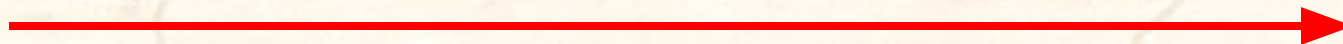
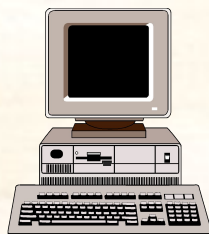
Everyone (SID)

Пользовательские права
SeSystemtimePrivelege



Маркер безопасного доступа

Пользователь
Master (SID)
Группы
Users (SID)
Interactive (SID)
Everyone (SID)
Пользовательские права
SeSystemtimePrivilege



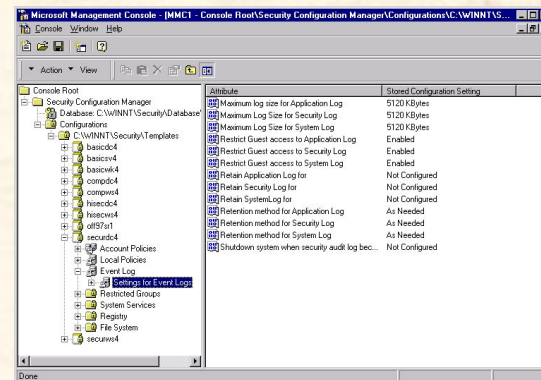
Субъект доступа



=

Пользователь
Master

...



Субъект доступа = Маркер безопасного доступа + Программа

- Простой субъект
- Субъект-сервер

Объект

- Тип данных
- Атрибуты
- Набор операций, выполняемых над объектом

An orange folder icon with a white border and a shadow, containing the word "Объект" in white text.

Объект

Объект доступа

D:\Winnt\System32\regedt32.exe

Owner: Administrator

ACL:

Grant: (all) Administrator

Grant: (R): Users

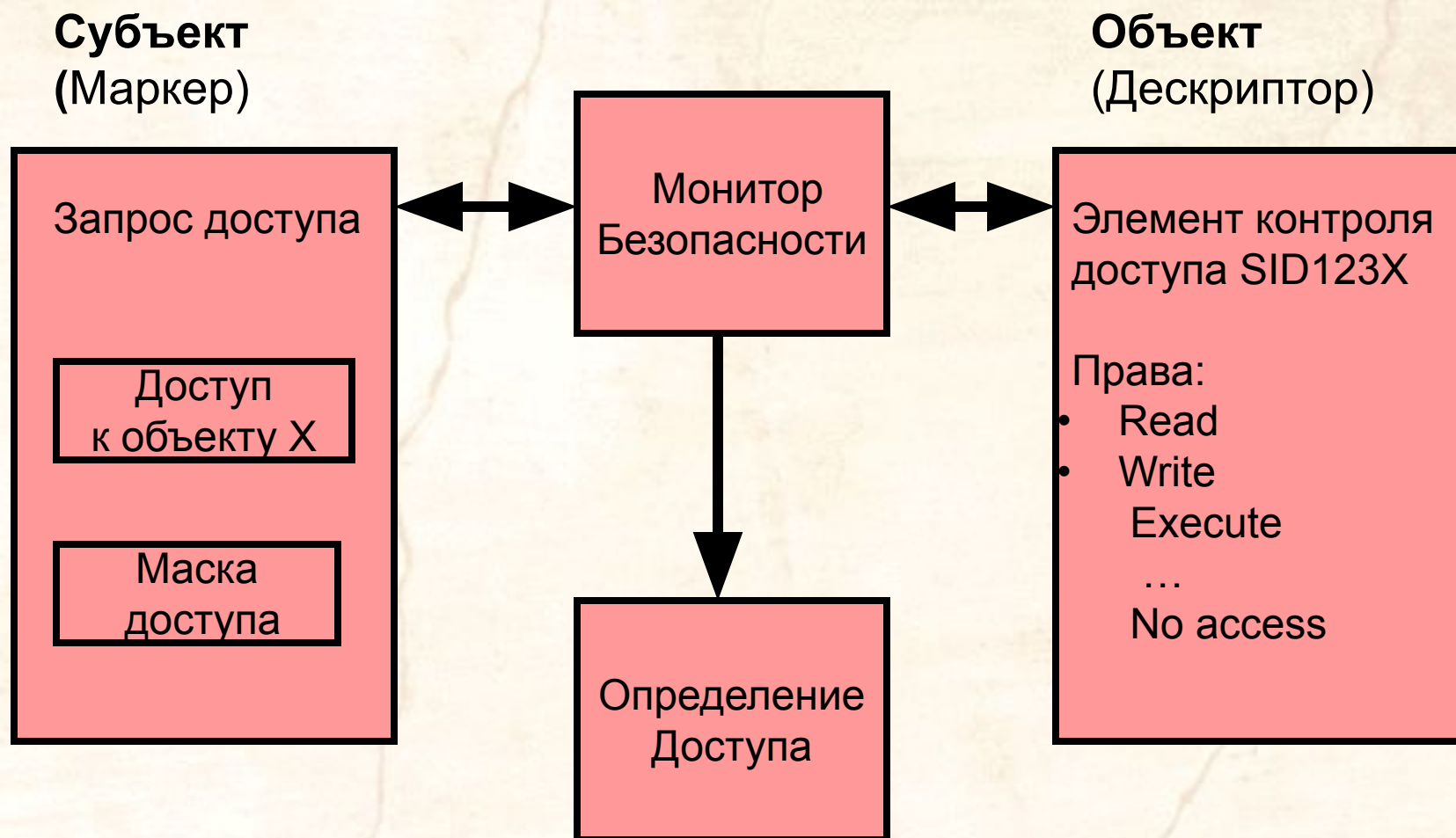
Revoke: Everyone

System ACL:

Audit: (R): Users

Пример объекта - файл

Получение доступа



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.



+



= хэш (16 байт)

База данных SAM

Windows NT Password.

user: user1

password: qwerty

1. Конвертирование в UNICODE
2. Шифрование по MD4

Шифрование SAM

Утилита SYSKEY

- Секретный ключ на жёстком диске
- Секретный ключ на дискете
- Секретный ключ – пароль пользователя

Фильтр для паролей

Passfilt.dll

- Длина пароля не менее 6 знаков
- Обязательные символы (верхний/нижний регистр, числа, спецсимволы)
- Пароль не должен содержать имя пользователя

Утилита Passprop

- Включение режима усложнения пароля
- Управление блокировкой учётной записи «Administrator»

Утилита Passprop

Пароль должен содержать символы
обоих регистров (**Aa, Gf, Ud**)

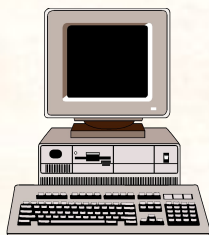
или

Пароль должен содержать цифры или
спецсимволы (**a1, g3, G%, &\$**)

Требования к паролям

Сетевая аутентификация

Клиент



Установление связи



Сервер



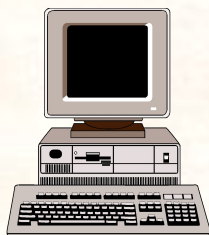
Запрос пароля



- Передача пароля в открытом виде
- Передача хэша пароля
- Механизм «запрос/отклик»

Сетевая аутентификация

Клиент



Сервер



Установление связи



SMB_CON_NEGOTIATE



Запрос пароля



SMB_SESSION_SETUP&X



Зашифрованный запрос

Аналогичная
операция и
сравнение

Механизм «запрос/отклик» в Windows NT

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

Системная политика

Настройка прав пользователей

Исправление ошибок ОС

Настройка доступа к объектам

Установка ключей реестра

Системная политика

Account Policy [X]

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

Настройка прав пользователей



Исправление ошибок ОС

Приложен
ие
Win32

Подсисте
ма
Win32

Режим пользователя

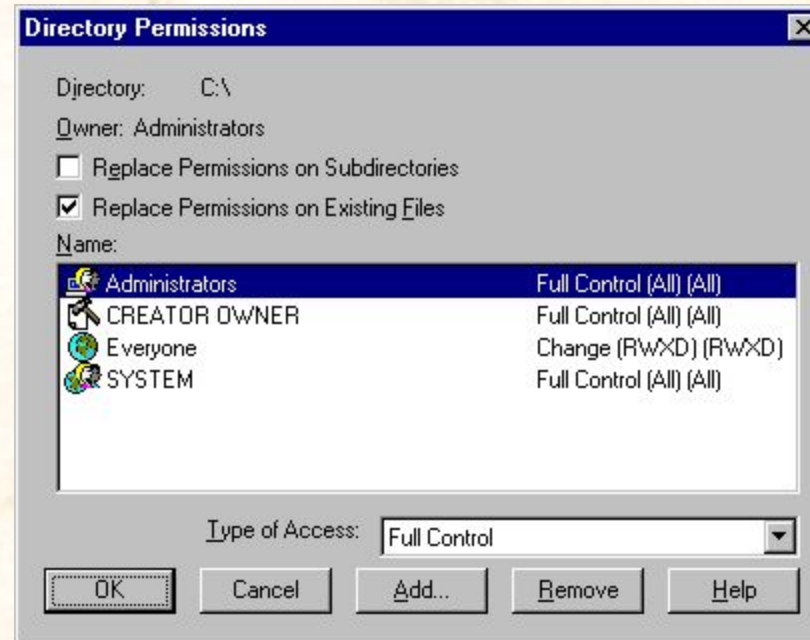
Режим ядра

Исполнительная
система
(NTExecutive)

ядро

Аппаратура

Настройка доступа к объектам



Файл подкачки

Hive: HKEY_LOCAL_MACHINE

Key: System\CurrentControlSet\Control\
\Session Manager\Memory Management

Name: ClearPageFileAtShutdown

Type: REG_DWORD

Value: 1

Установка ключей реестра

Task Manager

Hive: HKEY_CURRENT_USER

Key: Software\Microsoft\Windows\CurrentVersion
\Policies\System

Name: DisableTaskMgr

Type: REG_DWORD

Value: 1

Установка ключей реестра

Null Session

Hive: HKEY_LOCAL_MACHINE

Key: System\CurrentControlSet\Control\Lsa

Name: RestrictAnonymous

Type: REG_DWORD

Value: 1

Установка ключей реестра

Общие ресурсы

Hive: HKEY_LOCAL_MACHINE

Key: System\CurrentControlSet\Services\
\LanmanServer\Parameters

Name: AutoShareServer

Type: DWORD

Value: 0

Установка ключей реестра

Утилиты для настройки

C2 Config - Windows NT Resource Kit

Security Configuration Manager (SCM)

Руководства по настройке

- NSA Guide
- Windows NT Security Guidelines

NT Security Guidelines

Структура документа

- Level 1
- Level 2

Level 1 – незначительная модификация установок по умолчанию

Level 2 – для узлов с повышенными требованиями к безопасности

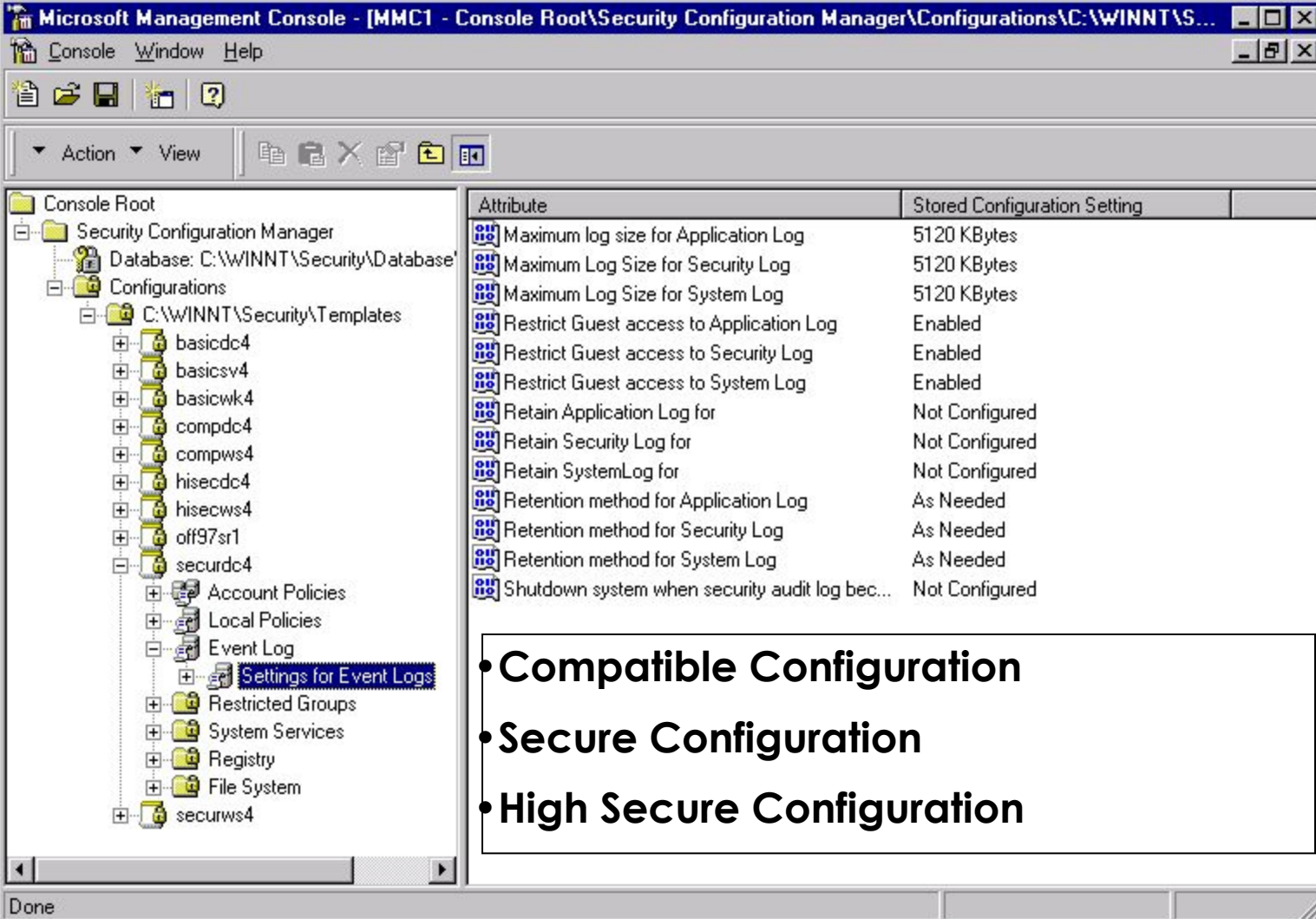
NT Security Guidelines

19
частей

1. Введение
2. Обзор документа
3. Процесс инсталляции
 1. Не копировать установленную систему
 2. Отключить неиспользуемые подсистемы
HKEY_LOCAL_MACHINE\System\CurrentControlSet\Control\Session Manager\Subsystems
 3. Отключить не нужные устройства
 4. ...

Security Configuration

Ma



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

Console Window Help

Action View

Console Root

- Security Configuration Manager
 - Database: C:\WINNT\Security\Database
 - Configurations
 - C:\WINNT\Security\Templates
 - basicdc4
 - basicsv4
 - basicwk4
 - compdc4
 - compws4
 - hisecc4
 - hisecls4
 - off97sr1
 - securdc4
 - Account Policies
 - Local Policies
 - Event Log
 - Settings for Event Logs
 - Restricted Groups
 - System Services
 - Registry
 - File System
 - securws4

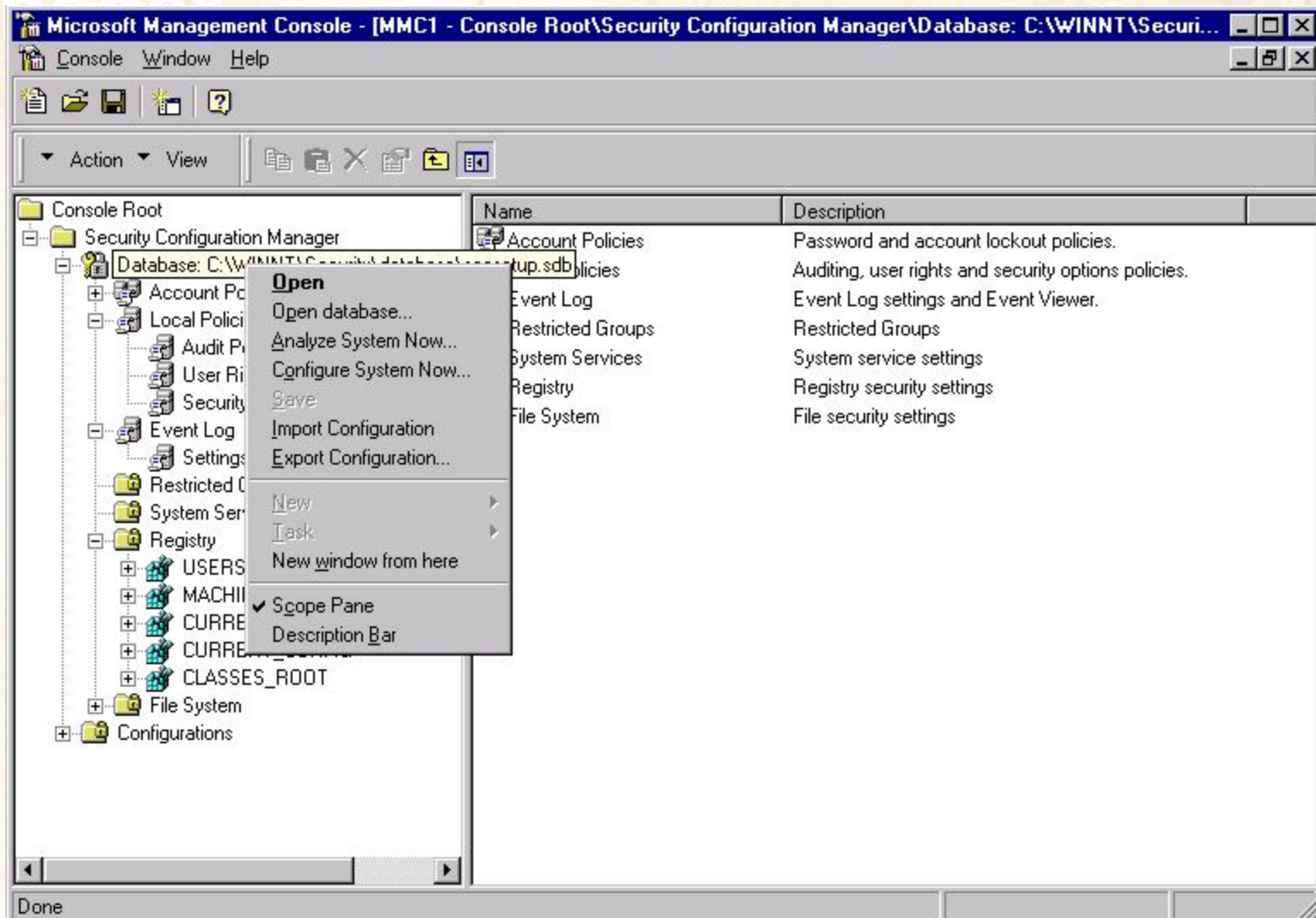
Attribute	Stored Configuration Setting
Maximum log size for Application Log	5120 KBytes
Maximum Log Size for Security Log	5120 KBytes
Maximum Log Size for System Log	5120 KBytes
Restrict Guest access to Application Log	Enabled
Restrict Guest access to Security Log	Enabled
Restrict Guest access to System 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

Done

Security Configuration

Manager



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