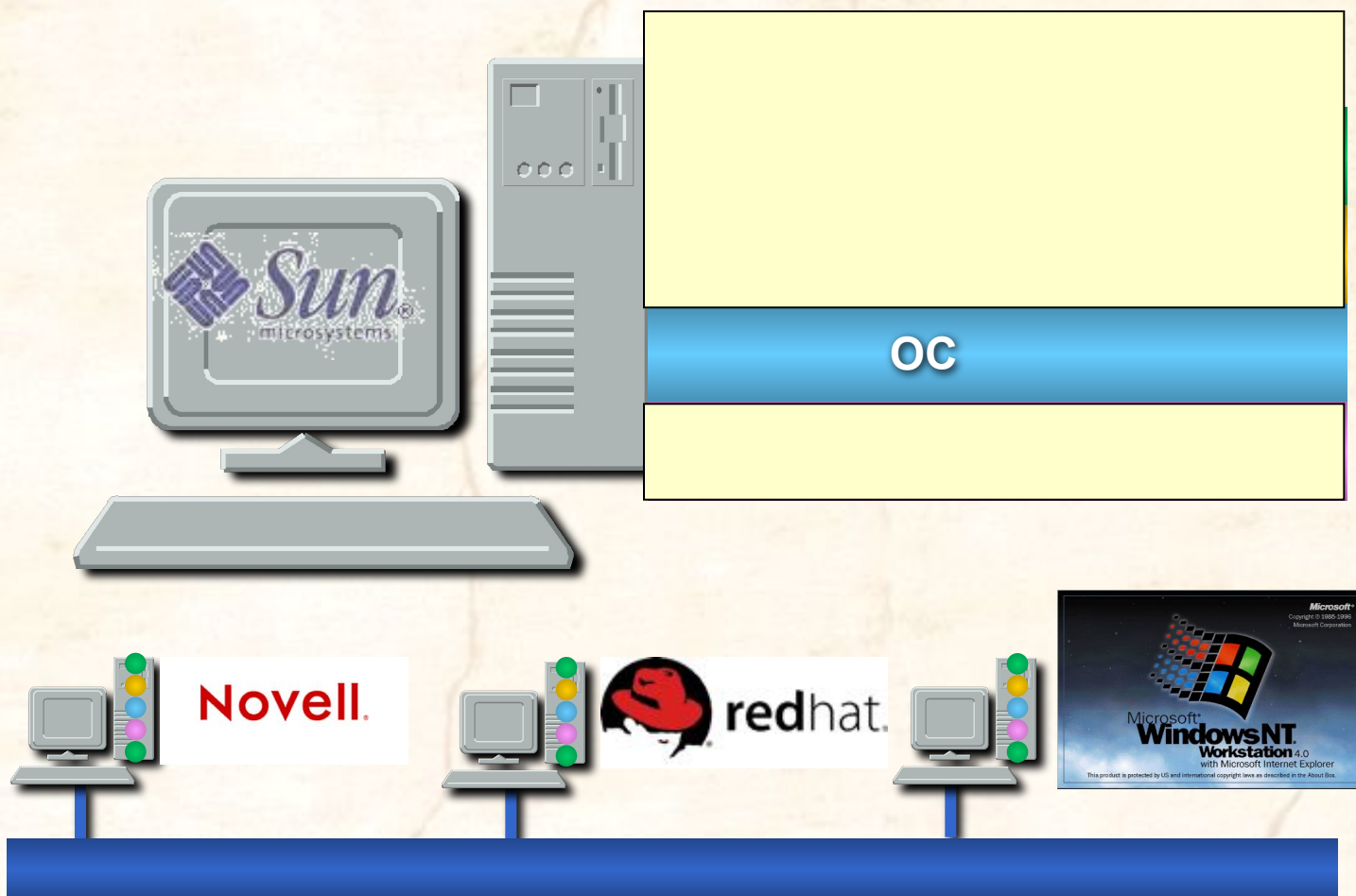


Безопасность сетевых ОС (на примере Windows NT)



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

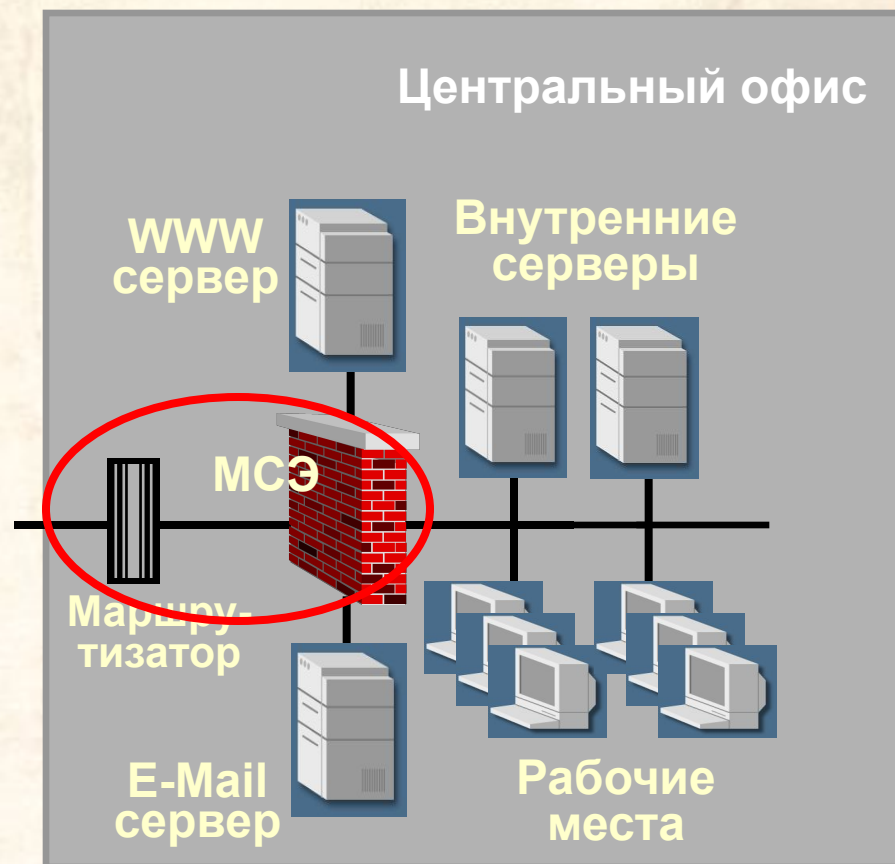
- Клиентские рабочие станции
- Серверы бизнес приложений
- Серверы БД
- Серверы файлов и печати
- **Серверы DMZ**



Корпоративная сеть

Windows NT

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

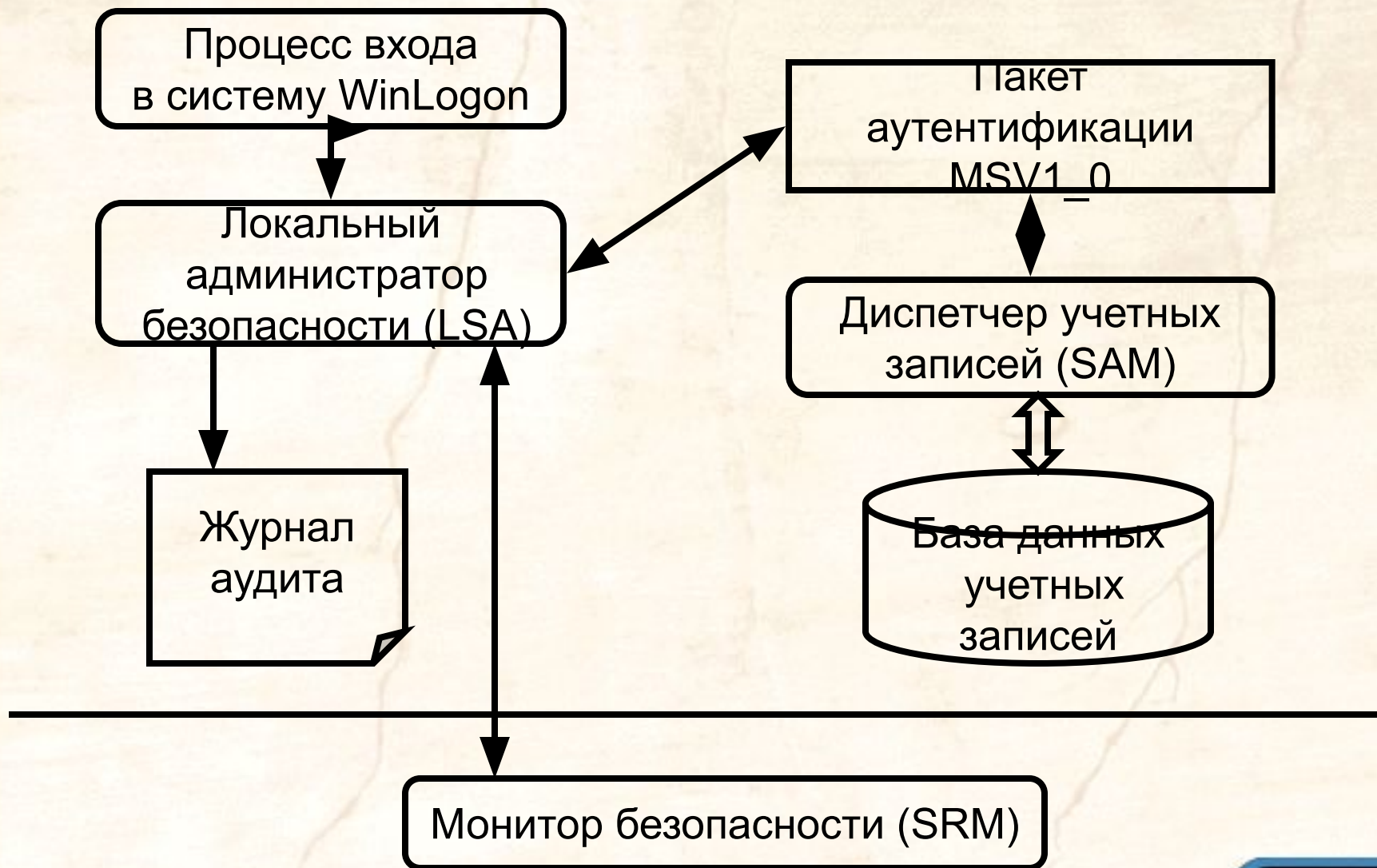


Защитные механизмы

- идентификация и аутентификация
- разграничение доступа (и авторизация)
- регистрация событий (аудит)
- контроль целостности
- затирание остаточной информации
- криптографические механизмы

...встроенные в большинство ОС

Система безопасности NT



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)

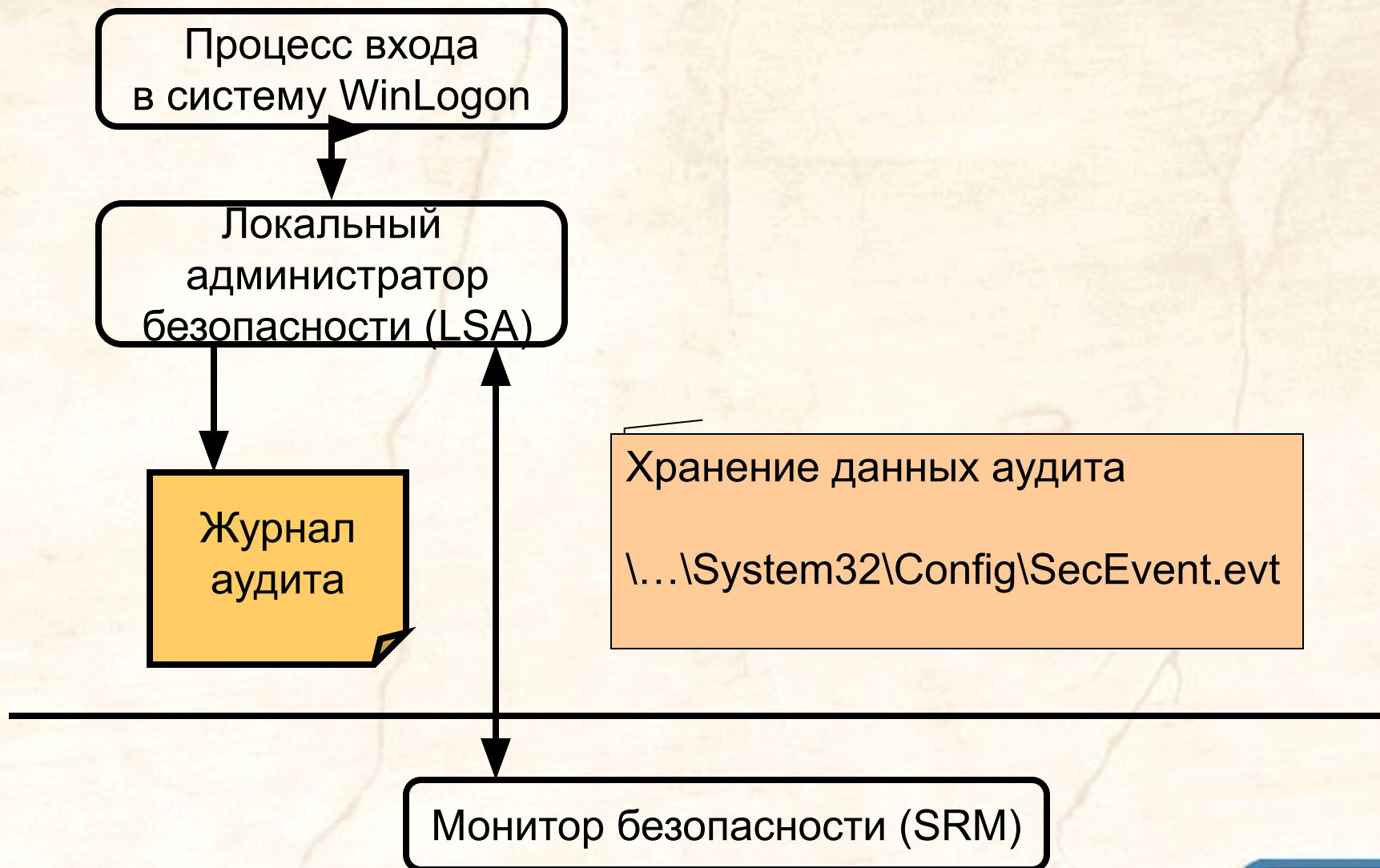
Журнал
аудита

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

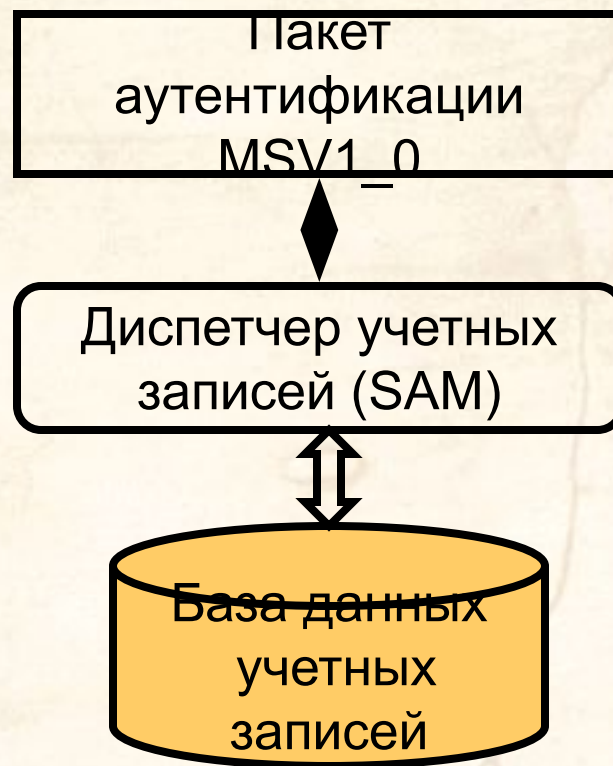
Монитор безопасности (SRM)

Система безопасности

Хранение информации о
бюджетах пользователей, групп,
компьютеров

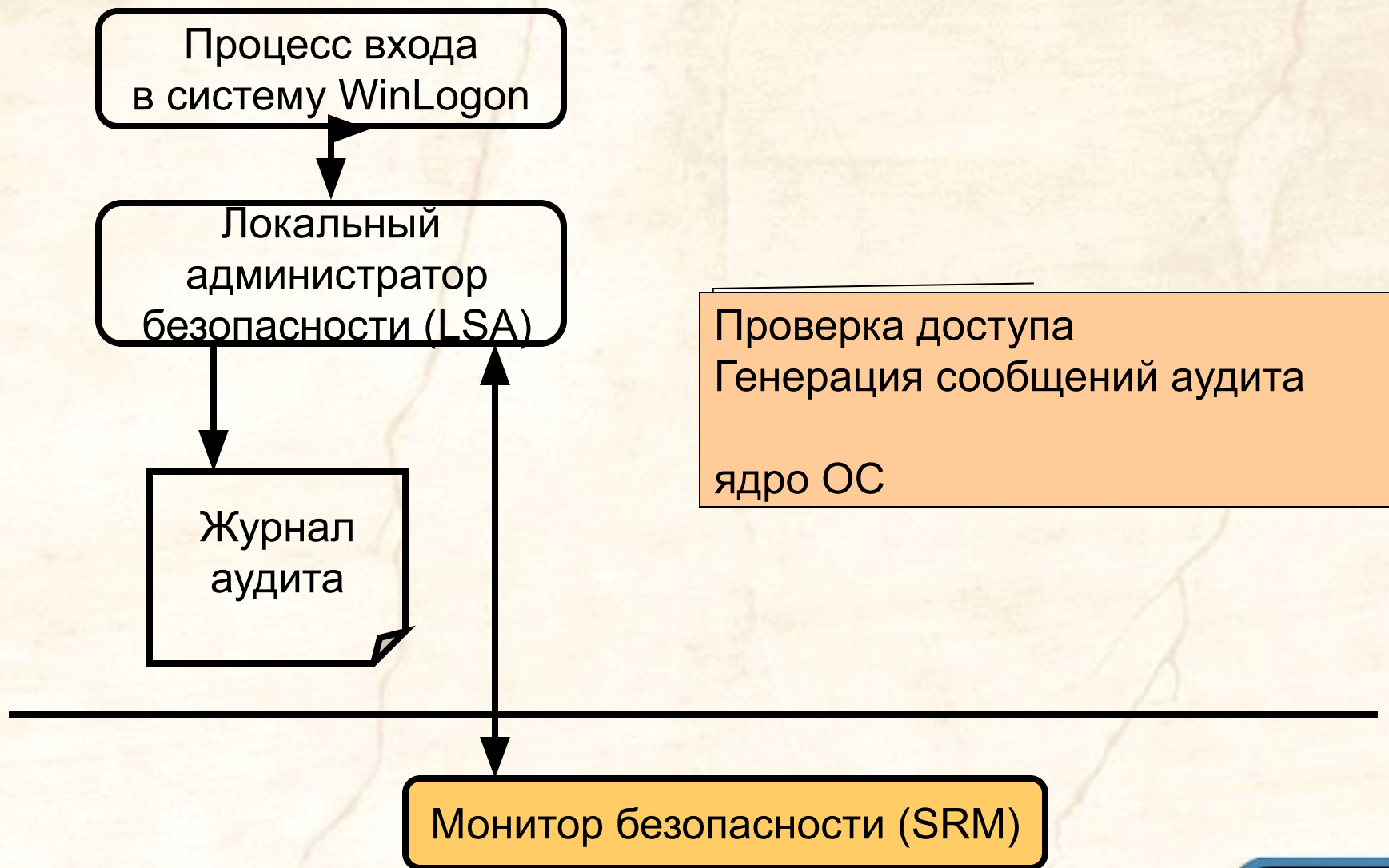
Хранится в нескольких местах

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

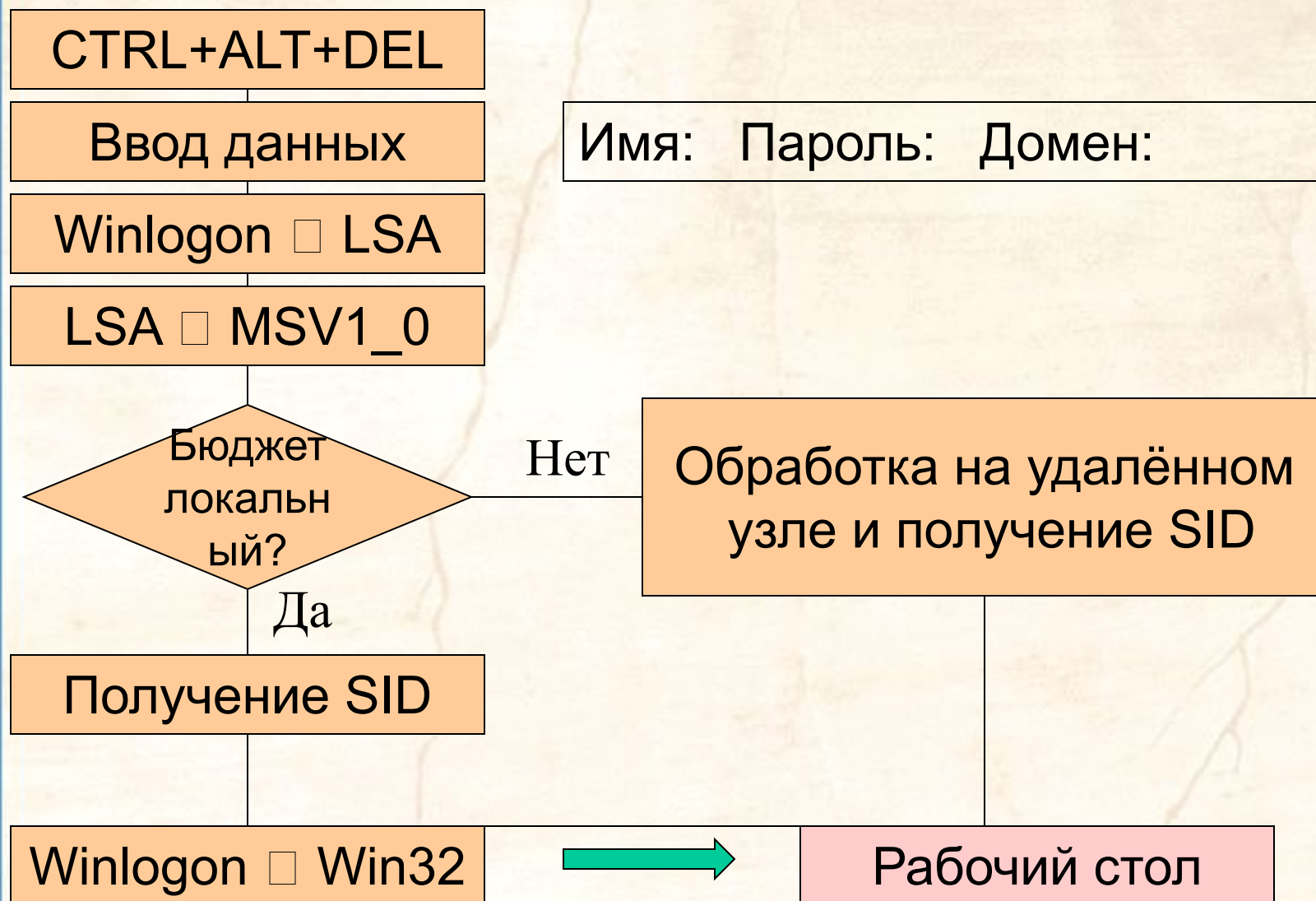


Монитор безопасности (SRM)

Система безопасности



Процесс регистрации

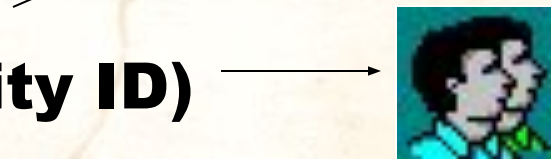


Бюджеты

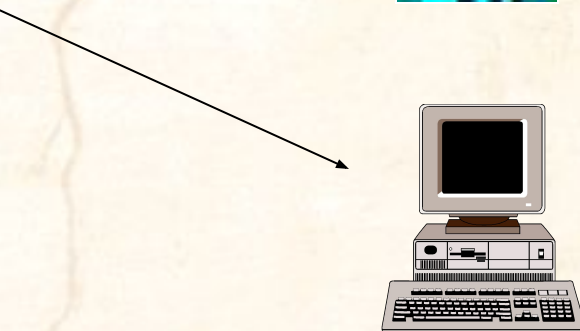
SID (Security ID)



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)

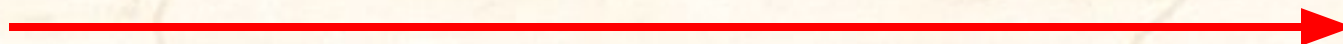
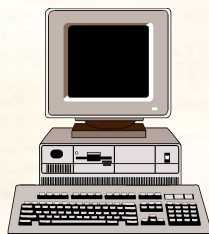
Everyone (SID)

Пользовательские права
SeSystemtimePrivelege



Маркер безопасного доступа

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



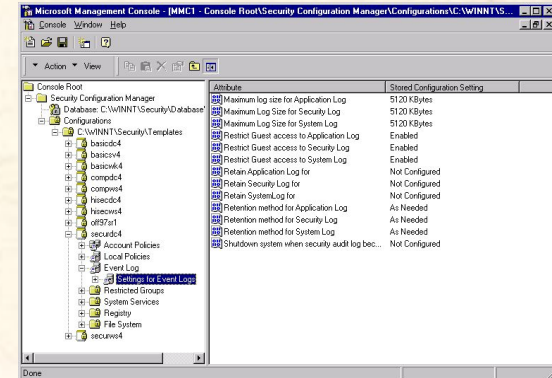
Субъект доступа



=

Пользователь
Master
...

+



Субъект доступа = Маркер безопасного доступа + Программа

- Простой субъект
- Субъект-сервер

Объект

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



Объект

Объект доступа

D:\Winnt\System32\regedt32.exe

Owner: Administrator

ACL:

Grant: (all) Administrator

Grant: (R): Users

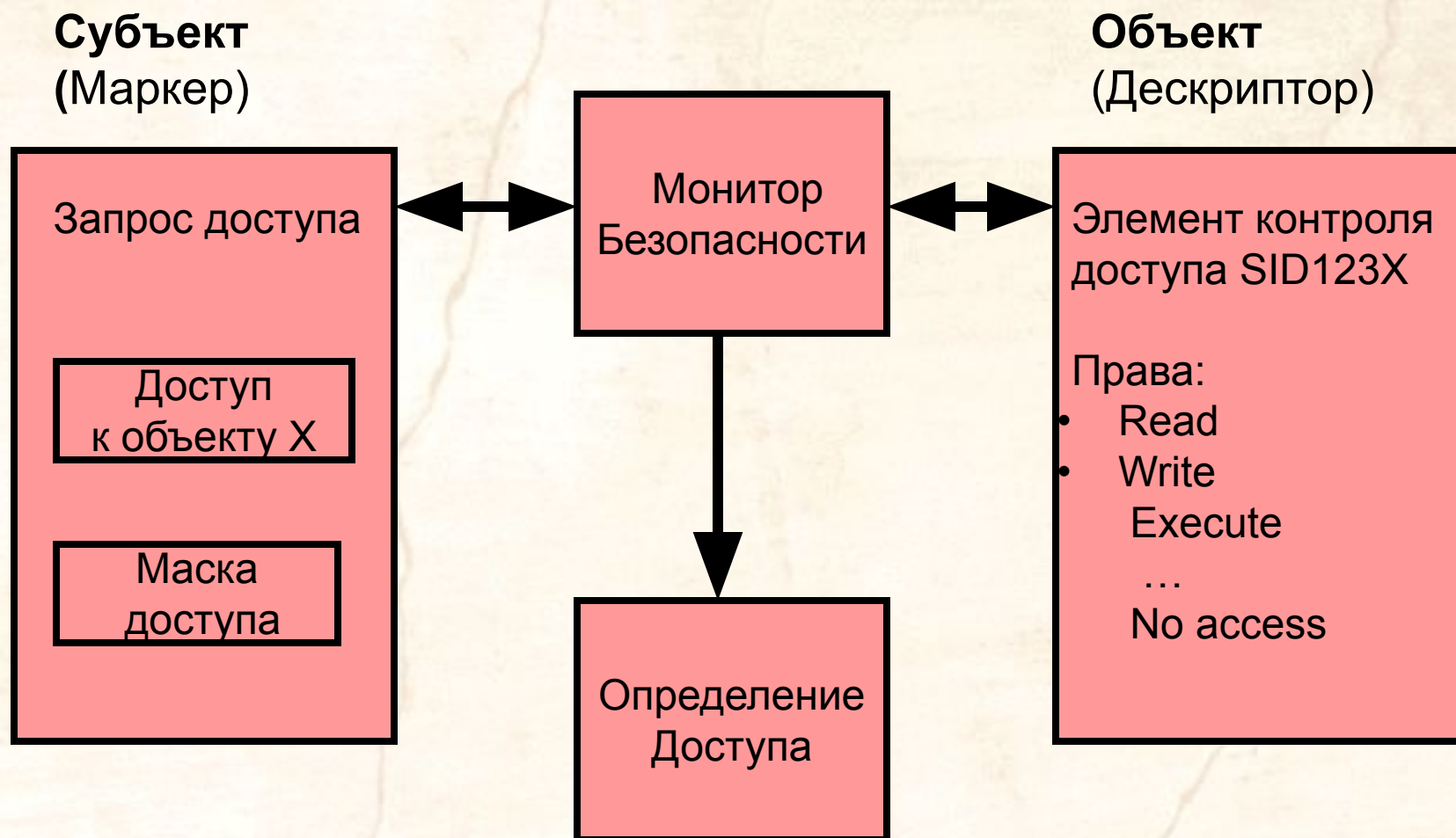
Revoke: Everyone

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**)

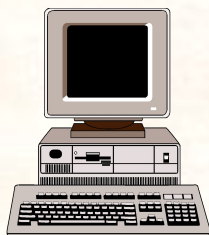
или

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

Требования к паролям

Сетевая аутентификация

Клиент



Установление связи



Сервер



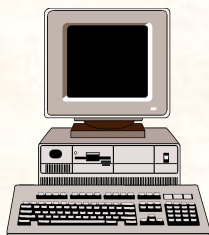
Запрос пароля



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

Сетевая аутентификация

Клиент



Сервер



Установление связи



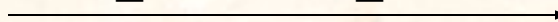
SMB_CON_NEGOTIATE



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

Политика безопасности и ОС



Политика безопасности и ОС

Общие рекомендации
по различным областям

Связующее звено между
политикой безопасности
и процедурой настройки
системы

Политика
безопасности

Общие стандарты

Пример:
British Standard BS7799

Руководства по настройке

Windows NT

UNIX

Другие ОС

Структура стандарта BS7799

- Политика в области безопасности
- Организация системы безопасности
- Классификация ресурсов и управление
- Безопасность и персонал
- Физическая и внешняя безопасность
- Менеджмент компьютеров и сетей
- Управление доступом к системе
- Разработка и обслуживание системы
- Обеспечение непрерывности работы

109
элем
ентов

Политика безопасности и ОС

Детальные рекомендации
по настройке различных ОС

Пошаговые руководства
типа «Step-by-step»

Пример: Руководство
Стива Саттона
по настройке Windows NT

Политика
безопасности

Общие стандарты

Руководства по настройке

Windows NT

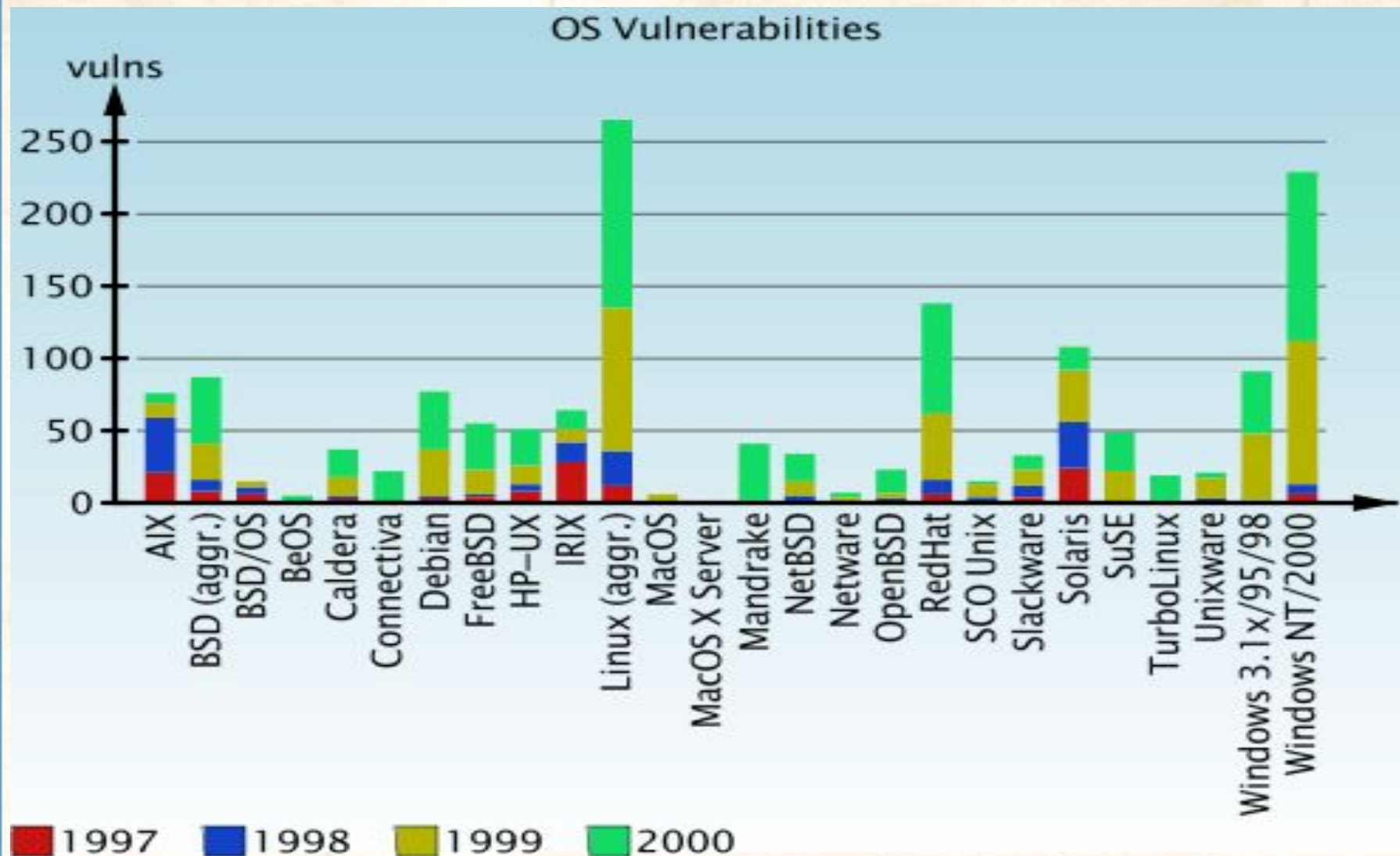
UNIX

Другие ОС

Причины возникновения уязвимостей ОС

- ✓ ошибки проектирования (компонент ядра, подсистем)
- ✓ ошибки реализации (кода)
- ✓ ошибки эксплуатации (неправильная настройка, неиспользуемые компоненты, слабые пароли)

Уязвимости ОС



Ошибки проектирования

Ошибки, допущенные при проектировании алгоритмов и принципов работы компонент ядра, подсистем:

- отсутствие ограничений на количество создаваемых объектов
- шифрование (хэширование) и хранение паролей
- ...



Ошибки реализации

```
int i, offset=OFFSET;
if (argv[1] != NULL)
    offset = atoi(argv[1]);
buff = malloc(BSIZE);
egg = malloc(EGGSIZE);
addr = get_sp() - offset;
printf("Using address: 0x%x\n", addr);
ptr = buff;
addr_ptr = (long *) ptr;
for (i = 0; i < BSIZE; i+=4)
    *(addr_ptr++) = addr;
/* Now it fills in the egg */
ptr = egg;
for (i = 0; i < EGGSIZE -
...
```

Ошибки кода ОС

Ошибки реализации

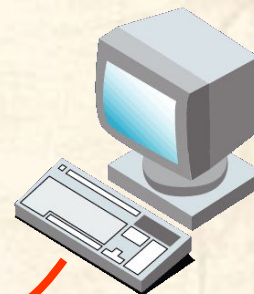
Переполнение буфера – наиболее распространённая техника использования ошибок реализации

Переполнение буфера – манипуляции с данными без проверок соответствия их размера выделенному для них буферу

Если буфер расположен в стеке, возможна перезапись адреса возврата из функции

Исправление ошибок реализации

Производитель ПО



Клиент

Проблема аутентификации обновлений

Исправление ошибок реализации

- Цифровая подпись не используется вообще
- Нет прямого пути, чтобы проверить, что используемый ключ действительно принадлежит производителю ПО
- Цифровая подпись, используемая в оповещении о выходе обновлений, не аутентифицирует само обновление

Проблема аутентификации обновлений

Аутентификация обновлений

- Использование отозванных сертификатов Sun Microsystems (CERT® Advisory CA-2000-19)
- Троянский конь в одной из версий «TCP Wrappers» (CERT® Advisory CA-1999-01)
- Троянский конь в пакете «util-linux-2.9g» (securityfocus)

Примеры инцидентов

Исправление ошибок реализации

- PGP (GnuPG)
- HTTPS
- SSH

Способы получения обновлений

Ошибки обслуживания



**Ошибки использования встроенных в ОС
механизмов защиты**

Настройка системы безопасности

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

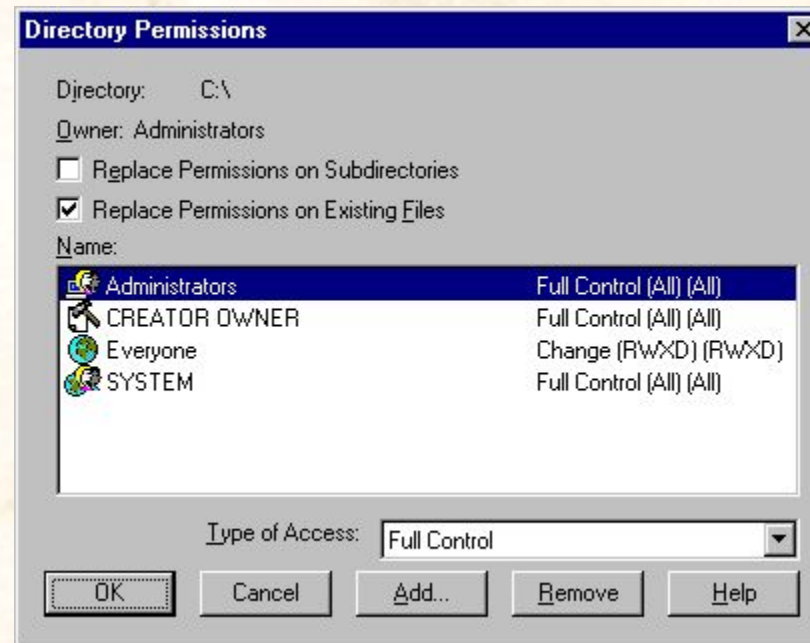
Режим ядра

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

- Windows NT Security Guidelines

NT Security Guidelines

Структура документа

- Level 1
- Level 2

Level 1 – незначительная модификация установок по умолчанию

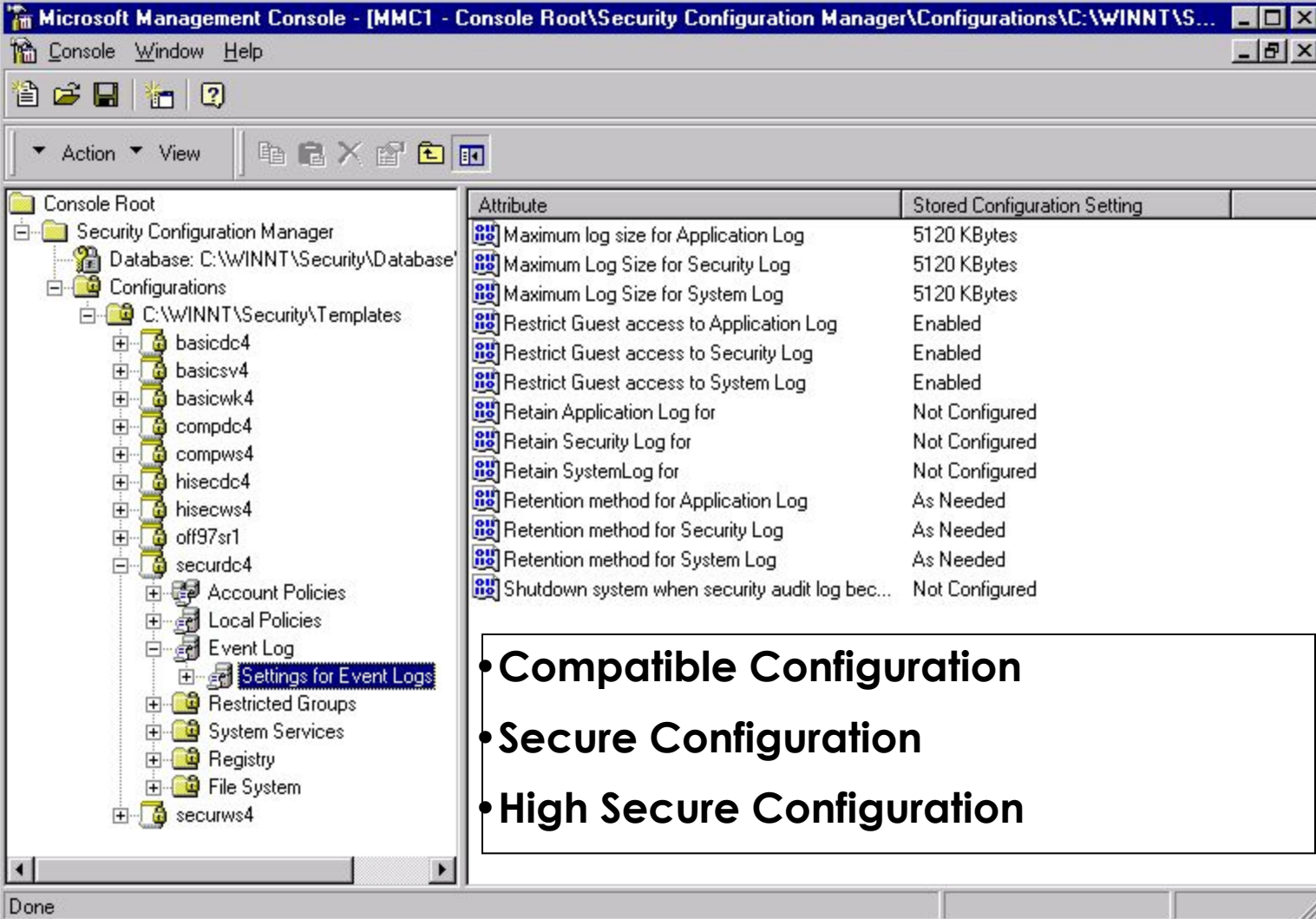
Level 2 – для узлов с повышенными требованиями к безопасности

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 Manager



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

Console Window Help

Action View

Console Root

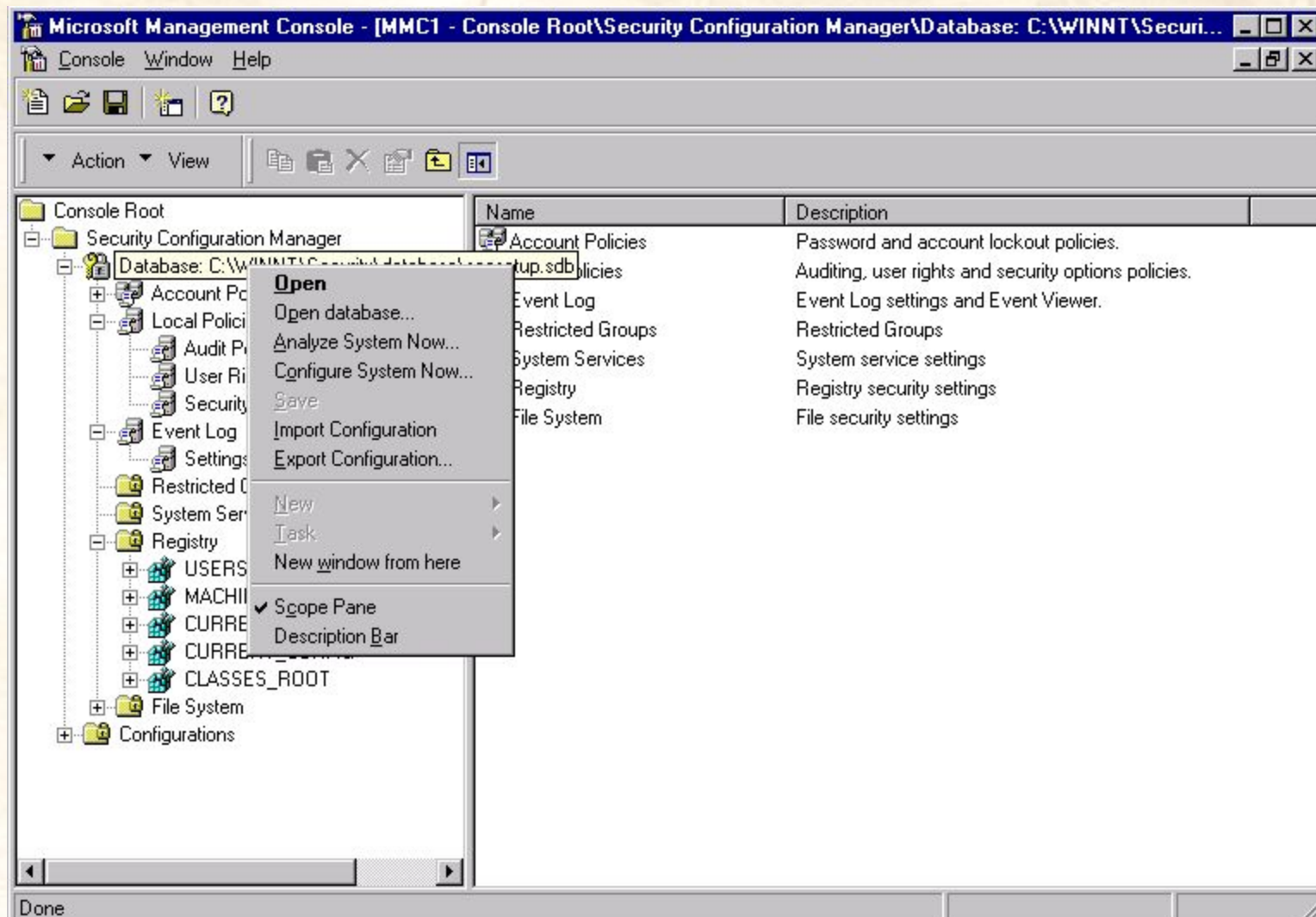
- Security Configuration Manager
 - Database: C:\WINNT\Security\Database
 - Configurations
 - C:\WINNT\Security\Templates
 - basicdc4
 - basicsv4
 - basicwk4
 - compdc4
 - compws4
 - hisecc4
 - hisecls4
 - off97sr1
 - securdc4
 - Account Policies
 - Local Policies
 - Event Log
 - Settings for Event Logs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

