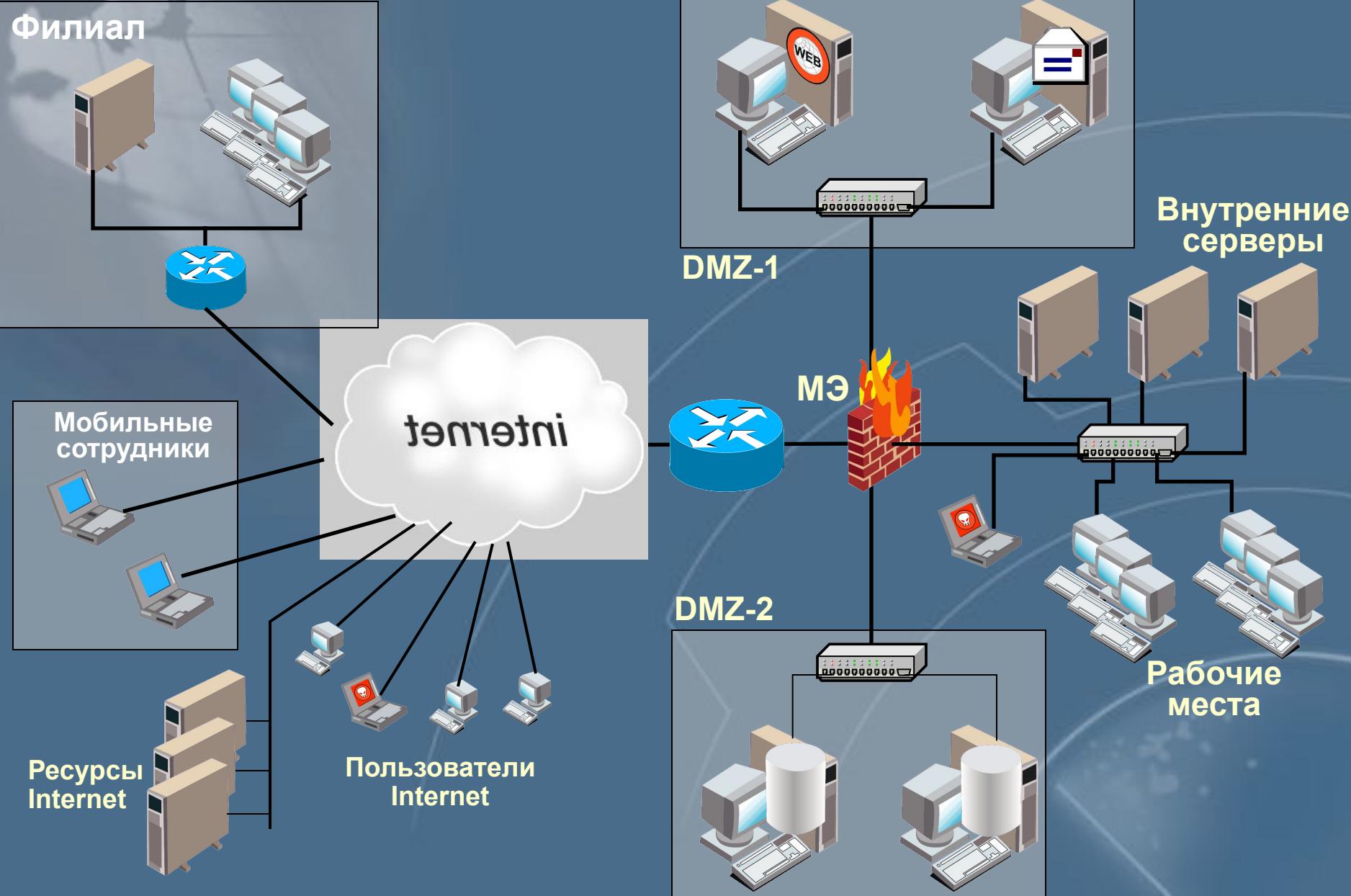


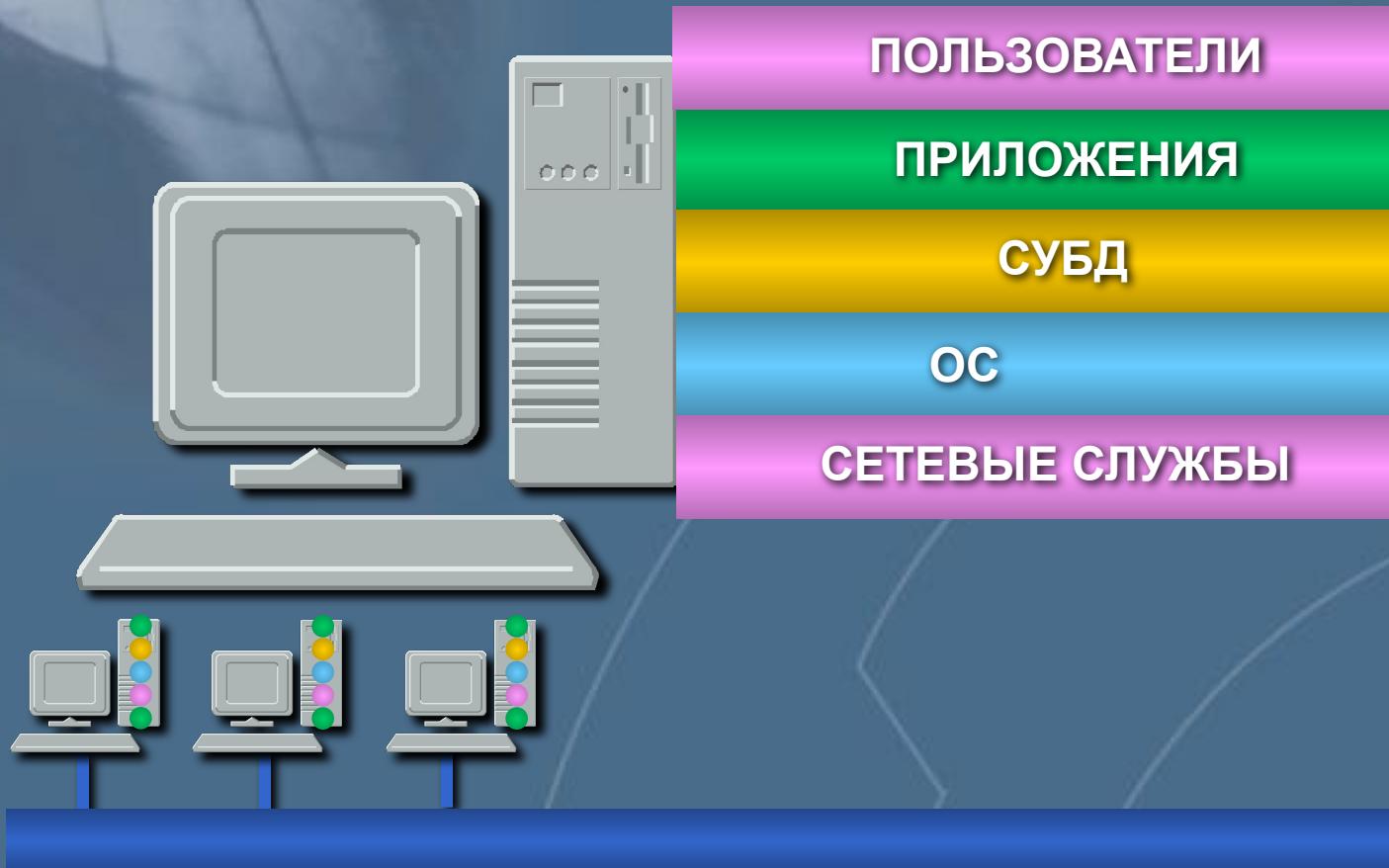
# Проблемы обеспечения безопасности сетевых операционных систем

Лепихин В. Б.  
УЦ «Информзащита»

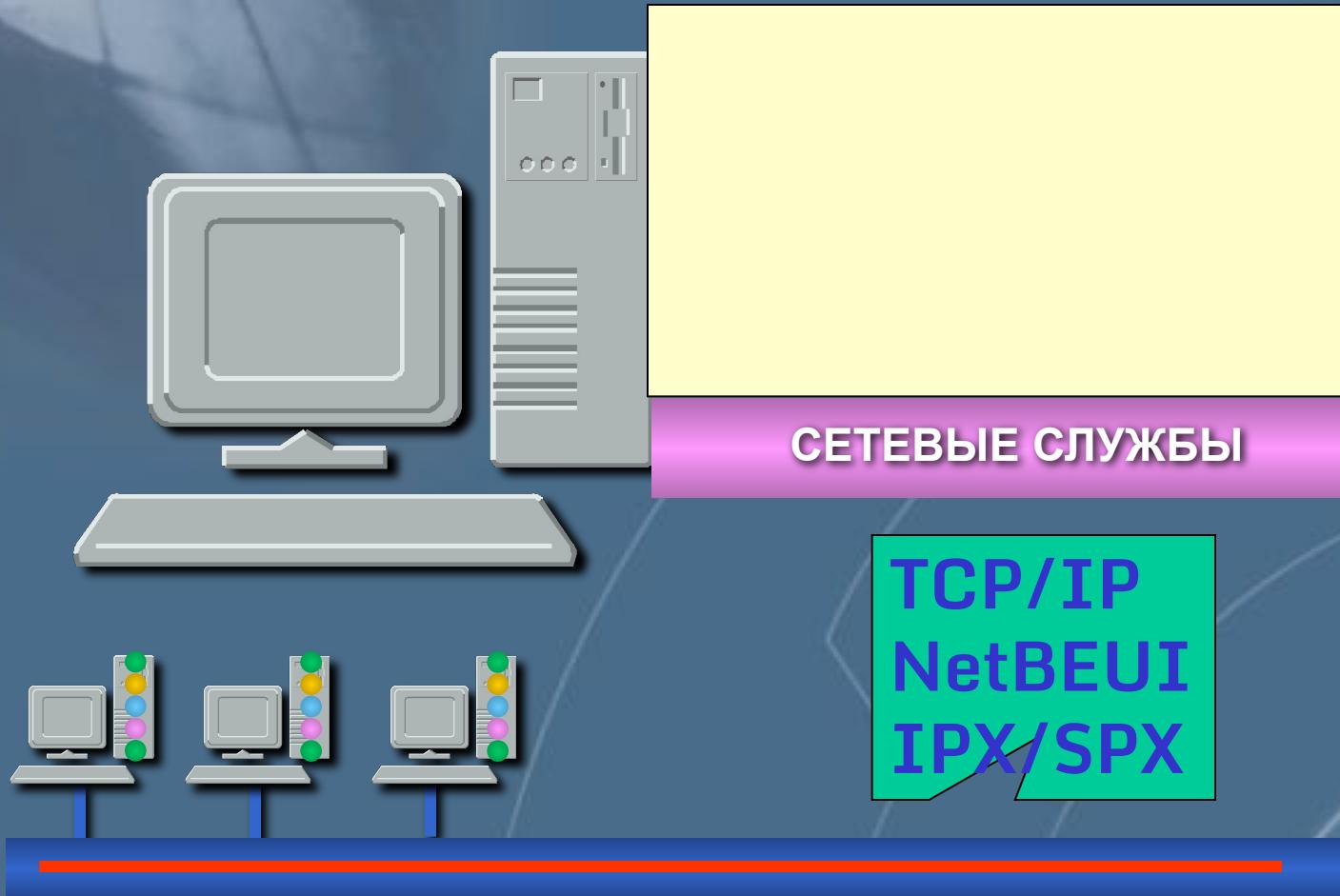
# Корпоративная сеть



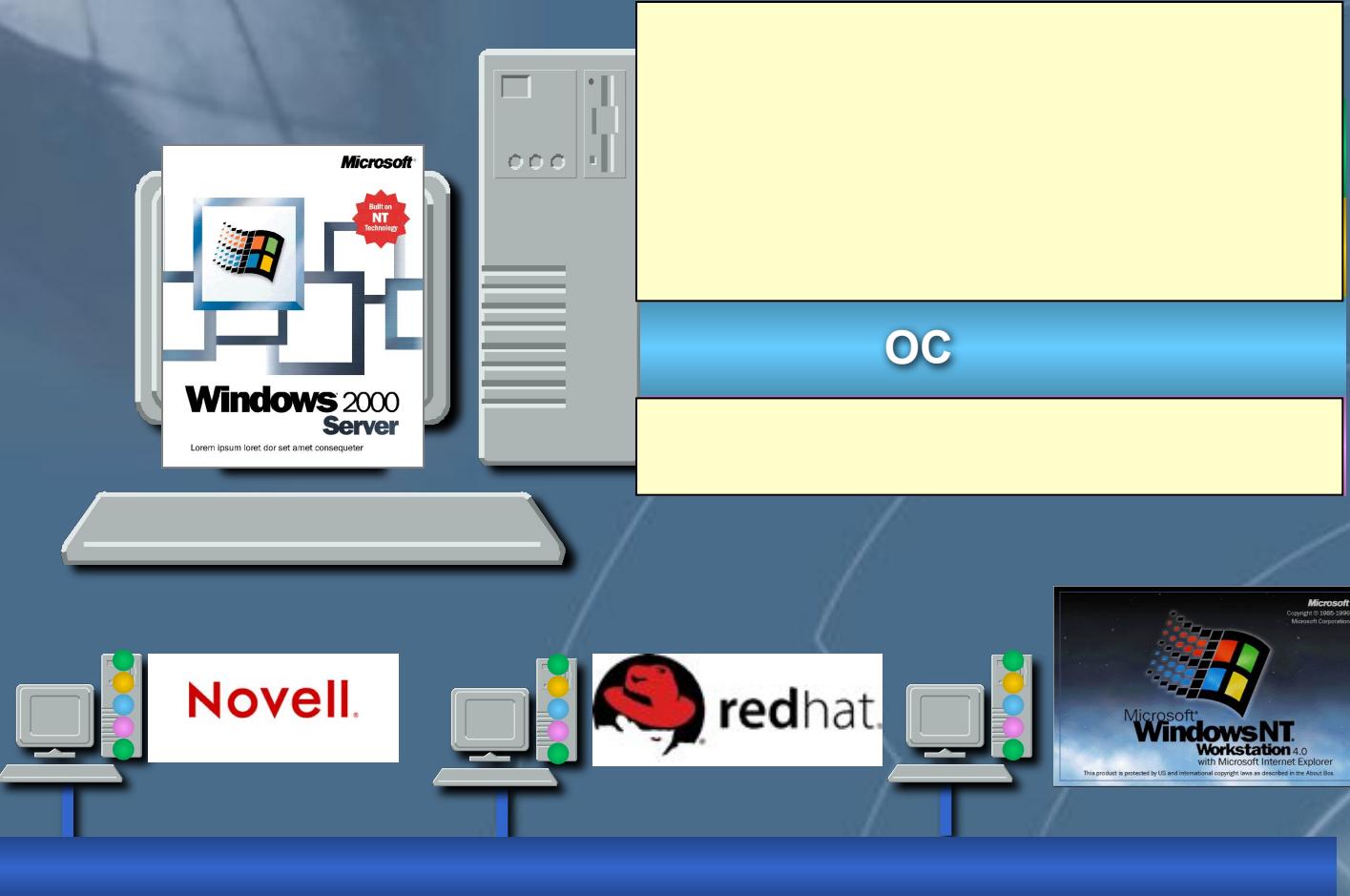
# Уровни информационной инфраструктуры



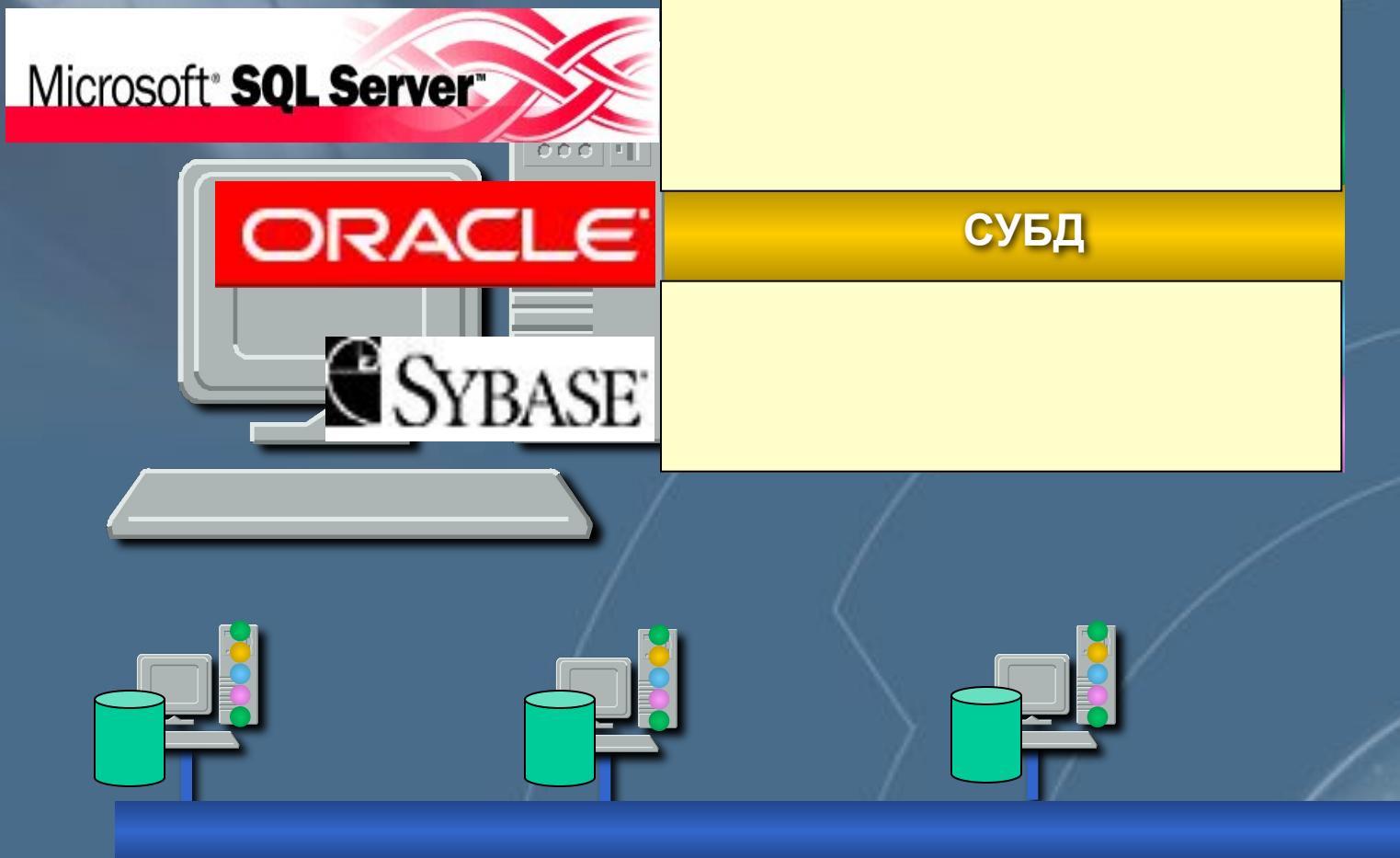
# Уровни информационной инфраструктуры



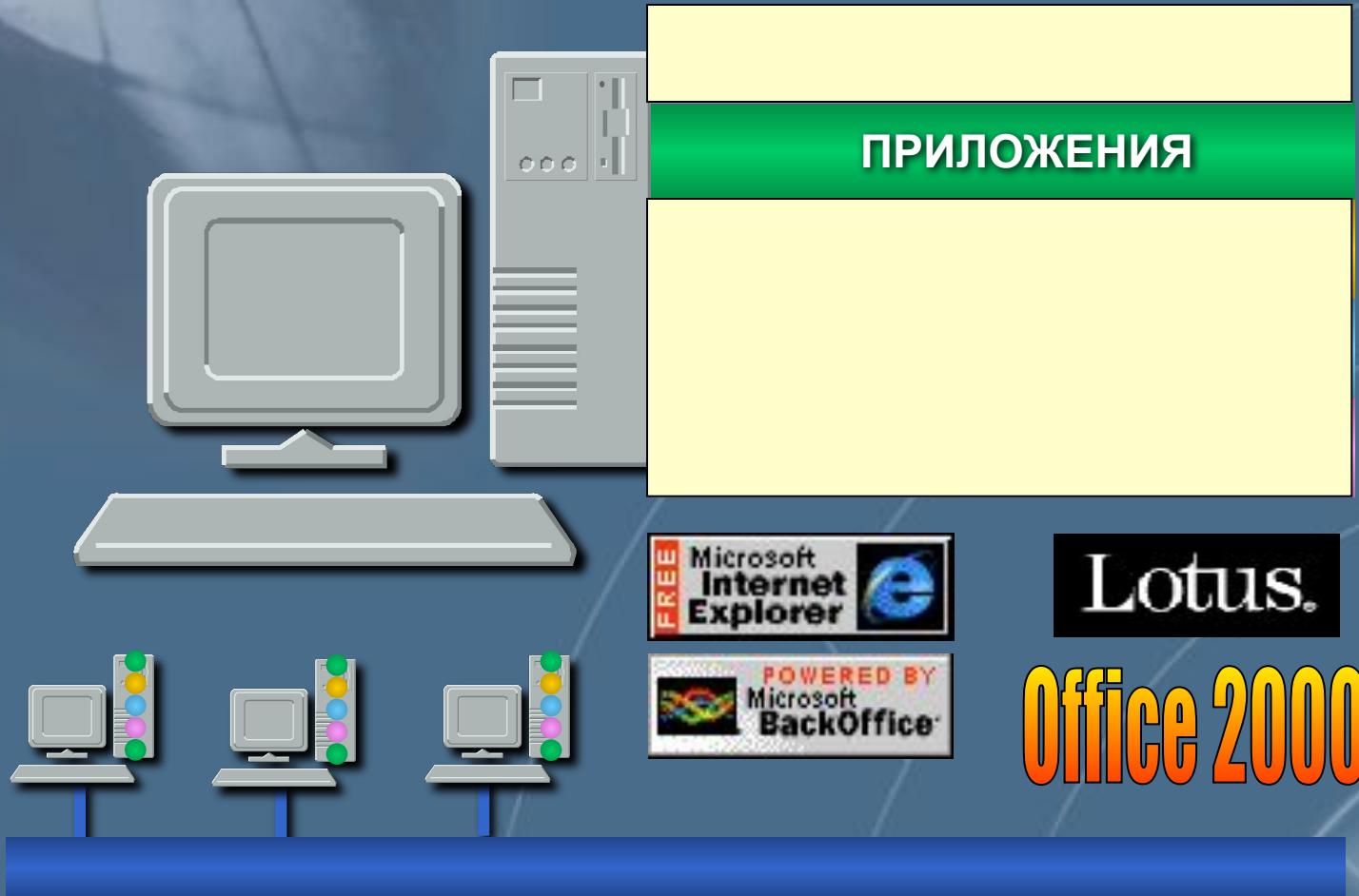
# Уровни информационной инфраструктуры



# Уровни информационной инфраструктуры

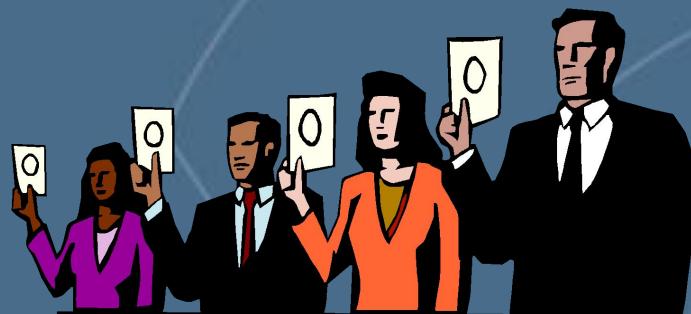


# Уровни информационной инфраструктуры

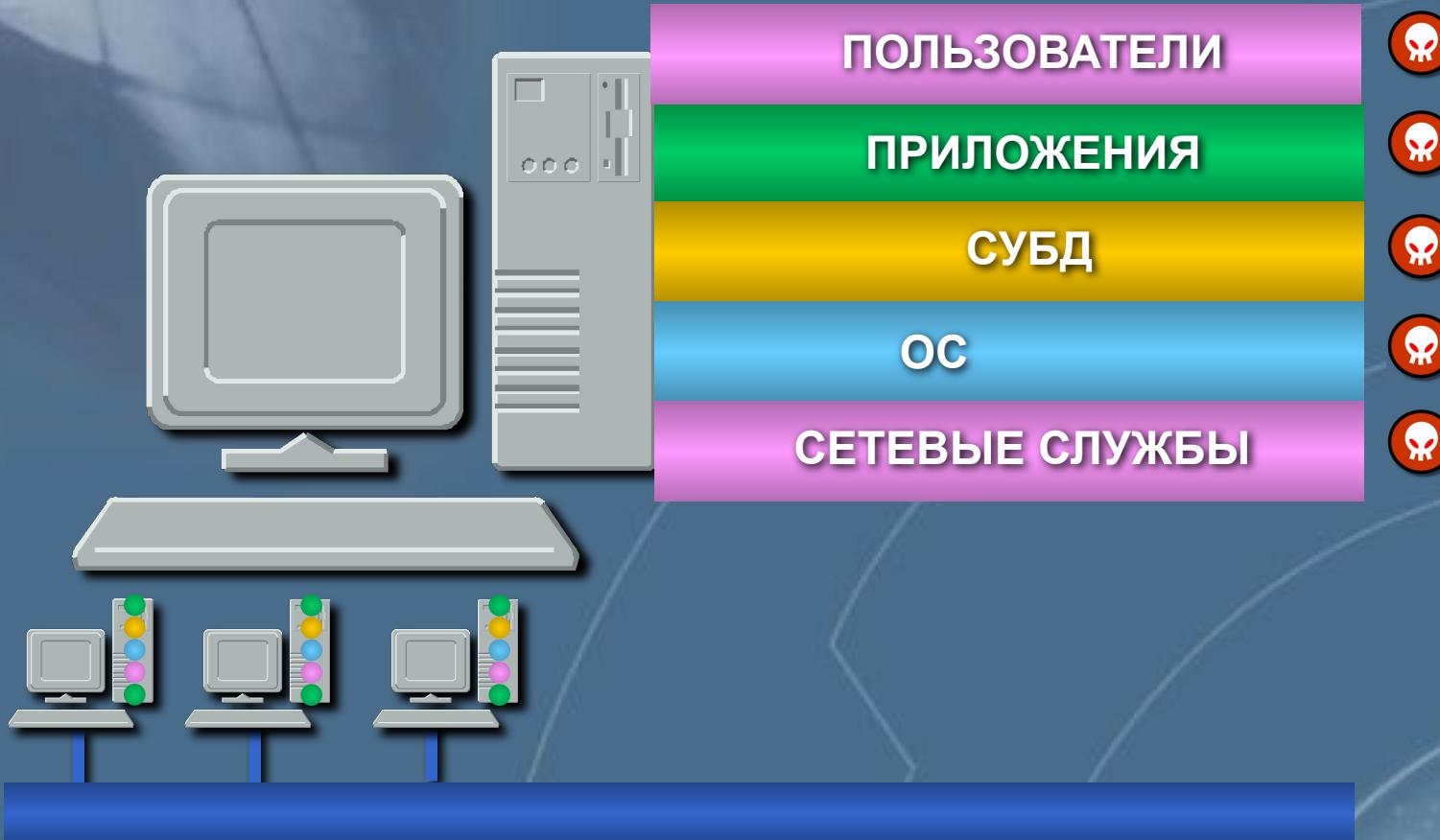


# Уровни информационной инфраструктуры

ПОЛЬЗОВАТЕЛИ



# Уровни информационной инфраструктуры



# Уязвимости по уровню в информационной инфраструктуре



*Уровень персонала*



*Уровень приложений*



*Уровень баз данных*



*Уровень операционной системы*

---



*Уровень сети*



# Причины возникновения уязвимостей ОС

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

# Источники информации о новых уязвимостях

- [www.cert.org](http://www.cert.org)* - координационный центр  
*CERT/CC*
- [www.iss.net/xforce](http://www.iss.net/xforce)* - база данных компании ISS
- А также:
- [www.sans.org](http://www.sans.org)*
- [www.securityfocus.com](http://www.securityfocus.com)*
- [www.ciac.org/ciac/](http://www.ciac.org/ciac/)*

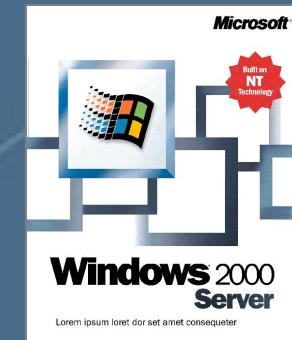
# Дополнительные источники информации о безопасности NT/2000

*[www.microsoft.com/security](http://www.microsoft.com/security)*

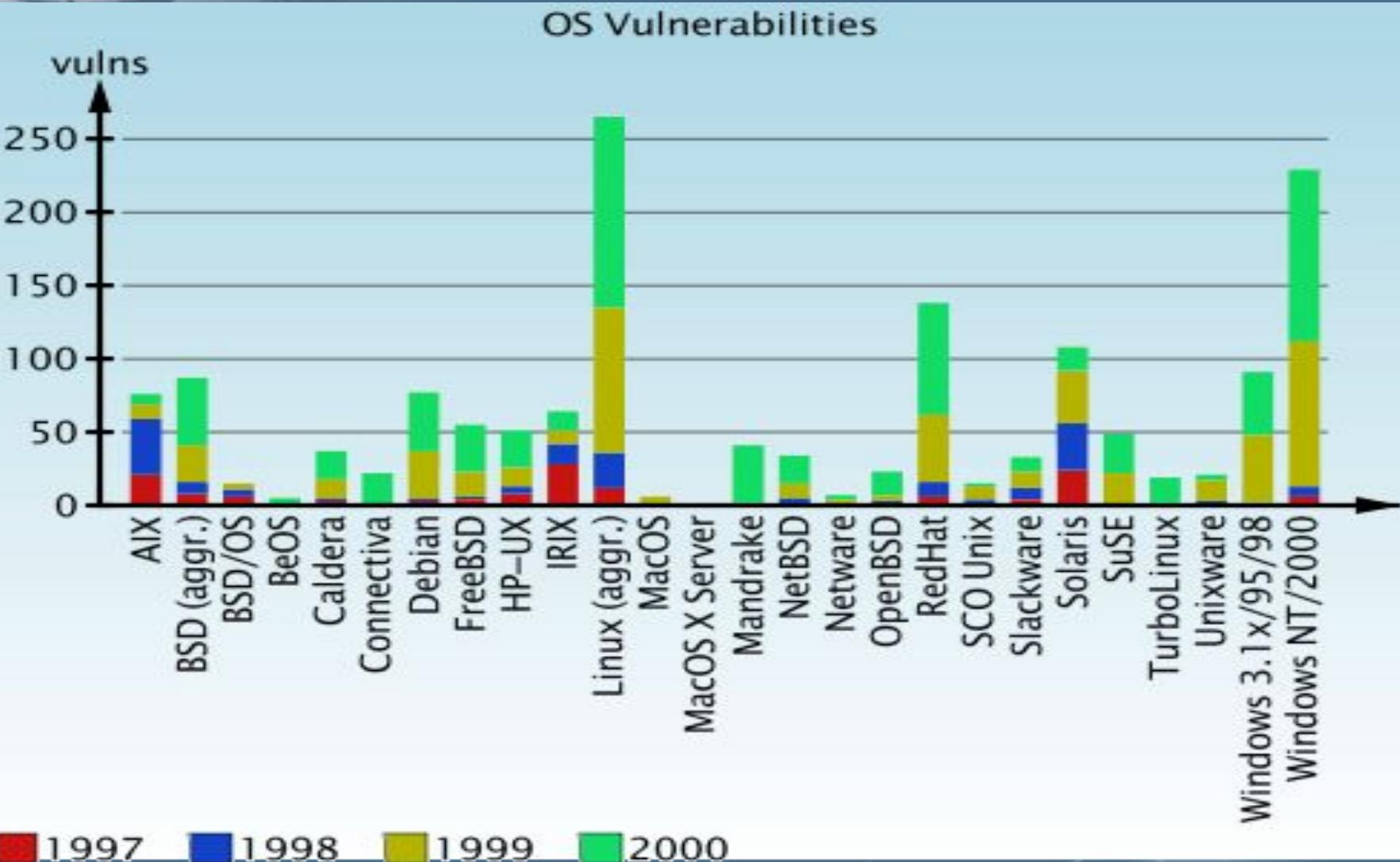


*[www.winternals.com](http://www.winternals.com)*

*[www.ntsecurity.com](http://www.ntsecurity.com)*



# BUGTRAQ Vulnerability Database Statistics



# Примеры уязвимостей

Название: nt-getadmin-present

Описание: проблема одной из функций ядра ОС Windows NT, позволяющая злоумышленнику повысить привилегии обычного пользователя до привилегий администратора

Источник возникновения: ошибки реализации

# Примеры уязвимостей

## Название: explorer-relative-path-name

**Описание:** в реестре Windows NT/2000 указан относительный путь к файлу *explorer.exe* (*Windows shell*) вместо абсолютного пути.

## Источник возникновения: ошибки реализации



# Common Vulnerabilities and Exposures

The Key to Information Sharing

**Единая система наименований для уязвимостей**

**Стандартное описание для каждой уязвимости**

**Обеспечение совместимости баз данных уязвимостей**

[http://cve.mitre.org/c  
ve](http://cve.mitre.org/cve)



# Common Vulnerabilities and Exposures

The Key to Information Sharing

CAN-1999-00  
67

Кандидат CVE

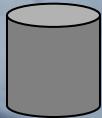


CVE-1999-00  
67

Индекс CVE

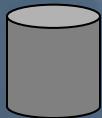
<http://cve.mitre.org/cve>

# Ситуация без CVE



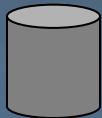
Bugtraq  
Database

'NTLMSSP'  
Privilege Escalation Vulnerability

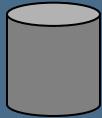


ISS  
RealSecure

ntlm-ssp-elevate-privileges(6076)



Bindview  
20010207 Local promotion vulnerability  
in NT4's NTLM Security Support Provider

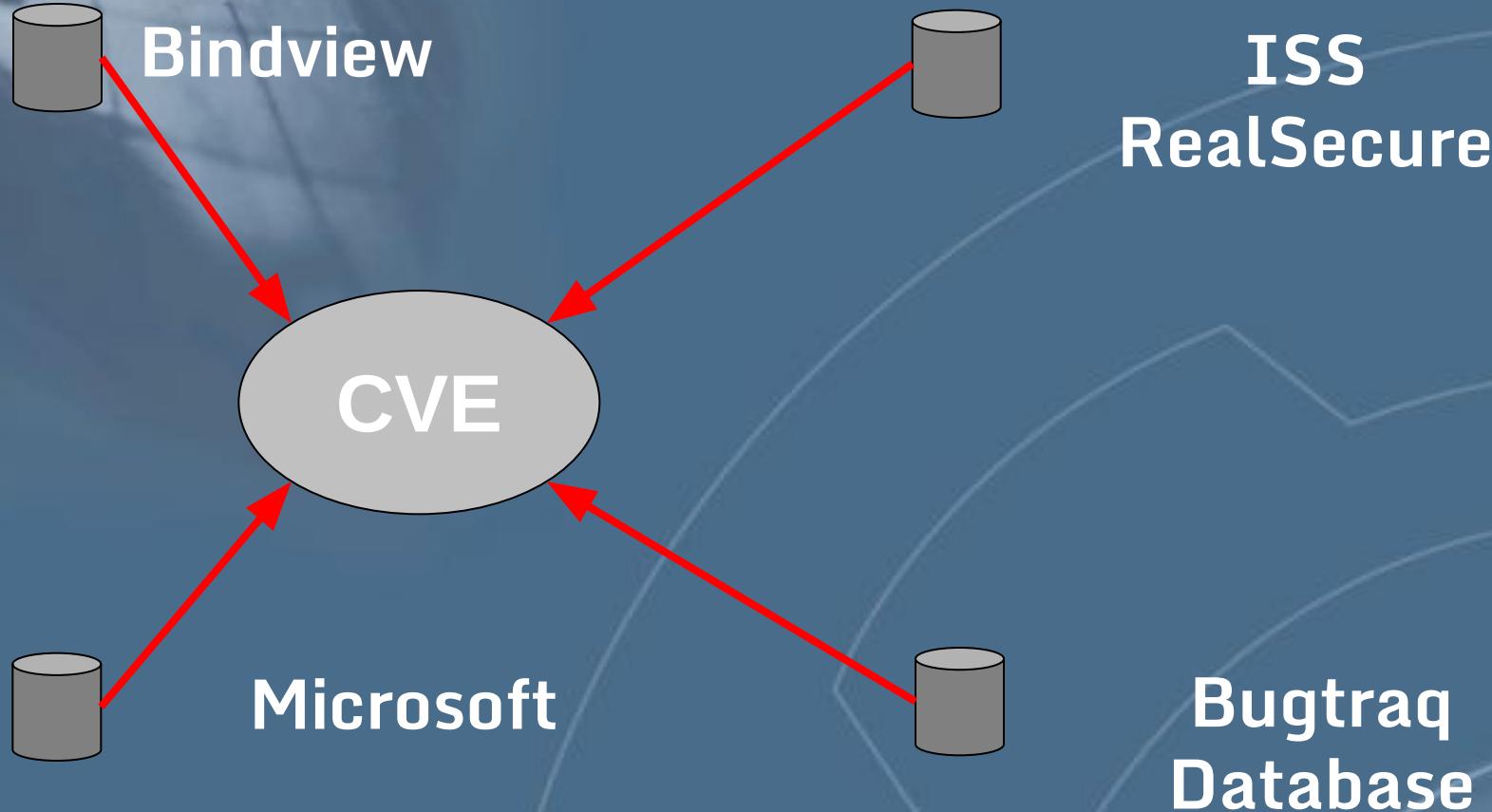


Microsoft

MS:MS01-008

**Уязвимость в NTLM Security Support Provider**

# Поддержка CVE



**CVE-2001-0016 vulnerability in NTLM  
Security Support Provider**

# CVE entry

Номер

Описание

**CVE-2001-0016**

**NTLM Security Support Provider (NTLMSSP) service does not properly check the function number in an LPC request, which could allow local users to gain administrator level access.**

**Reference: BINDVIEW:20010207 Local promotion vulnerability in NT4's NTLM Security Support Provider**

**Reference: MS:MS01-008**

**Reference: BID:2348**

**Reference:**

**XF:ntlm-ssp-elevate-privileges(6076)**

Ссылки

# Ошибки проектирования

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

- отсутствие ограничений на количество создаваемых объектов
- особенности шифрования (хэширования) 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

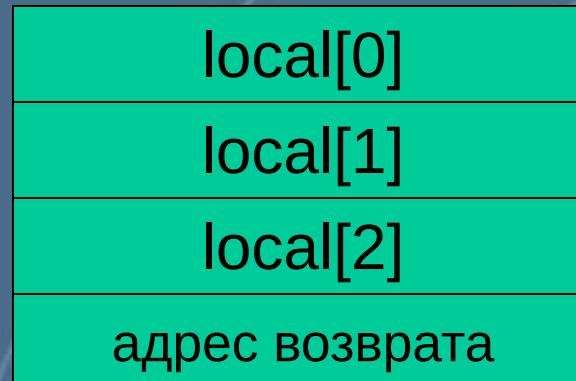
Переполнение буфера – манипуляции с данными без проверок соответствия их размера выделенному для них буферу

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

# Переполнение стека

```
f_vulner()
{
    char local[3]
    ...
    ...
}
```

Буфер



Стек

# «Переполнение стека»

```
int f_vuln (char arg)
{
    char local[100]
    //обработка
    return 0
}
void main()
{
    char arg[200]
    gets (arg)
    .
    .
    f_vuln (arg)
    printf(arg)
    return 0
}
```

*strcpy(local, arg)*

*Обычный ход выполнения программы*

Переменная  
arg [100]

адрес возврата

Стек

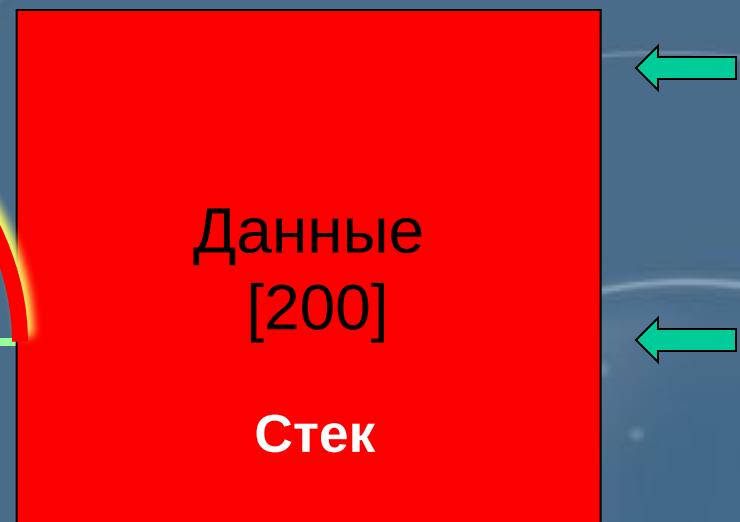
# «Переполнение стека»

```
int f_vuln (char arg)
{
    char local[100]
    //обработка
    return 0
}
void main()
{
    char arg[200]
    gets (arg)
    .
    .
    f_vuln (arg)
    printf(arg)
    return 0
}
```

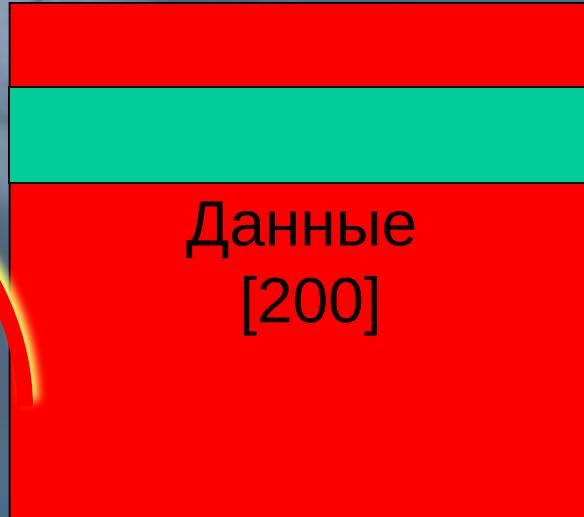
*strcpy(local, arg)*  
Ошибка !

*Переполнение стека*

*Вместо возврата  
запуск кода*



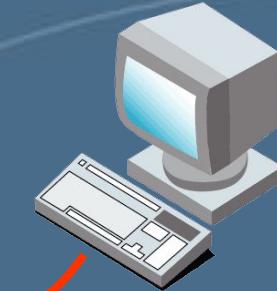
# «Переполнение стека»



Использование функции  
«WinExec»

# Исправление ошибок реализации

Производитель ПО



Клиент

*INTERNET*

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 отзываемых 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

# Защитные механизмы

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

...встроенные в большинство сетевых ОС

# Субъекты и объекты



# Субъекты и объекты

**Объект доступа - пассивная сущность операционной системы (файл, каталог, блок памяти)**

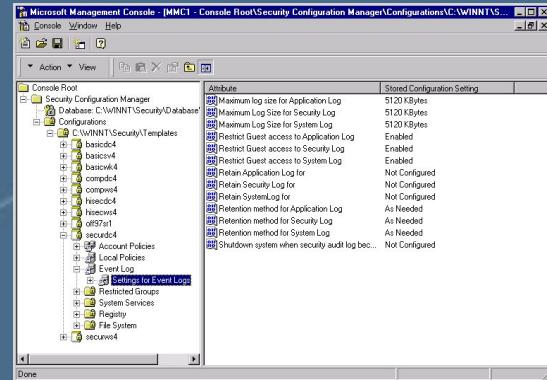
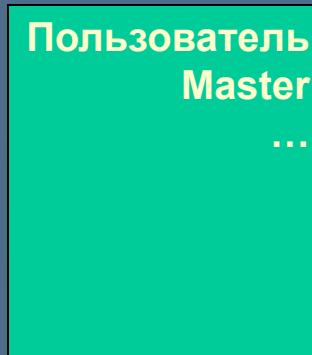


**Субъект доступа - активная сущность операционной системы (процесс, программа)**

# Пример субъекта доступа



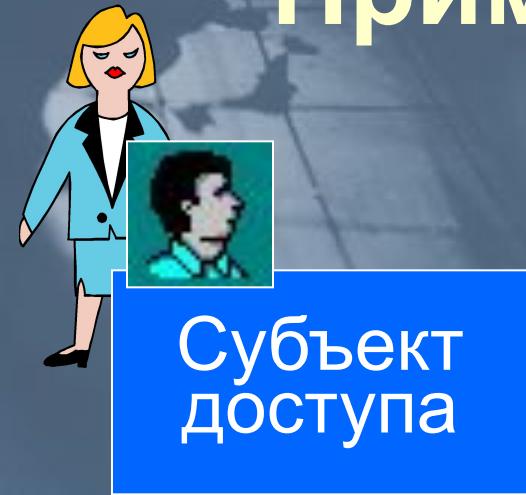
=



Субъект доступа = Маркер безопасного доступа + Процесс (поток)

Субъект доступа в ОС Windows NT

# Пример субъекта доступа

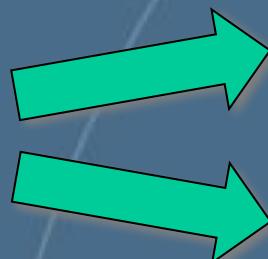


В роли субъектов доступа в Linux выступают процессы

Процессы :

- Получают доступ к файлам
- Управляют другими процессами

Процесс



Файл

процесс

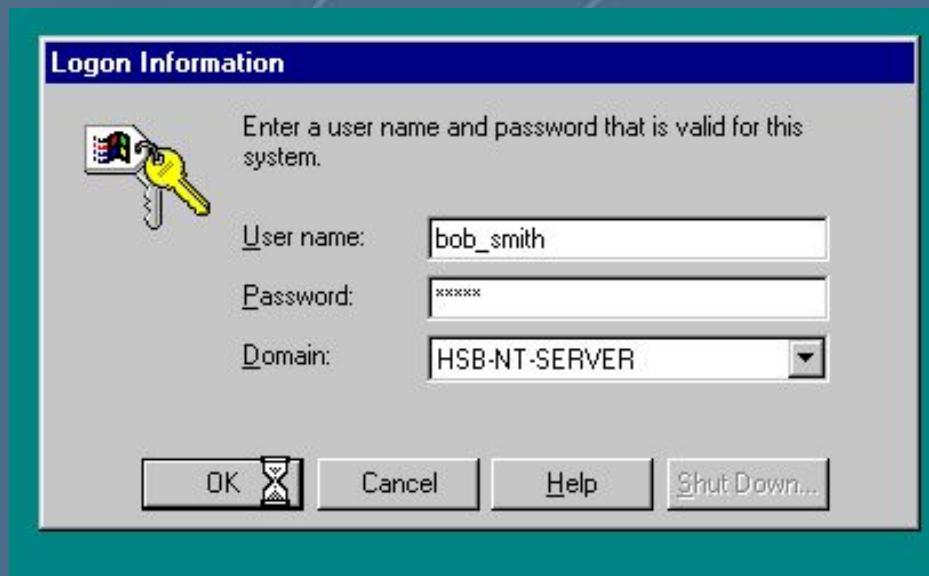
Субъект доступа в Linux

# Идентификация и аутентификация

**Идентификация (субъекта или объекта):**

- 1) **именование** (присвоение имен-идентификаторов);
- 2) **опознавание** (выделение конкретного из множества).

**Аутентификация (субъекта или объекта) - подтверждение подлинности** (доказательство того, что он именно тот, кем представился).



# Сетевая аутентификация

Клиент



Сервер



Установление связи



Запрос пароля



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

# Сетевая аутентификация

Клиент



Сервер



Установление связи



Запрос пароля



Зашифрованный запрос



Механизм «запрос/отклик»

# Уязвимости аутентификации (по паролю)

**Возможность перехвата и повторного использования  
пароля (получение доступа к файлам с паролями)**

**«Троянские кони» в процедуре входа в систему**

**Социальная инженерия**

**Повторяющийся запрос при сетевой аутентификации**

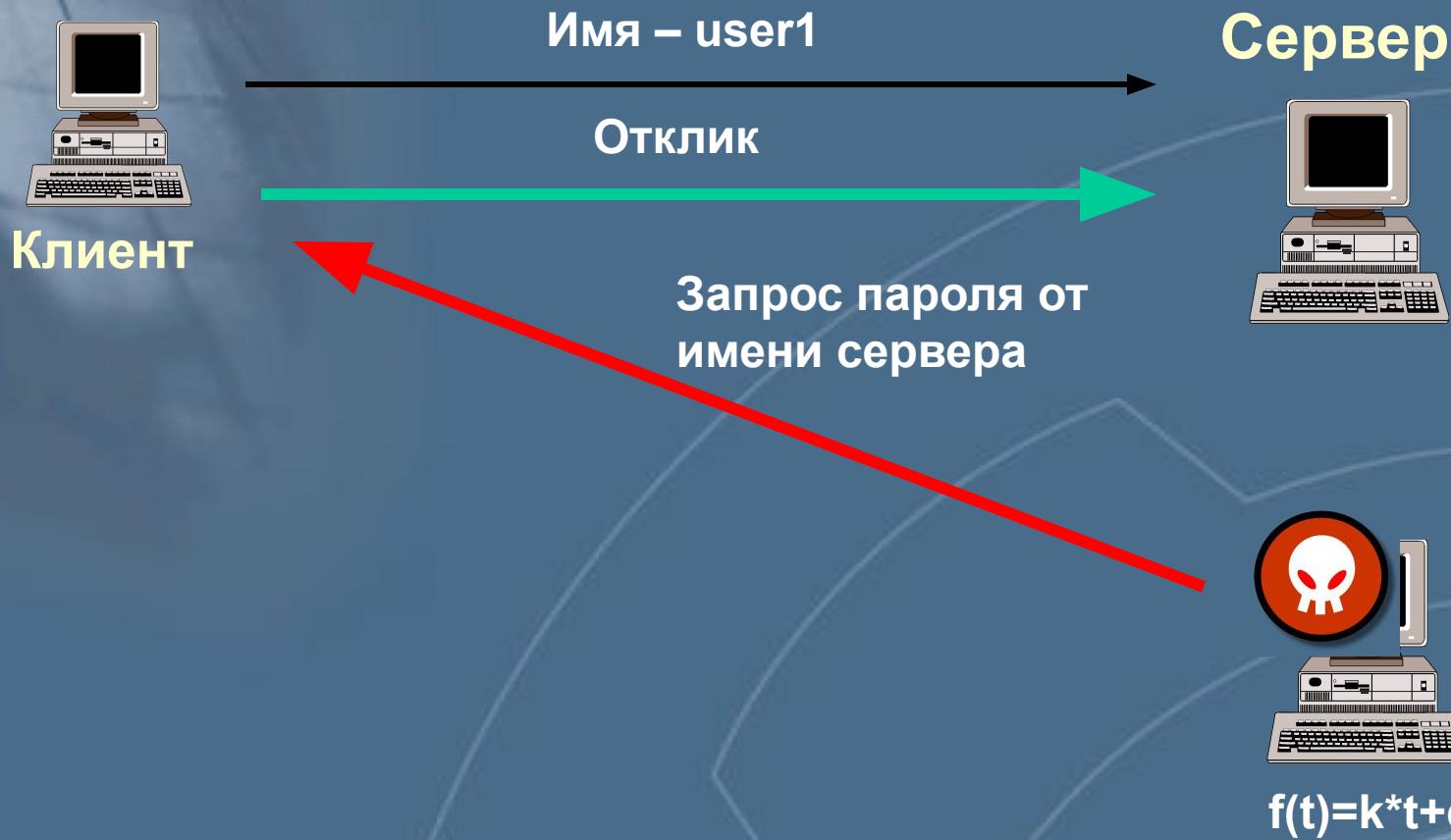
# Сетевая аутентификация



$$f(t)=k*t+c$$

Предсказуемый запрос

# Сетевая аутентификация



Предсказуемый запрос

# Сетевая аутентификация

$$f(t)=k*t+c$$



Сервер



Запрос на аутентификацию

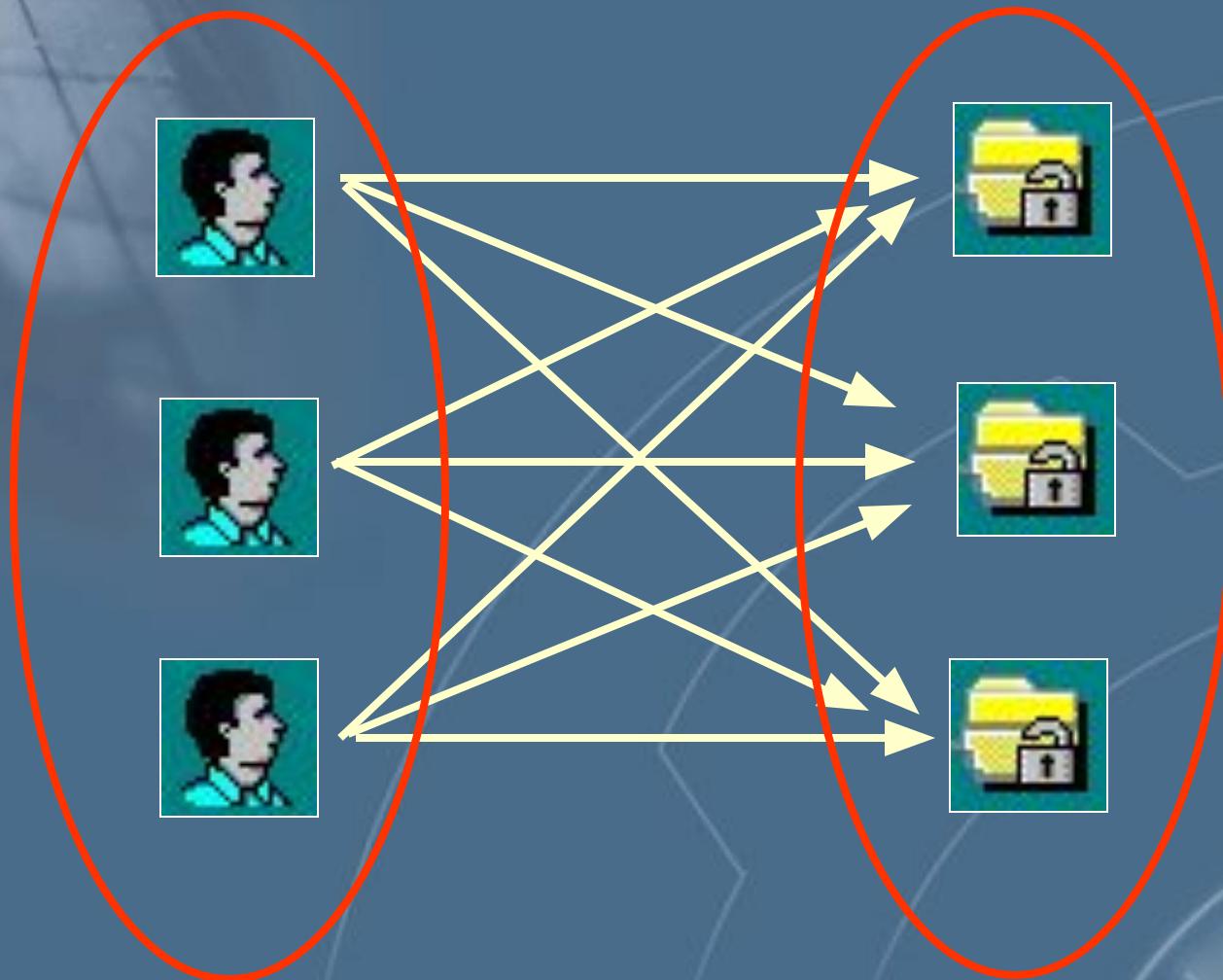
«Случайный» запрос пароля

Совпал  
с предсказанным

Полученный ранее  
от клиента отклик

Предсказуемый запрос

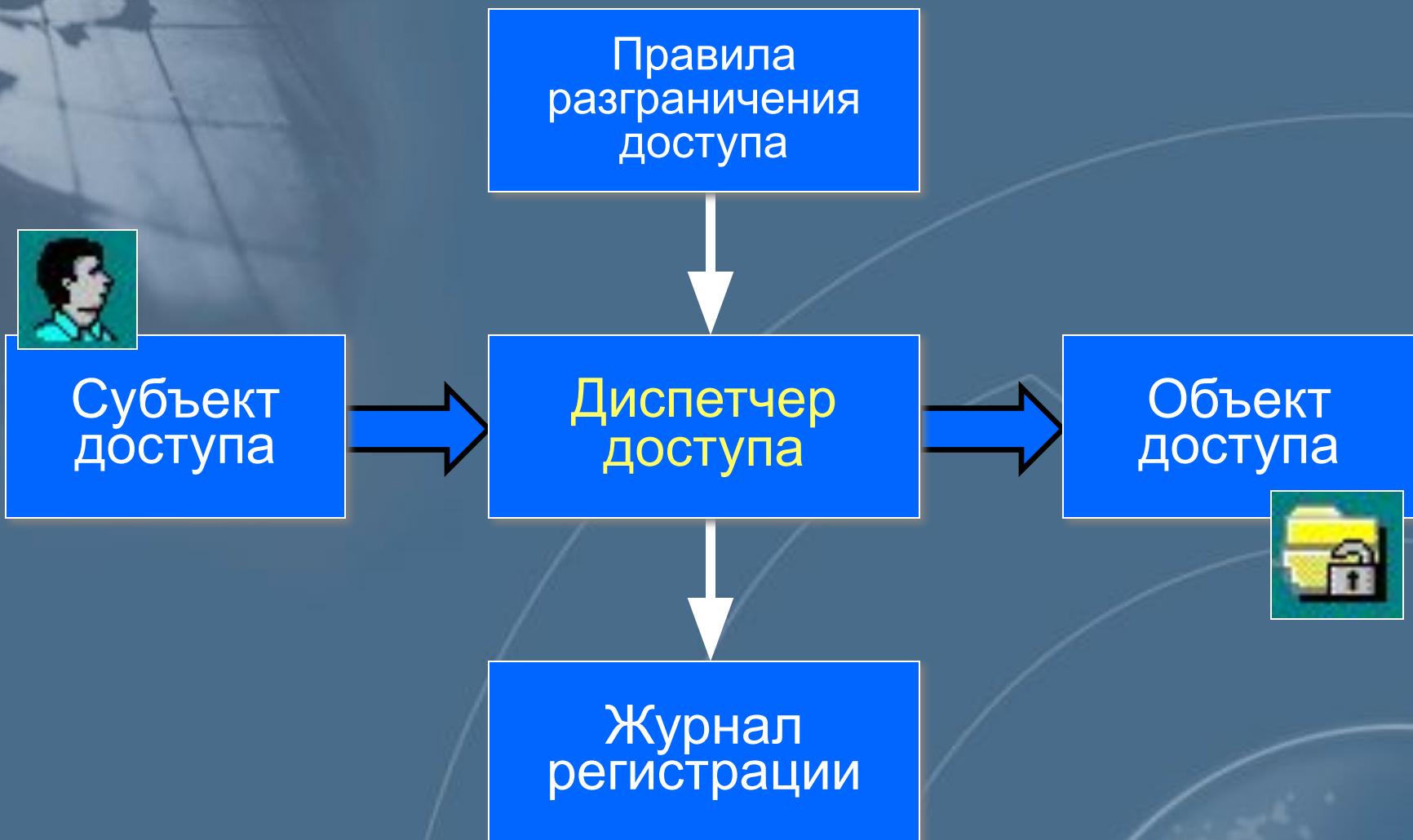
# Разграничение доступа



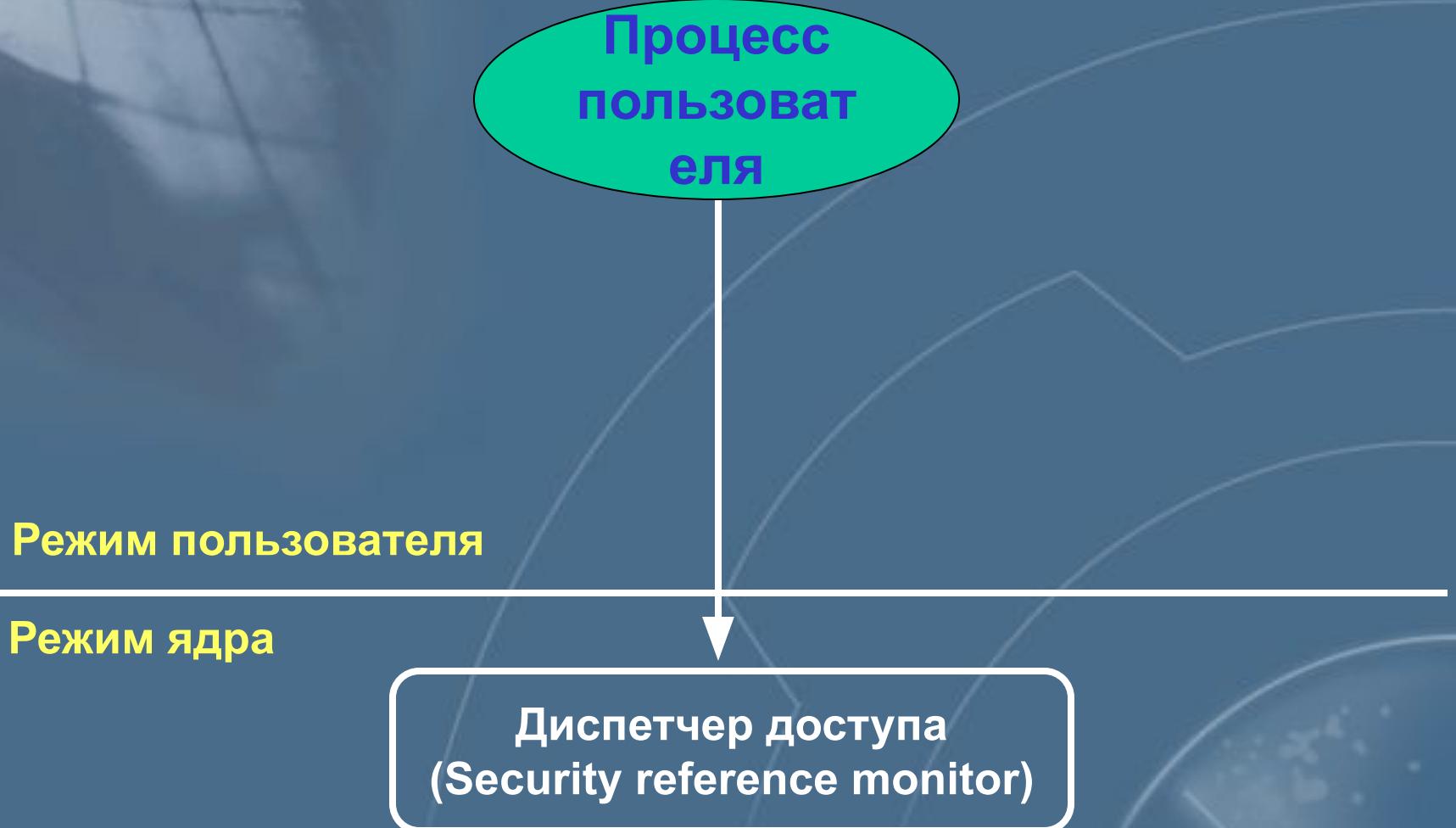
# Разграничение доступа

**избирательное управление доступом  
полномочное управление доступом**

# Разграничение доступа



# Разграничение доступа



# Матрица избирательного управления доступом

		объекты						
		1	2	...	$J$	$J+1$	...	$K$
субъекты	1				$R$			
	2				$RW$			
$I$	$RW$	-		$RWX$	-			$R$
$N$								

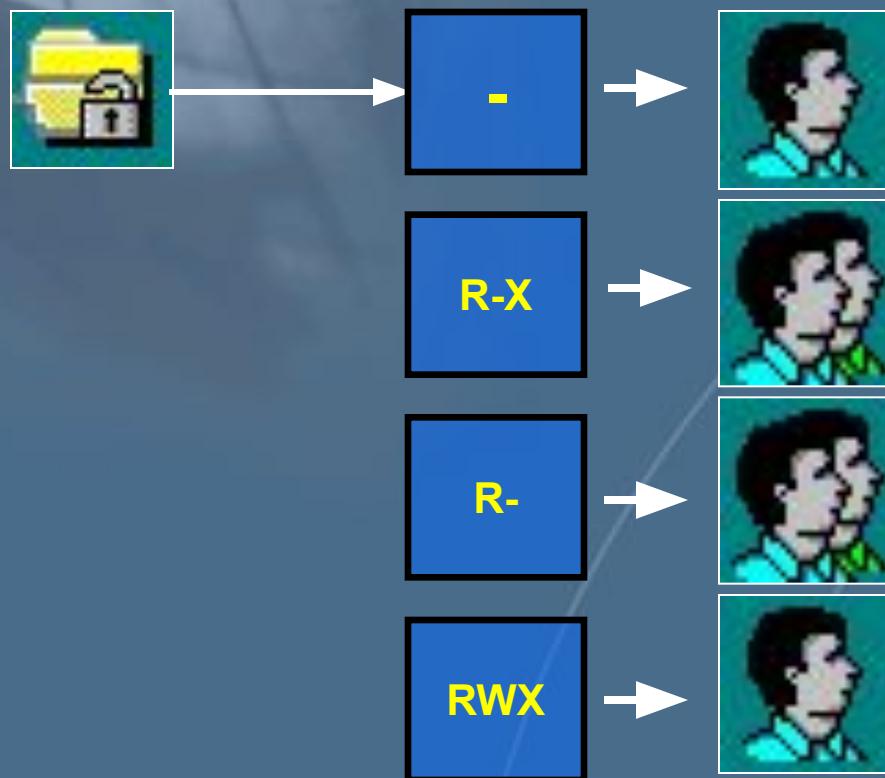
Права доступа  
i-го субъекта  
к j-му объекту



# Списки управления доступом в Windows NT (NTFS)

C:\Program Files

Access Control List (ACL)



User 1

Buchg

Audit

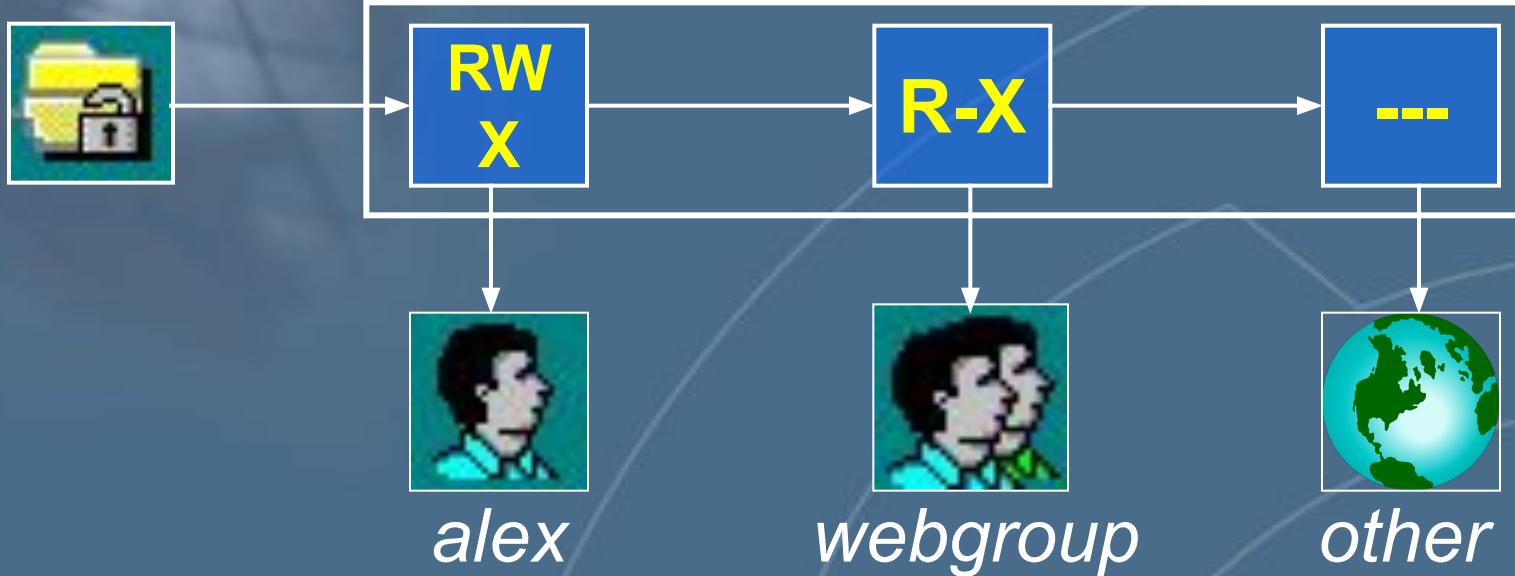
Administrator

*Реализация матрицы доступа «по столбцам»*

# Списки управления доступом в UNIX

/home/www

Владелец      Группа      Остальные



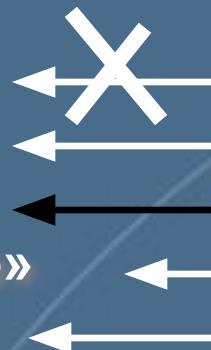
Права доступа хранятся в служебной  
информации файла

# Полномочное управление доступом



Иерархия меток (грифов) конфиденциальности:

«Особой важности»  
«Совершенно секретно»  
«Секретно»  
«Строго конфиденциально»  
«Конфиденциально»

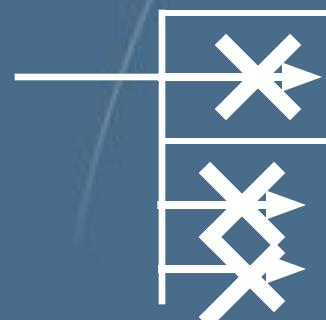


Уровень допуска:

«Совершенно секретно»



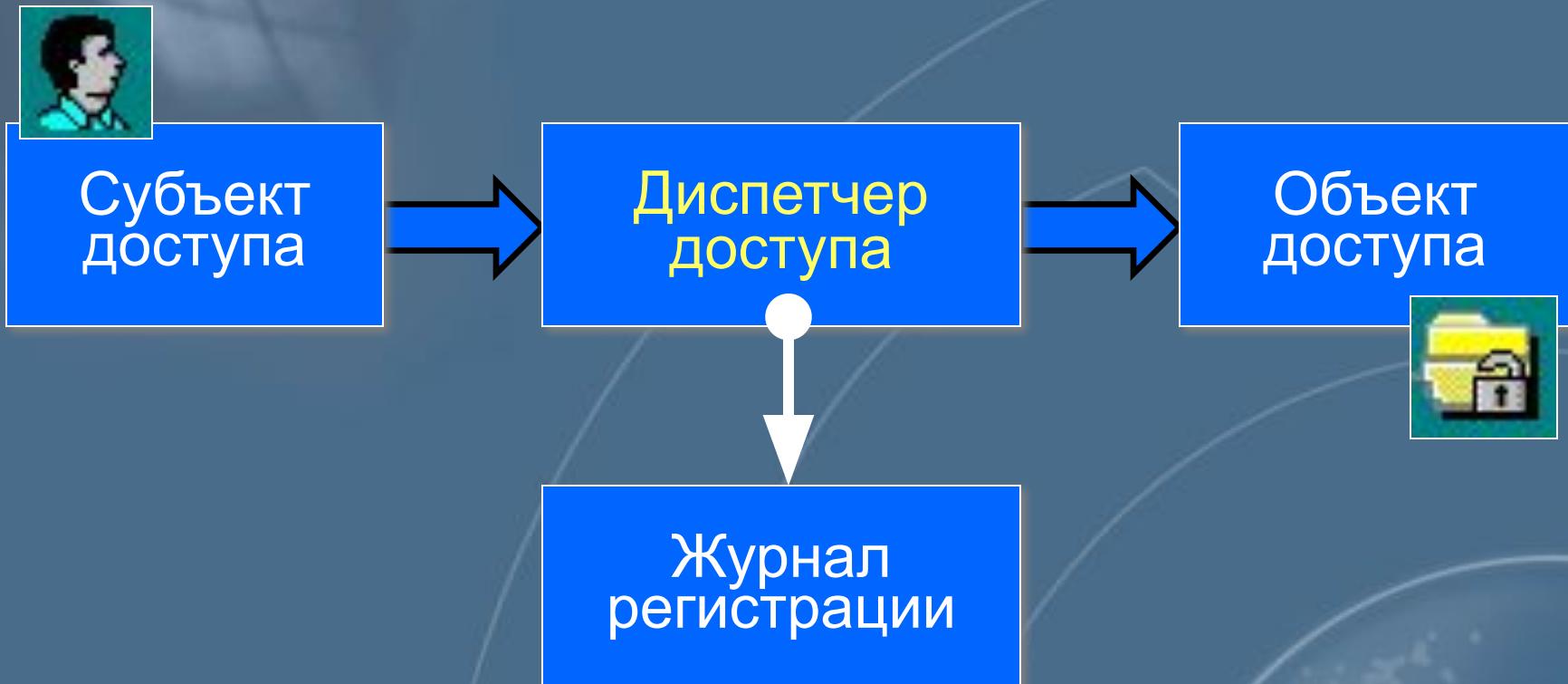
Уровни допуска:  
«Геология»  
«Физика»



Неиерархическая система меток конфиденциальности:

«Геология»  
«Математика»  
«Физика»  
«Строительство»  
и др.

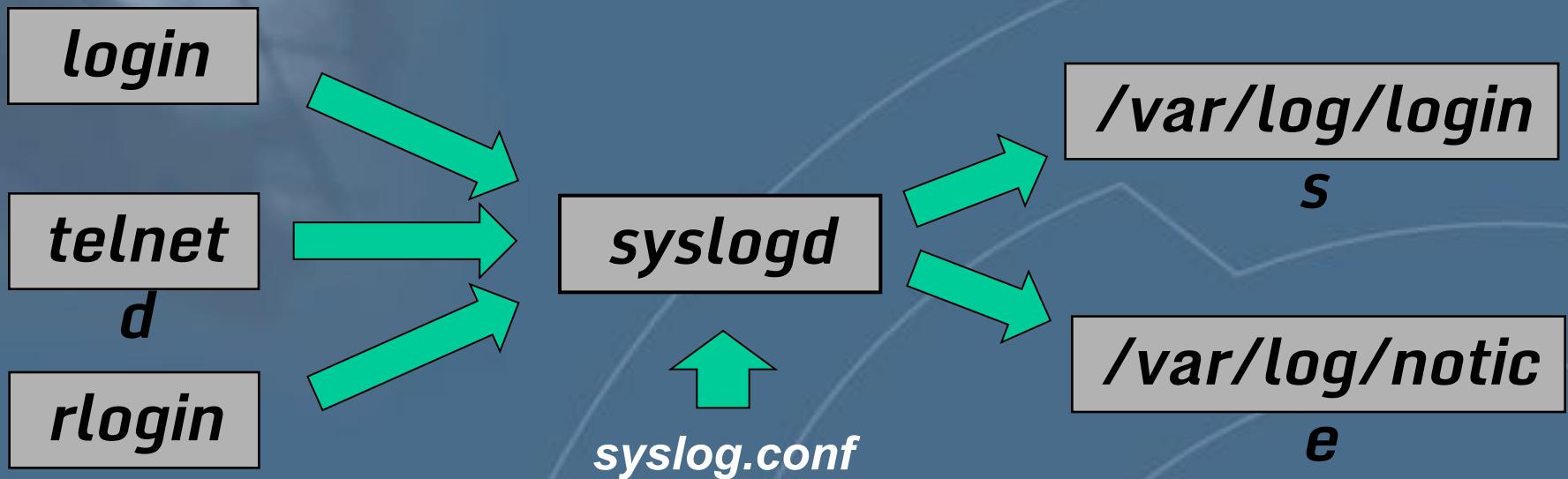
# Механизм регистрации и аудита событий



# Механизм регистрации и аудита событий (Windows NT)



# Система регистрации событий в UNIX



# Контроль целостности



**Механизм контроля целостности  
предназначен для своевременного  
обнаружения фактов модификации  
(искажения, подмены) ресурсов  
системы (данных, программ и т.п.).**

# Контроль целостности

Контролируемые ресурсы:

- файлы и каталоги
- элементы реестра
- сектора дисков

Контролируемые параметры:

- содержимое ресурса
- списки управления доступом
- атрибуты файлов

Алгоритмы контроля:

- сравнение с эталоном
- вычисление контрольных сумм (сигнатур)
- формирование ЭЦП и имитовставок

Время контроля:

- до загрузки ОС
- при наступлении событий
- по расписанию



# Контроль целостности (Windows 2000)

Подсистема Windows File Protection

Повреждённый системный файл заменяется копией из каталога %systemroot%\system32\dllcache

Настройка – при помощи утилиты  
System File Checker (sfc.exe)

```
sfc [/scannow] [/scanonce] [/scanboot] [/cancel]  
[/quiet] [/enable] [/purgecache] [/cachesize=x]
```

# Затирание остаточной информации

**Удаление информации с диска**  
**Очистка области памяти**

# Затирание остаточной информации

Hive: HKEY\_LOCAL\_MACHINE

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

Name: ClearPageFileAtShutdown

Type: REG\_DWORD

Value: 1

**Очистка файла подкачки**

# Политика безопасности и ОС



# Политика безопасности и ОС

Общие рекомендации  
по различным областям

Связующее звено между  
политикой безопасности  
и процедурой настройки  
системы

Пример:  
**British Standard BS7799**

Общие стандарты

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  
элеме  
нтов

# 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

# 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

1. Введение
2. Обзор документа
3. Процесс инсталляции
  1. Особенности клонирования операционной системы
  2. Отключение неиспользуемых подсистем  
**HKEY\_LOCAL\_MACHINE\System\CurrentControlSet\Control\Session Manager\Subsystems**
  3. Отключение ненужных устройств
  4. ...

19

частей

# NT Security Guidelines

19

частей

## 1. Домены и ограничение доступа

1. Domain&Trust (деление на домены и доверительные отношения)

2. Logon Rights (Log on locally, Logon Remote)

3. Ограничение входа только с определённых узлов

## 2. Привилегии администратора

1. Бюджет администратора

2. Группа администраторов

3. Domain Operators&Power Users

# NT Security Guidelines

6. General Policies (общие рекомендации)
  1. Ограничение доступа к FDD и CD
  2. Ограничение удалённого доступа к реестру
  3. Утилиты SYSKEY, C2Config....
7. ACL для файловой системы и реестра
8. Установка приложений и пользовательские каталоги
9. Бюджеты пользователей и групп
10. Пароли
11. Редактор системной политики
12. Права пользователей

19

частей

# NT Security Guidelines

13. Журнал безопасности
14. Службы
15. Доступ к общим ресурсам
16. Сетевые возможности
17. Удалённый доступ
18. Атаки
19. Рекомендации для пользователей

19  
частей

# Утилиты для настройки

**Анализ текущего состояния системы**

**Автоматизация процесса  
настройки системы**

# Утилиты для настройки

**C2 Config - Windows NT Resource Kit**

**Security Configuration Manager (SCM)**

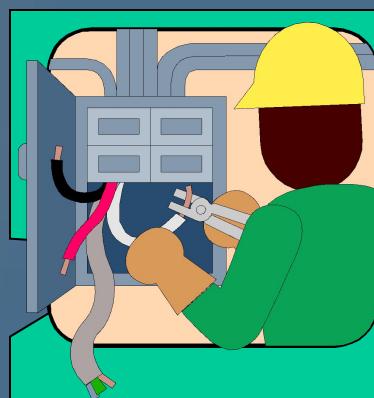
**Security Configuration Tool Set**

**Windows NT (2000)**

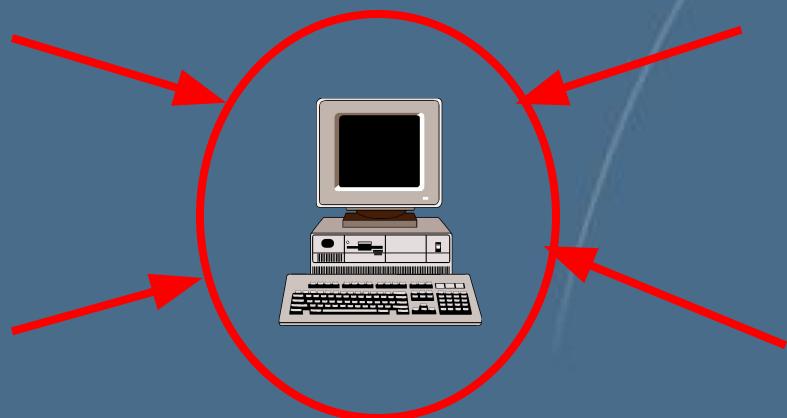
# Дополнительные средства



Дополнительные средства защиты



Средства анализа защищённости



Средства обнаружения и  
блокировки вторжений

# Дополнительные средства



## Дополнительные средства защиты

Средства, расширяющие возможности встроенных механизмов защиты

Средства, реализующие дополнительные механизмы защиты

# Дополнительные средства



**Усиление процедуры аутентификации**

**Дополнительные требования к паролям**

- Фильтр passfilt.dll для Windows NT
- Модули PAM для Linux

# Фильтр для паролей

Passfilt.dll

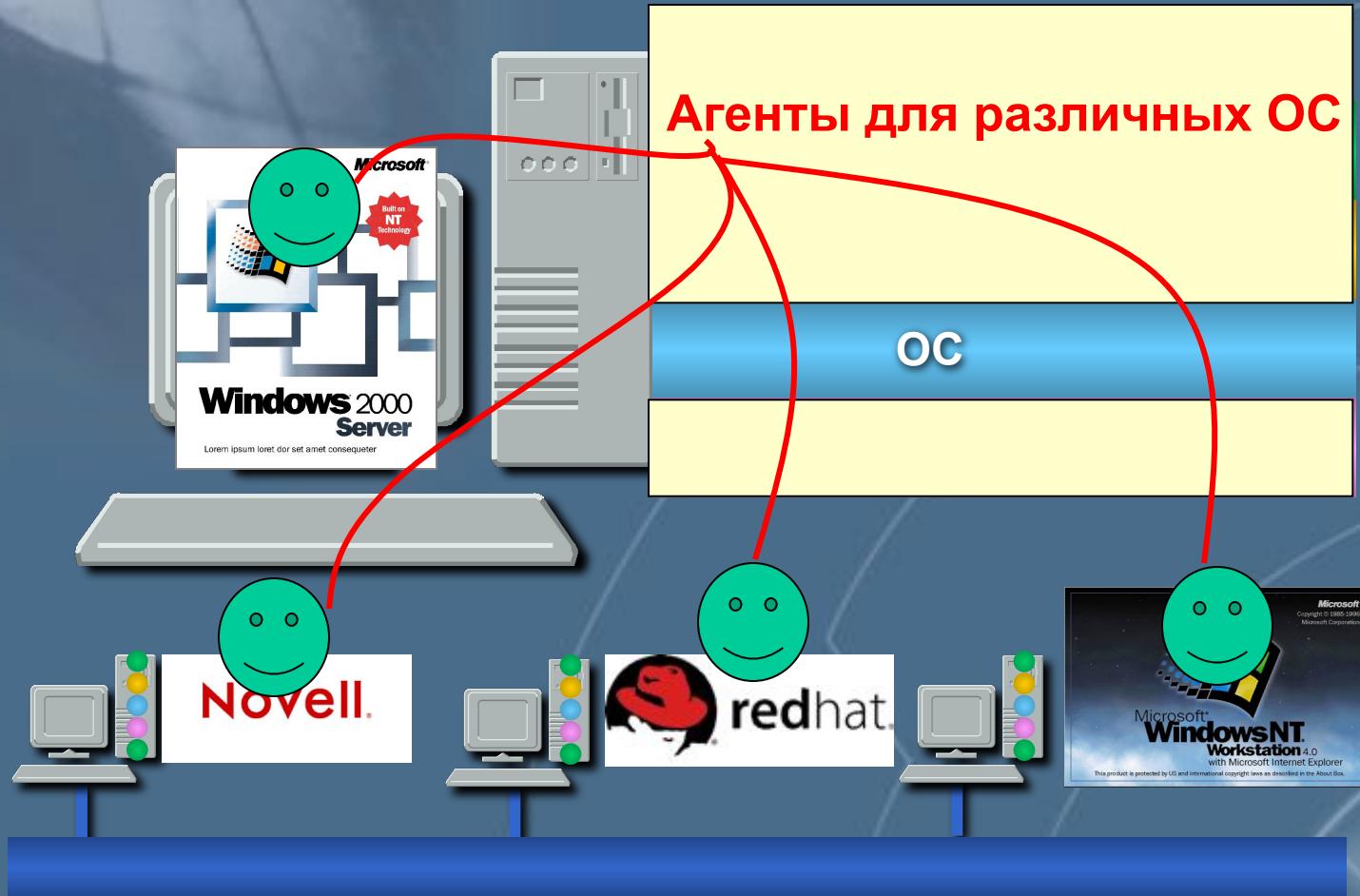
- Длина пароля не менее 6 знаков
- Обязательные символы  
(верхний/нижний регистр, числа, спецсимволы)
- Пароль не должен содержать имя пользователя

# Дополнительные средства

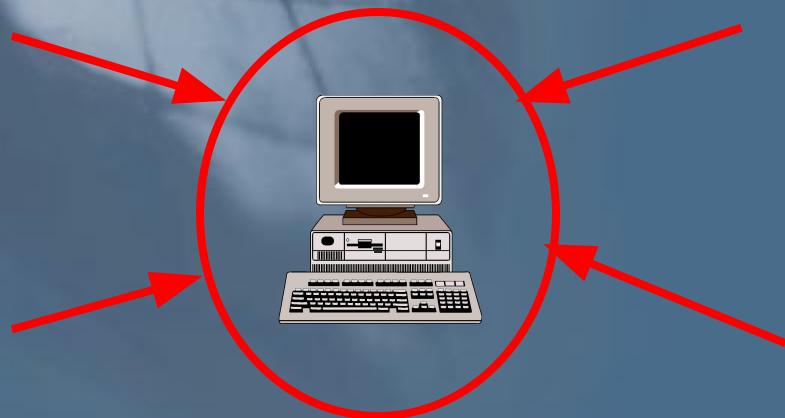
## Утилита Passprop

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

# Анализ защищенности на уровне операционной системы



# Дополнительные средства



Средства обнаружения и  
блокировки вторжений

- Системы обнаружения атак на базе узла
- Персональные МЭ

# Системы обнаружения атак на базе узла

Источники данных:

- Журналы аудита
- Действия пользователей

Необязательно:

Сетевые пакеты (фреймы),  
направленные к узлу и от узла



# Рекомендации по выбору ОС



- Доступность исходных текстов
- Уровень квалификации персонала
- Варианты осуществления технической поддержки
- Требования к ОС и цели её использования
- Стоимость «железа», программного обеспечения и сопровождения

Критерии выбора

# Вопросы?

Учебный Центр «ИНФОРМЗАЩИТА»  
([www.infosec.ru/edu](http://www.infosec.ru/edu))

Лепихин Владимир  
([lepihin@infosec.ru](mailto:lepihin@infosec.ru))

Телефон: (095) 937-3385  
Факс: (095) 289-4232

