

# Безопасность уровня операционных систем (узлов)

Раздел 3

# Рассматриваемые темы

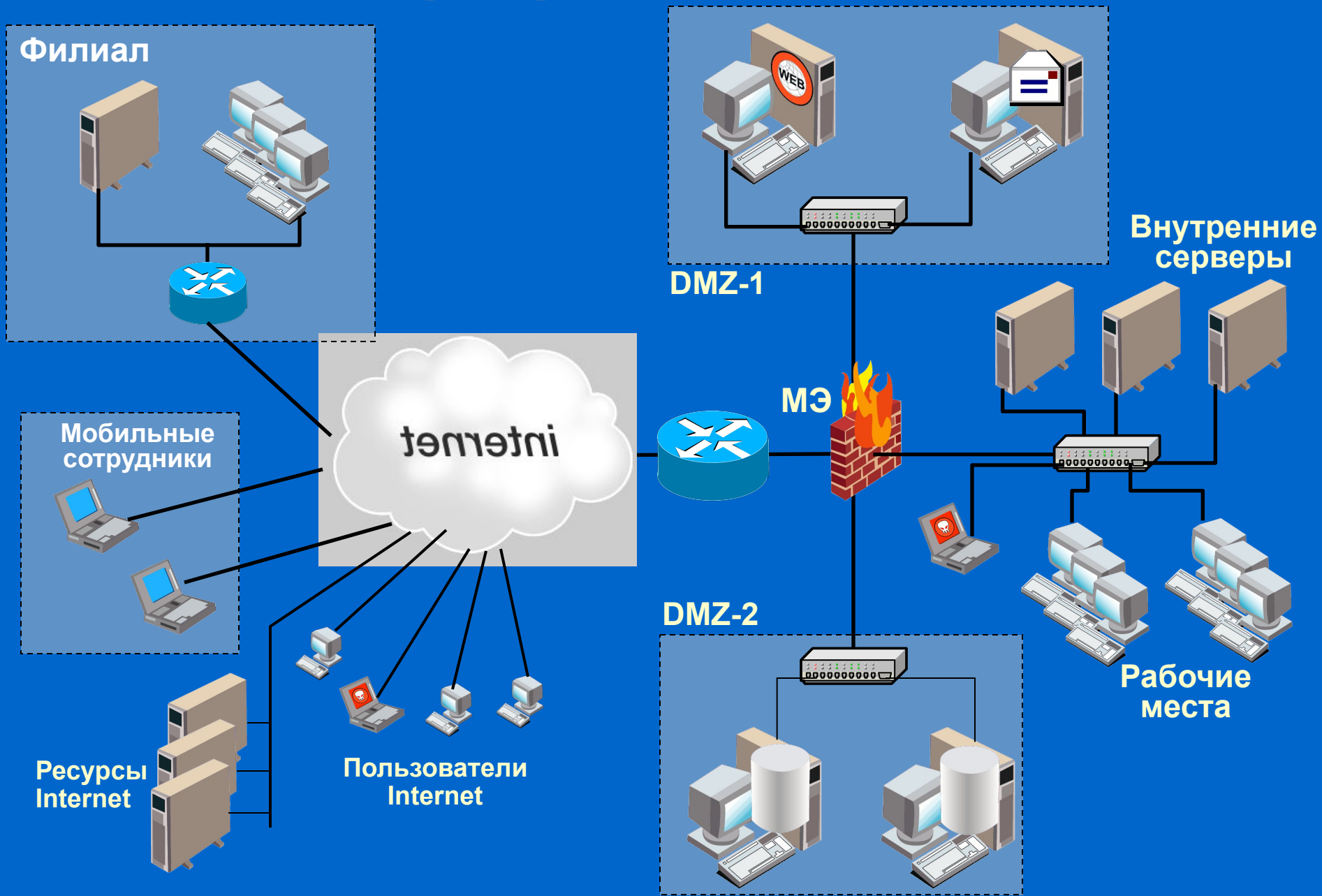
Тема 16. Проблемы обеспечения безопасности сетевых ОС

Тема 17. Анализ защищённости на уровне ОС

# Проблемы обеспечения безопасности сетевых операционных систем

Раздел 3 – Тема 16

# Корпоративная сеть



# Уровень ОС



# Причины возникновения уязвимостей ОС

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

# 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

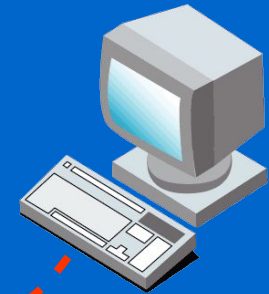
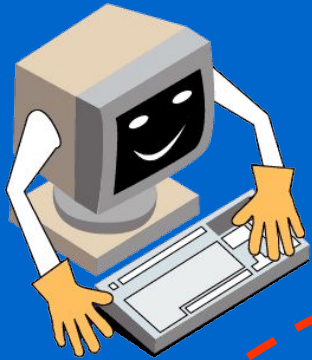
Переполнение буфера – наиболее распространённая техника использования ошибок реализации

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

# 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



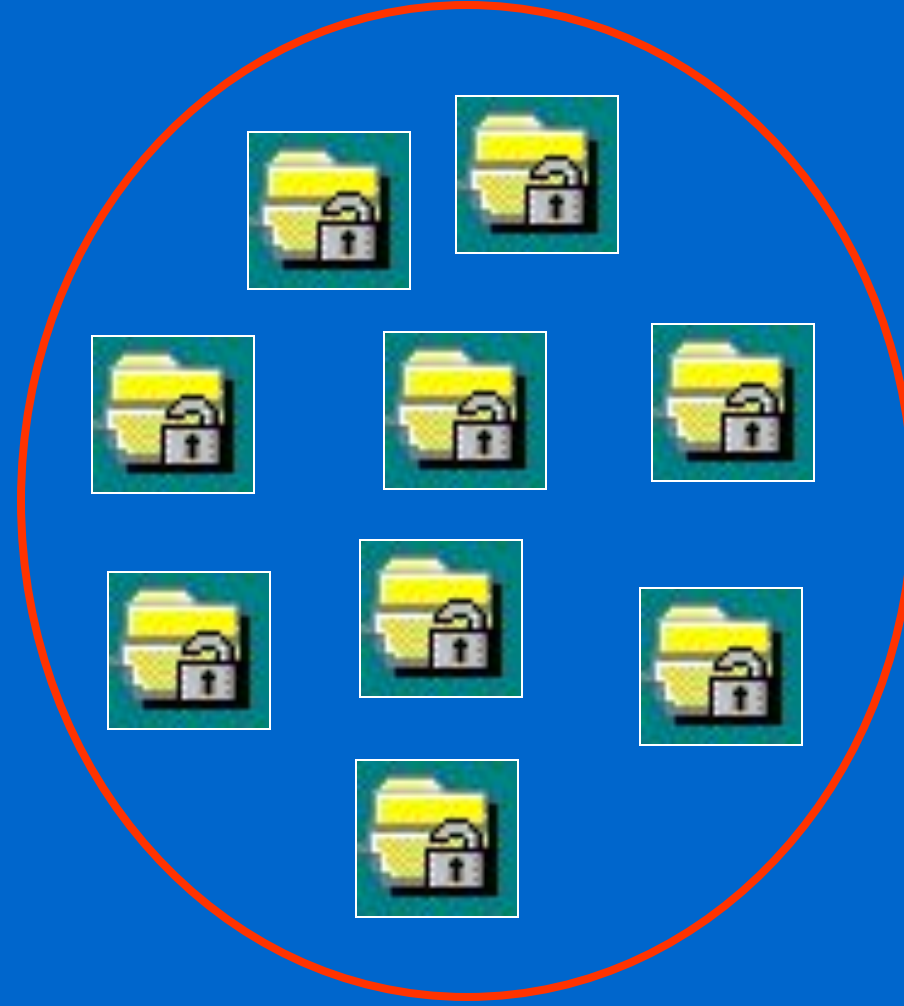
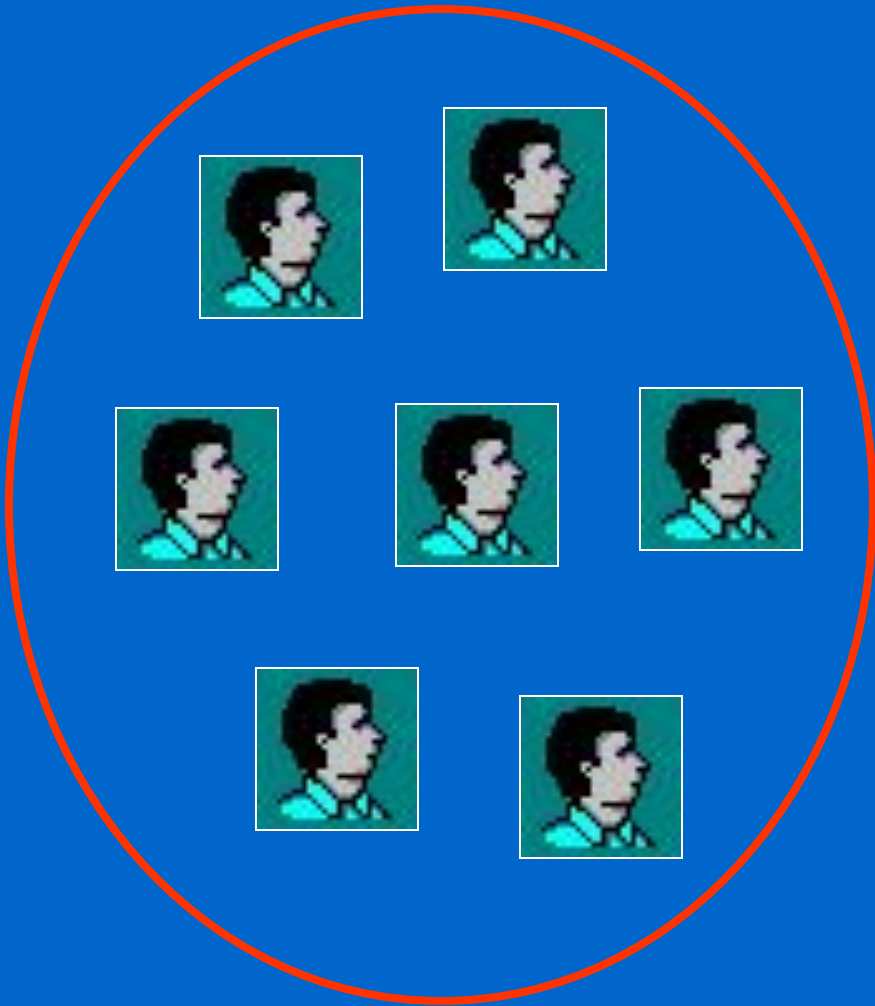
Ошибки использования встроенных в ОС  
механизмов защиты

# 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)

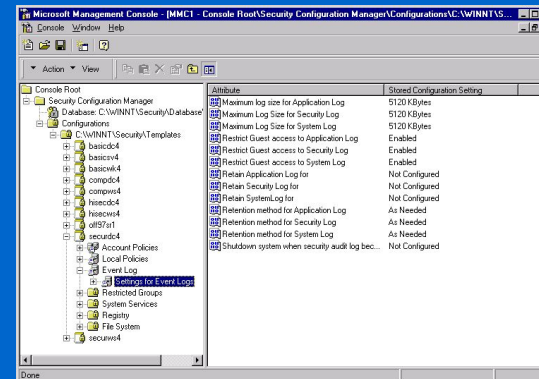
# Пример субъекта доступа



=

Пользователь  
Master

+



Субъект доступа = Маркер безопасного доступа + Процесс (поток)

Субъект доступа в ОС Windows NT

# Пример субъекта доступа



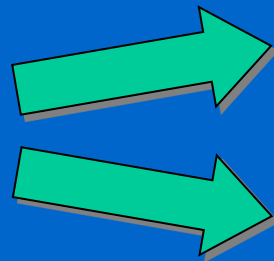
Субъект  
доступа

В роли субъектов доступа в Linux  
выступают процессы

Процессы :

- Получают доступ к файлам
- Управляют другими процессами

Процесс



файл

процесс

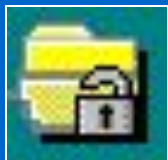
Субъект доступа в Linux

# 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).



**Logon Information**

Enter a user name and password that is valid for this system.

 User name:

Password:

Domain:  ▾

OK  Cancel Help Shut Down...

# 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



Запрос пароля



Зашифрованный запрос



Аналогичная  
операция и  
сравнение

Механизм «запрос/отклик»

# Уязвимости аутентификации (по паролю)

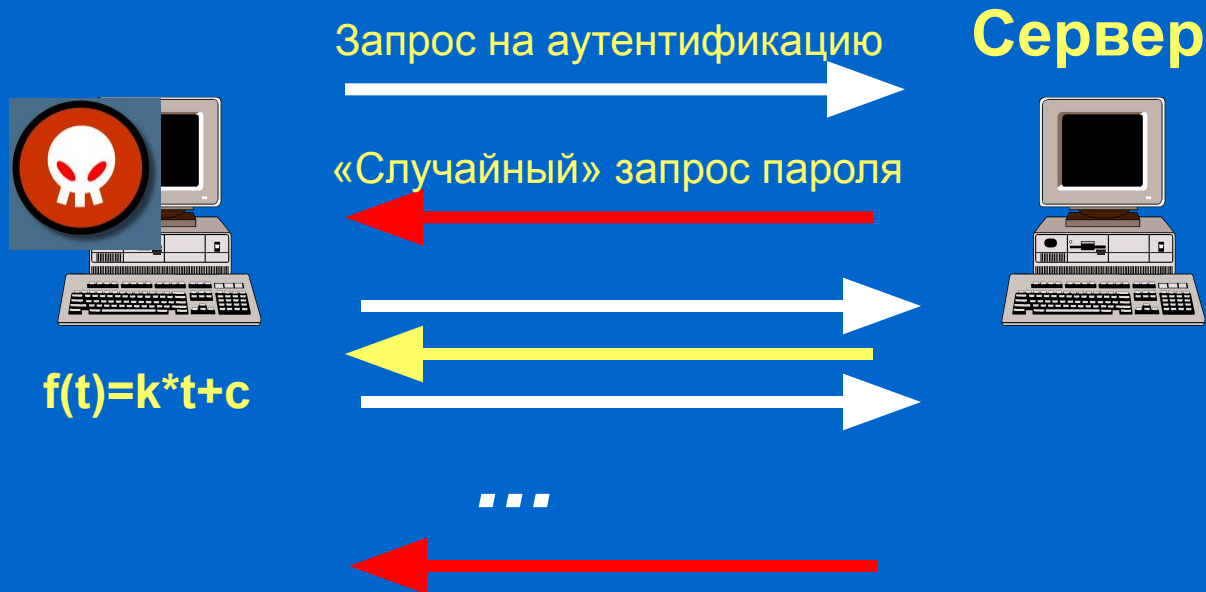
Возможность перехвата и повторного использования пароля (получение доступа к файлам с паролями)

«Троянские кони» в процедуре входа в систему

Социальная инженерия

Повторяющийся запрос при сетевой аутентификации

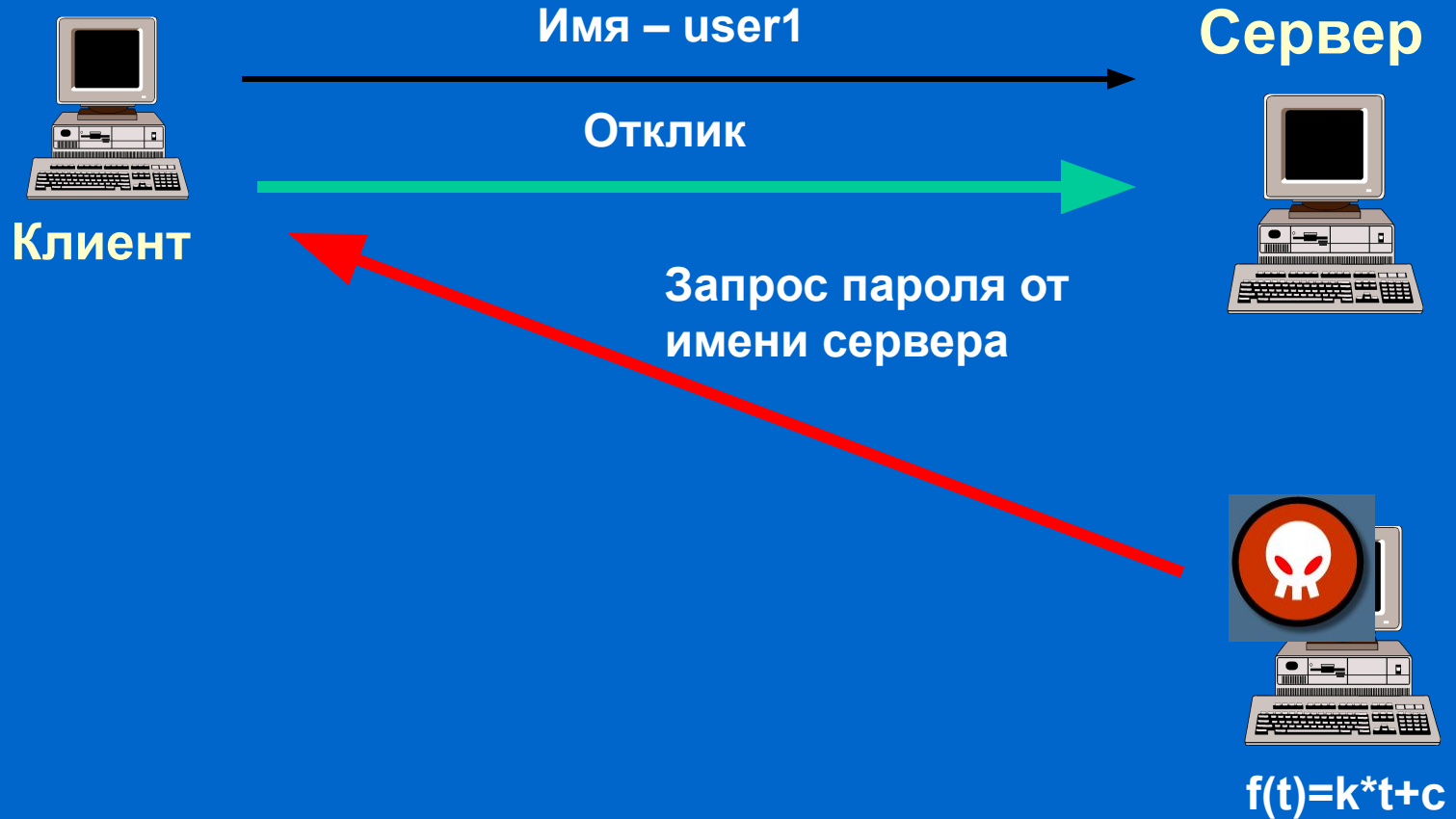
# Сетевая аутентификация



**Предсказуемый запрос**



# Сетевая аутентификация



**Предсказуемый запрос**

# Сетевая аутентификация

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



Сервер



Запрос на аутентификацию

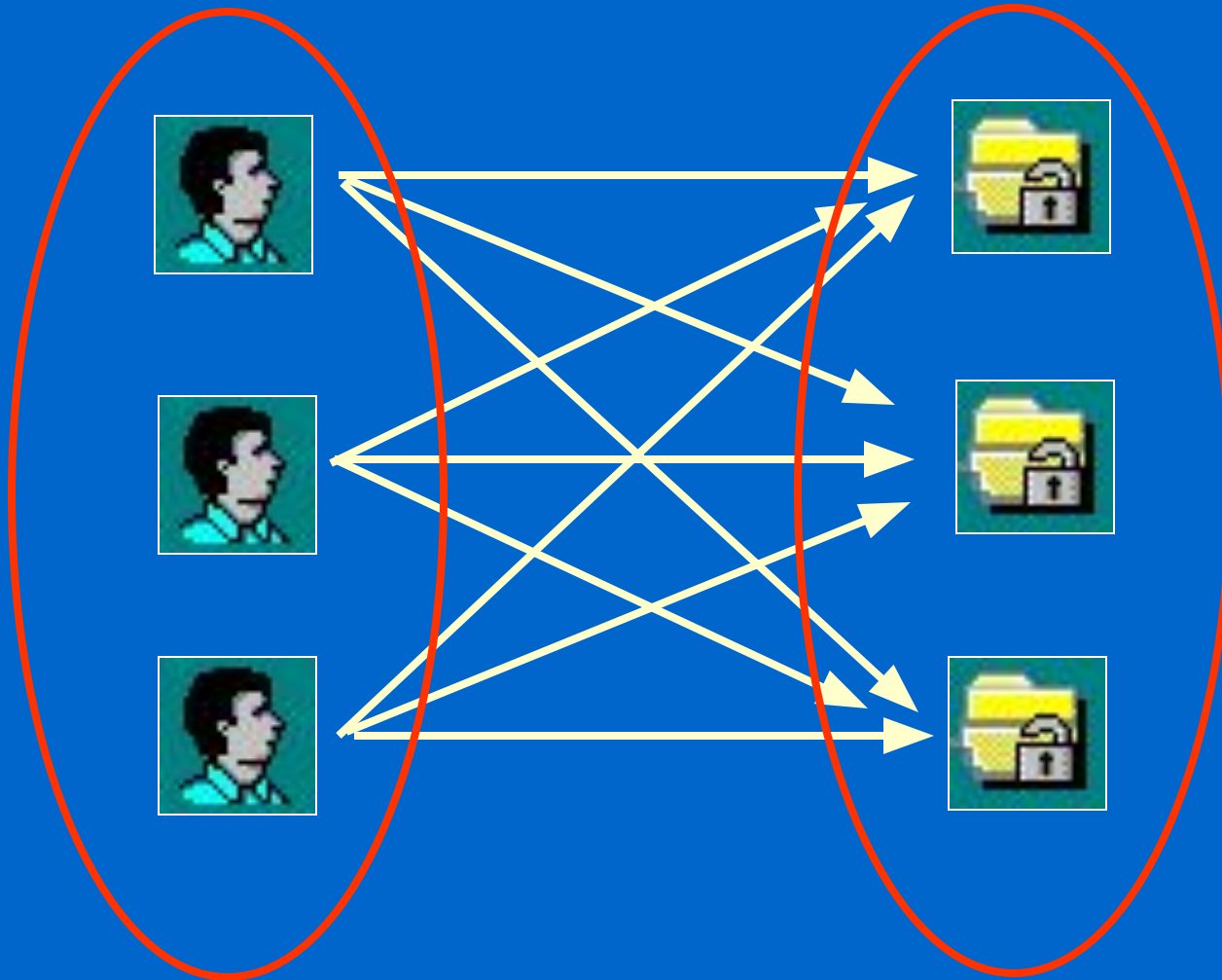
«Случайный» запрос пароля

Совпал  
с предсказанным

Полученный ранее  
от клиента отклик

Предсказуемый запрос

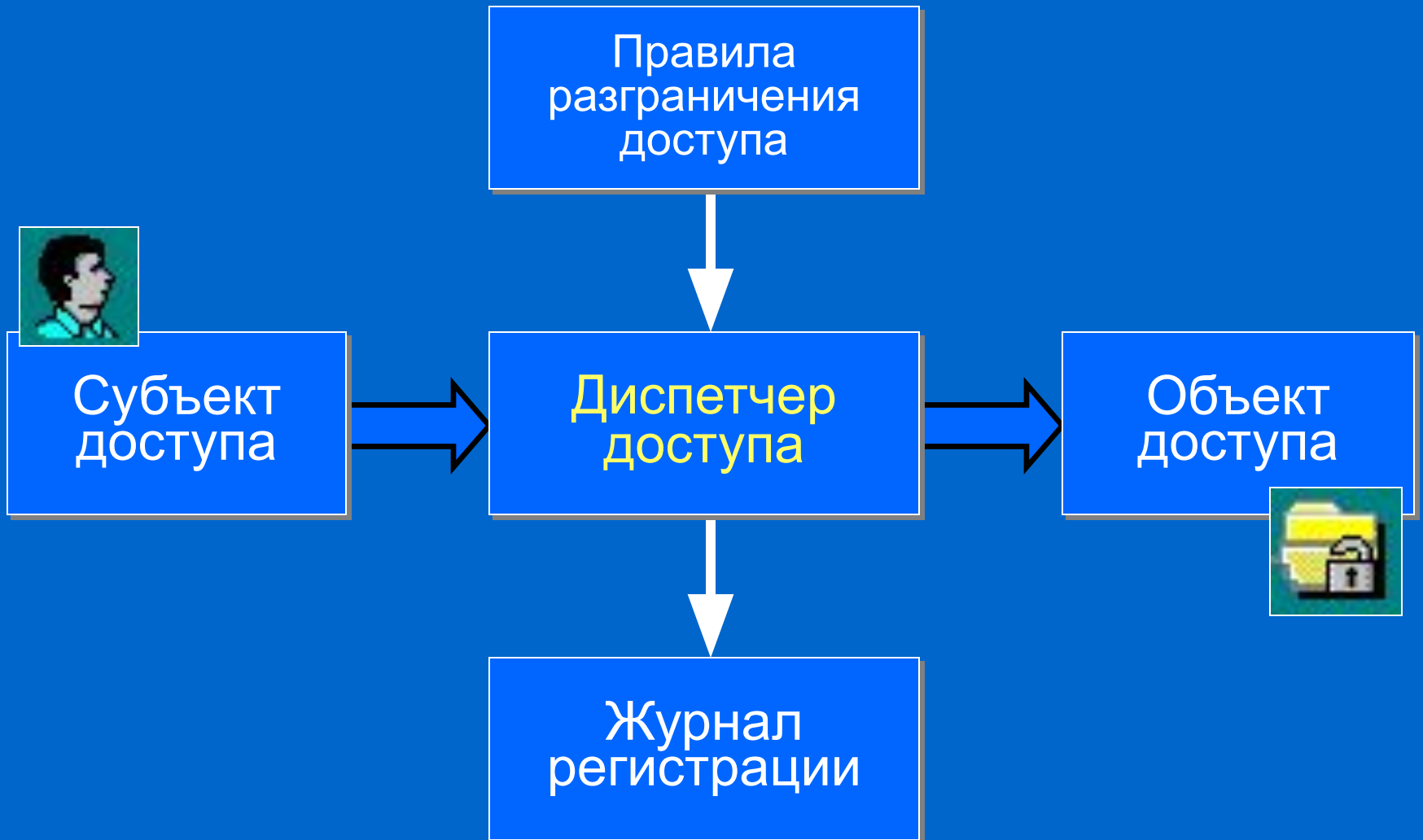
# Разграничение доступа



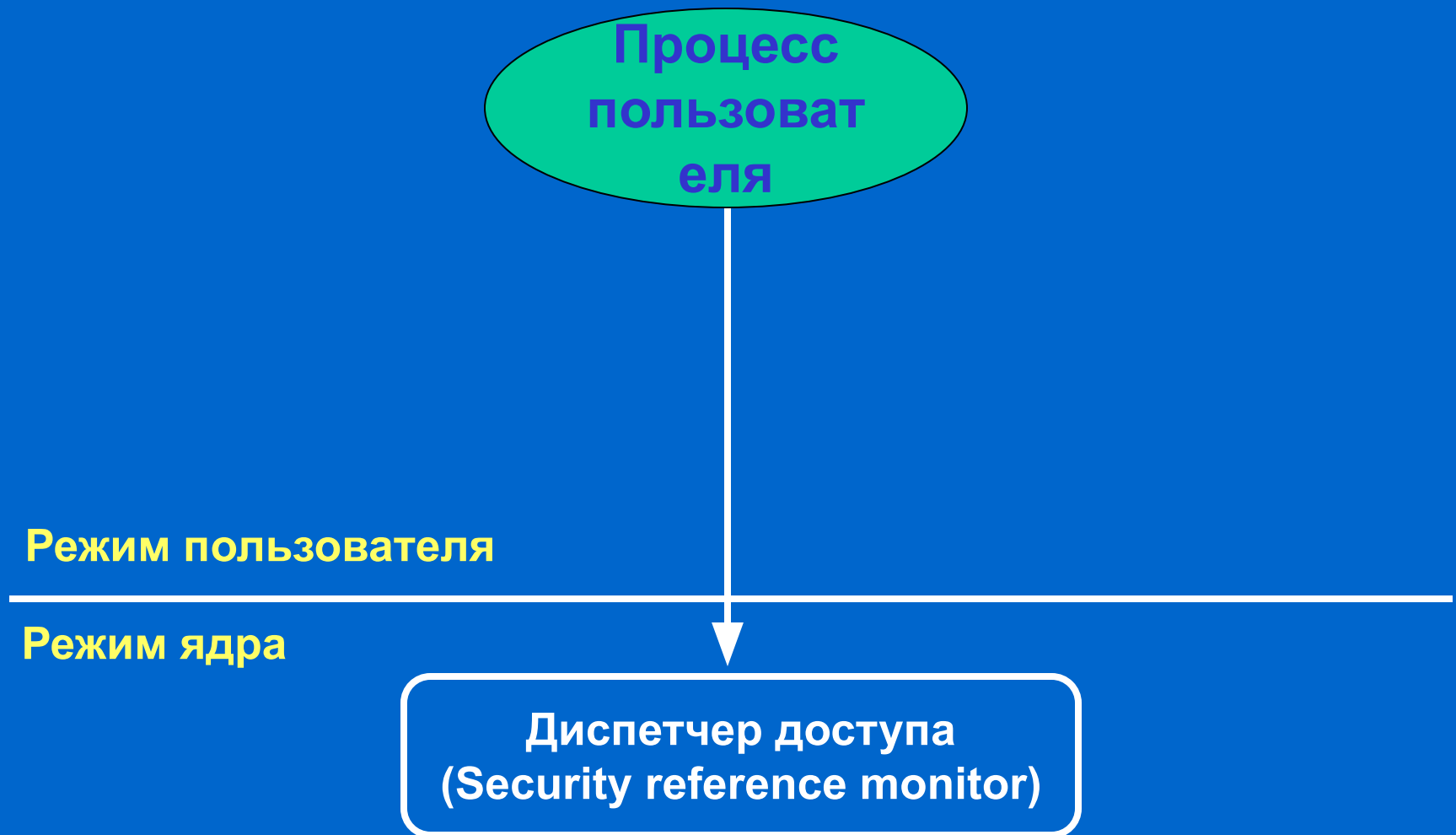
# Разграничение доступа

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
	...							
	$N$							

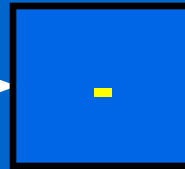
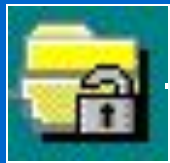
Права доступа  $i$ -го субъекта к  $j$ -му объекту



# Списки управления доступом в Windows NT (NTFS)

C:\Program Files

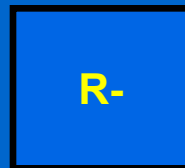
Access Control List (ACL)



User 1



Buchg



Audit

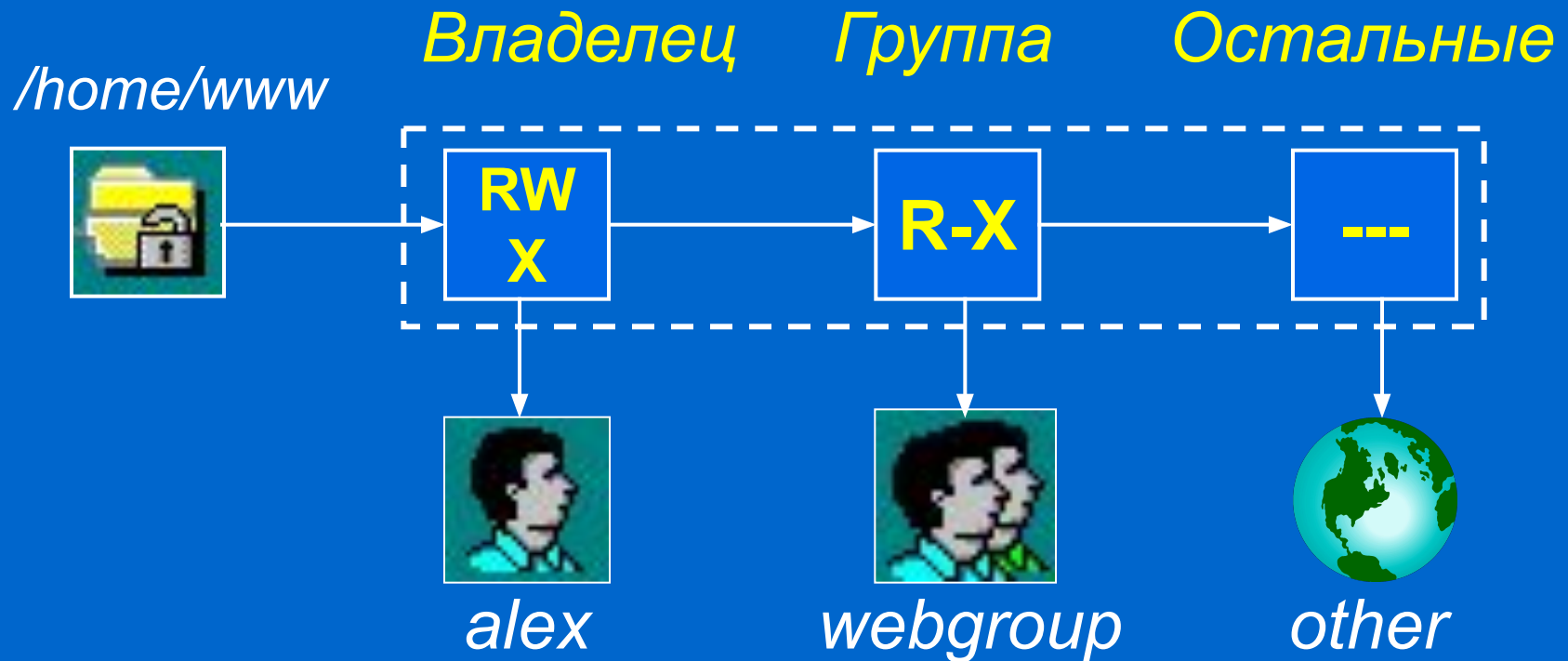


Administrator

*Реализация матрицы доступа «по столбцам»*

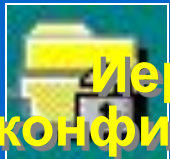


# Списки управления доступом в UNIX



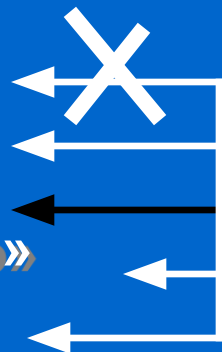
**Права доступа хранятся в служебной информации файла**

# Полномочное управление доступом



Иерархия меток (грифов) конфиденциальности:

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



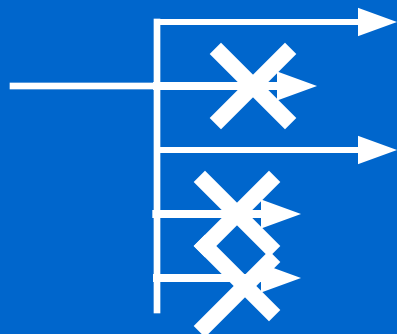
Уровень допуска:

«Совершенно секретно»



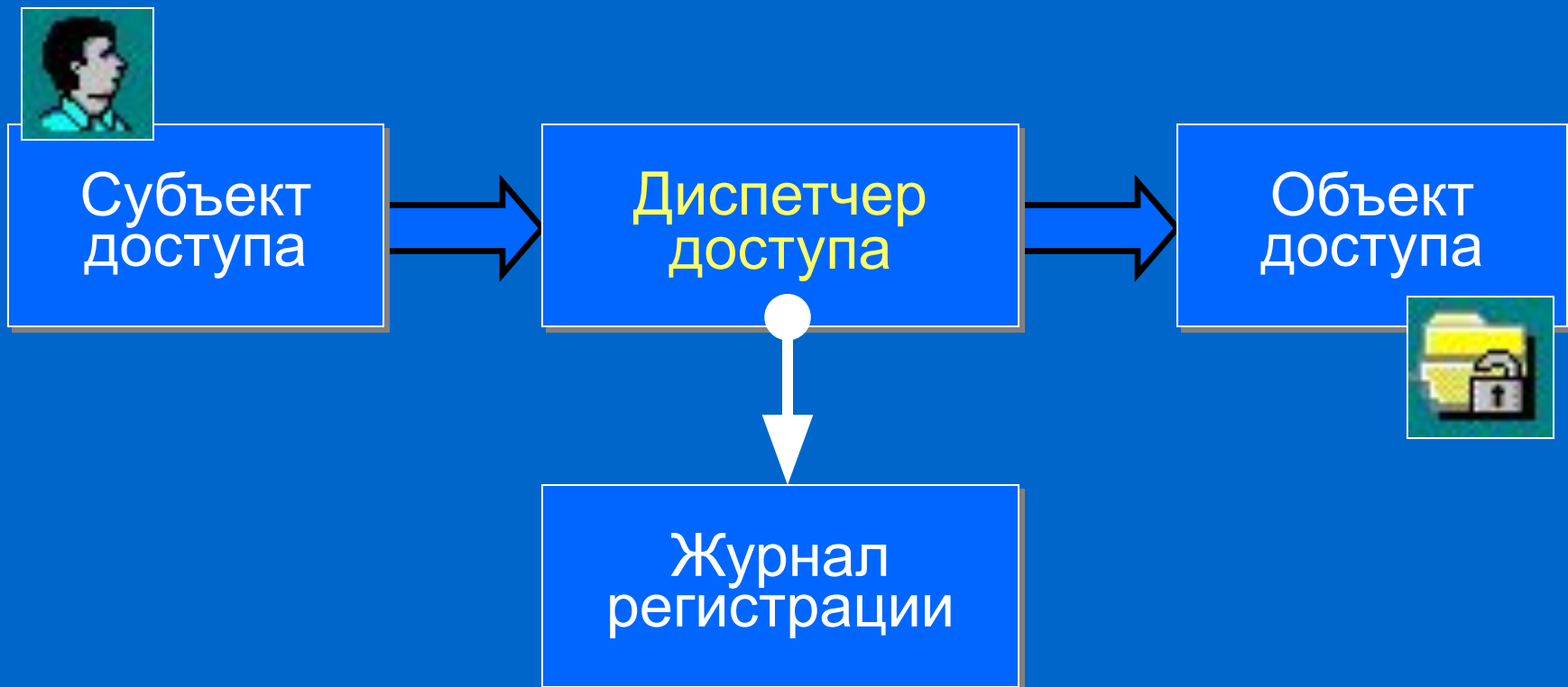
Неиерархическая система меток конфиденциальности:

Уровни допуска:  
«Геология»  
«Физика»



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

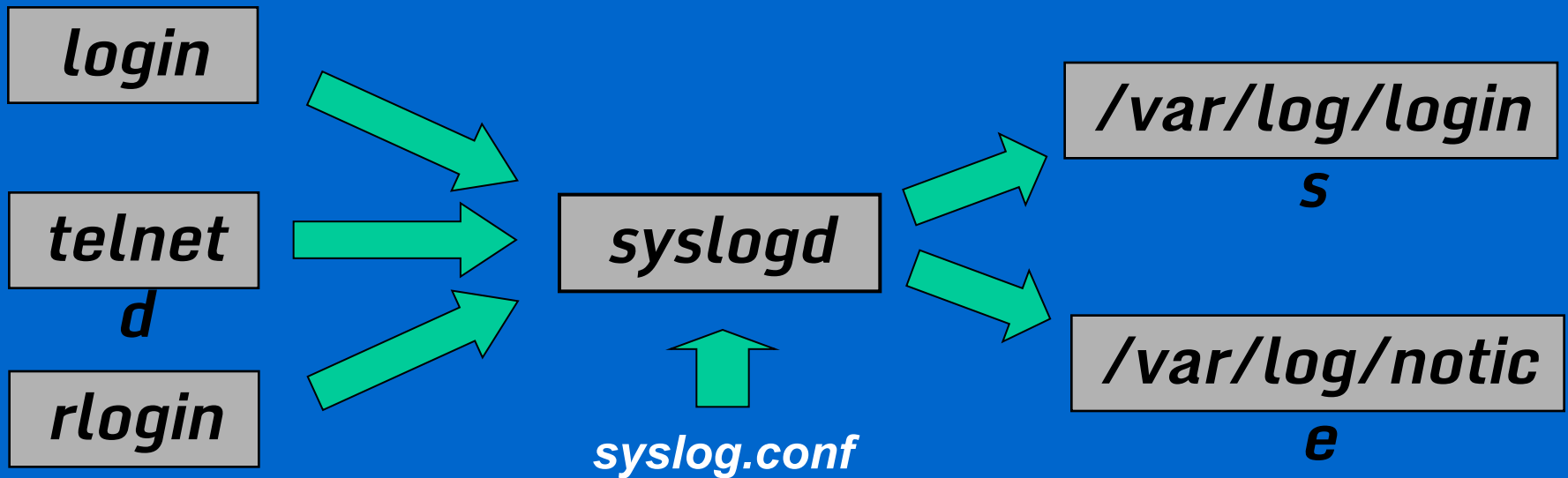
# Механизм регистрации и аудита событий



# 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:

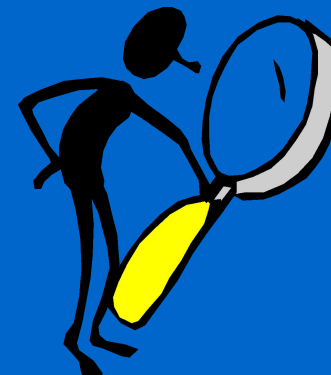
- содержимое ресурса
- списки управления доступом
- атрибуты файлов

## 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**

# Этапы настройки

Отслеживание уязвимостей реализации и установка исправлений;

Настройка параметров субъектов (например, назначение привилегий пользователям);

Разграничение доступа к объектам (например, папкам, файлам, ключам реестра);

Настройка параметров системы, влияющих на безопасность (например, установка ключей реестра).

Настройка системной политики (длина паролей, их сложность, параметры блокировки и т. д.).

# 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



# 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  
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



# Утилиты для настройки

**Анализ текущего состояния системы**

**Автоматизация процесса  
настройки системы**

# Утилиты для настройки

**C2 Config - Windows NT Resource Kit**

**Security Configuration Manager (SCM)**

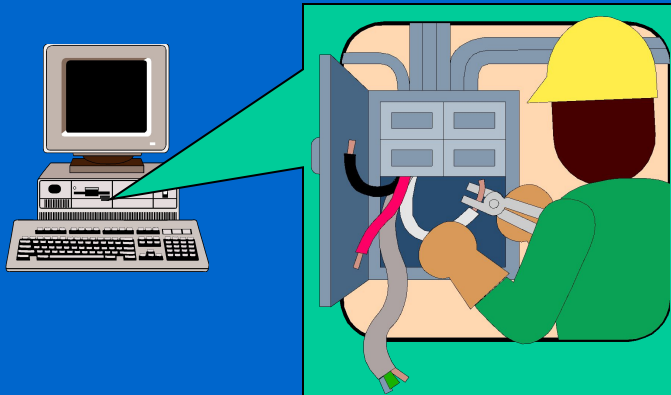
**Security Configuration Tool Set**

**Windows NT (2000)**

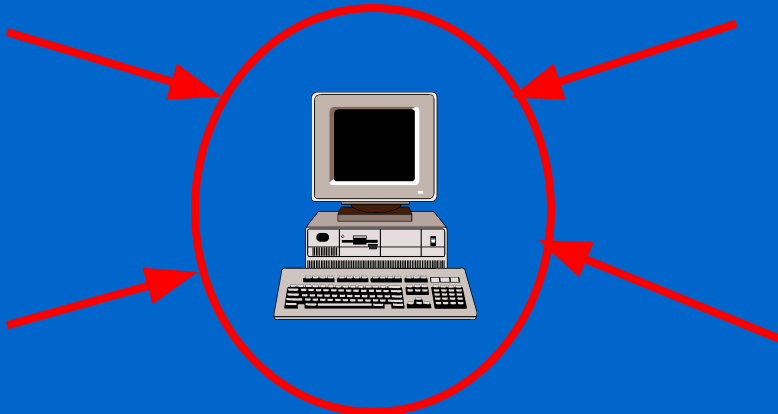
# Дополнительные средства



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**

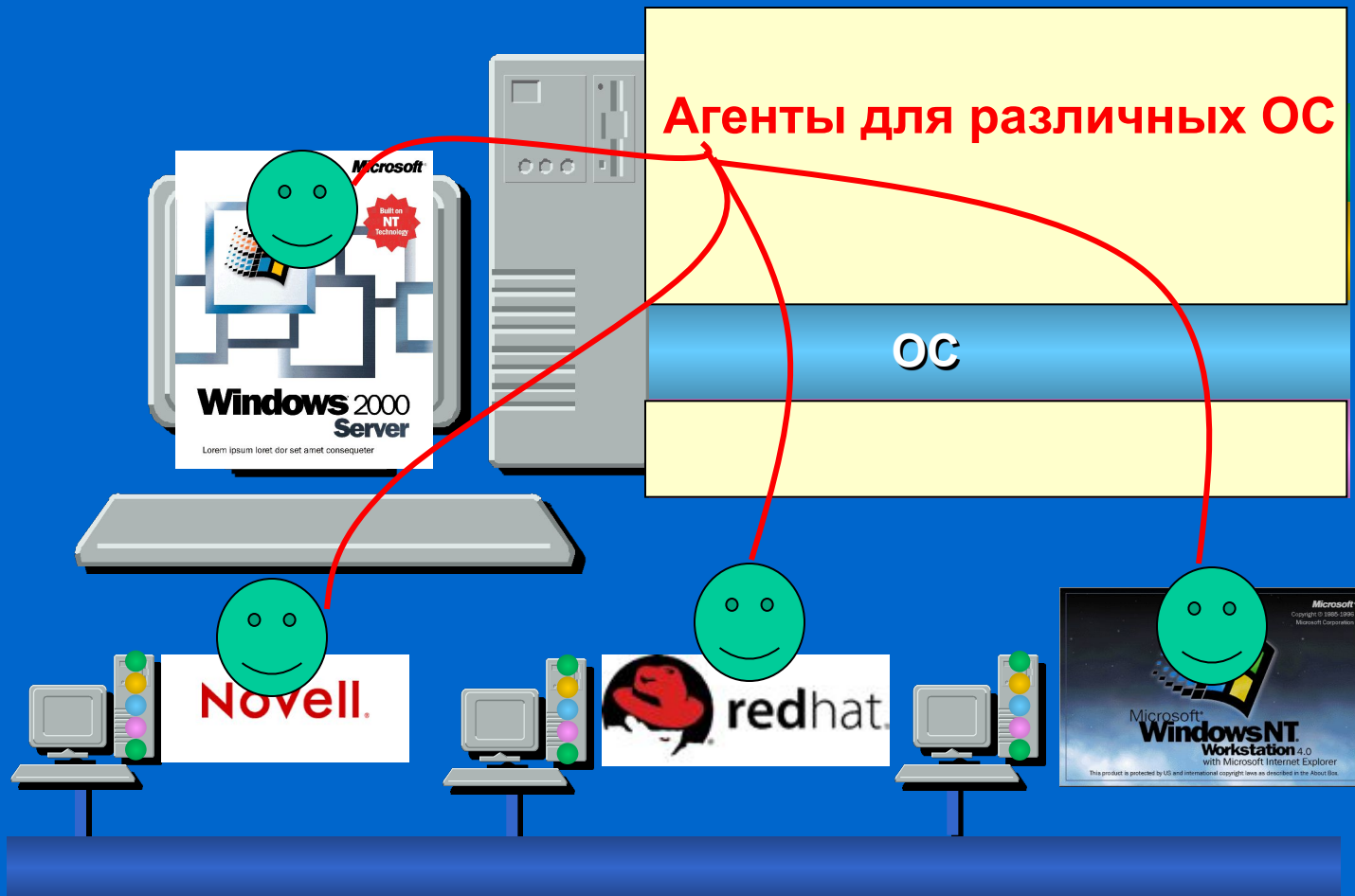
- Длина пароля не менее 6 знаков
- Обязательные символы  
(верхний/нижний регистр, числа, спецсимволы)
- Пароль не должен содержать имя пользователя

# Дополнительные средства

## Утилита Passprop

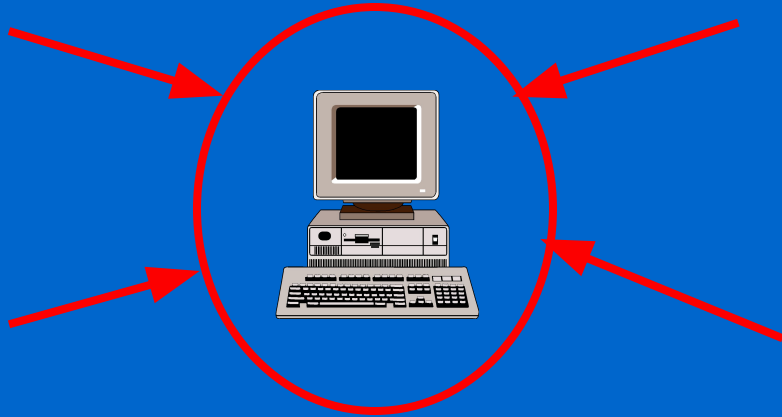
- Включение режима усложнения пароля
- Управление блокировкой учётной записи «Administrator»

# 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

