

# 5. АТАКИ ИЗНУТРИ СИСТЕМЫ

# 5.1 ТРОЯНСКИЕ КОНИ

```
echo $PATH
```

```
:/usr/ast/bin:/usr/local/bin:/usr/bin\  
:/bin:/usr/bin/X11:/usr/ucb:/usr/man\  
:/usr/java/bin:/usr/java/lib:/usr/local/man
```

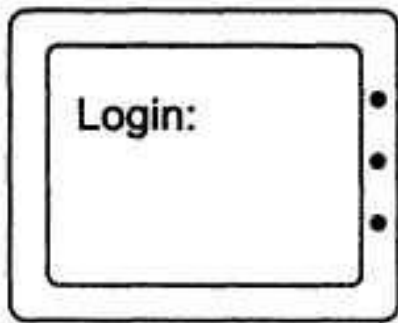
```
prog
```

```
cd/usr/anton
```

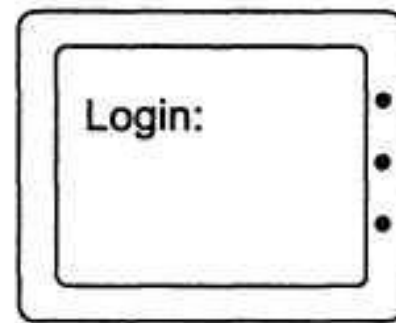
```
ls -l
```

## **5.2 ФАЛЬШИВАЯ ПРОГРАММА РЕГИСТРАЦИИ**

Настоящий экран регистрации  
(а);  
фальшивый экран регистрации  
(б)



а



б

## **5.3 ЛОГИЧЕСКИЕ БОМБЫ**

## **5.4 ПОТАЙНЫЕ ДВЕРИ**



## Нормальная программа (а)

```
while (TRUE) {  
    printf("login: ");  
    get_string(name);  
    disable_echoing( );  
    printf("password: ");  
    get_string(password);  
    enable_echoing( );  
    v = check_validity(name, password);  
    if (v) break;  
}  
execute shell(name);
```

## Программа с установленной потайной дверью (б)

```
while (TRUE) {  
    printf("login: ");  
    get_string(name);  
    disable_echoing( );  
    printf("password: ");  
    get_string(password);  
    enable_echoing( );  
    v = check_validity(name, password);  
    if (v || strcmp(name, "zzzzz") == 0) break;  
}  
execute shell(name);
```

## **5.5 ПЕРЕПОЛНЕНИЕ БУФЕРА**

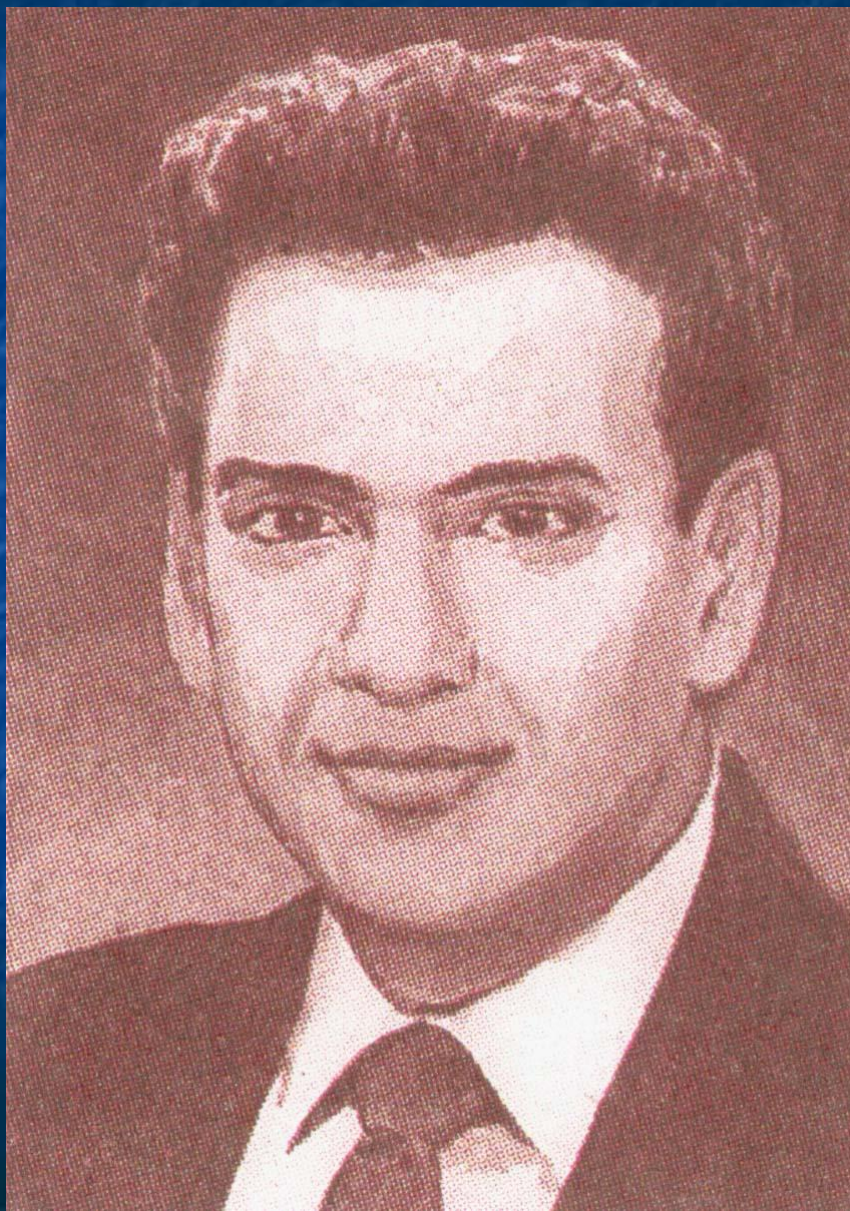
```
int i;  
char c[1024];  
i = 12000;  
c[i] = 0;
```

# Атака с использованием переполнения буфера



## **5.6 ТЕСТОВОЕ ПРОНИКНОВЕНИЕ**

# Айрэ Винклер



## **Пять видов атак, применённых Винклером:**

- **поиск по открытым источникам;**
- **маскарад;**
- **превышение прав доступа;**
- **хакерство штатного сотрудника;**
- **внутренняя координация действий  
внешних сообщников.**

## **5.6.1 Поиск по открытым источникам**



## **5.6.2 Маскарад**

## **5.6.3 Превышение прав доступа**

## **5.6.4 Хакерство штатного сотрудника**

## **5.6.5 Внутренняя координация действий внешних сообщников**

# **5.7 ПРОВЕРКА НАДЕЖНОСТИ СИСТЕМЫ БЕЗОПАСНОСТИ**

# **5.8 ПЕЧАЛЬНО ЗНАМЕНИТЫЕ ДЕФЕКТЫ СИСТЕМЫ БЕЗОПАСНОСТИ**

# **5.8.1 Знаменитые дефекты системы безопасности UNIX**

lpr

core

mkdir foo

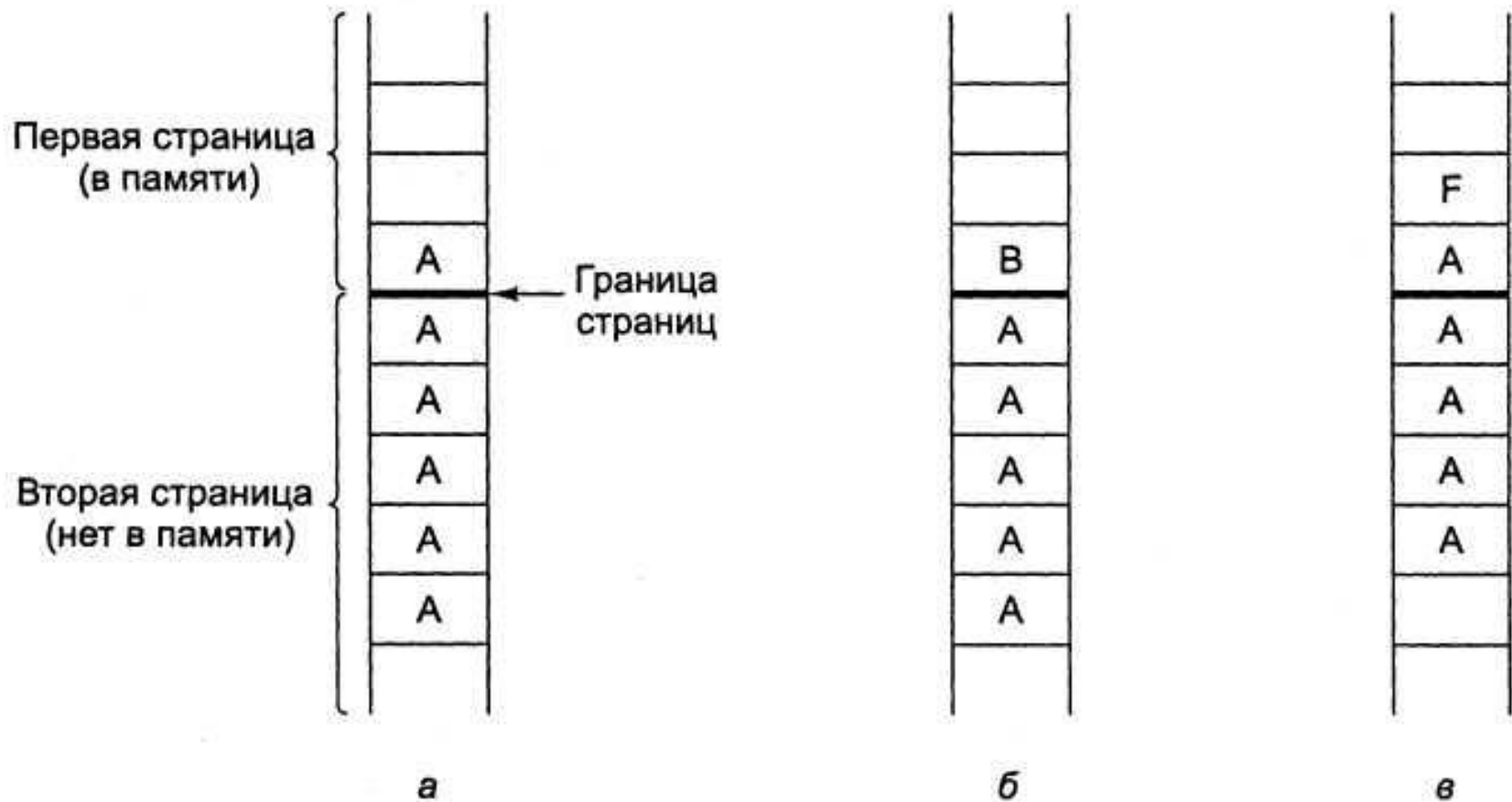
mkdir

chown



## **5.8.2 Знаменитые дефекты системы безопасности TENEX**

# Взлом пароля в системе TENEX



# **5.8.3 Знаменитые дефекты системы безопасности OS/360**

# **5.8.4 Дефекты системы безопасности Linux**

# **5.8.5 Дефекты системы безопасности Windows**

## **5.8.6 Самые безопасные ОС**

# **5.9 ПРИНЦИПЫ ПРОЕКТИРОВАНИЯ СИСТЕМ БЕЗОПАСНОСТИ**