

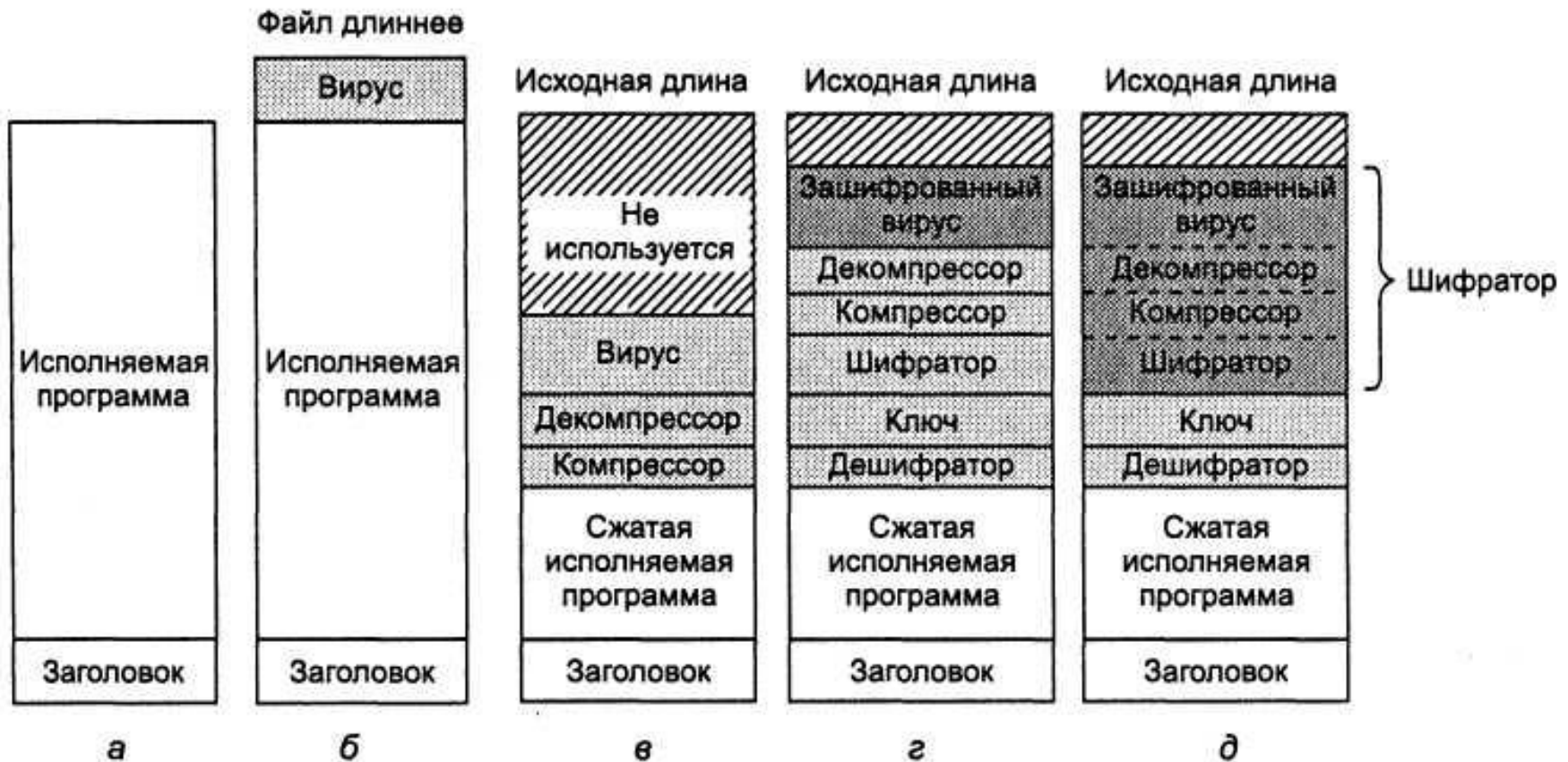
# 6. АТАКИ СИСТЕМЫ СНАРУЖИ

## **6.2 АНТИВИРУСНЫЕ ПРОГРАММЫ И АНТИ-АНТИВИРУСНЫЕ ТЕХНОЛОГИИ**

## **6.2.1 Где прячутся вирусы**

## **6.2.2 Сканеры вирусов**

Программа (а); инфицированная программа (б);  
 сжатая инфицированная программа (в); зашифрованный вирус (г);  
 сжатый вирус с зашифрованной программой компрессии (д)





# Примеры полиморфного вируса

MOV A.R1	MOV A.R1	MOV A.R1	MOV A.R1	MOV A.R1
ADD B.R1	NOP	ADD #0.R1	OR R1.R1	TST RI
ADD C.R1	ADD B.R1	ADD B.R1	ADD B.R1	ADD C.R1
SUB #4.R1	NOP	OR R1.R1	MOV R1.R5	MOV R1.R5
MOV RI.X	ADD C.R1	ADD C.R1	ADD C.R1	ADD B.R1
NOP	SHL#0,R1	SHL R1.0	CMP R2.R5	
SUB #4,R1	SUB #4.R1	SUB #4,R1	SUB #4.R1	
NOP	JMP .+1	ADD R5.R5	JMP .+1	
MOV RI.X	MOV RI.X	MOV RI.X	MOV RI.X	
	MOV R5.Y	MOV R5.Y		

*a*

*б*

*в*

*г*

*д*

## **6.2.3 Проверка целостности**

## **6.2.4 Проверка поведения**



## **6.2.5 Предохранение от вирусов**

## **6.2.6 Восстановление после вирусной атаки**

## **6.3 ИНТЕРНЕТ-ЧЕРВИ**

**Черви – это вирусы, которые  
размножаются сами, а не присоединяют  
свой код к чужой программе**



# Роберт Таппан Моррис

