Защита памяти

Введение

1. Защита памяти по граничным адресам
2. Защита памяти с помощью ключей
3. Защита с помощью уровней привилегий *(Itanium)*

Знать: состав и взаимодействие необходимых аппаратных и программных средств для каждого способа защиты памяти, их достоинства и недостатки.

Защита памяти

- **Уметь:** построить аппаратурную поддержку для заданного способа защиты памяти.
- **Помнить:** процессор прекращает выполнение текущей команды, откладывая операцию с памятью при возникновении запроса на прерывание по защите памяти.
- ***Литература:***
- Цилькер Б.Я., Орлов С.А. Организация ЭВМ и систем. Учебник для вузов. – СПб.: Питер, 2004. – 668 с. (с. 269-271).

Введение

- При мультипрограммном режиме работы ЭВМ в памяти одновременно находится несколько программ. Для исключения негативного взаимного влияния программ предусматриваются специальные меры.
- В простейшем случае каждая программа может иметь собственное изолированное адресное пространство, что исключит ее взаимодействие с другими программами.
- Однако особенности организации вычислительных процессов в ЭВМ требуют определенных контролируемых взаимодействий между программами. Например, взаимодействие программ пользователей и программ операционной системы.

Полномочия и защищенность программ

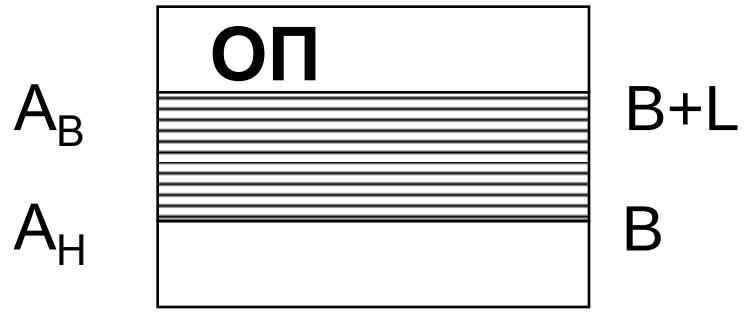
Полномочия P1 по отношению к другим программам

Чт	Зп	Вып
0	0	0
0	0	1
0	1	0
0	1	1
1	0	0
1	0	1
1	1	0
1	1	1

Защищенность программы P2 от других программ

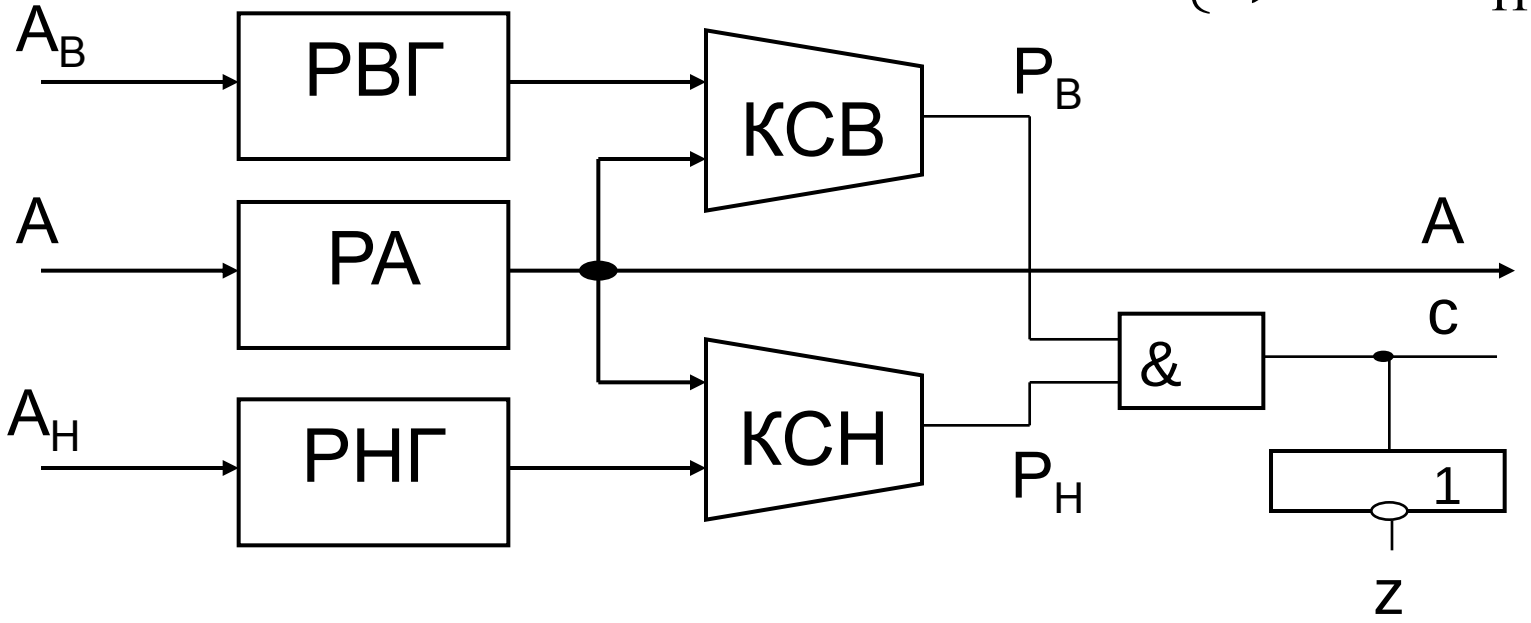
Чт	Зп	Вып
0	0	0
0	0	1
0	1	0
0	1	1
1	0	0
1	0	1
1	1	0
1	1	1

1. Защита памяти по граничным адресам



$$P_В = \begin{cases} 1, & A < A_В, \\ 0, & A \geq A_В. \end{cases}$$

$$P_Н = \begin{cases} 1, & A \geq A_Н, \\ 0, & A < A_Н. \end{cases}$$



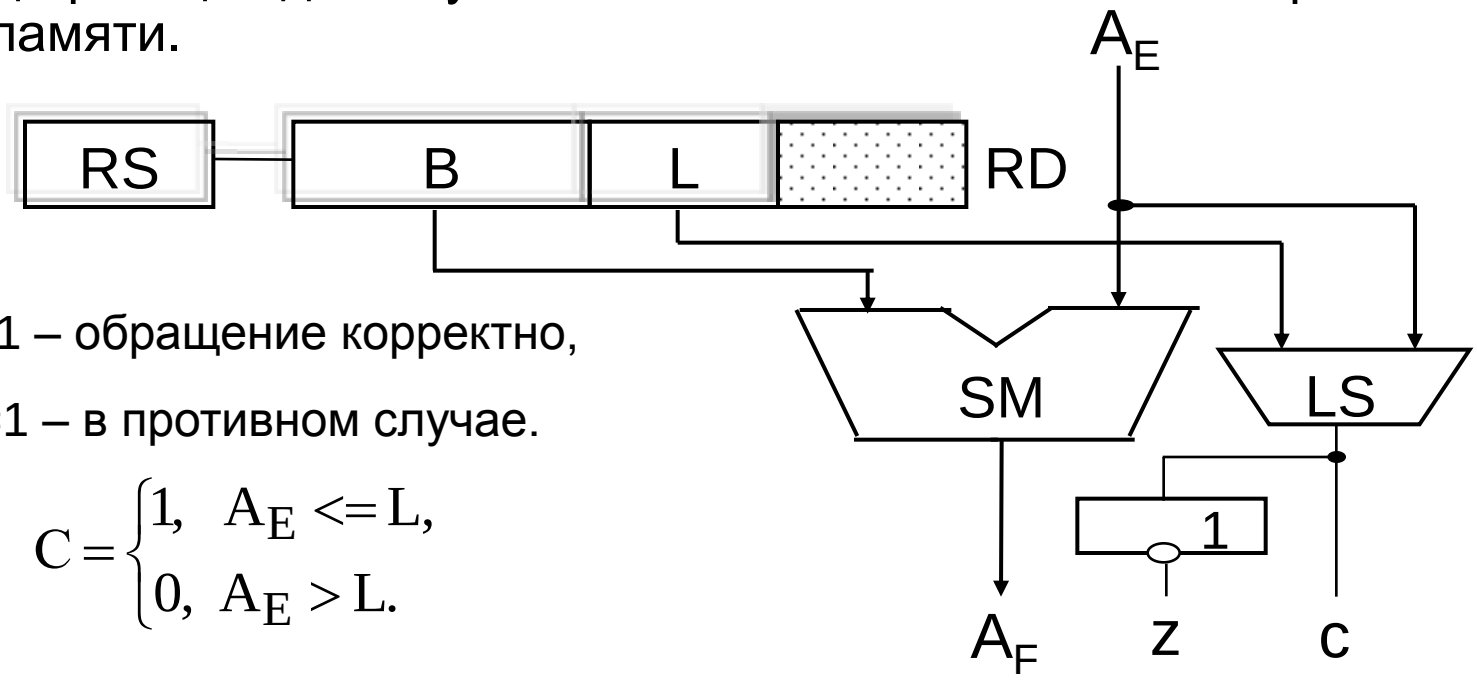
Оценка и модификация способа защиты памяти по граничным адресам

Достоинства:

- простота аппаратной поддержки,
- малое время проверки корректности адреса.

Недостаток: необходимость хранения программы в связной области памяти.

Модификация для случая использования сегментной организации памяти.



C=1 – обращение корректно,

Z =1 – в противном случае.

$$C = \begin{cases} 1, & A_E <= L, \\ 0, & A_E > L. \end{cases}$$

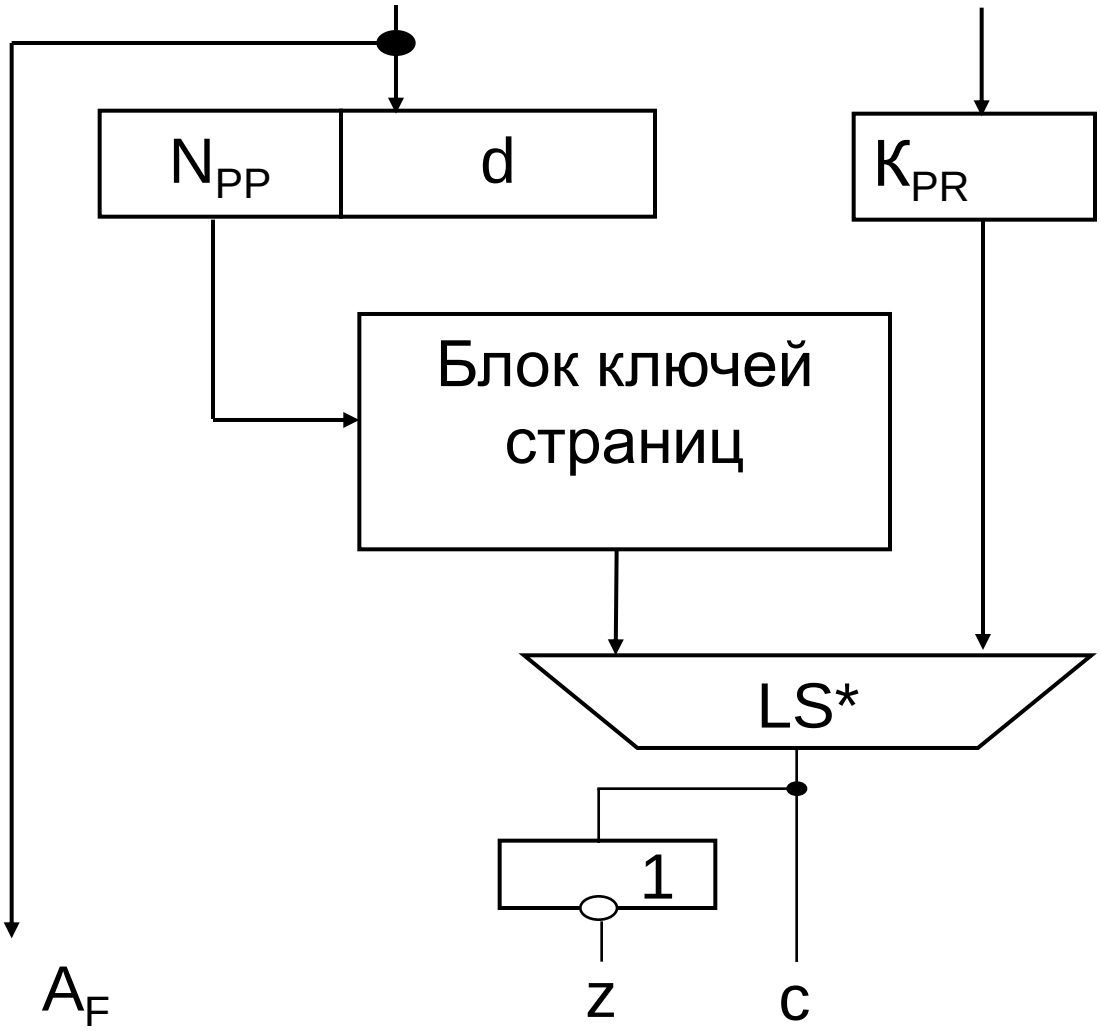
2. Защита памяти с помощью ключей

- Предполагается использование страничной организации памяти. Выделяется два множества: страниц и программ.
- Каждой программе присваивается уникальный код, называемый ключом программы.
- Каждая страница также имеет свой ключ.
- При этом в процессе выделения программе памяти назначаемым ей страницам задается ключ, совпадающий с ключом программы.
- Особую роль имеют ключи с нулевым кодом. Нулевой ключ считается совпадающим с любым другим ключом. Поэтому если программа имеет нулевой ключ, то ей доступны все страницы. А страница с нулевым ключом доступна всем программам.

Сравнение ключей программ и страниц

- При каждом обращении к памяти ключ текущей программы сравнивается с ключом страницы, к которой идет обращение.
- При совпадении ключей обращение считается корректным, в противном случае вырабатывается сигнал запроса на прерывание по защите памяти.
- Защиту памяти с помощью ключей иллюстрирует схема, где NPP – номер физической страницы; d – адрес объекта на странице; KPR – ключ текущей программы; LS* – логическая схема определения равенства ключей с учетом нулевых кодов.

Схема защиты памяти с помощью ключей



3. Защита с помощью уровней привилегий

- Четыре уровня привилегий с номерами 0…3 обеспечивают управление доступом к привилегированным командам, системным регистрам и системным областям памяти.
- Непривилегированные команды и регистры приложений могут быть доступны на любом уровне.
- Системные инструкции и регистры доступны только на уровне привилегий 0.

Механизм защиты памяти на основе привилегий

- Процессор содержит код текущего уровня привилегий (CPL) в специальном поле (cpl) регистра слова состояния процессора (PSR) (64 разряда).
- CPL может быть модифицирован только операционной системой.
- Механизм защиты виртуальной памяти, управляющий доступом к памяти основан на сопоставлении текущего уровня привилегий (CPL) и уровня привилегий (PL) страницы, к которой идет обращение.
- Пример управления доступом к страницам с использованием полей характеризующих страницу: AR – прав доступа, уровня привилегий страницы (PL) в зависимости от текущего уровня привилегий (CPL) показан в таблице.

Управление доступом к страницам

AR	PL	CPL			
		3	2	1	0
0	3	R	R	R	R
	2	–	R	R	R
	1	–	–	R	R
	0	–	–	–	R
1	3	RX	RX	RX	RX
	2	–	RX	RX	RX
	1	–	–	RX	RX
	0	–	–	–	RX
2	3	RW	RW	RW	RW
	2	–	RW	RW	RW
	1	–	–	RW	RW
	0	–	–	–	RW
3	3	RWX	RWX	RWX	RWX
	2	–	RWX	RWX	RWX
	1	–	–	RWX	RWX
	0	–	–	–	RWX
4	3	R	RW	RW	RW
	2	–	R	RW	RW
	1	–	–	R	RW
	0	–	–	–	RW

AR	PL	CPL			
		3	2	1	0
5	3	RX	RX	RX	RWX
	2	–	RX	RX	RWX
	1	–	`–	RX	RWX
	0	–	–	–	RWX
6	3	RWX	RW	RW	RW
	2	–	RWX	RX	RW
	1	–	–	RWX	RW
	0	–	–	–	RW
7	3	X	X	X	RX
	2	XP2	X	X	RX
	1	XP1	XP1	X	RX
	0	XP0	XP0	XP0	RX

R – разрешено чтение, W – запись, а X – исполнение (код в странице рассматривается как программа); Pn,– установка нового текущего уровня привилегий (CPL) в PSR (при выполнении привилегированных команд n=0…3, а при выполнении команд пользователя n=3 только).