УДК 681.3

МОДЕЛИРОВАНИЕ ПРОЦЕССА ОБРАБОТКИ АППАРАТНЫХ ПРЕРЫВАНИЙ В МИКРОКОНТРОЛЛЕРНЫХ СИСТЕМАХ

Виктор Куценко, Тарас Левченко

Научно-технический комплекс "Импульс", г. Киев

Аннотация: **Предложен теоретико-численный подход к моделированию процесса обработки аппаратных прерываний в микроконтроллерных системах, используемых в системах информационной безопасности. По результатам моделирования даны рекомендации по оптимизации загрузки многозадачных микроконтроллерных систем.**

Summary: **There is offered theoretic and numerical approach to simulation of process of hardware interrupts processing i n microcontroller systems. By results of simulation the guidelines on optimization of a loading multitask microcontroller systems are given.**

Ключевые слова: **Информационная безопасность, технические средства защиты информации, несанкционированный доступ, микроконтроллерная система, микроконтроллер, аппаратные прерывания, моделирование, математическое ожидание, дисперсия, автокорреляционная функция.**

I Введение

В технических средствах защиты информации, используемых в системах информационной безопасности, широко применяются микроконтроллерные системы (МКС).

Под МКС понимают микроконтроллер (МК) с соответствующим аппаратным и программным обеспечением, предназначенный для приема информационных сигналов от внешних устройств (ВУ) и выдачи управляющих сигналов на исполнительные устройства [1, 2].

Во время выполнения МКС текущей программы внутри МК и в связанной с МКС внешней среде (например, в системе информационной безопасности, управляемой МКС) могут возникать события, требующие немедленной реакции на них со стороны МК.

Реакция состоит в том, что МК прерывает обработку текущей программы и переходит к выполнению некоторой другой программы, специально предназначенной для данного события. По завершении этой программы МК возвращается к выполнению прерванной программы. Рассматриваемый процесс называется *прерыванием программ*. Принципиально важным является то, что моменты возникновения событий, требующих прерывания программ, заранее неизвестны и поэтому не могут быть учтены при программировании.

Каждое событие, требующее прерывания, сопровождается сигналом, оповещающим МК – *запросом прерывания*. Программу, затребованную запросом прерывания, назовем *прерывающей подпрограммой*, противопоставляя ее *основной программе*, выполнявшейся МК до появления запроса [3, 4]. Процесс выполнения прерывающей подпрограммы назовем *обработкой прерывания.*

Запросы на прерывания могут возникать внутри самой МКС и в ее внешней среде. *Внутренние аппаратные прерывания* возникают, например, при возникновении в МК таких событий, как появление ошибки в работе, переполнение разрядной сетки, попытка деления на ноль, выход из установленной для данной программы области памяти, затребование ВУ для операции ввода-вывода, завершение операции ввода–вывода или возникновение при этой операции особой ситуации и др. Хотя, некоторые из указанных событий порождаются самой программой, моменты их появления, как правило, невозможно предусмотреть. *Внешние аппаратные прерывания* инициируются контроллерами периферийного оборудования или сопроцессорами от аварийных и некоторых других датчиков несанкционированного доступа, портов ввода–вывода, клавиатуры, таймеров и т. п.

Возможность прерывания программ – важное архитектурное свойство МК, позволяющее эффективно использовать производительность МК при наличии нескольких протекающих параллельно во времени процессов, требующих в произвольные моменты времени управления и обслуживания со стороны МК. В первую очередь это относится к организации многозадачных МКС с параллельной во времени работой МК и ВУ, а также к использованию МКС для управления в реальном времени системой информационной безопасности.

Простейшая схема обработки прерывания выглядит следующим образом:

- прием запроса на прерывание;
- сохранение состояния текущего процесса;
- выполнение инструкций по обработке прерывания; т. е. прерывающей программы;
- восстановление состояния процесса и возврат к выполнению основной программы.

II Постановка задачи

Запросы нескольких прерываний могут происходить в моменты времени, определяемые ВУ, и обрабатываться в промежутках времени, определяемых готовностью МК. В зависимости от характеристик ВУ запросы прерываний возникают периодически и случайно. Готовность МК определяется по его состоянию после выполнения предыдущих операций.

Общее время обработки всех аппаратных прерываний определяется временами выполнения прерывающих подпрограмм и не должно превышать характерного времени работы основной программы МК.

При одновременном получении запросов прерывания от нескольких ВУ в зависимости от типа и способа настройки МК обработка прерываний может происходить двояко. Если в МК разрешено вложение прерываний, то их обработка происходит поочередно в зависимости от заданного приоритета, при этом обработка прерывания с низшим приоритетом приостанавливается до завершения обработки прерывания с более высоким приоритетом. Если МК обладает одноуровневой обработкой прерываний, то обработка последующих прерываний в соответствии с их приоритетом начинается после завершения обработки предыдущего прерывания. Нетрудно убедиться, что количество уровней обработки прерываний влияет только на последовательность обработки прерываний и не влияет на интегральные временные характеристики процесса.

Такой подход позволяет рассматривать процесс прерывания (состояние 0) выполнения основной программы (состояние 1) МК как случайный процесс ψ, зависящий от входных k_c случайных и k_n периодических сигналов, готовности МК, определяемой предыдущим состоянием МК, и времени обработки прерываний.

Задача оптимизации процесса ψ с целью рационального использования системных ресурсов МКС является актуальной. Для подробного изучения статистических характеристик результирующего случайного процесса ψ рассмотрим статистические характеристики его составляющих.

III Процесс обработки случайно возникающего прерывания

Примем, что время появления в МКС запроса случайного прерывания, например, прерывания по нажатию клавиатуры, определяется некоторым числом взаимно независимых случайных событий. В таком приближении можно считать процесс появления запроса случайного прерывания пуассоновским процессом со средней плотностью числа событий α_c и плотностью распределения интервалов времени t между последовательным появлением событий

$$\varphi(t) = \alpha_c e^{-\alpha_c t}. \tag{1}$$

Предположим, что МК начинает выполнять прерывающую подпрограмму без запаздывания и заканчивает через N_i машинных циклов продолжительностью τ секунд. Тогда общее время обработки полученных за время T прерываний

$$t = \sum_i N_i \tau = \alpha_c T N_{cp} \tau, \tag{2}$$

где $N_{cp}\tau$ – среднее время обработки прерывания, математическое ожидание времени обработки прерываний

$$M\psi = t/T = \alpha_c N_{cp} \tau = \phi(0), \tag{3}$$

и, соответственно, математическое ожидание времени выполнения МК основной программы

$$\phi(1) = 1 - M\psi. \tag{4}$$

Очевидно, что соотношения (3) и (4) определяют дискретную плотность распределения ϕ случайного процесса ψ.

Момент второго порядка

$$M\psi^2 = 1*\phi(1) + 0*\phi(0) = \alpha_c N_{cp} \tau, \tag{5}$$

и, соответственно, дисперсия

$$D\psi = M\psi^2 - (M\psi)^2 = \alpha_c \tau N_{cp}(1 - N_{cp}\tau). \tag{6}$$

Автокорреляционная функция (АКФ), определяемая как

$$K(\xi) = M(\psi(t)\psi(t+\xi)), \tag{7}$$

может быть выражена в следующем виде [5]:

$$K(\xi) = (M\psi)^2 \qquad \forall\, |\xi| > N_{cp}\tau,$$
$$K(\xi) = D\psi\left(1 - |\xi| / (N_{cp}\tau)\right) + (M\psi)^2 \qquad \forall\, |\xi| \le N_{cp}\tau. \tag{8}$$

IV Процесс обработки периодически возникающего прерывания

Учитывая то, что при расчете временных характеристик процесса обработки периодически возникающего прерывания, например, от таймера, нас не интересуют фазовые соотношения, а также возможные различия во времени обработки последовательных прерываний, квантованность временных интервалов работы МК и, как следствие, возникающую апериодичность обработки будем считать рассматриваемый процесс частным случаем процесса обработки случайно возникающего прерывания ψ с плотностью распределения α_n.

При таком подходе функция (1) становится дискретной и равной

$$\varphi(t) = 1 \quad \forall t \approx 1/\alpha_n,$$
$$\varphi(t) = 0 \quad \textit{в остальных случаях.} \tag{9}$$

Выражения (3)–(7) остаются справедливыми при замене α_c на α_n. Однако АКФ становится периодичной:

$$K(\xi) = (M\psi)^2 \qquad \forall\, |\xi| > N_{cp}\tau + nT_0,$$
$$K(\xi) = D\psi\left(1 - |\xi| / (N_{cp}\tau)\right) + (M\psi)^2 \qquad \forall\, |\xi| \le N_{cp}\tau + nT_0,. \tag{10}$$

где $T_0 = 1/\alpha_n$ средний период между началом обработки последовательных прерываний.

V Численное моделирование процесса обработки прерываний

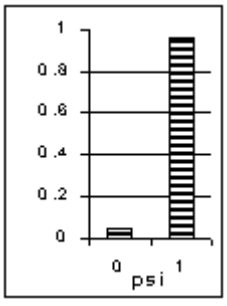
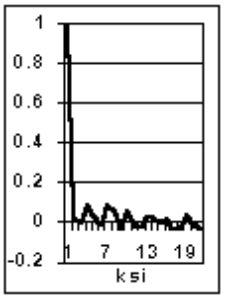
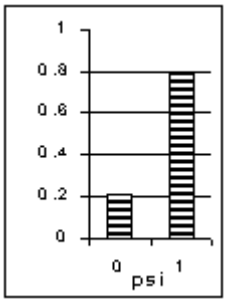
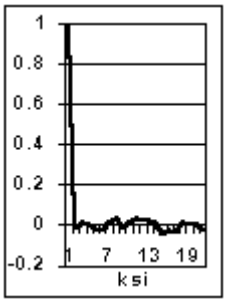
Полученные выше теоретические результаты являются фундаментом для получения временных статистических характеристик процесса обработки нескольких прерываний в МКС. Однако из-за наличия вложенности прерываний указанный процесс оказывается неаддитивным и, следовательно, его статистические характеристики многомерны. Сложность обобщенного описания теоретической модели требует применения численного моделирования.

Для численного моделирования на ЭВМ процесса возникновения прерываний в дискретные моменты времени применим двумерный массив INTRPTS[*k, L*], где $L = T/\tau$ – число подлежащих учету дискретных моментов времени, k – общее число прерываний. В каждом столбце массива INTRPTS[*k, L*] через 0 обозначим отсутствие запроса прерывания в данный момент времени, через 1 – наличие запроса прерывания. Зная состояние каждой строки массива INTRPTS[*k, L*] и время обработки каждого прерывания, можно построить массив PROCINT[*L*], каждый элемент которого фиксирует состояние процессора (1 – выполнение основной программы, 0 – состояние обработки прерывания) в каждый момент времени, т. е. является реализацией процесса ψ.

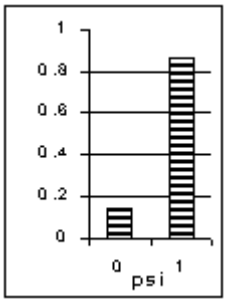
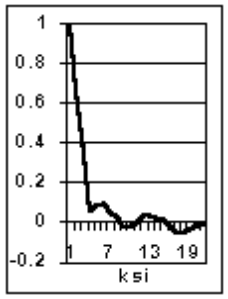
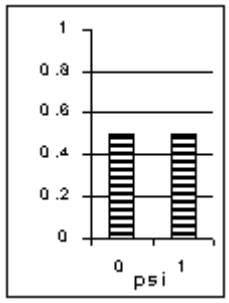
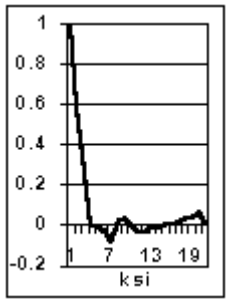
Принятые допущения позволяют считать процесс ψ стационарным и эргодическим. Поэтому для анализа его статистических характеристик ограничимся набором из 10 временных реализаций продолжительностью 10000 машинных тактов каждая.

В табл. 1 – 4 приведены результаты численных расчетов дискретной плотности распределения $\phi(\psi)$ и автокорреляционных функций $K(\xi)$ процесса обработки прерывания. Масштаб по оси ξ уменьшен в 10 раз.

Таблица 1 – Процесс обработки одного случайного прерывания

N_{cp}	α_c =0.05		α_c =0.20	
	$\phi(\psi)$	$K(\xi)$	$\phi(\psi)$	$K(\xi)$
10				

Продолжение таблицы 1

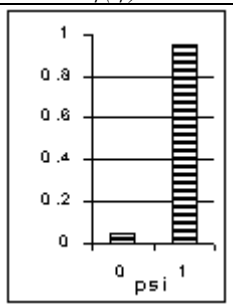
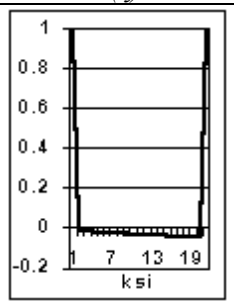
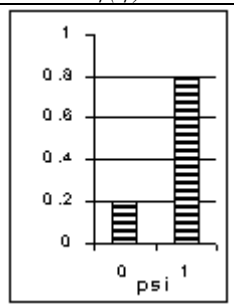
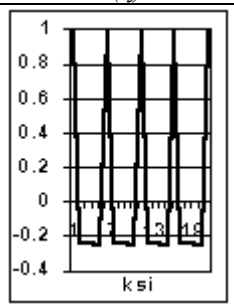
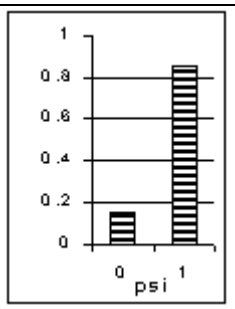
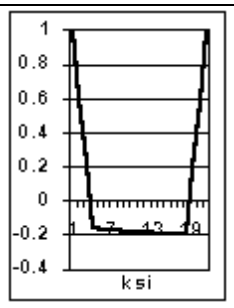
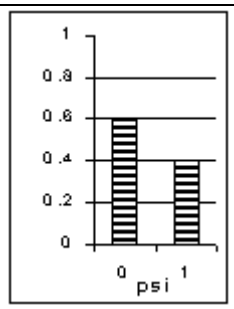
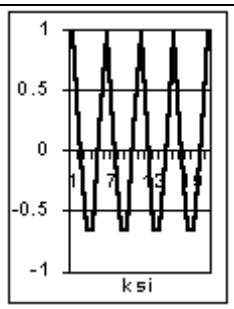
30				

Анализируя результаты, приведенные в табл. 1, отметим следующее.

1. По мере увеличения плотности числа прерываний АКФ процесса обработки прерывания практически не изменяется и хорошо аппроксимируется формулой (8). Корреляционное расстояние процесса при использованных допущениях определяется исключительно средним временем обработки прерывания.

2. При постоянной плотности числа прерываний по мере увеличения времени обработки прерывания относительное время занятости процессора выполнением основной программы $\phi(1)$, определяемое выражением (4), уменьшается. Из-за статистических флуктуаций процесса возникновения прерываний (1) при $N_{\text{ср}}=1/\alpha_{\text{с}}$ МК сможет выполнять основную программу.

Таблица 2 – Процесс обработки одного периодического прерывания

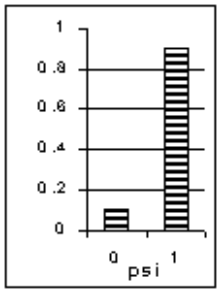
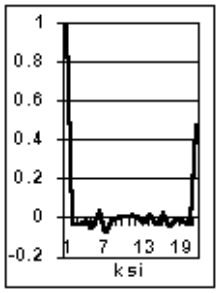
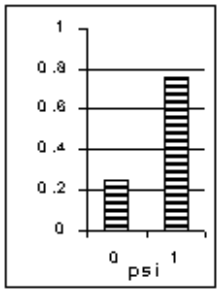
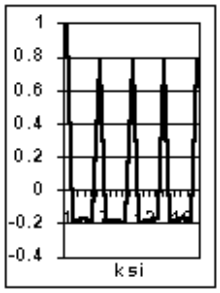
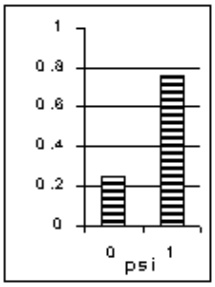
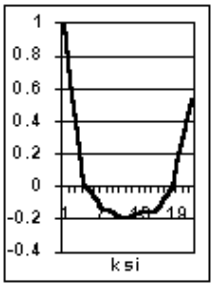
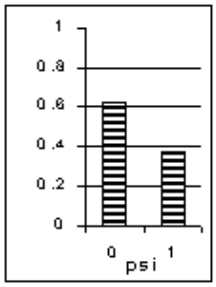
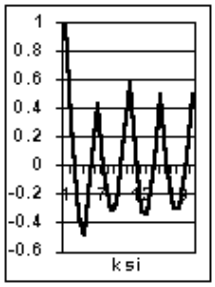
N_{cp}	α_n =0.05		α_n =0.20	
	$\phi(\psi)$	$K(\xi)$	$\phi(\psi)$	$K(\xi)$
10				
30				

Результаты, приведенные в табл. 2, позволяют отметить следующее.

1. АКФ процесса обработки прерывания периодична с периодом $1/\alpha_{\text{п}}$ и имеет значения локальных экстремумов, совпадающие со значением $K(0)$. По мере увеличения плотности числа прерываний период АКФ уменьшается. АКФ хорошо аппроксимируется формулой (10). Корреляционное расстояние процесса при использованных допущениях определяется исключительно средним временем обработки прерывания.

2. При постоянной плотности числа прерываний по мере увеличения времени обработки прерывания относительное время занятости МК выполнением основной программы $\phi(1)$, определяемое выражением (4), уменьшается. При $N_{cp}=1/\alpha_{\text{п}}$ МК вообще не сможет выполнять основную программу.

Таблица 3 – Процесс обработки одного случайного (плотность α_c=0.05) и одного периодического прерываний

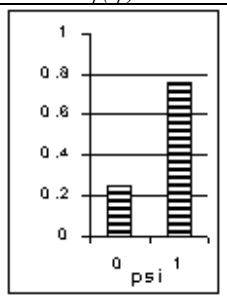
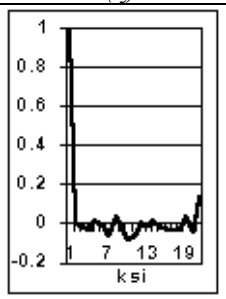
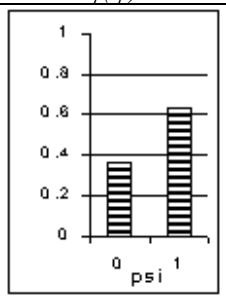
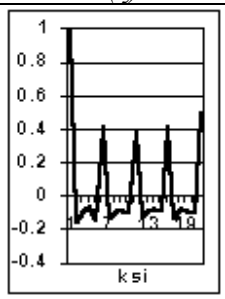
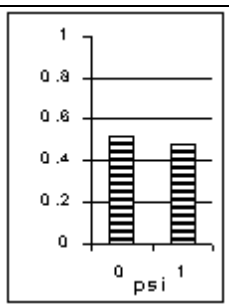
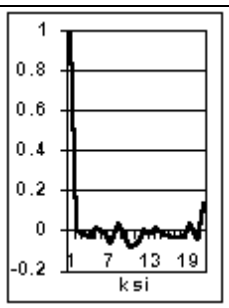
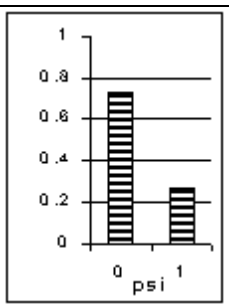
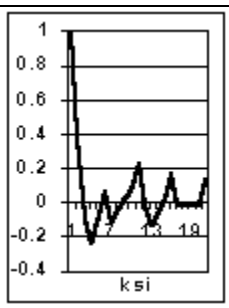
$N_{ср}$	α_n=0.05		α_n=0.20	
	$\phi(\psi)$	$K(\xi)$	$\phi(\psi)$	$K(\xi)$
10				
30				

Результаты, приведенные в табл. 3, позволяют отметить следующее.

1. АКФ процесса обработки прерывания периодична с периодом $1/\alpha_n$. Значения локальных экстремумов оказываются меньше, чем *K(0).* По мере увеличения плотности числа периодических прерываний период АКФ уменьшается. Среднее корреляционное расстояние процесса при использованных допущениях определяется исключительно средним временем обработки прерывания.

2. При постоянной плотности числа прерываний по мере увеличения времени обработки прерывания относительное время занятости МК выполнением основной программы $\phi(1)$, определяемое выражением (4), уменьшается. При $N_{ср}=1/(\alpha_n \alpha_c)$ МК сможет выполнять основную программу.

Таблица 4 – Процесс обработки одного случайного (плотность α_c=0.20) и одного периодического прерываний

$N_{ср}$	α_n=0.05		α_n=0.20	
	$\phi(\psi)$	$K(\xi)$	$\phi(\psi)$	$K(\xi)$
1				
3				

Результаты, приведенные в табл. 4, позволяют отметить следующее.

1. По мере увеличения плотности случайного прерывания АКФ процесса обработки прерывания периодична с периодом $1/\alpha_п$, хотя значения локальных экстремумов оказываются значительно меньше, чем *K(0)*. По мере увеличения плотности числа периодических прерываний период АКФ уменьшается.

2. При постоянной плотности числа прерываний по мере увеличения времени обработки прерывания относительное время занятости МК выполнением основной программы $\phi(1)$, определяемое выражением (4), уменьшается. В случае $N_{ср}=1/(\alpha_п \alpha_с)$ МК не сможет выполнять основную программу.

VI Выводы

1. Предложен теоретико-числовой подход к моделированию процесса обработки аппаратных прерываний в микроконтроллерных системах, позволивший получить значения указанного процесса в каждый момент времени.

2. Результаты анализа показали, что процесс обработки аппаратных прерываний является стационарным и эргодичным. Вследствие этого он описывается дискретной функцией распределения, которая зависит от плотности появления прерываний и среднего времени обработки прерывания. Значения дискретной функции распределения $\phi(1)$ и $\phi(0)$ являются фактически описанием относительного времени выполнения МК основной программы и обработки прерывания.

3. АКФ процесса обработки прерываний при отсутствии периодических прерываний определяется исключительно средним временем обработки прерывания.

4. АКФ и дискретная функция распределения процесса обработки прерываний оказываются взаимно зависимыми.

5. При наличии периодических прерываний АКФ процесса также является периодической.

6. Совокупное воздействие случайных и периодических прерываний уменьшает время выполнения МК основной программы и может привести к полному прекращению обработки основной программы. При этом случайная составляющая в АКФ оказывается доминирующей.

7. Для того, чтобы МКС могла выполнять основную программу, необходимо выполнение соотношения

$$\phi(1) \le 0{,}5$$

Литература: 1. Каган Б. М. Электронные вычислительные машины и системы: Учеб. пособие для вузов./ 3-е изд., перераб. и доп. // М.: Энергоатомиздат. – 1991. – 592 с. 2. Фрир Дж. Построение вычислительных систем на базе перспективных микропроцессоров: Пер. с англ. // М.: Мир. – 1990. – 413 с. 3. Гивоне Д., Россер Р. Микропроцессоры и микрокомпьютеры. //М.: – Мир. – 1983. – 463 с. 4. Бродин В. Б., Шагурин И. И. Микроконтроллеры. Архитектура, программирование, интерфейс. //М.: Экон. – 1999. – 400 с. 5. Справочник по математике (для научных работников и инженеров) Г. Корн, Т. Корн – Изд. 4. – М.: Наука, 1978. – 831 с.

УДК 638.235.231

СЕРТИФИКАЦИЯ СЛОЖНЫХ ЭЛЕКТРОННЫХ СИСТЕМ С ИСПОЛЬЗОВАНИЕМ ФУНКЦИОНАЛЬНОЙ МОДЕЛИ ОБЪЕКТА НА ПОЛНОМ НАБОРЕ ВХОДНЫХ СЛОВ

Валерий Горбачев, Владимир Степаненко, Сергей Саранча
Харьковский национальный университет радиоэлектроники

Анотація: **Розглядаються питання, пов'язані з розробкою методів та засобів сертифікації складних електронних систем на відповідність специфікованим функціям.**
Summary: **In the given work the questions connected with development of methods and means of certification of complex electronic systems for conformity to the specified functions are considered.**
Ключові слова: **Інформація, апаратні засоби, закладний пристрій, інформаційна безпека.**

В настоящее время во всем мире активно разрабатываются всевозможные программные средства защиты информации от несанкционированного доступа к ней и ее разрушения [1]. В то же время проблема поиска цифровых закладных устройств в вычислительной технике и любой цифровой технике вообще является практически не исследованной. Поскольку уровень аппаратных средств является самым низким уровнем доступа к информации, то контроль за доступом, осуществляемым при помощи аппаратных средств,