УДК: 681.327.8

МЕТОДИКА ОПТИМИЗАЦИИ СТРУКТУРЫ ПЕРСПЕКТИВНЫХ АППАРАТНЫХ СРЕДСТВ КРИПТОГРАФИЧЕСКОЙ ЗАЩИТЫ ИНФОРМАЦИИ В АВТОМАТИЗИРОВАННЫХ СИСТЕМАХ УПРАВЛЕНИЯ

Ф.Г.Хисамов, доктор технических наук, профессор
Краснодарский военный институт, 350035, г. Краснодар, ул. Красина, дом 4,
кафедра математики и физики, раб. тел. (8-8612) 68-14-56; факс: (8-8612) 68-37-80;
e-mail:pr-khisamov@yandex.ru; дом. тел.(8-8612) 24-80-58

В последнее время повысился интерес к перспективным аппаратным средствам криптографической защиты информации (АСКЗИ). Это обусловлено, прежде всего, простотой и оперативностью их внедрения. Для этого достаточно у абонентов на передающей и приемной сторонах иметь аппаратуру АСКЗИ и комплект ключевых документов, чтобы гарантировать конфиденциальность циркулирующей в автоматизированных системах управления (АСУ) информации.

Перспективная АСКЗИ строится на модульном принципе, что дает возможность комплектовать структуру АСКЗИ по выбору заказчика. При отсутствии опыта использования АСКЗИ, выбор структуры АСКЗИ осуществляется интуитивно или приобретается типовой набор модулей, который не всегда оказывается оптимальным, с точки зрения оперативности прохождения информации.

В данной работе на базе использования системного подхода и аппарата дифференциальных уравнений предлагается методика нахождения обобщенного критерия эффективности структуры перспективных АСКЗИ, используемых в АСУ различного назначения.

Введение. Широкая информатизация общества, внедрение компьютерной технологии в сферу управления привела к необходимости обеспечения безопасности информации, циркулирующей в автоматизированных системах управления (АСУ). Факты многочисленного вмешательства в работу государственных и коммерческих систем управления, как со злым умыслом, так и просто из «спортивного интереса» нанесли непоправимый ущерб владельцам информации.

Поэтому в настоящее время резко повысился спрос на перспективные аппаратные средства криптографической защиты информации (АСКЗИ). Они позволяют оперативно и достаточно просто закрыть конфиденциальную информацию, циркулирующую в АСУ, при наличии аппаратуры и комплекта ключевой документации.

Перспективные АСКЗИ состоят из функционально законченных модулей, из которых заказчик имеет возможность комплектовать структуру средств защиты информации. Как правило, из-за отсутствия опыта заказчик приобретает типовой комплект аппаратуры, который не всегда может обеспечить заданную эффективность функционирования АСУ.

Цель работы - используя системный подход и аппарат дифференциальных уравнений разработать методику нахождения обобщенного критерия эффективности структуры АСКЗИ для АСУ различного назначения.

Постановка задачи

При разработке перспективной АСКЗИ приходится учитывать большое количество факторов, влияющих на эффективность ее функционирования, что усложняет нахождение аналитических оценок по выбору обобщенного критерия оптимальности ее структуры.

К перспективным АСКЗИ, как элементу АСУ предъявляют повышенные требования по безопасности, надежности и быстродействию обработки циркулирующей в системе информации.

Безопасность обеспечивается гарантированной стойкостью шифрования и выполнением специальных требований, выбор которых обусловлен криптографическими стандартами, поэтому их можно считать заданными априори и опустить из рассмотрения.

Надежность и быстродействие обработки информации зависят от выбранной структуры АСКЗИ и, следовательно, поддаются оптимизации. Перспективная АСКЗИ включает в себя ряд функционально завершенных узлов и блоков, обеспечивающих заданную надежность и быстродействие. В зависимости от уровня управления соответствующий набор типовых блоков может быть расширен или продублирован, для обеспечения заданных количественных критериев надежности и быстродействия. К таким функционально законченным узлам и блокам необходимо отнести:

входные устройства, предназначенные для ввода информации в АСКЗИ;

устройства преобразования информации, предназначенные для передачи информации от входных устройств на устройства вывода в зашифрованном, расшифрованном или открытом виде;

устройства вывода, предназначенные для вывода информации на соответствующие носители (бумажный бланк, перфолента, дискета, дисплей и т.д.).

В общем виде перспективную АСКЗИ можно представить структурной схемой, изображенной на рис.1.

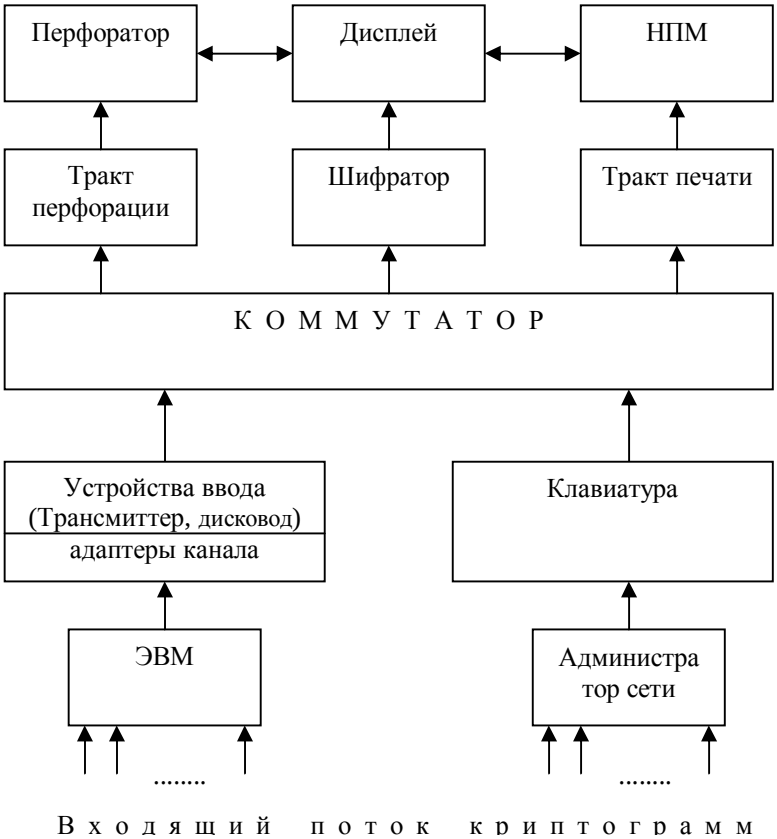

Рис. 1 Структурная схема перспективного аппаратного средства криптографической защиты информации

На АСКЗИ информация может поступать от оператора при вводе вручную или от компьютера. Как в первом, так и во втором случае алгоритм работы АСКЗИ будет одинаковым за исключением скорости обработки поступающей информации. Поступающая информация от устройств ввода подается на устройства преобразования, где в зависимости от выбранного режима, рода и способа работы поступает или сразу на устройства вывода или вначале в шифратор, где шифруется или расшифровывается, а затем на выходные устройства.

Таким образом, для нахождения обобщенного критерия оценки оптимальной структуры перспективной АСКЗИ достаточно рассмотреть основную цепь прохождения информации: адаптеры ввода, входные устройства, состоящие из клавиатуры, трансмиттера или фотосчитывателя, шифратор, устройства преобразования и устройства вывода. Остальные узлы и блоки не оказывают существенного влияния на прохождение информации и поэтому могут быть опущены из рассмотрения.

Математическое описание перспективного аппаратного средства криптографической защиты информации как сложной системы

Из методологии системного подхода известно [1], что математическое описание сложной системы осуществляется путем иерархического разбиения ее на элементарные составляющие для разработки пакета взаимосвязанных математических моделей составных частей. Математическая модель составной части находится относительно выбранного обобщенного критерия, который должен отражать целевое предназначения данного объекта и поэтому находится вне объекта. Частные критерии отражают эффективность выполнения той или иной задачи данным объектом и поэтому будут находиться внутри системы.

Таким образом, в математические модели вышестоящих уровней в качестве частных критериев всегда должны входить обобщенные критерии нижестоящих уровней. Тем самым, осуществляется взаимосвязь моделей функционирования составных частей сложной системы в рамках единой математичкой модели. То есть комплект математических моделей сложной системы должен строится таким образом, чтобы модели и критерии чередовались между собой: модель, критерий, модель, критерий, и т.д. Следовательно, одно и то же понятие может выступать по отношению к низшему

уровню в качестве обобщенного критерия (цели), а по отношению в высшему - в качестве частного критерия (задачи).

Исходя из методологии системного подхода разобьем перспективную АСКЗИ, как сложную систему, на три уровня иерархии, как показана на рис.2.

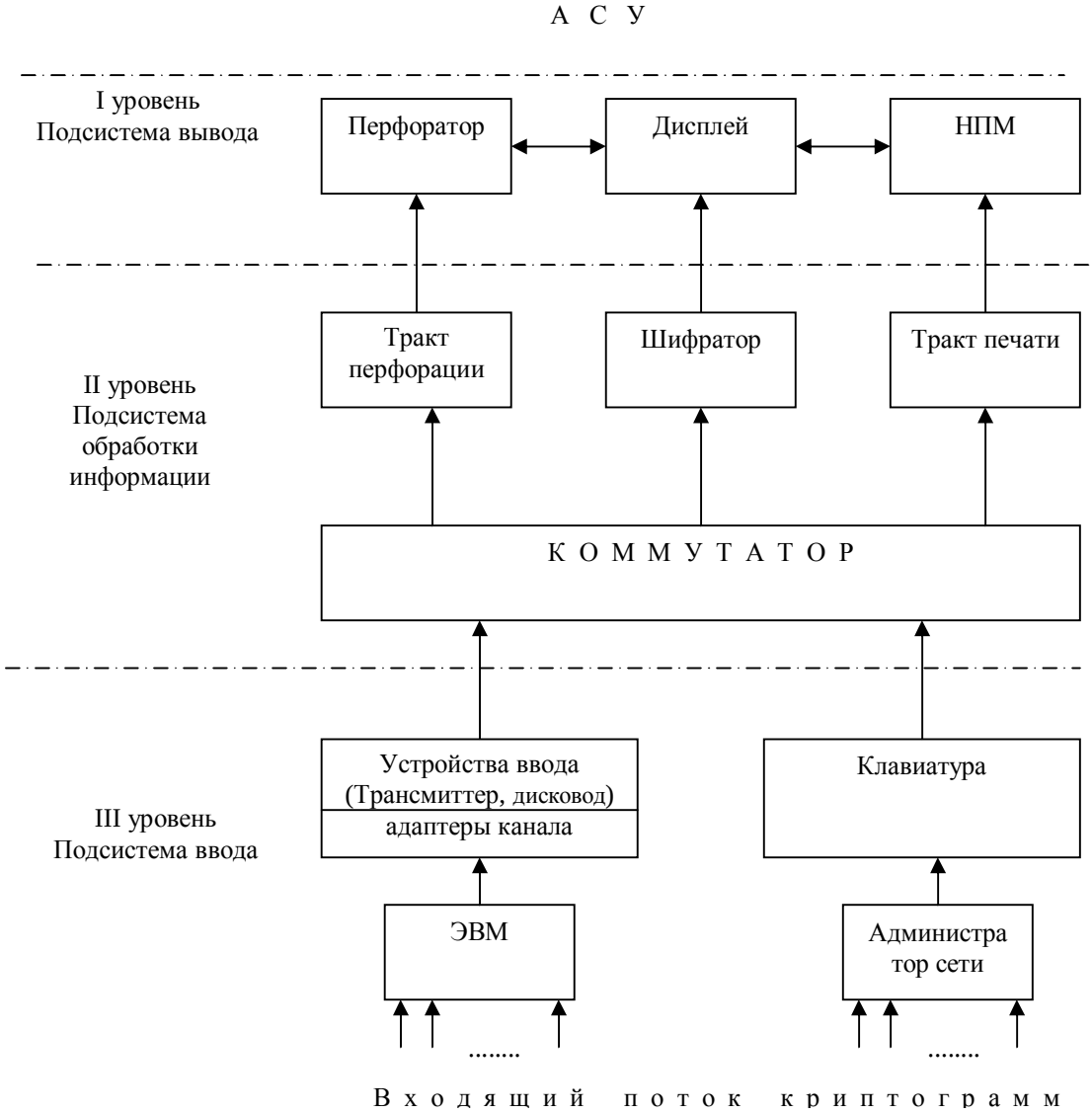

Рис. 1 Разбиение на три уровня иерархии перспективного аппаратного средства криптографической защиты информации

Это такие уровни как:

1. Подсистема вывода.
2. Подсистема обработки информации.
3. Подсистема ввода.

Подсистема вывода является оконечным устройством АСКЗИ, то есть находится на высшей ступени иерархии и включает в себя устройства отображения, печати и перфорации. Следовательно, на этом уровне в качестве целевой установки с точки зрения интересов системы управления будет выступать быстрота обработки входящих криптограмм.

Тогда в качестве обобщенного критерия целесообразно выбрать время обработки потока криптограмм за один цикл функционирования перспективной АСКЗИ не превышающего заданного интервала времени и обусловленного необходимостью принятия управленческих решений. Под циклом функционирования понимается время обработки одной криптограммы объемом не более 300 пятизначных групп.

Время обработки потока криптограмм хорошо приспособлено для использования в математической модели вышестоящего уровня, в качестве которого выступает АСУ. Следовательно, данный критерий согласно методологии системного подхода может выступать в качестве обобщенного критерия эффективности для перспективной АСКЗИ в целом.

Подсистема обработки информации находится на втором уровне иерархии и включает в себя тракты печати и перфорации, шифратор и систему управления и распределения потока информации (коммутатор). На этом уровне в качестве обобщенного критерия целесообразно выбрать пропускную способность l_2, которая позволяет оценить оптимальность подсистемы с точки зрения оперативности обработки информации и дает возможность выработать соответствующие требования к АСКЗИ. Кроме того, данный критерий хорошо приспособлен для включения его в качестве независимой переменной в математическую модель вышестоящего уровня.

Наконец, на низшей ступени иерархии находится подсистема ввода, которая включает клавиатуру, трансмиттер или дисковод, а также входные адаптеры, предназначенные для согласования их с выходами сетевого компьютера. Как и ранее в качестве обобщенного критерия на этом уровне целесообразно выбрать пропускную способность l_1 подсистемы. Этот критерий также приспособлен для включения в качестве независимой переменной в математическую модель вышестоящего уровня и, следовательно, позволит оценить оптимальность устройств данного уровня и сформулировать соответствующие требования к ним.

Согласно математическое описание структуры перспективной АСКЗИ начнем с самой низшей ступени иерархии. Поэтому рассмотрим подсистему ввода информации. Данная подсистема включает в себя устройства ввода, на которые поступает поток входящих криптограмм с плотностью l из компьютера сети, см. рис.2.

Каждый адаптер соединен с соответствующим устройством ввода и имеет производительность $m_{ад}$. Поток входящих криптограмм из сети или оператора через адаптеры поступает на считывание в соответствующие устройства ввода. Производительность устройств ввода намного превосходит производительность клавиатуры, которая определяется возможностями оператора $m >> m_{кл}$ и поэтому производительность подсистемы в наихудшем случае должна была бы определяться в основном производительностью оператора. Однако, если входящий поток криптограмм превосходит производительность оператора, то это приведет к образованию нарастающей очереди у администратора сети, что снижает оптимальность подсистемы. Поэтому клавиатуру следует рассматривать как резервное средство ввода входящих криптограмм, а оптимизацию подсистемы осуществлять на уровне технических устройств ввода (трансмиттер, дисковод и т.д.).

На устройства ввода криптограммы поступают или от оператора через дискету, перфоленту, или от компьютера сети через адаптеры ввода. Причем все поступившие криптограммы рано или поздно попадают на считывание.

Производительность адаптеров ввода намного превосходит производительность технических устройств ввода $m_{ад} >> m$ и поэтому производительность подсистемы ввода в целом будет определяться производительностью технических устройств ввода. Найдем производительность подсистемы ввода l_1, среднее число сообщений в очереди S и среднее время ожидания в очереди $t_{оч}$.

Формально эта задача описывается одноканальной «чистой» системой массового обслуживания (СМ), на вход которой поступает простейший поток заявок с плотностью l, равной среднему числу криптограмм, поступающих в единицу времени. Время обслуживания показательное со средним значением $t_{обс} = \frac{1}{m}$, где m производительность одноного устройства ввода. Длина очереди и время пребывания в ней неограниченны, следовательно, заявки, попавшие в очередь, не покидают ее, а дожидаются обслуживания. Предполагается также, что соответствующее устройство ввода может обслуживать только одну заявку, а каждая заявка обслуживается только одним устройством ввода. Состояния такой системы описываются системой дифференциальных уравнений вида (1):

$$\begin{aligned}
&\frac{dP_0(t)}{dt} = -l\,P_0(t) + m\,P_1(t)\\
&\frac{dP_1(t)}{dt} = -(l+m)P_1(t) + l\,{}_0P_0(t) + 2m\,P_2(t)\\
&\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\\
&\frac{dP_{1+S}(t)}{dt} = -(l+(1+S)m)P_{1+S}(t) + l\,P_S(t) + (2+S)m\,P_{2+S}(t)\\
&\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots,
\end{aligned} \qquad (1)$$

где $P_0(t)$- вероятность того, что в момент времени t система находится в состоянии x_0.

Проинтегрировав систему (1) при начальных условиях $P_0(0)=1$, $P_1(0)=0$ и устремив t в бесконечность, получим предельные вероятности состояний вида:

$$P_1 = \frac{P(1,a)}{R(1,a)+P(1,a)\dfrac{a}{1-a}}, \tag{2}$$

$$P_{1+S} = \frac{P(1,a)a^{S}}{R(1,a)+P(1,a)\dfrac{a}{1-a}}, \tag{3}$$

где $P(1,a)=a\,e^{-a}$, $R(1,a)=e^{-a}+a\,e^{-a}$, $a=\dfrac{l}{m}$.

Известно, что стационарный режим для «чистой» СМО существует только при $l \le 1$.

Среднее число заявок, ожидающих в очереди:

$$S = \frac{\dfrac{a^2}{(1-a)^2}}{1+a+\dfrac{a^2}{(1-a)}}, \tag{4}$$

Тогда: $t_{оч} = \dfrac{S}{l}$. (5)

Параметры (4) и (5) характеризуют внутренние параметры подсистемы ввода, позволяющие оценить технические возможности отдельных устройств и подсистемы в целом.

В качестве обобщенного критерия, как уже отмечалось ранее, здесь выступает пропускная способность подсистемы l_1, которая определяется производительностью подсистемы ввода. Производительность устройств ввода с учетом плотности потока заявок будет равна:

$$l_1 = P_{обс} \cdot l = l. \tag{6}$$

Следовательно, пропускная способность подсистемы ввода оценивается величиной:

$$l_1 = \begin{cases} l & если \quad a \le 1 \\ m & a > 1 \end{cases}. \tag{7}$$

Аналогичные формулы выводятся для подсистемы обработки информации, которые имеют вид:

$$S_1 = \frac{\dfrac{a_1}{(1-a_1)^2}}{1+a_1+\dfrac{a_1^2}{(1-a_1)}}, \tag{8}$$

где $a_1 = \dfrac{l_1}{m_1}$.

Тогда: $t_{оч1} = \dfrac{S_1}{l_1}$. (9)

А пропускная способность подсистемы будет равна:

$$l_2 = \begin{cases} l_1 & если \quad a \le 1 \\ m_1 & a > 1 \end{cases}.$$

Обобщенный критерий подсистемы управления и распределения информации l_2 будет использоваться в качестве независимой переменной в математической модели подсистемы вывода.

Математическая модель подсистемы вывода включает в себя в качестве внутренних характеристик выходные параметры нижестоящих подсистем и поэтому будет представлять из себя обобщенную модель перспективной АСКЗИ в целом. Решение системы дифференциальных уравнений для АСКЗИ в целом приводит к следующим результатам:

$$S_2 = \frac{\dfrac{a_2}{(1-a_2)^2}}{1+a_2+\dfrac{a_2^2}{(1-a_2)}}, \qquad (10)$$

где $a_2 = \dfrac{l_2}{m_2}$.

Тогда: $t_{оч2} = \dfrac{S_2}{l_2}$. (11)

Параметры S_2 и $t_{оч2}$ характеризуют внутренние, технические параметры перспективной АСКЗИ.

В качестве обобщенного критерия на этом уровне, как отмечалось, выступает время обработки криптограммы в перспективной АСКЗИ, которое не должно превышать заданное:

$t_{об\ АСКЗИ} \le t_{зад}$. (12)

Указанный критерий позволяет количественно оценить оптимальность АСКЗИ в целом, так как является аналитическим описанием всего комплекса АСКЗИ с учетом всех его основных характеристик и динамики функционирования подсистем.

Левая часть неравенства (12) складывается из следующих интервалов времени:

среднего времени ввода криптограммы через входные устройства $t_{вв}$;

среднего времени обработки криптограммы в шифраторе $t_ш$;

среднего времени печати сообщения в наборно-печатающей машине (НПМ) $t_{НПМ}$;

среднего времени устранения общих искажений $t_{ои}$;

среднего времени считывания и корректировки расшифрованного текста по экрану дисплея t_k;

среднего времени ожидания криптограммы в очереди на подачу в компьютер $t_{оч}$;

среднего времени ожидания криптограммы в очереди на расшифрование $t_{оч1}$;

среднего времени ожидания расшифрованного текста в очереди на печать $t_{оч2}$.

То есть имеем:

$t_{об\ АСКЗИ} = t_{вв} + t_ш + t_{НПМ} + t_{ои} + t_к + t_{оч} + t_{оч1} + t_{оч2}$. (13)

Проанализируем правую часть выражения (13). Параметры $t_{вв}, t_ш, t_{нпм}$ определяются техническими возможностями соответственно: устройств ввода, шифратора и НПМ. В каждом конкретном, случает они будут заданы и равны соответственно:

$$t_{вв} = \frac{1}{m}, \qquad t_ш = \frac{1}{m_1}, \qquad t_{нпм} = \frac{1}{m_2}. \qquad (14)$$

Значения $t_{ои}$ и $t_к$ будут зависеть от квалификации и опыта работы специалиста-оператора. В качестве их количественной оценки можно взять показатели «среднего» оператора, которые определяются статистическим путем.

При сравнительной оценке АСКЗИ любой структуры можно считать эти параметры постоянными величинами , поскольку независимо от структуры АСКЗИ исправление общих искажений и корректировку текста осуществляет оператор.

И, наконец, $t_{очi}$ $(i = 0,1,2)$ полностью определяются техническими возможностями АСКЗИ и поэтому могут служить переменными величинами, по которым оптимизируется обобщенный показатель $t_{об\ АСКЗИ}$, а , следовательно, структура и технические характеристики АСКЗИ.

Время пребывания криптограммы в очередях $t_{очi}$ можно уменьшить либо путем повышения производительности соответствующих устройств подсистем, либо путем увеличения количества обслуживающих устройств (дублирования).

Очевидно, при оптимизации перспективной АСКЗИ по обобщенному критерию (12) необходимо использовать оба эти пути. При этом наиболее эффективным с точки зрения сокращения

$t_{об\ АСКЗИ}$ является первый путь, когда повышая производительность устройств АСКЗИ , мы тем самым одновременно уменьшаем все слагаемые формулы (13), кроме $t_{ои}$ и $t_{к}$.

А увеличивая число обслуживающих устройств мы уменьшаем только непосредственно величины $t_{очi}$. Однако в некоторых случаях, когда повышение производительности отдельных устройств или их надежности сдерживается существующим уровнем развития технологии, второй путь оказывается наиболее предпочтительным. Например, это в полной мере можно отнести к наборно-печатающим машинам. Учитывая, что НПМ является наиболее узким местом АСКЗИ, с точки зрения быстродействия, которое может сдерживать применение наиболее быстродействующих устройств ввода и обработки информации, например, шифраторов, то целесообразно для вышестоящих уровней управления, когда интенсивность потока криптограмм резко возрастает, в комплект АСКЗИ включать более одной НПМ с соответствующей выходной памятью.

Для оптимизации структуры АСКЗИ целесообразно общее время обработки криптограмм для наглядности разбить по следующим этапам:

1. Ввод криптограммы в АСКЗИ.
2. Расшифрование криптограмм.
3. Считывание и корректировка расшифрованного текста.
4. Распечатка расшифрованного и откорректированного текста.

Тогда общее время обработки $t_{об\ АСКЗИ}$ распределяется по этапам следующим образом:

$$\begin{aligned} t_1 &= t_{вв} + t_{оч}, \\ t_2 &= t_{ш} + t_{ои} + t_{оч1} + t_{оч2}, \\ t_3 &= t_{к}, \\ t_4 &= t_{НПМ}. \end{aligned} \quad . \qquad (15)$$

Такое разбиение позволяет определить этапы, которые вносят существенные задержки в обработку криптограмм и оптимизировать устройства соответствующих этапов, путем дублирования или повышения их производительности.

Полученные выражения (2)-(15) легко программируются на ЭВМ и позволяют оценить оперативность обработки криптограмм при различной структуре и заданных технических характеристик устройств АСКЗИ и тем самым осуществить оптимальный выбор ее структуры относительного обобщенного критерия $t_{об\ АСКЗИ}$.

ЛИТЕРАТУРА

1. Л. фон Берталанфи. Общая теория систем. Критический обзор \\ Сборник переводов. - М.: Прогресс, 1969