УДК 004.414.2

АНАЛИЗ РАЗЛИЧНЫХ ВАРИАНТОВ РЕАЛИЗАЦИИ АЛГОРИТМА ЗА/РАСШИФРОВАНИЯ С ИСПОЛЬЗОВАНИЕМ ДВУХУРОВНЕВОГО МАКРОМОДЕЛИРОВАНИЯ

ИЛЬИН Валерий Николаевич, заведующий кафедрой Московского авиационного института (государственного технического университета), д.т.н., профессор.
Тел. (499) 263-81-94 (раб.), (495) 690-41-19 (дом.), e-mail: vnil2005@yandex.ru

IL'IN Valery N. Professor in MAI. D. Sci.
Tel. (499) 263-81-94 (раб.), e-mail: vnil2005@yandex.ru

ГРИШИН Роман Анатольевич, ассистент Московского авиационного института (государственного технического университета).
Тел. (495) 392-89-75 (дом.), (916) 239-78-96 (моб), e-mail: GrishinRA@gmail.com

Roman A. GRISHIN, assistant Professor at the MAI.
Mobile phone: (916) 239-78-96, e-mail: GrishinRA@gmail.com

Статья посвящена анализу различных вариантов реализации алгоритма за/расшифрования по ГОСТ 28147-89 с целью определения наилучшего варианта уже на ранних этапах проектирования. Основное внимание уделено оценке выходных параметров заданного алгоритма при его реализации на программируемой логической интегральной схеме (ПЛИС). Для оценки выходных параметров применяется метод двухуровневого макромоделирования, что позволяет существенно уменьшить вычислительные затраты по сравнению с известными методами. В статье показано, что полученные с использованием двухуровневого макромоделирования результаты являются адекватными и достаточно точными. В результате анализа вариантов реализации алгоритма было принято решение о реализации алгоритма с использованием ПЛИС и определена наилучшая, в выбранном смысле, структура устройства.

An analysis of en/decryption GOST 28147-89 algorithm implementation variants' is carried out in order to determine the best variant at the early design stages. The algorithm field programmable array implementation's(FPGA) output parameters evaluation is mainly considered. In order to evaluate the output parameters the two-level macromodeling method is used. It's usage enabled the substantial computational complexity reduction in comparison with known methods. It's shown that the results obtained using the two-level macromodeling method are adequate and precise enough. As a result of the carried out analysis the decision was taken to implement the algorithm using FPGA and the best, in the selected matter, device structure was determined.

Ключевые слова: ПЛИС, макромодель, системное проектирование.

Key words: macromodel, system-level design, FPGA.

Постановка задачи

Целью данной работы является выбор наилучшего варианта реализации алгоритма за/расшифрования по ГОСТ 28147-89 в режиме простой замены (далее А1) по критерию максимизации скорости обработки данных. В качестве альтернатив рассматриваются два основных варианта реализации устройства: аппаратная реализация на основе ПЛИС и программная с использованием универсального процессора Pentium или цифрового сигнального процессора (ЦСП) Blackfin. В данной работе основное внимание уделено оценке выходных параметров А1 при его реализации на ПЛИС. Выходные параметры при программной реализации А1 считаются заданными.

Для ПЛИС-реализации А1 требуется определить:

- *затраты логических элементов* L_{A1}, шт. — количество логических элементов (ЛЭ) ПЛИС, необходимых для реализации устройства;
- *затраты памяти* MS_{A1} ,шт. — количество блоков встроенной памяти ПЛИС, необходимых для реализации устройства;
- *максимальная пропускная способность* C_{A1}, МБайт/с — количество данных, которое может быть обработано устройством в единицу времени при условии, что ПЛИС работает на максимальной частоте — F_{A1};
- *предельная тактовая частота работы схемы* F_{A1}, МГц — максимально возможная для данного устройства тактовая частота работы ПЛИС.

Оценку ПЛИС-реализации требуется выполнить для ПЛИС EP2C8TC144C-8 серии Cyclone-II фирмы Altera.

Программная реализация A1 характеризуется следующими выходными параметрами: тип процессора, тактовая частота процессора F_{CPU}, пропускная способность устройства C_{A1}.

Используемые методы

В настоящее время наибольшее распространение для оценки выходных параметров устройств на ПЛИС получил подход на основе синтеза [1]. Данный подход позволяет получить наиболее точные оценки выходных параметров, однако требует выполнения следующих шагов: в специальную САПР вводится подробное описание устройства в виде схемы или на языке описания аппаратуры; выполняется логический и технологический синтез устройства в заданном базисе; полученная структура анализируется для получения выходных параметров устройства. Легко видеть, что метод оценки на основе синтеза не соответствует задачам ранних этапов проектирования (этапы технического предложения и эскизного проектирования [2]), поскольку требует значительных затрат времени как на ввод исходного описания, так и на получение оценки. Указанные особенности метода не позволяют проанализировать значительное количество вариантов за приемлемый срок.

Данная работа иллюстрирует применение метода двухуровневого макромоделирования (МДМ) [3] для оценки выходных параметров устройства на основе ПЛИС. МДМ позволяет существенно упростить как процесс ввода исходных данных, так и процесс получения оценки по сравнению с методом синтеза. Покажем, как выполнить оценку выходных параметров с использованием метода двухуровневого макромоделирования, на примере устройства, реализующего A1. Будем, условно, называть далее данное устройство «шифрователь».

Анализ алгоритма

В соответствии с МДМ необходимо разбить структуру устройства на отдельные узлы, для которых имеются или могут быть созданы макромодели (ММ). Для определения структуры шифрователь рассмотрим алгоритм A1 [4, 5]. Блок-схема A1 приведена на рис. 1.

Входные данные разбиваются на блоки по 64 двоичных разряда, и над каждым из них выполняется алгоритм A1. На рис.1 обозначены: T — массив входных открытых (о) или шифрованных (ш) данных; n — количество 64-битных блоков во входном массиве данных; $И_{32\text{-}3}$ — 32-кратное повторение основного шага криптопреобразования (ОШК). Петлей на рисунке показан цикл по переменной i, принимающей целые значения от 1 до n. Данный цикл отражает процесс поблочной обработки массива входных данных.

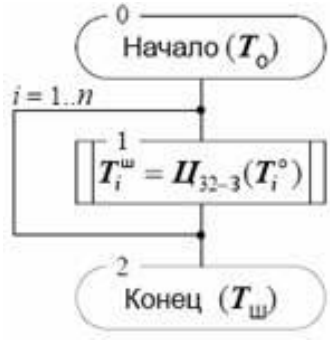

Рис. 1. Блок-схема алгоритма за/расшифрования по ГОСТ 28147-89 в режиме простой замены

Как видно из приведенной блок-схемы, основой A1 является ОШК, так как A1 состоит в многократном исполнении ОШК. Блок схема ОШК представлена на рис. 2.

На рис. 2 обозначены: N — 64-битный блок входных данных; X — 32-битный элемент ключа, прочие обозначения пояснены ниже.

ОШК включает в себя следующие этапы:

1) осуществляется операция сложения по модулю 2^{32} (mod^{32}) над двумя 32-битными операндами;

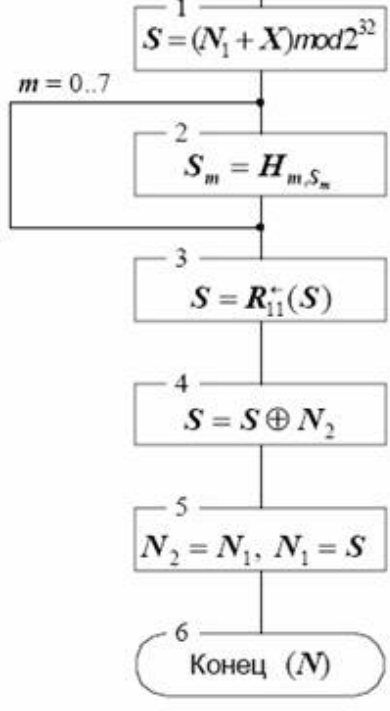

Рис. 2. Блок-схема ОШК

2) производятся замены (H_m) всех m-х тетрад из S. Младшая половина блока входных данных N_1 разбивается на 8 тетрад. Значение каждой тетрады заменяется на новое в соответствии со специальной таблицей замен. Ключом для выбора значения из таблицы является текущее содержимое тетрады. Для каждой тетрады используется своя таблица замен. После выполнения замены тетрады снова объединяются в 32-разрядное слово, порядок следования тетрад при этом не меняется;

3) полученный на втором этапе 32-битный новый результат сдвигается циклически влево, в сторону старших разрядов, на 11 бит (R11);

4) осуществляется побитовое сложение по модулю 2 двух 32-битных целых чисел;

5) старшая и младшая половины входного блока данных меняются местами.

На каждой итерации выполнения ОШК используется 32-разрядная часть 256-битового ключа.

Для оценки выходных параметров шифратора рассмотрим сначала подсхему, реализующую ОШК на ПЛИС (далее — модуль ОШК), и оценим ее выходные параметры.

Специфика аппаратной реализации любого алгоритма заключается в том, что для каждой операции выделяются отдельные аппаратные блоки. Как видно из блок-схемы ОШК, в структуру ОШК войдут макромодели (ММ) следующих узлов: сумматора, таблицы подстановки, схемы сдвига, сложения по модулю два. Процесс создания ММ всех узлов из-за ограниченности объема статьи приводить не будем, для иллюстрации покажем, как создать ММ таблицы замен.

Создание макромодели таблицы замен

Основными входными параметрами таблицы замен являются количество входов W_1 и количество выходов W_2. В нашем случае каждый вход и выход представлен двоичной переменной.

Операция замены реализуется на ПЛИС весьма эффективно за счет того, что структура микросхем ПЛИС выбранного типа основана на табличных преобразователях (LUT — Look-Up-Table), которые позволяют реализовать любую требуемую функцию замены. Преобразователь LUT имеет четыре входа и только один выход, поэтому для реализации таблицы замен с W_2 выходами потребуется не менее W_2 LUT, а значит, и W_2 ЛЭ. Затраты ЛЭ зависят также от числа входных двоичных переменных. Так как каждая LUT имеет четыре входа, то для реализации таблицы замен с W_1 входами потребуется не менее $\lceil W_1/4 \rceil$ ЛЭ (здесь и далее квадратные скобки означают округление числа до ближайшего целого числа в большую сторону). Тогда окончательно затраты ЛЭ на таблицу замен можно определить как

$$L_{tzam} = W_2 \cdot \lceil W_1/4 \rceil.$$

Время срабатывания можно оценить, основываясь на следующих соображениях: для выполнения замены всегда используется один уровень ЛЭ, однако если количество входов таблицы превышает четыре, то несколько ЛЭ объединяются цепью переноса, поэтому время срабатывания таблицы замен можно оценить как

$$t_{tzam} = t_{conn} + t_{carr} \cdot \lceil W_1/4 \rceil,$$

где t_{conn} — задержка на передачу сигнала между соседними уровнями ЛЭ в выбранной ПЛИС;

t_{carry} — задержка на передачу сигнала между соседними ЛЭ одного уровня.

Оценка выходных параметров ОШК

Для данной модуля наиболее существенными являются следующие выходные параметры: затраты ЛЭ, памяти, время срабатывания.

Структура модуля ОШК представлена на рис. 3.

В соответствии со структурой на рис. 3, в состав модуля ОШК войдет сумматор, восемь таблиц замены, операция сложения по модулю два. После того как задана структура модуля ОШК, созданы все необходимые ММ, заданы их входные параметры можно рассчитать выходные параметры модуля ОШК.

Затраты ЛЭ на модуль ОШК можно оценить по формуле [3]

$$L_{\text{osk}} = L_{\text{summ}}(32) + L_{\text{tzam}}(4, 4) + L_{\text{XOR}}(32) =$$

$$= 32 + 4 \cdot 8 + 32 = 96 \text{ ЛЭ},$$

где L_{summ}, L_{XOR} — затраты ЛЭ на сумматор и узел сложения по модулю два соответственно.

В соответствии с [3], для определения времени срабатывания схемы необходимо выделить все ком-

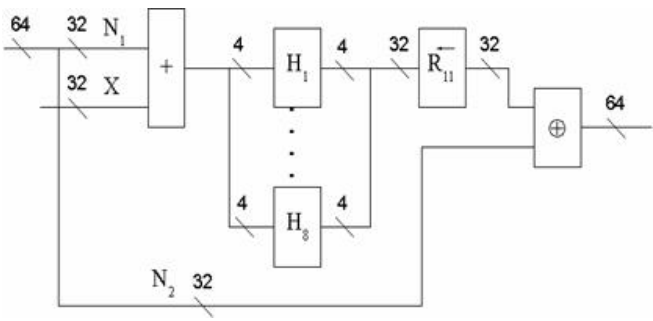

Рис. 3. Структура модуля ОШК

бинационные пути в схеме и найти наиболее длинный из них. ММ ОШК содержит несколько комбинационных путей, но большинство из них состоят из одинаковых элементов (одна из восьми таблиц замены) и являются эквивалентными. Из-за ограниченности объема статьи опустим этап поиска максимального комбинационного пути и сразу приведем формулу для расчета времени срабатывания модуля ОШК:

$$t_{osk} = t_{summ}\,(32) + t_{tzam}(4,\,4) + t_{XOR}\,(32) =$$

$$= 5{,}1 + 1{,}2 + 1{,}2 = 7{,}5 \text{ нс},$$

где t_{summ}, t_{XOR} — задержки на сумматоре и узле сложения по модулю два соответственно.

Более подробно процесс расчета времени срабатывания будет показан ниже для устройства в целом.

Оценка выходных параметров устройства в целом

Можно предложить несколько вариантов реализации A1, основанных на ММ модуля ОШК. Рассмотрим некоторые из них, которые условно назовем:

1. М-автомат [6].
2. I-автомат.
3. I-автомат с конвейеризацией.

М-автомат

Устройство имеет один исполнительный блок, который выполняет основной шаг криптопреобразования. Для зашифрования одного блока данных (64р.) по A1 требуется 32 такта. Структура данного варианта представлена на рис. 4.

На рис. 4 обозначены: Reg N — 64-разрядный регистр, хранящий входной блок данных и промежуточные результаты; Упр. — блок управления; Mem — память ключа. Блок управления, в основном, представлен пятиразрядным счетчиком, формирующим номер сегмента ключа, используемого на текущей итерации. Входом схемы является точка 1, выходом — точка 8. В соответствии с приведенной схемой можно рассчитать следующие выходные параметры устройства:

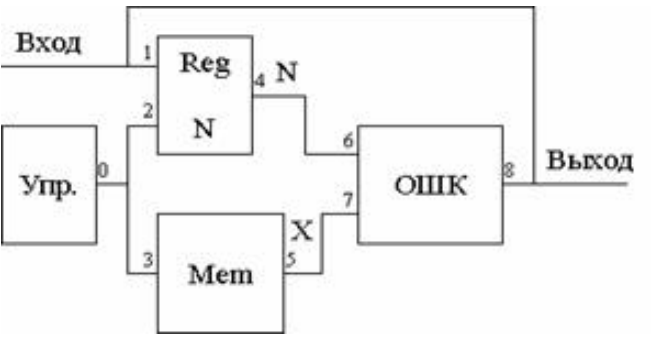

Рис. 4. Структура шифрователя для варианта М-автомата

— затраты ЛЭ

$$L_{A1} = L_{cnt}\,(5) + L_{reg}\,(64) + L_{osk} =$$

$$= 5 + 64 + 96 = 165 \text{ ЛЭ};$$

— затраты памяти. Память должна быть организована как массив из восьми 32-разрядных слов:

$$MS_{A1} = MS\,(32,\,8) = 1.$$

Для расчета прочих выходных параметров необходимо определить время срабатывания устройства. Для этого следует выделить все комбинационные пути в устройстве и определить самый длинный из них. Блок управления память и регистр содержат регистровые элементы на входе и на выходе. В табл. 1 перечислены все комбинационные пути в устройстве.

Таблица 1

Комбинационные пути для варианта М-автомата

№	Путь	Время прохождения сигнала по данному пути
1	0	t_{cnt} (5)
2	0-2; 0-3	t_{conn}
3	3-5	t_{mem} (32,8)
4	4-6-8-1	$t_{osk} + t_{conn}$
5	5-7-8-1	$t_{osk} + t_{conn}$

В таблице обозначены:

t_{cnt}, t_{mem} — задержки на счетчике и блоке памяти соответственно.

В столбце «Путь» указаны номера узлов (см. рис. 4), через которые проходит данный путь. Путь № 1 соответствует задержке сигнала на управляющем блоке, который в простейшем случае представлен пятиразрядным двоичным счетчиком.

После того как выделены все комбинационные пути в устройстве, можно исключить из их числа эквивалентные пути, а также пути, заведомо не являющиеся максимальными. Можно сказать, что пути №1 и №2 имеют малую длительность и не могут определять время срабатывания устройства. Пути №4 и №5 имеют одинаковую длительность, следовательно, можно определить время срабатывания устройства как

$$t_{A1} = \max\,(\,t_{mem}\,(32{,}8)\,;\,t_{osk} + t_{conn}) =$$

$$= \max\,(6{,}13;\,7{,}5 + 1{,}2) = 8{,}7 \text{ нс};$$

$$F_{A1} = 1000 / t_{A1} = 114{,}9 \text{ МГц}.$$

Как было отмечено выше, в данном варианте устройства для зашифрования одного блока данных требуется 32 такта, следовательно, пропускную способность устройства можно определить как:

$$C_{A1} = (F_{A1} / 32)\cdot 8 = (F_{A1} / 4) = 114{,}9 / 4 =$$

$$= 28{,}75 \text{ Мбайт/с.}$$

I-автомат

В данном варианте все 32 цикла алгоритма зашифрования в режиме простой замены реализованы аппаратно (каждой итерации цикла соответствует отдельный модуль ОШК). Вариант характеризуется наибольшими затратами аппаратуры и наибольшей пропускной способностью. В отличие от M-автомата для хранения ключей используются ЛЭ, что также несколько увеличивает затраты аппаратуры. Встроенная память ПЛИС не используется.

Структура шифрователя для варианта I-автомат приведена на рис. 5.

Регистр X хранит весь ключ полностью (256 бит); регистры $T_о$ и $T_ш$ хранят текущий блок открытых и зашифрованных данных соответственно.

Рассчитаем выходные параметры для данного варианта шифрователя.

Регистры $T_о$ и $T_ш$ подключены непосредственно ко входам(выходам) комбинационных функций, поэтому для их реализации не требуются ЛЭ [3]. Затраты ЛЭ на шифрователь составят:

$$L_{A1} = L_{reg}(256) + 32\cdot L_{osk} = 256 + 32\cdot 96 =$$

$$= 3328 \text{ ЛЭ,}$$

где L_{reg} — затраты ЛЭ на регистр заданной разрядности (256 бит).

В данном варианте шифрователя можно выделить следующие комбинационные пути: от точки 0 к точке 2 через все модули ОШК; 32 пути от точки 1 к точке 2 через различное число модулей ОШК. Очевидно, что наибольшим будет путь от точки 0 к точке 2, поэтому для краткости опустим описание процедуры поиска максимального пути и приведем выражение для расчета времени срабатывания:

$$t_{A1} = 32 \cdot t_{osk} + t_{conn} = 32\cdot 7{,}5 + 1{,}2 = 241 \text{ нс;}$$

$$F_{A1} = 1000 / t_{A1} = 4{,}2 \text{ МГц.}$$

Данный вариант шифрователя не содержит обратных связей, включающих элементы памяти, поэтому пропускная способность определяется как произведение частоты работы на размер одного блока данных в байтах:

$$C_{A1} = F_{A1} \cdot 8 = 4{,}2\cdot 8 = 33{,}6 \text{ Мбайт/с.}$$

I-автомат с конвейеризацией

Данный вариант аналогичен предыдущему, но длинные комбинационные пути разделены синхронными регистрами, что способствует повышению предельной рабочей частоты и стабильности работы схемы. А именно, регистры добавлены между 11 и 12, 22 и 23 модулями ОШК. Затраты аппаратуры при этом не изменятся, так как регистры объединяются со смежными комбинационными схемами в одном ЛЭ.

Длины комбинационных путей уменьшатся в среднем в три раза, поэтому можно записать:

$$t_{A1} = (32 \cdot t_{osk} + t_{conn}) / 3 = (11\cdot 7{,}5 + 1{,}2)/3 =$$

$$= 80{,}3 \text{ нс;}$$

$$F_{A1} = 1000 / t_{A1} = 12{,}5 \text{ МГц.}$$

Данный вариант шифрователя не содержит обратных связей, включающих элементы памяти, поэтому пропускная способность определяется как произведение частоты работы на размер одного блока данных в байтах:

$$C_{A1} = F_{A1} \cdot 8 = 12{,}5\cdot 8 = 100 \text{ Мбайт/с.}$$

Анализ результатов

В табл. 2 приведены выходные параметры различных вариантов реализации A1. Результаты, по-

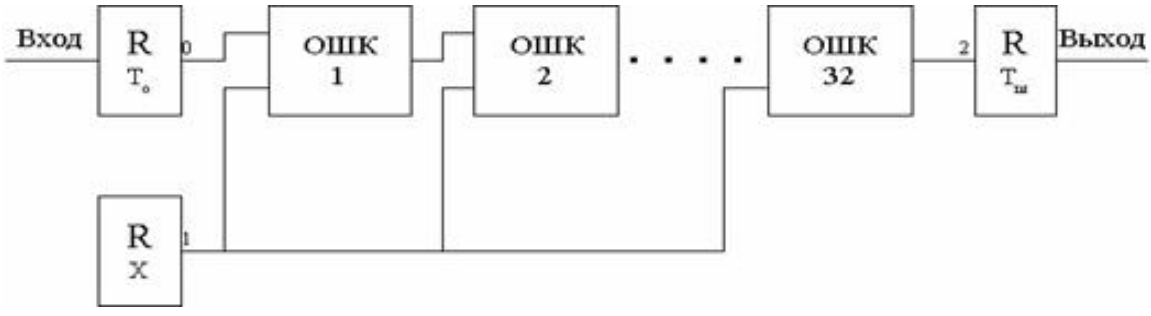

Рис. 5. Структура шифрователя для варианта I-автомата

Таблица 2

Выходные параметры различных вариантов реализации A1

Вариант			L_{A1}, шт.	M_{A1}, шт.	F_{max}/ F_{CPU}, МГц	C, МБ/с	Степень ЛЭ ПЛИС, %
ПЛИС EP2C8...-8	M-автомат	МДМ	165	1	114,9	28,7	2
		факт.	162	1	124	31	2
		ошибка, %	1,8	0	7	7	0
	I-автомат	МДМ	3328	0	4,2	33,6	40
		факт.	3235	0	4,83	38,6	39
		ошибка, %	2,9	0	13	13	
	I-автомат с конвейеризацией	МДМ	3328	0	12,5	100	41
		факт.	3174	0	14,5	116	38
		ошибка, %	4,9	0	14	14	
ADSP-BF533		—	—	—	750	2,1	—
Acer Pentium-66		—	—	—	66	0,4	—

лученные с использованием МДМ, сравниваются с фактическими затратами.

Как видно из табл. 2, пропускная способность ПЛИС-реализации A1 значительно превышает пропускную способность программных вариантов реализации даже при минимальных затратах ЛЭ. Наибольшая пропускная способность достигается для варианта I-автомата с конвейеризацией. При этом в выбранной ПЛИС имеется достаточный запас свободных ЛЭ для перспективной модификации устройства.

Использование двухуровневого макромоделирования позволило существенно сэкономить время выполнения оценки: создание полноценного описания алгоритма A1 на языках описания аппаратуры для различных вариантов реализации, его синтез с использованием САПР проектирования ПЛИС может занять около трех рабочих дней при условии наличия у разработчика опыта проектирования на ПЛИС. В то же время оценка выходных характеристик с использованием макромоделей может быть выполнена за несколько часов при ручном расчете. В случае, если будет разработана САПР, реализующая МДМ, время выполнения оценки может быть сокращено до одного часа. Благодаря МДМ за короткий срок может быть выполнена оценка различных вариантов структурного построения устройства с использованием различных типов ПЛИС. МДМ легко может быть интегрирован с известными методами оптимизации, такими как, например, генетические методы, метод искусственного отбора и др. Это позволит в значительной степени автоматизировать выбор входных параметров узлов устройства и типа используемой ПЛИС.

Выводы

1. Наилучшим вариантом реализации алгоритма за/расшифрования по ГОСТ 28147-89 в режиме простой замены с точки зрения максимизации скорости обработки данных является реализация на ПЛИС в виде I-автомата с конвейеризацией.

2. Применение метода двухуровневого макромоделирования для оценки выходных параметров ПЛИС-реализации алгоритма позволило существенно сэкономить время выполнения оценки по сравнению с известными методами.

Библиографический список

1. *Грушвицкий Р.И., Мусаев А.Х., Угрюмов Е.П.* Проектирование систем на микросхемах с программируемой структурой. — 2-е изд. перераб. и доп. — СПб.: БХВ-Петербург, 2006.

2. Единая система конструкторской документации. Стадии разработки. ГОСТ 2.103-68, М., 1968. С. 1—3.

3. *Ильин В.Н., Гришин Р.А.* Методика оценки основных параметров цифровых устройств на ПЛИС на ранних этапах проектирования с использованием двухуровневого макромоделирования // Информационные технологии. 2009. №7. С. 39—46

4. Системы обработки информации. Защита криптографическая. Алгоритм криптографического преобразования ГОСТ 28147-89. Гос. ком. СССР по стандартам. — М., 1989. С.4—9.

5. *Винокуров А.* Алгоритм шифрования ГОСТ 28147-89, его использование и реализация для компьютеров платформы Intel x86. Код доступа: http://www.enlight.ru/crypto/articles/vinokurov/gost_i.htm, дата создания: 09 мая 2001 г.

6. *Майоров С.А., Новиков Г.И.* Структура электронных вычислительных машин. — Л.: Машиностроение, 1979.