УДК 681.3

СТАН ТА НАПРЯМКИ РОЗВИТКУ НАДВЕЛИКИХ ІНТЕГРОВАНИХ СХЕМ ЗАХИСТУ ІНФОРМАЦІЇ

Анатолій Мельник, Тимур Коркішко

Державний університет "Львівська політехніка", Тернопільська академія народного господарства

Анотація: **Проведений аналіз сучасних НВІС та ядер НВІС захисту інформації, які підтримують виконання симетричних блокових та асиметричних алгоритмів шифрування. Відзначено можливі варіанти роботи НВІС у системах захисту інформації. Виділено два основних способи підключення НВІС захисту інформації – як криптографічних акселераторів та пристроїв обробки потоку даних. Оцінені перспективні напрямки розвитку НВІС захисту інформації.**

Summary: **Analysis of the modern information protection VLSI's and VLSI's cores which supports symmetric block and asymmetric ciphers execution was provided. The possible variants of VLSI usage in the information protection systems were highlighted. Two main aspectcs in VLSI usage were distinguished – as the cryptographic accselerators and as the data stram processing devices. The development perspectives of these VLSI's are estimated.**

Ключові слова: **захист інформації, спеціалізовані НВІС, симетричні блокові алгоритми шифрування, асиметричні алгоритми шифрування, core-технологія, VHDL, Verilog.**

I Вступ

Сучасна комп'ютерна система надає своїм користувачам функції захисту інформації, яка у ній зберігається або обробляється. До переліку цих функцій входять: аутентифікація користувача, розмежування доступу до інформації, забезпечення цілісності, конфіденційності інформації, її захист від модифікації або знищення, електронний цифровий підпис та інше [1]. Частина перелічених функцій традиційно реалізується за допомогою криптографічних алгоритмів перетворення інформації у вигляді програмних модулів для універсальних процесорів. Однак, такій реалізації притаманні поряд з перевагами у гнучкості використання та модифікації модуля і недоліки: проблема підтримки цілісності програмного модуля при запуску системи та, особливо, при її роботі, невисока продуктивність перетворення даних. Підтримка цілісності програмного модуля, який відповідає за криптографічні перетворення, необхідна для уникнення спотворення ключових даних та самого алгоритму криптографічного перетворення. Невисока продуктивність роботи програмних модулів зумовлена невідповідністю системи команд універсальних процесорів характерним операціям, які застосовуються в криптографічних алгоритмах. Тому постає задача створення модулів захисту інформації, які забезпечують цілісність алгоритму та ключової інформації, виконують обробку даних із найвищою продуктивністю.

Одним із можливих шляхів розв'язання цієї задачі є використання у модулях захисту інформації спеціалізованих апаратних засобів – надвеликих інтегрованих схем (НВІС) захисту інформації. Виконання криптографічних алгоритмів на спеціалізованих НВІС дозволяє уникнути проблем із цілісністю алгоритму обробки та ключових даних, так як для цього необхідно отримати вільний доступ до працюючої НВІС та застосувати спеціальне обладнання для зміни її структури або впливу на її роботу, що є практично неможливим. Завдяки структурній спеціалізації складових частин НВІС захисту інформації, зокрема відображенню структури виконуваного алгоритму на тракт обробки даних, досягається висока продуктивність обробки даних.

Відкритість криптографічних алгоритмів дозволила ряду фірм-виробників виготовити спеціалізовані НВІС захисту інформації, орієнтовані на виконання одного чи декількох алгоритмів. У даній роботі проводиться аналіз сучасних НВІС захисту інформації, які підтримують виконання симетричних блокових та асиметричних алгоритмів шифрування та окреслюються перспективні напрямки їх розвитку.

II Алгоритми захисту інформації

Для розв'язання задач захисту інформації – забезпечення приватності або конфіденційності, цілісності даних, аутентифікації та неможливості зречення [2], на практиці використовують вузький перелік алгоритмів перетворення інформації. Як за рубежем, так і в Україні запроваджені відповідні стандарти на алгоритми захисту інформації. До переліку алгоритмів входять: алгоритми цифрового підпису, алгоритми обчислення хеш-функцій, алгоритми симетричного шифрування та інші. Сучасні НВІС захисту інформації підтримують, як правило, виконання симетричних блокових та асиметричних алгоритмів шифрування.

До переліку симетричних блокових шифрів входять: ГОСТ28147-89 [3], DES [4], IDEA [5]. Ці алгоритми використовують невеликий набір базових операцій: додавання (віднімання) за заданим модулем частини блоку із ключем, множення за модулем, зсув на задану кількість біт, перестановка біт, заміна частин блоку у відповідності із таблицею чи функцією. Алгоритм перетворення даних складається із декількох раундів, кількість яких строго визначена для конкретного алгоритму, у кожному з яких виконуються перелічені операції. Також у перетворенні даних бере участь ключ чи його елементи, обчислені за відповідним алгоритмом. Розмір вхідного блоку складає, як правило, 64 біт, розмір ключа змінюється від 56 до 256 біт.

Асиметричні алгоритми шифрування RSA [6], DSA [7], ГОСТ Р34.10-94 [8] використовують такі базові операції: множення, додавання, піднесення до степеня за модулем. Як особливість цього класу алгоритмів необхідно зазначити виконання перелічених операцій над числами із розрядною сіткою порядку 160 – 2048 біт.

Виконання базових операцій перелічених алгоритмів шифрування на універсальних процесорах приводить до значних часових затрат на виконання цих операцій, і, як наслідок, зниження продуктивності обробки даних. Це зумовлено невідповідністю систем команд процесора та режимів адресації використовуваним операціям. Тому зусилля фірм-виробників НВІС сконцентровані на розробці спеціалізованих НВІС захисту інформації, орієнтованих на реалізацію конкретних криптографічних алгоритмів.

ІІІ НВІС захисту інформації

Традиційно НВІС захисту інформації виконують один із режимів роботи заданого криптографічного алгоритму, який може бути вибраний споживачем при створенні НВІС. НВІС захисту інформації поділяються на НВІС симетричного блокового шифрування та НВІС асиметричного шифрування, що зумовлено відмінністю структур алгоритмів та параметрів оброблюваних даних.

НВІС симетричного блокового шифрування орієнтовані на (1) обробку потоків даних чи (2) роботу в якості криптографічних акселераторів для систем, у складі яких використовується універсальний процесор.

У першому випадку НВІС обладнана окремими інтерфейсами для вхідних - вихідних даних, специфічними для конкретного використання, та службовим інтерфейсом, призначеним для управління процесом обробки даних та індикації статусу НВІС. Характеристики службового інтерфейсу випливають із параметрів кінцевої системи, у якій застосовується НВІС. Оскільки, у системах обробки потоків даних для загального управління широко застосовуються універсальні процесори, то службовий інтерфейс НВІС виконується у відповідності до вимог системної шини відповідного універсального процесора.

У другому випадку інтерфейси вхідних - вихідних даних та службовий інтерфейс об'єднуються в один суміщений інтерфейс, який під'єднується до системної шини універсального процесора. Для розділення даних та службової інформації застосовується відображення портів НВІС у адресний простір пам'яті чи пристроїв вводу/виводу універсального процесора.

Основними характеристиками НВІС захисту інформації, що виконують симетричні блокові алгоритми шифрування (табл. 1), є:

- алгоритм обробки даних;
- режими роботи;
- організація інтерфейсу даних та службового інтерфейсу, який може бути спеціалізованим або суміщеним;
- тип інтерфейсу для шини універсального процесора (ШД);
- ємність внутрішньої пам'яті ключів (ПКЛ);
- тактова частота (ТЧ);
- продуктивність роботи (SingleDES/TrippleDES);
- технологія виконання НВІС.

НВІС асиметричного шифрування орієнтовані, як правило, на роботу в якості криптографічних акселераторів універсальних процесорів. Це зумовлено характером базових операцій алгоритмів асиметричного шифрування та розрядністю оброблюваних даних. До складу виконуваних операцій таких НВІС включають операції модульного додавання та віднімання, модульного множення, модульного піднесення до степеня, обчислення зворотного елементу. За допомогою комбінації перелічених операцій можна здійснити виконання поширених асиметричних алгоритмів. Характерною особливістю НВІС асиметричного шифрування є можливість задання розміру оброблюваних даних при її ініціалізації, що зумовлено різноманітністю розмірів даних асиметричних алгоритмів шифрування.

Основними характеристиками НВІС захисту інформації, що виконують асиметричні блокові алгоритми шифрування (табл. 2), є:

- перелік виконуваних операцій;
- перелік величин розрядності оброблюваних даних;
- тип інтерфейсу для шини універсального процесора (ШД);
- тактова частота (ТЧ);

- продуктивність роботи;
- технологія виконання НВІС.

Таблиця 1

НВІС симетричного блокового шифрування

Виробник	Назва НВІС	Алго-ритм.	Режими Роботи	Інтер-фейс	ШД, біт	ПКЛ	ТЧ МГц	Прод. Мбіт/с	Техно-логія
AMD	ADSP2141L	DES	ECB,CBC,OFB CFB 1,8,64	Спец.	16/32	8	66	640/214	
AMD	Am9518	DES	ECB,CBC, CFB 8	Суміщ.	8	1		8	
AMD	Am9568	DES	ECB			1	4	12	
AT&T	T7000A	DES	ECB, CBC, CFB, OFB			1		15.3	
AT&T	DEP229ER	DES	ECB, CBC, CFB1,8,64 OFB			1		1	
AWT	AWT404	DES	ECB	Спец.	64	1	33	192	
CE-Infosys	SyperCrypt CE99C003	DES				1	20	100	
CE-Infosys	SuperCrypt CE99C003A	DES				1	30	160	
Cognitive Design	CDI2100	DES	ECB,CBC,OFB CFB 1,8,64		32	1	33	264/88	
Cryptech	Cry12C102	DES				1	20	22.4	
Cylink	CY1045	DES	ECB,CBC,OFB CFB 1,8,64	Спец.	8	1		45	
Cylink	DES52M	DES	OFB	Спец.		1		52	
Cylink	DES2M1CFB	DES	ECB, CFB1	Спец.		1		2	
HiFn	7711	DES	ECB	Суміщ.	32	3	66	245/82	
HiFn	7751	DES	ECB	Суміщ.	32	3	66	164/83	
Newbridge	CA20C03A	DES					25	30.8	
Newbridge	CA20C03W	DES					8	5.12	
Newbridge	CA95C68/18/09	DES					33	117.36	
PIJNEN-BURG	PCC101	DES	ECB,CBC,OFB CFB 8,16,64	Суміщ.	33	1	33	132	
Sandia	GaAsDES	DES	ECB, CBC	Спец.	64	1		1024	GaAs
Semaphore Communications	Roadrunner284	DES					40	284	
VLSI	VMS113	DES	ECB, CBC		16		40	284/100	
Western Digital	WD2001/2002	DES					3	1.84	
НПО «Восток»		ГОСТ 28147	повний перелік	Суміщ.	8	1	20	16	CMOS, 2um
ASCOM	IDEACrypt	IDEA	ECB, CBC, OFB, CFB1,8,16,64	Спец.	32	1	33	245	CMOS, 0.5um

Примітки до табл. 1: пусті клітинки – відсутня у авторів інформація

Таблиця 2

НВІС асиметричного шифрування

Виробник	Назва НВІС	Операції[1)]	Розрядність даних	Інтерфейс	ТЧ МГц	Продуктивність Кбіт/с	Технологія
AlphaTech		^	1024		25	13	2um
AT&T		^	298		15	19	1.5um
British Tel		^	256		10	5.1	2.5um
Business Sim. Ltd.		^	32		5	3.8	GateArray
Calmos Syst. Inc.		^	593		20	28	2um
CNET		^	1024		25	5.3	1um
Cryptech		^	120		14	17	GateArray
Cylink		^	1024		30	6.8	1.5um
GEC Marconi		^	512		25	10.2	1.4um
HiFn	6500PKP[*]	^ * + – / mod	512 – 2048	PCI 32	66	606 – 54	0.5um
Pijnenburg	PC201	^ * mod	256 – 1024	8, 16	25	58 – 21	1um
Sandia		^	272		8	10	2um
Siemens		^	512		5	8.5	1um

Примітки до табл. 2: пусті клітинки – відсутня у авторів інформація

[1)] – виконувані операції: ^ - піднесення до степеня, * - множення, + - додавання, – віднімання, / – обчислення зворотного елементу, mod - модуль числа;

[*] –використовується зовнішня пам'ять.

IV Ядра НВІС захисту інформації

Завдяки досягненням в галузях засобів проектування та мікроелектронного виробництва на сьогодні зусиллями ряду фірм сформований новий підхід до проектування НВІС. Цей підхід передбачає розробку на фірмі відпрацьованої конструкторської документації на виготовлення НВІС та передачі цієї документації замовнику із наданням йому можливостей доповнення НВІС необхідними додатковими функціональними вузлами та виготовлення закінченої НВІС. За рубежем такий підхід дістав назву core-технологія (core – ядро, серцевина) [9, 10].

Звичайно ядра є завершеними проектами НВІС чи їх вузлів, розробка яких є досить складною задачею, створеними для використання в ролі базової складової частини при проектуванні НВІС. Ядра НВІС захисту інформації виготовляються у вигляді написаної на одній із мов опису апаратних засобів, як правило VHDL чи Verilog:

- моделі тракту обробки даних та системи керування із найпростішими інтерфейсами даних та службової інформації – такий підхід дозволяє розробнику системи захисту інформації використати готову чи розробити свою специфічну інтерфейсну логіку і максимально наблизити технічні параметри отриманої таким чином НВІС до своїх потреб;
- закінченої моделі НВІС захисту інформації із фіксованою інтерфейсною логікою – такий підхід дозволяє будувати НВІС одразу, без додаткових затрат, однак отримана система захисту інформації може не володіти оптимальними параметрами продуктивності роботи.

Обидва підходи дозволяють виготовити як закінчені НВІС захисту інформації у вигляді замовлених інтегральних схем чи систем захисту інформації, побудованих за принципом "системи-на-кристалі" [11]. При цьому для кожного варіанту виготовлення кінцевої НВІС застосовується специфічний стиль написання моделі ядра із орієнтацією на конкретну бібліотеку примітивів НВІС чи орієнтацією на певну архітектуру програмованого логічного пристрою (ПЛП).

Для ядер НВІС застосовується дещо змінений перелік характеристик:

- технологія виготовлення НВІС;
- виробник та тип ПЛП;
- швидкісний індекс ПЛП;
- кількість використаних примітивів;

- тактова частота (ТЧ);
- мова опису моделі ядра.

Крім того, для ядер НВІС захисту інформації до перелічених додаються специфічні для типу ядра характеристики:

- для ядер НВІС симетричного шифрування (табл. 3) – алгоритм обробки даних; режими обробки даних, організація інтерфейсу даних та службового інтерфейсу, тип інтерфейсу для шини універсального процесора, ємність внутрішньої пам'яті ключів (ПКЛ);
- для ядер НВІС асиметричного шифрування (табл. 4) – перелік виконуваних операцій, перелік величин розрядності оброблюваних даних, тип інтерфейсу для шини універсального процесора.

Таблиця 3

Ядра НВІС симетричного шифрування

Виробник	Тип пристрою/ бібліотека	Шв. Інд.[1)]	Алго-ритм	Режими роботи	Інтер-фейс[2)]	ШД.[3)], біт	ПКЛ[4)]	ТЧ, МГц	Кількість примітив.
Alatek	EPF6016	-2	DES	ECB	Спец.	64	1	39	623LC
	EPF81500	-2	DES	ECB	Спец.	64	1	36	634LC
	EPF10K50V	-1	DES	ECB	Спец.	64	1	43	663 LC
	XLC30	-3	DES	ECB	Спец.	64	1	24	264CLB
	XC4013XL	-08	DES	ECB	Спец.	64	1	55	266CLB
	V150	-6	DES	ECB	Спец.	64	1	100	281Slices
CAST	Virtex V150	-6	DES	ECB	Спец.	64	1	101	255Slices
	EPF6016	-2	DES	ECB	Спец.	64	1	37	540 LC
	EPF81500	-2	DES	ECB	Спец.	64	1	35	540 LC
	EPF10K20	-3	DES	ECB	Спец.	64	1	44	540 LC
	EPF10K30A	-1	DES	ECB	Спец.	64	1	73	570 LC
	EPF10K50V	-1	DES	ECB	I8051	8	1	27	574 LC
Inventra	CBA library		DES	ECB	Спец.	64	1	100	4000gates
Inventra	CBA library		DES	ECB,CBC	Спец.	64	1	100	7000gates
Memec	XC4000E/XL		DES	ECB	Спец.	64	1	43	316CLB
Design	Spartan		DES	ECB	Спец.	64	1	25	316CLB

Примітки до табл. 3: пусті клітинки – відсутня у авторів інформація

[1)] – швидкісний індекс;

[2)] – спец. – спеціалізований;

[3)] – шина даних;

[4)] – розмір пам'яті ключів.

Таблиця 4

Ядра НВІС асиметричного шифрування

Виробник	Тип пристрою/ бібліотека	Шв. інд.[1)]	Операції[2)]	Розрядність даних	Інтер-фейс[3)]	ШД[4)], біт	ТЧ МГц	Кількість примітивів
Sican			^,*,+,mod	до 8192	i8051	8	100	8500gates*
Inventra	CBA library		^,*,+,mod	1024	Спец.	8	40	7000gates*
WPI	XC4000	-6	^,*	160 – 1024	Спец.	16	50	1220 - 6700CLB

Примітки до табл. 4: пусті клітинки – відсутня у авторів інформація

[1)] – швидкісний індекс;

[2)] – спец. – спеціалізований;

[3)] – виконувані операції: ^ - піднесення до степеня, * - множення, + - додавання, mod - модуль числа;

[4)] – шина даних;

* – без врахування зовнішньої пам'яті.

V Напрямки розвитку НВІС захисту інформації

Сучасні НВІС захисту інформації характеризуються високим ступенем інтеграції, добрими показниками продуктивності, широким набором функціональних можливостей по роботі у різних режимах.

Гнучкість у виборі режимів обробки даних дозволяє ефективно використовувати НВІС симетричного шифрування у системах захисту даних. Однак, системи захисту даних використовують меншу кількість режимів шифрування, ніж пропонують НВІС. Таким чином, з одного боку, не використовується частина обладнання

НВІС, а з другого – вимога мінімальних затрат обладнання зумовлює застосування такої структурної організації НВІС, при якій неможливо досягнути максимальної продуктивності її роботи. Тому перспективним напрямком розвитку НВІС симетричного шифрування є оптимізація архітектури тракту обробки даних та структурної організації в цілому під таку кількість режимів обробки даних, яка необхідна розробнику для конкретної системи захисту інформації – вузька спеціалізація НВІС під конкретне застосування. При цьому буде звужене коло галузей застосування таких НВІС, однак буде ефективно використане обладнання НВІС та досягнута максимальна продуктивність роботи.

НВІС асиметричного шифрування характеризуються високою складністю структурної організації, що зумовлено специфікою виконуваних алгоритмів та розрядністю оброблюваних даних, оскільки розвиток обчислювальних методів по «зламу» алгоритмів асиметричного шифрування зумовлює нарощення розрядності даних – це в свою чергу приводить до зменшення продуктивності виконання операцій модульної арифметики. Обмеженість набору виконуваних над даними операцій та відсутність достатньої пам'яті всередині НВІС зумовлює часті пересилання великого об'єму даних між універсальним процесором та криптографічним акселератором, що завантажує системну шину універсального процесора та накладає обмеження на ріст продуктивності роботи системи захисту інформації в цілому. Тому перспективною є інтеграція у НВІС асиметричного шифрування достатньої внутрішньої пам'яті чи створення інтерфейсу до окремої пам'яті, відокремленої від системної шини. Для обробки даних великої розрядності (більш ніж 2048 біт) доцільним є включення у НВІС засобів підтримки багатопроцесорних конфігурацій. Також розширення та спеціалізація системи команд НВІС відповідно до алгоритму дозволить підвищити ефективність виконання алгоритмів асиметричного шифрування. Поява нових асиметричних алгоритмів шифрування та їх застосування при побудові криптографічних протоколів наштовхує на необхідність створення програмованих НВІС асиметричного шифрування, які б могли виконувати послідовність операцій над числами великої розрядності і таким чином перенести процедуру організації протоколу на спеціалізовану НВІС.

З іншого боку, існують задачі захисту інформації у смарт-картках, де необхідна продуктивність роботи пристрою шифрування повинна бути вищою ніж в універсальних процесорах, але такий пристрій повинен використовувати мінімум ресурсів з точки зору площі кристалу та споживаної потужності. В такому випадку перспективними є «мінімальні» структури пристроїв шифрування, які апаратно виконують заданий алгоритм із використанням мінімуму ресурсів.

Окремо необхідно зазначити, що технічні характеристики НВІС у значній мірі залежать від типу та рівня оптимізації використаних алгоритмів. Тому актуальною є розробка нових алгоритмів шифрування та алгоритмів виконання модульних операцій, орієнтованих на виконання у вигляді НВІС.

На сьогоднішній день від розробників вимагається гнучкість у проектуванні, якість продукту та швидкість створення систем захисту інформації. Тому актуальним є створення параметризованих моделей та бібліотек ядер НВІС, що дозволить створювати нові та модифікувати існуючі системи захисту інформації, використання яких дозволить досягнути наступних переваг у порівнянні із ситуацією, коли розробник повинен розробляти НВІС захисту інформації від початку:

- суттєво спрощується та прискорюється процес проектування, адже основна робота по проектуванню НВІС уже виконана розробником ядра (сюди входить перелік робіт по розробці загальної структури, системи та форматів команд і даних, проектуванню операційного пристрою, пристрою управління, пам'яті, інтерфейсів і т.д., оптимізації архітектури, перевірці та тестуванні);
- практично виключається можливість помилок та досягаються високі рівні інтеграції, оскільки розробник ядра, звичайно, має великий досвід у питаннях проектування НВІС і випускає на ринок добре відпрацьовані та оптимізовані продукти;
- знаючи ринок ядер розробники НВІС мають можливість вибору ядра, здатного забезпечити потрібні значення продуктивності та споживаної потужності, виходячи із наявних технологій проектування.

VI Висновки

В роботі проведений аналіз НВІС захисту інформації. Окремо розглянуті НВІС симетричного та асиметричного шифрування, виконані у вигляді замовлених НВІС та у вигляді ядер. Відзначено можливі варіанти роботи НВІС у системах захисту інформації. Виділено два основних способи підключення НВІС захисту інформації – як криптографічних акселераторів та пристроїв обробки потоку даних.

Аналіз технічних характеристик та способів використання НВІС захисту інформації дозволив окреслити напрямки розвитку НВІС захисту інформації:

- для НВІС симетричного шифрування – вузька спеціалізація на малу кількість режимів роботи, включаючи спеціалізацію лише на зашифрування чи розшифрування, оптимізація трактів обробки даних, використання оптимізованих інтерфейсів, які дозволяють проводити ввід/вивід даних за мінімальний час;

- для НВІС асиметричного шифрування – інтеграція пам'яті даних, розширення системи команд, більша орієнтація НВІС на виконуваний алгоритм, включення в склад НВІС засобів підтримки колективної роботи при обробці даних великої розрядності;
- для обох типів пристроїв захисту даних актуальною є задача розробки оптимальних структур для використання у системах із жорсткими обмеженнями щодо споживаної потужності та площі кристалу/кількості задіяних елементів.

Актуальною є розробка нових алгоритмів шифрування та алгоритмів виконання модульних операцій, орієнтованих на виконання у вигляді НВІС та створення параметризованих моделей та бібліотек ядер НВІС, що дозволить створювати нові та модифікувати існуючі системи захисту інформації.

На жаль, авторам невідомі НВІС та ядра НВІС захисту інформації українського виробництва. Розробка вітчизняної елементної бази для захисту інформації є необхідним елементом у становленні України як країни із добрим рівнем безпеки інформації та забезпеченням впевненості у відсутності прихованих умисних «закладок» у придбаній за кордоном компонентній базі. Наявність сучасних засобів підтримки розробки цифрових пристроїв із використанням мов опису апаратних засобів VHDL та Verilog – компіляторів та симуляторів, засобів синтезу розроблених моделей пристроїв на конкретні кристали ПЛП провідних фірм-виробників створюють потенційну можливість налагодження дослідного та промислового виготовлення необхідних НВІС захисту інформації науковими інституціями та комерційними фірмами України.

Література: 1. Романец Ю.В., Тимофеев П.А., Шаньгин В.Ф. Защита информации в компьютерных системах и сетях/Под ред. В.Ф. Шаньгина. – М.: Радио и связь, 1999. – 328 с. 2. Alfred J. Menezes, Paul C. van Oorschot and Scott A. Vanstone «Handbook of Applied Cryptography», CRC Press, October 1996, 816p. 3. ГОСТ28147-89. Система обработки информации. Защита криптографическая. Алгоритм криптографического преобразования. 4. FIPS 46, "Data Encryption Standard", Federal Information Processing Standard (FIPS), Publication 46, National Bureau of Standards, U.S. Department of Commerce, Washington D.C. 5. X. Lai, J.L. Massey A proposal for a New Block Encryption Standard. Advances in Cryptology – EUROCRYPT-90 Proceedings, New York, NY: Springer-Verlag, pp.389-404. 6. R. Rivest, A. Shamir, L. Adleman «A Method for Obtaining Digital Signatures and Public Key Cryptosystems», Communications of ACM, February 1978. 7. NIST, A proposed federal information proceedings standard for digital signature standard (DSS), Federal Register 56 (1991), 42980-42982. 8. ГОСТР34.10-94. Информационная технология. Криптографическая защита информации. Процедуры выработки и проверки электронной цифровой подписи на базе асимметричного криптографического алгоритма.9. P.Lapsley and J.Bier «DSP Cores Bring New Levels of Integration»//Microprocessor report, August 1994.10. DSP Design Tools and Methodologies, Berkeley Design Technology, Inc. (Fremont, California), 1995.11. M. Keating, P. Bricaud «Reuse Methodology Manual for System-On-a-Chip Design», Kluwer Academic Publishers, 1999, pp. 224.