

УТВЕРЖДЕН  
СЕИУ.00009-01 33 - ЛУ

Инв. № подл.	Подп. и дата	Взам. инв. №	Инв. № дубл.	Подп. и дата

СРЕДСТВО КРИПТОГРАФИЧЕСКОЙ ЗАЩИТЫ ИНФОРМАЦИИ  
MagПро КриптоПакет вер. 1.0

**Библиотека реализации алгоритмов ГОСТ libcryptocom.  
Руководство системного администратора**

СЕИУ.00009-01 33  
Листов 17

Литера О

## Аннотация

Настоящий документ содержит руководство системного администратора для работы с библиотекой реализации алгоритмов ГОСТ libcryptocom из состава СКЗИ «МагПро КриптоПакет», реализующей российские алгоритмы для библиотеки OpenSSL.

Общие сведения по использованию СКЗИ «МагПро КриптоПакет» приведены в документе «Средство криптографической защиты информации «МагПро КриптоПакет в. 1.0». Описание применения» (СЕИУ 00009-01 31).

Авторские права на СКЗИ «МагПро КриптоПакет» принадлежат ООО «Криптоком». «МагПро» является зарегистрированной торговой маркой ООО «Криптоком».

## Содержание

<b>1</b>	<b>НАЗНАЧЕНИЕ БИБЛИОТЕКИ</b>	<b>4</b>
<b>2</b>	<b>УСЛОВИЯ РАБОТЫ БИБЛИОТЕКИ</b>	<b>5</b>
2.1	Требования к конфигурации ПЭВМ . . . . .	5
2.1.1	Аппаратные требования . . . . .	5
2.1.2	Программные требования . . . . .	5
2.2	Служебные файлы . . . . .	5
<b>3</b>	<b>СБОРКА OpenSSL</b>	<b>6</b>
3.1	Общие принципы сборки OpenSSL . . . . .	6
3.2	Особенности сборки OpenSSL в системах WIN32 . . . . .	6
<b>4</b>	<b>УСТАНОВКА БИБЛИОТЕКИ</b>	<b>7</b>
<b>5</b>	<b>ЗАГРУЗКА БИБЛИОТЕКИ ЧЕРЕЗ КОНФИГУРАЦИОННЫЙ ФАЙЛ OpenSSL</b>	<b>8</b>
<b>6</b>	<b>ИСПОЛЬЗОВАНИЕ БИБЛИОТЕКИ</b>	<b>10</b>
6.1	Вычисление хэш-сумм . . . . .	10
6.2	Создание закрытого ключа и запроса на сертификат . . . . .	10
6.3	Поддержка удостоверяющего центра . . . . .	10
6.4	Работа с сообщениями формата S/MIME . . . . .	10
6.4.1	Выработка и проверка подписи под сообщениями . . . . .	10
6.4.2	Зашифрование сообщений . . . . .	10
6.4.3	Расшифрование сообщений . . . . .	11
6.5	Использование алгоритма симметричного шифрования GOST 28149-89 . . . . .	11
<b>7</b>	<b>КОНФИГУРИРОВАНИЕ ПРИЛОЖЕНИЙ</b>	<b>12</b>
7.1	Список приложений, работающих с OpenSSL в. 0.9.8 и с библиотекой реализации алгоритмов ГОСТ libcryptocom . . . . .	12
7.2	Серверные приложения . . . . .	12
7.2.1	www-сервер Apache . . . . .	12
7.2.2	Серверное приложение Stunnel . . . . .	13
7.2.3	Сервер каталогов OpenLDAP . . . . .	13
7.3	Клиентские программы . . . . .	13
7.3.1	Web-браузер lynx . . . . .	13
7.3.2	Программа получения файлов wget . . . . .	13
7.3.3	Почтовый клиент mutt . . . . .	13
7.4	Средства разработки . . . . .	14
7.4.1	tcclts . . . . .	14
<b>8</b>	<b>ПРИЛОЖЕНИЯ</b>	<b>15</b>
8.1	Датчики случайных чисел для работы библиотеки libcryptocom . . . . .	15
8.2	Названия и параметры алгоритмов . . . . .	15

Порядковый № изменения	Подпись лица, ответственного за изменение	Дата внесения изменения

# 1 НАЗНАЧЕНИЕ БИБЛИОТЕКИ

Библиотека реализации алгоритмов ГОСТ libcryptocom из состава СКЗИ «МагПро КриптоПакет», реализующая российские криптоалгоритмы, является подгружаемым модулем для OpenSource-библиотеки OpenSSL в. 0.9.8.

В сочетании с патчем, входящим в состав СКЗИ «МагПро КриптоПакет», данная библиотека дает возможность использования российских стандартных криптоалгоритмов при работе с приложениями, использующими библиотеку OpenSSL.

В целях совместимости с разработками компании «Крипто-Про» в библиотеке реализованы российские криптоалгоритмы подписи и шифрования в вариантах, разработанных компаниями «Криптоком» и «Крипто-Про».

Библиотека реализации алгоритмов ГОСТ libcryptocom реализует следующие криптографические алгоритмы:

- Алгоритм хэширования по ГОСТ Р 34.11-94
- Алгоритм выработки подписи по ГОСТ Р 34.10-94 в варианте Cryptocom
- Алгоритм выработки подписи по ГОСТ Р 34.10-94 в варианте CryptoPro
- Алгоритм выработки подписи по ГОСТ Р 34.10-2001 в варианте Cryptocom
- Алгоритм выработки подписи по ГОСТ Р 34.10-2001 в варианте CryptoPro
- Алгоритм имитозащиты по ГОСТ 28147-89
- Алгоритм шифрования по ГОСТ 28147-89

Использует один из нескольких ДСЧ по выбору пользователя. Выбор осуществляется с помощью переменной среды RNG (см. п. 8.1).

Порядковый № изменения	Подпись лица, ответственного за изменение	Дата внесения изменения

## 2 УСЛОВИЯ РАБОТЫ БИБЛИОТЕКИ

### 2.1 Требования к конфигурации ПЭВМ

#### 2.1.1 Аппаратные требования

Для работы библиотеки `libcryptocom` необходимы следующие условия:  
 для архитектуры x86 — процессор Pentium и выше  
 для архитектуры Sparc — процессор UltraSparc

#### 2.1.2 Программные требования

Для работы библиотеки `libcryptocom` требуется установить в системе криптобиблиотеку OpenSSL версии 0.9.8 с соответствующим патчем из комплекта МагПро КриптоПакет.

Библиотека `libcryptocom` поставляется в собранном виде. Предназначена для работы в операционных системах:

- Windows 2000/XP, Windows Server 2003, Windows Vista
- Debian GNU/Linux 3.1, 4.0
- AltLinux Master 2.4
- Red Hat Enterprise Linux 4, 5
- Fedora Core linux 5
- SUSE Linux 9, 10
- ASP Linux 9.2, 10, 11
- Mandriva Linux 2006
- Mandrake Linux 10.1
- FreeBSD 4.x 5.x 6.x
- Solaris Sparc 8,9
- Solaris Intel 8,9,10
- HP-UX 11.11

### 2.2 Служебные файлы

Библиотека реализации алгоритмов ГОСТ `libcryptocom` представляет собой подгружаемую динамическую библиотеку.

Библиотека содержится в файле `libcryptocom.so` или `cryptocom.dll`.

Порядковый № изменения	Подпись лица, ответственного за изменение	Дата внесения изменения

## 3 СБОРКА OpenSSL

### 3.1 Общие принципы сборки OpenSSL

Для сборки OpenSSL для работы с библиотекой `libcryptocom` необходимы исходники OpenSSL версии 0.9.8 с приложенным патчем (необходимый патч содержится в файле `openssl-asymm-*.diff`).

Пакет OpenSSL должна быть сконфигурирован при сборке так, чтобы потом можно было использовать подгружаемые модули.

Для конфигурирования и сборки OpenSSL необходимо:

1. Распаковать дистрибутив (исходники) OpenSSL
2. Перейти в директорию верхнего уровня в распакованном дистрибутиве.
3. Приложить патч.
4. Сконфигурировать OpenSSL с использованием динамических библиотек

```
>./config shared
```

5. Собрать OpenSSL

```
>make
```

### 3.2 Особенности сборки OpenSSL в системах WIN32

К настоящему времени сборка под Win32 тестировалась только с помощью компиляторов MingW32. Можно использовать как собственный компилятор MINGW32, который можно загрузить с сайта <http://www.mingw.org>, так и компилятор MingW32 из комплекта cygwin, или кросс-компилятор, запускаемый на какой-либо платформе Unix.

После применения патча необходимо регенерировать файл `util/libeay.num` с помощью команды

```
>util/mkdef.pl 32 libeay
```

Собрать OpenSSL с помощью Mingw32 можно двумя способами:

1. использовать командный файл `ms/mingw.bat`
2. использовать скрипт `Configure`, как в системах Unix.

Рекомендуется использовать скрипт `Configure`, поскольку он лучше поддерживается и всегда соответствует текущему состоянию исходников.

Чтобы запустить скрипт `Configure` под Windows, необходим набор утилит POSIX (например MSYS, который можно загрузить с сайта MingW) и интерпретатор языка Perl (рекомендуется ActiveState perl, который можно загрузить с сайта <http://perl.activestate.com>).

При запуске скрипта `Configure` или командного файла `/mingw.bat` обязательно следует указать опцию `shared`.

Порядковый № изменения	Подпись лица, ответственного за изменение	Дата внесения изменения

## 4 УСТАНОВКА БИБЛИОТЕКИ

Для установки библиотеки `libcryptosom` необходимо разместить файл динамической библиотеки в каталоге, в котором размещаются все динамически подгружаемые модули библиотеки OpenSSL.

В конфигурации по умолчанию это каталог `/usr/local/ssl/lib`.

При установке OpenSSL из пакета Debian это каталог `/usr/lib/ssl/engines`.

Для работы библиотеки `libcryptosom` необходимо выбрать один из сертифицированных датчиков случайных чисел, установив значение переменной среды `RNG`, соответствующее выбранному датчику (см. п. 8.1). Если при использовании библиотеки `libcryptosom` значение переменной среды `RNG` не будет установлено или будет установлено некорректно, произойдет ошибка.

Порядковый № изменения	Подпись лица, ответственного за изменение	Дата внесения изменения

## 5 ЗАГРУЗКА БИБЛИОТЕКИ ЧЕРЕЗ КОНФИГУРАЦИОННЫЙ ФАЙЛ OpenSSL

Библиотека `libcryptocom` предоставляет новые алгоритмы. Поэтому данную библиотеку необходимо загружать ДО того, как будут разобраны опции команд `openssl`. Иначе некоторые команды, например `dgst`, не смогут понять имена новых алгоритмов в командной строке.

Лучше всего загружать библиотеку через конфигурационный файл OpenSSL.

Для этого необходимо добавить в конфигурационный файл OpenSSL следующую информацию:

1. До названия первой секции (первая строка [в квадратных скобках]) следует поместить команду `openssl_conf`, указывающую на секцию с глобальными параметрами конфигурации (по умолчанию этой секции не существует в файле, ее необходимо будет добавить):

```
openssl_conf = openssl_def
```

2. Где-то в файле (например, в конце) добавить секцию, указанную выше, и вставить в нее команду `engines`, указывающую на секцию со списком модулей, которые необходимо подгрузить:

```
[openssl_def]
engines = engine_section
```

3. Добавить секцию `engines`, содержащую строку с ID MagPro Engine и название секции, описывающей его конфигурацию:

```
[engine_section]
cryptocom = cryptocom_section %(для Cryptocom Engine)
```

4. Добавить секцию, описывающую конфигурацию библиотеки. Эта секция должна содержать по меньшей мере две строки — в одной указывается полный путь к модулю, во второй указывается его ID.

```
[cryptocom_section]
dynamic_path = /usr/local/ssl/lib/engines/libcryptocom.so
(для систем Unix)
dynamic_path = C:/OpenSSL/lib/engines/cryptocom.dll (для систем Win32)

engine_id = cryptocom
default_algorithms = ALL
```

Значение `dynamic_path` должно указывать на файл, содержащий установленную библиотеку, а значение `engine_id` должно быть `cryptocom`.

Необходимо добавить также строку `default_algorithms = ALL`. Иначе библиотека не сможет использовать сертифицированные датчики случайных чисел.

Рекомендуется поместить библиотеку `libcryptocom` в директорию, по умолчанию содержащую динамически подгружаемые модули OpenSSL, чтобы приложения, имеющие свои собственные конфигурационные файлы и подгружающие модули по их названиям (например, `apache/mod_ssl`) могли подгружать его.

Порядковый № изменения	Подпись лица, ответственного за изменение	Дата внесения изменения

Утилита `openssl` выбирает для загрузки конфигурационный файл либо по умолчанию (обычно это файл `openssl.cnf` из каталога, название которого можно получить в результате выполнения команды `openssl version -d`), либо указанный в качестве значения переменной среды `OPENSSL_CONF`.

Некоторые команды `openssl`, такие как `req` или `ca`, позволяют явным образом указывать конфигурационный файл `OpenSSL` в командной строке. Это позволяет работать с индивидуальными конфигурационными файлами, в том числе с файлами, содержащими информацию о сертификатах пользователя (описание формата конфигурационного файла `OpenSSL` можно найти на <http://www.openssl.org/docs/apps/config.html>). Такие конфигурационные файлы также должны содержать секции с конфигурацией библиотеки `libcryptocom`, как указано выше.

Такой файл конфигурации обеспечивает работу с библиотекой `libcryptocom` утилиты `openssl` и всех приложений, которые читают файл конфигурации `OpenSSL` по умолчанию.

Порядковый № изменения	Подпись лица, ответственного за изменение	Дата внесения изменения

## 6 ИСПОЛЬЗОВАНИЕ БИБЛИОТЕКИ

В этом разделе приводится описание особенностей работы пакета OpenSSL при использовании библиотеки libcrypto.com.

Перед запуском любой программы, использующей библиотеку, необходимо установить значения переменных среды RNG и, если используемый датчик случайных чисел требует параметры, RNG\_PARAMS (см. п. 1).

### 6.1 Вычисление хэш-сумм

Утилита openssl предоставляет специальные команды вычисления хэш-сумм для встроенных алгоритмов, таких как openssl md5, openssl sha1 и так далее. Подгружаемый модуль не может добавлять новые команды. Поэтому, чтобы посчитать хэш-сумму по алгоритму ГОСТ Р 34.11-94, следует использовать общую команду dgst с опцией -md\_gost94:

```
>openssl dgst -md_gost94 filename
```

### 6.2 Создание закрытого ключа и запроса на сертификат

Следует использовать опцию -newkey. Аргумент этой опции состоит из наименования алгоритма и параметров этого алгоритма, разделенных двоеточием (наименования и параметры алгоритмов см. п. 8.2).

Например, алгоритм GOST94 в варианте Cryptocom не имеет параметров, поэтому после двоеточия не нужно ничего указывать (пустая строка):

```
>openssl req -newkey gost94: -keyout mykey.p8 -out mykey.req
```

### 6.3 Поддержка удостоверяющего центра

Не следует использовать скрипты CA.pl и CA.sh. Следует вызывать openssl ca непосредственно. CA.pl и CA.sh имеют некоторые умолчательные параметры, не подходящие для алгоритмов GOST.

### 6.4 Работа с сообщениями формата S/MIME

#### 6.4.1 Выработка и проверка подписи под сообщениями

Работа с незашифрованными сообщениями формата S/MIME не зависит от алгоритмов. Если требуется воспользоваться алгоритмами из библиотеки libcrypto.com, необходимо просто получить и использовать сертификаты GOST.

#### 6.4.2 Зашифрование сообщений

Чтобы воспользоваться алгоритмом GOST 28147-89 для зашифровки сообщения, необходимо использовать опцию -gost89 команды openssl smime:

```
>openssl smime -encrypt -gost89 -in message.txt -out message.encr  
addressee.crt
```

Порядковый № изменения	Подпись лица, ответственного за изменение	Дата внесения изменения

Указанный алгоритм имеет параметры (см. п. 8.2).

Библиотека `libcryptocom` предоставляет алгоритм шифрования с параметром `Cryptocom` и с параметрами `CryptoPro`. Если для зашифрования сообщения необходимо использовать алгоритм с параметром `Cryptocom`, указывать параметр необязательно, т.к. этот алгоритм используется по умолчанию. Если для зашифрования сообщения необходимо использовать алгоритм с параметрами `CryptoPro`, необходимый параметр следует указать в качестве значения переменной среды `CRYPT_PARAMS`.

### 6.4.3 Расшифрование сообщений

Вся необходимая информация содержится в зашифрованных сообщениях, поэтому, если библиотека `libcryptocom` подгружена и пользователь располагает необходимым закрытым ключом, пользователь сможет расшифровать сообщение.

## 6.5 Использование алгоритма симметричного шифрования GOST 28149-89

Для зашифрования:

```
>openssl enc -gost89 -e -pass <pass-phrase source> -in file -out
cryptedfile
```

Для расшифрования:

```
>openssl enc -gost89 -d -pass <pass-phrase source> -in cryptedfile -out
file
```

Порядковый № изменения	Подпись лица, ответственного за изменение	Дата внесения изменения

## 7 КОНФИГУРИРОВАНИЕ ПРИЛОЖЕНИЙ

### 7.1 Список приложений, работающих с OpenSSL в. 0.9.8 и с библиотекой реализации алгоритмов ГОСТ libcryptocom

Ниже приводится список приложений, для которых гарантируется работа с библиотекой реализации алгоритмов ГОСТ libcryptocom.

- WWW-сервер Apache
- Серверное приложение Stunnel
- Сервер каталогов OpenLDAP
- Web-браузер lynx
- Программа получения файлов wget
- Почтовый клиент mutt
- Средство разработки tcclts

Для работы с библиотекой libcryptocom необходимо соответствующее конфигурирование этих приложений. Подробно конфигурирование каждого приложения описано ниже.

### 7.2 Серверные приложения

#### 7.2.1 www-сервер Apache

Apache (<http://httpd.apache.org>) — один из самых распространенных в мире www-серверов.

Для Apache существуют модули организации защищенных соединений. Наиболее распространенным из существующих является модуль `mod_ssl` (<http://www.modssl.org>).

В коде `mod_ssl` предполагается, что существует только два типа асимметричных ключей — RSA и DSA. Поэтому для реализации поддержки подгружаемых алгоритмов при работе с Apache требуется внести небольшие изменения в код `mod_ssl`, дважды заменив в коде явное указание константы `EVP_PKEY_DSA` на обращение к типу ключа из загруженного сертификата. Патч, выполняющий эту задачу, можно загрузить с сайта <http://www.cryptocom.ru>.

Кроме того, при сборке `apache+mod_ssl mod_ssl` следует конфигурировать с указанием ключа `-enable-rule=SSL_EXPERIMENTAL`, так как возможность указания используемого модуля до сих пор является экспериментальной возможностью, не включаемой по умолчанию.

Для подключения российских алгоритмов к Apache следует:

1. Создать закрытый ключ соответствующего алгоритма и получить сертификат на него.
2. Указать в файле конфигурации Apache (`httpd.conf`) директиву `SSLCryptoDevice <имя engine>`
3. Указать в том же файле с помощью директивы `SetEnv` тип и, если необходимо, параметры ДСЧ.

```
SSLCryptoDevice cryptocom
SetEnv RNG VJUGA
SetEnv RNG_PARAMS /dev/ttyUSB0
```

Порядковый № изменения	Подпись лица, ответственного за изменение	Дата внесения изменения

## 7.2.2 Серверное приложение Stunnel

Stunnel ([www.stunnel.org](http://www.stunnel.org)) — небольшое серверное приложение, позволяющее «обернуть» в TLS работу практически любой сетевой программы, использующей протокол TCP. Может быть использован для организации защищенного доступа к почтовым (IMAP4 и POP3) серверам.

Stunnel версии 4.x поддерживает указание динамически подгружаемых модулей в своем конфигурационном файле. Но в коде приложения имеется одно место, где явным образом предполагается использование RSA. Поэтому, если предполагается использование только российских алгоритмов, `stunnel` следует собрать с опцией `-disable-rsa`, либо, если предполагается что один и тот же бинарный файл `stunnel` может быть использован как для российских, так и для международных алгоритмов, в зависимости от указанных в файле конфигурации сертификатов/ключей, заменить в файле `ssl.c` вызов функции `SSL_CTX_use_RSAPrivateKey` на вызов более общей функции `SSL_CTX_use_PrivateKey`.

Следует задать в скрипте запуска `stunnel` переменные среды, определяющие тип ДСЧ.

## 7.2.3 Сервер каталогов OpenLDAP

Пакет OpenLDAP (<http://www.openldap.org>) объединяет в себе сервер, клиентскую библиотеку и ряд утилит для работы с протоколом LDAP.

В конфигурационном файле сервера `FileNameslapd` версии `openldap 2.2.23` не предусмотрено возможности явного указания динамически подключаемого модуля. Разработан патч, который обеспечивает считывание библиотекой `libldap` конфигурационного файла OpenSSL, что решает проблему подгрузки модулей как в серверных, так и клиентских приложениях, использующих библиотеку. Патч может быть загружен с сайта <http://www.cryptocom.ru>.

## 7.3 Клиентские программы

### 7.3.1 Web-браузер lynx

`lynx` — текстовый web-браузер. После пересборки `lynx` с использованием OpenSSL с нашими модификациями позволяет осуществлять доступ к сайтам, использующим российские алгоритмы в HTTPS. Для подключения библиотеки `libcryptocom` использует конфигурационный файл OpenSSL.

### 7.3.2 Программа получения файлов wget

`wget` — неинтерактивная программа получения файлов по протоколам HTTP/HTTPS/FTP/FTPS. Для использования библиотеки `libcryptocom` требуется добавить считывание конфигурационного файла OpenSSL.

### 7.3.3 Почтовый клиент mutt

`mutt` — почтовый клиент. Поддерживает работу с S/MIME посредством вызова внешней утилиты OpenSSL и использование TLS при работе с удаленными IMAP и POP3-серверами. Для использования библиотеки `libcryptocom` при работе с TLS требуется добавить считывание конфигурационного файла OpenSSL. Для использования российских криптоалгоритмов в S/MIME изменения исходных текстов не требуется. В конфигурационном файле необходимо указать

Порядковый № изменения	Подпись лица, ответственного за изменение	Дата внесения изменения

```
set smime_encrypt_with="cipher_alg gost89"
```

## 7.4 Средства разработки

### 7.4.1 tcltls

tcltls — расширение Tcl, позволяющее создавать как клиенты, так и сервера различных TLS-протоколов на языке Tcl. Для поддержки библиотеки libcryptocom необходима либо возможность чтения файла конфигурации OpenSSL, либо возможность явного указания библиотеки. Данная возможность реализуется патчем #1353033 в patch manager на <http://www.sourceforge.net/project/tls>.

Порядковый № изменения	Подпись лица, ответственного за изменение	Дата внесения изменения

## 8 ПРИЛОЖЕНИЯ

### 8.1 Датчики случайных чисел для работы библиотеки libcryptocom

В таблице 1 приведен список датчиков случайных чисел, которые может использовать библиотека libcryptocom. Выбор датчика осуществляется установкой соответствующего значения переменной среды \$RNG. Для некоторых датчиков необходима также установка значения переменной среды \$RNG\_PARAMS.

Значения переменной среды \$RNG и необходимость установки значения переменной среды \$RNG\_PARAMS для каждого из возможных ДСЧ указаны в таблице 1.

Таблица 1  
Датчики случайных чисел, с которыми работает библиотека libcryptocom

№	Название датчика	Значение переменной RNG	Примечание
1.	Программный	PROGRAM	Требует указания файла начального заполнения в переменной RNG_PARAMS. Не может быть использован для создания долговременных ключей.
2.	Системный	SYSTEM	
3.	Клавиатурый	KEYBOARD	Требует взаимодействия с пользователем. Может быть использован только в специальных приложениях, написанных с учетом использования этого датчика.
4.	Аккорд	ACCORD	Аппаратный ДСЧ с платы «Аккорд». Поддерживается под Windows и Linux.
5.	Соболь	SOBOL	Аппаратный ДСЧ с платы «Соболь». Поддерживается под Windows и Linux.
6.	Вьюга	VJUGA	Аппаратный ДСЧ разработки ООО «Криптоком», подключаемый через интерфейс USB. В системах FreeBSD требует указания имени устройства, к которому подключается, в переменной RNG_PARAMS. В системах Solaris не поддерживается.

### 8.2 Названия и параметры алгоритмов

В таблице 2 приведены названия и параметры алгоритмов, которые следует указывать в командной строке в тех случаях, когда команда или опция требуют указания алгоритма и его параметров (например, в качестве аргумента опции `-newkey` команды `openssl req` при создании ключей).

Работа с параметрами алгоритмов в варианте CryptoPro подробно описана в документе RFC 4357. Параметры XA и XB используются для обмена.

Порядковый № изменения	Подпись лица, ответственного за изменение	Дата внесения изменения

Таблица 2  
 Названия и параметры алгоритмов библиотеки libcryptocom

Алгоритм	Название	Поддерживаемые параметры
Подпись ГОСТ Р 34.10-94 вариант Cryptocom	gost94	
Подпись ГОСТ Р 34.10-94 вариант CryptoPro	gost94cp	A,B,C,D
Хэш ГОСТ Р 34.11	md_gost94	
Подпись ГОСТ Р 34.10-2001 вариант Cryptocom	gost2001	
Подпись ГОСТ Р 34.10-2001 вариант Cryptopro	gost2001cp	A,B,C,XA,XB
Шифрование ГОСТ 28147-89 вариант Cryptocom	gost89	cc_cipher_param
Шифрование ГОСТ 28147-89 вариант Cryptopro		cp_cipher_param_a
		cp_cipher_param_b
		cp_cipher_param_c
		cp_cipher_param_d

Порядковый № изменения	Подпись лица, ответственного за изменение	Дата внесения изменения

