

УТВЕРЖДЕН  
СЕИУ.00009-04 34 05 - ЛУ

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

СРЕДСТВО КРИПТОГРАФИЧЕСКОЙ ЗАЩИТЫ ИНФОРМАЦИИ  
«МагПро КриптоПакет» 3.0

**Средство контроля целостности СКЗИ и СФК integrity**  
**Руководство по использованию**

СЕИУ.00009-04 34 05  
Листов 16

Литера О

## Аннотация

Настоящий документ содержит сведения, необходимые для работы со средством контроля целостности СКЗИ и СФК integrity, входящим в состав средства криптографической защиты информации «МагПро КриптоПакет» 3.0.

Авторские права на средство криптографической защиты информации «МагПро КриптоПакет» 3.0 принадлежат ООО «Криптоком».

«МагПро» является зарегистрированным товарным знаком ООО «Криптоком».

## Содержание

<b>1</b>	<b>НАЗНАЧЕНИЕ СРЕДСТВА INTEGRITY</b>	<b>4</b>
<b>2</b>	<b>УСЛОВИЯ ВЫПОЛНЕНИЯ СРЕДСТВА INTEGRITY</b>	<b>5</b>
<b>3</b>	<b>ФУНКЦИИ СРЕДСТВА INTEGRITY</b>	<b>6</b>
3.1	ФУНКЦИИ СРЕДСТВА INTEGRITY НА UNIX-ПОДОБНЫХ ОПЕРАЦИОННЫХ СИСТЕМАХ . . .	6
3.2	ФУНКЦИИ СРЕДСТВА INTEGRITY НА ОПЕРАЦИОННЫХ СИСТЕМАХ СЕМЕЙСТВА WINDOWS	6
<b>4</b>	<b>СОСТАВ СРЕДСТВА INTEGRITY</b>	<b>7</b>
4.1	ПРОГРАММА SKCS (ТОЛЬКО ДЛЯ UNIX-ПОДОБНЫХ ОС) . . . . .	7
4.2	ПРОГРАММА GOST12SUM . . . . .	7
<b>5</b>	<b>УСТАНОВКА И НАСТРОЙКА СРЕДСТВА INTEGRITY</b>	<b>8</b>
<b>6</b>	<b>ИСПОЛЬЗОВАНИЕ СРЕДСТВА INTEGRITY</b>	<b>9</b>
<b>7</b>	<b>ЗАПУСК ПРОГРАММ</b>	<b>10</b>
7.1	ЗАПУСК ПРОГРАММЫ SKCS (ТОЛЬКО ДЛЯ UNIX-ПОДОБНЫХ ОС) . . . . .	10
7.2	ЗАПУСК ПРОГРАММЫ GOST12SUM . . . . .	10
<b>8</b>	<b>ВЫПОЛНЕНИЕ ПРОГРАММ</b>	<b>12</b>
8.1	КОНТРОЛЬНЫЙ РАСЧЕТ ХЭШ-СУММ . . . . .	12
8.1.1	ПРОЦЕДУРА РАСЧЕТА ДЛЯ UNIX-ПОДОБНЫХ ОС . . . . .	12
8.1.2	ПРОЦЕДУРА РАСЧЕТА ДЛЯ ОС СЕМЕЙСТВА WINDOWS . . . . .	12
8.1.3	КОНТРОЛЬНЫЙ ФАЙЛ . . . . .	12
8.1.4	СОХРАНЕНИЕ РЕЗУЛЬТАТОВ РАСЧЕТА И СОЗДАНИЕ КОНТРОЛЬНОГО НОСИТЕЛЯ . .	13
8.2	КОНТРОЛЬ ЦЕЛОСТНОСТИ СКЗИ И СИСТЕМНЫХ ФАЙЛОВ . . . . .	13
<b>9</b>	<b>СООБЩЕНИЯ ОПЕРАТОРУ</b>	<b>14</b>

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

# 1 НАЗНАЧЕНИЕ СРЕДСТВА INTEGRITY

Средство контроля целостности СКЗИ и СФК integrity предназначено для осуществления контроля целостности как программных модулей СКЗИ, так и среды функционирования криптосредства (модулей операционной системы, используемых при работе СКЗИ).

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

## 2 УСЛОВИЯ ВЫПОЛНЕНИЯ СРЕДСТВА INTEGRITY

Средство контроля целостности СКЗИ и СФК integrity предназначено для использования как в среде операционных систем семейства Windows, так и на unix-подобных операционных системах.

В unix-подобных операционных системах средство контроля целостности СКЗИ и СФК integrity может быть использовано в полном объеме, однако для работы программы skcs создания контрольного файла необходимо, чтобы в системе был установлен интерпретатор языка Python версии 2.

В операционных системах семейства Windows возможно использование только входящей в состав средства integrity программы вычисления хэш-векторов файлов gost12sum.

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

## 3 ФУНКЦИИ СРЕДСТВА INTEGRITY

### 3.1 Функции средства integrity на unix-подобных операционных системах

Средство integrity на unix-подобных операционных системах выполняет следующие действия:

1. Выполняет контрольный расчет хэш-сумм по алгоритму ГОСТ Р 34.11-2012:
  - (1) Анализирует исполняемые файлы, указанные в конфигурационном файле, а также их зависимости, с помощью системной утилиты ldd.
  - (2) Объединяет всю полученную информацию в единый список. Для каждого файла из этого списка рассчитывает хэш-функцию.
  - (3) Результаты вычисления хэш-функции сохраняет в контрольном файле. При этом отдельно выводятся хэши для модулей СКЗИ и отдельно — хэши файлов ОС. Такой порядок нужен для удобства сравнение хэшей СКЗИ с зафиксированными в формуляре.
2. Выполняет проверку целостности СКЗИ и СФК:
  - (1) Повторно вычисляет хэш-суммы по алгоритму ГОСТ Р 34.11-2012 всех файлов, указанных в контрольном файле, полученном в результате контрольного расчета хэш-сумм;
  - (2) сравнивает полученные хэш-суммы с содержащимися в контрольном файле.

### 3.2 Функции средства integrity на операционных системах семейства Windows

Средство integrity на операционных системах семейства Windows выполняет следующие действия:

1. Выполняет контрольный расчет хэш-сумм по алгоритму ГОСТ Р 34.11-2012.
2. Выполняет проверку целостности СКЗИ и СФК:
  - (1) Повторно вычисляет хэш-суммы по алгоритму ГОСТ Р 34.11-2012 всех файлов, указанных в контрольном файле, полученном в результате контрольного расчета хэш-сумм;
  - (2) сравнивает полученные хэш-суммы с содержащимися в контрольном файле.

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

## 4 СОСТАВ СРЕДСТВА INTEGRITY

Средство integrity состоит из:

- Программы skcs для создания контрольного файла;
- Программы gost12sum для расчета хэш-сумм по алгоритму ГОСТ Р 34.11-2012.

### 4.1 Программа skcs (только для unix-подобных ОС)

Программа skcs используется для первоначального контрольного расчета хэш-сумм (см. раздел 8.1) и создания контрольного файла.

Программа универсальна для всех Unix-подобных ОС.

### 4.2 Программа gost12sum

В unix-подобных ОС Программа gost12sum используется при работе средства integrity в двух режимах:

1. При первоначальном расчете хэш-сумм программа вызывается программой skcs;
2. При последующем контроле целостности СКЗИ и СФК (см. раздел 8.2) программа запускается пользователем.

В операционных системах семейства Windows программа gost12sum запускается пользователем как при первоначальном расчете хэш-сумм, так и при последующем контроле целостности СКЗИ и СФК (см. 6).

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

## 5 УСТАНОВКА И НАСТРОЙКА СРЕДСТВА INTEGRITY

В соответствии с требованиями безопасности средство integrity не устанавливается на жесткий диск компьютера. Программы, входящие в данное средство, запускаются с внешнего защищенного от записи файлового накопителя (например, непосредственно с дистрибутивного диска).

Средство integrity использует в своей работе конфигурационный файл, описывающий, какие модули СКЗИ входят в дистрибутив «МагПро КриптоПакет» 3.0 для данной операционной системы. Конфигурационный файл формируется поставщиком СКЗИ и записывается на дистрибутивный диск.

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



## 6 ИСПОЛЬЗОВАНИЕ СРЕДСТВА INTEGRITY

При использовании средства integrity следует придерживаться следующего порядка действий:

1. После установки СКЗИ выполнить создание контрольного файла, описывающего состояние как самого СКЗИ, так и используемых им компонентов операционной системы, и сохранить этот файл на съемном носителе (см раздел 8.1). Защитить этот носитель от записи физически. Выполнить ручной контроль целостности файлов СКЗИ путем сличения хэш-сумм в созданном контрольном файле с суммами, приведенными в формуляре СКЗИ.
2. На регулярной основе проводить контроль целостности системы посредством запуска gost12sum с защищенного от записи носителя. (см раздел 8.2)
3. При любых обновлениях программного обеспечения на контролируемой системе (как обновлений СКЗИ, так и обновлений операционной системы), выполнить следующую последовательность действий:
  - (1) Перед установкой обновлений выполнить процедуру контроля целостности системы. (см раздел 8.2)
  - (2) Установить обновления
  - (3) Выполнить заново процедуру создания контрольного файла (см. раздел 8.1).
  - (4) Если устанавливались обновленные версии пакетов СКЗИ выполнить ручной контроль целостности файлов СКЗИ путем сличения хэш-сумм в созданном контрольном файле с суммами, приведенными в формуляре СКЗИ.

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

## 7 ЗАПУСК ПРОГРАММ

В соответствии с требованиями безопасности средство integrity не устанавливается на жесткий диск компьютера. Программы, входящие в данное средство, запускаются с внешнего защищенного от записи файлового накопителя (например, непосредственно с дистрибутивного диска).

Средство integrity имеет командно-строчный интерфейс.

Для запуска программ, входящих в состав средства integrity, необходимо:

1. Подключить внешний защищенный от записи накопитель со средством integrity к компьютеру и смонтировать;
2. Перейти в каталог integrity на смонтированном носителе. Каталог содержит три файла: исполняемые файлы skcs и gost12sum и конфигурационный файл.
3. Набрать в командной строке имя необходимой программы с соответствующими параметрами в зависимости от выполняемой операции и запустить программу нажатием Enter.

**ВНИМАНИЕ!** На unix-подобных ОС имя программы необходимо набирать в формате ./[имя программы], указание текущего каталога перед именем исполняемого файла необходимо, так как установки файлов на жесткий диск не производится.

### 7.1 Запуск программы skcs (только для unix-подобных ОС)

Для запуска программы skcs необходимо набрать в командной строке:

```
./skcs <имя конфигурационного файла средства integrity> <имя контрольного файла>
```

Имя конфигурационного файла необходимо указывать, так как этот файл содержит список файлов СКЗИ, подлежащих обработке.

Контрольный файл — это выходной файл данной программы, в который будут записаны хэш-суммы всех обработанных файлов. Если файла с таким именем не существует, программа создает его при работе. Если файл с таким именем существует, программа его перезаписывает.

Пример запуска программы skcs:

```
./skcs config /tmp/control.out
```

Здесь config — имя конфигурационного файла, а control.out — имя контрольного выходного файла.

При указании имени контрольного файла следует указывать путь до директории, доступной текущему пользователю для записи.

Рекомендуется запускать процедуру создания с правами суперпользователя, так как некоторые файлы, целостность которых следует контролировать, могут быть недоступны для чтения обычному пользователю.

### 7.2 Запуск программы gost12sum

Для запуска программы gost12sum на unix-подобных ОС необходимо набрать в командной строке:

```
./gost12sum [-с имя контрольного файла]
```

Для запуска программы gost12sum на операционных системах семейства Windows необходимо набрать в командной строке:

```
gost12sum [-с имя контрольного файла]
```

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

Здесь:

-с — параметр, указывающий, что контрольный файл необходимо использовать как источник хэш-сумм для проверки.

Пример запуска программы gost12sum:

```
./gost12sum -c control.out
```

Здесь control.out — имя контрольного файла.

Запуск программы gost12sum следует производить от имени того же пользователя, от имени которого создавался контрольный файл.

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

## 8 ВЫПОЛНЕНИЕ ПРОГРАММ

### 8.1 Контрольный расчет хэш-сумм

Для того, чтобы получить возможность периодически выполнять процедуру контроля целостности СКЗИ и СФК, необходимо выполнить контрольный расчет хэш-сумм всех компонентов СКЗИ и СФК сразу же после установки СКЗИ. Впоследствии эту процедуру следует повторять после каждой установки обновлений в системе или СКЗИ.

#### 8.1.1 Процедура расчета для unix-подобных ОС

1. Подключить внешний защищенный от записи файловый накопитель, содержащий средство integrity (например, дистрибутивный диск «МагПро КриптоПакет» 3.0) к компьютеру и смонтировать.
2. Перейти в каталог integrity на смонтированном диске и запустить программу skcs с указанием имен используемого конфигурационного файла и выходного контрольного файла в качестве параметров (описание формата запуска программы skcs см. в разделе 7.1).
3. Во время работы программа выводит сообщения:

Анализируются модули СКЗИ...

Анализируются зависимости...

Вычисляются хэш-суммы...

По окончании работы программа записывает результаты в выходной файл, название которого указано в качестве второго параметра программы. Если такого файла нет, программа его создает; если файл существует, программа его перезаписывает.

По завершении расчета необходимо выполнить ручной контроль файлов СКЗИ путем сличения хэш-сумм в созданном контрольном файле с суммами, приведенными в формуляре СКЗИ.

#### 8.1.2 Процедура расчета для ОС семейства Windows

1. Подключить внешний защищенный от записи файловый накопитель, содержащий средство integrity (например, дистрибутивный диск «МагПро КриптоПакет» 3.0) к компьютеру.
2. Перейти в каталог integrity на смонтированном диске.
3. Путем ручного запуска программы gost12sum (см. раздел 7.2) выполнить формирование файла контрольных сумм в соответствии с описанием формата этого файла (см. раздел 8.1.3). Перечень файлов операционной системы, подлежащих контролю целостности, приведен в «Правилах пользования» СКЗИ «МагПро КриптоПакет» 3.0.

По завершении расчета необходимо выполнить ручной контроль файлов СКЗИ путем сличения хэш-сумм в созданном контрольном файле с суммами, приведенными в формуляре СКЗИ.

#### 8.1.3 Контрольный файл

Контрольный файл представляет собой текстовый файл в кодировке UTF-8.

В контрольном файле приводятся вычисленные хэш-суммы файлов СКЗИ и системных файлов, от которых зависит работа файлов СКЗИ.

Контрольный файл состоит из разделов «Файлы СКЗИ» и «Системные файлы». В разделе «Файлы СКЗИ» перечисляются хэш-суммы файлов, указанных в конфигурационном файле

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

средства integrity. В разделе «Системные файлы» перечисляются хэш-суммы файлов, от которых зависит работа файлов СКЗИ.

В каждой строке файла приводится хэш-сумма файла и полный путь к нему.

В случае если в процессе расчета хэш-сумм файлов возникают ошибки, то в контрольный файл будет добавлен раздел «Файлы, для которых не удалось рассчитать контрольную сумму и причина ошибки.» В этом разделе будут указаны файлы, рассчитать контрольную сумму для которых не удалось и причина ошибки.

#### 8.1.4 Сохранение результатов расчета и создание контрольного носителя

После вычисления контрольных сумм и формирования выходного файла следует немедленно:

1. Скопировать программу gost12sum на жесткий диск;
2. Отмонтировать дистрибутивный диск и отключить его от компьютера;
3. Создать контрольный носитель. Для этого записать выходной файл и программу gost12sum на отчуждаемый носитель.

Требования к контрольному носителю:

- Носитель должен иметь защиту от записи. Это может быть CD-ROM (но не CD-RW) или flash-носитель с аппаратной защитой от записи.
  - В случае записи на CD-ROM носитель должен быть финализирован.
  - Выходной файл и программа gost12sum должны быть записаны в один каталог.
4. Отмонтировать контрольный носитель и отключить от компьютера. Если выполнена запись на flash-носитель, включить аппаратную защиту от записи.
  5. Поместить носитель с записью в сейф.
  6. Удалить с жесткого диска выходной файл и программу gost12sum.

## 8.2 Контроль целостности СКЗИ и системных файлов

Для последующего контроля целостности СКЗИ и системных файлов необходимо:

1. Подключить к компьютеру и смонтировать контрольный носитель.
2. Перейти в каталог, в котором содержатся контрольный файл и программа gost12sum.
3. Запустить программу gost12sum (описание формата запуска программы gost12sum см. в разделе 7.2).

Программа gost12sum выполняет расчет хэш-суммы каждого файла, указанного в контрольном файле, и сравнивает с хэш-суммой соответствующего файла, указанной в контрольном файле.

Если все хэш-суммы совпадают, программа заканчивает работу.

Если какие-то хэш-суммы не совпадают, программа для каждого несовпадения выводит сообщение вида:

```
./gost12sum: GOST hash sum check failed for '/usr/bin/file'
```

В конце работы программа сообщает общее количество измененных файлов:

```
./gost12sum: WARNING 3 of 2436 file(s) failed GOST hash sum check
```

В случае наличия таких сообщений СКЗИ или СФК признается скомпрометированной. Необходимо произвести переустановку СКЗИ или соответствующих системных пакетов с заведомо корректного дистрибутивного диска. После этого необходимо сразу же выполнить процедуру контрольного расчета хэш-сумм и создать новый контрольный файл (см. раздел 8.1).

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

## 9 СООБЩЕНИЯ ОПЕРАТОРУ

Сообщение	Причина возникновения	Рекомендуемые действия
<b>Сообщения при запуске программы skcs</b>		
Ошибка при работе с конфигурационным файлом.	При запуске программы skcs указан некорректный конфигурационный файл	При следующем запуске программы указать корректный конфигурационный файл
couldn't open [имя выходного файла]: permission denied	Попытка создать выходной файл в каталоге, защищенном от записи (в каталоге, в котором данный пользователь не имеет права записи)	При следующем запуске программы skcs создать выходной файл в каталоге, не защищенном от записи (в каталоге, в котором данный пользователь имеет право записи)
Использование: ./skcs файл-конфигурации выходной-файл	Некорректный формат запуска программы (не указан один из параметров или оба)	Запустить программу в корректном формате
<b>Сообщения при запуске программы gost12sum</b>		
./gost12sum: GOST hash sum check failed for [имя файла]	Вычисленная контрольная сумма не совпадает с содержащейся в контрольном файле. Целостность СКЗИ или СФК нарушена	Произвести переустановку СКЗИ или соответствующих системных пакетов с заведомо корректного дистрибутивного диска. После переустановки немедленно произвести процедуру контрольного расчета хэш-сумм и создания контрольного носителя (см. раздел 8.1).
./gost12sum: WARNING [число] of [число] file(s) failed GOST hash sum check	Контрольные суммы указанного количества проверенных файлов не совпадают с содержащимися в контрольном файле. Целостность СКЗИ или СФК нарушена	Произвести переустановку СКЗИ или соответствующих системных пакетов с заведомо корректного дистрибутивного диска. После переустановки немедленно произвести процедуру контрольного расчета хэш-сумм и создания контрольного носителя (см. раздел 8.1).
Программа выводит хэш-сумму контрольного файла	Программа запущена без указания параметра -с	Запустить программу с указанием параметра -с
Программа указывает все файлы как некорректные	СКЗИ и СФК искажены полностью	Провести полное восстановление СКЗИ и СФК
	Контрольный файл был создан до установки обновлений СКЗИ или СФК	Считать СКЗИ или СФК скомпрометированным и произвести переустановку СКЗИ или соответствующих системных пакетов с заведомо корректного дистрибутивного диска. После переустановки немедленно произвести процедуру контрольного расчета хэш-сумм и создания контрольного носителя (см. раздел 8.1).

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

Сообщение	Причина возникновения	Рекомендуемые действия
	В случае наличия более одного компьютера — возможно, использован контрольный файл, созданный на другом компьютере.	Провести перерасчет с использованием контрольного файла, созданного на данном компьютере.
[имя файла]No such file or directory ./gost12sum: WARNING [число] of [число] file(s) cannot be processed ()	Контрольный файл был создан до установки обновлений СКЗИ или СФК  В случае наличия более одного компьютера — возможно, использован контрольный файл, созданный на другом компьютере.	Считать СКЗИ или СФК скомпрометированным и произвести переустановку СКЗИ или соответствующих системных пакетов с заведомо корректного дистрибутивного диска. После переустановки немедленно произвести процедуру контрольного расчета хэш-сумм и создания контрольного носителя (см. раздел 8.1).  Провести перерасчет с использованием контрольного файла, созданного на данном компьютере.

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

Изм.	Номера листов (страниц)				Всего листов (страниц) в докум.	№ документа	Входящий сопроводительного докум. и дата	Подпись	Дата
	измененных	замененных	новых	аннулированных					

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