УТВЕРЖДЕН
СЕИУ.00009-02 34 05 - ЛУ

СРЕДСТВО КРИПТОГРАФИЧЕСКОЙ ЗАЩИТЫ ИНФОРМАЦИИ
«МагПро КриптоПакет» в. 2.0

Средство контроля целостности СКЗИ и СФК integrity

Руководство оператора

СЕИУ.00009-02 34 05
Листов 14

Литера О

2011

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

Аннотация

Настоящий документ содержит сведения, необходимые оператору для работы со средством контроля целостности СКЗИ и СФК integrity.

Содержание

1 НАЗНАЧЕНИЕ СРЕДСТВА integrity 4

2 СОСТАВ СРЕДСТВА integrity 6
2.1 Программа skcs 6
2.2 Программа gostsum 6
2.3 Конфигурационный файл 6

3 ИСПОЛЬЗОВАНИЕ СРЕДСТВА INTEGRITY 7

4 ЗАПУСК ПРОГРАММ 8
4.1 Запуск программы skcs 8
4.2 Запуск программы gostsum 8

5 ВЫПОЛНЕНИЕ ПРОГРАММ 10
5.1 Контрольный расчет хэш-сумм 10
5.1.1 Процедура расчета 10
5.1.2 Контрольный файл 10
5.1.3 Сохранение результатов расчета и создание контрольного носителя 10
5.2 Контроль целостности СКЗИ и системных файлов 11

6 СООБЩЕНИЯ ОПЕРАТОРУ 12

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).

Средство контроля целостности СКЗИ и СФК integrity может быть использовано в следующих операционных системах:

- Семейство Linux:
  - Debian GNU/Linux etch/lenny/squeeze
  - AltLinux 4.0, 5.0, Кольчуга
  - Red Hat Enterprise Linux 4, 5, 6
  - Fedora 11, 12, 13
  - CentOS 4, 5
  - SUSE Linux 10, 11
  - ASP Linux 12, 14
  - ASP Linux Server IV, V
  - Mandriva PowerPack 2008.1, 2009.1, 2010.1
  - Mandriva Flash 2008.1, 2009.1, 2010.1
  - Mandriva Corporate Server 4 update 3, 5
  - Ubuntu 8.04, 9.04, 10.04
  - МСВСфера 5.2, 5.4
- FreeBSD 6.x, 7.x, 8.x, 9.x
- Sun Solaris 9, 10

Для контроля целостности СКЗИ и СФК в операционной системе Windows может быть использована программа контроля целостности файлов calchash.

Средство integrity выполняет следующие действия:

1. Выполняет контрольный расчет хэш-сумм:
   (1) Запрашивает у менеджера пакетов, какие пакеты из состава СКЗИ были установлены в данной системе и в какие каталоги они были установлены.
   (2) На основании информации о том, какие модули СКЗИ устанавливает каждый пакет, указанной в конфигурационном файле, а также полученной в результате выполнения предыдущего действия, формирует список полных путей к файлам СКЗИ, установленным в системе.
   (3) Для каждого модуля СКЗИ с помощью системной утилиты ldd формирует список системных модулей, влияющих на работу СКЗИ.
   (4) Получает от пакетного менеджера информацию о пакетах, от которых зависят пакеты СКЗИ, и полные списки файлов, входящих в эти пакеты.
   (5) Объединяет всю полученную информацию в единый список. Для каждого файла из этого списка рассчитывает хэш-функцию.
   (6) Результаты вычисления хэш-функции сохраняет в контрольном файле. При этом отдельно выводятся хэши для модулей СКЗИ и отлельно — хэши файлов ОС. Такой порядок нужен для удобства сравнение хэшей СКЗИ с зафиксированными в формуляре.
2. Выполняет проверку целостности СКЗИ и СФК:

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

(1) Повторно вычисляет хэш-суммы всех файлов, указанных в контрольном файле, полученном в результате контрольного расчета хэш-сумм;
(2) сравнивает полученные хэш-сумм с содержащимися в контрольном файле.

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

2 СОСТАВ СРЕДСТВА integrity

Средство integrity состоит из:

- Программы создания контрольного файла skcs;
- Программы расчета хэш-сумм по алгоритму ГОСТ gostsum;
- Конфигурационного файла.

2.1 Программа skcs

Программа skcs используется для первоначального контрольного расчета хэш-сумм (см. раздел 5.1) и создания контрольного файла.

Программа универсальна для всех Unix-подобных ОС.

2.2 Программа gostsum

Программа gostsum используется при работе средства integrity в двух режимах:

1. При первоначальном контрольном расчете хэш-сумм программа вызывается программой skcs;
2. При последующем контроле целостности СКЗИ и СФК (см. раздел 5.2) программа запускается пользователем.

Программа gostsum существует в нескольких вариантах, соответствующих различным Unix-подобным ОС.

У программы gostsum также есть ряд других режимов работы, которые не используются при работе средства integrity.

2.3 Конфигурационный файл

Конфигурационный файл средства integrity состоит из секций, каждая из которых соответствует одному из пакетов дистрибутива «МагПро КриптоПакет» в. 2.0 для данной операционной системы. Поэтому конфигурационный файл существует в нескольких вариантах, соответствующих различным Unix-подобным ОС.

В каждой секции перечислены файлы «МагПро КриптоПакет» в. 2.0, входящие в соответствующий пакет.

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

3 ИСПОЛЬЗОВАНИЕ СРЕДСТВА INTEGRITY

Для использования средства integrity для контроля целостности операционной системы, следует выполнять следующий порядок 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 5.1). Защитить этот носитель от записи физически.
2. На регулярной основе проводить контроль целостности системы посредством запуска gostsum с защищенного от записи носителя. (см раздел 5.2)
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 5.2)
   (2) Установить обновления
   (3) Выполнить заново процедуру создания контрольного файла (см. раздел 5.1).
   (4) Если устанавливались обновленные версии пакетов СКЗИ выполнить ручной контроль файлов СКЗИ путем сличения хэщ-сумм в созданном контрольном файле с суммами, приведенными в формуляре СКЗИ.

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

4 ЗАПУСК ПРОГРАММ

В соответствии с требованиями безопасности средство integrity не устанавливается на жесткий диск компьютера. Программы, входящие в данное средство, запускаются непосредственно с дистрибутивного диска.

Средство integrity имеет командно-строчный интерфейс.

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

1. Подключить дистрибутивный носитель (CD-ROM) к компьютеру и смонтировать;
2. Перейти в каталог integrity на смонтированном носителе. Каталог содержит три файла: исполняемые файлы skcs и gostsum и конфигурационный файл.
3. Набрать в командной строке имя необходимой программы в формате ./[имя программы] с соответствующими параметрами в зависимости от выполняемой операции и запустить программу нажатием Enter.
   ВНИМАНИЕ. Указание текущего каталога перед именем исполняемого файла необходимо, так как установки файлов на жесткий диск не производится.

4.1 Запуск программы skcs

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.

4.2 Запуск программы gostsum

Для запуска программы gostsum необходимо набрать в командной строке:

```
./gostsum -t -c [имя контрольного файла]
```

Здесь:

-t — параметр, определяющий использование тестовых параметров алгоритма шифрования ГОСТ (для совместимости с программой CALCHASH, которая использует при вычислении хэш-сумм именно этот набор параметров).

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

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

Пример запуска программы gostsum:

```
./gostsum -t -c control.out
```

Здесь control.out — имя контрольного файла.

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

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

5 ВЫПОЛНЕНИЕ ПРОГРАММ

5.1 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.

5.1.1 Процедура расчета

1. Подключить дистрибутивный диск «МагПро КриптоПакет» в. 2.0 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 4.1).
3. Во время работы программа выводит сообщения:

   ```
   Анализируются пакеты СКЗИ..
   Анализируются зависимости 20 пакетов
   Вычисляются хэш-суммы
   ```

   Количество пакетов в различных операционных системах может быть различным (пример приведен для Debian Linux).
   Во время вычисления хэш-сумм демонстрируется прогресс-бар, показывающий степень завершенности процесса.
   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.

5.1.2 Контрольный файл

Контольный 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 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.

5.1.3 Сохранение результатов расчета и создание контрольного носителя

После вычисления контрольных сумм и формирования выходного файла следует немедленно:

1. Скопировать программу gostsum на жесткий диск;
2. Отмонтировать дистрибутивный диск и отключить его от компьютера;

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

3. Создать контрольный носитель. Для этого записать выходной файл и программу gostsum 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 gostsum 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 gostsum.

5.2 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 gostsum.
3. Запустить программу gostsum (описание формата запуска программы gostsum см. в разделе 4.2).

Программа gostsum 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:

/tt ./gostsum: GOST hash sum check failed for '/usr/bin/file'

В конце работы программа сообщает общее количество измененных файлов:

/tt ./gostsum: 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 5.1).

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

6 СООБЩЕНИЯ ОПЕРАТОРУ

Сообщение	Причина возникновения	Рекомендуемые действия
Сообщения при запуске программы skcs		
Invalid syntax of configuration file	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
Сообщения при запуске программы gostsum		
./gostsum: 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 5.1).
./gostsum: 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 5.1).
Программа выводит хэш-сумму контрольного файла	Программа запущена без указания параметра -c	Запустить программу с указанием параметра -c
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 5.1).

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 ./gostsum: WARNING [число] of [число] file(s) cannot be processed ()	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 5.1).
	В случае наличия более одного компьютера — возможно, использован контрольный файл, созданный на другом компьютере.	Провести перерасчет с использованием контрольного файла, созданного на данном компьютере.

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

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

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