

ЗАО «Сигнал-КОМ»

УТВЕРЖДЕН
ШКНР.00046-01 90 05-ЛУ

СРЕДСТВО КРИПТОГРАФИЧЕСКОЙ ЗАЩИТЫ ИНФОРМАЦИИ
«Крипто-КОМ 3.4»

ПРОГРАМНОЕ ОБЕСПЕЧЕНИЕ КОНТРОЛЯ ЦЕЛОСТНОСТИ
РУКОВОДСТВО ПОЛЬЗОВАТЕЛЯ

ШКНР.00046-01 90 05

Листов 9

2017

АННОТАЦИЯ

Данный документ содержит руководство по использованию утилиты *rush*, предназначенной для контроля целостности состава прикладного программного обеспечения средств криптографической защиты информации (СКЗИ) «Крипто-КОМ 3.4».

Контроль целостности, выполняемый с помощью утилиты *rush*, обеспечивается за счет вычисления значений хэш-функции для контролируемых файлов и сравнения полученных значений с заранее вычисленными эталонными значениями.

Утилита контроля целостности входит в комплект поставки библиотеки криптографических преобразований «Крипто-КОМ 3.4».

СОДЕРЖАНИЕ

Аннотация	2
Содержание	3
1. Общие сведения	4
2. Описание применения	5
2.1. Вычисление контрольных сумм	5
2.2. Контроль целостности файлов	5
3. Регистрационная карточка контролируемых файлов	7
Приложение. Список объектов контроля целостности	8
Литература	9

1. ОБЩИЕ СВЕДЕНИЯ

СКЗИ «Крипто-КОМ 3.4» включает средство контроля целостности, выполненное в виде утилиты *rush*. Утилита *rush* обеспечивает вычисление значений хэш-функции для произвольных файлов с использованием алгоритмов ГОСТ Р 34.11-94 ([1]), ГОСТ Р 34.11-2012 [2].

Утилита *rush* представляет собой консольное приложение, т.е. осуществляет печать выходных данных в стандартный вывод.

2. ОПИСАНИЕ ПРИМЕНЕНИЯ

Запуск утилиты *rush* производится из командной строки.

При этом предусмотрено два режима работы:

- режим вычисления контрольных сумм;
- режим контроля целостности файлов.

2.1. Вычисление контрольных сумм

Формат запуска утилиты при вычислении контрольных сумм имеет следующий вид:

rush [-a|-t|-stribog256|-stribog512] [-r] [<file>|<dir>|-l <list>] ...

где

- file** - имя файла;
- dir** - имя каталога; при этом обработке подлежат все файлы, содержащиеся в указанном каталоге;
- r** - обрабатывать каталоги рекурсивно;
- list** - имя файла, содержащего список файлов и каталогов, подлежащих контролю; каждое имя файла или каталога приводится в отдельной строке; пустые строки, а также строки, начинающиеся с символа '#', игнорируются;
- a** - использовать для ГОСТ Р 34.11-94 узлы замены блока подстановки id-GostR3411-94-CryptoProParamSet;
- t** - использовать для ГОСТ Р 34.11-94 тестовые узлы замены блока подстановки;
- stribog256** - использовать ГОСТ Р 34.11-2012 (256 бит) [2];
- stribog512** - использовать ГОСТ Р 34.11-2012 (512 бит) [2].

Результат работы *rush* выводится на консоль построчно - число строк равно числу контролируемых файлов, задаваемых при запуске утилиты. В каждой строке указывается имя файла и вычисленное значение хэш-функции, например:

rush ccom.dll rush.exe wipe.exe

GOSTH (ccom.dll) = fc0a137f254c32154260e18f9e9ddad520eed9cfc4d9cacb40a6dc3462241245

GOSTH (rush.exe) = 89fc70e4fc5fca6fd449435fa375ac6fc1efa2327ac83933d869430417ec1d70

GOSTH (wipe.exe) = fac06409fe496a7796e0a175542a77f1df4555d9af358b483b9cfcd95fc2df36

При необходимости результаты работы утилиты могут быть сохранены в отдельном файле (регистрационный файл), для которого также с помощью *rush* может быть вычислена хэш-функция:

rush ccom.dll rush.exe wipe.exe > etalon.crc

2.2. Контроль целостности файлов

В процессе эксплуатации ПО СКЗИ пользователь, с помощью утилиты *rush*, должен периодически вычислять значения хэш-функции для контролируемых файлов и полученные значения сравнивать с эталонными. Эталонные значения вычисляются поставщиком ПО, либо вычисляются самим пользователем и сохраняются в регистрационном файле (см.п. 2.1).

Формат запуска утилиты в режиме контроля целостности файлов имеет следующий вид:

rush [-a|-t] -c <list> ...

где

- list** - имя файла, содержащего список подлежащих контролю объектов, а также их контрольные суммы¹; каждое имя файла или каталога в списке приводится в отдельной строке; пустые строки, а также строки, начинающиеся с символа '#', игнорируются;
- a** - использовать для ГОСТ Р 34.11-94 узлы замены блока подстановки id-GostR3411-94-CryptoProParamSet;
- t** - использовать для ГОСТ Р 34.11-94 тестовые узлы замены блока подстановки.

Выбор алгоритма хэширования осуществляется в режиме контроля целостности автоматически.

Для каждого файла выводится его имя и результат проверки, например:

rush -c etalon.crc

```
ccom.dll: ok  
rush.exe: ok  
wipe.exe: ok  
valid:3 errors:0
```

Если все файлы успешно проверены, *rush* возвращает код 0, в противном случае – 255.

¹ Формат данных регистрационного файла соответствует формату вывода утилиты *rush* в режиме вычисления контрольных сумм.

3. РЕГИСТРАЦИОННАЯ КАРТОЧКА КОНТРОЛИРУЕМЫХ ФАЙЛОВ

Эталонные значения хэш-функции для контролируемых файлов ПО СКЗИ вычисляются администратором безопасности и передаются на регистрационной карточке вместе с комплектом ПО СКЗИ.

Регистрационная карточка представляет собой файл или его бумажную копию, которые содержат:

- название продукта и номер версии;
- список контролируемых файлов;
- эталонное значение хэш-функции для каждого из файлов списка.

В качестве примера ниже приводится содержимое текстового файла регистрационной карточки с перечнем контролируемых файлов:

РЕГИСТРАЦИОННАЯ КАРТОЧКА контролируемых файлов

СКЗИ «Крипто-КОМ 3.4»

GOSTH (ccom.dll) = fc0a137f254c32154260e18f9e9ddad520eed9cfc4d9cacb40a6dc3462241245

GOSTH (rush.exe) = 89fc70e4fc5fca6fd449435fa375ac6fc1efa2327ac83933d869430417ec1d70

GOSTH (wipe.exe) = fac06409fe496a7796e0a175542a77f1df4555d9af358b483b9cfd95fc2df36

Дата

Подпись

ПРИЛОЖЕНИЕ. СПИСОК ОБЪЕКТОВ КОНТРОЛЯ ЦЕЛОСТНОСТИ

В настоящем приложении приводятся списки объектов, целостность которых должна контролироваться пользователем в процессе эксплуатации ПО СКЗИ.

Для операционных систем Windows:

- все динамические библиотеки, входящие в состав СКЗИ «Крипто-КОМ 3.4» (в соответствии с формуляром);
- все исполняемые модули и динамические библиотеки, использующие СКЗИ «Крипто-КОМ 3.4» в динамической либо статической компоновке;
- файлы операционной системы (файлы с расширениями .dll, .sys, .exe, размещенные в каталоге %SystemRoot% и его подкаталогах).

Для операционной системы Linux/FreeBSD/Solaris:

- все разделяемые библиотеки, входящие в состав СКЗИ «Крипто-КОМ 3.4» (в соответствии с формуляром);
- все исполняемые модули и разделяемые библиотеки, использующие СКЗИ «Крипто-КОМ 3.4» в динамической либо статической компоновке;
- файлы операционной системы (т.е. содержимое каталогов /boot, /dev, /etc и их подкаталогов).

ЛИТЕРАТУРА

1. ГОСТ Р 34.11-94. Государственный стандарт Российской Федерации. Информационная технология. Криптографическая защита информации. Функция хеширования.
2. ГОСТ Р 34.11-2012. Государственный стандарт Российской Федерации. Информационная технология. Криптографическая защита информации. Функция хеширования.
3. СКЗИ «Крипто-КОМ 3.4». Формуляр.