ЗАО «Сигнал-КОМ»

УТВЕРЖДЕН
ШКНР.00035-07 90 04-ЛУ

СРЕДСТВО КРИПТОГРАФИЧЕСКОЙ ЗАЩИТЫ ИНФОРМАЦИИ «Крипто-КОМ 3.3»

ПРОГРАММНОЕ ОБЕСПЕЧЕНИЕ КОНТРОЛЯ ЦЕЛОСТНОСТИ РУКОВОДСТВО ПОЛЬЗОВАТЕЛЯ

ШКНР.00035-07 90 04

Страниц 7

2012 г.

АННОТАЦИЯ

Данный документ содержит руководство по использованию утилиты *rush*, предназначенной для контроля целостности состава прикладного программного обеспечения средств криптографической защиты информации (СКЗИ) «Крипто-КОМ 3.3».

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 3.3».

СОДЕРЖАНИЕ

1. Общие сведения

СКЗИ «Крипто-КОМ 3.3» включает средство контроля целостности, выполненное в виде утилиты *rush.* Утилита *rush* обеспечивает вычисление значений хэш-функции для произвольных файлов с использованием алгоритма ГОСТ Р 34.11-94 ([1]).

Максимальный размер обрабатываемых файлов – 2 Гб.

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

2. Работа с утилитой rush

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] [<file>] [[-r] <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 блок подстановки GostR3411-94-CryptoProParamSet

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] -c <list> …

где

list - имя файла, содержащего список подлежащих контролю объектов, а также их контрольные суммы[1]; каждое имя файла или каталога в списке приводится в отдельной строке; пустые строки, а также строки, начинающиеся с символа ‘#’, игнорируются;

-a - использовать блок подстановки GostR3411-94-CryptoProParamSet.

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.

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 3.3»

GOSTH (ccom.dll) = fc0a137f254c32154260e18f9e9ddad520eed9cfc4d9cacb40a6dc3462241245
GOSTH (rush.exe) = 89fc70e4fc5fca6fd449435fa375ac6fc1efa2327ac83933d869430417ec1d70
GOSTH (wipe.exe) = fac06409fe496a7796e0a175542a77f1df4555d9af358b483b9cfcd95fc2df36

Дата

Подпись

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

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 2000/XP/2003/Vista/2008/7/2008 R2:

- динамическая библиотека ccom.dll (если есть);
- все исполняемые модули и динамические библиотеки, использующие СКЗИ «Крипто-КОМ 3.3» 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:

- разделяемая библиотека libccom.so (если есть);
- все исполняемые модули и разделяемые библиотеки, использующие СКЗИ «Крипто-КОМ 3.3» в динамической либо статической компоновке;
- файлы операционной системы (т.е. содержимое каталогов /boot, /dev, /etc и их подкаталогов).

Для операционной системы Solaris:

- разделяемая библиотека libccom.so (если есть);
- все исполняемые модули и разделяемые библиотеки, использующие СКЗИ «Крипто-КОМ 3.3» в динамической либо статической компоновке;
- файлы операционной системы (т.е. содержимое каталогов /kernel, /dev, /etc и их подкаталогов).

Для операционной системы FreeBSD:

- разделяемая библиотека libccom.so (если есть);
- все исполняемые модули и разделяемые библиотеки, использующие СКЗИ «Крипто-КОМ 3.3» в динамической либо статической компоновке;
- файлы операционной системы (т.е. файл /kernel, а также содержимое каталогов /modules, /dev, /etc и их подкаталогов).

Для операционных систем Windows Mobile 2003/5.0/6.0:

- динамическая библиотека ccom.dll (если есть);
- все исполняемые модули и динамические библиотеки, использующие СКЗИ «Крипто-КОМ 3.3» в динамической либо статической компоновке;
- файлы операционной системы (т.е. содержимое каталога %SystemRoot% и его подкаталогов).

Литература

1. ГОСТ Р 34.11-94. Государственный стандарт Российской Федерации. Информационная технология. Криптографическая защита информации. Функция хеширования.
2. СКЗИ «Крипто-КОМ 3.3». Формуляр.