Хеш-функция - преобразование по определённому алгоритму входного массива данных произвольной длины в выходную битовую строку фиксированной длины.

Контроль целостности, выполняется с помощью утилиты rush. При этом вычисляются значения хэш-функции для контролируемых файлов, и полученные значения сравниваются с заранее вычисленными эталонными значениями.

1. 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.

1.1. 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

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

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 > etalon.crc

1.2. Контроль целостности файлов

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.

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

2. 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).

3. Эталонные значения контрольных сумм файлов СКЗИ «Крипто-КОМ 3.3»

Имя файла	Контрольная сумма GOSTH
Утилита контроля целостности (rush), утилита для удаления файлов (wipe)	
Для операционных систем Windows (x86, 32, 64 бит)	
rush.exe	df26b8899f909b7161f82c8b20d8b87f3d2b38b1f00fd3c654cfe33c8479ce4f
wipe.exe	aaef5e00c8638fc7de0b39ee68270b93f9e8ce77dc741babbf485b150bf1b7b6
Для операционных систем Linux (x86, 32 бит)	
rush	7b501e5e3fee1b67b38d01b8e5e48cb9f13d7f72fa1a7037be25c553cf55d964
wipe	f2166bd034a9774f522c91b38ecd7eee58c88193590a81eb02d64f1f3939d102
Для операционных систем Linux (x86, 64 бит)	
rush	b444a21b9e4e9d9df39c6d875c8c6c0cf28f3c1f5dd966df5b11f5393ddbcbeb
wipe	29e0e027adae7b1bfab52da64d11853f6247a8f3f343fd19b52572dd17d85a01
Модуль СКЗИ «Крипто-КОМ-3.3»	
Для операционных систем Windows (x86, 32 бит)	
ccom.dll	a939d4ea46ddbfd7e0ba88571c18cd3d83eb4d746997eefc20f67b8515bbbddc
ccom.dll.sig	61aa406ed76b715adac6f5820425e614401abffd2717dab5ec87b33bea44ac32
ibank2ccom.dll	f8ba85312d26e05a933a2ed010de45c3ee59753059e0a24fdcb58479ebd0a364
Для операционных систем Windows (x86,64 бит)	
ccom.dll	3a640cd9d0c07766df455983f39b1682fefdff9de7985d546ff2946a2bb65977
ccom.dll.sig	49f1d4f8da53f828ca25291fcdd4bf41ecae7fb4346c0abf6155b513a3df35fe
ibank2ccom.dll	4639f7f56612338a5b73c4d893bbbe18eb9dc9e8aac06cf12e0fb4df7125a2b3
Для операционных систем Linux (x86, 32 бит)	
libccom.so	64c54e404e73bce7e6360af35281bbdc6e571e1ab15c6fd31423f449c7658bf1
libccom.so.sig	1bb4d9ea9baa6f6a39c9377ed0e7d4a3adcfee08ca1fef8c655fd3ad77eb8f44
Iibibank2ccom.so	cea797d5fee5f6dfed95dea1aab4bdfa869e9b21a807c8c0bd20a4bb0cca7120
Для операционных систем Linux (x86, 64 бит)	

libccom.so	c95a2a5d28535e8862004f445f158c71af75bb898f8f982b74bc78d6d4b605ef
libccom.so.sig	997492e2ecb71a11b3672a6ac38e8750f264a6e6d6d97838e4aa0d688e0a60d1
libibank2ccom.so	739bb6ed80d7d84bc3f9125a331733cf230696512b3305d866cba43e6bfa9e53