Инструкция по контролю целостности
СКЗИ «Крипто-КОМ 3.4» и его среды исполнения

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|-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 блок подстановки 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);

-stribog512 - использовать ГОСТ Р 34.11-2012 (512 бит).

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|-t] -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 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.

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:

- 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).

3. Эталонные значения контрольных сумм файлов СКЗИ «Крипто-КОМ 3.4»

Имя файла	Контрольная сумма GOSTH
Утилита контроля целостности (rush), утилита для удаления файлов (wipe)	
Для операционных систем Windows (x86, 32, бит)	
rush.exe	3ad3af146161708cd5f67374ff0eece9933c67a1461144cd34fd3503e37b073f
wipe.exe	aaef5e00c8638fc7de0b39ee68270b93f9e8ce77dc741babbf485b150bf1b7b6
Для операционных систем Windows (x86, 64 бит)	
rush.exe	8bb7e72267ed2dd4425b575a9b02efc45430592b42cdd99751ec881c7fda51c1
wipe.exe	e658d524316c209c2ca737177c3d361160d1131695361fd3c897592c321b212a
Для операционных систем Linux (x86, 32 бит)	
rush	227449ae1a7423446324fd0225f7e1b379cbea47cabe7a76651db5199334ee40
wipe	fb59e6fb8c1710303bbc76cd6843541366a796fbfaa6e6ed97d4f68d2333f64b
Для операционных систем Linux (x86, 64 бит)	
rush	a6137f6d2499a05fef6ae45846fbf6b77caa270160cd2990bacd04361d6907b1
wipe	d51887758e86f67327b9ae16a2cdff0d31d20144a4609ac7b254dcff68c31ac3
Модуль СКЗИ «Крипто-КОМ-3.4»	
Для операционных систем Windows (x86, 32 бит)	
ccom.dll	cd10c3adbafa335ac373fe153d2a8d817171e9e950d993c2f618a9f380730d1b
ccom.dll.sig	61186ad52202c134390b122e2479465c0ec8ca98afc2dc936b811421698e27e9
ibank2ccom.dll	3de5cb5eeaa1e3b2c586aa8fe587adffed0ccbbeda1a672994a20b26a2560221
Для операционных систем Windows (x86,64 бит)	
ccom.dll	50970aec5457cc7585a6f1267df500619ee6cdd9f74adb6e249f4063ca95df7b
ccom.dll.sig	acf3122792ff24a78afde2b00ef9c90da4b04b8aa9b37655268ce5273c512fad
ibank2ccom.dll	e8250200b96a8292b9a9938f8a1dc4e04a2452e7751de5cda7e86ffbf1f059dc
Для операционных систем Linux (x86, 32 бит)	
libccom.so	90943531fbe7354537cf1ec62d1a2aebab19aa03cb5b8ed08bcccff5743eb164
libccom.so.sig	6a77cb008259aeba13de3e4526095d75d1d44862942f1849a0b421f9c6ff6d89
Iibibank2ccom.so	123f4902f985dfac7997fecab54829a751dafdb70adea50fb4e739b7a67605fc
Для операционных систем Linux (x86, 64 бит)	
libccom.so	0df37275f534cfb7ee27258dc2efcac21fb65350473eeec8ee3f90d99372de61
libccom.so.sig	cf8f7d4f335b37c11208e2a65a58b7943aaf5c59c7ffd0037ddcc05627be21d8
libibank2ccom.so	1c846f12ad654667215b8d0eda4c5deb63e3a3893a5361b5965de5b7f62ac5a6