АО «СИГНАЛ-КОМ»

СРЕДСТВО КРИПТОГРАФИЧЕСКОЙ ЗАЩИТЫ ИНФОРМАЦИИ «Крипто-КОМ 3.5»

ПРОГРАММНОЕ ОБЕСПЕЧЕНИЕ РЕГЛАМЕНТНОГО КОНТРОЛЯ ДСЧ
Руководство оператора

ШКНР.00064-01 34 03

Листов 8

2022

ШКНР.00064-01 34 03

АННОТАЦИЯ

Данный документ содержит руководство по использованию утилиты *ccrandreg*, предназначенной для проведения регламентного контроля биологического датчика случайных чисел (БДСЧ) и программного датчика случайных чисел (ПДСЧ) средства криптографической защиты информации (СКЗИ) «Крипто-КОМ 3.5» (варианты исполнения 1, 2).

Регламентный контроль ДСЧ, выполняемый с помощью утилиты *ccrandreg*, обеспечивается за счёт проведения группы статистических тестов выходной последовательности ПДСЧ и БДСЧ с выводом результата об успешности прохождения всей группы тестов.

Утилита регламентного контроля ДСЧ входит в комплект поставки библиотеки криптографических преобразований «Крипто-КОМ 3.5» (варианты исполнения 1, 2).

СОДЕРЖАНИЕ

1. НАЗНАЧЕНИЕ ПРОГРАММЫ

СКЗИ «Крипто-КОМ 3.5» (варианты исполнения 1, 2) включает утилиту *ccrandreg*, предназначенную для проведения регламентного контроля ПДСЧ и БДСЧ, входящих в комплект поставки библиотеки криптографических преобразований «Крипто-КОМ 3.5» (варианты исполнения 1, 2). Регламентный контроль обеспечивается за счёт проведения группы статистических тестов NIST STS [3] на выходной последовательности ПДСЧ (для 1000000 бит) и БДСЧ (для 260 или более бит) с выводом результата об успешности прохождения группы всех тестов, применимых к данной длине последовательности.

Утилита позволяет провести проверку: отдельно модуля БДСЧ; ПДСЧ, инициализированный сохраненным ранее вектором состояния ПДСЧ; ПДСЧ, инициализированный методом инициализации по умолчанию в СКЗИ (см. раздел «Инициализация датчика случайных чисел» в Руководстве программиста ШКНР.00064-01 33 01 [2]).

2. УСЛОВИЯ ВЫПОЛНЕНИЯ ПРОГРАММЫ

Утилита *ccrandreg* представляет собой консольное приложение, т.е. осуществляет печать выходных данных в стандартный вывод. Для работы тестов в путях поиска динамических библиотек утилиты должны располагаться модули (динамические библиотеки) *scbrng* и *ccom*.

3. ВЫПОЛНЕНИЕ ПРОГРАММЫ

Запуск утилиты *ccrandreg* производится из командной строки. Формат запуска утилиты имеет следующий вид:

ccrandreg [[-test-brng] | [-test-prng [-default-init] | [-pse <path>]]] [-verbose-level <(0-2)>]

где

-test-brng – провести регламентный контроль только модуля БДСЧ;

-test-prng – провести регламентный контроль ПДСЧ;

-default-init – использовать метод инициализации ПДСЧ от ФДСЧ или БДСЧ;

-pse – использовать метод инициализации ПДСЧ от вектора состояния, сохранённого в контексте ключевого контейнера (PSE); path – путь к существующему ключевому контейнеру;

-verbose-level – задание уровня вывода информации о состоянии выполнения тестов:

0 – не выводить дополнительную информацию, только основную для утилиты;

1 – дополнительно выводить ошибки и финальные результаты в процессе тестов (значение по умолчанию);

2 – дополнительно выводить промежуточные результаты каждого применимого теста из пакета NIST [3].

4. СООБЩЕНИЯ ОПЕРАТОРУ

Промежуточные и окончательные результаты работы и возможные ошибки выводятся в консоль построчно, например:

```
ccrandreg -test-prng -pse .\pse1
PRNG Test Passed OK
ccrandreg -test-brng
BRNG Test Passed OK
```

Утилита *ccrandreg* возвращает 0 в случае успешного прохождения проверки и -1 в случае неуспешного. Также утилита выводит в консоль наименование протестированного ДСЧ «PRNG» или «BRNG» и затем текстовое обозначение успешности или неуспешности проверки: «Test Passed OK», если группа применимых к последовательности статистических тестов проведена успешно, т.е. последовательность является случайной; «Test FAILED!», если статистические тесты пройдены не успешно.

В случае ошибок связанных с инициализацией модулей и их функций соответствующие ошибки будут выведены в консоль.

Для вывода в консоль промежуточных результатов выполнения применимых тестов следует вызвать утилиту с флагом "-verbose-level 2". Анализ промежуточных результатов следует проводить изучив документацию по пакету статических тестов NIST STS [3].

ЛИТЕРАТУРА

1. Средство криптографической защиты информации «Крипто-КОМ 3.5». Формуляр. ШКНР.00064-01 30 01. АО «СИГНАЛ-КОМ», 2022.
2. Средство криптографической защиты информации «Крипто-КОМ 3.5». Руководство программиста. ШКНР.00064-01 33 01. АО «СИГНАЛ-КОМ», 2022.
3. National Institute of Standards and Technology (NIST) A Statistical Test Suite for Random and Pseudorandom Number Generators for Cryptographic Applications. Special Publication 800-22. 2001, https://csrc.nist.gov/projects/random-bit-generation/documentation-and-software