**БЕЗОПАСНОСТЬ ИНФОРМАЦИОННЫХ РЕСУРСОВ**

**НА ОСНОВЕ СОВРЕМЕННЫХ ТЕХНОЛОГИЙ**

****

**РЕШЕНИЯ ПО ЗАЩИТЕ КОНФИДЕНЦИАЛЬНОЙ ИНФОРМАЦИИ ОТ НЕСАНКЦИОНИРОВАННОГО ДОСТУПА**

ГЕНЕРАТОР СЛУЧАЙНЫХ ЧИСЕЛ

**«ГСЧ Гроссмейстер»**

**РАЗРАБОТКА И ПРОИЗВОДСТВО ООО «ГРОССМЕЙСТЕР»**



Роберт Кавью:

«Генерация случайных чисел слишком важна, чтобы оставлять её на волю случая»

ГЕНЕРАТОР СЛУЧАЙНЫХ ЧИСЕЛ

«ГСЧ Гроссмейстер»

**НАЗНАЧЕНИЕ**

«ГСЧ Гроссмейстер» – генератор случайных чисел, использующий свойства случайного физического процесса. Разработан и производится для применения в Средствах Криптографической Защиты Информации (СКЗИ) в качестве источника случайных двоичных последовательностей для:

* выработки ключей электронной подписи в соответствии с ГОСТ Р 34.10-2001, ГОСТ Р 34.10-2012;
* выработки ключей симметричного шифрования в соответствии с ГОСТ 28147-89;
* выработки ключей парной связи по схеме Диффи-Хеллмана в соответствии с RFC4357;
* генерации шума.

**ПРИНЦИП РАБОТЫ**

«ГСЧ Гроссмейстер» использует в качестве источника случайных событий шумящий диод, специально разработанный для этих целей.

Работа диода основана на туннельном пробое обратно смещенного (p-n) – перехода. Данный физический процесс носит случайный характер. Микроконтроллер оцифровывает полученную последовательность случайных событий и проводит ее алгоритмическую обработку, которая придает выработанной двоичной последовательности необходимые статистические свойства. Генератор осуществляет постоянный статистический контроль вырабатываемой последовательности.

При производстве «ГСЧ Гроссмейстер» используется специальная технология, которая обеспечивает защиту от несанкционированной перепрошивки микроконтроллера генератора.

«ГСЧ Гроссмейстер» обеспечивает необходимую стойкость защиты информации при использовании СКЗИ, так как гарантирует невозможность восстановления ключевой последовательности методами реверс-инжиниринга.

«ГСЧ Гроссмейстер» в заводском исполнении оснащен микро-разъемом DF12-10DP и обеспечивает встраивание в различные электронные устройства по интерфейсам SPI и I2C. Устройство имеет небольшие геометрические размеры и устойчиво к вибрациям. По заказу возможна комплектация с разъемами USB и Micro-USB.

**ОБЛАСТИ ПРИМЕНЕНИЯ**

* Устройства аутентификации пользователей;
* Устройства электронной подписи;
* Поточные шифраторы;
* Устройства защиты видеоконференций;
* Устройства защиты потока с наружных видеокамер;
* Устройства защиты потока на наружные видео-щиты;
* Устройства защиты от перехвата.

В 2017 году руководством войсковой части 43753-Б утверждено положительное «Заключение о соответствии «ГСЧ Гроссмейстер» «Требованиям к средствам криптографической защиты информации, не содержащей сведения, составляющие государственную тайну» в части инженерно-криптографических требований, требований к анализу программного и аппаратного обеспечения, требований к генераторам случайных чисел для класса КВ».

«ГСЧ Гроссмейстер» в 2016 году удостоен главного приза Национальной отраслевой Премии "За Укрепление Безопасности России" (ЗУБР-2015).

|  |  |
| --- | --- |
| **ВНЕШНИЙ ВИД** |  |
| 151014_1_фото со стороны РР12 | со стороны МК3 |
| Внешний вид «ГСЧ Гроссмейстер» со стороны рабочего разъема  | Внешний вид «ГСЧ Гроссмейстер» со стороны микроконтроллера |

1 - Шумящий диод, 2 - Рабочий разъемDF12-10DP, 3 – Микроконтроллер

**ГЕОМЕТРИЧЕСКИЕ РАЗМЕРЫ**

15 мм. х 13 мм. х 4,5 мм.





ООО «ГРОССМЕЙСТЕР»

Производитель ГСЧ – ООО “Гроссмейстер”, наряду с разработкой и производством СКЗИ, разрабатывает прикладные информационные системы, в том числе в защищенном исполнении.

105187, Москва, ул. Щербаковская, д.53

Тел./факс: +7 (499) 558-38-16, E-mail: gm@gm.ru, <http://www.gm.ru>