



ФЕДЕРАЛЬНАЯ СЛУЖБА  
ПО ИНТЕЛЛЕКТУАЛЬНОЙ СОБСТВЕННОСТИ  
ГОСУДАРСТВЕННАЯ РЕГИСТРАЦИЯ ПРОГРАММЫ ДЛЯ ЭВМ

Номер регистрации (свидетельства):  
2022610829

Дата регистрации: 17.01.2022

Номер и дата поступления заявки:  
2021682348 29.12.2021

Дата публикации и номер бюллетеня:  
17.01.2022 Бюл. № 1

Контактные реквизиты:  
115409, Москва, Каширское ш., 31, НИЯУ  
МИФИ ОУИС, info@mephi.ru

Автор(ы):

Чугунков Илья Владимирович (RU),  
Боронин Ростислав Викторович (RU),  
Маркова Дарья Александровна (RU)

Правообладатель(и):

федеральное государственное автономное  
образовательное учреждение высшего  
образования «Национальный исследовательский  
ядерный университет «МИФИ» (НИЯУ  
МИФИ) (RU)

Название программы для ЭВМ:

«Инструментальное средство для криптоанализа генераторов псевдослучайных чисел на основе регистров сдвига с нелинейными обратными связями»

**Реферат:**

Программа предназначена для определения таблиц замен блоков стохастического преобразования, входящих в состав обратной связи регистра сдвига с задаваемыми параметрами образующего многочлена. Основные функции: задание образующего многочлена, задание разрядности регистров, инвертирование алгоритма зашифрования, определение заполнения таблиц блоков стохастического преобразования в цепи обратной связи на основе известного фрагмента последовательности заданной длины. Область применения: анализ качества построения и заполнения таблиц замен стохастических алгоритмов защиты информации. Тип ЭВМ: IBM PC-совмест. ПК; ОС: Windows 7 и выше.

**Язык программирования:** Delphi 7

**Объем программы для ЭВМ:** 293 МБ