автоматизированных систем обработки информации» показывает, что изучаемые в рамках лекционных, семинарских и особенно практических занятий вопросы осваиваются с большим интересом. Это способствует подготовке курсантов к правильной организации мероприятий по обеспечению безопасности АСОИ и самостоятельной эксплуатации комплексных систем обеспечения безопасности АСОИ, выработке практических навыков работы с основными средствами защиты информации, формирования политики информационной безопасности.

Современный этап развития общества характеризуется возрастающей ролью информационной сферы. Информационная сфера активно влияет на состояние политической, экономической, оборонной и других составляющих национальной безопасности. Поэтому развитие и расширение дисциплины «Методы и средства обеспечения безопасности автоматизированных систем обработки информации» представляется весьма вероятной.

Литература

1. Концепция национальной безопасности Республики Беларусь. Утверждена Указом Президента РБ № 390 от 17.07.2001.

2. Жук А.П. Защита информации: учебное пособие. М., 2017. 359 с.

ПРОГРАММА СТАТИСТИЧЕСКОГО ТЕСТИРОВАНИЯ БИТОВЫХ ПОСЛЕДОВАТЕЛЬНОСТЕЙ

И.В. Дайняк, Н.Г. Киевец, А.М. Ярук

Программа статистического тестирования битовых последовательностей предназначена для исследования сгенерированной каким-либо способом последовательности битов, в том числе полученной от физического генератора случайных чисел, на предмет пригодности к применению в криптографических системах. В основе программы лежат алгоритмы частотных тестов, тестов подпоследовательностей, тестов аппроксимированной энтропии и других тестов, основанных на статистических характеристиках.

Программа статистического тестирования реализована в виде Windows-приложения на языке Си в среде Bloodshed Dev-C++ версии 4.9.9.2. Основными требованиями при реализации программы были: 1) реализация каждого теста в виде отдельной функции с целью возможности его запуска в отдельности; 2) возможность запуска серии тестов с отслеживанием времени, затраченного на каждый тест и тестирование в целом; 3) получение отчета о тестировании, содержащего для каждого задействованного теста описание критерия прохождения и полученных при этом значений вероятности. В программе реализованы 14 основных тестов входной битовой последовательности и 7 двухуровневых тестов подпоследовательностей.

Интерфейс программы реализован на Windows API в виде простого окна с горизонтальным меню, так как на текущем этапе разработки и отладки повышенных требований к программе не предъявляется. Меню содержит набор стандартных операций по работе с файлами (загрузка битовой последовательности из файла и формирование файла отчета с результатами тестирования), группу основных тестов и группу двухуровневых тестов, обеспечивая тем самым двухуровневое тестирование битовой последовательности [1] с отображением результатов непосредственно в окне программы.

Литература

1. Киевец Н. Г. Статистическое тестирование генераторов случайных чисел электронных пластиковых карт // Математические методы в технике и технологиях : сб. тр. Междунар. науч. конф., Санкт-Петербург, Минск, Самара, окт.–нояб. 2017 г. Ч. 2. С. 19–22.

РАЗРАБОТКА ПРОГРАММНОГО КОМПЛЕКСА СТАТИСТИЧЕСКОГО ТЕСТИРОВАНИЯ КРИПТОГРАФИЧЕСКИХ ГЕНЕРАТОРОВ НА ОСНОВЕ МАРКОВСКИХ МОДЕЛЕЙ

М.Ю. Деркач, Ю.С. Харин

Проблема защиты информации затрагивает практически все сферы деятельности человека. Среди способов защиты информации важнейшим считается криптографический [1].