УДК: 004 621:621.3.06

Пискун С.Ж., Хорошко В.А.

ПОСТРОЕНИЕ ПРОФИЛЯ ОПЕРАТИВНОГО ТЕСТИРОВАНИЯ СЛУЧАЙНЫХ ПОСЛЕДОВАТЕЛЬНОСТЕЙ

В данной статье рассмотрено создания профиля отбора случайных последовательностей. Дана оценка количества тестов в зависимости от уровня значимости каждого теста и ошибки первого ряда.

Ключевые слова: криптографическая защита информации, профиль защищенности, случайная последовательность.

Введение. Для построения систем криптографической защиты информации (КЗИ) на основе использования шифров с одноразовой гаммой возникает острая необходимость получения заданного одноразовой гаммой с заданным качеством и в заданное время. Прямые затраты на получения одноразовой гаммой будут являться основным фактором при определении ее стоимости.

Можно выделить две основных этапа получения одноразовой гаммы: непосредственно генерация случайных последовательностей и статистического тестирования с целью выявления и отбраковки неслучайных последовательностей. Нашей задачей является создание профиля отбора последовательностей основанных на статистическом тестировании последовательности множеством тестов T = { i }, t ϵ N с соответствующими им уровнями значимости каждого теста {ά i}. Последовательность считается годной к использованию в случае, если она прошла испытание всеми тестами.

Цель работы. В работе дана оценка количества тестов в зависимости от уровня значимости каждого теста и ошибки первого ряда.

Основная часть. Рассмотри выявления тестов по значимости к ошибке

$$n = [-\acute{\alpha}^{-1} \ln (1-A)] \quad (1)$$

где n- количество тестов; A – ошибка первого ряда; ά – уровень значимости теста.

Исходя из выражения (1) определим среднее значения уровня значимости каждого из тестов

$$\acute{\alpha} = n^{-1} \ln (1-A) \quad (2)$$

Аллегория основана на возможности каждого из тестов t_i, определять искажения α_i из выбранного множества $D = \{d_i\}, j \in N$ искажений в случайны последовательностях. Следует заметить, что множество искажений D и множества тестов T определяется в каждом конкретном случае отдельно.

Для определения профиля отбора последовательностей составляется таблица чувствительности каждого теста на каждый тип искажений (табл.1)

Где S_{ij} - чувствительность *i*-того теста на *J*- ое искажение. В качестве значения чувствительности теста предлагается использовать коэффициент крутизны статистической характеристики K_S, который получается в результате тестирования пакетового количества случайных последовательностей и определяется согласно выражения:

$$K_S = \frac{(N_0 - N_1)}{P_1} \quad (3)$$

где: N_0 - начальное значение количества пропущеных последовательностей при отсутствии искажений; N_1 - количество пропущенных последовательностей при одном прощете

искажений; P_1 - значения процента искажений, при котором количество пропущенных последовательностей равно нулю, ибо в противном случае P_1=1.

Таблица 1

	d_1	d_2	…	d_K
t_1	S_{11}	S_{12}	…	S_{1k}
t_2	S_{21}	S_{22}	…	S_{2k}
⋮	⋮	⋮		⋮
t_n	S_{n1}	S_{n2}	…	S_{nk}

Учитывая, то что значения S_{ij} могут быть отрицательными и нас интересует не абсолютные значения величин S_{ij} , а только разница между ними, следует линейно сместить все значения в таблице в соответствии с выражением $S_{ij} = S_{ij} - S_{\min}$

Следующим шагом является определения значимости каждого из искажений. Для этого введем значение абсолютного значения «определяемости» *j*-го искажения - g_j^d, вычисляемого так

$$g_j^d = \sum_{i-1}^{n} S_{ij}. \tag{4}$$

Значимость искажения можно найти по формуле ;

$$c_j^d = \frac{g_{\max}^d - g_j^d}{\sum_{j=1}^{k}(g_{\max}^d - g_j^d)}. \tag{5}$$

Используя выражения (4) получим множество значимостей искажений $C = \{C_j^d\}$ в котором как минимум одно из значений равно нулю.

Очередным шагом является определение абсолютного значения значимости теста C_i^t, определяемого как

$$C_i^t = \sum_{j=1}^{k} S_{ij} C_j^d. \tag{6}$$

Последующим шагом является определения уровня значимости теста по формуле

$$d_i = d_c \frac{C_j^t}{\sum_{i=1}^{n} C_j^t} \tag{7}$$

Таким образом получаем профиль отбора последовательностей который представляет собой множество тестов $\{t_i\}$ с соответствующими уровнями значимости каждого теста $\{\alpha_i\}$.

В случае отсутствия результатов статистических исследований полученных в ходе эксперимента и невозможности настроить таблицу чувствительности тестов на различные искажения, существует другой способ построения профиля отбора основанный на попарном сравнении субъективных мнений о вероятности тех или иных критериев.

Выводы. Следует заметить, что такой подход, с одной стороны дает возможность построить оптимальный профиль защищенности под конкретную задачу а с другой стороны отобрать множество наиболее пригодных тестов для решений задач.

Надійшла: 15.12.2011

Рецензент: д.т.н., проф. Юдін О.К.