

их количеств в водной фазе (серуме), оставшейся после отделения от нее образовавшейся крошки каучука. При введении кислого порошкообразного наполнителя на основе целлюлозы с дозировкой 7-10% мас. на каучук полная коагуляция латекса проходит без добавления подкисляющего агента.

Анализ физико-механических показателей вулканизатов содержащих, кислый органический порошкообразный наполнитель показал, что порошкообразные наполнители целесообразно вводить в количестве 5-10% мас. на каучук. Резиновые смеси с этим содержанием наполнителя обладают необходимым уровнем вязкости, позволяющим обеспечить их переработку на существующем оборудовании. Физико-механические свойства вулканизатов, содержащих органический кислый порошкообразный наполнитель на основе целлюлозо-содержащего волокна, соответствуют требованиям, предъявляемым к резинотехническим изделиям.

#### Список литературы

1. Никулин С.С., Пугачева И.Н., Черных О.Н. Композиционные материалы на основе бутадиен-стирольных каучуков. – М.: Академия Естествознания, 2008. – 145 с.

### ЭФФЕКТИВНОСТЬ ПРОСТОГО УСЛОЖНЕНИЯ ВИРТУАЛЬНОГО ШИФРОВАНИЯ

Румянцев К.Е., Котенко В.В.,  
Болдырев А.С., Ежов А.И.

*Южный федеральный университет, Таганрог,  
e-mail: virtsecurity@mail.ru, rke2004@mail.ru*

Методы виртуального шифрования впервые предложены в работах В.В. Котенко. Целью исследования являлось определение эффективности простого усложнения примитивных виртуальных шифров пакетом NISTSTS и сравнение полученных результатов с имеющимися аналогами.

Проводилось простое усложнение примитивного варианта виртуального шифрования путём увеличения числа исходных ключей до 10 и преобразования их в элементы дискретной формы выборочного пространства ансамбля виртуализации, определяющие параметры гармонических колебаний, составляющих виртуальный ключ. Результат дискретизации виртуального ключа квантовался на  $N_{quant} = 10^{12}$  уровней:

$$s_i = \sum_{k=0}^{N-1} U_k \cdot \cos \left( 2 \cdot \pi \cdot f_k \cdot \frac{i}{1000,01} + \Theta_k \right),$$

где  $N$  – количество составляющих сложной функции;  $U_k$  – амплитуда  $k$ -й составляющей;  $f_k$  – частота  $k$ -й составляющей;  $\Theta_k$  – фаза  $k$ -й составляющей;  $i$  – номер отсчёта.

Полученная в ходе последующего выделения шума цифрового представления и его кван-

тования на два уровня двоичная последовательность тестировалась пакетом NISTSTS. При этом параметры тестирования задавались так же, как и при тестировании примитивного варианта реализации.

Анализ результатов тестирования и их сравнение с результатами аналогичного тестирования ключевых последовательностей примитивного варианта реализации и ключевых последовательностей криптоалгоритма BBS показывает, что в принципе незначительное увеличение длины исходного ключа от 1 до 4 бит, позволяет обеспечить 74% прохождения тестов даже по правилу 1. Это существенно превосходит показатели тестирования криптоалгоритма BBS и свидетельствует о значительном потенциале виртуального шифрования.

#### Прохождение тестов даже по правилу 1

Генератор	Количество тестов, у которых тестирование прошли более 99% последовательностей	Количество тестов, у которых тестирование прошли более 96% последовательностей
BBS	134 (70,8%)	189 (100%)
Примитивный вариант ВШ	134 (70,8%)	189 (100%)
Простой вариант ВШ	140 (74,1%)	189 (100%)

Приведенные результаты можно рассматривать, как отражение потенциала роста эффективности виртуального шифрования в ходе последующей реализации методов с последовательным и параллельным усложнением виртуальных выборочных пространств ансамбля ключей.

#### Список литературы

1. Котенко В.В. Оптимизация стратегии шифрования на основе виртуализации информационных потоков // Информационное противодействие угрозам терроризма // Науч.-практ. журн. – 2005. – №5. – С. 57-58.

2. Котенко В.В. Принципы кодирования для канала с позиций виртуального представления выборочных пространств ансамблей сообщений и кодовых комбинаций // Информационное противодействие угрозам терроризма // Науч.-практ. журн. – 2004. – №3. – С. 65-71.

3. Котенко В.В. Новый взгляд на условия обеспечения абсолютной недешифруемости с позиции теории информации // Информационное противодействие угрозам терроризма // Науч.-практ. журн. – 2004. – №2. – С. 36-43.

4. Котенко В.В., Румянцев К.Е., Поликарпов С.В., Левендян И.Б. Шифрование с последовательным усложнением виртуальных выборочных пространств ансамблей ключа // Фундаментальные исследования. – 2004. – № 5. – С. 98-98.

5. Котенко В.В., Румянцев К.Е., Поликарпов С.В., Левендян И.Б. Шифрование с параллельным усложнением виртуальных выборочных пространств ансамблей ключа // Фундаментальные исследования. – 2004. – № 5. – С. 97-98.

6. Котенко В.В., Румянцев К.Е., Поликарпов С.В., Левендян И.Б. Шифрование на основе многомерного представления виртуальных выборочных пространств ансамблей ключа // Фундаментальные исследования. – 2004. – № 5. – С. 97-97.