ходимо подчеркнуть, что здесь для исследователя открывается широкое поле деятельности. Например, в качестве этой процедуры могут быть использованы суммирование и произведение результатов девиртуализации каналов. В первом случае алгоритм формирования развернутого ключа принимает вид, представленный выражением (3), во втором – выражением (4)

$$K_r^M(i) = \prod_{j=1}^{M} DVIR_j(K_V^j(t)) : \quad (3)$$

$$K_r^M(i) = \sum_{j=1}^{M} DVIR_j(K_V^j(t)) \quad (4)$$

Реализация приведенных алгоритмов позволила создать программный комплекс шифрования, открывающий возможность обеспечения абсолютной недешифруемости. Исследования, проводимые в направлении совершенствования данного комплекса дают обнадеживающие результаты, представляющий научный и практический интерес. Приведенные результаты получены в ходе исследований при поддержке гранта Министерства образования РФ Т02-03.1-816.

Список литературы

1. Котенко В.В., Поликарпов С.В. Стратегия формирования виртуальных выборочных пространств ансамблей ключа при решении задач защиты информации // Вопросы защиты информации. 2002. №2. С.47 − 52.

ШИФРОВАНИЕ С ПОСЛЕДОВАТЕЛЬНЫМ УСЛОЖНЕНИЕМ ВИРТУАЛЬНЫХ ВЫБОРОЧНЫХ ПРОСТРАНСТВ АНСАМБЛЕЙ КЛЮЧА

Котенко В.В., Румянцев К.Е, Поликарпов С.В., Левендян И.Б.
Таганрогский Государственный Радиотехнический Университет, Таганрог

Актуальность решения проблемы обеспечения абсолютной недешифруемости в современных условиях определяется неуклонным возрастанием роли информационных технологий. В последнее время в этом направлении наметился определенный прогресс. Так, в [1] была предложена стратегия решении данной проблемы на основе виртуализации выборочных пространств ансамблей ключа. Последующие исследования позволили получить ряд вариантов реализации данной стратегии. Одним из таких вариантов является шифрование, основанное на последовательном усложнении виртуальных выборочных пространств ансамблей ключа. Его основу составляет рекуррентный алгоритм (1) формирования виртуального ключа:

$$K_V^j(t) = VIR_j(DVIR_{j-1}(K_V^{j-1}(t))), j = 1...N \quad (1)$$

где

$VIR_j(\,.\,)$ – процедура виртуализации;

$DVIR_j(\,.\,)$ – процедура девиртуализации;

j – порядок уровня усложнения.

Полученный алгоритм предполагает многократную последовательную виртуализацию и девиртуализацию ансамбля ключа. При этом на каждом шаге виртуализации в качестве исходного ключа выступает результат девиртуализации виртуального ключа, полученного на предыдущем шаге. Начальным условием $DVIR_0(K_V^0(t))$ функционирования данного алгоритма является исходный ключ $K_{nd}(i)$, формируемый на основании заданных ключевых данных K_d:

$$DVIR_0(K_V^0(t)) = K_{nd}(i) . \quad (2)$$

Развернутый ключ $K_n^N(i)$ формируется путем девиртуализации виртуального ключа, полученного на конечном N-ом шаге усложнения:

$$K_n^N(i) = DVIR_N(K_V^N(t)) \quad (3)$$

На основании приведенного подхода было получено семейство способов шифрования с последовательным усложнением виртуального ключа, открывающих возможность обеспечения абсолютной недешифруемости. Реализация данных способов позволила создать программный комплекс шифрования, обладающий уникальными возможностями. Экспериментальные исследования показали высокую надежность и эффективность данного комплекса.

Приведенные результаты получены в ходе исследований при поддержке гранта Министерства образования РФ Т02-03.1-816.

Список литературы

1. Котенко В.В., Поликарпов С.В. Стратегия формирования виртуальных выборочных пространств ансамблей ключа при решении задач защиты информации // Вопросы защиты информации. 2002. №2. С.47 − 52.

ЭЛЕКТРОХИМИЧЕСКАЯ РАЗМЕРНАЯ ОБРАБОТКА ПОЛИГОНАЛЬНЫМ КАТОДОМ

Котляр Л.М., Миназетдинов Н.М., Хайруллин А.Х.
Камский государственный политехнический институт, Набережные Челны

Электрохимическая размерная обработка металлов – один из современных методов изготовления деталей из металлов и сплавов с заданной формой, размерами и качеством поверхности. Метод основан на принципе локального растворения анода – обрабатываемой заготовки в проточном электролите. Роль катода – обрабатывающего инструмента выполняет электрод с заданной геометрической формой поверхности. Протекание электрохимических процессов обеспечивается прокачкой раствора электролита через межэлектродный промежуток (МЭП) с целью выноса из зоны обработки продуктов реакции (газа, шлама) и выделившегося тепла