АЛГОРИТМ ЧАСТОТНО-ВРЕМЕННОГО КОДИРОВАНИЯ ИНФОРМАЦИИ В СЕТИ ПРЕДПРИЯТИЯ

Ю.С. Перченкова

Белорусский государственный университет информатики и радиоэлектроники
Институт информационных технологий
г. Минск, Республика Беларусь

Митюхин А. И. – доцент

Представлен алгоритм защиты информации передаваемой по сети предприятия. Решение задачи информационной защиты осуществляется путем использования эффективного кодирования в частотной области, зональной фильтрации трансформант и последующего их кодирования псевдослучайным кодом во временной области.

В работе рассматривается алгоритм защиты $1D(2D)$ информации передаваемой (хранимой) в сети предприятия, где предъявляются повышенные требованиями к информационной безопасности. Пусть источника информации в сети формирует $1D$ сигнал. Во времени он описывается функцией, отображающей амплитуду $g(x)$ и время x. Так как добавление пространственной координаты принципиально не меняет вычислительную структуру алгоритма, далее рассматривается одномерная функция $g(x)=(g(0),...,g(N-1))$, N – число отсчетов сигнала (отражает дискретное время). Перехват информации значительно усложняется, если временные затраты T на распознавание, различение, идентификацию, декодирование наблюдаемого процесса в сети превышают реальное время N. Первый шаг предлагаемого алгоритма решает задачу уменьшения времени нахождения в открытой сети. Для этого производится кодирование процесса на выходе источника с целью декорреляции данных. Операция декорреляции реализуется путем перехода к описанию сигнала в частотной области, т.е. получения функции $\hat{g}(v)=(\hat{g}(0),...,\hat{g}(N-1))$, v – частота. В общем виде функция $\hat{g}(v)$ определяется с помощью линейного унитарного преобразования на поле комплексных чисел, для которых существует внутреннее произведение. В работе применялось дискретное косинусное преобразование (ДКП), которое является наиболее близким к оптимальному преобразованию Карунена-Лоева [1] с точки зрения наилучшей декорреляции. Ядро ДКП в N - мерном пространстве имеет вид [1]

$$c_{nv}=\sqrt{\frac{2}{N}}\cos\left(\frac{\pi n v}{N}\right), v=0,1,...,N-1.$$

Уменьшение времени активного пребывания в сети достигается путем применения фильтрации к трансформантам $\hat{g}(v)$, попадающих в зону со значениями их максимальной дисперсии.

В работе приведены результаты экспериментальных исследований (на базе приложения Matlab) оценки временного выигрыша нахождения в сети и различия форм спектров кодовых слов псевдослучайного m - кода [2] длиной $n=127$ над полем $GF(2)$ Для этого были выбраны все 9 неприводимых проверочных полиномов, порождающих m - код. Для информационной последовательности состоящей из $N=64$ отсчетов достаточно было передавать по сети $k=5\div7$ трансформант из $N=64$. Это же значение k соответствовало параметру размерности кода. Передача осуществлялась при условии полного восстановления на приемной стороне исходных данных после выполнения обратного преобразования. Кодирование трансформант постоянной энергии, в рассматриваемом случае бинарных векторов длиной k, приводило к расширению спектра передаваемого сигнала. Тем самым снижалась спектральная плотность мощности сигнала. Вероятность правильного декодирования сигнала в канале перехвата уменьшалась до величины $\leq 10^{-3}$.

Список использованных источников:

1. Jähne, B. Digital Image Processing / B. Jähne. – Springer-Verlag, Berlin, Heidelberg, 2005, 584 p.

2. Ipatov, V. Spread Spectrum and CDMA. Principles and Application / V. Ipatov. – John Wiley & Sons, Ltd, 2005, 488 p.

3. Mitsiukhin, A. Efficient Description of the Boundary of the Object under Observation / A. Mitsiukhin. – Proceedings 59th IWK TU-Ilmenau, 2017. Db thueringen.de/rsc/viewer/dbt_derivate_00039296/ilm1-2017iwk-018.pdf? page=6.