УДК 681.3.06:519.248.681

КОСТЕНКО П. Ю., АНТОНОВ А. В., КОСТЕНКО Т. П.

АНАЛИЗ ЭФФЕКТИВНОСТИ ОБЕСПЕЧЕНИЯ ИНФОРМАЦИОННОЙ СКРЫТНОСТИ В КОММУНИКАЦИОННЫХ СИСТЕМАХ И СЕТЯХ МЕТОДАМИ ХАОТИЧЕСКОЙ ДИНАМИКИ

Проанализирована информационная скрытность в коммуникационных системах и сетях, которая обеспечивается методами хаотической динамики. В отличие от традиционных методов решения задачи защиты информации, основанных на «вычислительной сложности» криптоанализа, скрытность предложенного в работе метода обусловлена неоднозначностью обращения хаотического отображения. Рассмотрены и определены характеристики стойкости метода к некоторым видам криптоатак.

В результате широкого распространения коммуникационных систем и сетей выросла потребность в решении задач конфиденциального обмена информацией — обеспечения информационной скрытности, защиты информации от несанкционированного доступа и других нарушений. Решение этих задач возможно различными средствами криптографической защиты информации. Совокупность средств криптографической защиты информации, а также необходимой ключевой, нормативной, эксплуатационной и другой документации (в том числе и определяющей меры безопасности), обеспечивающих необходимый уровень безопасности информации, обрабатываемой и (или) передаваемой в коммуникационных системах и сетях составляют криптографическую систему (криптосистему). В более узком математическом смысле под криптосистемой $S = \{X, Y, K_e, K_d, f_e, f_d\}$ понимают некоторые однозначные преоб-

разования $f_e: X \times K_e \to Y$ и $f_d: Y \times K_d \to X$ информации, определенные на множестве исходных состояний X (открытый текст), конечных состояний Y (шифрованный текст) и ключей K_e и K_d. Состояние $x \in X$ представляет обрабатываемое сообщение. В компьютерной криптографии множества начальных и конечных состояний, а также ключей заданы бинарным алфавитом $\{0, 1\}$, а преобразования f определяются программой (алгоритмом), реализуемой машиной Тьюринга.

В современной криптографии задача совершенствования традиционных и поиска новых подходов к защите информации, созданию перспективных криптосистем, обеспечивающих максимально высокий уровень ее защиты, остается актуальной.

Один из новых подходов к совершенствованию криптосистем основан на их рассмотрении с позиций нелинейной хаотической динамики [1, 2]. При этом можно единообразно оценить, как существующие криптосистемы, так и вновь разрабатываемые. Кроме того, есть основания утверждать, что решения задач защиты информации в коммуникационных системах и сетях с использованием методов хаотической динамики могут оказаться достаточно эффективными, с точки зрения их криптостойкости. Разработке криптосистем с позиций хаотической динамики посвящены работы зарубежных авторов, например [3–5].

Рассмотрим криптографические системы с открытым ключом [6]. Их криптостойкость основана на «вычислительной сложности» криптоанализа теоретико-числовых алгоритмов. Однако «вычислительная сложность» зависит от развития математических методов решения теоретико-числовых задач (например: разложения чисел на простые множители, дискретного логарифмирования), что делает эти системы потенциально уязвимыми [7–9]. Поэтому разработка потенциально стойкой криптосистемы с открытым ключом в современной криптографии методами нелинейной динамики представляется актуальной задачей.

Цель работы. В настоящее время стандартом шифрования, получившим наибольшее признание и распространение, является RSA [10]. Он используется для обмена ключами, создания цифровой подписи и шифрования данных. Применяются также DSS [11] (цифровая подпись), схемы Эль-Гамаля [12] (шифрование данных), Шнорра [13], криптопреобразования в группе точек эллиптических кривых и др. Дискретные преобразования, применяемые в некоторых из них, можно встретить в хаотической динамике.

В работе предложена криптосистема с открытым ключом функционирующая, как нелинейная хаотическая динамическая система. Ее специфика состоит в том, что криптопреобразования выполняются над действительными числами. Секретность системы основана на неоднозначности обращения хаотического отображения (оценки его порядка) в случае незнания личного клю-