ПОВЫШЕНИЕ НАДЕЖНОСТИ КРИПТОГРАФИЧЕСКОЙ ЗАЩИТЫ С ИСПОЛЬЗОВАНИЕМ ВРЕМЕННЫХ ХАРАКТЕРИСТИК ПРОЦЕССА ШИФРОВАНИЯ

Е.А. КАРАСИК

Криптографическая защита является в настоящее время важным аспектом обработки информации. Стойкость большинства применяемых шифров основывается на секретности ключа, используемого для расшифровки, сам же шифрующий алгоритм предполагается известным. Следовательно, криптосистема поддается взлому путем перебора ключей, причем технические возможности для этого со временем расширяются, а при использовании в качестве ключа осмысленных комбинаций символов, например, вводимых пользователем паролей, эффективность перебора возрастает многократно. Криптостойкость повышается последовательным применением нескольких различных, в том числе динамически сменяемых ключей либо комбинированием нескольких способов генерации составного ключа. Эффективным средством противодействия могло бы стать также принципиальное ограничение минимального времени одной попытки предъявления подбираемого ключа.

Автором предлагается следующий подход к повышению надежности криптографических систем: в состав комбинированного ключа шифрования включается элемент, генерируемый способом, зависящим от времени, т.е. ключ шифрования с заданной временной периодичностью, меняется по секретному алгоритму. Главное свойство этого алгоритма заключается в защищенности от взлома и воспроизведения. Этого можно достичь несколькими способами: использование сложных математических алгоритмов, понижающих читаемость дизассемблированного кода, а также использование функций реального времени в качестве аргументов алгоритма, тем самым, усложняя отладку запущенного приложения.

В работе рассматриваются варианты применения данного подхода к практическим задачам, а также различные подходы к усложнению взлома секретного алгоритма.