ИССЛЕДОВАНИЕ ЭПК РАЗЛИЧНЫХ ПРОИЗВОДИТЕЛЕЙ

П.Б. Капля, Н.Г. Киевец, А.И. Корзун

Значительно повысить информационную безопасность позволяет использование смарт-карт. Смарт-карты характеризуются следующими преимуществами перед картами с магнитной полосой: большей емкостью памяти; более надежная система защиты; осуществление передачи информации в зашифрованном виде; большей долговечностью

Архитектура смарт-карт состоит из следующих структурных блоков: центральный процессор (ЦП); оперативная память (ОЗУ); постоянное запоминающее устройство (ПЗУ); электрически программируемое постоянное запоминающее устройство (ЭСППЗУ); сопроцессор.

Использование процессора в смарт-картах позволяет обрабатывать хранящуюся и поступающую в карту информацию. Кроме этого наличие сопроцессора разгружает ЦП от трудоемких операций криптозащиты, что дает возможность достижения высокого быстродействия смарт-карт при обработке данных и реализации криптографических алгоритмов. Надежность и безопасность смарт-карт обусловлена тем, что она может контролировать доступ к информации, которая содержится в ее памяти.

Смарт-карты позволяют реализовывать процедуры аутентификации и идентификации пользователя ПК, автоматизированных рабочих мест и диспетчерских устройств. Реализация процедуры аутентификации осуществляется посредством ввода PIN-кода. Число попыток ввода неверного PIN-кода, как правило, фиксировано, и при превышении числа попыток карта блокируется. Если PIN-код введен верно, то карта путем обмена криптограммами по определенному протоколу получает у системы доступ к локальным или сетевым ресурсам.

Как было отмечено выше, смарт-карты позволяют реализовывать различные процедуры шифрования данных. Однако в современной литературе отсутствуют сведения о скорости выполнения процедур по различным криптоалгоритмам. Вследствие различных подходов проектировщиков карты различных производителей могут выполнять процедуры шифрования по одним и тем же стандартам с различным уровнем качества.

в работе рассматриваются методы оценки качества шифрования картами различных производителей. Для сравнения результатов разработана методика и аппаратно-программный комплекс оценки процедур шифрования картами различных производителей. Исследовано влияние длины пакетов данных и времени выполнения процедур.